

# Guía instalación Elasticsearch

Primero, vamos a instalar Elasticsearch desde este [enlace](#). Se descargará el zip de Elasticsearch, y hay que asegurarse de que está seleccionado el SO correcto (Windows, Linux, MacOS, etc), y acto seguido descargarlo para el SO que estamos utilizando. En este caso, el sistema operativo es Windows, pero si se estuviese usando uno diferente, hay que cambiarlo.

**1 Download and unzip Elasticsearch**

Choose platform:

Windows

↓ Windows    ↓ sha    ↓ asc

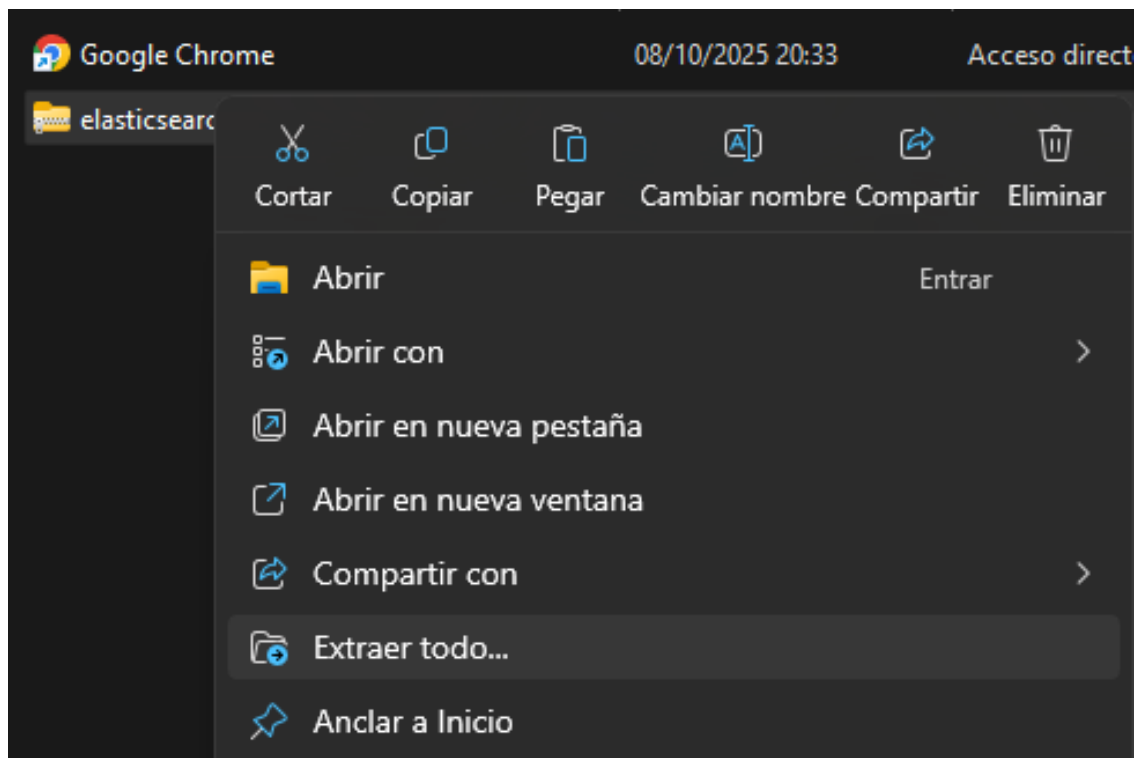
Containers:

Docker →

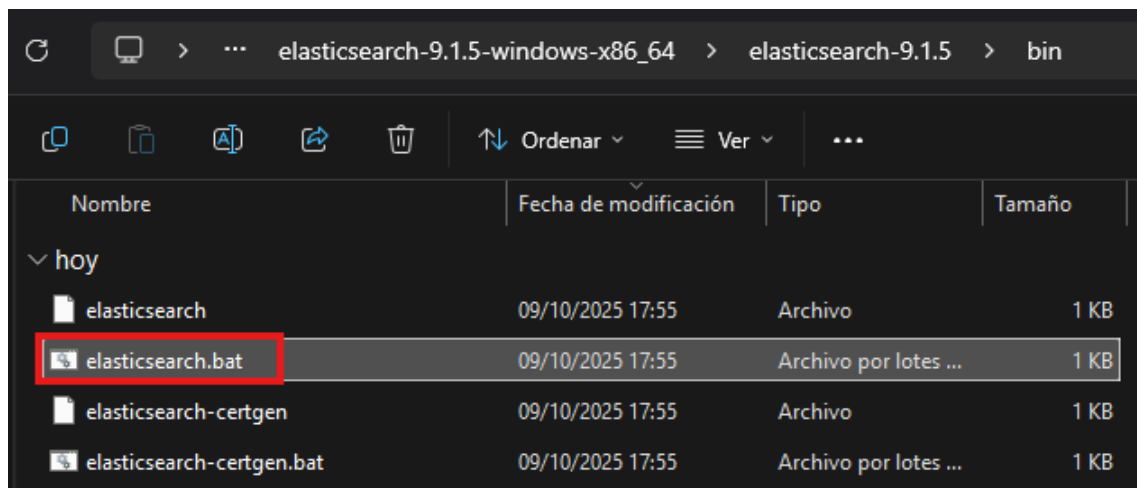
Elasticsearch can also be installed from our package repositories using apt or yum. See [Repositories in the Guide](#).

