Universidad de Alcalá
Escuela Politécnica Superior

Máster Universitario en
Ciberseguridad

Autores:
Aryan Rezaeian Hernández

14 de Octubre de 2024

Índice general

Capítulo 1

Configuración de entorno con SIEM

El objetivo de esta práctica es utilizar **Splunk** para realizar análisis de datos de registro y generar visualizaciones útiles.

1.1. Instalación de Splunk

Después de actualizar nuestra máquina virtual con los siguientes comandos.

```
sudo apt update
sudo apt upgrade -y
```

Ya podemos empezar con la descarga e instalación de **Splunk**.

Primero tenemos que crearnos una cuenta y comenzar el periodo de prueba 1.1.

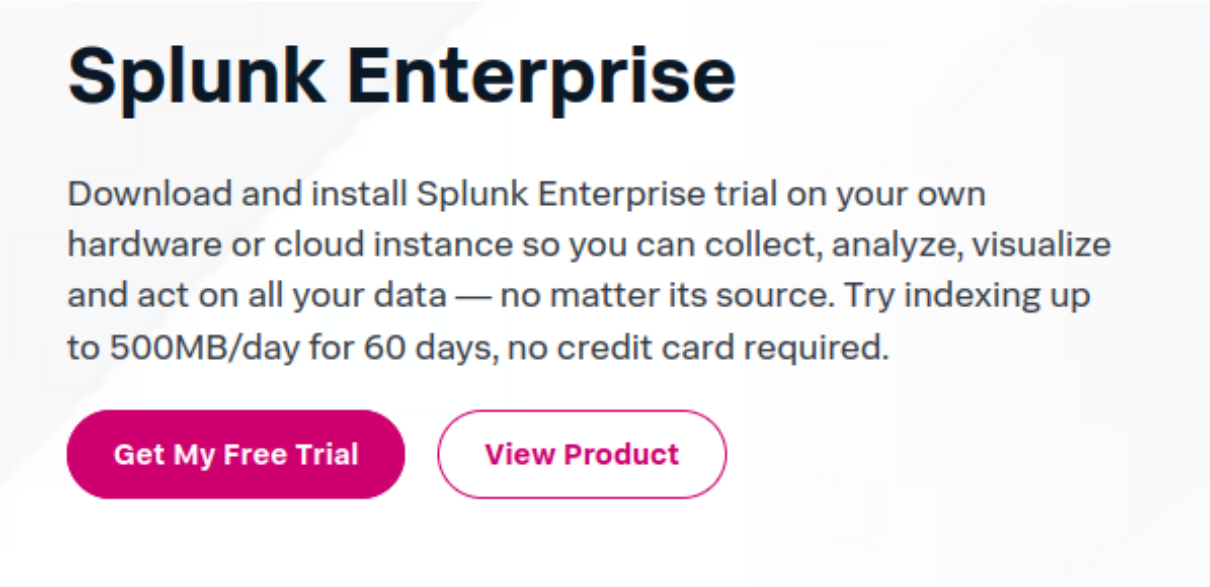

Figura 1.1: Prueba gratis de splunk enterprise

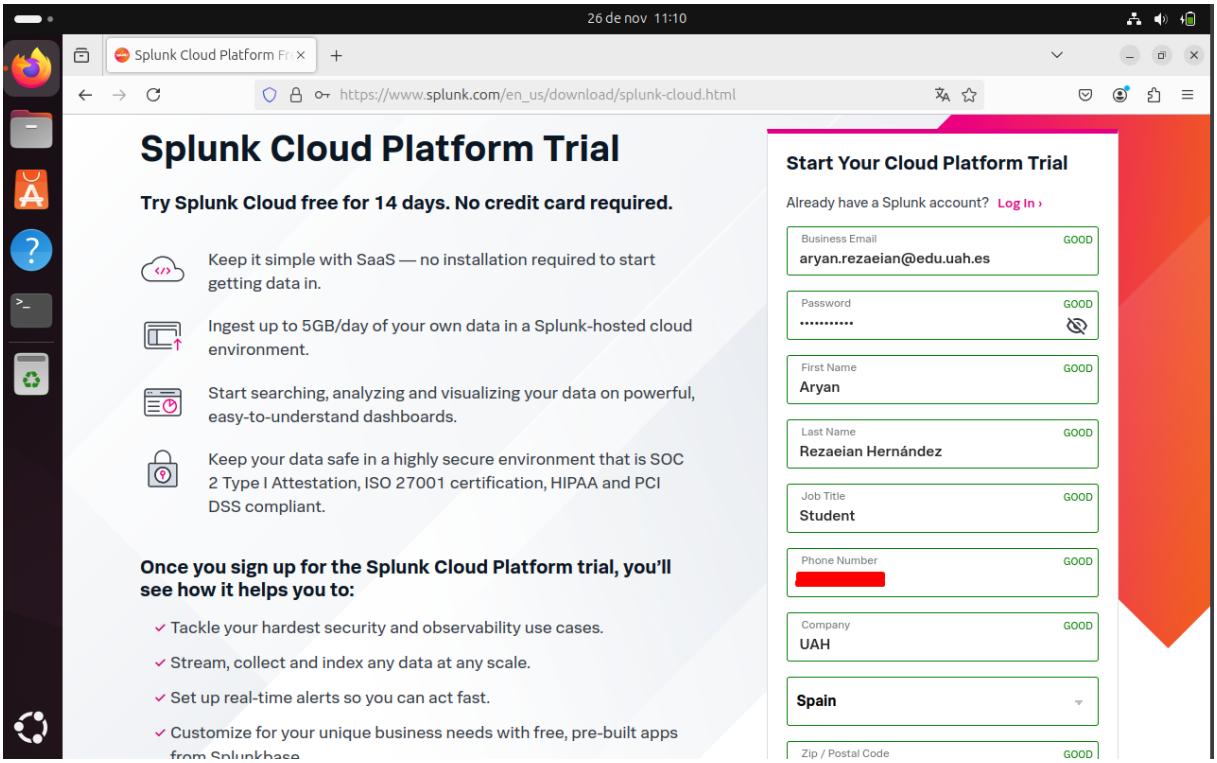

Figura 1.2: Registrarse en splunk

Una vez registrados seleccionamos el producto **Splunk Enterprise** y lo descargamos 1.3.

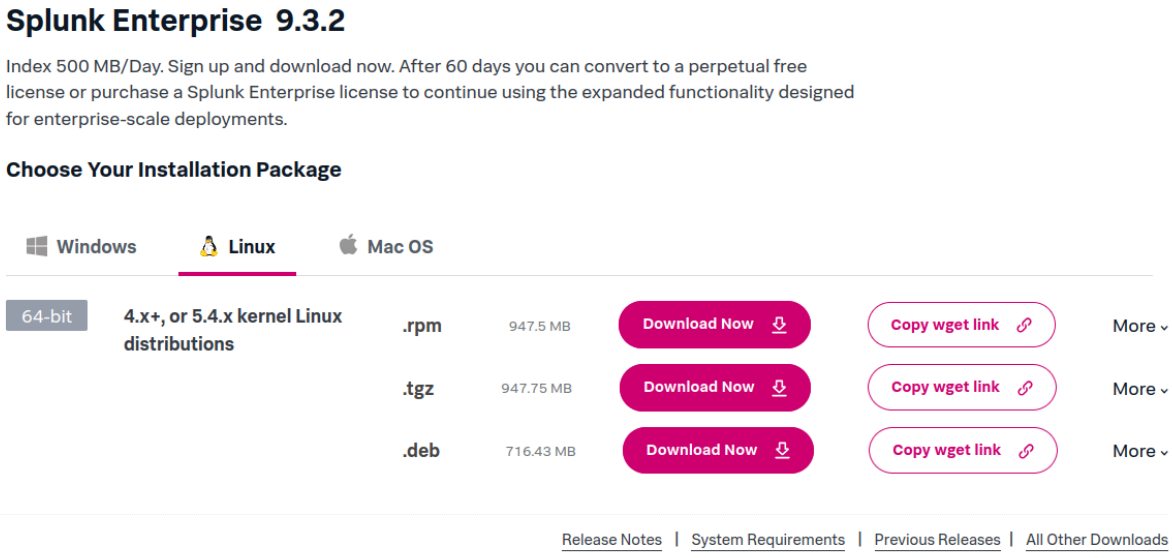

Figura 1.3: Descarga de Splunk

Vamos a nuestra máquina ubuntu 24.04 e introducimos estos comandos en la terminal:

```
cd ~/Descargas

wget -O splunk-9.3.2-d8bb32809498-Linux-x86_64.tgz
"https://download.splunk.com/products/splunk/releases
/9.3.2/linux/splunk-9.3.2-d8bb32809498-Linux-x86_64.tgz"

tar -xvzf splunk-9.3.2-d8bb32809498-Linux-x86_64.tgz
```

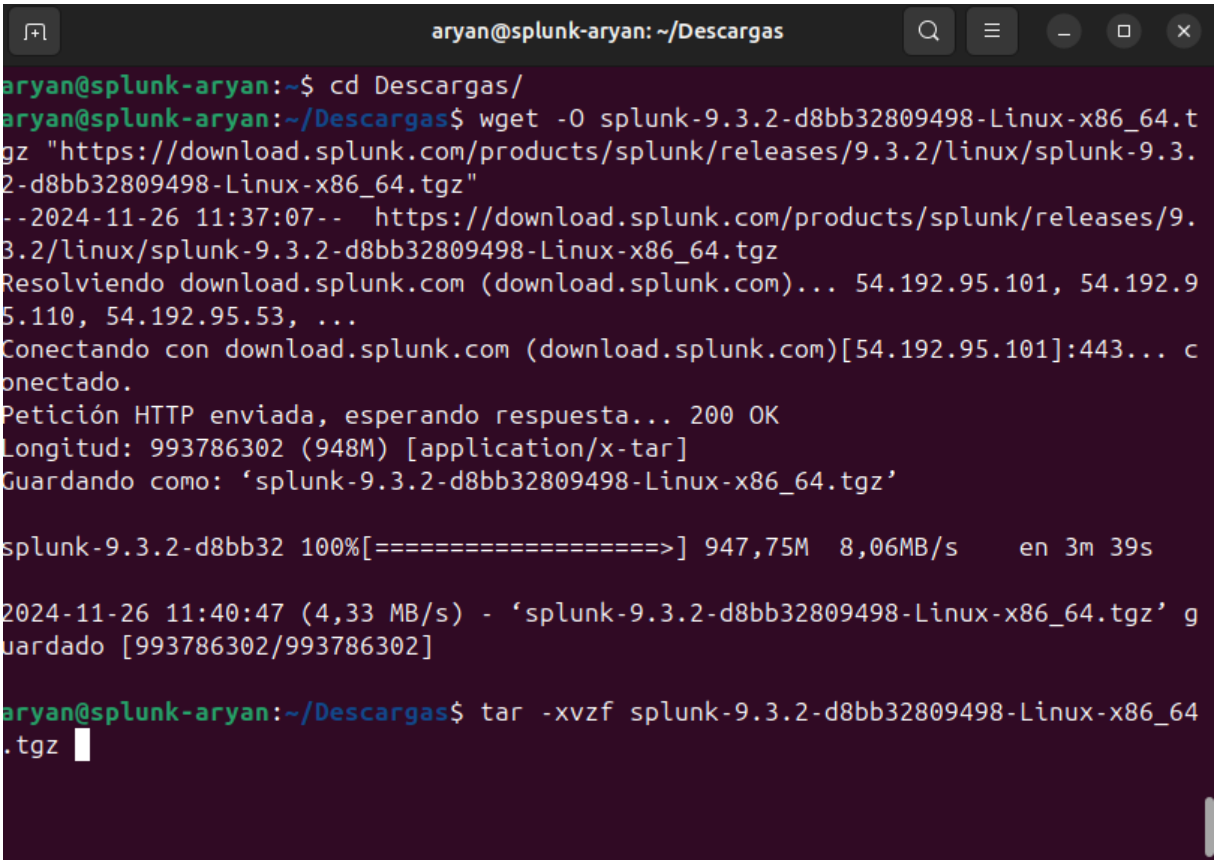

Figura 1.4: Descargar y descomprimir splunk

Una vez descargado y descomprimido **Splunk** lo iniciamos 1.5.

```
cd ~/Descargas/splunk

sudo ./bin/splunk start
```

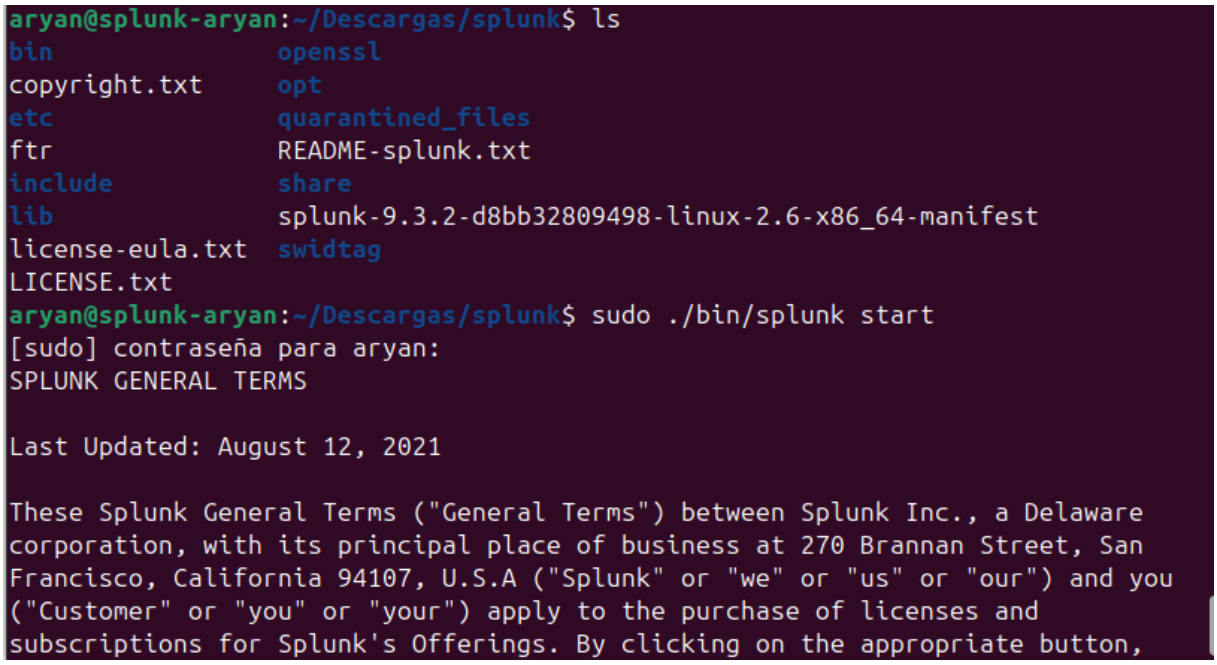

Figura 1.5: Iniciamos Splunk

Nos pedirá un nombre de administrador y una contraseña: **aryan:aryan123** y una vez finalice ya tendremos splunk activado.

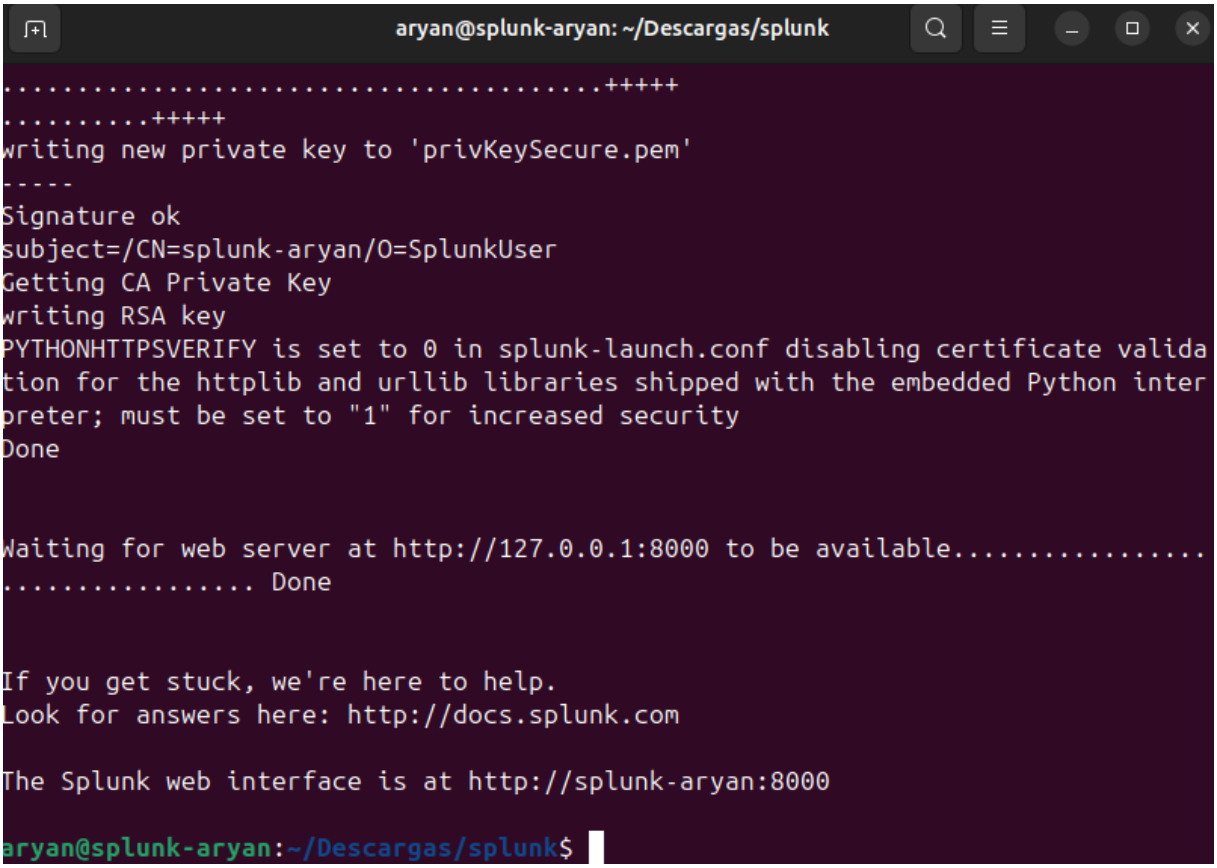

Figura 1.6: Splunk activado

Para que **Splunk** arranque automáticamente al reiniciar el sistema podemos usar el siguiente comando:

```
./bin/splunk enable boot-start
```

1.2. Primer contacto con Splunk

Accedemos a la página que aparece en 1.6 tras activarse y nos aparece un formulario para iniciar sesión 1.7.

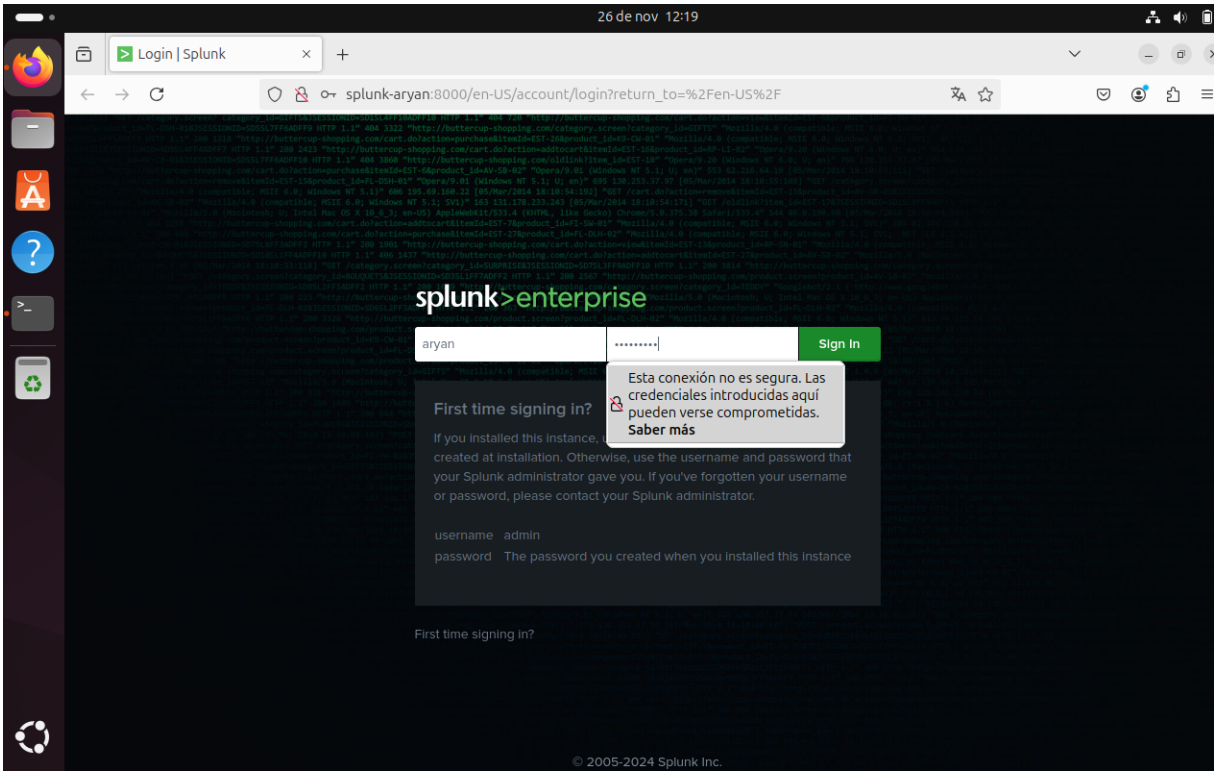

Figura 1.7: Log in Splunk

Introducimos las credenciales que configuramos en la iniciación de **splunk** y accedemos 1.8.

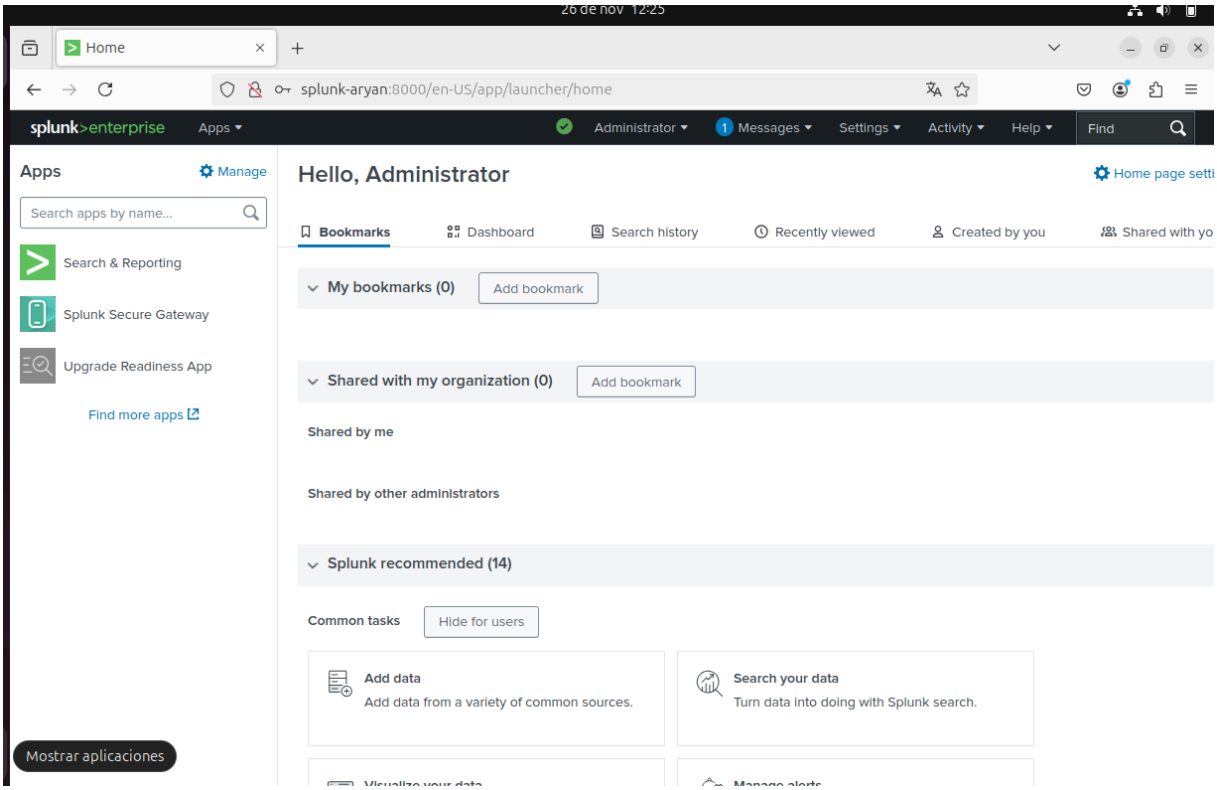

Figura 1.8: Conexión Splunk

1.3. Configuración inicial de Splunk

Lo primero que vamos a hacer es definir la arquitectura de nuestra práctica 1.9.

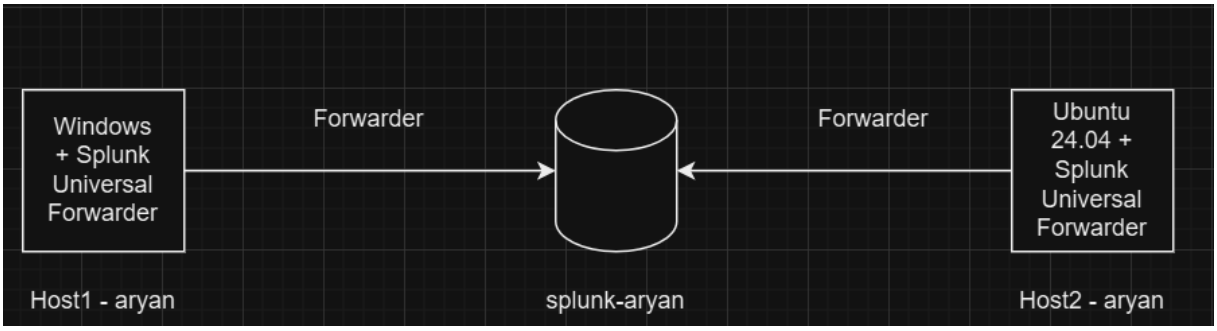

Figura 1.9: Arquitectura

Para que todo se pueda llevar acabo hay que configurar en nuestro splunk un puerto donde recibir los datos. Para ello accedemos al portal de splunk y vamos a ajustes y seleccionamos **Forwarding and Receiving** 1.10.

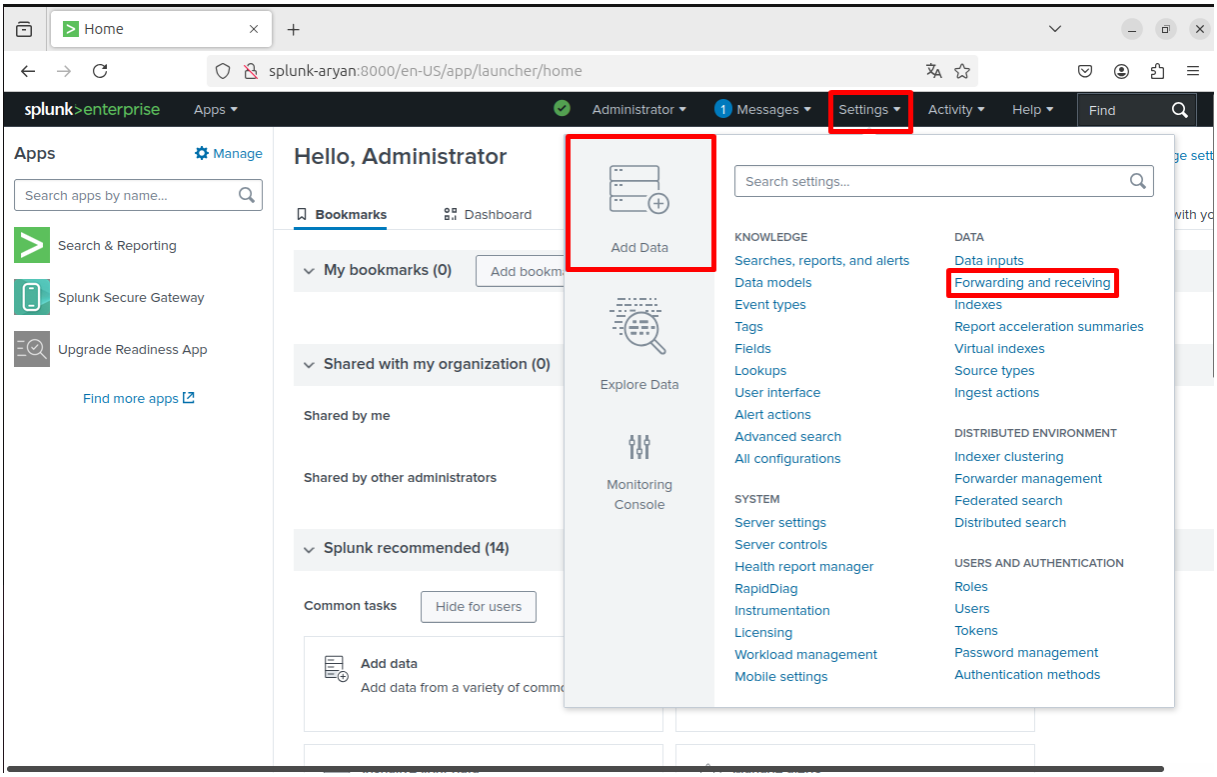

Figura 1.10: Añadir datos a Splunk, Forwarding and Receiving

Después seleccionamos hacemos clic en **Add New** para configurar los ajustes de recepción de datos 1.11

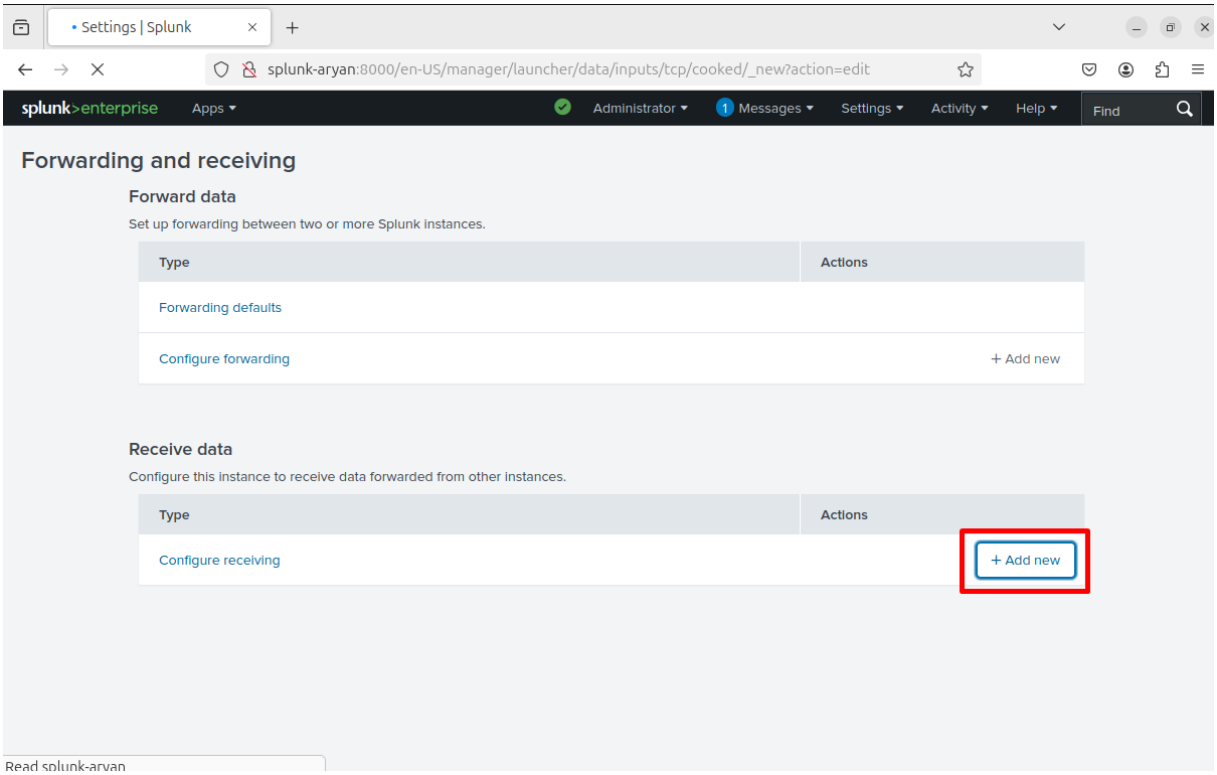

Figura 1.11: Añadir new reciving data a Splunk

E Introducimos el puerto 9997 y hacemos clic en **Save** para guardar la configuración 2.56.

