

Trabajo elasticsearch

**Por Juan Jose Marín Molina
IES Cura Valera
2ºASIR**

índice

Objetivo del proyecto.....	3
¿Qué es Elasticsearch?.....	3
Información sobre elasticsearch.....	3
Para que se utiliza Elasticsearch.....	3
Ventajas de Elasticsearch.....	3
Desventajas de Elasticsearch.....	3
Donde se creó Elasticsearch.....	4
¿Quién va a usar Elasticsearch?.....	4
¿Qué es Kibana?.....	4
¿Qué puede hacer Kibana?.....	4
Precios.....	5
Estándar.....	5
SEGURIDAD.....	5
OBSERVABILIDAD.....	5
BÚSQUEDA.....	5
SOPORTE.....	6
Oro.....	6
SEGURIDAD.....	6
SOPORTE.....	6
Platino.....	6
SEGURIDAD.....	6
OBSERVABILIDAD.....	7
BÚSQUEDA.....	7
SOPORTE.....	7
Enterprise.....	7
SEGURIDAD.....	7
OBSERVABILIDAD.....	7
BÚSQUEDA.....	8
SOPORTE.....	8
Bibliografía.....	8
Solucionar error memoria virtual para maquina docker.....	8
Instalación de elasticsearch con docker.....	9
Instalación de kibana.....	11
Instalando en fleet.....	18
Ver con más detalle la información.....	23
Cómo añadir nuevas máquinas a la flota y asignarles un agente de elastic.....	29
Windows.....	29
Ubuntu.....	31
Como instalar agente standalone.....	35
Conclusión.....	39

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 también los intereses futuros para las empresas y para ti mismo.

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.

Aparte, el programa proporciona:

- Agrupación y alta disponibilidad.
- Potente búsqueda y análisis.
- Visualización y dashboards de datos.
- Seguridad del stack.

SEGURIDAD

- Alertas, incluidos motor de detección y reglas pre-diseñadas.
- 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.

- Cuentas 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, a parte de tener todo lo incluido en la suscripción Estándar, incluye además:

- 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, con todo incluido de las dos versiones anteriores, añade:

- 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 Monitoring2 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, a parte de tener todo lo anterior, incluye:

- 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.

Bibliografía

-*Elasticsearch*. (s/f). Elastic. Recuperado el 18 de junio de 2024, de <https://www.elastic.co/es/elasticsearch>

-Wikipedia contributors. (2024, mayo 10). *Elasticsearch*. Wikipedia, The Free Encyclopedia. <https://en.wikipedia.org/w/index.php?title=Elasticsearch&oldid=1223163717>

Solucionar error memoria virtual para maquina docker

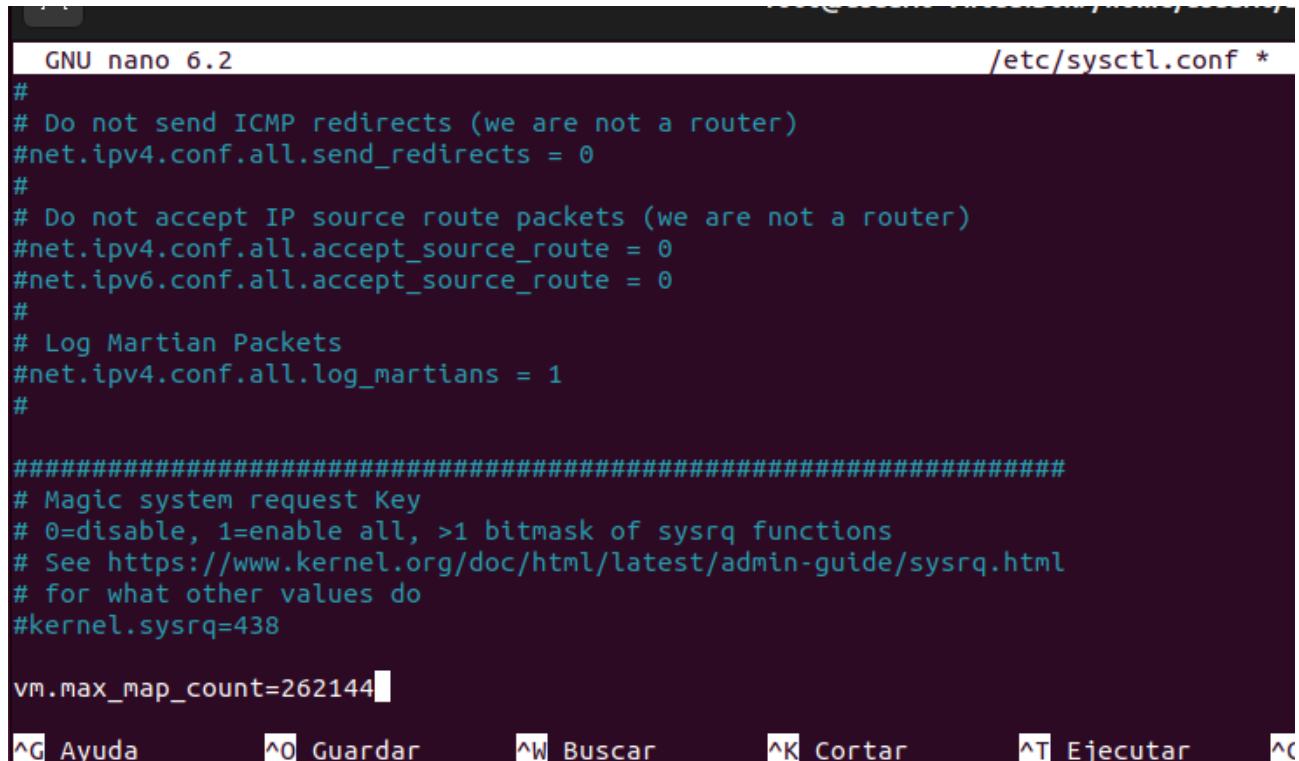
Debemos ejecutar el siguiente comando como administrador:

```
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 al final del mismo:

```
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
```

Una vez hecho lo anterior, guardamos el archivo para que de esta forma, al reiniciar el programa, no debamos meter el comando nuevamente.

Instalación de elasticsearch con docker

Empezaremos con un cluster de un solo nodo, partiendo de que ya tengamos instalado docker en nuestra máquina, con ello, iniciaremos creando una red para elasticsearch usando el siguiente comando en la consola: `docker network create elastic`.

En mi caso, me daba problemas y acabé usando la red host, pero solo hay que usarla si la red es segura, si no, no es recomendable usarla.