Una vez descargado el zip, hay que extraerlo. Podemos extraerlo desde entorno gráfico, o desde entorno comando.

Para extraerlo en entorno gráfico, hacemos click derecho > **Extraer Todo...**



Tras extraerlo, ejecutaremos el archivo por lotes .bat llamado **elasticsearch.bat**. Para ejecutarlo en entorno gráfico, simplemente hacemos doble click sobre él.



Si por lo contrario quisiéramos ejecutarlo en entorno comando, navegamos hasta la ruta en la que se ubica (la carpeta bin dentro de la carpeta extraída) y ejecutamos `elasticsearch.bat` en el cmd

```
Directorio de C:\Users\CursosTardes\Downloads\elasticsearch-9.1.5-windows-x86_64\elasticsearch-9.1.5
09/10/2025 17:55 <DIR>      .
09/10/2025 17:55 <DIR>      ..
09/10/2025 17:55 <DIR>      bin
09/10/2025 17:55 <DIR>      config
09/10/2025 17:55 <DIR>      jdk
09/10/2025 17:55 <DIR>      lib
09/10/2025 17:55          3.860 LICENSE.txt
01/02/1980 00:00 <DIR>      logs
09/10/2025 17:55 <DIR>      modules
09/10/2025 17:55          2.382.169 NOTICE.txt
01/02/1980 00:00 <DIR>      plugins
09/10/2025 17:55          10.283 README.asciidoc
          3 archivos      2.396.312 bytes
          9 dirs 372.684.734.464 bytes libres

C:\Users\CursosTardes\Downloads\elasticsearch-9.1.5-windows-x86_64\elasticsearch-9.1.5>cd bin

C:\Users\CursosTardes\Downloads\elasticsearch-9.1.5-windows-x86_64\elasticsearch-9.1.5\bin>elasticsearch.bat
[2025-10-09T18:19:47,267][INFO ][o.e.b.Elasticsearch      ] [T04W15] version[9.1.5], pid[6780], build[zip/90ee222e7e0136
dd8ddb34015538f3a00c129b7/2025-10-02T22:07:12.966975992Z], OS[Windows 11/10.0/amd64], JVM[Oracle Corporation/OpenJDK 64
-Bit Server VM/25/25+36-3489]
[2025-10-09T18:19:47,279][INFO ][o.e.b.Elasticsearch      ] [T04W15] JVM home [C:\Users\CursosTardes\Downloads\elasticsearch-9.1.5-windows-x86_64\elasticsearch-9.1.5\jdk], using bundled JDK [true]
[2025-10-09T18:19:47,281][INFO ][o.e.b.Elasticsearch      ] [T04W15] JVM arguments [-Des.networkaddress.cache.ttl=60, -Des.networkaddress.cache.negative.ttl=10, -XX:+AlwaysPreTouch, -Xss1m, -Djava.awt.headless=true, -Dfile.encoding=UTF-8, -Djna.nosys=true, -XX:-OmitStackTraceInFastThrow, -Dio.netty.noUnsafe=true, -Dio.netty.noKeySetOptimization=true, -Dio.netty.recycler.maxCapacityPerThread=0, --add-opens=org.apache.lucene.core/org.apache.lucene.codecs.lucene99=org.elasticsearch.server, --add-opens=org.apache.lucene.backward_codecs/org.apache.lucene.backward_codecs.lucene90=org.elasticsearch.server, --add-opens=org.apache.lucene.backward_codecs/org.apache.lucene.backward_codecs.lucene91=org.elasticsearch.server, --add-opens=org.apache.lucene.backward_codecs/org.apache.lucene.backward_codecs.lucene92=org.elasticsearch.server, --add-opens=org.apache.lucene.backward_codecs/org.apache.lucene.backward_codecs.lucene94=org.elasticsearch.server, --add-opens=org.apache.lucene.backward_codecs/org.apache.lucene.backward_codecs.lucene95=org.elasticsearch.server, -Dlog4j.shutdownHookEnabled=false, -Dlog4j2.disable.jmx=true, -Dlog4j2.formatMsgNoLookups=true, -Djava.locale.providers=CLDR, -Dorg.apache.lucene.vectorization.upperJavaFeatureVersion=25, -Des.path.home=C:\Users\CursosTardes\Downloads\elasticsearch-9.1.5-windows-x86_64\elasticsearch-9.1.5, -Des.distribution.type=zip, -Des.java.type=bundled JDK, --enable-native-access=org.elasticsearch.nativeaccess,org.apache.lucene.core, --enable-native-access=ALL-UNNAMED, --illegal-native-access=deny, -XX:ReplayDataFile=logs/replay_pid%p.log, -Des.entitlements.enabled=true, -XX:+EnableDynamicAgentLoading, -Djdk.attach.allowAttachSelf=true, --patch-module=java.base=C:\Users\CursosTardes\Downloads\elasticsearch-9.1.5-windows-x86_64\elasticsearch-9.1.5\lib\entitlement-bridge\elasticsearch-entitlement-bridge-9.1.5.jar, --add-exports=java.base/org.elasticsearch.entitlement.bridge=org.elasticsearch.entitlement,java.logging,java.net.http,java.naming,jdk.net, -XX:+UseG1GC, -Djava.io
```