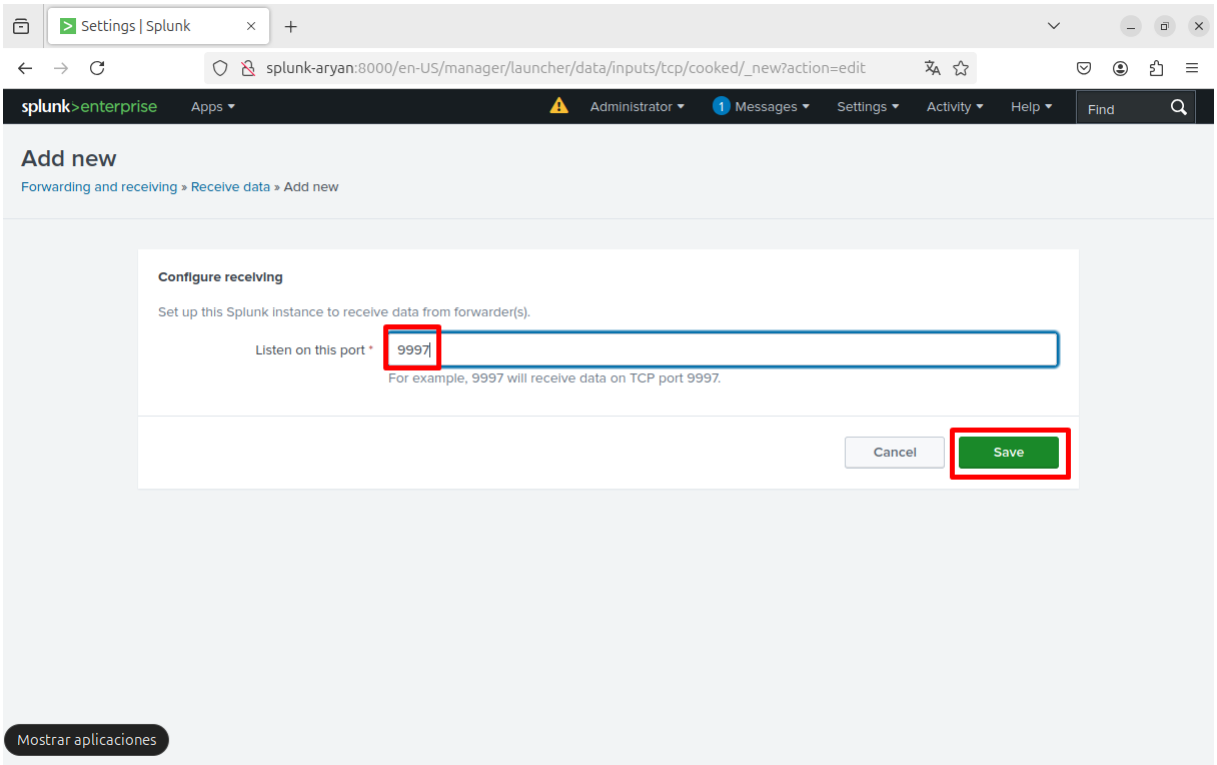

Figura 1.12: Añadir puerto y guardar ajustes en Splunk

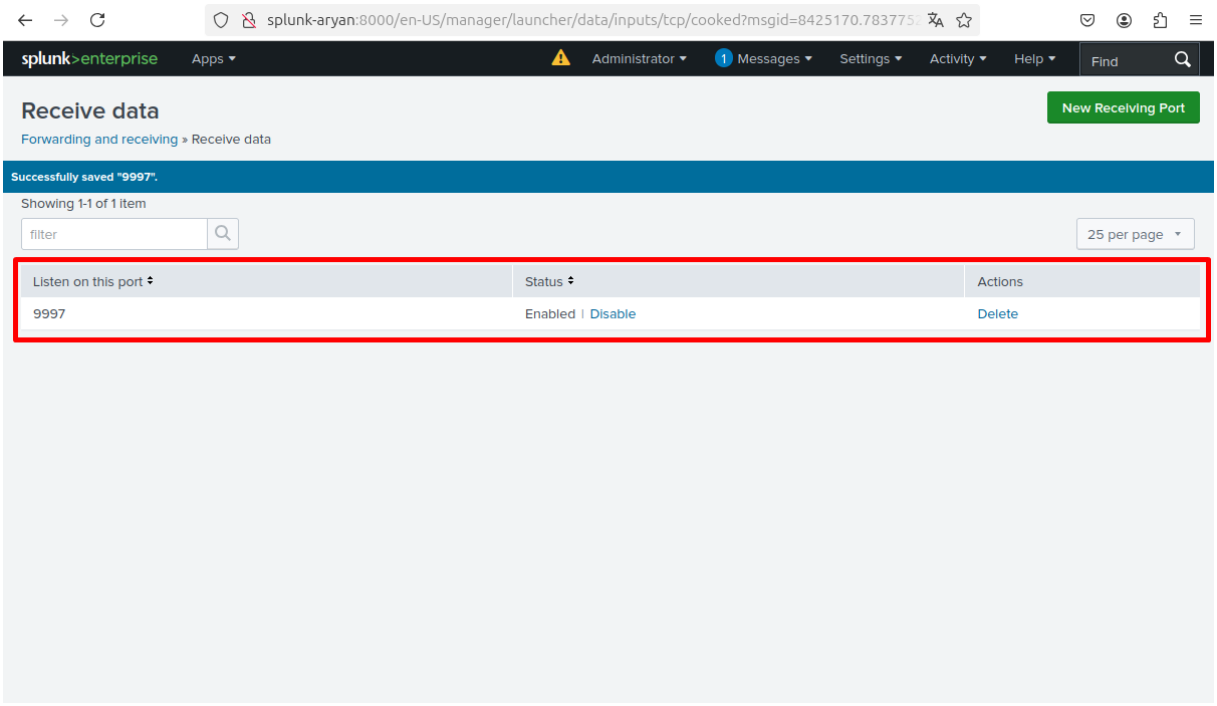

Figura 1.13: Puerto añadido Splunk

Como podemos ver 1.13 el puerto se ha añadido correctamente.

Después de configurar el puerto donde se recibirán los datos tenemos que crear nuestro repositorio donde se almacenarán los datos o el indexador.

Para ellos vamos a ajustes y le damos a **indexers** como podemos ver en 1.14

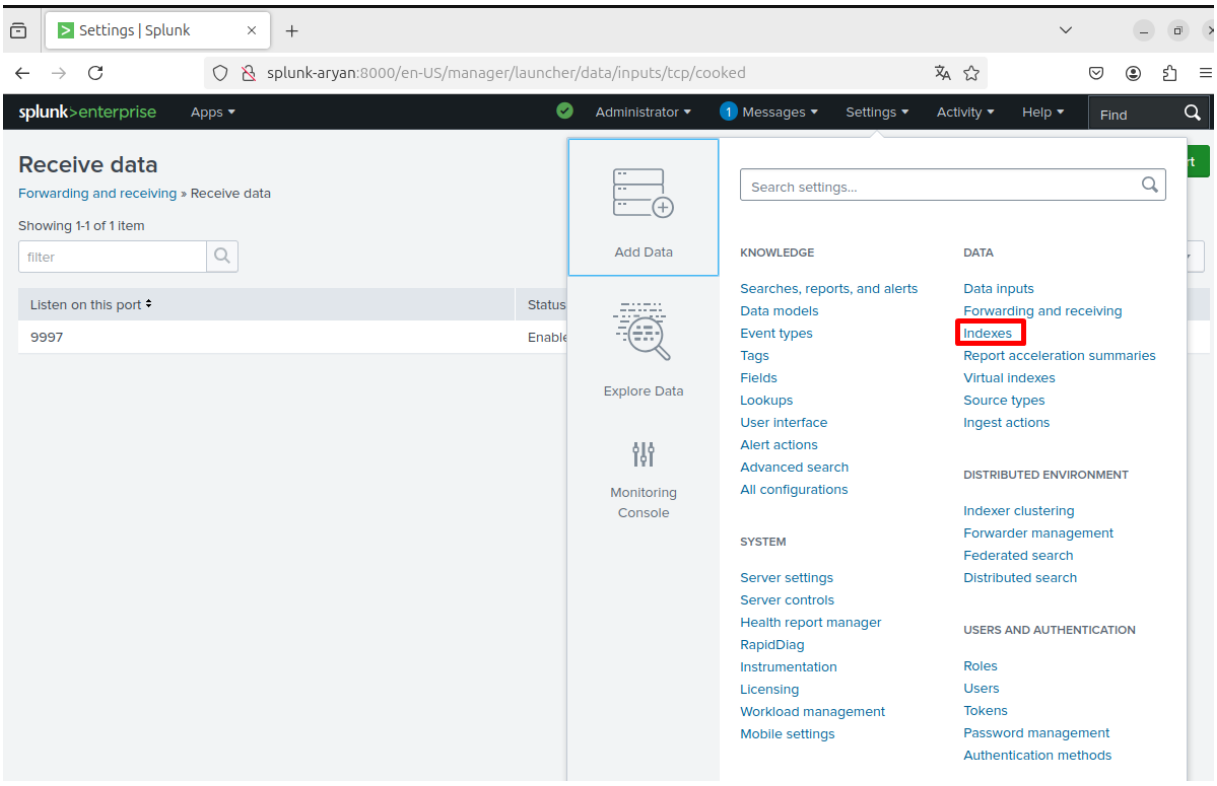

Figura 1.14: Crear Indexador

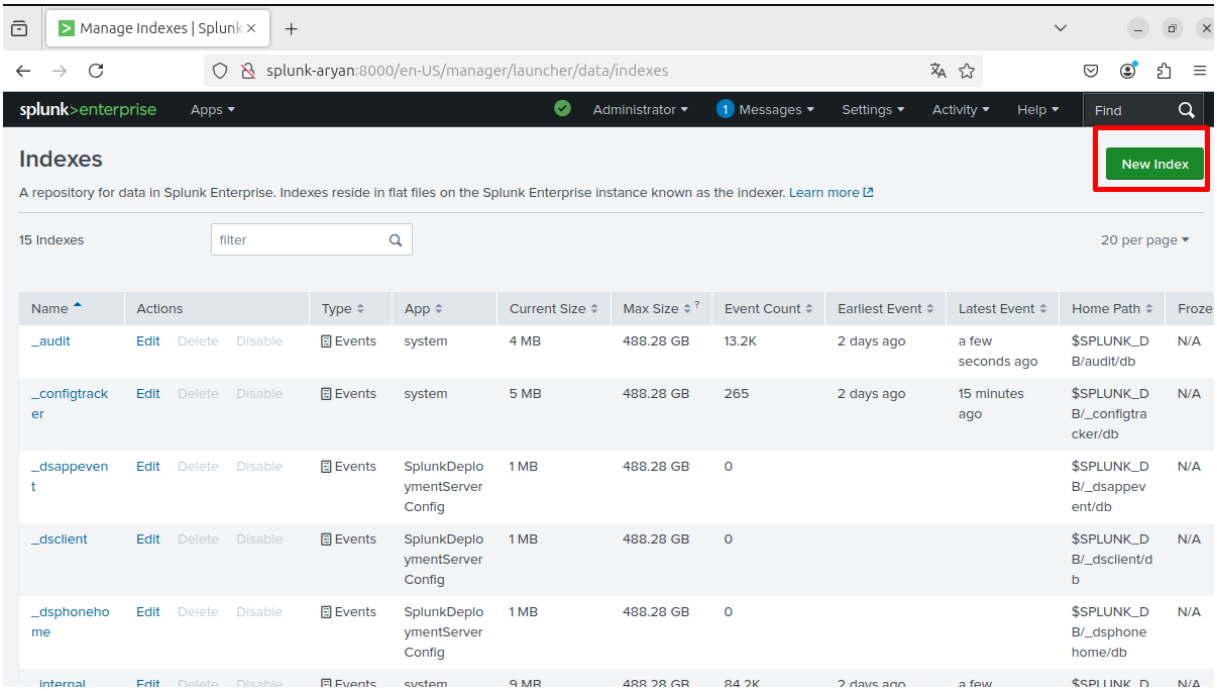

Figura 1.15: nuevo Indexador

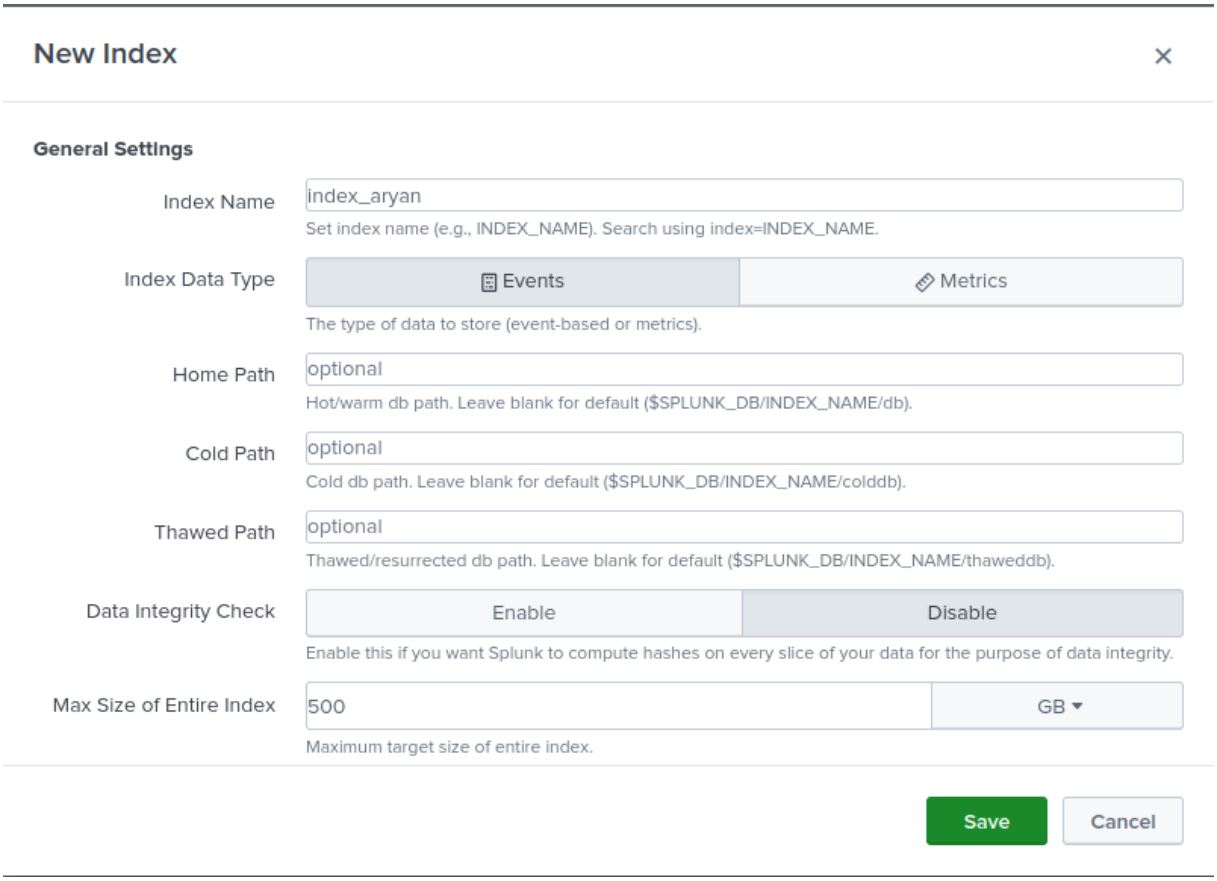

Figura 1.16: Indexador aryan

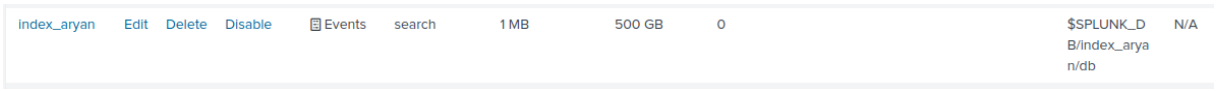

Figura 1.17: Creado indexador aryan

Una vez creado el indexador, ahora tenemos que instalar el agente y crear el monitoreo de los datos que se van a enviar.

1.4. Instalación de Splunk Universal Forwarder en Ubuntu

Vamos a instalar el agente ligero **splunk universal forwarder** en cada uno de nuestros hosts. **splunk universal forwarder** sirve para la recolección y reenvío de datos de diversas fuentes y enviarlos a una instancia central para su indexación y análisis.

Al primer hosts que le vamos a instalar splunk Universal Forwarder va a ser a un Ubuntu 24.04, para ello nos dirigimos a la página de descarga 1.18

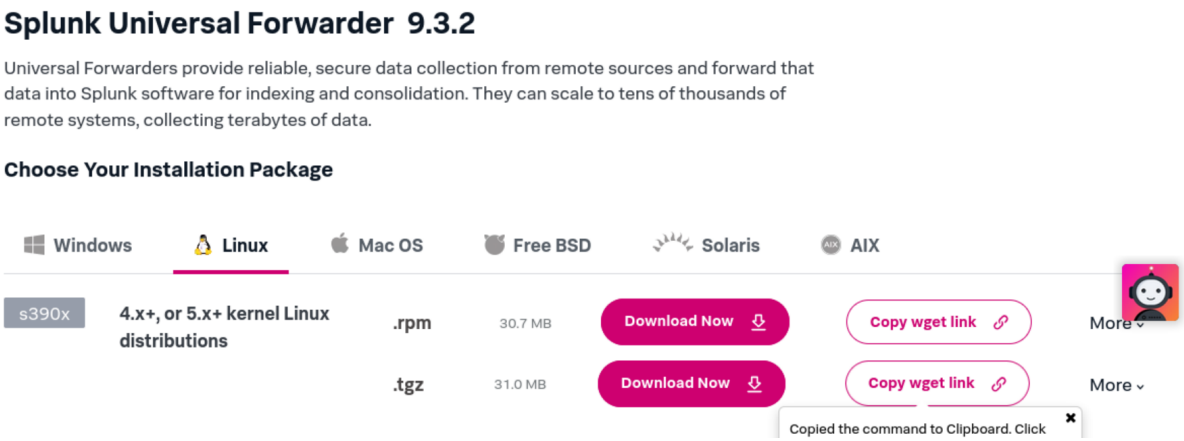

Figura 1.18: Página de descarga de Splunk Universal Forwarder

En nuestro ubuntu introducimos los comandos 1.19:

```
wget -O splunkforwarder-9.3.2-0dbe88b9ca7f-Linux-s390x.tgz
"https://download.splunk.com/products/universalforwarder/
releases/9.3.2/linux/splunkforwarder-9.3.2-0dbe88b9ca7f-Linux-s390x.tgz"

tar -xvzf splunkforwarder-9.3.2-0dbe88b9ca7f-Linux-s390x.tgz
```

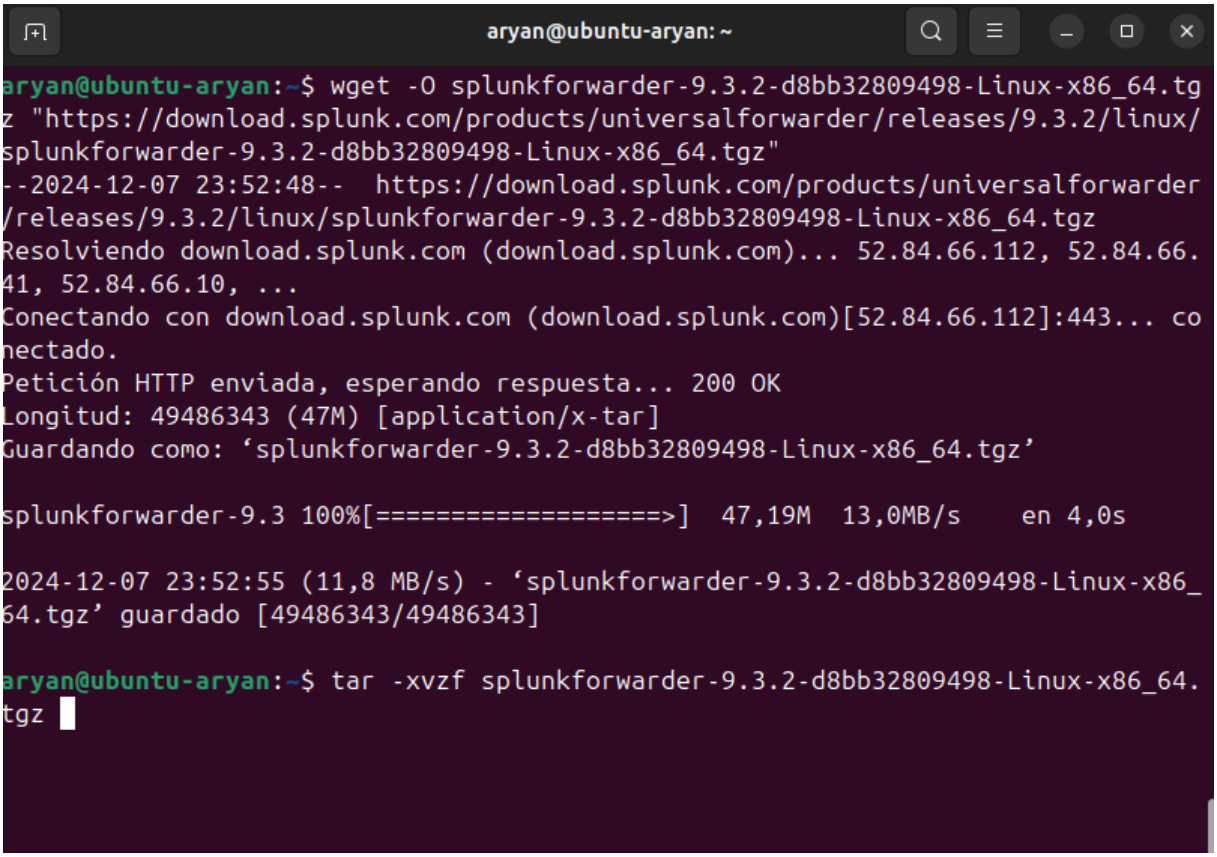

Figura 1.19: Comandos para la descarga de Splunk Universal Forwarder

```
cd splunkforwarder

sudo ./bin/splunk start --accept-license
```

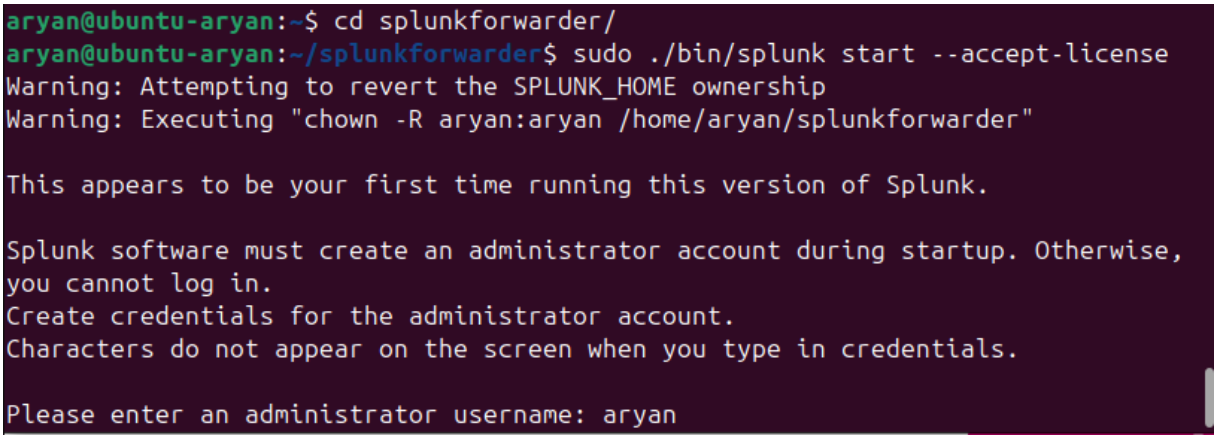

Figura 1.20: Comando para activar Splunk Universal Forwarder

Nos pedirá un nombre de administrador y una contraseña: **aryan:aryan123** 1.20 y una vez finalice ya tendremos splunk universal forwarder activado 1.21.

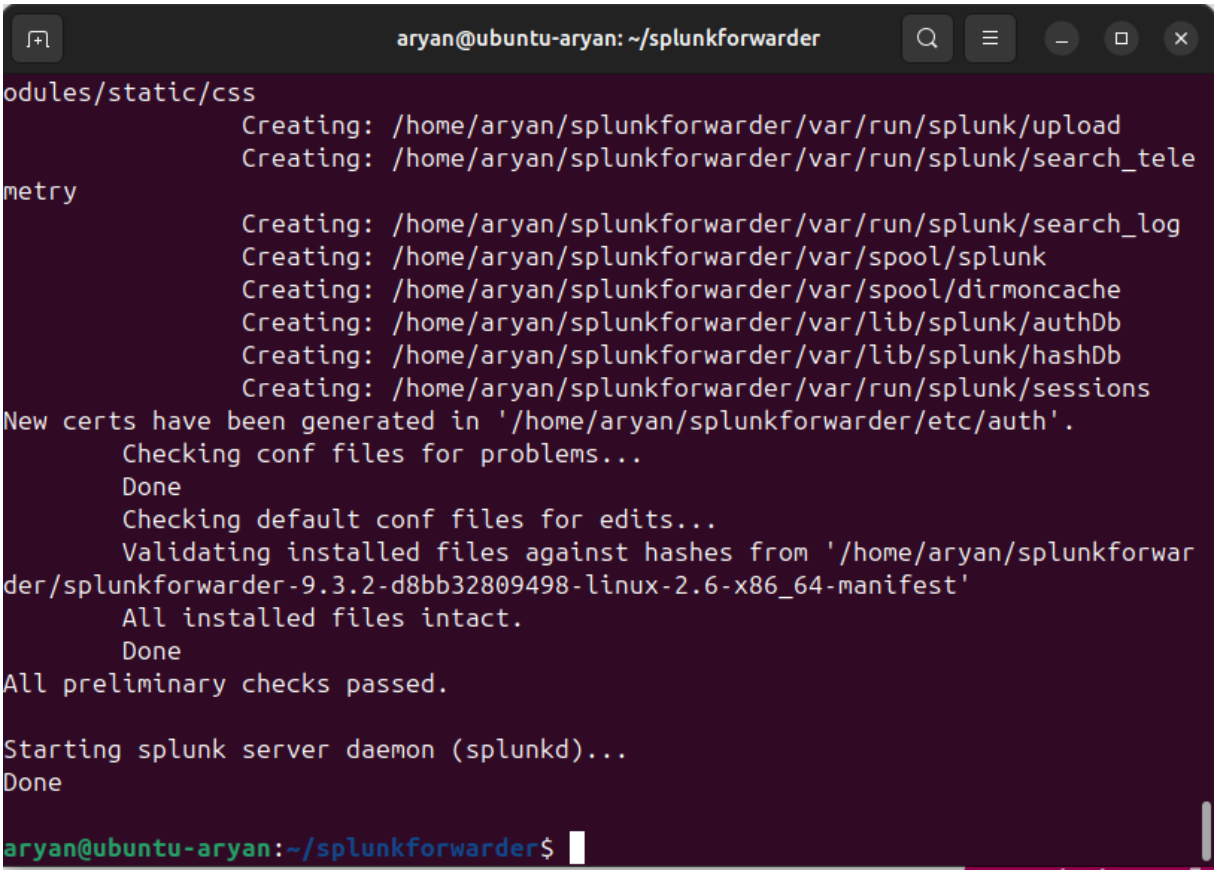

Figura 1.21: Splunk Universal Forwarder activado

Ahora tenemos que especificar el servidor con el splunk enterprise. Para ello vamos al ubuntu con el splunk Universal Forwarder y escribimos el siguiente comando:

```
~/splunkforwarder/bin/splunk add forward-server 192.168.1.155:9997
```

Lanzando este comando configuraremos la conexión del reenvío al servidor splunk enterprise y nos generará un archivo outputs.conf 1.22.

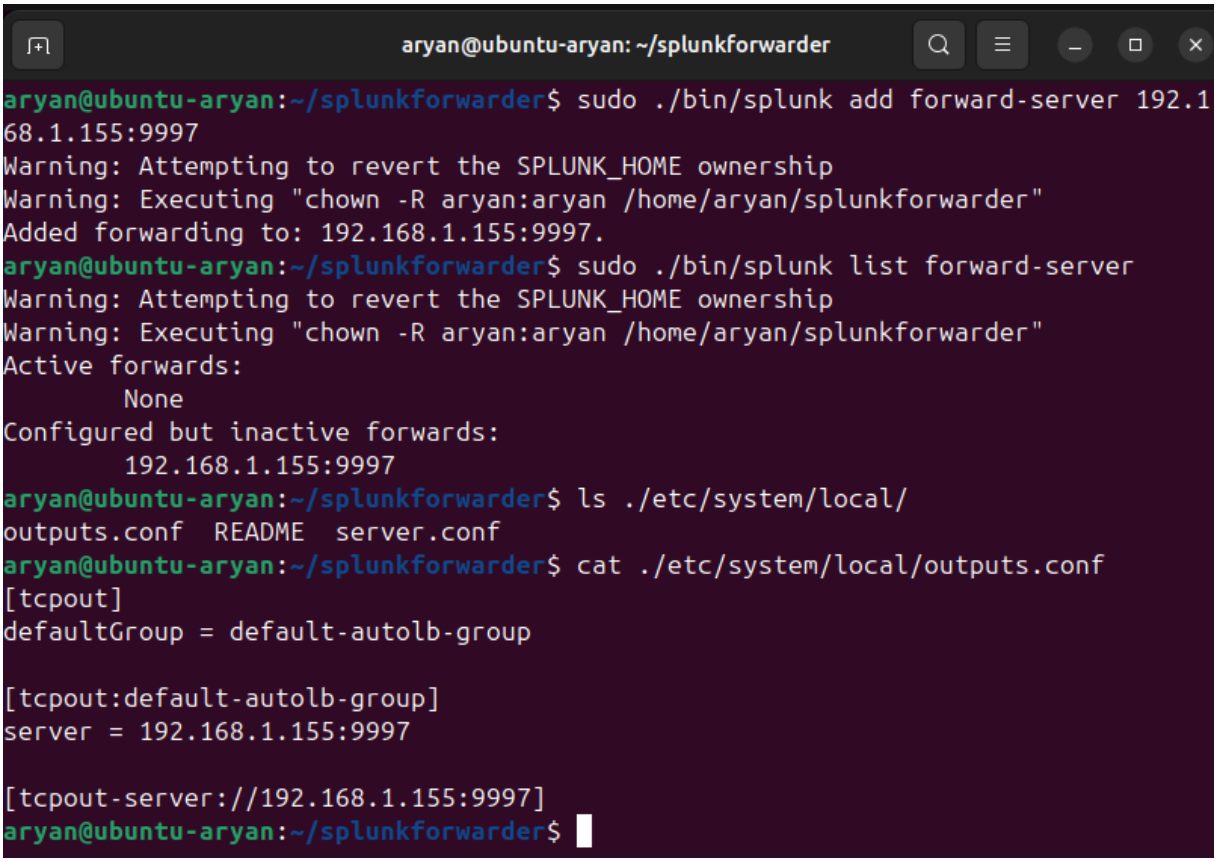

Figura 1.22: Pasos configuración Splunk Universal Forwarder

Como podemos ver en la imagen 1.22 cuando verificamos si el reenvio esta bien nos aparece que esta configurado el servidor pero tiene le reenvío inactivo, para ello vamos a modificar el archivo outputs.conf de la siguiente forma 1.23

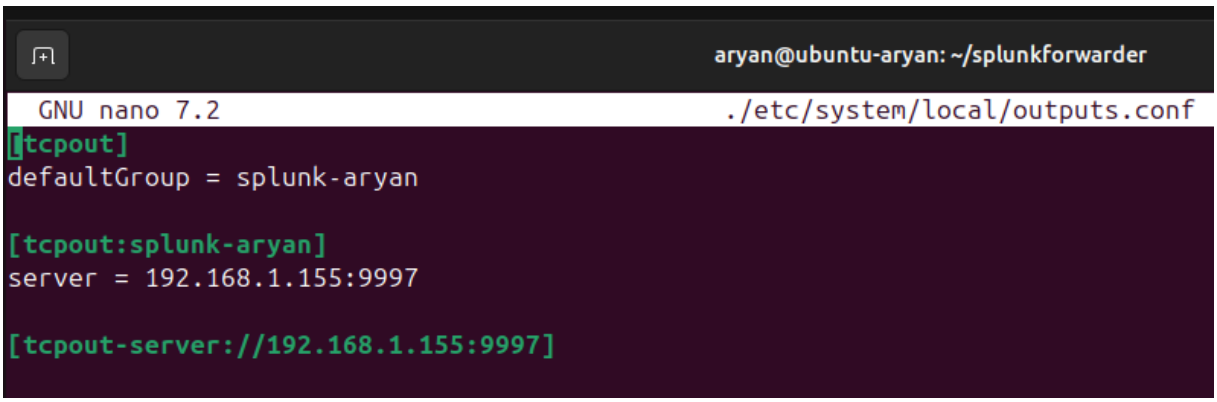

Figura 1.23: Archivo Outputs.conf

Una vez hecho esto vamos a reiniciar y el reenvio esta correcto.