```

root@usuario-VirtualBox: /home/usuario/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 elasticsearch 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:

```

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):
eyJ2ZXIiOiI4LjExLjQlCjZhZHIiOlstMTcyLjE4LjAuMjo5MjAwIl0sImZnciI6IjMyODFjMjQwMTFmMGQ4MTY0MWU5NzE1YTcwNjE2ZmQ4ZmM4MDRhYzUwYjUxMzE3YWMzZDc3ZWmxYjdmmMDQzNDQiLCjRZXkiOjJ40EV0LW93QnYzTVVjT3VvaGEwVTp2N3lpYkJpQ1RBuZJzb2NxMDRGWFR3In0=

[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):
eyJ2ZXIiOiI4LjExLjQlCjZhZHIiOlstMTcyLjE4LjAuMjo5MjAwIl0sImZnciI6IjMyODFjMjQwMTFmMGQ4MTY0MWU5NzE1YTcwNjE2ZmQ4ZmM4MDRhYzUwYjUxMzE3YWMzZDc3ZWmxYjdmmMDQzNDQiLCjRZXkiOjJ5Y0V0LW93QnYzTVVjT3VvaGEyCDppcmLTZFVhcVjXRzJlLU1EVzBQMHBnIn0=

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 elasticsearch, 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#
```

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, debemos hacer primero 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  
b032cb80beba: 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 configuración 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/kiban
```

<http://0.0.0.0:5601/>

```
i Kibana has not been configured.  
Go to http://0.0.0.0:5601/?code=652535 to get started.
```

A partir de aquí, tendremos que pegar el token que obtuvimos al instalar elasticsearch.



Configure Elastic to get started

Enrollment token

```
eyJ2ZXIiOiI4LjEyLjliLCJhZHliOlsiMTcyLjE4LjAuMjo5MjAwIi0slmZ  
ncil6ImVjZDYxNjAxMTAzNjEyMWIzMWU2NWU1MjRINDczODEx  
NGJmYzYxYzFhODgyOTRkY2I4ZmNkNjEyMGI0NGNiMzMlCJr  
ZXkiOiJ3UXVHcjQ0QIBxUkl0NjEwUjhUMzpPaktxN3F2bIR0NktY  
bmRJSnNsYWdnln0=
```

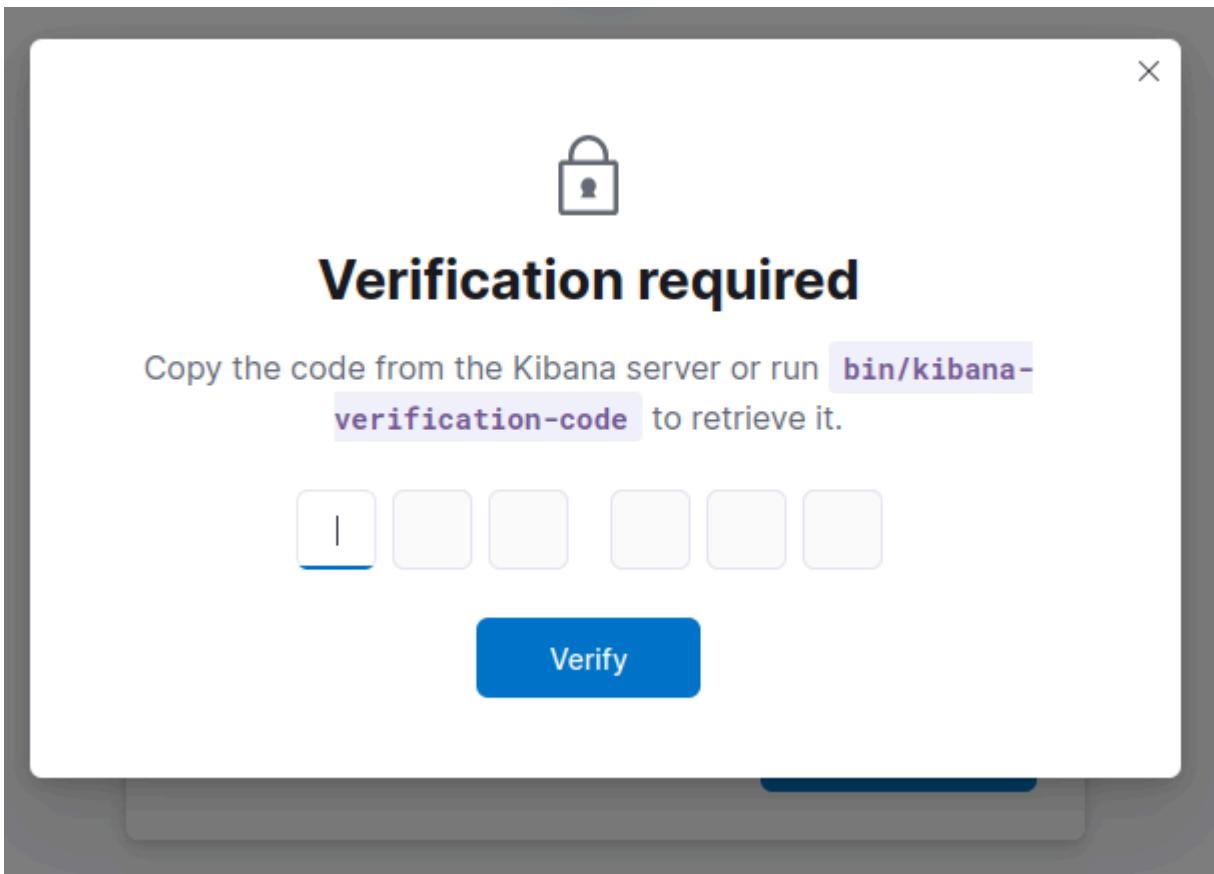
Connect to <https://172.18.0.2:9200>

Configure manually

Configure Elastic

Cuando tengamos en la pantalla una imagen similar a la anterior, pulsamos configure elastic para continuar.

Tras lo anterior, nos pedira un codigo que debemos sacar de la máquina del kibana:

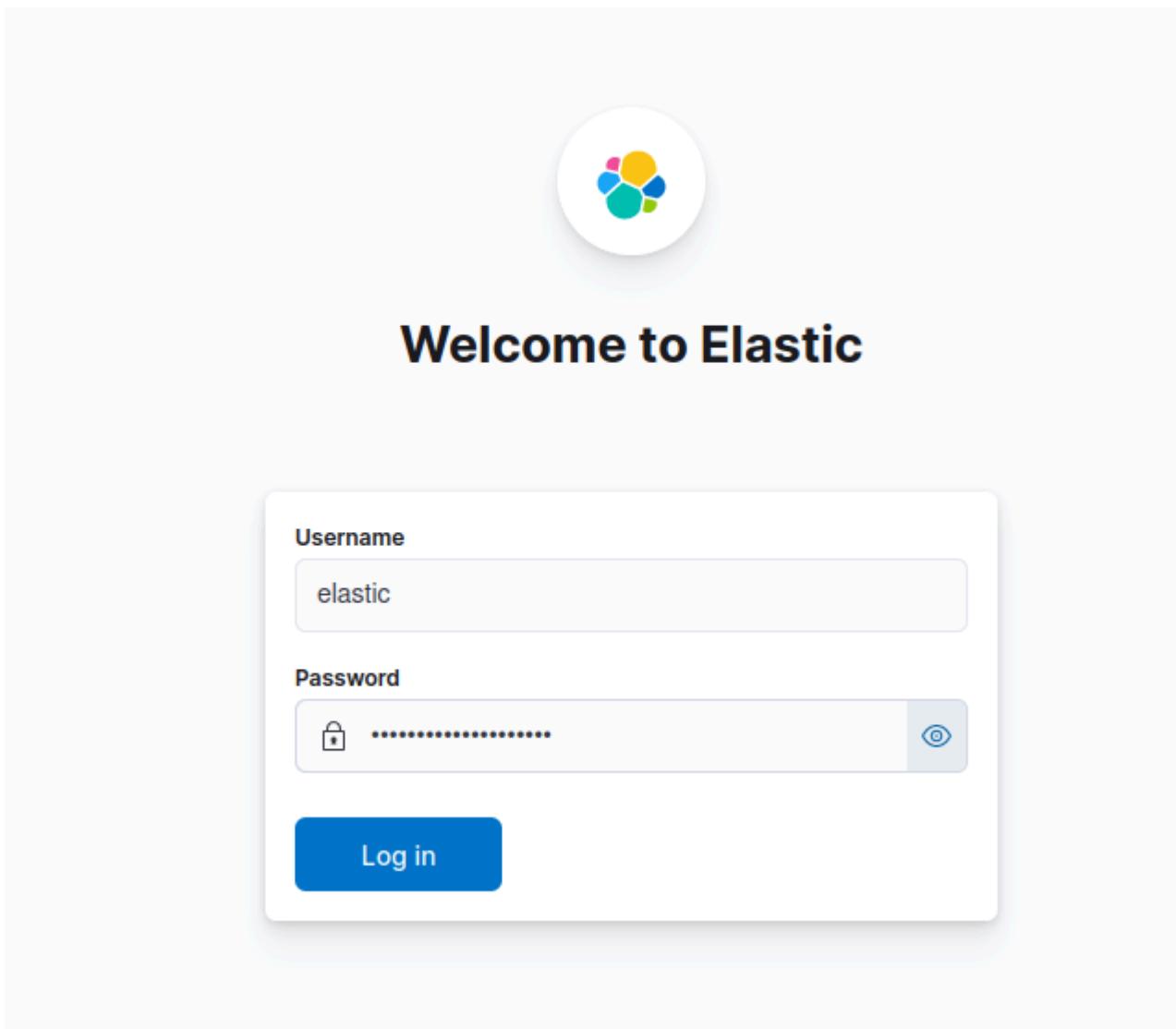


Entramos a la máquina del kibana y usamos el comando:
`bin/kibana-verification-code`