A continuación, instalaremos Kibana desde este [enlace](#). El proceso es idéntico al de Elasticsearch, y una vez descargado el zip, lo descomprimos, y ejecutamos el `.bat` de Kibana

## 1 Download and unzip Kibana

Choose platform:

Windows

Windows

sha asc

Aunque lo ejecutemos en entorno gráfico, se nos abrirá el Kibana en un cmd/terminal en Linux

```
C:\windows\system32\cmd.exe
{"log.level":"info","@timestamp":"2025-10-09T17:31:42.089Z","log.logger":"elastic-apm-node","ecs.version":"8.10.0","agentVersion":"4.13.0","env":{"pid":16560,"proctitle":"C:\\windows\\system32\\cmd.exe","os":"win32 10.0.26100","arch":"x64","host":"T04W15","timezone":"UTC+0200","runtime":"Node.js v22.17.1"},"config":{"active":{"source":"start","value":true},"breakdownMetrics":{"source":"start","value":false},"captureBody":{"source":"start","value":"off","commonName":"capture_body"},"captureHeaders":{"source":"start","value":false},"centralConfig":{"source":"start","value":false},"contextPropagationOnly":{"source":"start","value":true},"environment":{"source":"start","value":"production"},"globalLabels":{"source":"start","value":{"git_rev":"4a62c99c68a5156b84e1bf986d47e0a317591820"},"sourceValue":{"git_rev":"4a62c99c68a5156b84e1bf986d47e0a317591820"},"logLevel":{"source":"default","value":"info","commonName":"log_level"},"metricsInterval":{"source":"start","value":120,"sourceValue":"120s"},"serverUrl":{"source":"start","value":"https://kibana-cloud-apm.apm.us-east-1.aws.found.io/","commonName":"server_url"},"transactionSampleRate":{"source":"start","value":0.1,"commonName":"transaction_sample_rate"},"captureSpanStackTraces":{"source":"start","sourceValue":false},"secretToken":{"source":"start","value":"[REDACTED]","commonName":"secret_token"},"serviceName":{"source":"start","value":"kibana","commonName":"service_name"},"serviceVersion":{"source":"start","value":"9.1.5","commonName":"service_version"},"activationMethod":"require","message":"Elastic APM Node.js Agent v4.13.0"}
Native global console methods have been overridden in production environment.
[2025-10-09T19:31:46.690+02:00][INFO ][root] Kibana is starting
[2025-10-09T19:31:46.711+02:00][INFO ][node] Kibana process configured with roles: [background_tasks, ui]
[2025-10-09T19:31:54.871+02:00][INFO ][plugins-service] The following plugins are disabled: "cloudChat,cloudExperiments,cloudFullStory,dataUsage,onechat,profilingDataAccess,profiling,securitySolutionServerless,serverless,serverlessObservability,serverlessSearch".
[2025-10-09T19:31:54.925+02:00][INFO ][http.server.Preboot] http server running at http://localhost:5601
[2025-10-09T19:31:54.985+02:00][INFO ][plugins-system.preboot] Setting up [1] plugins: [interactiveSetup]
[2025-10-09T19:31:55.011+02:00][INFO ][preboot] "interactiveSetup" plugin is holding setup: Validating Elasticsearch connection configuration...
[2025-10-09T19:31:55.035+02:00][INFO ][root] Holding setup until preboot stage is completed.
```

Por último, para Elastic Agent, descargaremos el zip desde [aquí](#), asegurándonos de que lo descargamos para el SO correcto.