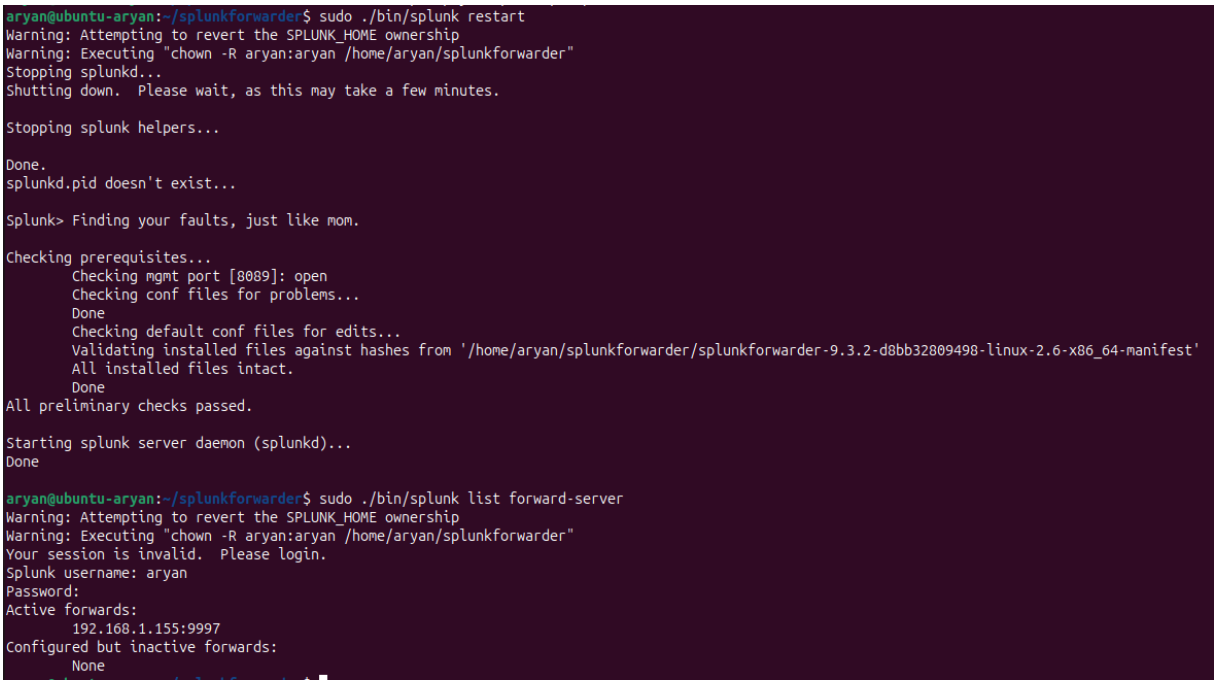

Figura 1.24: Reinicio y verificación

Y como podemos ver 1.24 ya se nos ha configurado correctamente. (También para que se aplique los cambios por si acaso hemos reiniciado el agente)

```
~/splunkforwarder/bin/splunk restart
```

1.4.1. Gestión de datos de registro

Una vez instalado y configurado todo, vamos a gestionar los datos que enviamos a nuestro indexador. Queremos enviar los datos de inicio de sesión en nuestro sistema operativo ubuntu 24.04, para ello tenemos que monitorear los datos:

```
~/splunkforwarder/bin/splunk add monitor /var/log/auth.log
-index index_aryan -sourcetype authlogs
```

Vamos a enviar a nuestro splunk enterprise, los logs de auth.log 1.25.

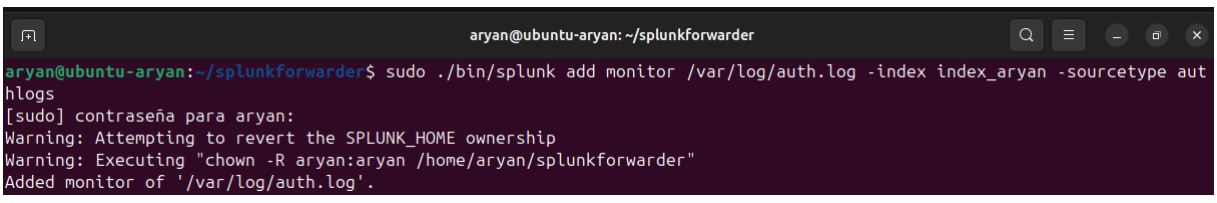

Figura 1.25: Enviar datos al indexador

Para verificar que se ha añadido correctamente vamos lanzar el siguiente comando 1.26:

```
~/splunkforwarder/bin/splunk list monitor
```

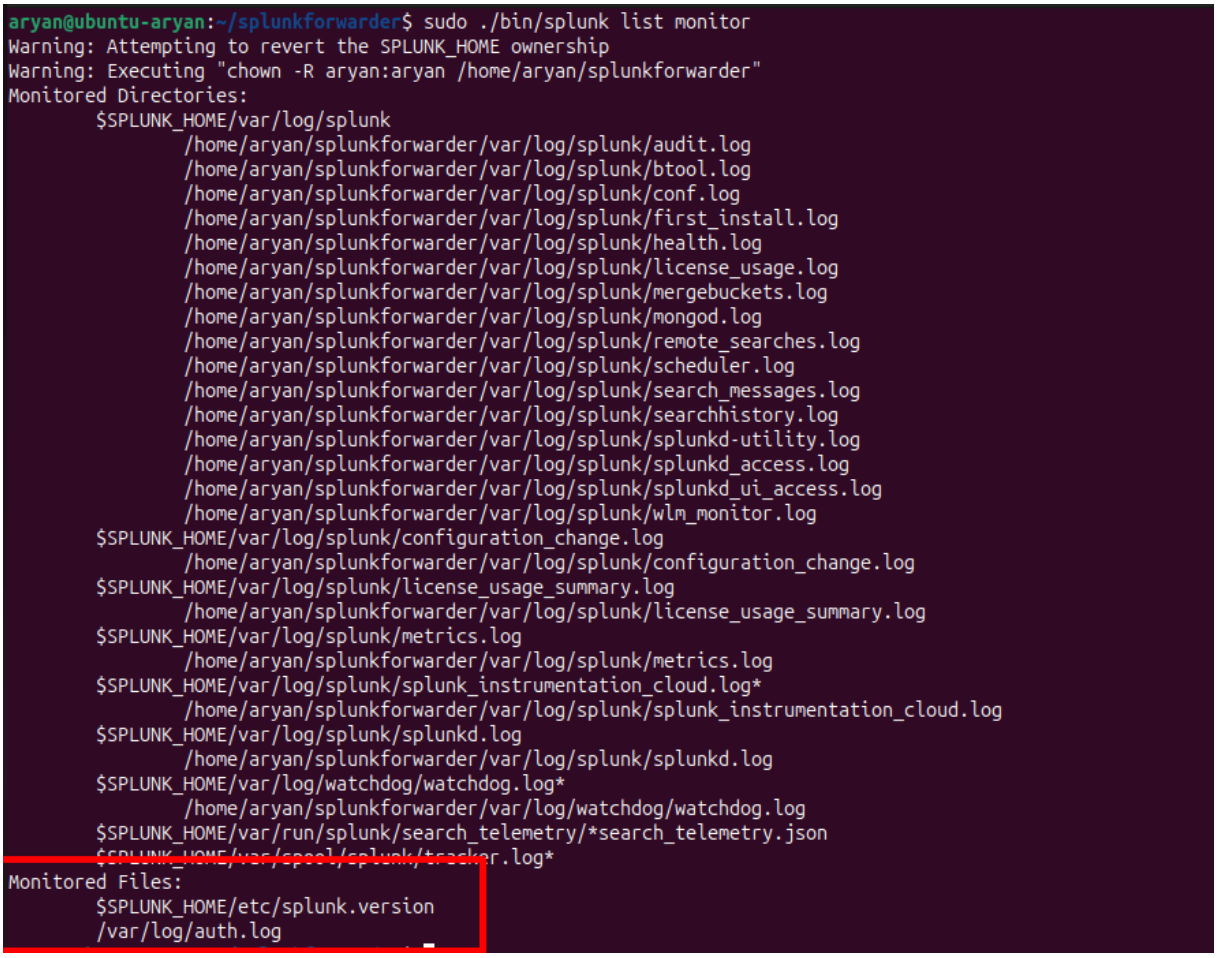

Figura 1.26: Verificación de monitoreo

Ahora los eventos se estarán enviando a nuestro indexador y como podemos ver 1.27 como se han enviado ya datos.

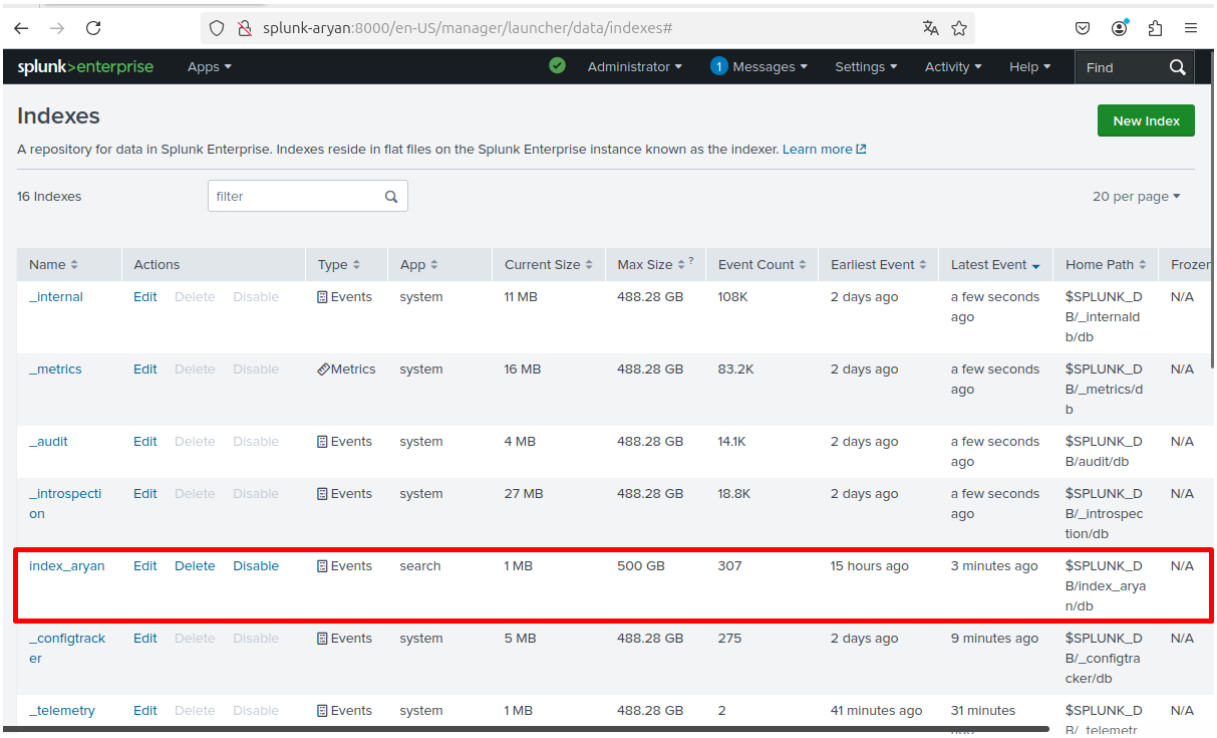

Figura 1.27: Verificación de datos enviados

1.4.2. Análisis de eventos

Para poder analizar los datos que se estan enviando desde nuestro sistema operativo ubuntu, vamos a ir a 1.28

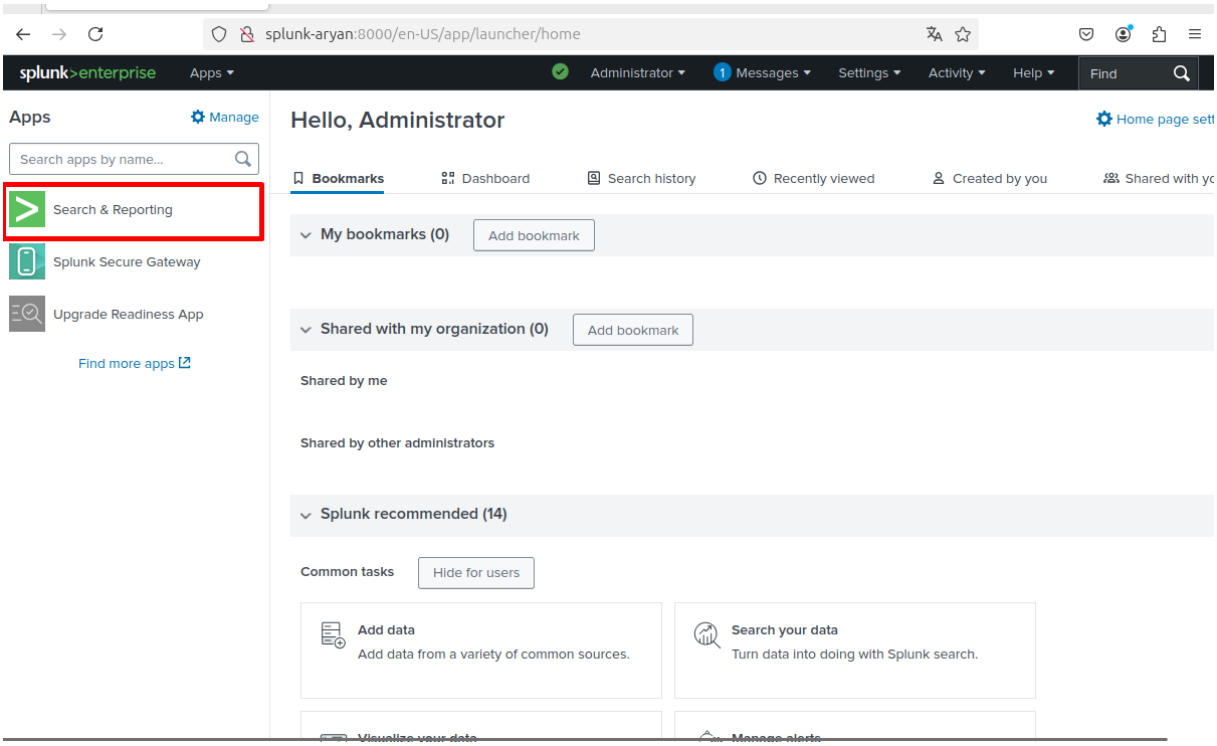

Figura 1.28: Buscar eventos

Una vez aqui ponemos en el buscador:

```
index=index_aryan
```

Que nos mostrará todos los eventos disponibles en index_aryan **??**.

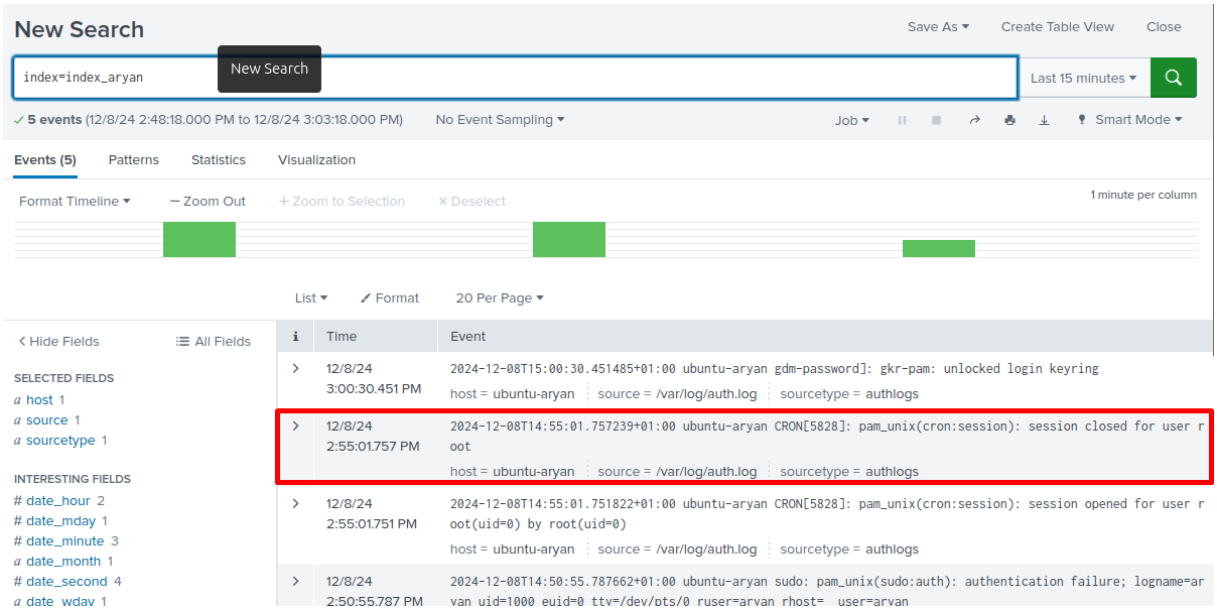

Figura 1.29: Eventos index_aryan

Ahora vamos a hacer una prueba y vamos a hacer unos inicios de sesión fallidos, introduciendo una contraseña incorrecta 1.30 y después iniciaremos correctamente.

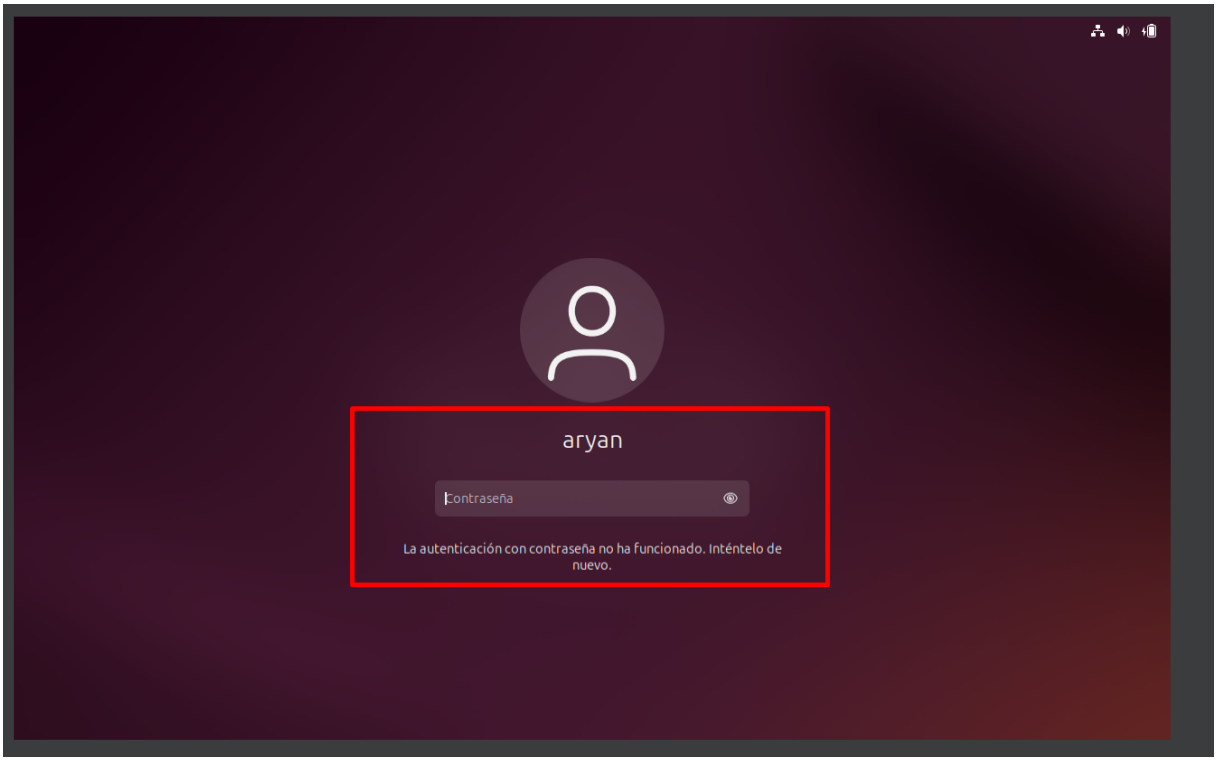

Figura 1.30: Inicio de sesión incorrecto

ahora vamos a ver si nuestro splunk enterprise nos muestra estos eventos, para ello buscamos

el indexador como inicimos anteriormente.

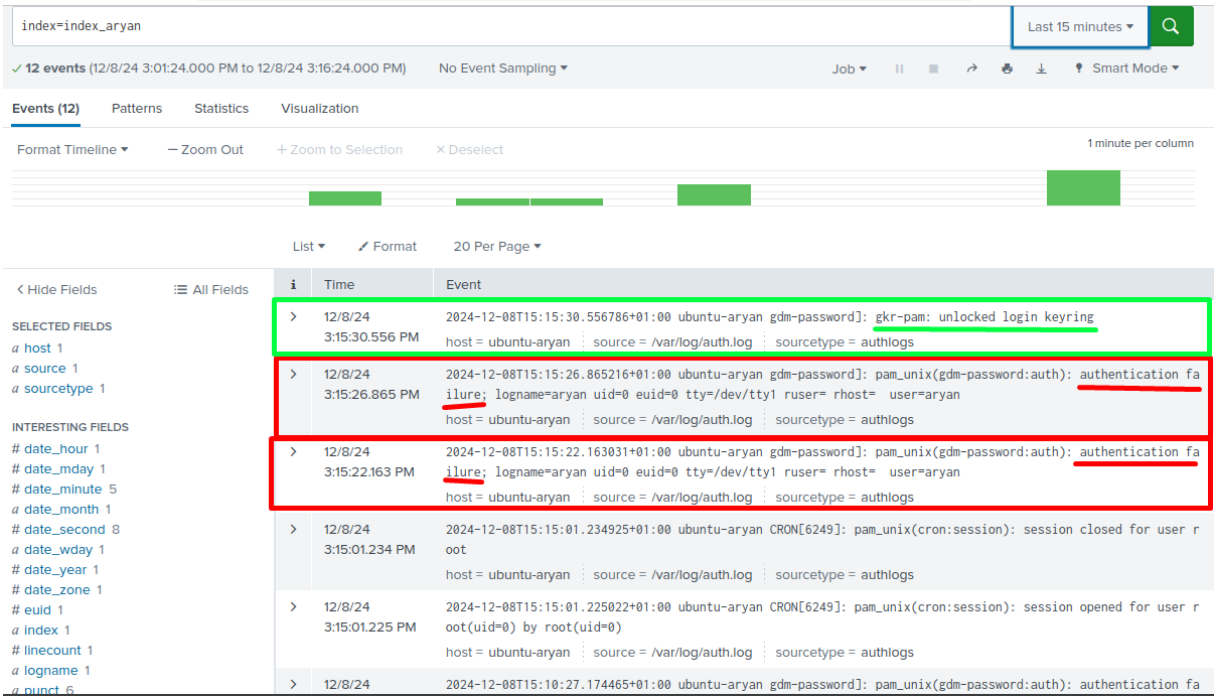

Figura 1.31: Pruebas Inicio de sesión

Comos podemos ver en 1.31 en color **rojo** tenemos los eventos que equivalen a los fallos de autenticación y en **verde** el log in correcto.

Además que podemos ver información sobre los eventos si lo desplegamos.

1.4.3. Creación de visualizaciones en Splunk

En este apartado vamos a crear un dashboard de barras que muestre la cantidad de eventos de inicio de sesión exitosos y fallidos.

Para ello primero vamos a hacer una busqueda para contabilizar los eventos.

```
index="index_aryan" sourcetype="authlogs" source="/var/log/auht.log"
| eval event_type=case(
like(_raw, "%unlocked login keyring%"), "Unlocked Keyring",
like(_raw, "%authtentication failure%"), "Authtentication Failure")
| stats cound by event_type
```

Con esta busqueda lo que hacemos es crear un campo event_type que se asigna con base en el contenido de los eventos. Se usa *like* para buscar patrones especificos en el campo *_raw*.

Si el campo *_raw* contiene unlocked login keyring, se marca como Unlocked Keyring y si tiene authtentication failure se marca como Authtentication Failure.

Y después cuenta cuantos eventos exiten para cada tipo. 1.40

Una vez tenemos listados todos los eventos y contado podemos darle a visualización 1.32.

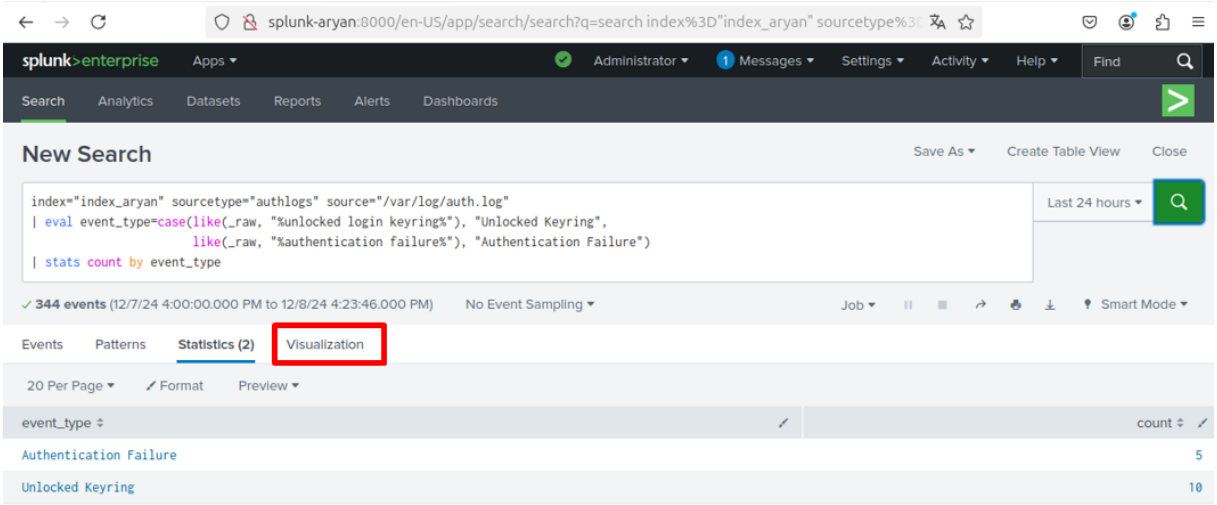

Figura 1.32: Visualización de eventos

Y podremos ver una grafica en columnas de los eventos 1.33.

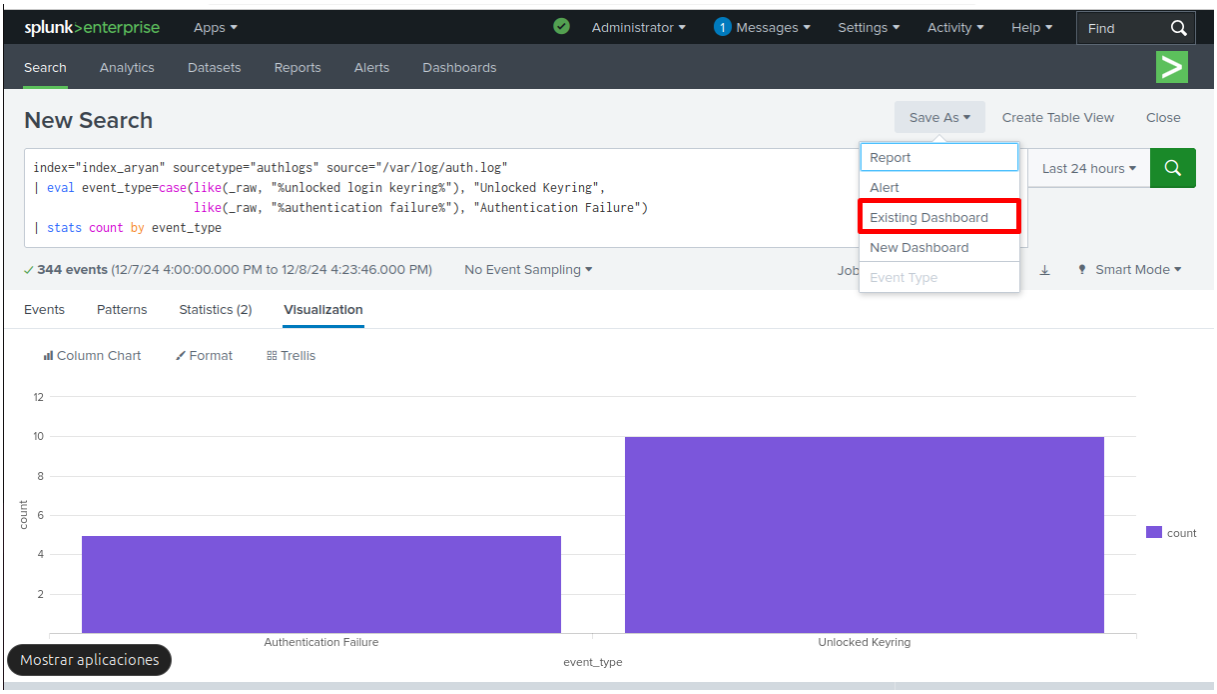

Figura 1.33: Gráfica en columnas

Una vez aqui le damos a Guardar como y elegimos un dashboard existente que ya teniamos creado 1.34.

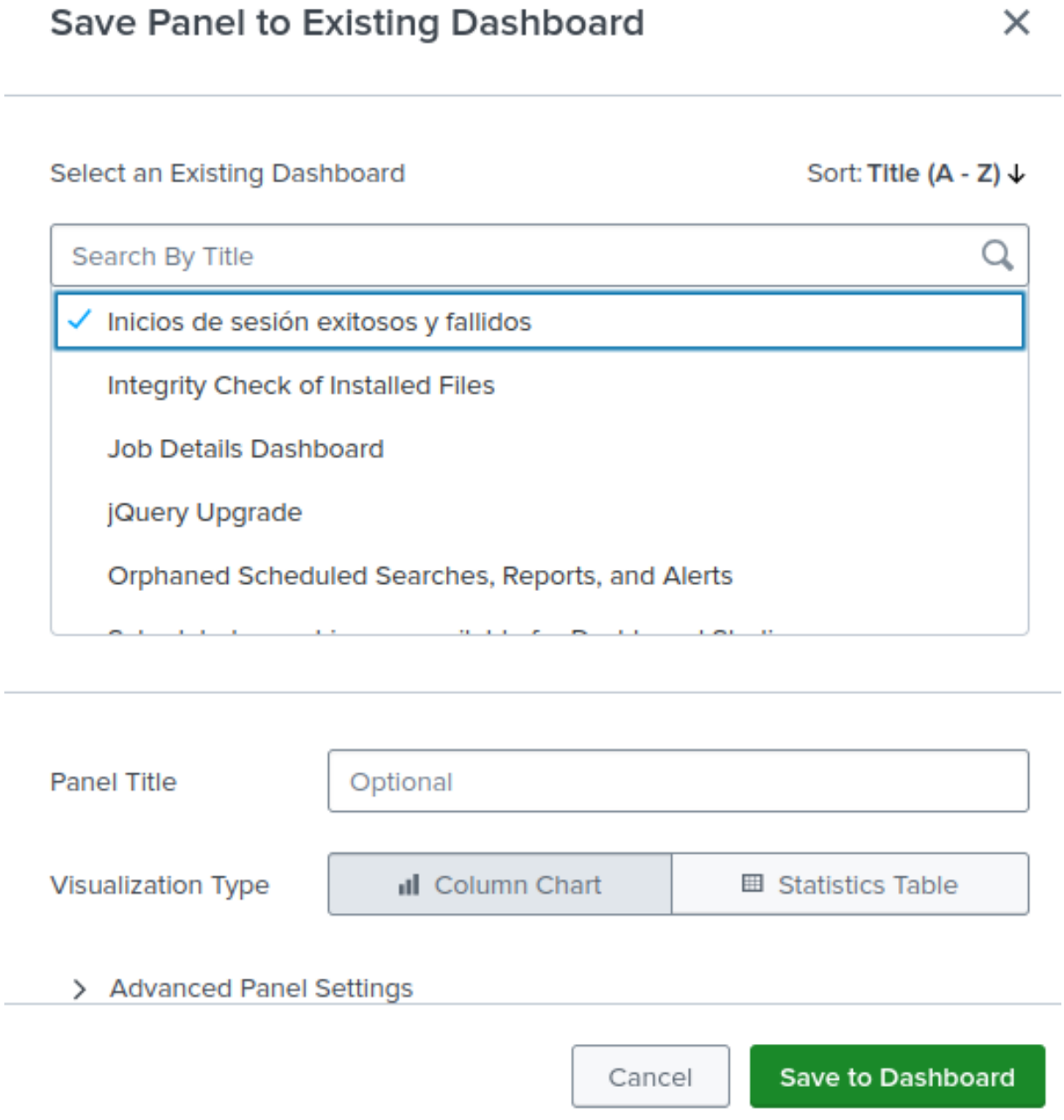

Figura 1.34: Guardar en dashboard existente

Nos saltará una alerta de que sea ha creado un panel en el dashboard y cuando accedamos a el veremos la gráfica de columnas pero lo editamos y elegios la gráfica de barras y ya tendriamos la gráfica y la visualización de ello 1.35.