```
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 pondremos el código y este se configura automáticamente. Una vez configurado, para iniciar sesión usaremos el usuario elastic y la contraseña de elasticsearch.



Cuando hayamos escrito el usuario y contraseña pulsaremos “log in”. En nuestro caso guardaremos la contraseña en el navegador. A partir de aquí, se nos dará la bienvenida y nos darán la opción de 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 esta situación, le daremos a explorar por nuestra cuenta e 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 este momento, añadiremos los datos que aparecen abajo, pero también podemos mirar el entorno de prueba de la demo.

▼ 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

Si hemos hecho todo bien hasta el momento, simplemente le daremos a add data y cuando se descarguen ya podremos explorar los datos de prueba. Pulsando en “view data” y empezaremos a explorar los datos de prueba. Aquí, nos aparecerán varias opciones, nosotros le daremos a dashboard

▼ Other sample data sets

Sample eCommerce orders

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

[Remove](#) [View data](#)

Sample flight data

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

[Remove](#) [View data](#)

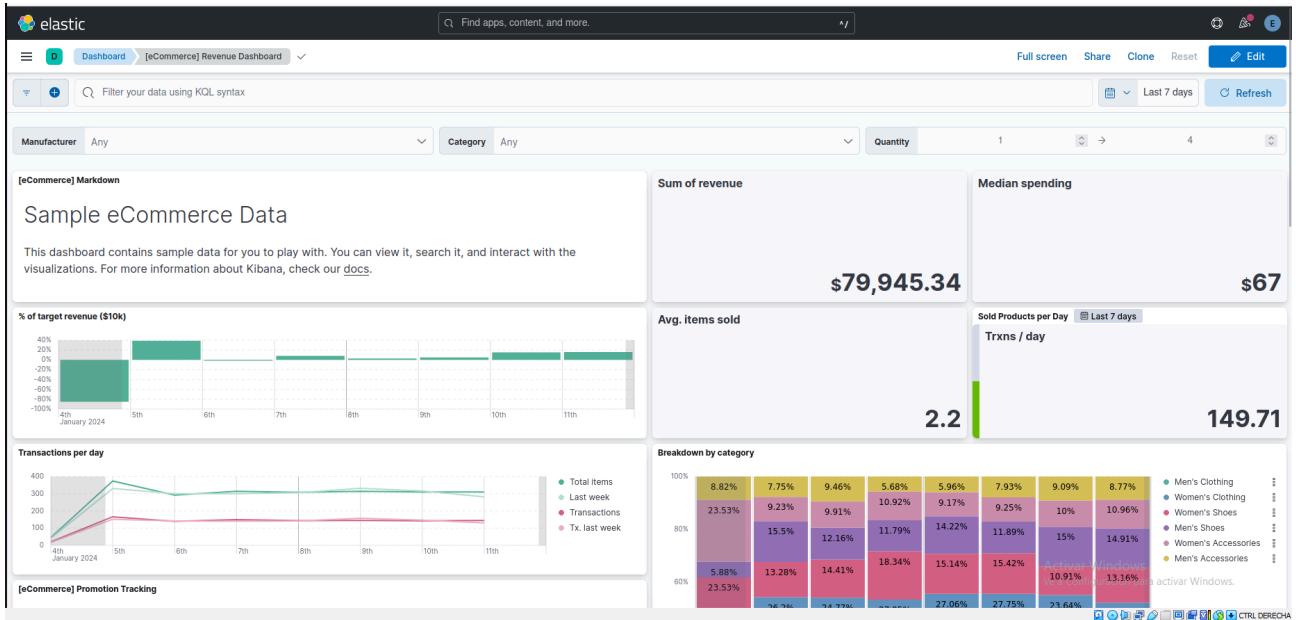
Sample web logs

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

[Remove](#) [View data](#)

Activar \ Ve a Config

Tras lo anterior, nos aparecerá algo como esto:



Y podremos ver el dashboard de los datos de prueba.