## 1 Download Elastic Agent

Download the Elastic Agent for your chosen platform and format. We recommend using the installers (TAR/ZIP) over system packages (RPM/DEB) because they provide the ability to upgrade your agent within Fleet.

Choose platform:

Windows 64-bit



Windows 64-bit



sha

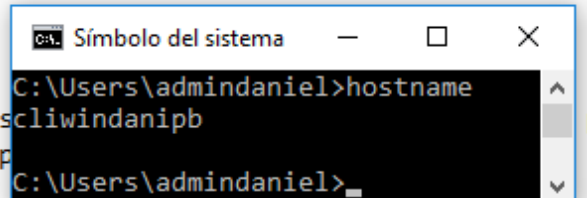


asc

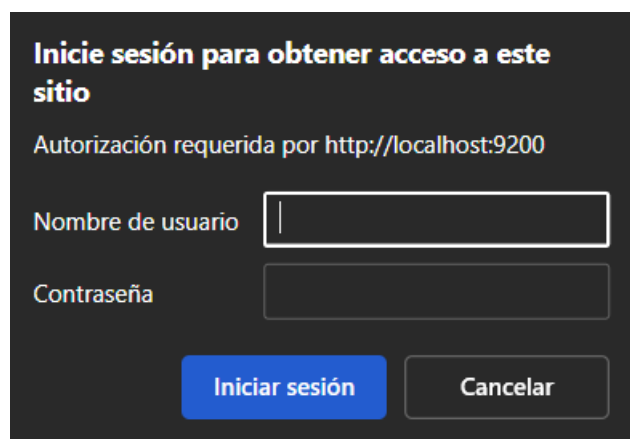
Una vez extraído todo, vamos a arrancar los servicios, empezando por Elasticsearch. Antes de ejecutarlo, para que se pueda acceder desde otras

máquinas, vamos a descomentar la línea de `network.host` y le cambiamos la IP a la `0.0.0.0` en el archivo `elasticsearch.yaml`, ubicado en la subcarpeta `config`

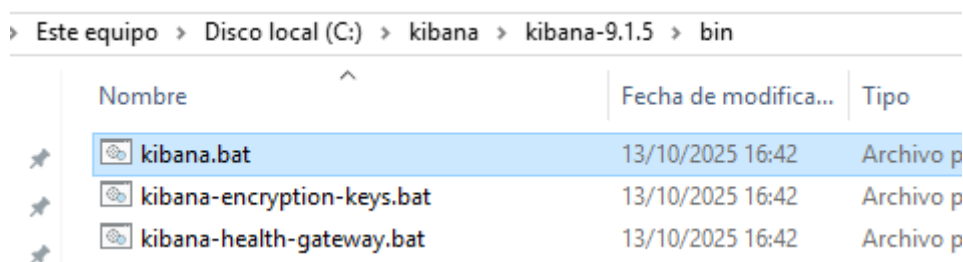
```
# ----- Network -----  
#  
# By default Elasticsearch is only accessible on localhost. Set a differ  
# address here to expose this node on the network:  
#  
network.host: 0.0.0.0  
#  
# By default Elasticsearch listens on a random port, which is  
# finds starting at 9200. Set a specific port to use here:  
#
```



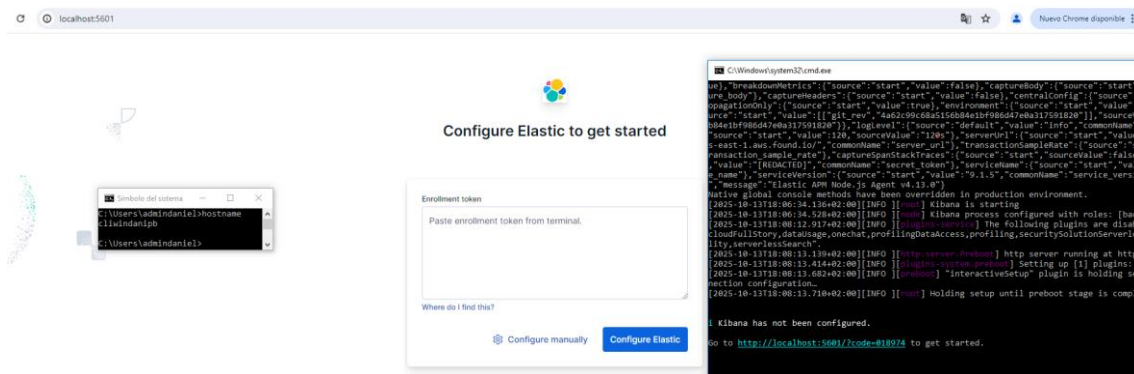
Una vez arrancado el servicio, si accedemos a <http://localhost:9200> (o la IP desde otra máquina), veremos esto. Aunque es un error, es correcto y el servicio está funcionando, lo único que de mostrar el panel se encarga Kibana.