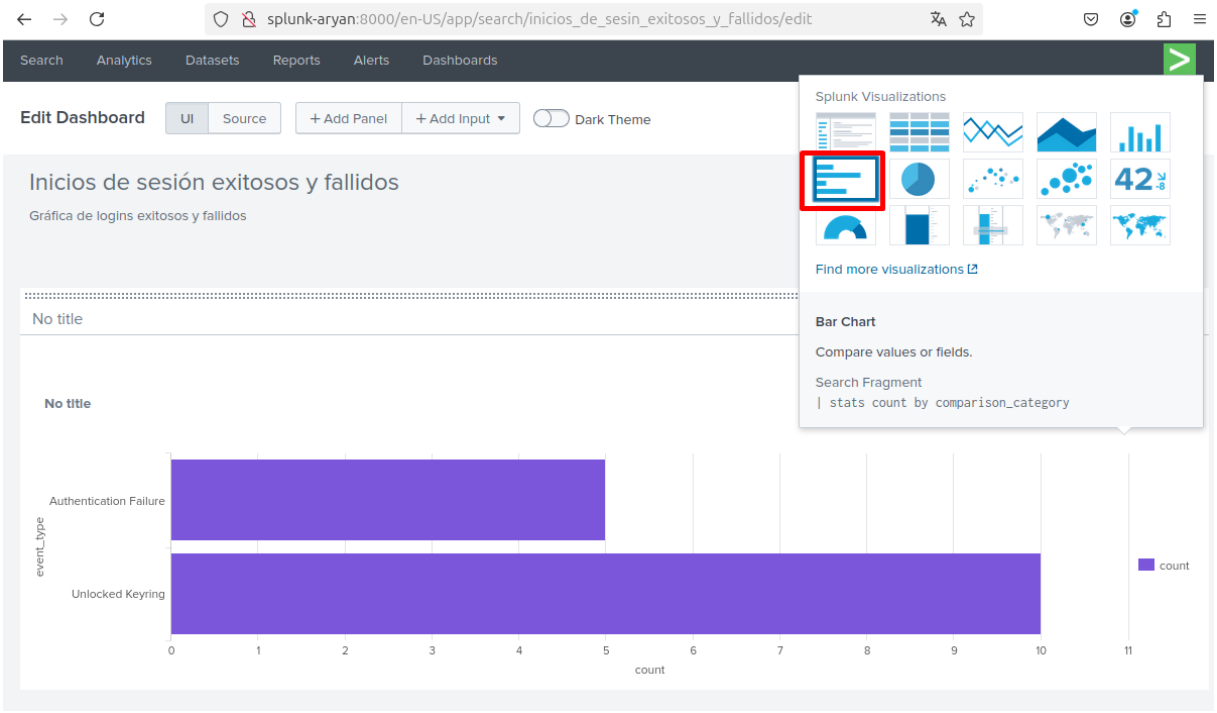

Figura 1.35: Gráfica de barras

Y ya tendremos en el dashboard la gráfica de barras.

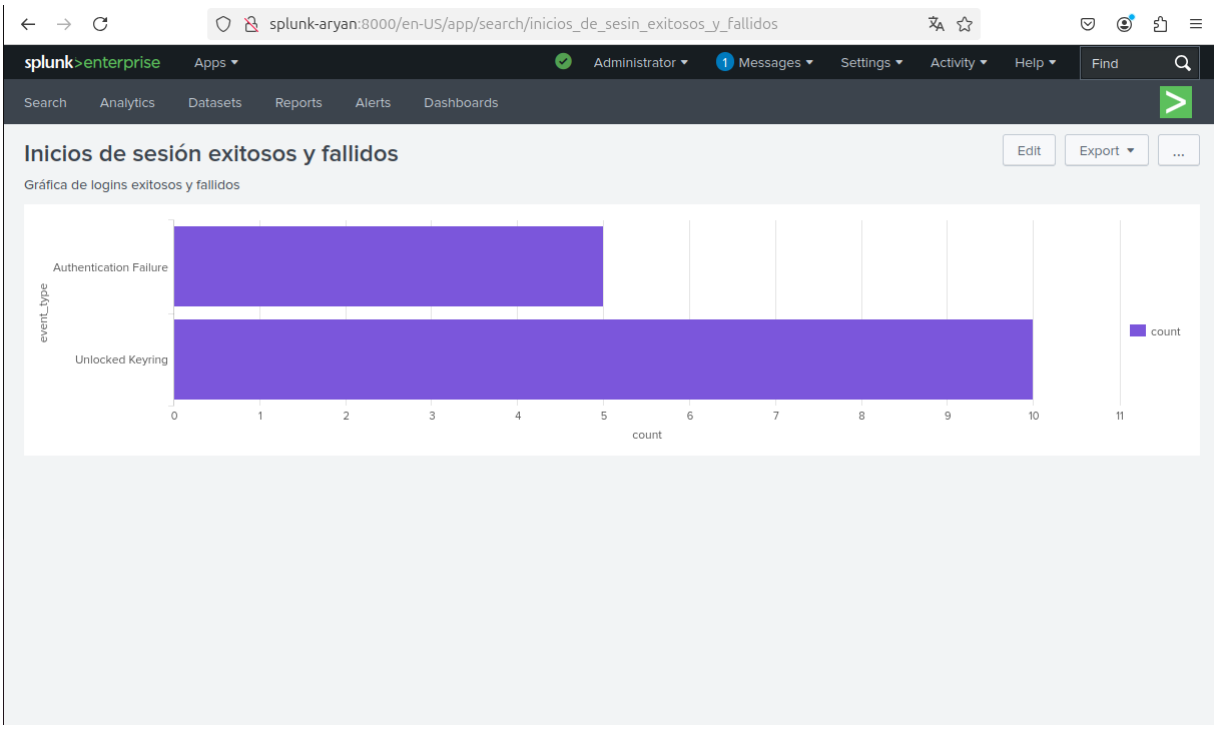

Figura 1.36: Gráfica de barras

Además se pueden crear muchas más gráficas y analizar eventos y exportarlos a PDF's.

Otra forma de generar los dashboard sería de la siguiente manera.

Para ello nos vamos a nuestro splunk enterprise y en el mismo sito que en 1.28, hacmeos clic en Dashboard 1.37

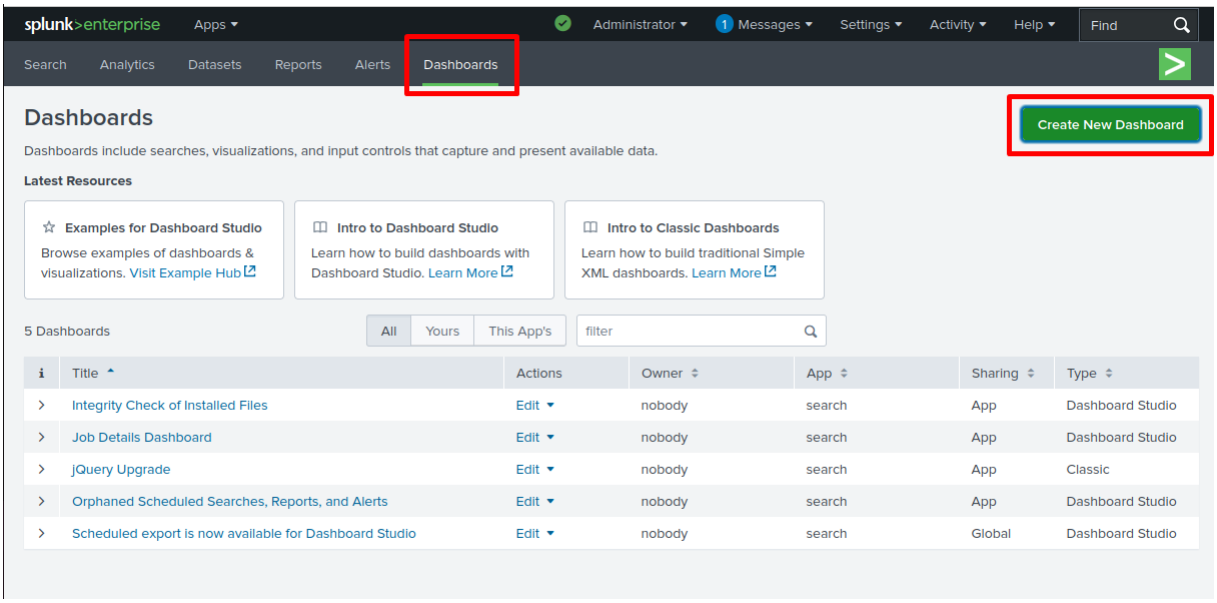

Figura 1.37: Nuevo dashboard

Después de seleccionar crear nuevo dashboard 1.38 introducimos un nombre y el constructor, en nuestro caso el clásico.

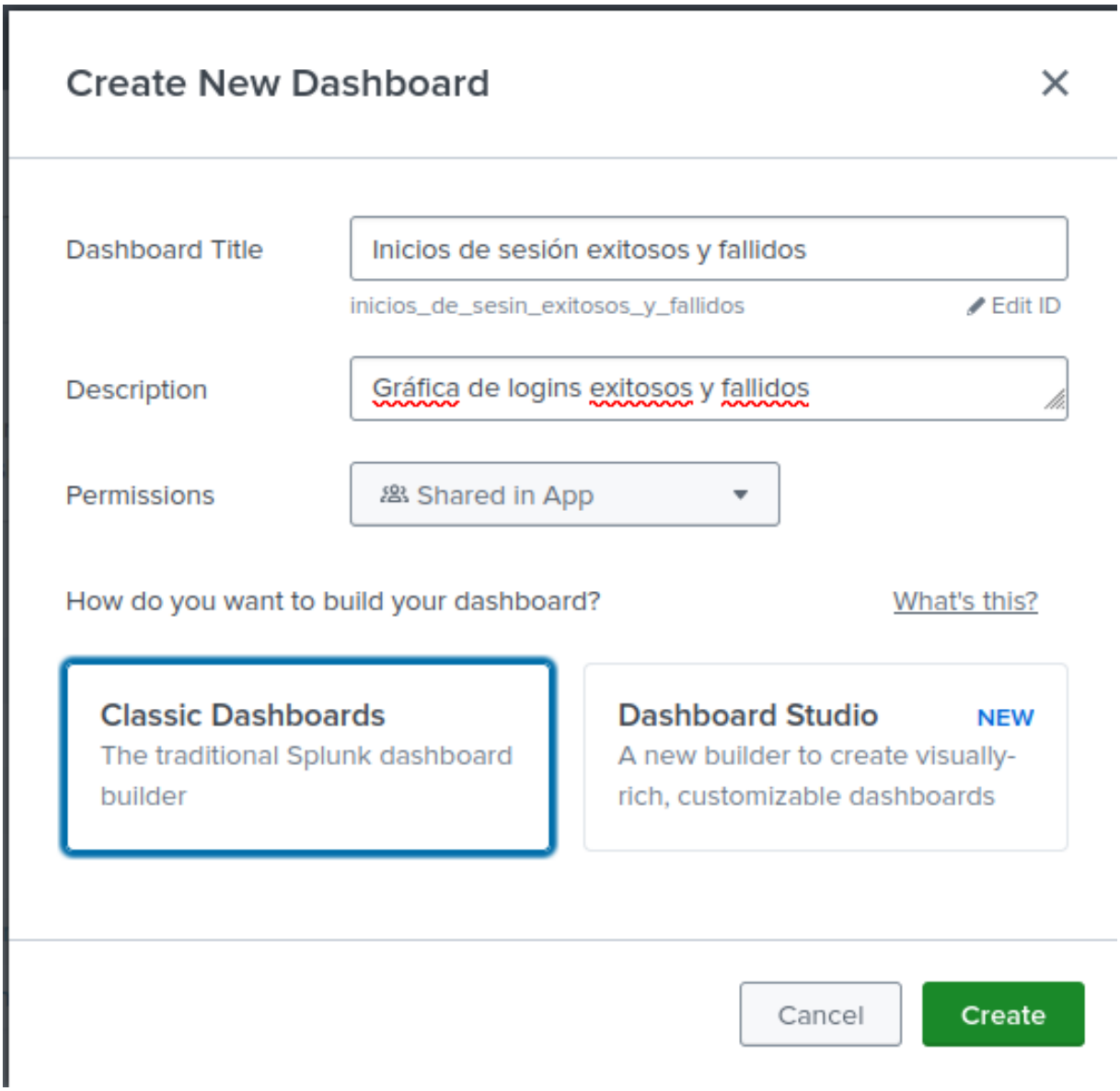

Figura 1.38: Crear nuevo dashboard

Y podremos añadir los paneles que queramos, haciendo clic en Add Panel 1.39 (si no lo vemos habrá que dar a editar) y podemos ver todos los paneles que se pueden crear y añadir.

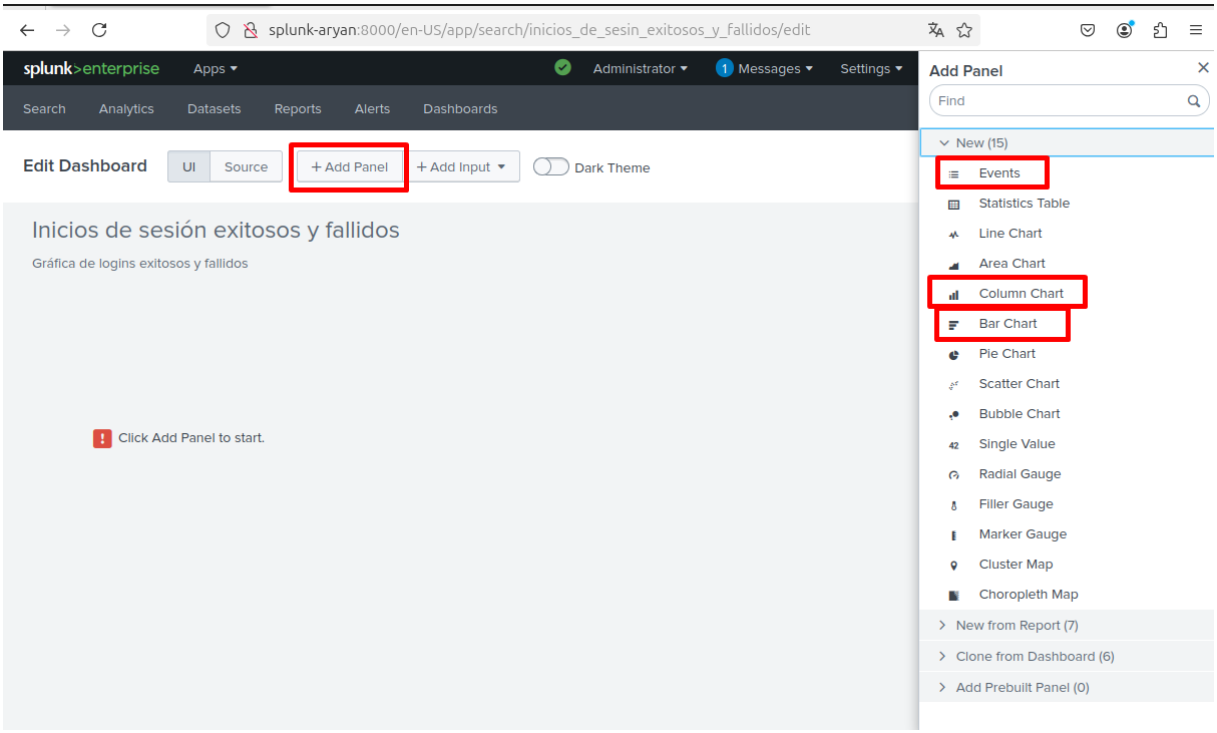

Figura 1.39: Añadir paneles

Aunque para ello hay que crear una query de busqueda como en el caso anterior y como vemos en 1.40

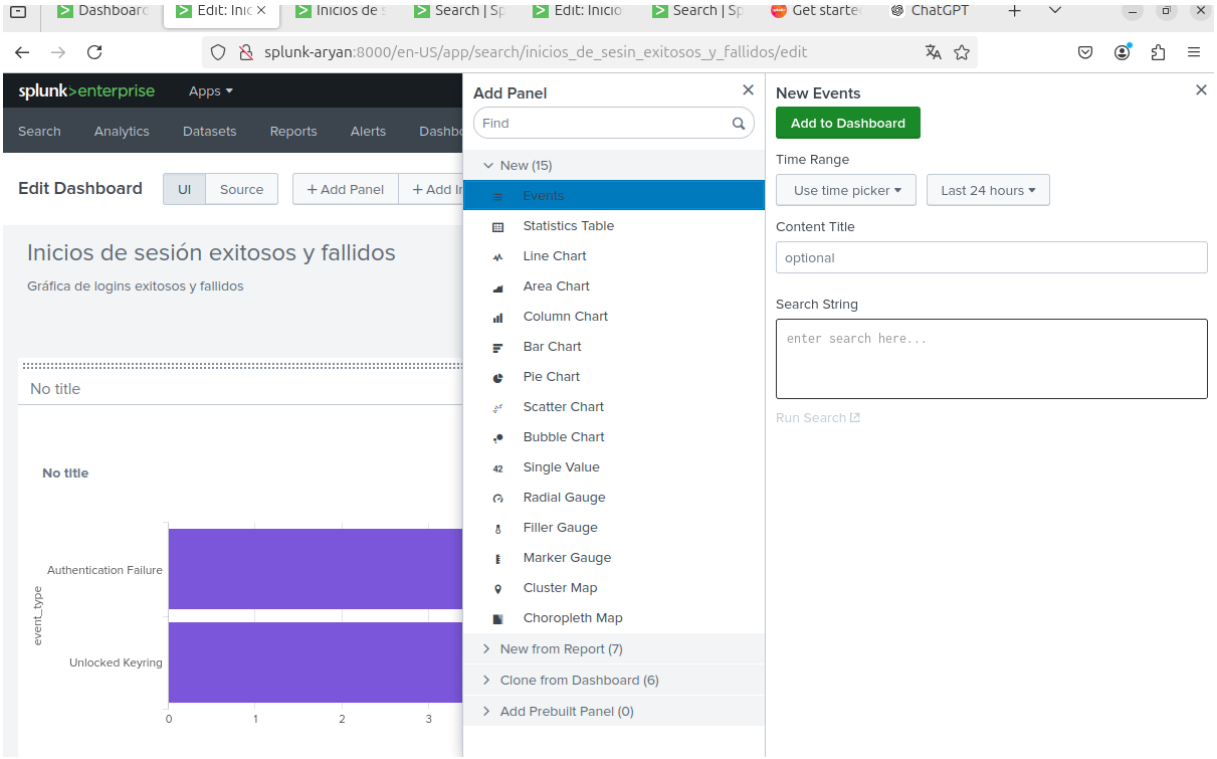

Figura 1.40: Añadir paneles nuevos, busqueda

1.5. Instalación de Splunk Universal Forwarder en Windows

Una vez visto como gestionar y enviar los eventos en un sistema operativo ubuntu vamos a hacer lo mismo pero en una máquina windows.

Antes de comenzar con la instalaciíon vamos a ver si las máquinas se ven entre si.

```
aryan@splunk-aryan:~$ ping -c 3 192.168.1.137
PING 192.168.1.137 (192.168.1.137) 56(84) bytes of data.
^C
--- 192.168.1.137 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2079ms
```

Figura 1.41: Ping fallido

Para evitar problemas vamos a desactivar el Firewall de nuesro máquina virtual windows.

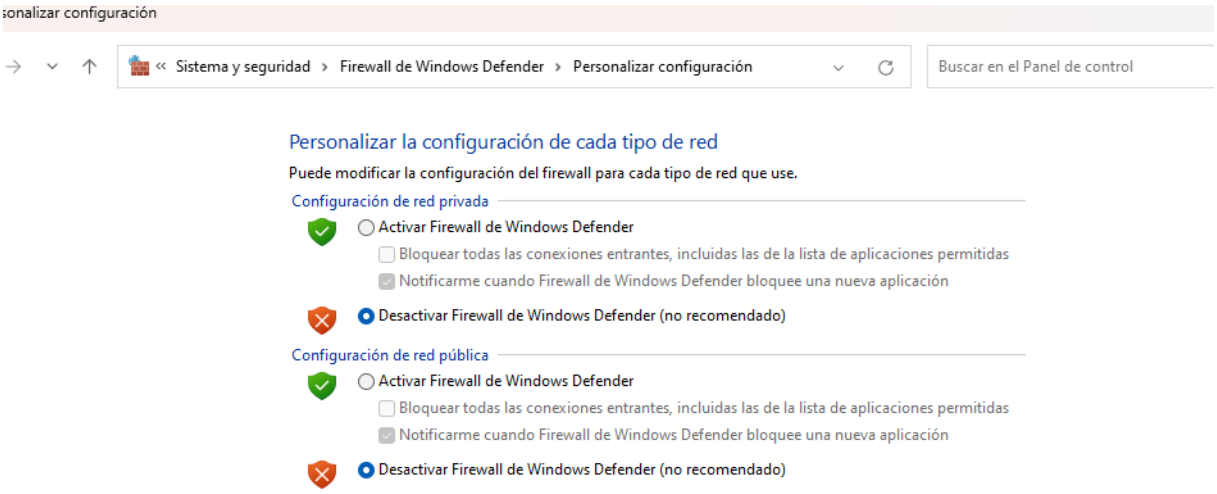

Figura 1.42: Desactivar Firewall MV

Y ahora ya nuestras máquinas podran verse.

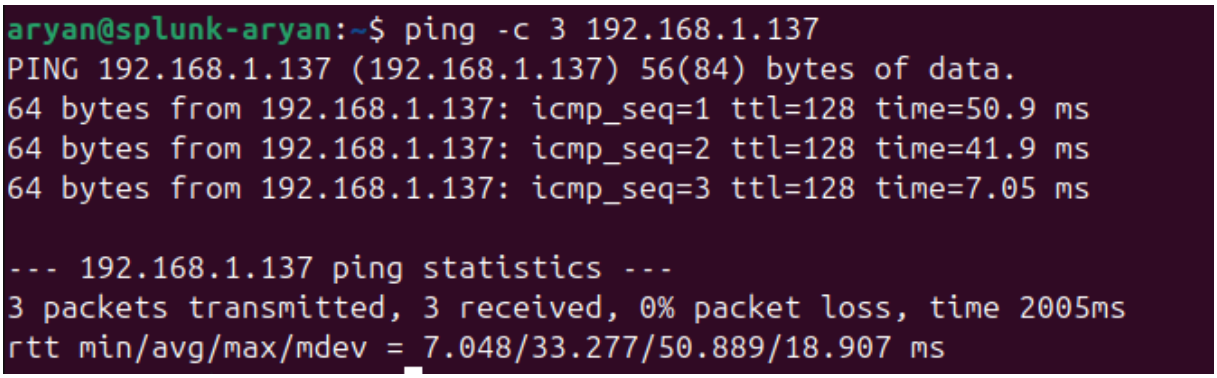

Figura 1.43: Ping exitoso

Ahora vamos a instalar el univeral forwarder para ello accedemos a la página de splunk y nos decargamos el agente Splunk Universal Forwarder en nuestra máquina windows 1.44.

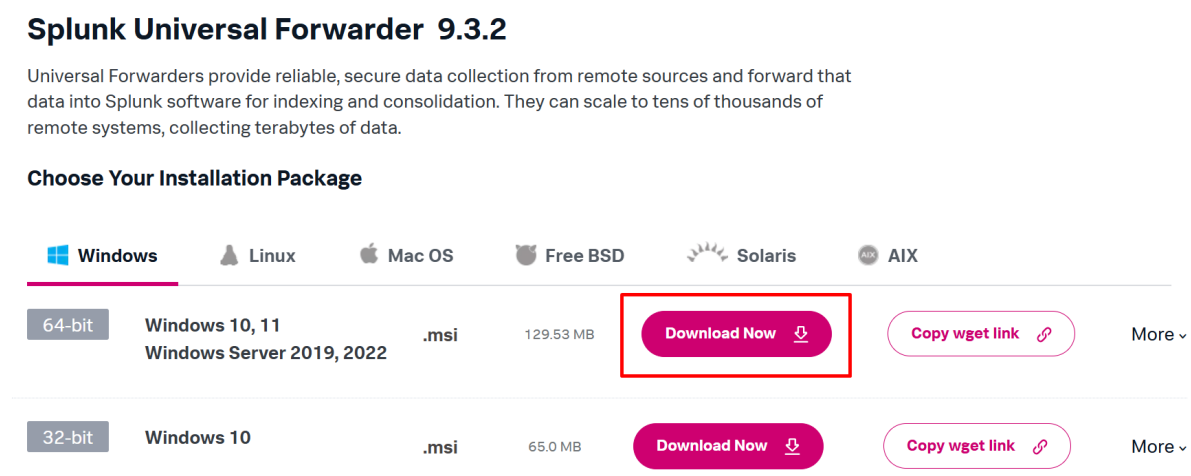

Figura 1.44: Descarga el agente para windows

Ejecutamos el archivo como administradores que se nos descarga y aceptamos la licencia, y le damos a **Customize Options**. Le damos **Next** a las siguientes dos pestañas que nos salg.

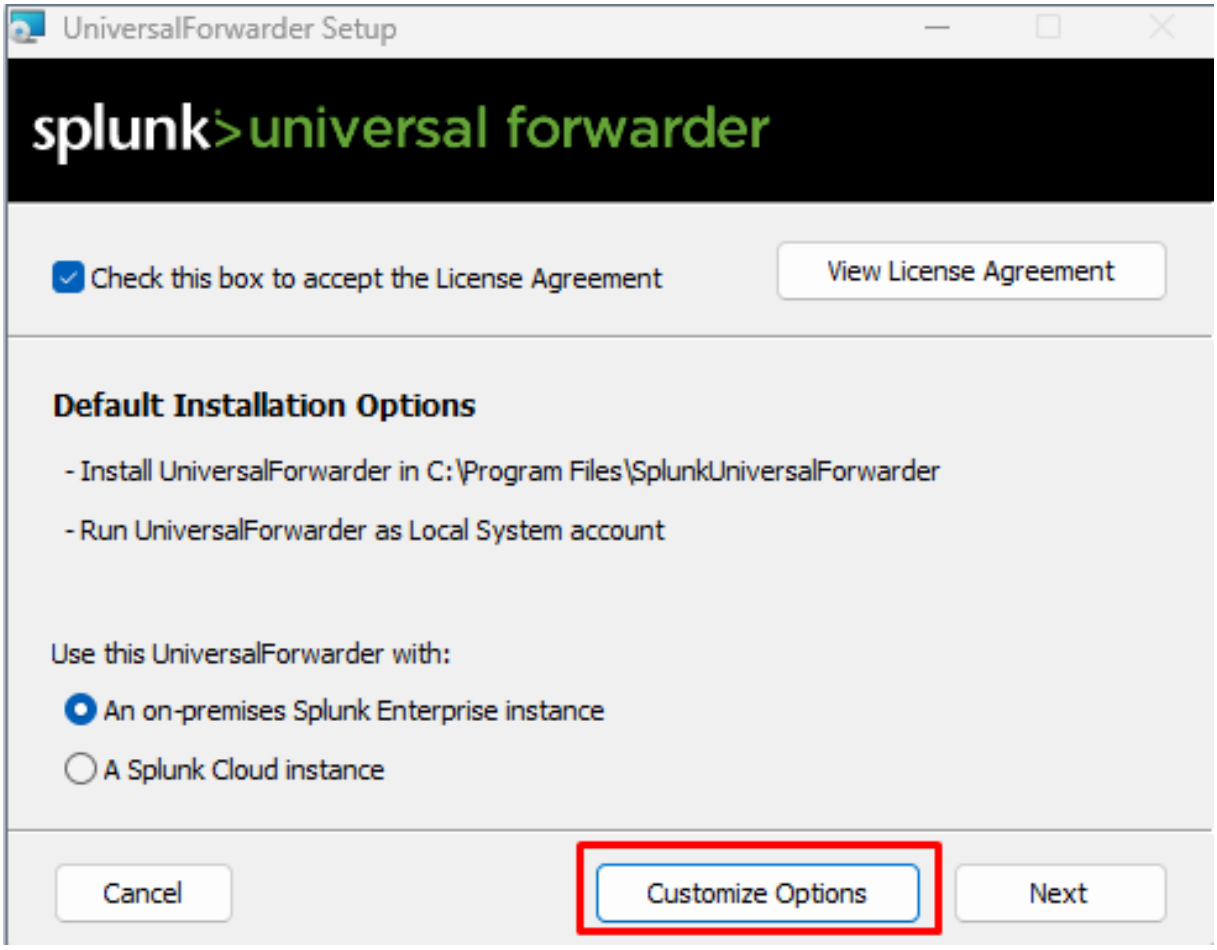

Figura 1.45: Licencia windows

Aqui seleccionamos **Local System** ya que tiene acceso completo al sistema local, ideal para configuraciones donde el Forwarder solo necesita leer datos del sistema local.

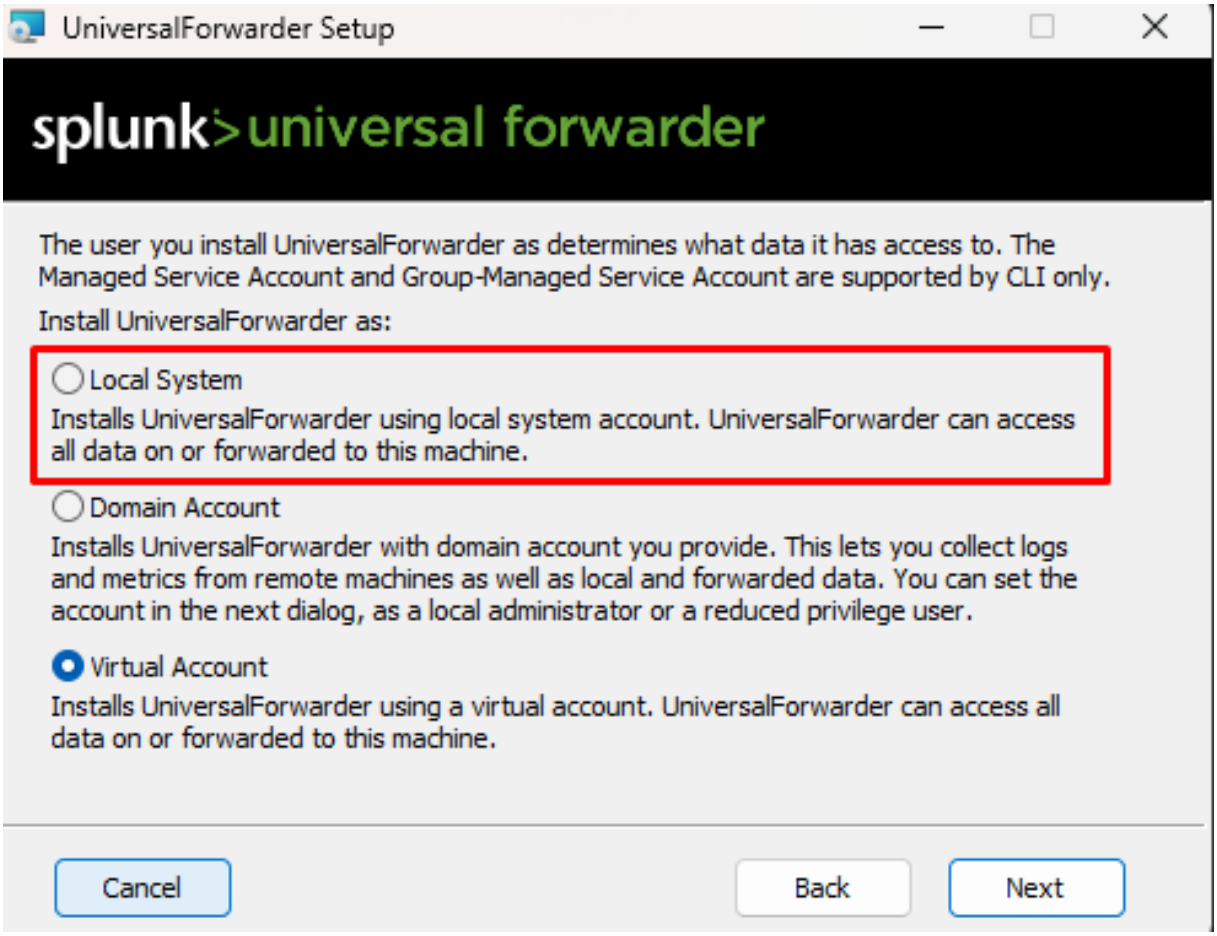

Figura 1.46: Local System

Ahora vamos a seleccionar los logs que queremos que registre de nuestro windows.