Instalando en fleet

Iremos a la pestaña fleet del menú. Creando primero 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=AAEAAWVsYXN0aWMvZmx1ZXQtc2VydmVyL3Rva2VuLTE3MDY0NzYzNzk2NDQ6UdvVzNCbFVTWG1QanLCVHVfVElqUQ \
--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=AAEAAWVsYXN0aWMvZmx1ZXQtc2VydmVyL3Rva2VuLTE3MDY0NzYzNzk2NDQ6UdvVzNCbFVTWG1QanLCVHVfVElqUQ \
> --fleet-server-policy=fleet-server-policy \
> --fleet-server-es-ca-trusted-fingerprint=46895f502781ac0ec7e4af09499c52aa87491c77c9a0d7b9e839a366b412da \
> --fleet-server-port=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... [4m10s] {"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... [5m40s] {"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#
```

```
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#
```

Una vez terminado, nos saldrá esto, a lo que 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 elasticsearch, mientras que en la sección fleet, vemos que está funcionando bien y recoge datos.

The screenshot shows the Fleet management interface. At the top, there's a banner with a green checkmark icon and the text "Fleet Server connected". Below it, a message says "You can now continue enrolling agents with Fleet." with a button "Continue enrolling Elastic Agent". The main title is "Fleet" with the subtitle "Centralized management for Elastic Agents.". Below the title, there are tabs: "Agents" (which is selected), "Agent policies", "Enrollment tokens", "Uninstall tokens", "Data streams", and "Settings". A yellow callout box says "Set up encryption key" with a note: "An encryption key will make your environment more secure. Click [here](#) to learn how to set up an encryption key." There's a "Dismiss" button. At the top right are buttons for "Agent activity", "Add Fleet Server", and "Add agent". Below that is a search bar with placeholder "Filter your data using KQL syntax" and filter options: Status (Healthy 1), Tags (0), Agent policy (2), and Upgrade available. It also shows "Showing 1 agent" and a "Clear filters" button. The main table lists one agent: "Healthy" host "usuario-virtualbox" with "Fleet Server Policy rev. 1", CPU usage "0.85 %", Memory "240 MB", Last activity "29 seconds ago", Version "8.12.0", and Actions. At the bottom, it says "Rows per page: 20" and has navigation arrows.

Ahora probaremos a añadir alguna integración, en nuestro caso añadiremos una que mide el tráfico de red de Iptables, para ello iremos a la pestaña agent policies y entramos a la política de nuestra flota.

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](#)

Management

Pulsamos “add integrations” y una vez dentro buscamos iptables.

Integrations

Choose an integration to start collecting and analyzing your data.

Browse integrations [Installed integrations](#)

All categories	348
APM	1
AWS	36
Azure	22
Cloud	7
Containers	15
Custom	39

iptables

 **Iptables**
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 left is a penguin icon. To its right is the title 'Iptables' and a button labeled 'Elastic Agent'. Below the title are three tabs: 'Overview' (underlined), 'Settings', and 'API reference'. On the far right, it says 'Version 1.15.1' and has a blue button with a plus sign and the text 'Add Iptables'. Underneath the tabs, there's a section titled 'Iptables Integration Logs' with a brief description: 'This is an integration for `iptables` and `ip6tables` logs. It parses logs received over the network via syslog (UDP), read from a file, or read from journald. Also, it understands the prefix added by some Ubiquiti firewalls, which includes the rule set name, rule number, and the'. To the right of this text is a 'Screenshots' section showing two small preview images of log data.

En nuestro caso, dejaremos los ajustes por defecto, para así de esta forma, ya tener la integración lista para funcionar.

The screenshot shows the 'Add Iptables integration' configuration page. At the top left is a penguin icon and a 'Cancel' link. The main title is 'Add Iptables integration'. Below it, a sub-instruction says 'Configure an integration for the selected agent policy.' A step indicator '1 Configure integration' is shown. The configuration area is divided into sections: 'Integration settings' (with a note: 'Choose a name and description to help identify how this integration will be used.'), 'Integration name' (set to 'iptables-1'), 'Description' (optional, empty), and 'Advanced options' (link). Below this is a section for collecting logs: 'Collect iptables application logs (input: udp)' (checked) and 'Collect iptables syslog logs (Beta)' (unchecked). The 'Syslog Host' is set to 'localhost'. A note explains: 'The interface to listen to UDP based syslog traffic. Set to 0.0.0.0 to bind to all available interfaces.' The 'Syslog Port' is set to '9001'. A note for this field states: 'The UDP port to listen for syslog traffic. Ports below 1024 require Elastagent to run as root.' At the bottom right are buttons for 'Activar Windows', 'Cancel', 'Preview API request', and a large blue 'Save and continue' button.