Hecho esto, procederemos a ejecutar Kibana.



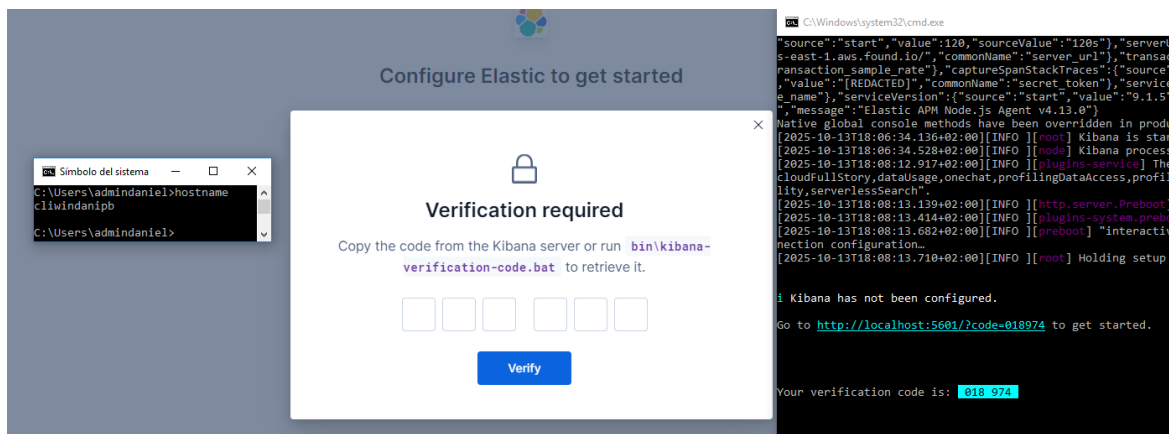
En el navegador, accederemos a <http://localhost:5601> y como podremos ver (y nos indicará el CMD), tendremos que configurar Kibana desde esa página.



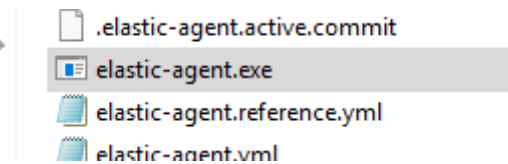
Copiamos el Token de nuestro elasticsearch y lo pegamos en la página de Kibana para poder configurarlo.



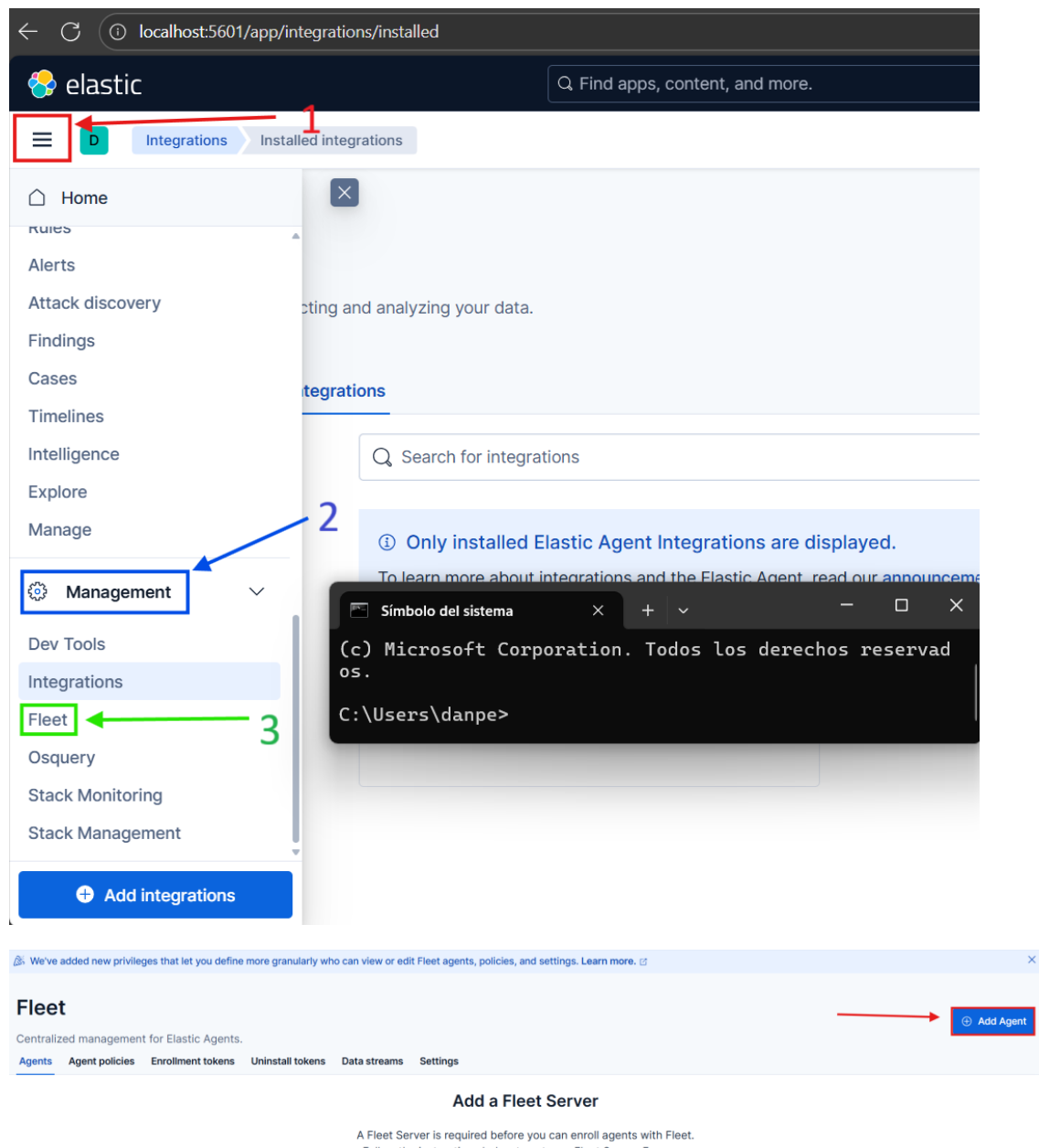
Hecho esto, nos pedirá el código que se generará en el terminal de Kibana para confirmar que somos nosotros y poder configurarlo.