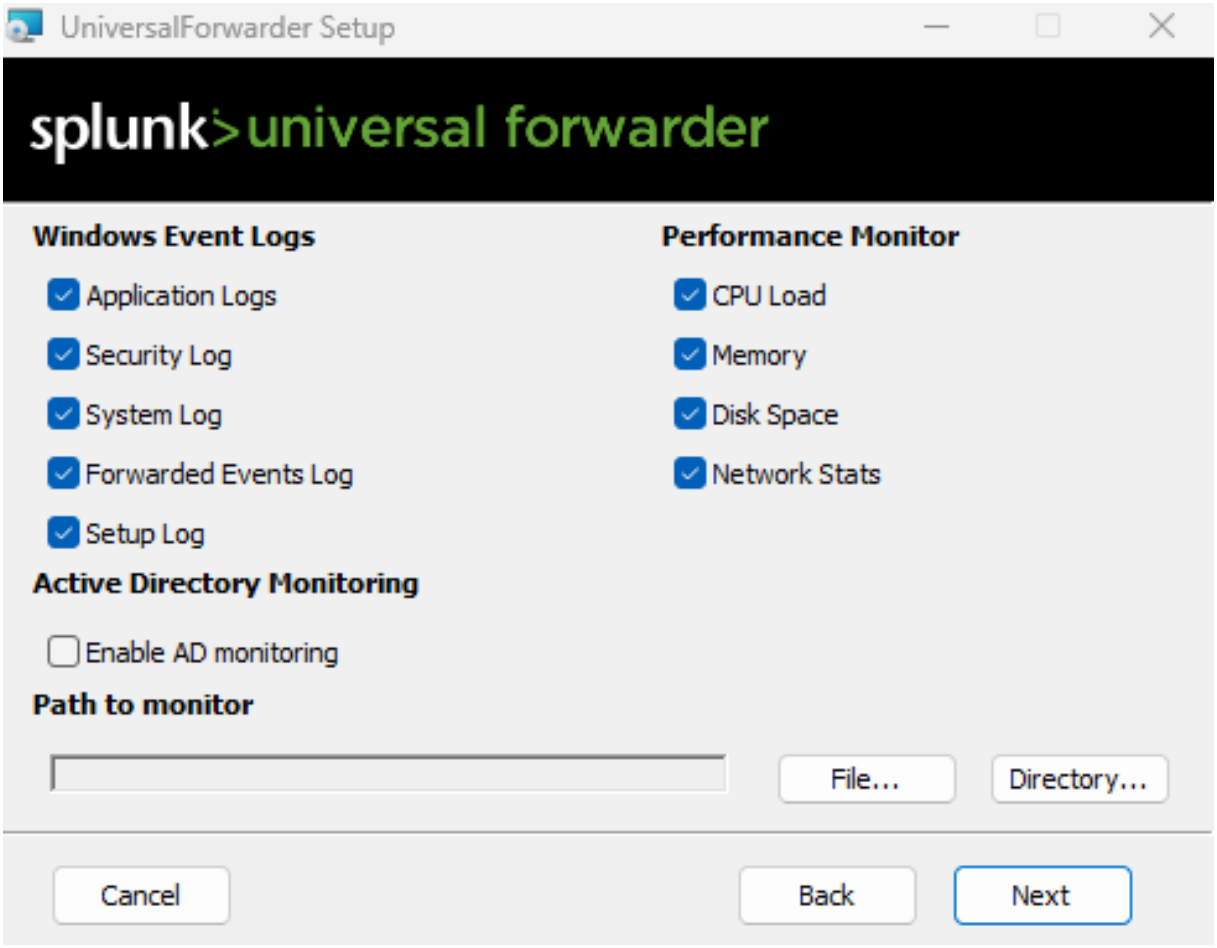

Figura 1.47: Ip deployment server

Ahora vamos a introducir un nombre de usuario y contraseña del administrador de la cuenta, aryan:aryan123.

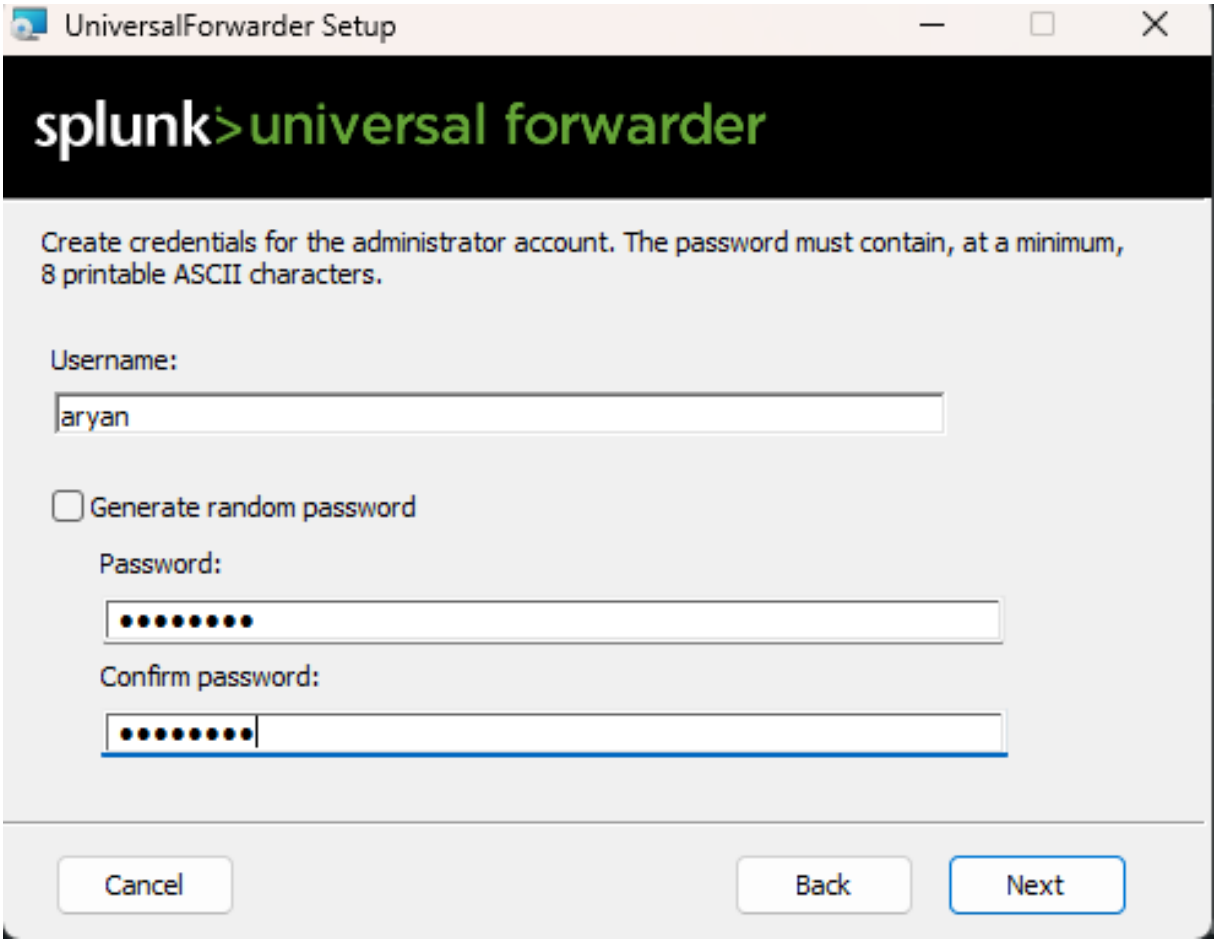

Figura 1.48: Credenciales

Ahora vamos a intorducir la ip de nuestro servidor con splunk enterprise para la configuración del deployment server, con puerto 8089 y del indexador con puerto 9997 (Esto lo configuramos anteriormente desde aqui 1.10).

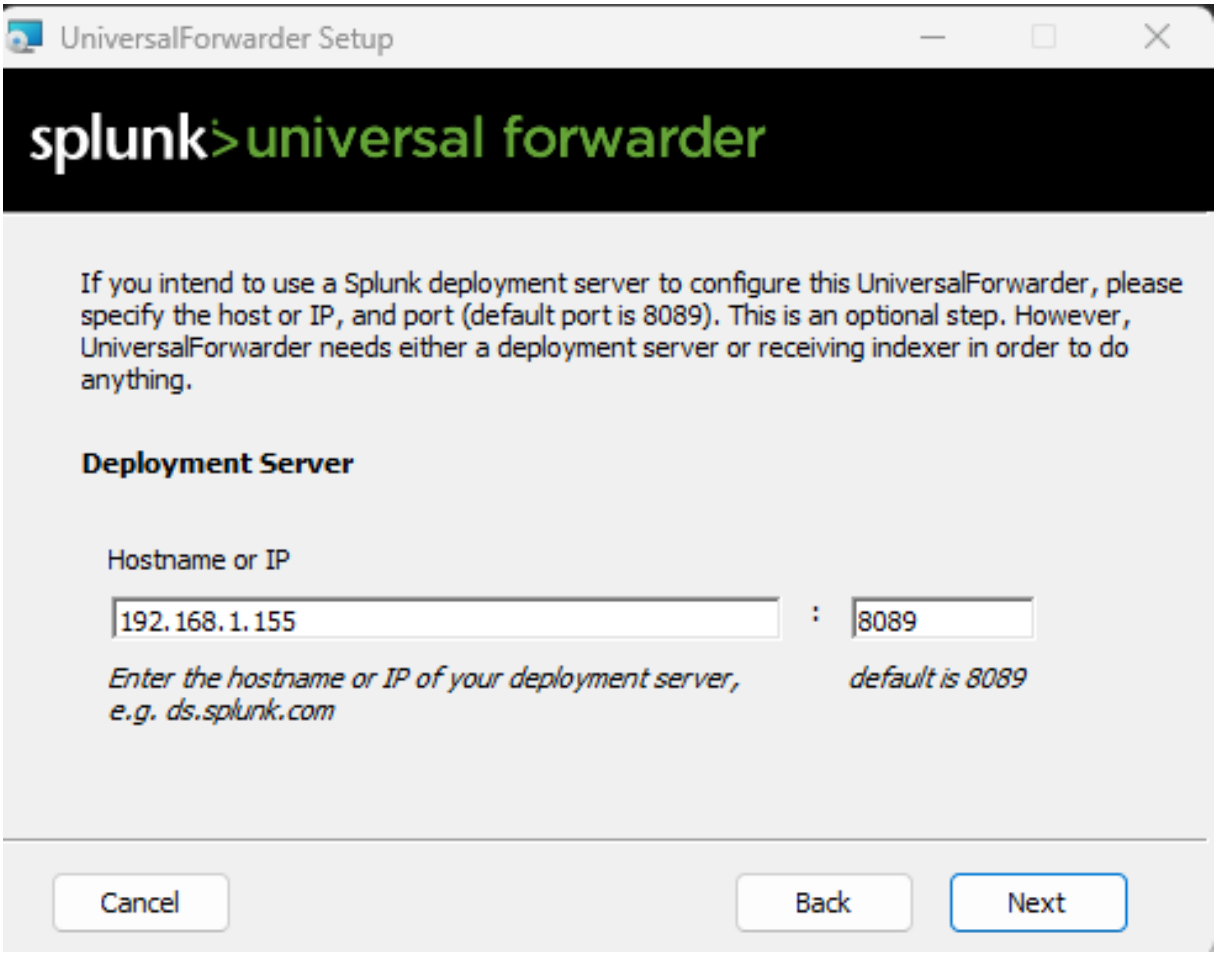

Figura 1.49: IP deployment server

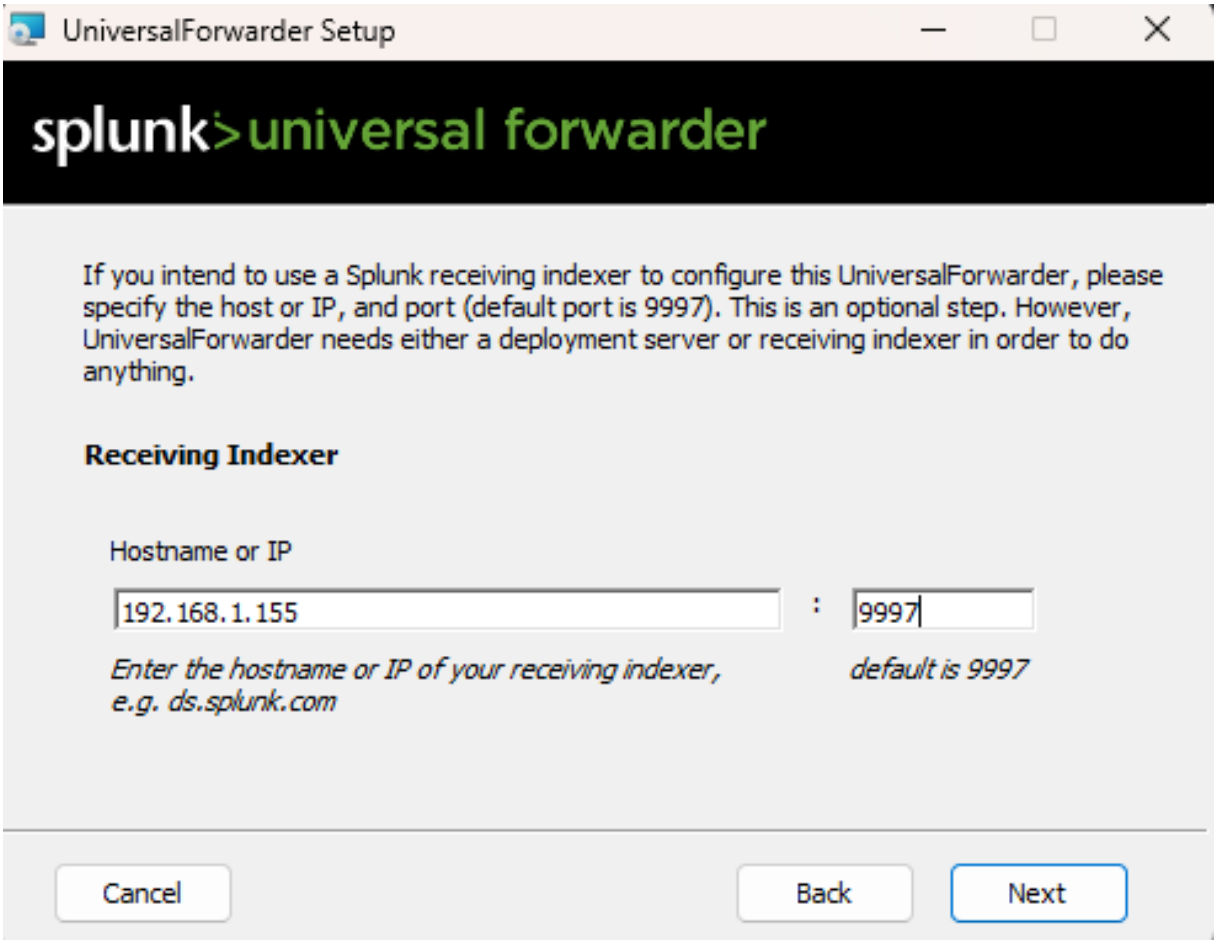

Figura 1.50: IP indexador

Y le damos a instalar dejamos que se instale y ya habriamos terminado con la instalación del agente para windows.

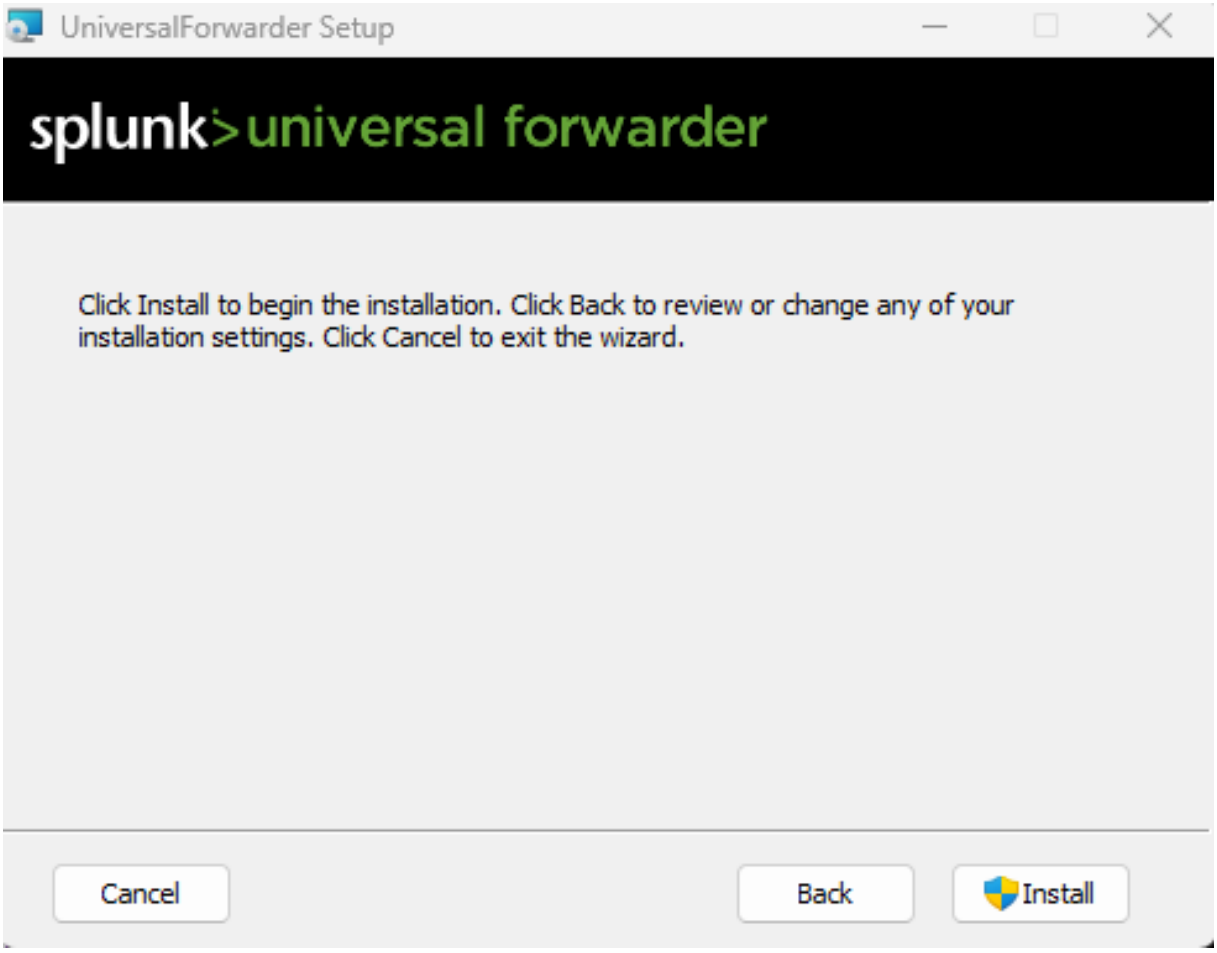

Figura 1.51: Instalar

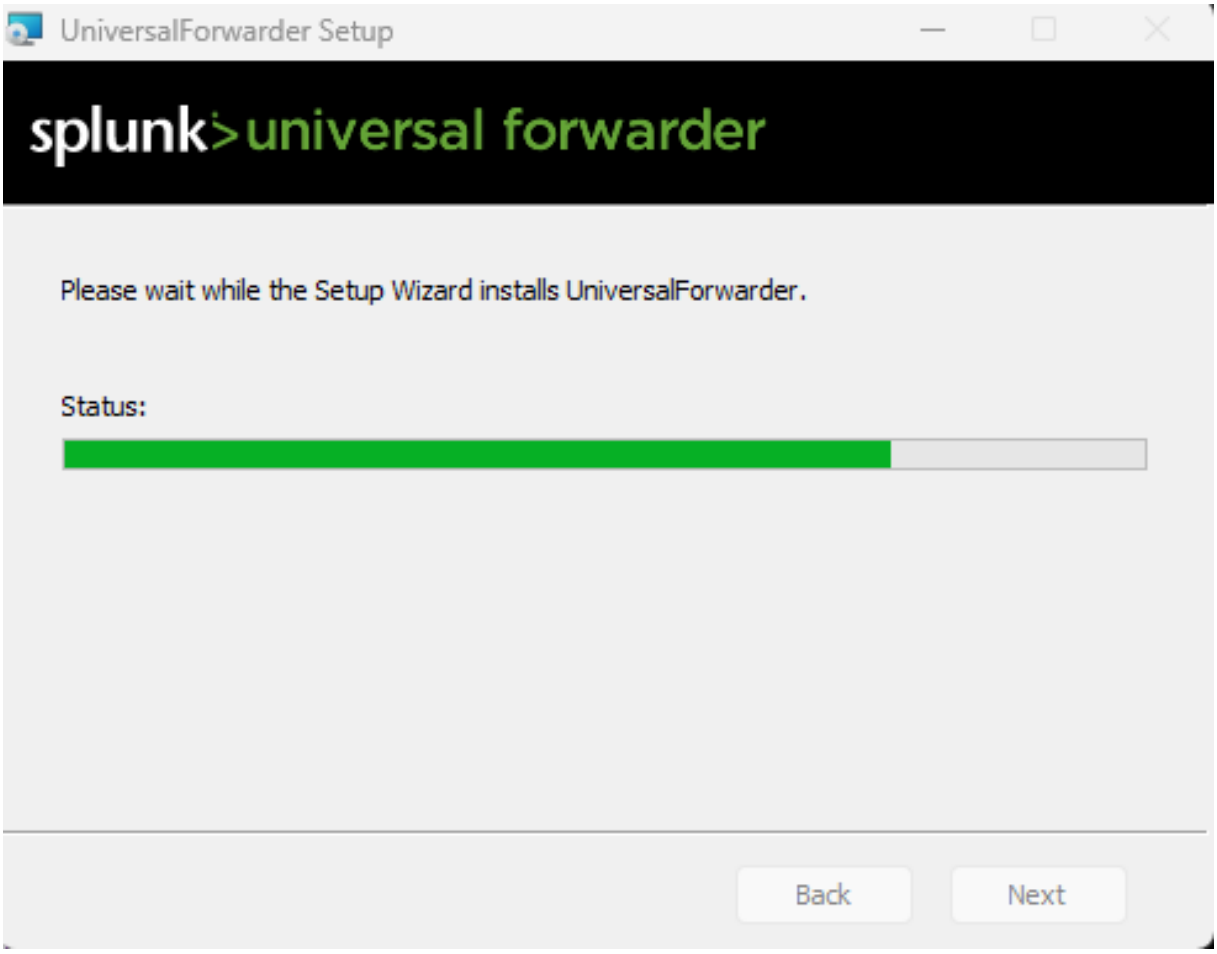

Figura 1.52: Status de la instalación

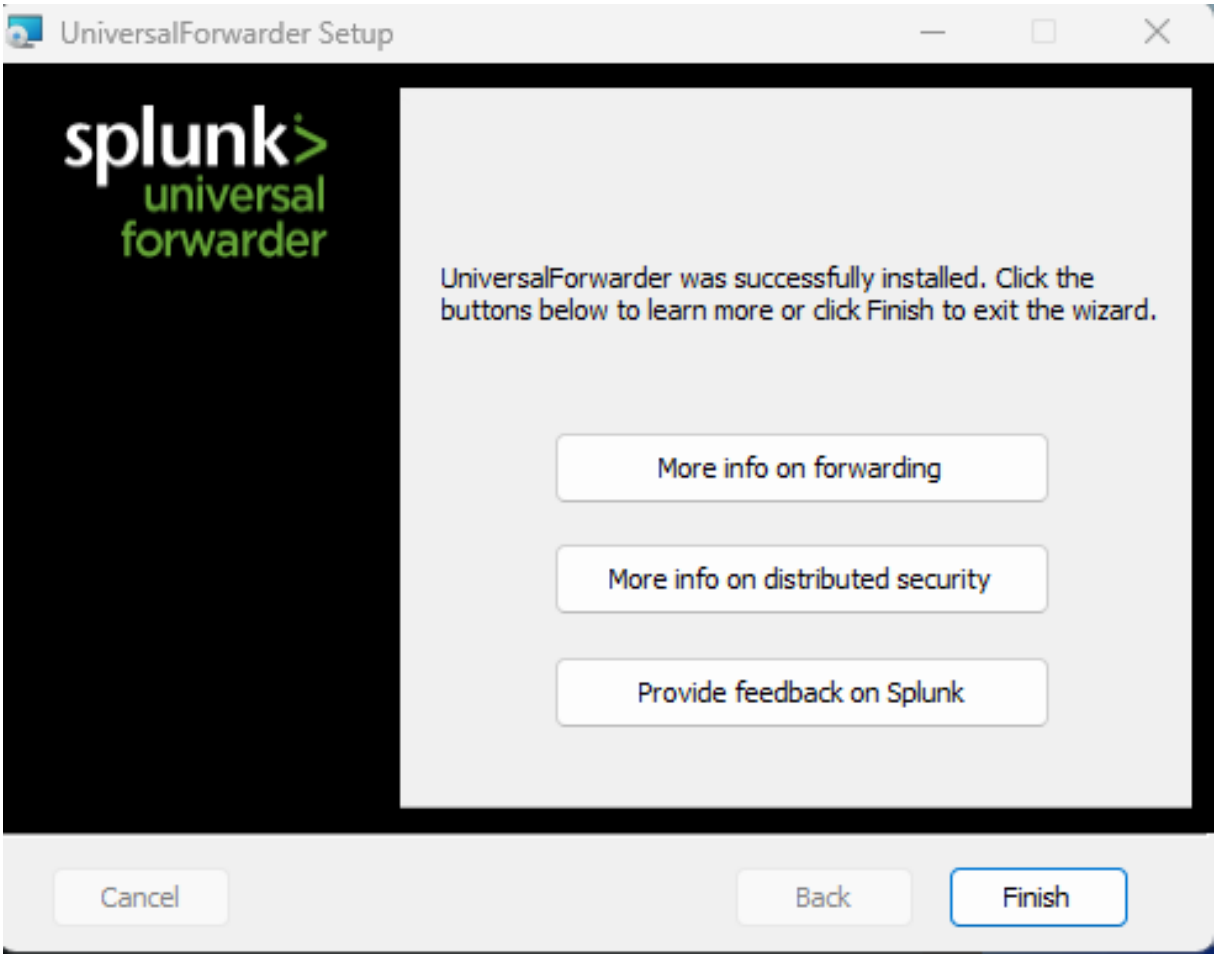

Figura 1.53: Fin de instalación de Universal forwarder

Y con esto ya hemos instalado el agente correctamente.

1.5.1. Gestión de datos de registro

Crearemos un indexador como hicimos anteriormente para los eventos de la máquina windows 1.15.

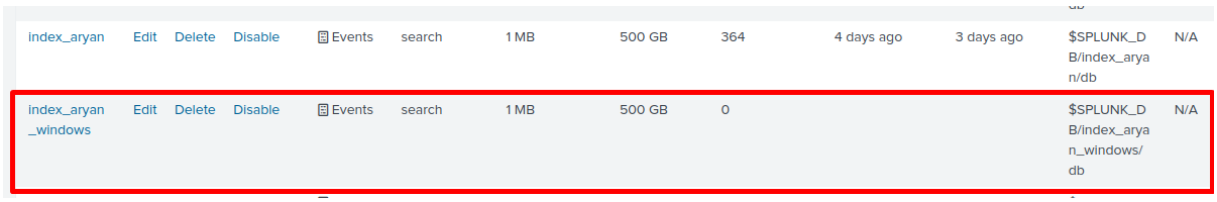

Figura 1.54: Indexador para windows

Para poder conectar nuestro datos al indexador vamos a seguir estos pasos.

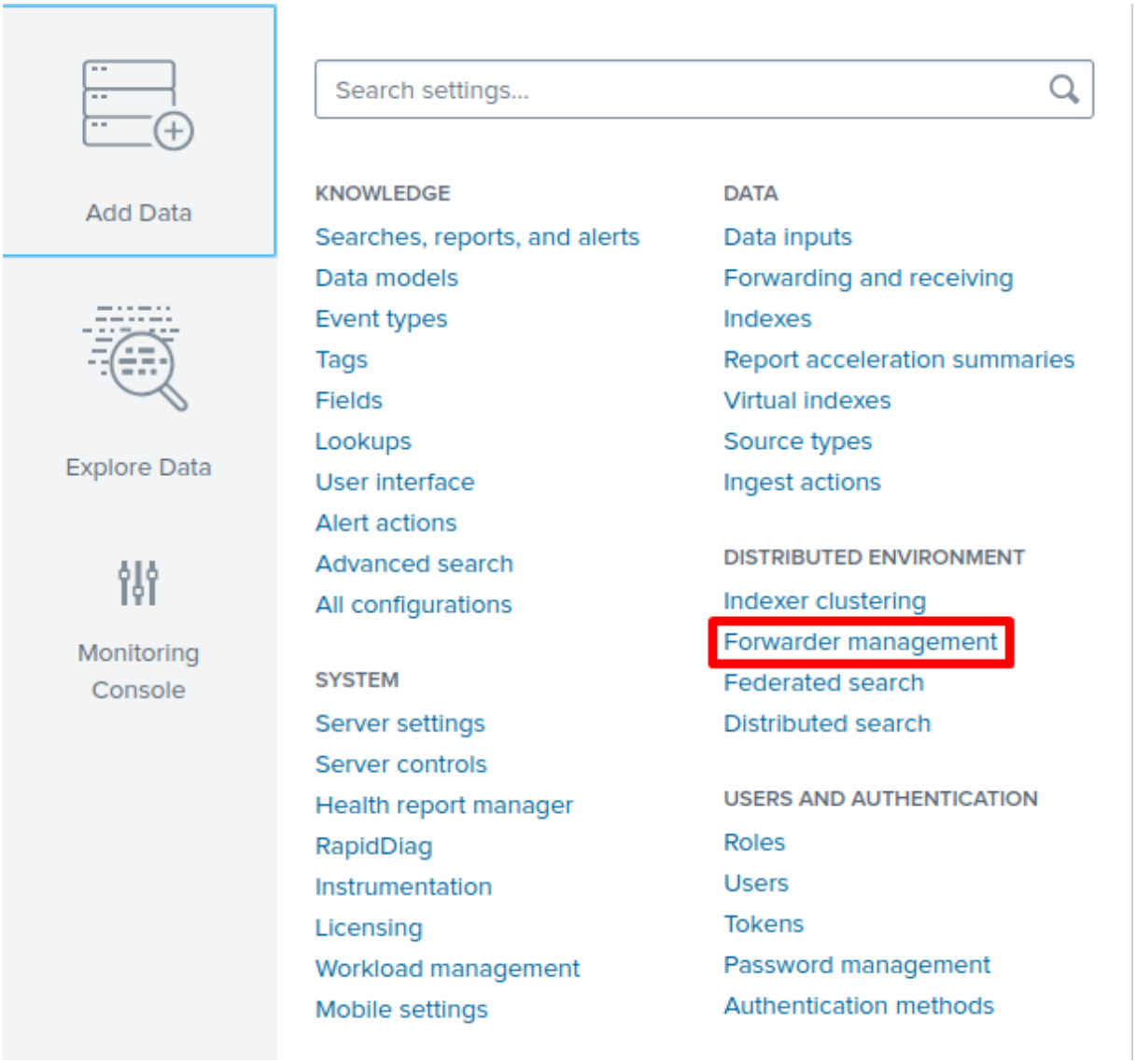

Figura 1.55: Forward Managment

En **Forward Managment** vamos a administrar el envio de datos a nuestro indexador de windows. Una vez dentro tenemos que ver a nuestro agente de la máquina windows, como cliente.

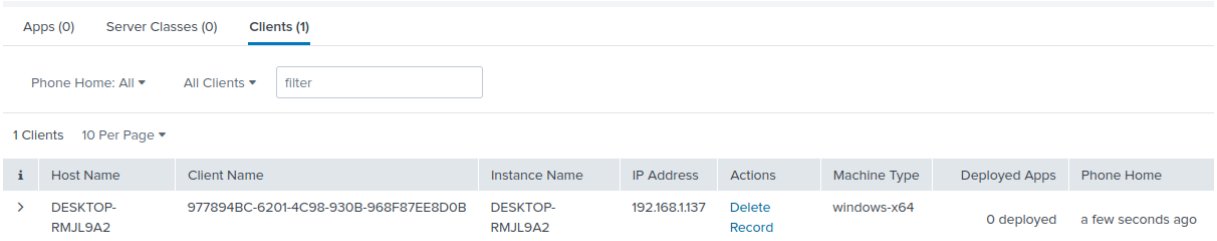

Figura 1.56: Clente Máquina windows

Le damos a **Server Class** que son una forma de agrupar y gestionar de manera eficiente los forwarders. Le damos a crear una nueva.

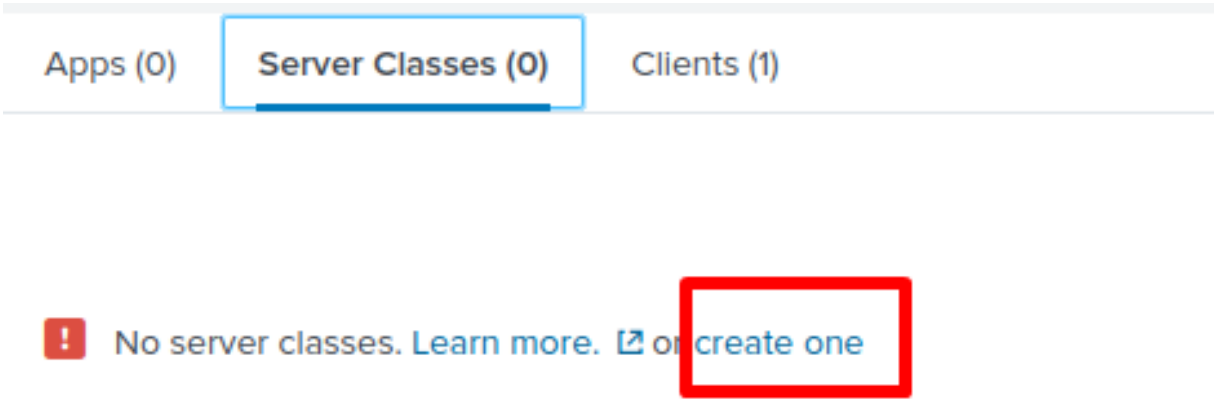

Figura 1.57: Crear server class

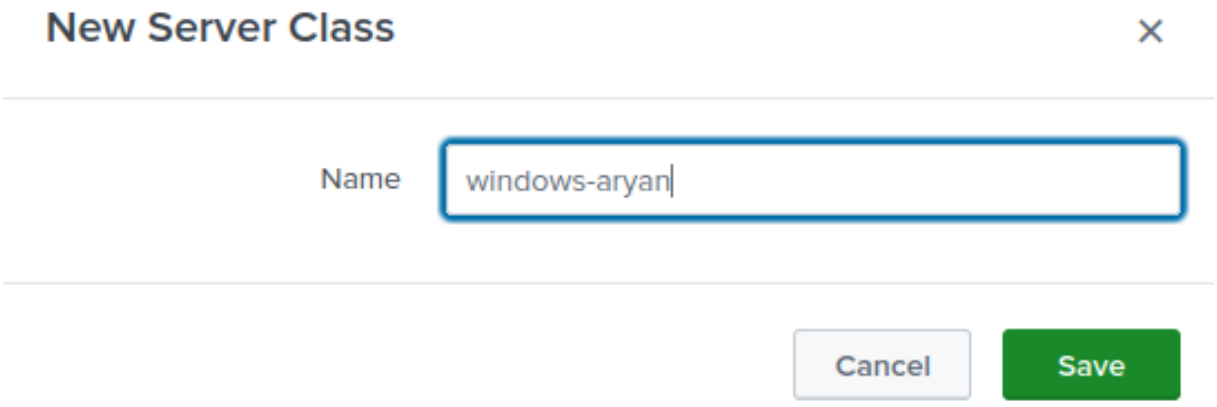

Figura 1.58: Server class windows

Como vemos en 1.58 lo nombramos windows-aryan. Una vez creado tenemos que añadir el cliente.