Ver con más detalle la información

Si entramos a los detalles, podemos ver que integraciones tiene instaladas el agente, siendo el agente de la flota, quien tiene instalada la integración de servidor de flota y la de monitorear la información del sistema. Además, en nuestro caso tenemos la integración para ver los datos del sistema, teniendo la opción para verlo con más detalle de irnos a la pestaña dashboards.

The screenshot shows the 'Agent details' tab selected for the agent 'usuario-virtualbox'. The page is divided into two main sections: 'Overview' on the left and 'Integrations' on the right.

Overview:

- 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: -

Integrations:

- system-2 (represented by a heart rate monitor icon)
- fleet_server-1 (represented by a network cluster icon)

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 the placeholder 'Search... syntax' and a large number '33.2'. A link 'go back to System c' is visible.

Dashboards

Search...		Recently updated	Tags	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.				
	Managed Security Solution System			
[System Windows Security] Group Management Events		29 minutes ago		
<input type="checkbox"/> Group management activity.				
	Managed Security Solution System			

Aquí seleccionaremos el que nos interesa, para este caso iremos a métricas del sistema.

The screenshot shows the Grafana interface with the title "[Metrics System] Host overview". It has two tabs: "Managed" (selected) and "System". Below the tabs, it says "Overview of host metrics". The main area is titled "[Metrics System] Overview" and "Overview of system metrics".

Host overview:

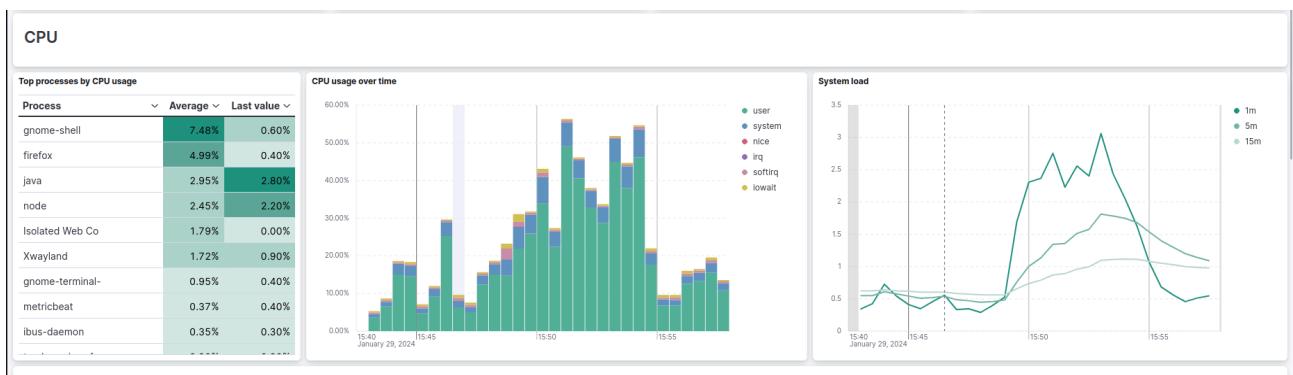
- CPU used: 9.50%
- Memory used: 87.10%
- Disk used: 50.07%
- Outbound traffic per second: 3.62MB (Total transferred 108.52MB)
- Processes: 21
- Memory used in bytes: 3.32GB (Total Memory 3.82GB)
- 5m load: 1.09
- Inbound traffic per second: 96.83MB (Total transferred 2.84GB)

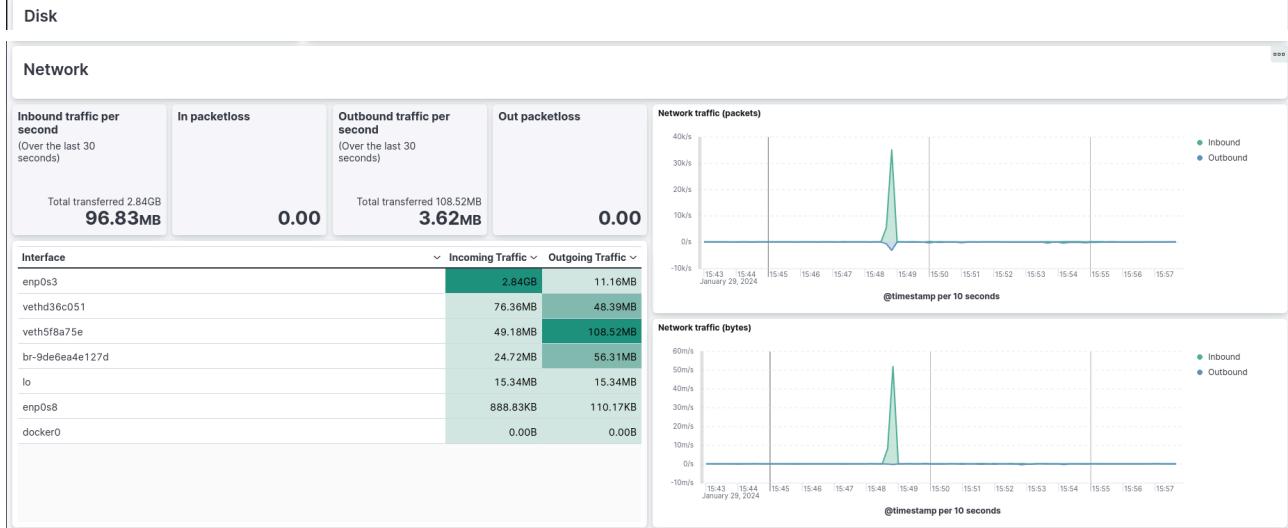
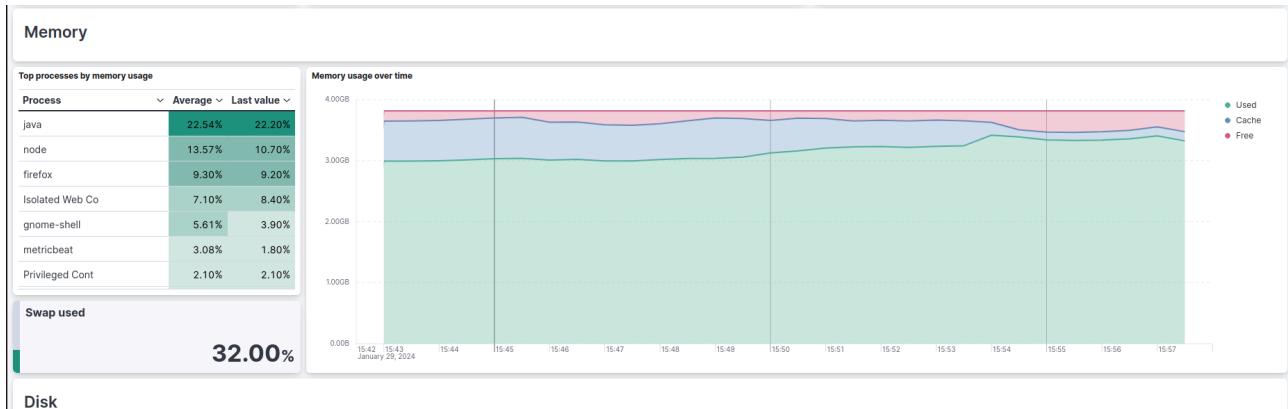
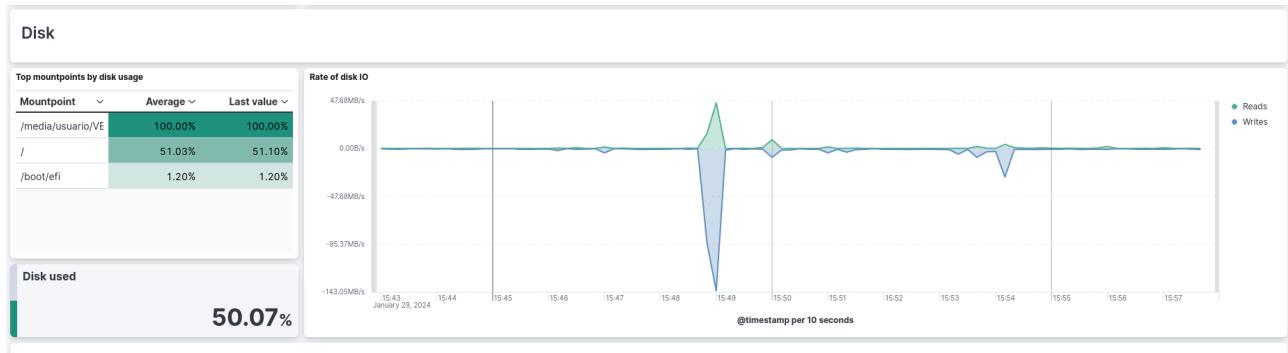
CPU:

- Top processes by CPU usage:

Process	Average	Last value
gnome-shell	7.48%	0.60%
firefox	4.99%	0.40%
- CPU usage over time: A stacked bar chart showing CPU usage by user, system, nice, irq, softirq, and lowlat.
- System load: A line chart showing 1m, 5m, and 15m load averages over time.

Como vemos, nos pone 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, etc... Y si bajamos, veremos los distintos apartados con más detalle:





Ahora veremos un poco la pestaña de fleet, donde 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

② 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							
<input type="checkbox"/>	Status	Host	Agent policy	CPU	Memory	Last activity	Version
<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, 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						
<input type="button" value="Reload"/>	<input type="button" value="Create agent policy"/>					
Name	Description	Last update...	Agents	Integrations	Actions	
Fleet Server Policy rev. 1	Fleet Server policy generated by Kibana	Jan 29, 2024	1	2	< 1 >	
Agent policy 1 rev. 3		Jan 29, 2024	0	2	< 1 >	

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						
<input type="button" value="Create enrollment token"/>						
Name	Secret	Agent policy	Created on	Active	Actions	
Default (00a0d92c-8c54-4d30-b9a2-16db...)	② Fleet Server Policy	Jan 29, 2024	●	< 1 >	
Default (645cf378-7fc8-4150-9c2b-771d78...)	② Agent policy 1	Jan 29, 2024	●	< 1 >	

Rows per page: 20 < 1 >

Por otro lado, 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.

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 qué integración:

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

Filter data streams Dataset Type Namespace Integration Reload

Dataset	Type	Namespace	Integration	Last activity	Size	Actions
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, además de decidir a qué dirección deben mandar los datos, que será la dirección de nuestro elasticsearch tenga dentro de docker.

Fleet

Centralized management for Elastic Agents.

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

Fleet server hosts

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 [Fleet and Elastic Agent Guide](#).

Name	Host URLs	Default	Actions
Servidor_Principal	https://192.168.100.193:8220	✓	✎

+ Add Fleet Server

Outputs

Specify where agents will send data.

Name	Type	Hosts	Status	Default	Actions
default	Elasticsearch	https://192.168.100.193:92...		Agent integrations Agent monitoring	✎

+ Add output

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
```