Por último, instalaremos elastic agent con su ejecutador (.exe)



Una vez esté todo instalado, vamos a acceder a elasticsearch desde la URL de Kibana, no desde la de Elasticsearch, y nos iremos a las tres rayas > Management > Fleet, y en Agents, le damos a Add Agent

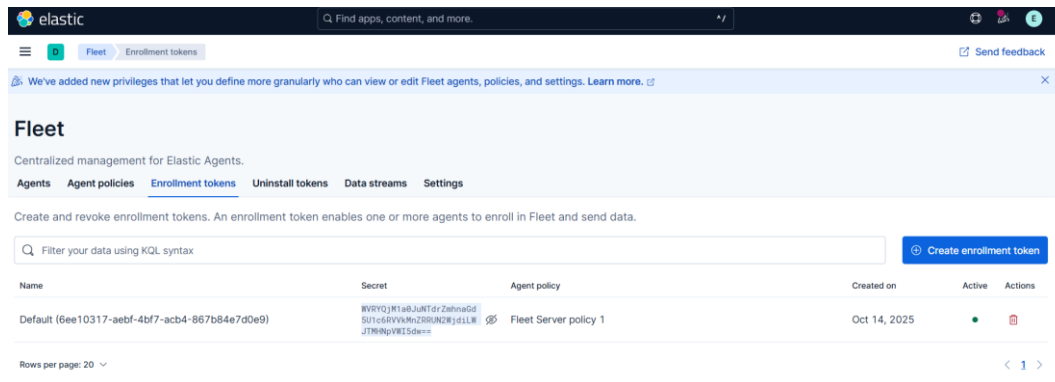


Podemos crear el agente desde ahí o en entorno comando. Si lo hacemos en entorno comando, tendremos que configurar la IP de kibana y generar un token