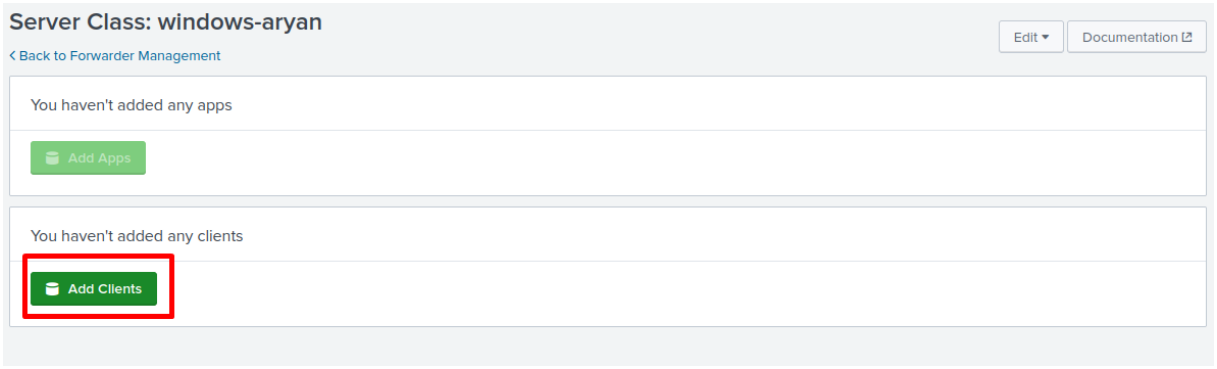

Figura 1.59: Añadir cliente

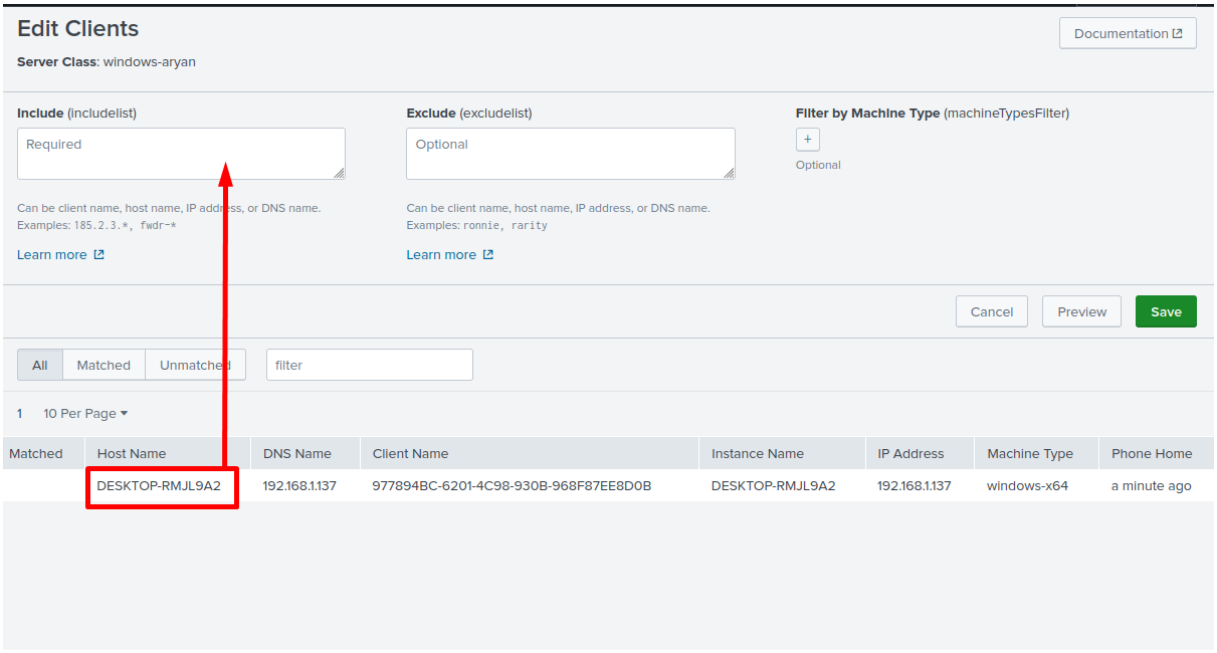

Figura 1.60: Añadir cliente

Y una vez agregado lo guardamos.

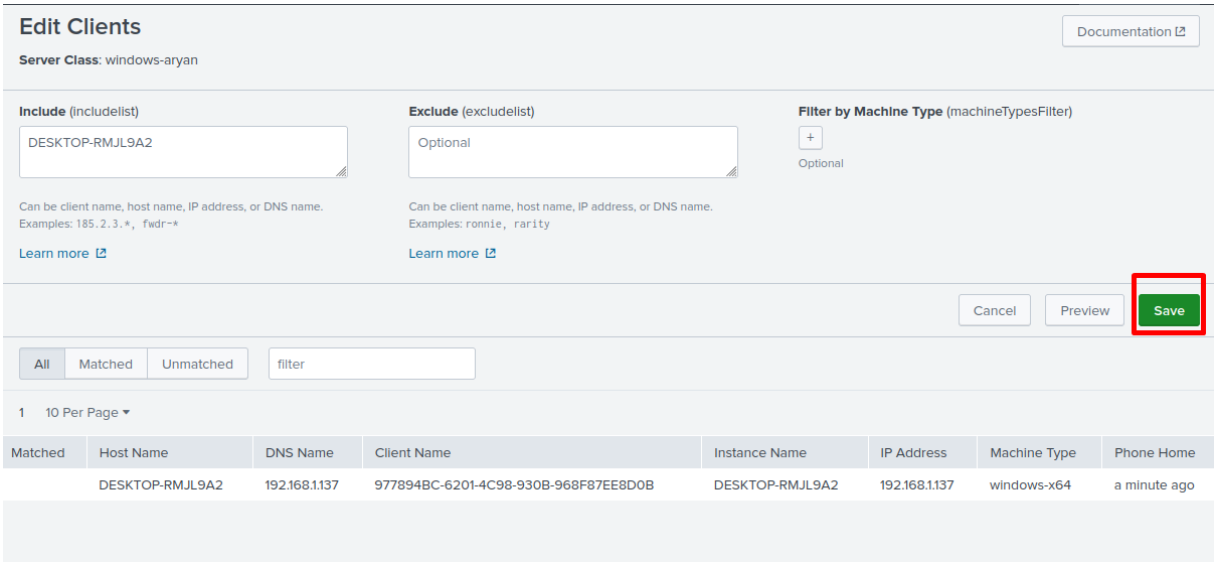

Figura 1.61: Guardar cliente en el server class

Y una vez guardado podemos ver nuestro cliente añadido.

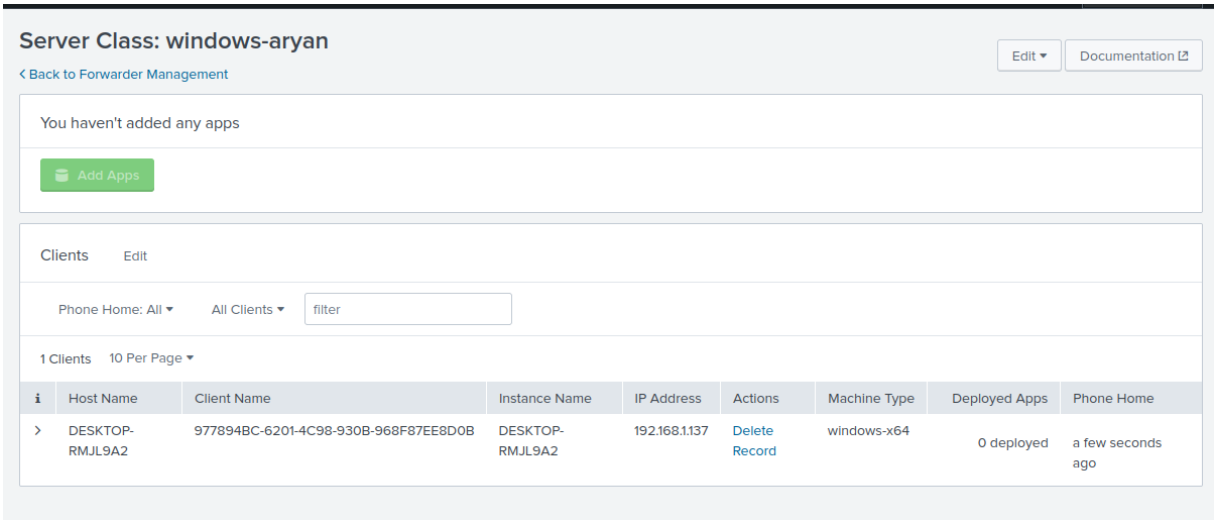

Figura 1.62: Cliente añadido

Habiendo creado el server class ahora vamos a enviar los datos al indexador. Para ello le damos a añadir datos.

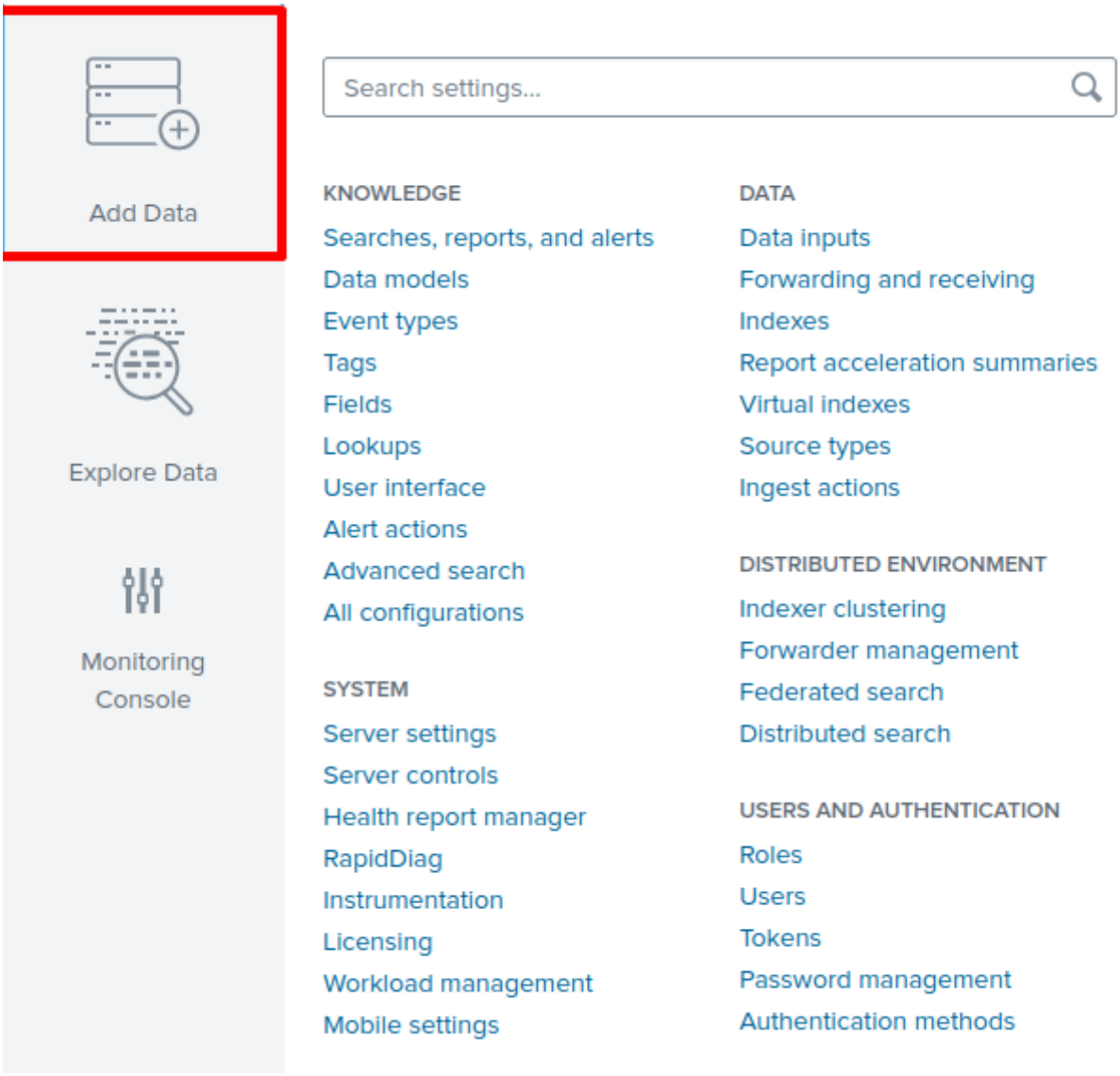

Figura 1.63: Añadir datos

Y seleccionamos el modo de envio de datos por forwarder, ya que usamos el Universal Forward.

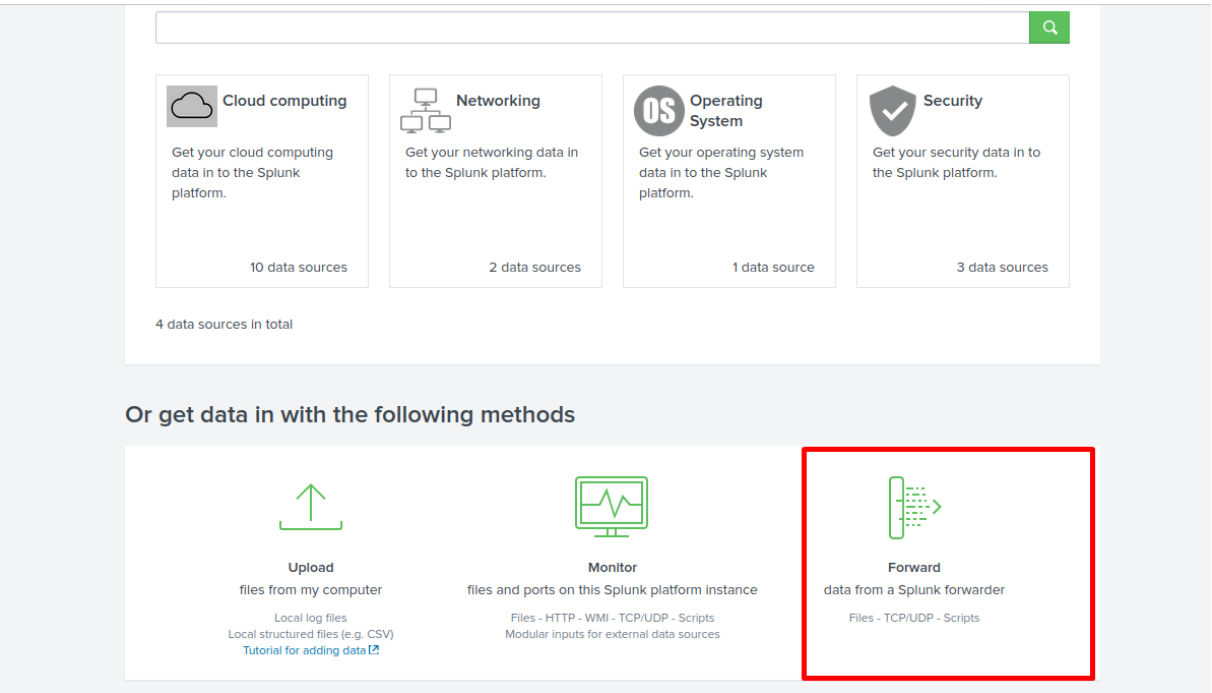

Figura 1.64: Forward

Una vez seleccionamos forward tenemos que seguir los pasos y elegir el forwarder, para ello elegimos un server class existente que es el que creamos anteriormente y darle a next.

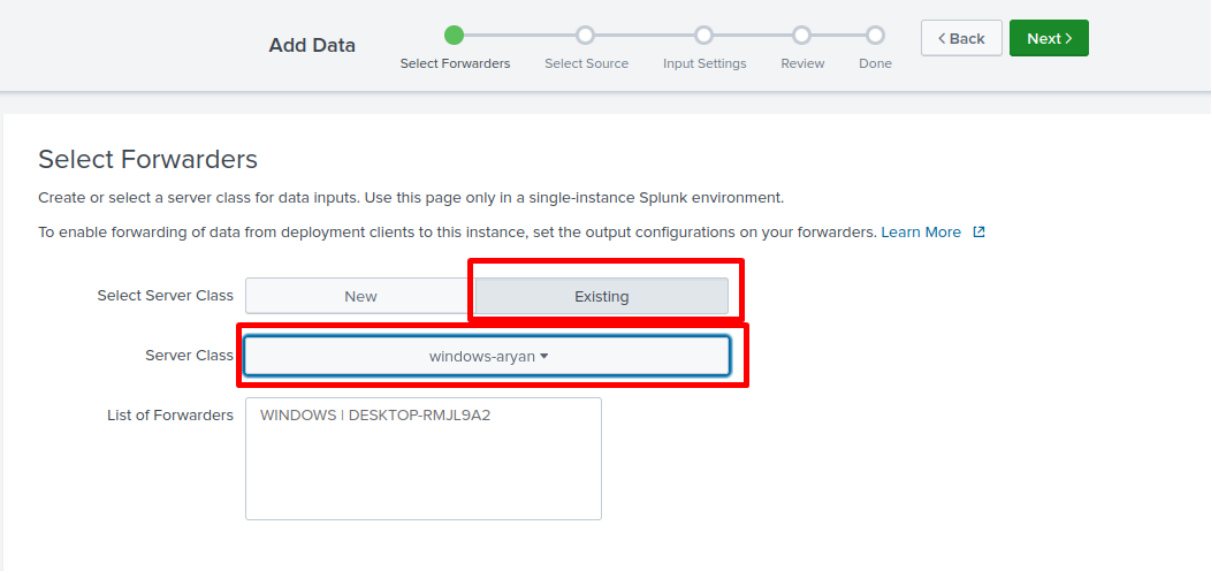

Figura 1.65: Seleccionar Forward

El siguiente paso es seleccionar los eventos que queremos enviar desde nuestro agente al indexador, seleccionamos Local Event logs ya que en la configuración elegimos este sistema y decidimos enviar estos eventos.

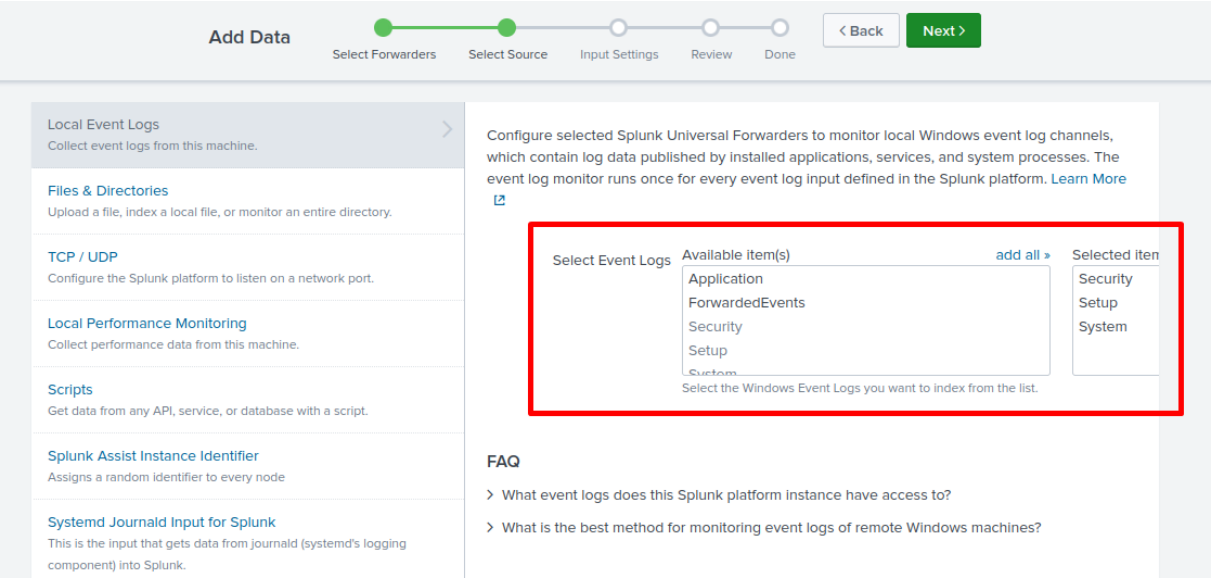

Figura 1.66: Elegir eventos para enviar

El tercer paso es elegir el indexador al que le vamos a enviar los eventos, elegimos el indexador que creamos para los eventos de windows.

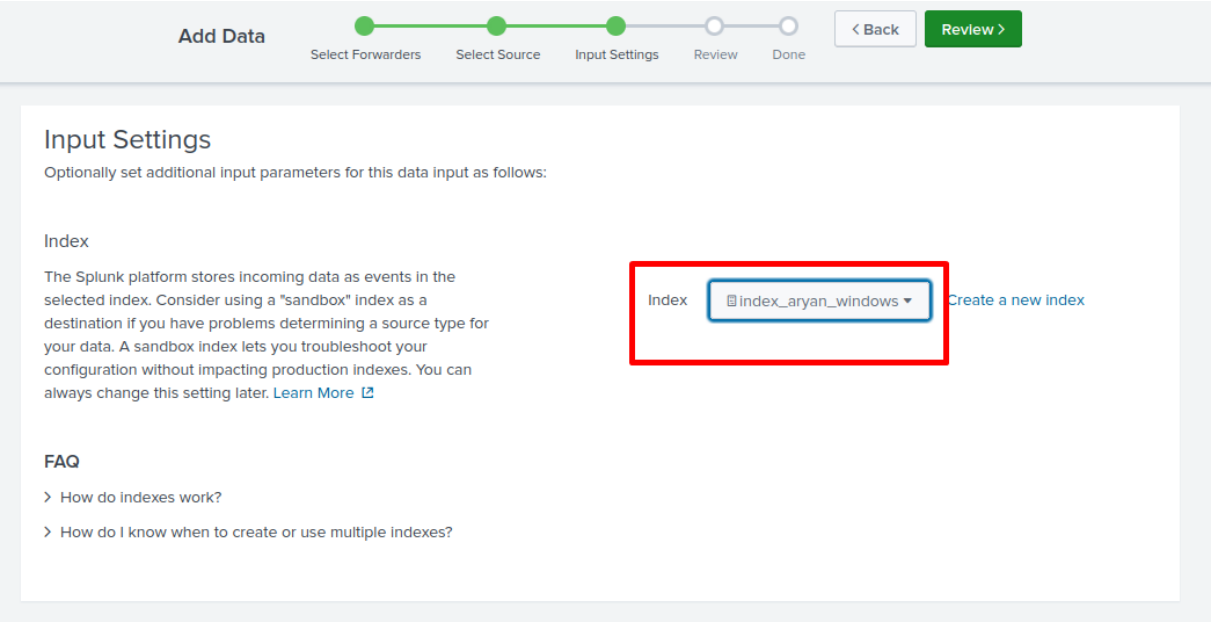

Figura 1.67: Elegir indexador para los eventos windows

Y los últimos pasos son revisar todos los pasos anteriores y la finalización de la configuración.

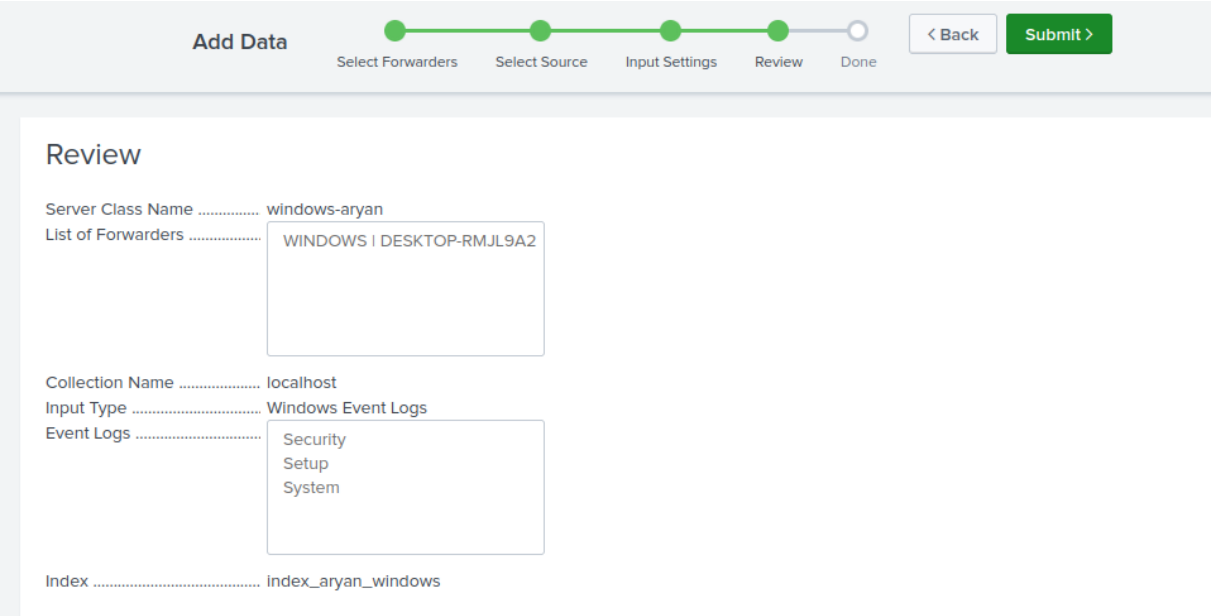

Figura 1.68: Review

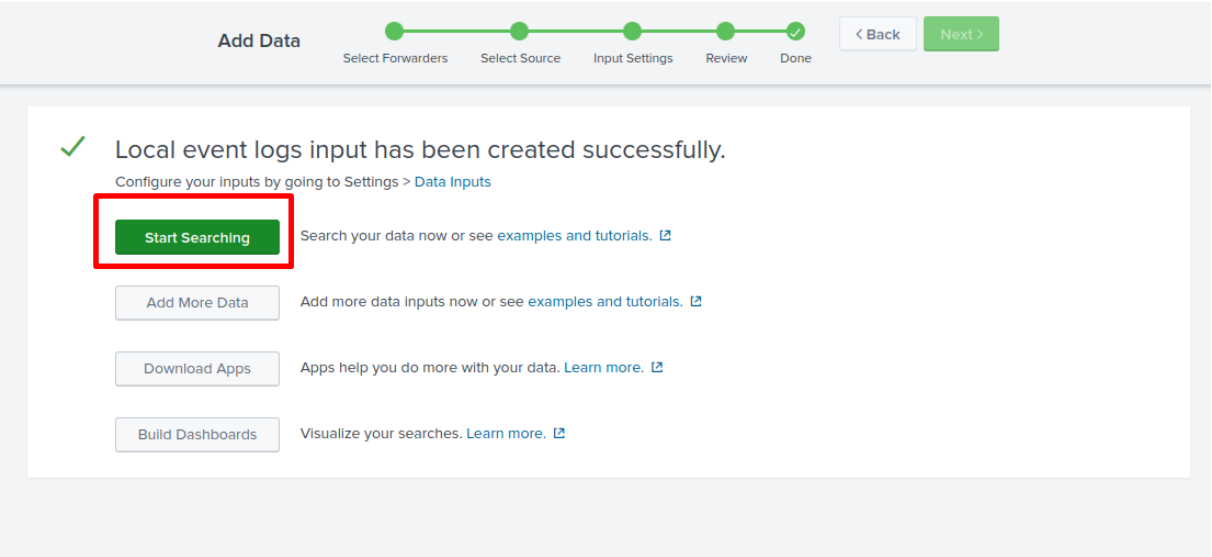

Figura 1.69: Buscar datos

Dando a buscar 1.69 nos lleva automaticamente al buscador y podremos ver los eventos que tiene el indexador, pero aun nuestro indexador esta vacío.

Esperando un rato y habiendo hecho todo lo explicado anteriormente, podemos ver como se han enviado datos al indexador.

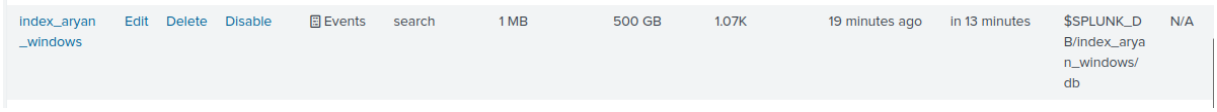

Figura 1.70: Datos ingestados en el Indexador windows

1.5.2. Análisis de eventos

Una vez añadido los datos al indexador, vamos a analizarlos. Para ello vamos a hacer lo mismo que hicimos en la imagen 1.28.

Una vez aqui ponemos en el buscador:

```
index=index_aryan_windows
```

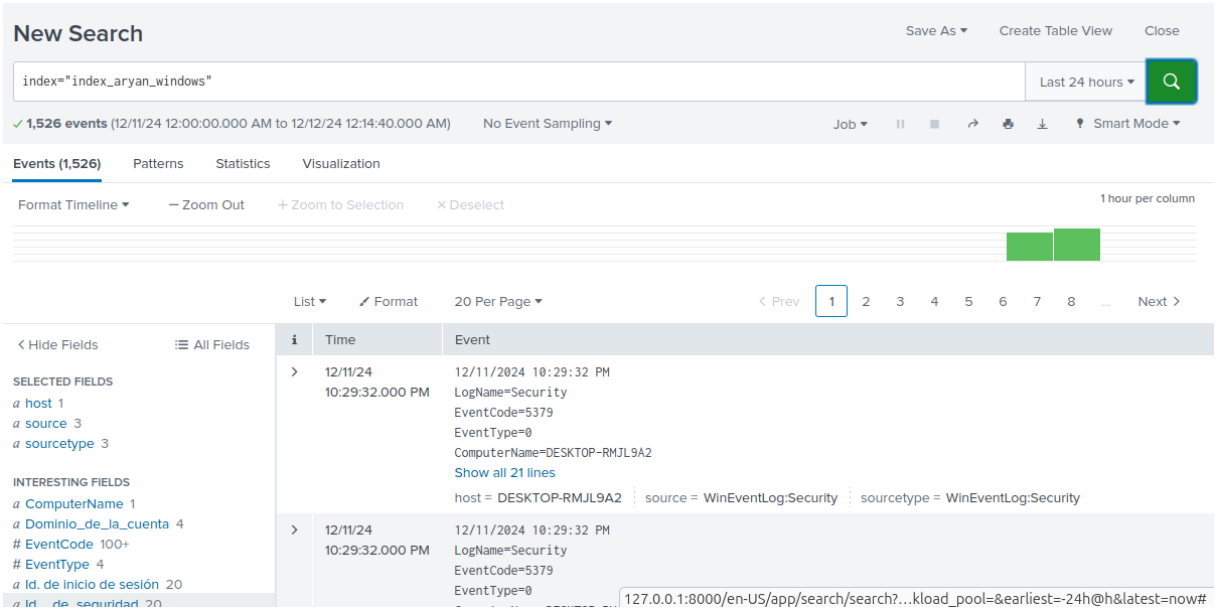

Figura 1.71: Eventos windows

Con esta busqueda podemos ver todos los eventos que hay en el indexador, los eventos de windows van identificados con un código de evento que podemos aplicar en el filtro para saber a qué equivalen.

El evento de fallo de sesión es el 4625 y el de login exitoso el 4624.