Entramos en powershell como administrador y pegamos el comando para instalar el agente:

```
Seleccionar Administrador: Windows PowerShell  
Windows PowerShell  
Copyright (C) Microsoft Corporation. Todos los derechos reservados.  
Prueba la nueva tecnología PowerShell multiplataforma https://aka.ms/pssc0re6  
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 -OutFile 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=VGZ2UFFvNEIxYmVrR28tYV1OV0cGNkH0VpzSw9SU1M3MXBZanNDZGpQdw==  
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":  
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>
```

Observaremos 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-  
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
```

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](#)

Ahora en kibana, deberíamos poder ver nuestro windows instalado en la pestaña fleet:

The screenshot shows the Kibana interface with the 'Agent Info Metrics' tab selected. At the top, there are tabs for 'Ingest Overview Metrics' and 'Agent Info Metrics'. Below the tabs are buttons for 'Agent activity', 'Add Fleet Server', and 'Add agent'. A search bar with placeholder text 'Filter your data using KQL syntax' is followed by a status filter section with dropdowns for 'Status' (4), 'Tags' (0), 'Agent policy' (3), and 'Upgrade available'. Below this, a message says 'Showing 3 agents' and 'Clear filters'. A legend indicates: Healthy (3 green dots), Unhealthy (0 yellow dots), Updating (0 blue dots), and Offline (0 grey dots). The main table lists one agent:

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, a sidebar navigation includes 'Home', 'Recently viewed' (with items like '[Logs iptables] Overview', '[Metrics System] Overview', '[Metrics System] Host overview', '[Logs System] Syslog dashboard', '[System Windows Security] Fail...', 'Cases', 'Timelines', 'Intelligence', 'Explore', 'Manage', and 'Management' (which is expanded to show 'Dev Tools', 'Integrations', 'Fleet' which is selected, 'Osquery', 'Stack Monitoring', and 'Stack Management'). The main area is titled 'Fleet' with the sub-header 'Centralized management for Elastic Agents.' It has tabs for 'Agents' (which is selected), 'Agent policies', 'Enrollment tokens', 'Uninstall tokens', 'Data streams', and 'Settings'. A prominent orange callout box says 'Set up encryption key' with the text 'An encryption key will make your environment more secure. Click here to learn how to set up an encryption key.' Below this is a 'Dismiss' button. At the top right are buttons for 'Agent activity', 'Add Fleet Server', and 'Add agent'. A search bar and status filter are at the top. The main table shows one agent:

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
<input type="checkbox"/> Healthy	usuario-virtualbox	Fleet Server Policy rev. 2	1.07 %	194 MB	28 seconds ago	8.12.0	...

At the bottom, it says 'Rows per page: 20' with navigation arrows.

Una vez dentro, nos vamos a “agent policies” y seleccionamos el agente que queremos o también podemos crear uno nuevo.

Fleet

Centralized management for Elastic Agents.

Agents Agent policies Enrollment tokens Uninstall tokens Data streams Settings

Filter your data using KQL syntax		Reload	Create agent policy		
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	...

Rows per page: 20 ▾

< 1 >

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

The screenshot shows the 'Agent policy 1' page in the Fleet interface. At the top, there are tabs for 'View all agent policies', 'Agent policy 1', 'Revision 4', 'Integrations 3', 'Agents Add agent', and 'Last updated on Jan 29, 2024'. Below these are 'Integrations' and 'Settings' tabs. A search bar labeled 'Search...' is present. The main table lists three agents: 'iptables-1' (Integration: Iptables v1.15.2, Namespace: default), 'sysmon_linux-1' (Integration: Sysmon for Linux v1.6.2, Namespace: default), and 'system-1' (Integration: System v1.53.0, Namespace: default). To the right of the table is an 'Actions' dropdown menu with options: 'Add agent' (highlighted with a blue underline), 'View policy', 'Duplicate policy', 'Delete policy', and 'Uninstall agents on this policy'.

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

Add agent

X

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.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=aUR1ZVZZ
```