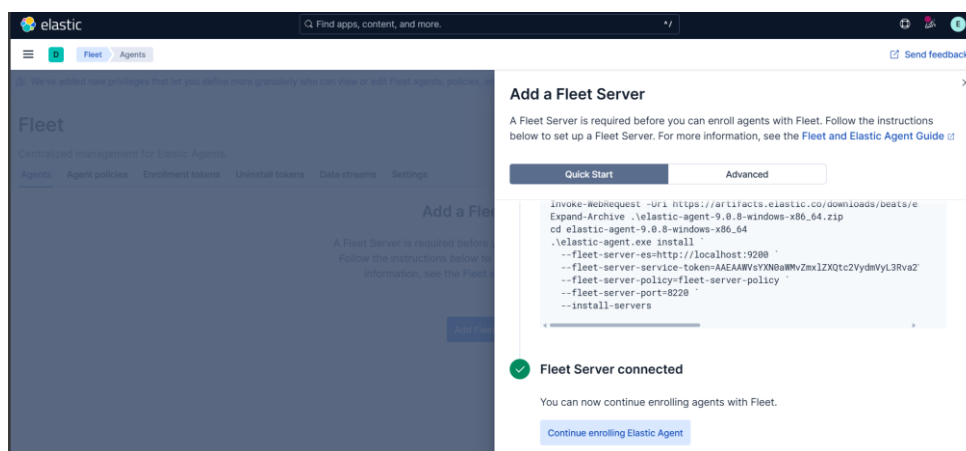
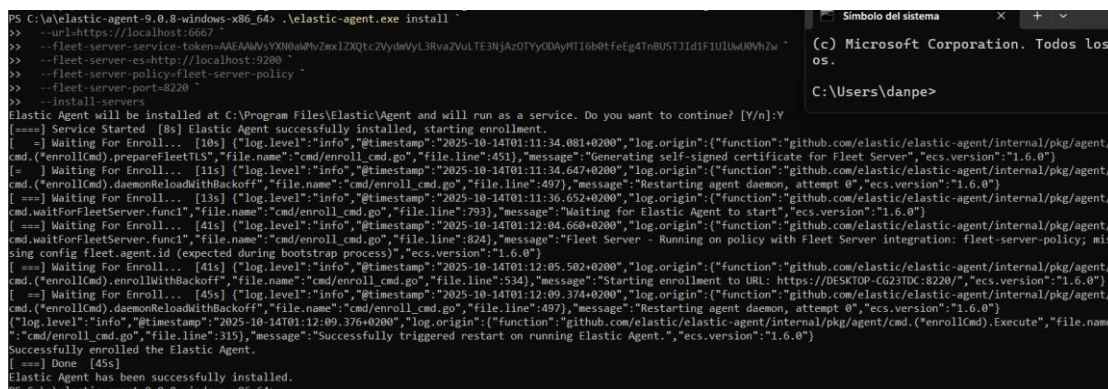


```
C:\a\elastic-agent-9.0.8-windows-x86_64>.elastic-agent.exe install
Elastic Agent will be installed at C:\Program Files\Elastic\Agent and will run as a service. Do you want to continue? [Y/n]:Y
Do you want to enroll this Agent into Fleet? [Y/n]:Y
URL you want to enroll this Agent into: http://localhost:5601
Fleet enrollment token: WVRyQjM1a0JuNTdrZmhmaGd5U1c6RVVhMnZRRUN2Wjd1LWJTMHlpVMI5dw==
[ =] Service Started [9s] Elastic Agent successfully installed, starting enrollment.
```

Para generar el token, desde Fleet, nos iremos a Enrollment tokens, y copiamos el token necesario para nuestro agente

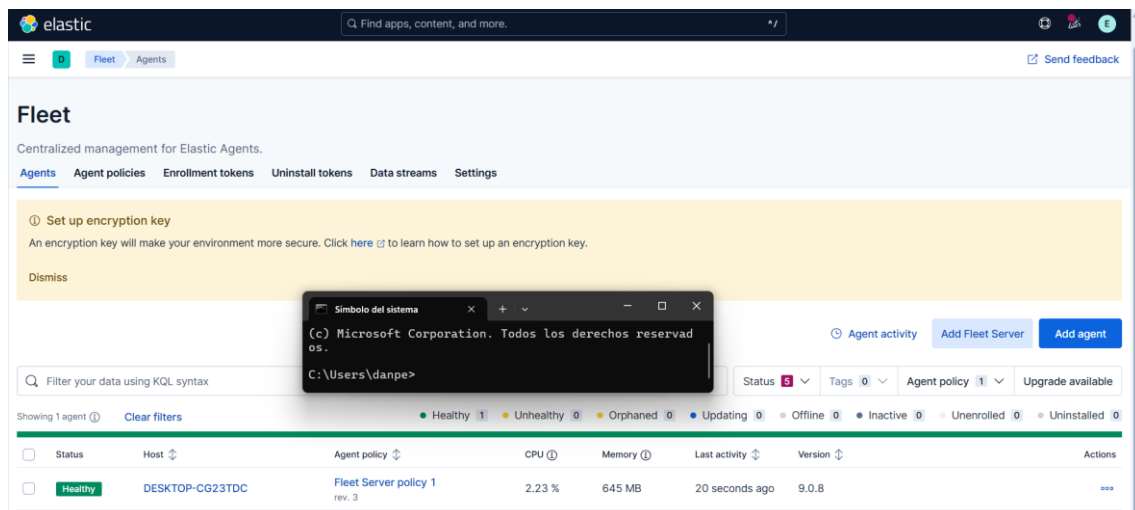


Una vez hecho esto, vamos a Agents > Add Agent y hacemos el “enroll fleet” con nuestro agente. Introducimos el comando que nos indica, y si todo va bien, en el Kibana veremos que se ha producido la conexión de forma satisfactoria.