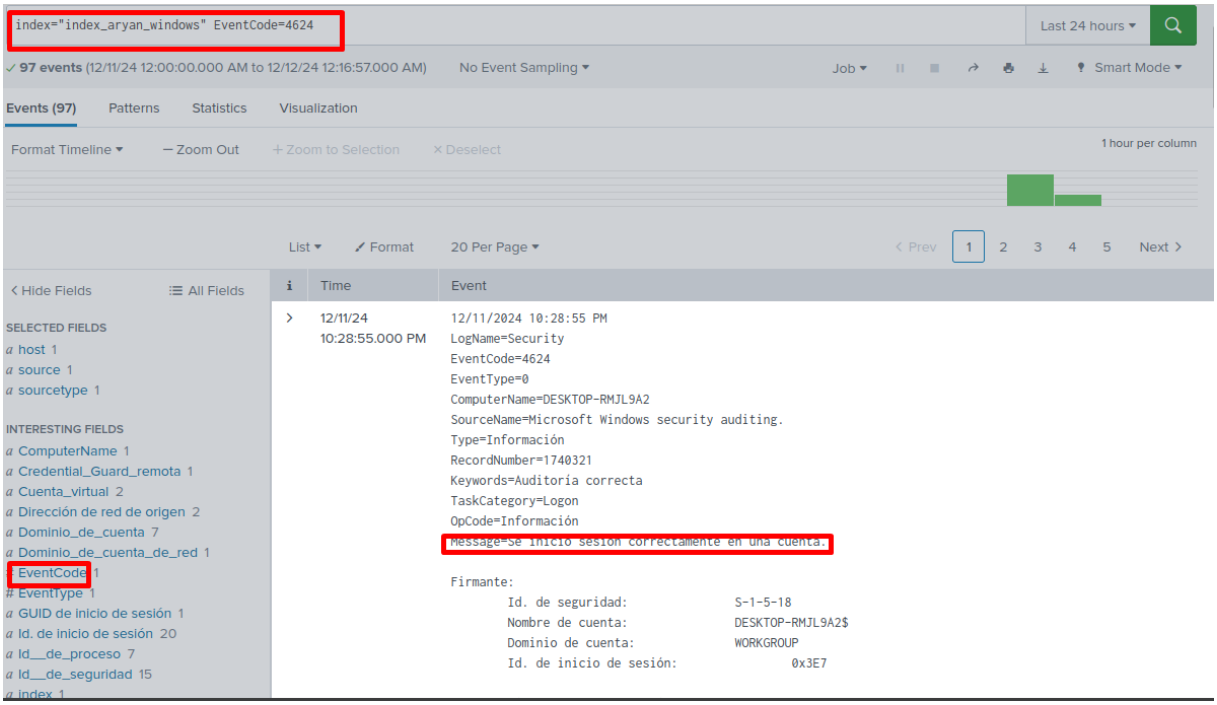

Figura 1.72: Eventos login exitoso

Gracias a este buscador podemos conseguir mucha información sobre el evento.

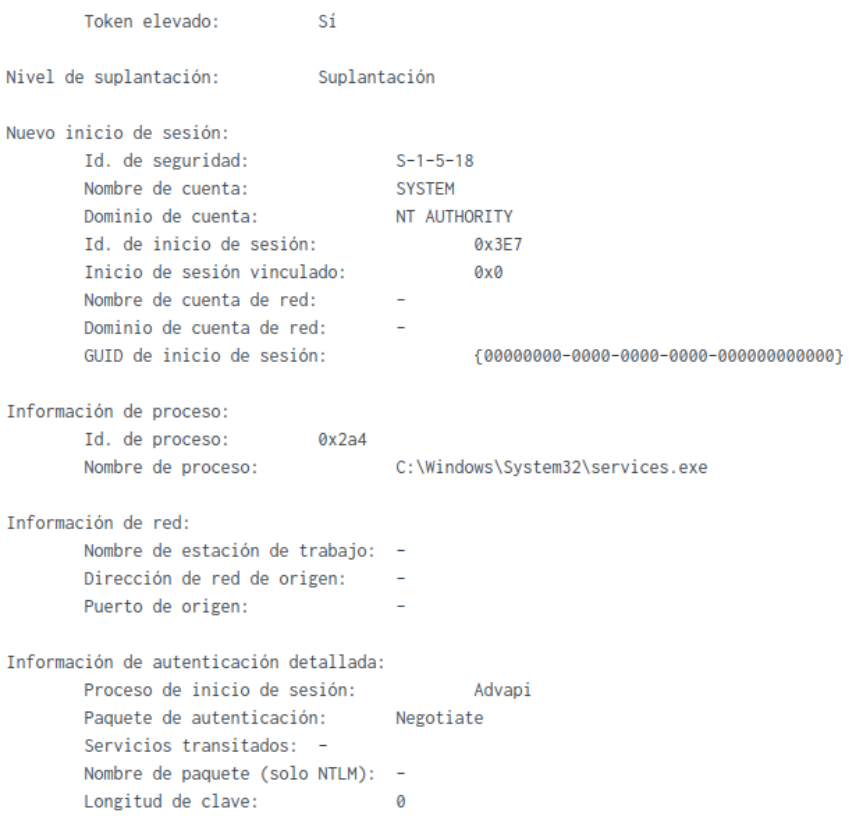

Figura 1.73: Información del evento

Y de esta forma se pueden analizar los eventos que hay en el indexador.

1.5.3. Creación de visualizaciones en Splunk

Ahora vamos a visualizar estos eventos en una gráfica para ello vamos a hacer lo mismo que hicimos anteriormente y vamos aprovechar el dashboard que creamos 1.37.

Para poder visualizar los eventos tenemos que crear una query de busqueda como hicimos anteriormente, para este aso vamos a hacer uso de los EventCode.

```
index="index_aryan_windows" (EventCode=4624 OR EventCode=4625)
| eval Login_status=if(EventCode=4624, "Login Exitoso", "Login Fallido")
| stats count by Login_status
```

Con esta query de busqueda lo que hacemos es filtrar los dos codigos de eventos y si es 4624 lo nombramos como exitoso y si no como fallido y los contamos.

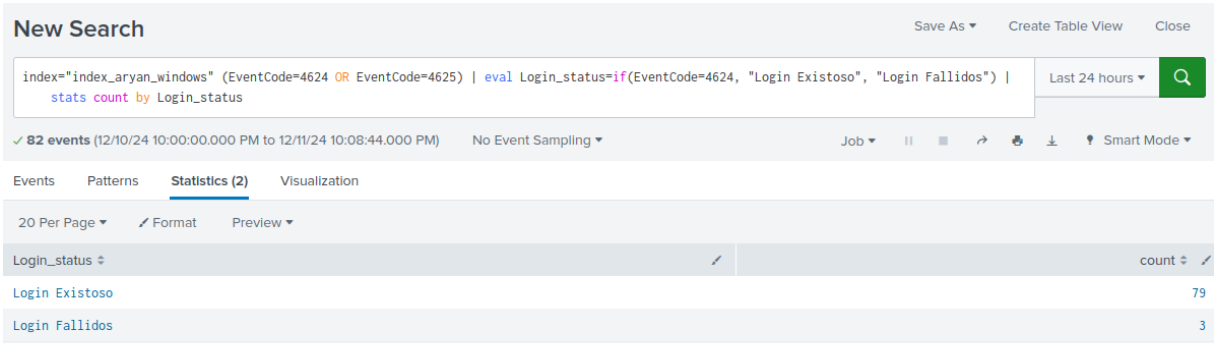

Figura 1.74: Busqueda de los eventos

Y una vez realizada la busqueda hacemos como anteriormente le damos a visualizar y veremos una gráica de columnas.

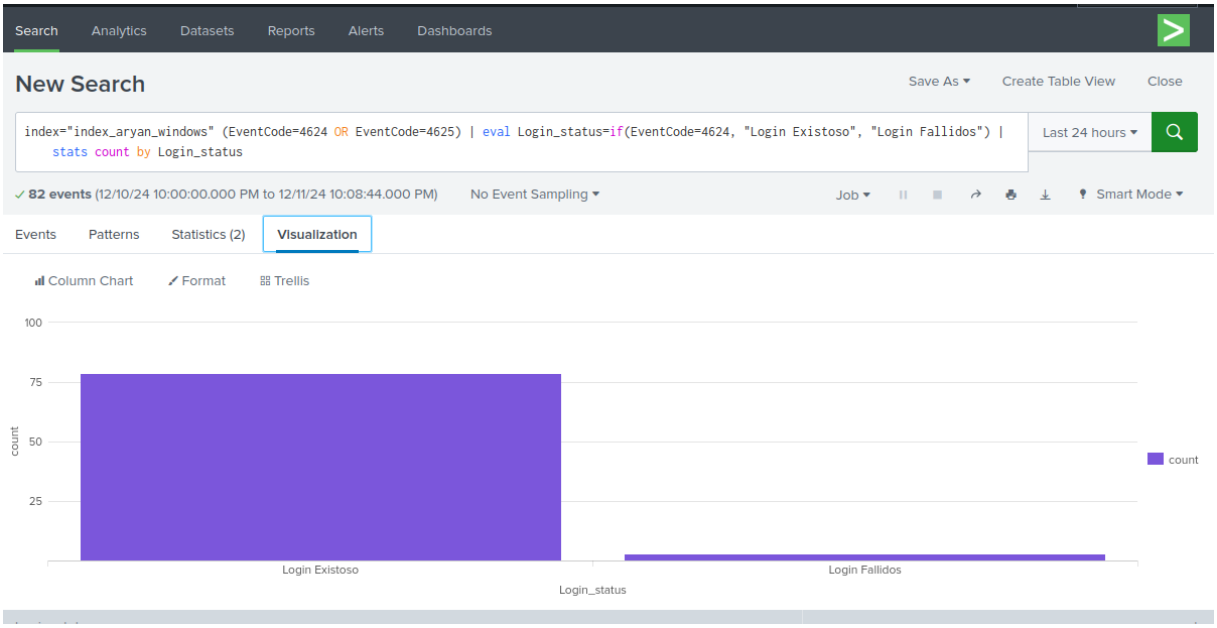

Figura 1.75: Eventos en grafica columnas

Le damos a guardar y lo enviamos a un dashboard existente y lo añadimos, como hicimos 1.33.

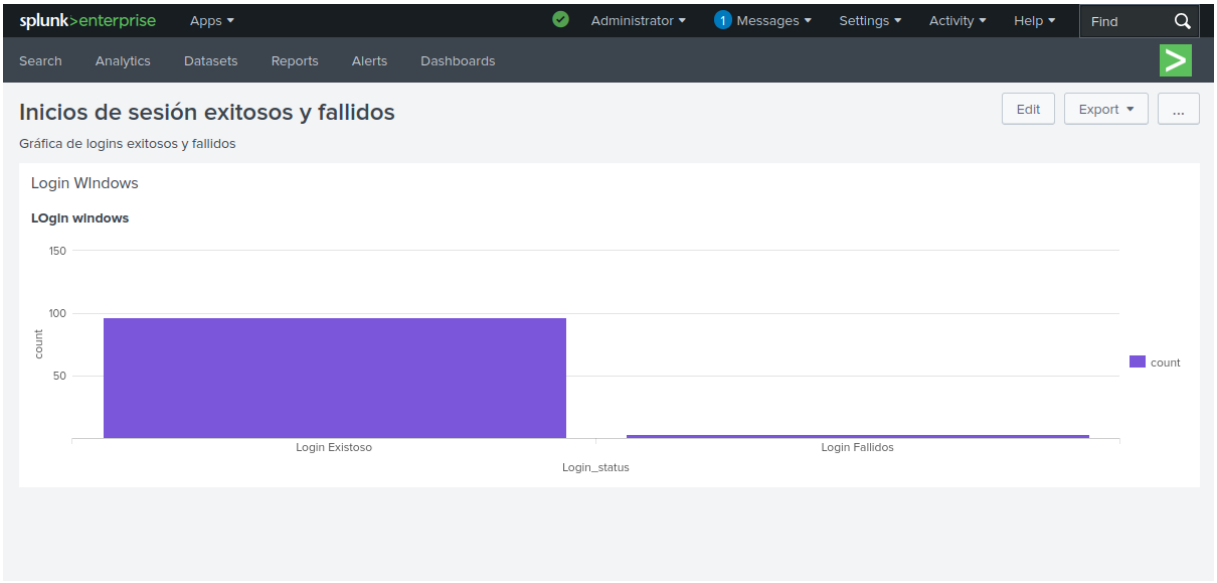

Figura 1.76: Eventos en grafica columnas windows en el dashboard

Ahora lo que vamos a hacer es unir ambas gráficas que hemos creado en el mismo dashboard y asi poder ver los eventos de los dos sistemas operativo.

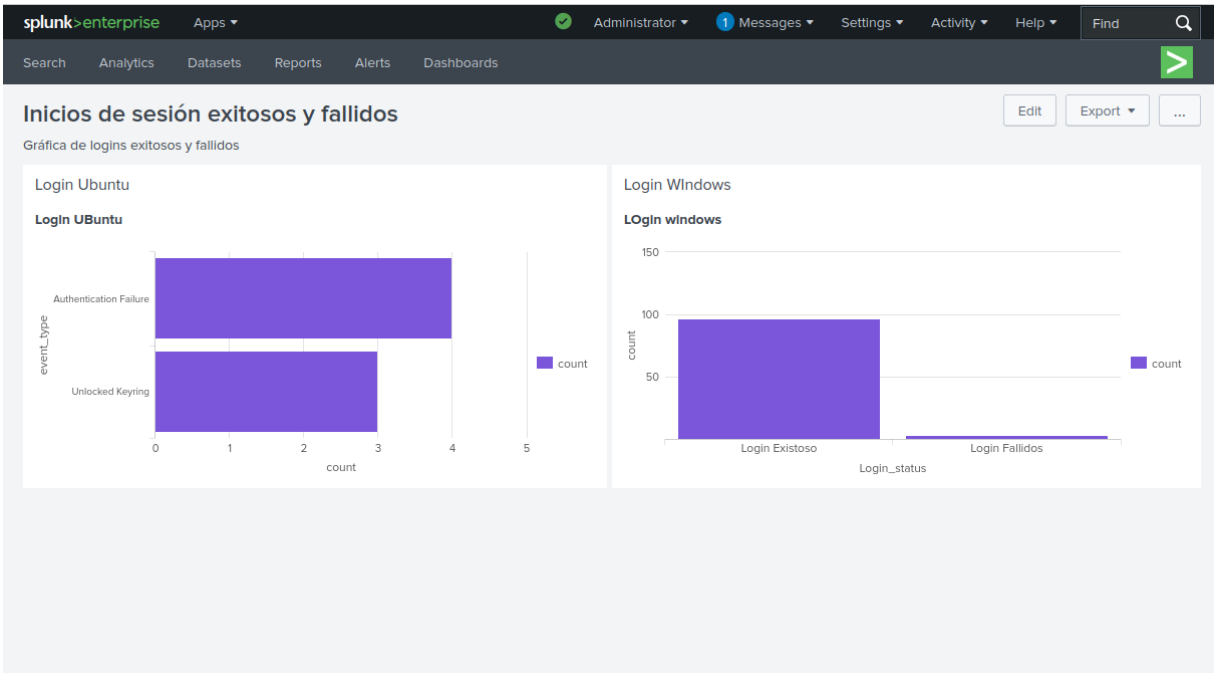

Figura 1.77: Eventos de los dos SO en el dashboard

Hemos realizado las mismas instrucciones que en los pasos anteriores, para la creación de las gráficas y hemos añadido al mismo dashboard ambas gráficas y asi poder ver ambos Sistema operativos ubuntu y windows.

Con esto hemos terminado con Splunk, es una poderosa herramienta, además que se podría unificar junto con un IDS o IPS y así tener más eventos para mostrar.

Capítulo 2

Elasticsearch

El objetivo de esta segunda parte de la práctica, es similar a la primera parte con splunk pero teniendo los logs en Elasticsearch y visualizar los logs con Kibana.

Elastic Stack es una colección de Software de Código Abierto producido por Elastic, que permite buscar, analizar y visualizar registros generados desde cualquier fuente y en cualquier formato.

A nivel de sistemas, podemos utilizarlo para analizar los registros de todos nuestros servidores y ver donde hay problemas. Elastic Stack cuenta con cuatro componentes principales:

- **ElasticSearch**: Es un motor de búsqueda distribuido que almacena todos los datos recopilados.
- **Logstash**: Es un componente de procesamiento de datos de Elastic Stack que envia datos entrantes a ElasticSearch.
- **Kibana**: Es una interfaz web par buscar y visualizar los registros.
- **Beats**: Es un transportador de datos ligeros de uso único que pueden enviar datos a cientos o miles de maquinas de ElasticSearch.

2.1. Instalación y configuración de Elasticsearch

Después de actualizar nuestra máquina virtual con los siguientes comandos.

```
sudo apt update
sudo apt upgrade -y
```

Ya podemos empezar con la descarga e instalación de **Elasticsearch**.

Lo primero que vamos a hacer es instalar dependencias, para ellos vamos a instalar estos paquetes que hacen referencia a la última versión disponible de Java en los repositorios..

```
sudo apt install default-jre default-jdk
```

```
aryan@ELK-aryan:~$ sudo apt install default-jre default-jdk
[sudo] contraseña para aryan:
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes adicionales:
  ca-certificates-java default-jdk-headless default-jre-headless
  fonts-dejavu-extra java-common libatk-wrapper-java libatk-wrapper-java-jni
  libice-dev libpthread-stubs0-dev libsm-dev libx11-dev libxau-dev libxcb1-dev
  libxdmcp-dev libxt-dev openjdk-21-jdk openjdk-21-jdk-headless openjdk-21-jre
  openjdk-21-jre-headless x11proto-dev xorg-sgml-doctools xtrans-dev
Paquetes sugeridos:
  libice-doc libsm-doc libx11-doc libxcb-doc libxt-doc openjdk-21-demo
  openjdk-21-source visualvm fonts-ipafont-gothic fonts-ipafont-mincho
  fonts-wqy-microhei | fonts-wqy-zenhei fonts-indic
Se instalarán los siguientes paquetes NUEVOS:
  ca-certificates-java default-jdk default-jdk-headless default-jre
  default-jre-headless fonts-dejavu-extra java-common libatk-wrapper-java
  libatk-wrapper-java-jni libice-dev libpthread-stubs0-dev libsm-dev
  libx11-dev libxau-dev libxcb1-dev libxdmcp-dev libxt-dev openjdk-21-jdk
  openjdk-21-jdk-headless openjdk-21-jre openjdk-21-jre-headless x11proto-dev
  xorg-sgml-doctools xtrans-dev
0 actualizados, 24 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 137 MB de archivos.
Se utilizarán 317 MB de espacio de disco adicional después de esta operación.
¿Desea continuar? [S/n] S
```

Figura 2.1: Instalar Java

Y una vez instalado comprobamos la versión.

```
aryan@ELK-aryan:~$ java --version
openjdk 21.0.5 2024-10-15
OpenJDK Runtime Environment (build 21.0.5+11-Ubuntu-1ubuntu124.04)
OpenJDK 64-Bit Server VM (build 21.0.5+11-Ubuntu-1ubuntu124.04, mixed mode, sharing)
```

Figura 2.2: Java Versión

Ahora nos dirigimos a la página de descarga de elasticsearch y accederemos al link de la imagen, ya que los componentes de ElasticSearch no se encuentran en los repositorios de Ubuntu, pero se pueden instalar por APT añadiendo los repositorios.

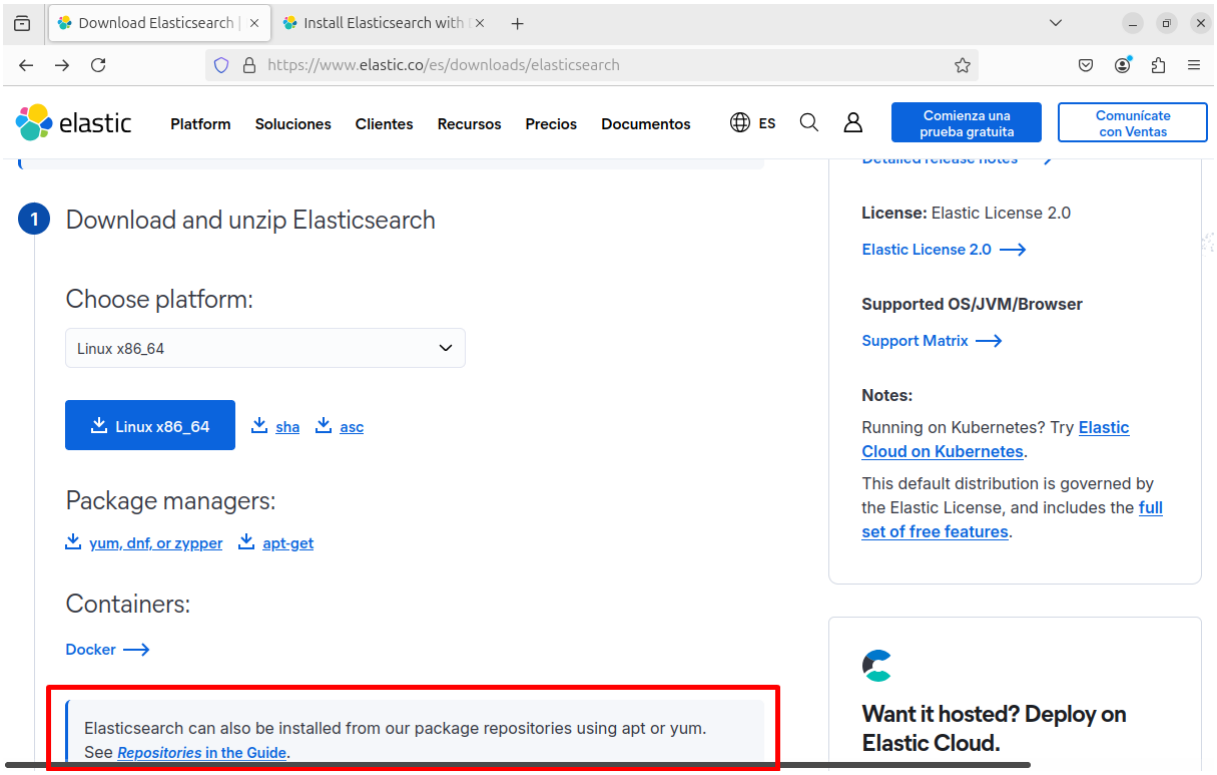

Figura 2.3: Pagina oficial ElasticSearch

Y seguiremos los pasos de la documentación oficial de Elasticsearch.

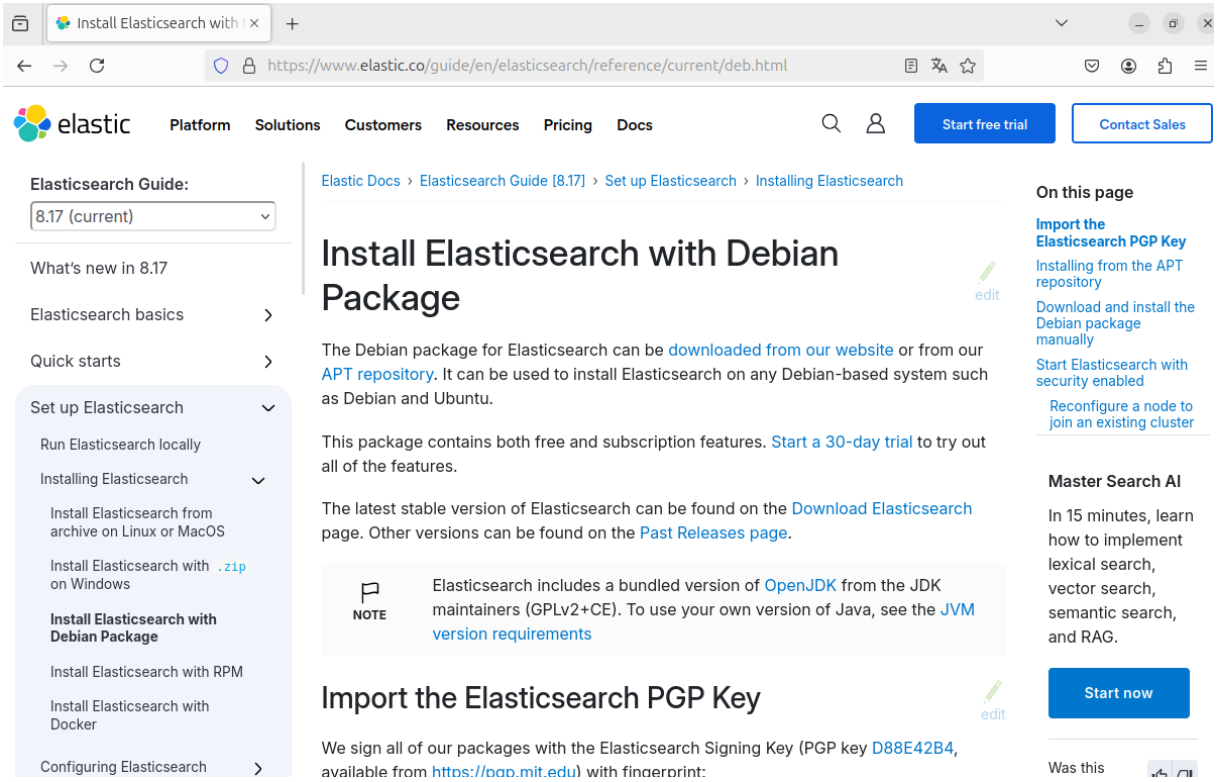

Figura 2.4: Guía oficial ElasticSearch

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch
| sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
```

Es posible que necesitemos instalar el apt-transport-httpspaquete en Debian.

```
sudo apt-get install apt-transport-https
```

Y una vez instalado guardamos la definición del repositorio en **/etc/apt/sources.list.d/elastic-8.x.list**

```
echo "deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg]
https://artifacts.elastic.co/packages/8.x/apt stable main"
| sudo tee /etc/apt/sources.list.d/elastic-8.x.list
```

Figura 2.5: Instalación desde el repositorio APT

Una vez finalizado actualizaremos el sistema y procederemos a instalar elasticsearch.

```
sudo apt update && sudo apt upgrade -y
```

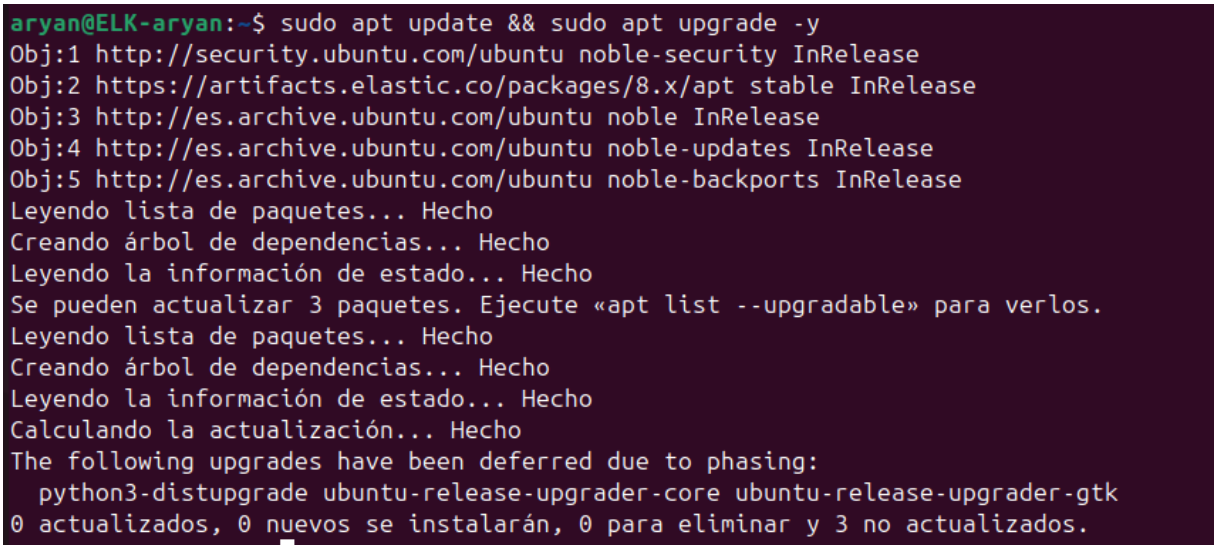

Figura 2.6: Actualización de repositorios

Y ahora podremos instalar elasicsearch mediante apt install.

```
sudo apt install elasticsearch
```

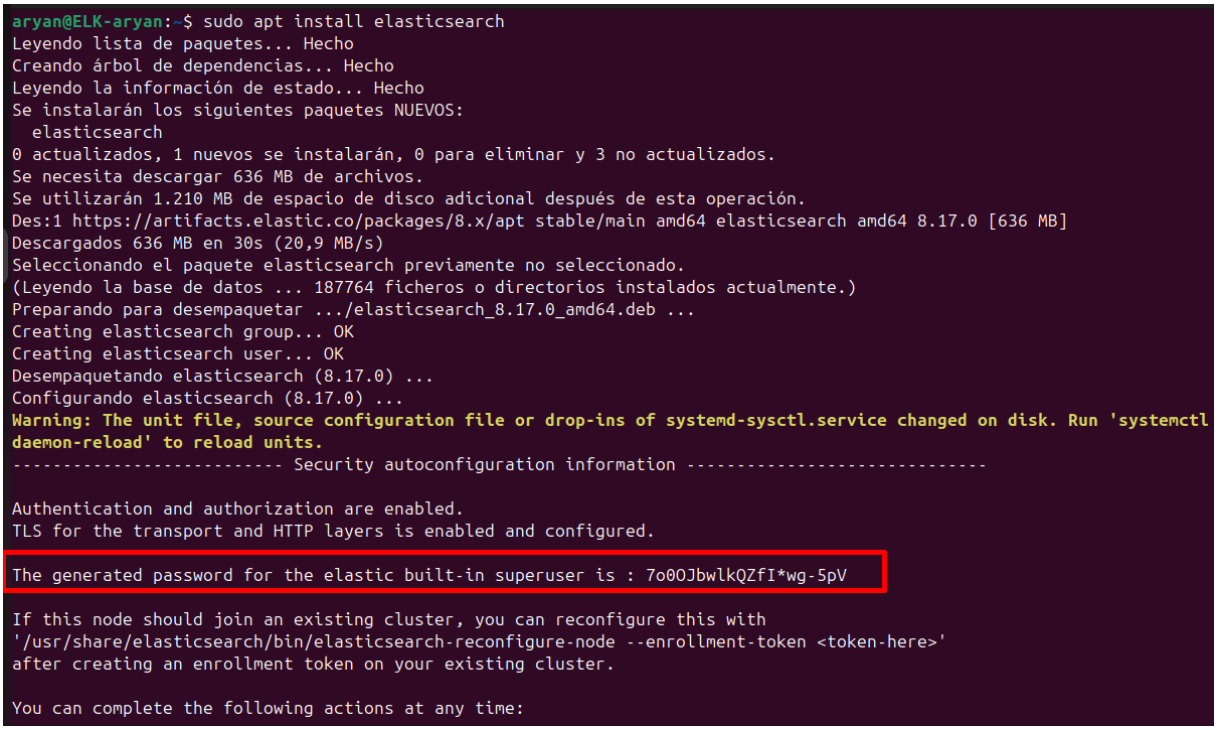

Figura 2.7: Instalación de elasticsearch

Una vez se complete la instalación vamos a comenzar con la configuración inicial de elasticsearch.

2.2. Configuración inicial de Elasticsearch

Para una primera configuración de ElasticSearch vamos a editar el archivo de configuración **/etc/elasticsearch/elasticsearch.yml**

Concedemos permisos para poder acceder a la carpeta de configuración.