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).

```
13:00:00) contraseña para usuario1:
root@usuario1:/home/usuario1/Escritorio# curl -L -O 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=aURlZVZZMEjjYVFudlppWGtSSjY6cGw0cVNiVmPSY0t4cVZUS2o0U1RRUQ==
% 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 último 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/Escritorio# ./elastic-agent install --url=https://192.168.100.193:5601 --enrollment-token=aURlZVZZMEjjYVFudlppWGtSSjY6cGw0cVNiVmPSY0t4cVZUS2o0U1RRUQ== --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.tar.gz
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.



Por último, en la pestaña de flota se verá de la siguiente manera:

Ingest Overview Metrics Agent Info Metrics Agent activity Add Fleet Server Add agent

Filter your data using KQL syntax Status 4 Tags 0 Agent policy 2 Upgrade available

Showing 2 agents Clear filters

Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
Healthy	usuario1	Linux-1 rev. 2	0.49 %	195 MB	34 seconds ago	8.12.2	...
Healthy	usuario-virtualbox	Fleet Server Policy rev. 1	0.88 %	223 MB	11 seconds ago	8.12.2	...

Rows per page: 20 < 1 >

Como instalar agente standalone

Esta parte, es de cuando no conseguía poner bien la flota y probé 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. En primera, iremos a la política que queremos usar y pulsamos “añadir agente”:

The screenshot shows the 'Prueba2' policy page. At the top, there are tabs for 'View all agent policies', 'Prueba2', 'Revision 2', 'Integrations 2', 'Agents 1', 'Last updated on Feb 25, 2024', and 'Actions'. The 'Actions' dropdown menu is open, showing options: 'Add agent', 'View policy', 'Duplicate policy', 'Delete policy', and 'Uninstall agents on this policy'. Below the menu, there is a table with two rows. The first row has 'sysmon_linux-3' under 'Name', 'Sysmon for Linux v1.6.2' under 'Integration', and 'default' under 'Namespace'. The second row has 'system-3' under 'Name', 'System v1.54.0' under 'Integration', and 'default' under 'Namespace'. A search bar and a 'Name' filter are also present.

Tras eso, seleccionamos la opción standalone:

The screenshot shows the 'Add agent' wizard. Step 1: 'Select enrollment token'. It says 'Prueba2 has been selected. Select which enrollment token to use when enrolling agents.' Under 'Authentication settings', it shows 'Enrollment token: Default (e78492f1-61a7-4902-b88d-b7b99428d703)'. Step 2: 'Enroll in Fleet?'. It has two options: 'Enroll in Fleet (recommended)' (selected) and 'Run standalone'. Step 3: 'Install Elastic Agent on your host'. There is a link to 'Get started with the Elastic Agent'.

Instalaremos el agente usando el comando que nos proporciona, lo que hará que nos pregunte durante la instalación, si queremos añadirlo a alguna fleet, a lo que nos negaremos.

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.tar.gz
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
```

Una vez instalado, debemos copiar la política 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