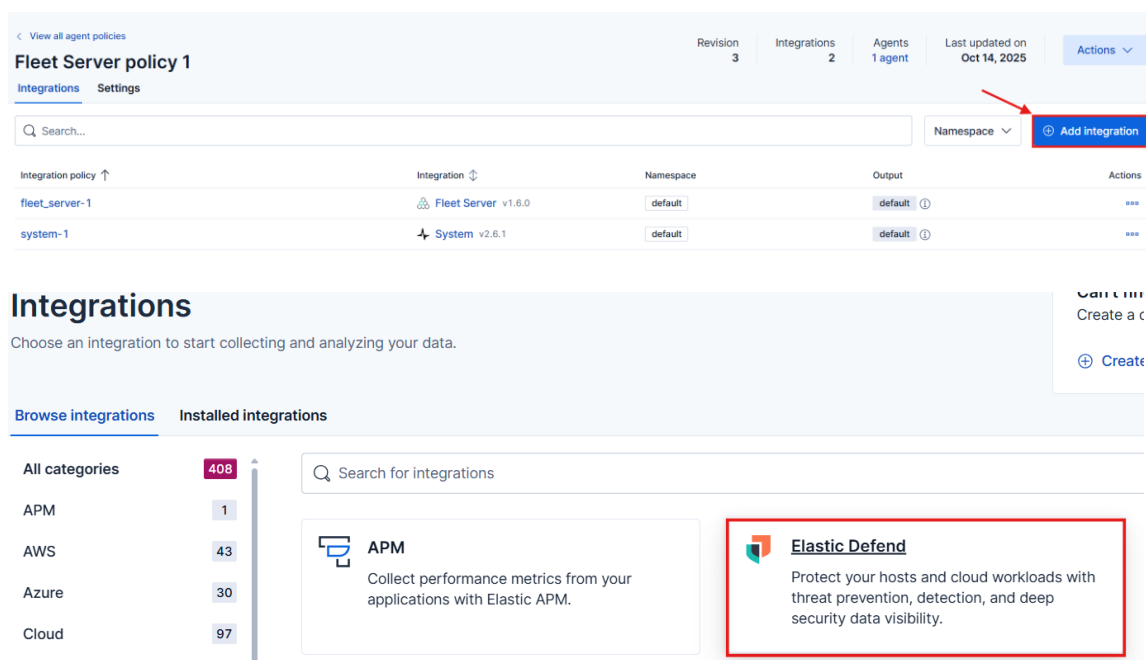


Tras darle a continue enrolling agent, veremos que finalmente, nuestro agente está listo y funcionando






Pues ya por último, lo último que nos queda por hacer, es que el agente recopile información de seguridad del host. Para ello, desde Kibana, nos vamos a Fleet > Agent Policies y modificamos la política de nuestro agente, y le damos a Add Integration para añadir la integración de Elastic Defend



Lo añadimos a la política de nuestro agente, con control total EDR, o por lo menos recopilación de datos, y listo

[Cancel](#)



## Add Elastic Defend integration

Configure an integration for the selected agent policies.

Requires root privileges

Elastic Agent needs to be run with root/administrator privileges for this integration.

This package has 2 transform assets which will be created and started with the same roles as the user installing the package.

1

### Configure integration

#### Integration settings

Choose a name and description to help identify how this integration will be used.

Integration name

Elastic Defend

Description

Optional

Everything in NGAV, plus file and network telemetry

Complete EDR (Endpoint Detection & Response)

Everything in Essential EDR, plus full telemetry

Note: advanced protections require a platinum license, and full response capabilities require an enterprise license. See [documentation](#) for more information.

2

### Where to add this integration?

[New hosts](#) [Existing hosts](#)

Agent policies

Agent policies are used to manage a group of integrations across a set of agents.

Agent policies

Fleet Server policy 1

1 agent is enrolled with the selected agent policies.

Cancel

Save and continue

Y listo, ya lo tenemos ejecutándose

[View all agent policies](#)

### Fleet Server policy 1

[Integrations](#) [Settings](#)

Q Search...

Símbolo del sistema

(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\danpe>




Revision 4

Integrations 3

Agents 1 agent

Last updated on Oct 14, 2025

Actions

Integration policy ↑	Integration ⇅	Namespace	Output	Actions
Elastic Defend	 Elastic Defend v0.0.2	default ⓘ	default ⓘ	...
fleet_server-1	 Fleet Server v1.0.0	default	default ⓘ	...
system-1	 System v2.6.1	default	default ⓘ	...

Y como podemos ver, si nos vamos a la pestaña de Seguridad en Kibana, Elastic Defend ya ha empezado a recopilar información y podremos ver dashboards bastante completos e interesantes