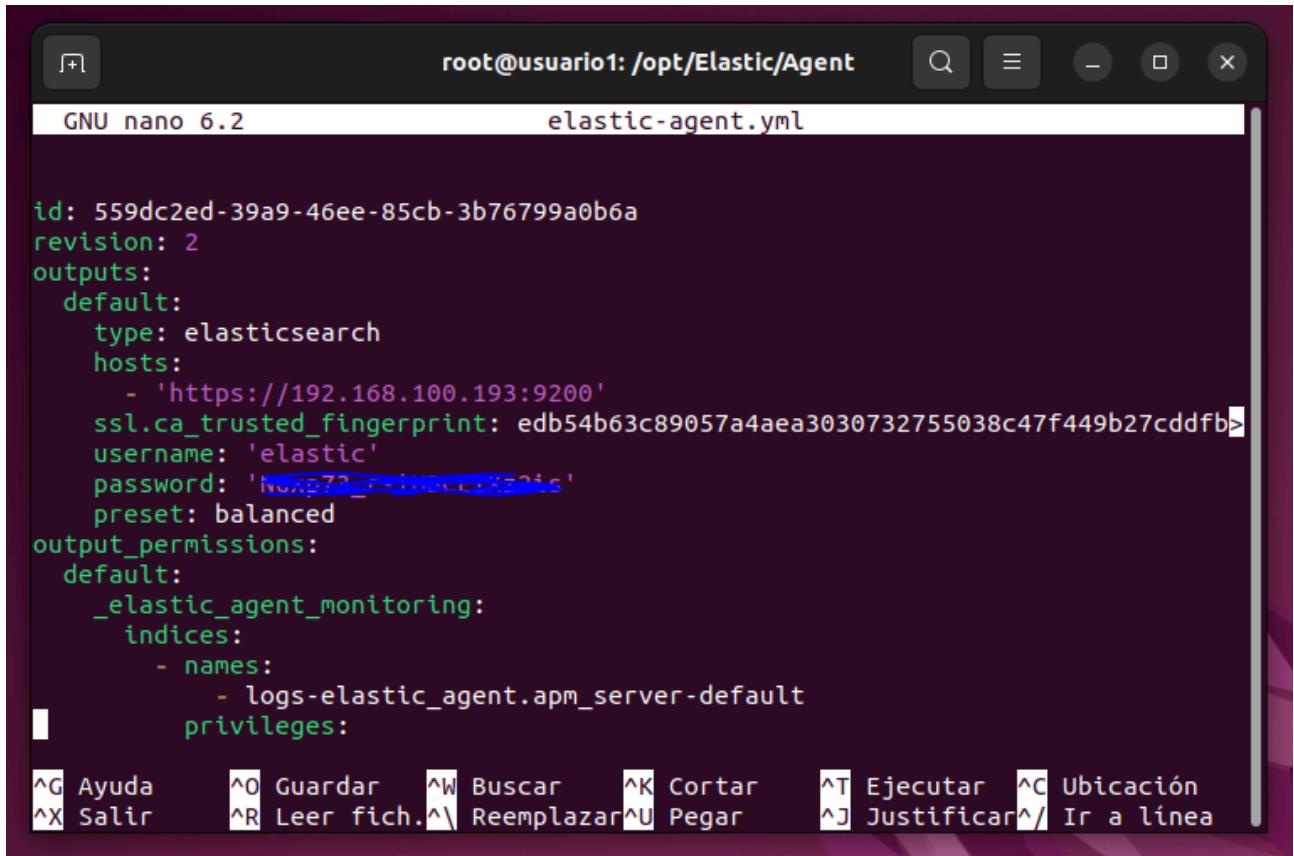
 Download Policy

```
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

Ya que, nos ha puesto la de elasticsearch que está dentro de la red elastic, básicamente una red que no puede acceder ni encontrar.



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

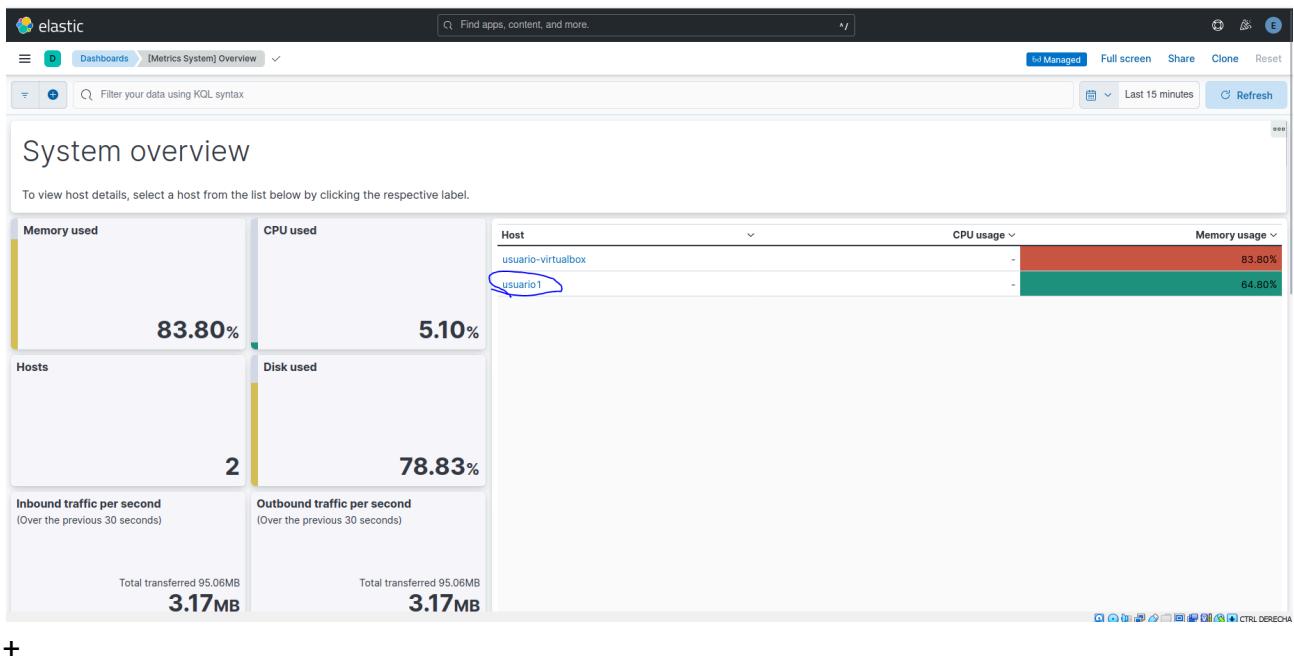
id: 559dc2ed-39a9-46ee-85cb-3b76799a0b6a
revision: 2
outputs:
  default:
    type: elasticsearch
    hosts:
      - 'https://192.168.100.193:9200'
    ssl.ca_trusted_fingerprint: edb54b63c89057a4aea3030732755038c47f449b27cddfb>
    username: 'elastic'
    password: 'NuMz72...[REDACTED]24s'
    preset: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

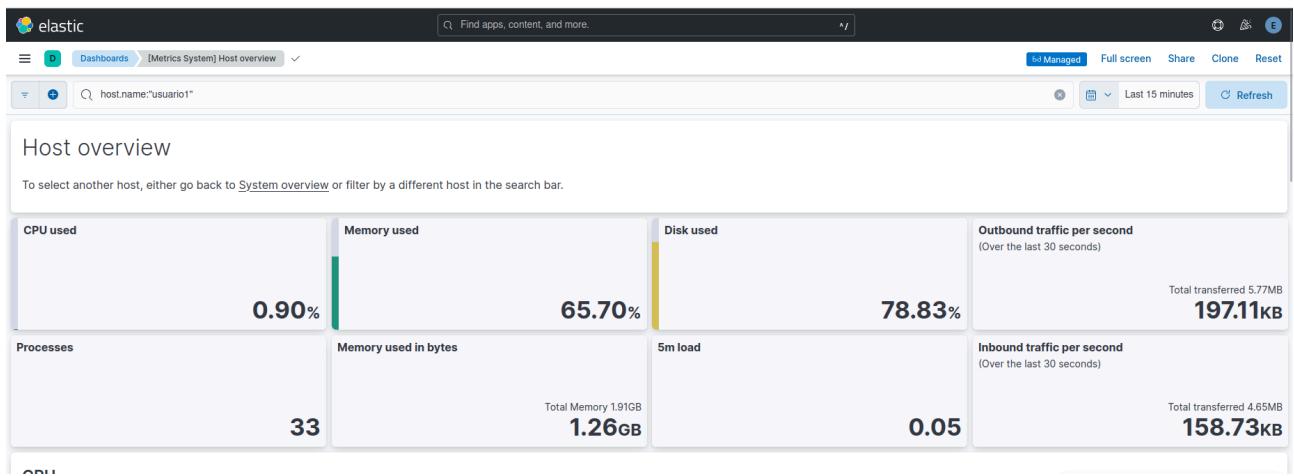
```
root@usuario1:/opt/Elastic/Agent# elastic-agent status
  fleet
    └─ status: (STOPPED) Not enrolled into Fleet
  elastic-agent
    └─ status: (HEALTHY) Running
root@usuario1:/opt/Elastic/Agent#
```

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 máquinas. Si lo hicimos bien, debería mostrarnos lo siguiente:



+

Vemos que nos muestra nuestra máquina host y el nuevo equipo, por lo que si entramos nos muestra lo siguiente:



Si por el contrario no muestra nada, debemos esperar unos minutos, pues a veces, tarda un poco en recibir los datos o en permitir la entrada de los mismos. Por ejemplo, si acabamos de encender los contenedores de docker.

Conclusión

Tras investigar e instalar este programa, vemos que se puede usar para monitorear los ordenadores de una organización, para comprobar el uso de los recursos de esas máquinas, comprobar el espacio disponible en los discos duros y revisar cuales son las aplicaciones con más gasto de recursos.

El programa es sencillo de utilizar una vez conoces todo el proceso de instalación, ya que dentro de esta misma acción, tuve que solucionar algunos problemas, como por ejemplo: el programa me cambiaba la dirección ip por una que no era. Tras varios intentos pude encontrar una solución, teniendo que poner los contenedores dentro de la red Host, pues en la red elastic, tenía una ip diferente a la del host, y los agentes instalados en otras máquinas, no podían alcanzar el contenedor de elasticsearch para enviar los datos.

En conclusión, a partir de este proyecto he podido aprender mucho sobre este programa, su utilidad y saber solucionar los diferentes problemas que puedan ir surgiendo con su instalación.