```
sudo chmod 755 elasticsearch/
```

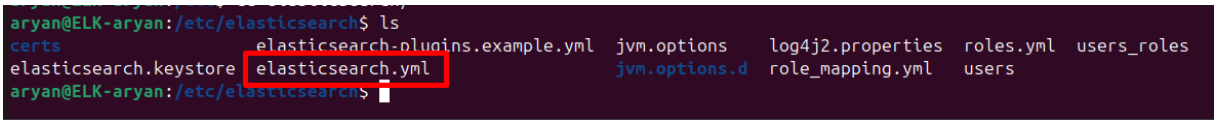

Figura 2.8: Archivos de elasticsearch

Editaremos el archivo de configuración **elasticsearch.yml** y descomentaremos las siguientes líneas con el comando:

```
sudo nano /etc/elasticsearch/elasticsearch.yml
```

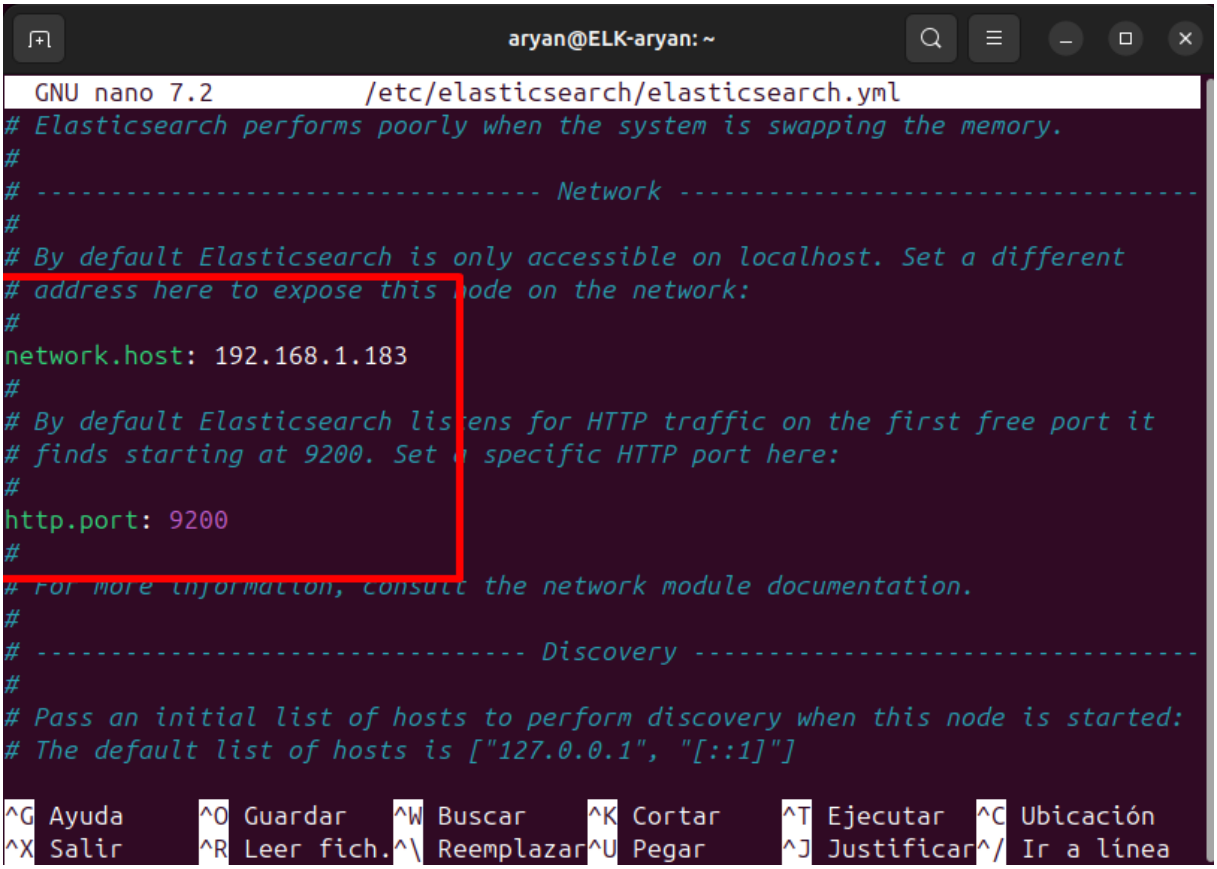

Figura 2.9: Edición archivo de elasticsearch.yml

Después de guardar los cambios, habilitaremos y arrancaremos el servicio de ElasticSearch:

```
sudo systemctl enable elasticsearch
sudo systemctl start elasticsearch
```

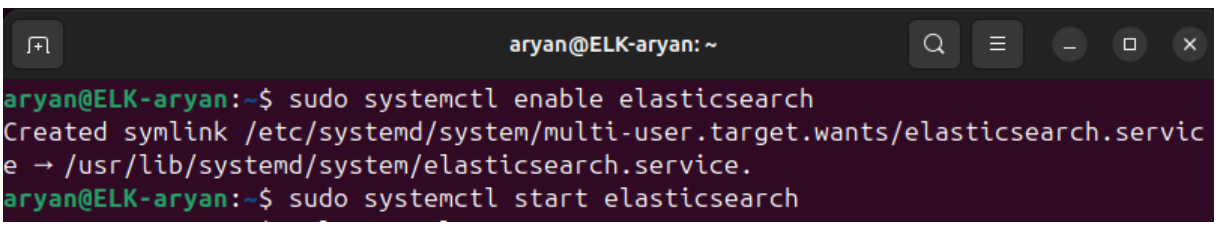

Figura 2.10: Arranque de elasticsearch

Y comprobaremos que todo ha ido correctamente viendo el estado del servicio.

```
sudo systemctl status elasticsearch
```

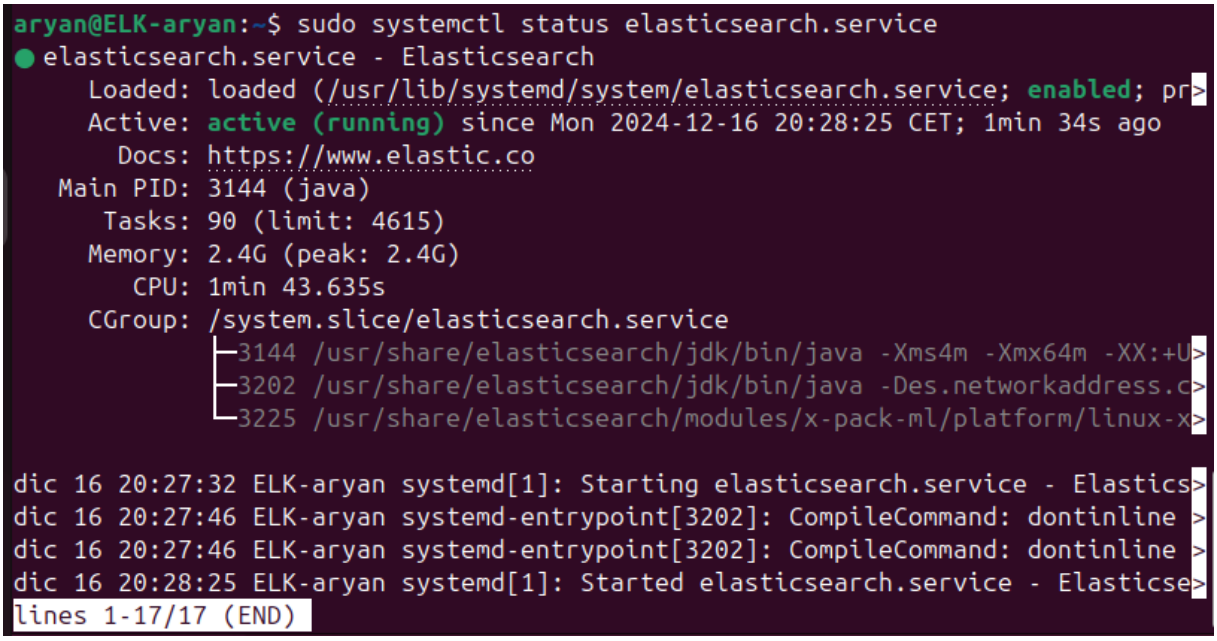

Figura 2.11: Estado de elasticsearch

Figura 2.12: Elasticsearch

Introducinedo esta url podremos acceder desde le navegador.

```
https://elastic:7o0OJbwlkQZfI*wg-5pV@localhost:9200
```

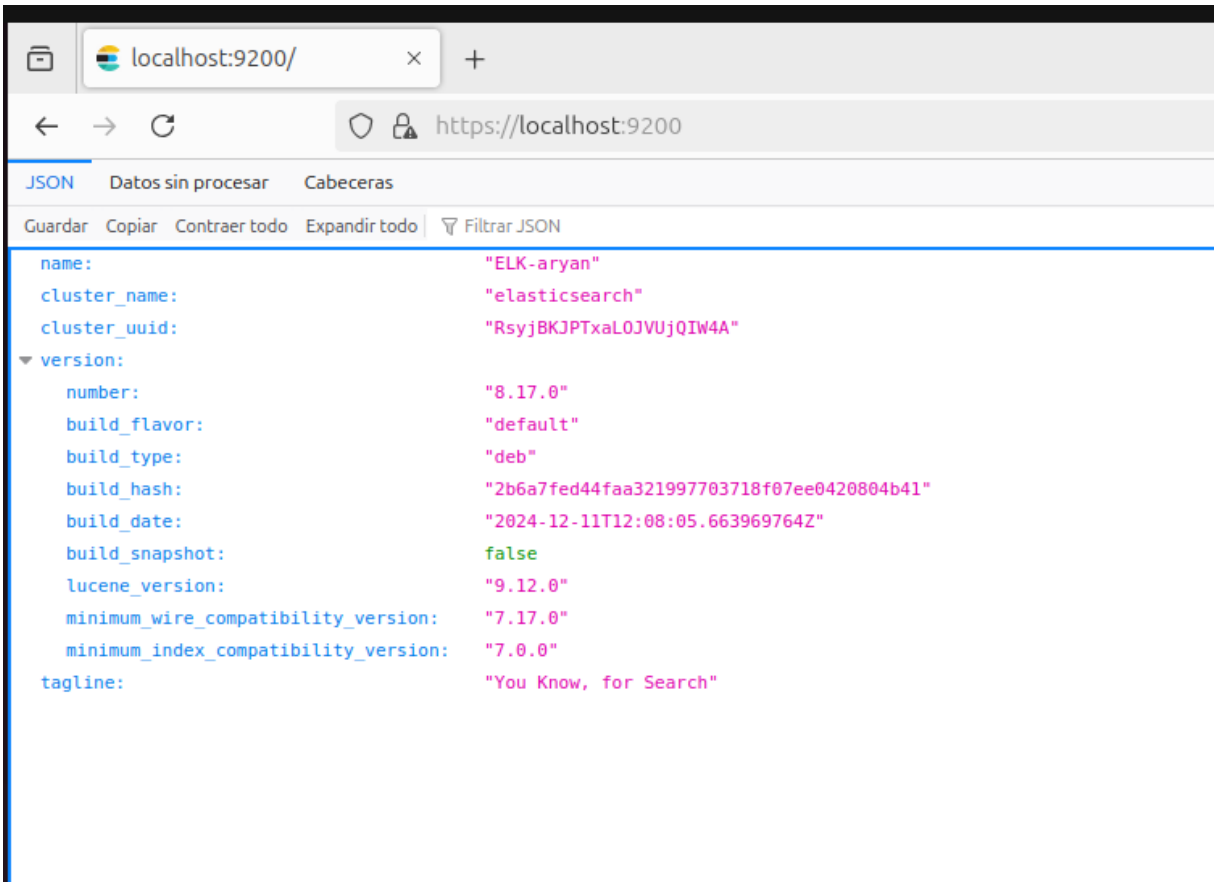

Figura 2.13: Elasticsearch en el navegador

2.3. Instalación y configuración de Kibana

Kibana es una plataforma de visualización de datos de código abierto para Elasticsearch. Instalaremos Kibana desde el mismo repositorio que Elasticsearch. Para ello usaremos el comando:

```
sudo apt install kibana
```

Figura 2.14: Instalación Kiabana

Habilitaremos y arrancaremos el servicio Kibana igual que hicimos con Elasticsearch y veremos si todo ha ido correctamente:

```
sudo systemctl enable kibana
sudo systemctl start kibana
sudo systemctl status kibana
```

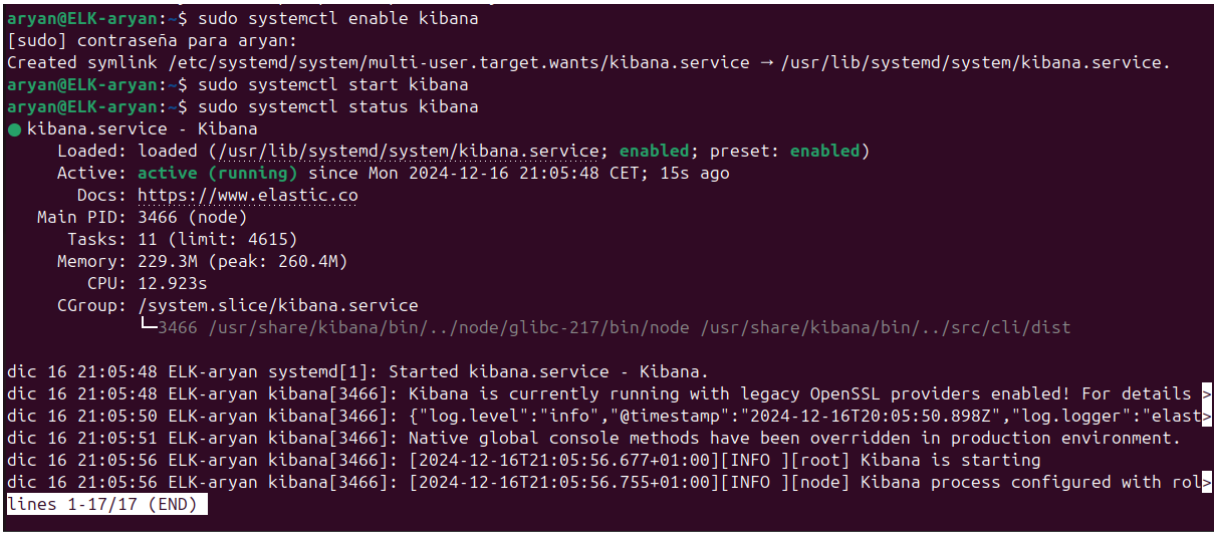

Figura 2.15: Arranque y Estado de Kibana

Editaremos el archivo de configuración de Kibana de la siguiente manera, **/etc/kibana/kibana.yml**

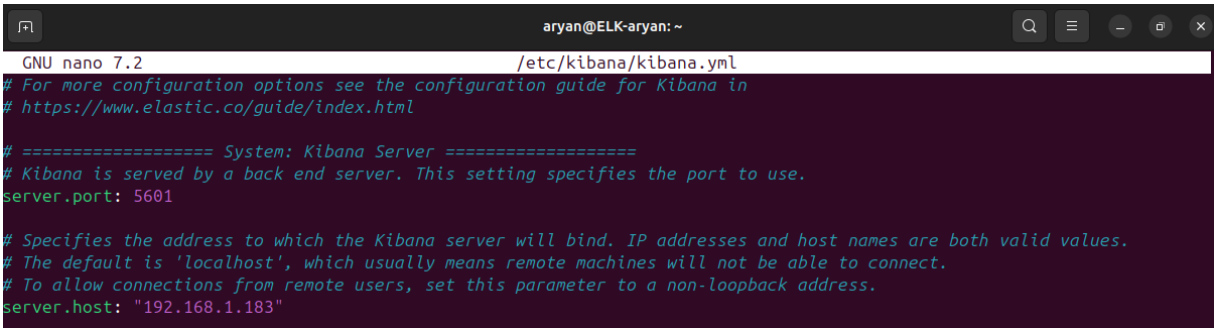

Figura 2.16: Archivo de configuración de Kibana

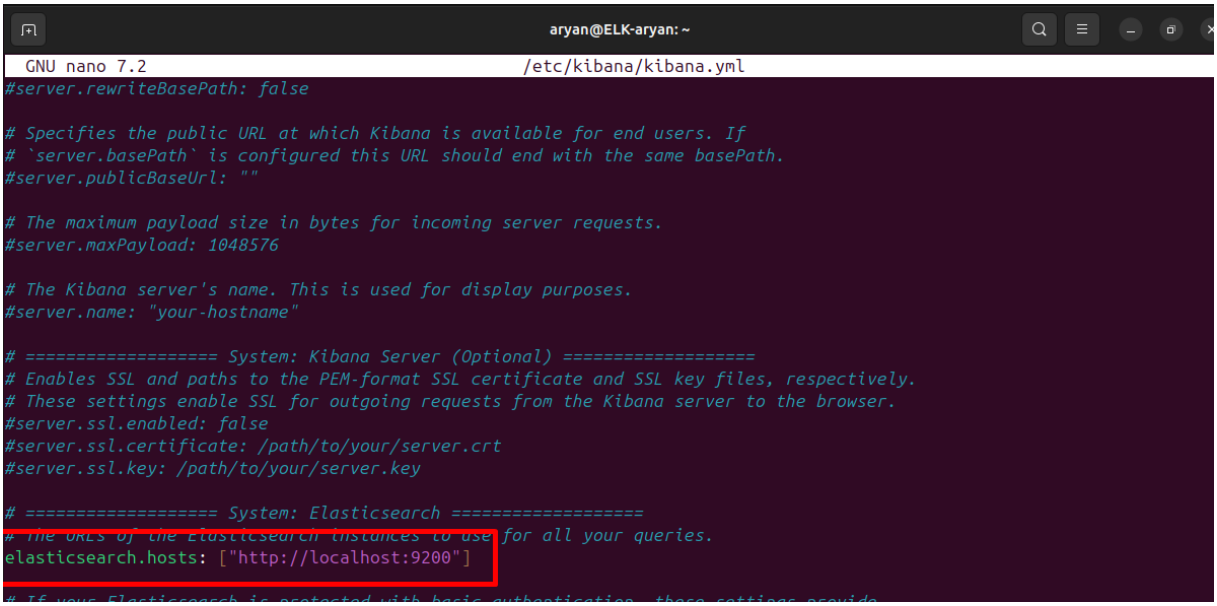

Figura 2.17: Archivo de configuración de Kibana

Y ahora accederemos a la siguiente url para poder entrar a kibana desde le navegador.

```
http://192.168.1.183:5601/
```

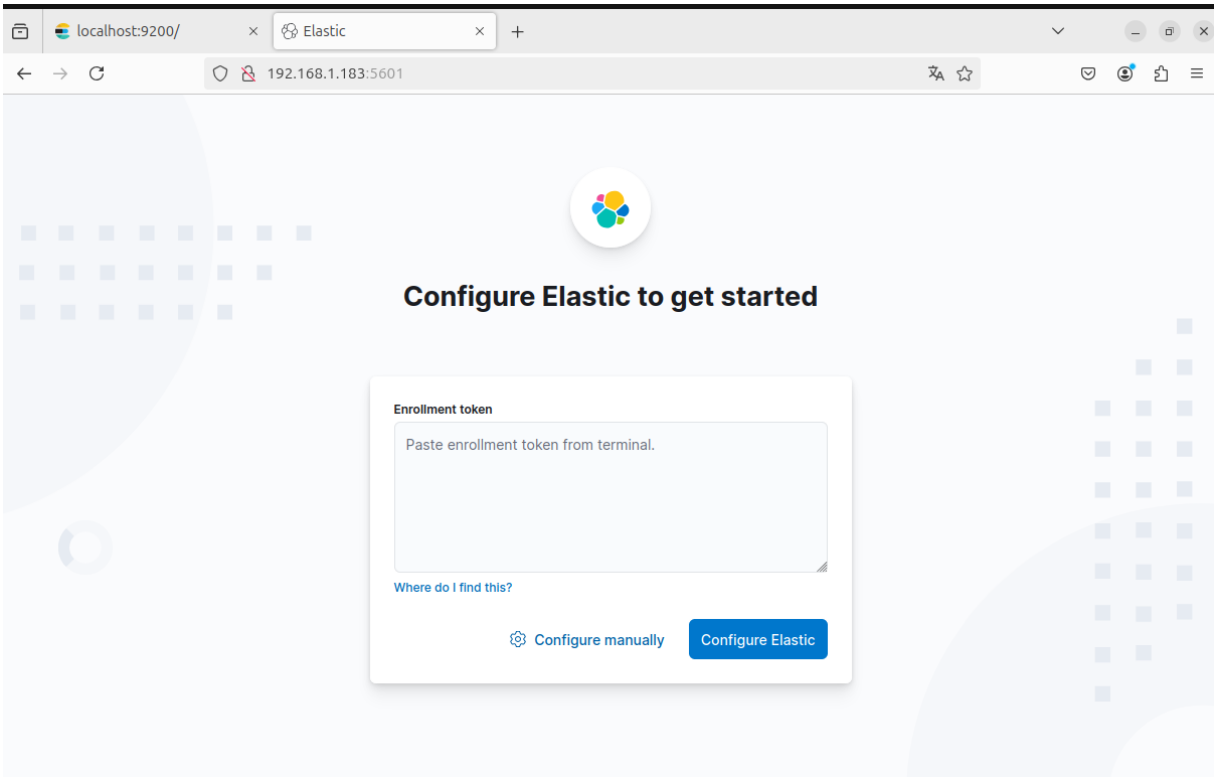

Figura 2.18: Kibana desde el navegador

Aquí podemos configurar un token que podemos crear en la configuración de Kibana, pero en nuestro caso utilizaremos la configuración manual. Hacemos clic en Configure manually y seguimos.

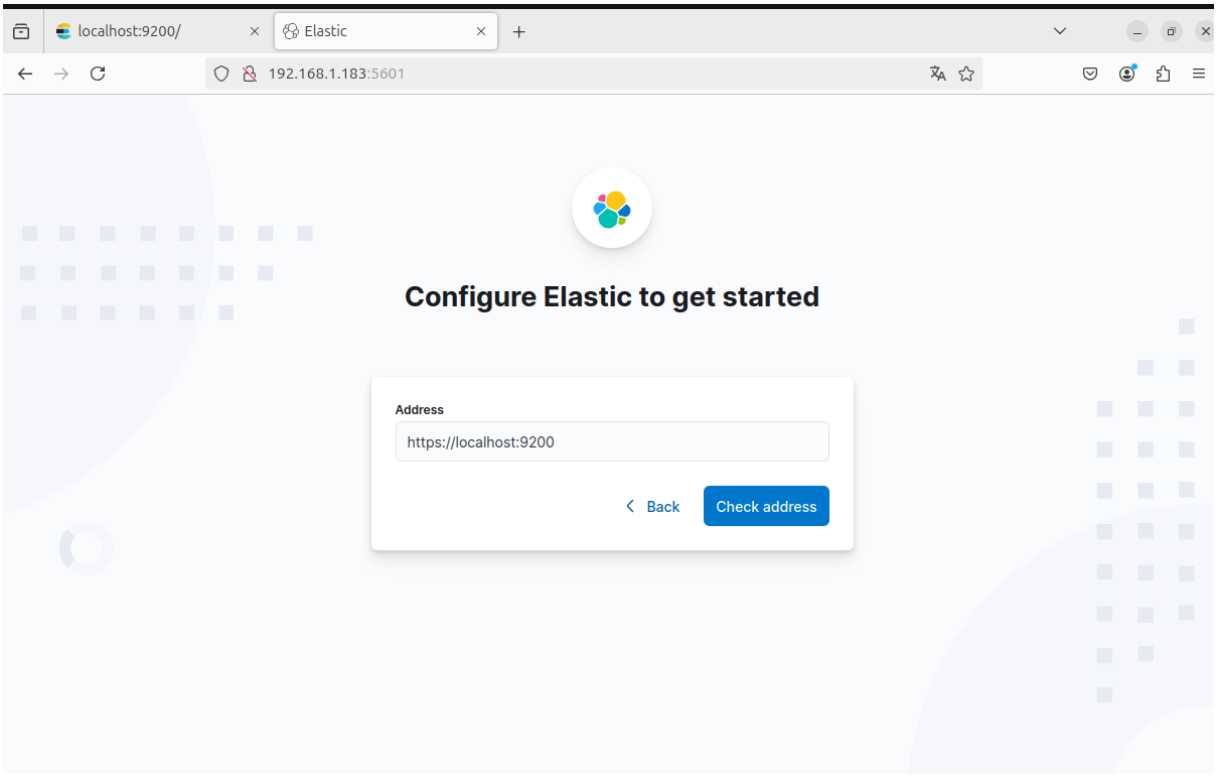

Figura 2.19: Kibana web paso dos

ElasticSearch lo tenemos escuchando al puerto 9200, por lo que seguiremos haciendo clic en Check Address.

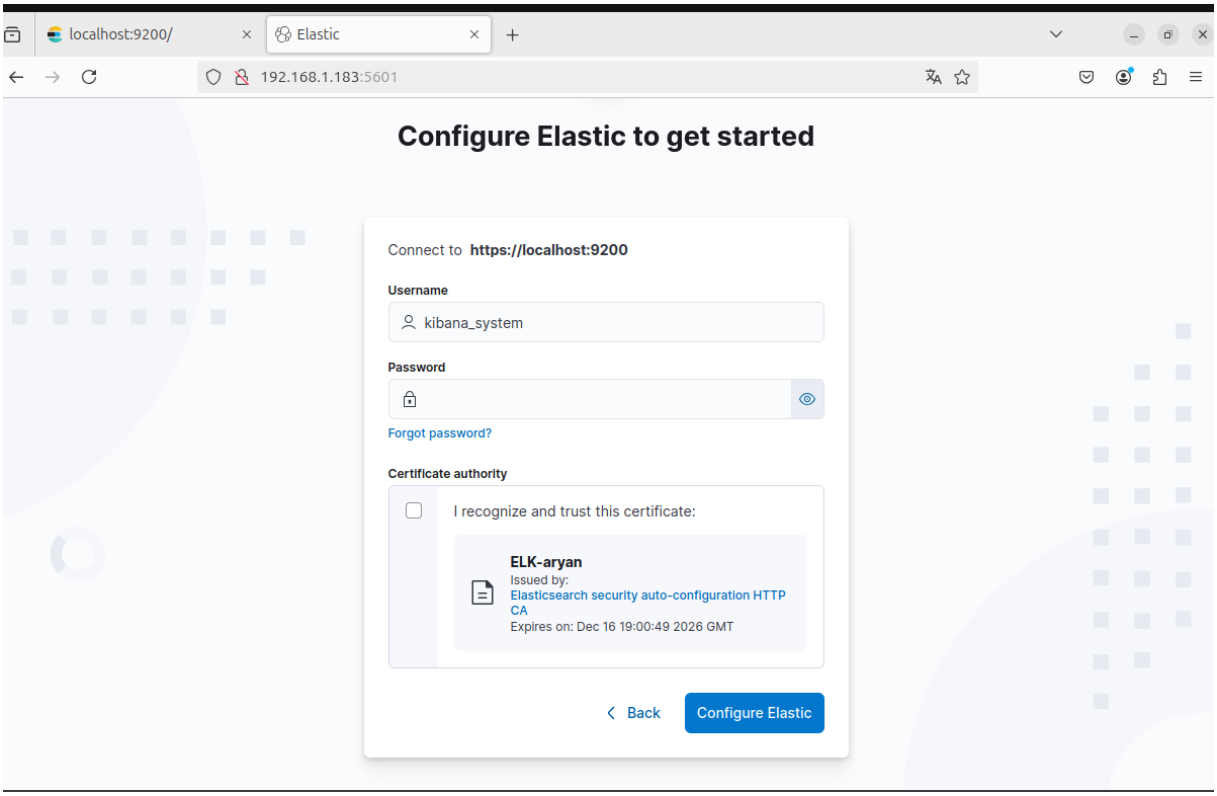

Figura 2.20: Kibana login

En este paso nos pide un login, pero no sabemos la contraseña para ello usamos el siguiente comando:

```
/usr/share/elasticsearch/bin/elasticsearch-reset-password -u kibana_system
--url http://localhost:9200 -f
```

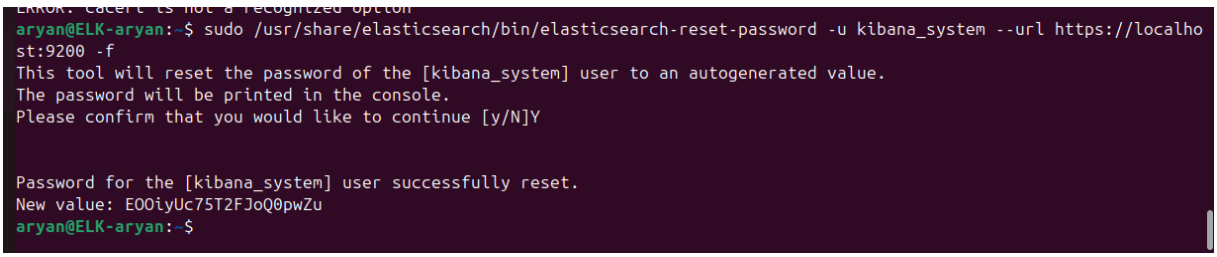

Figura 2.21: Kibana password

Luego marcaremos el certificado y haremos clic sobre Configure Elastic.

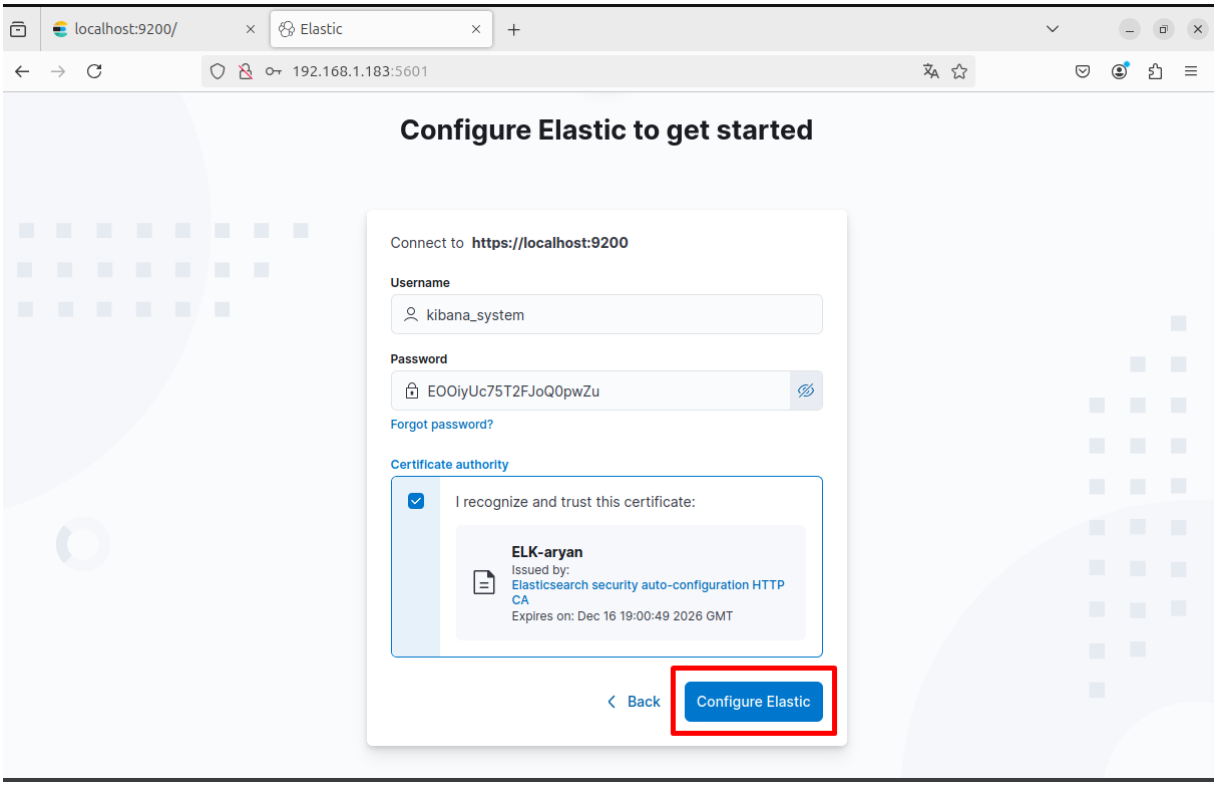

Figura 2.22: Kibana

Nos pedirá un código de verificación que podremos obtener ejecutando el siguiente comando que aparece en pantalla.

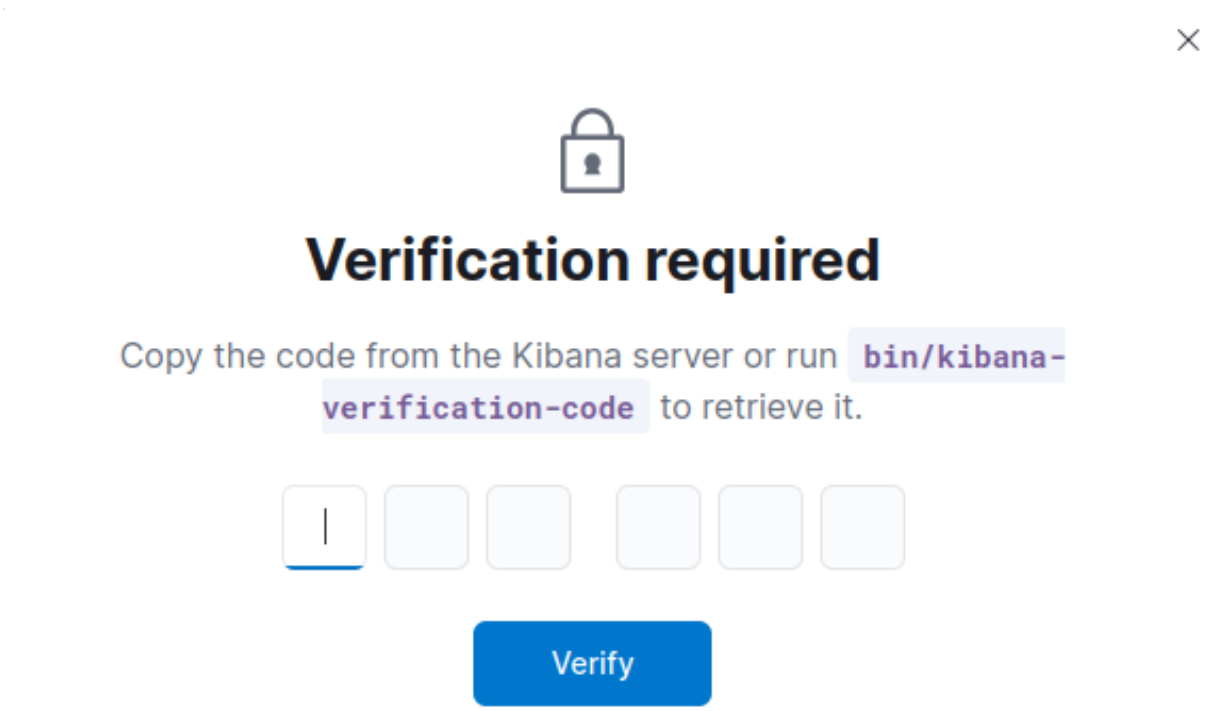

Figura 2.23: Kibana codigo

```
sudo ./usr/share/kibana/bin/kibana-verification-code
```

Figura 2.24: Kibana codigo

Y ahora accederemos después de introducir el codigo de verificación.

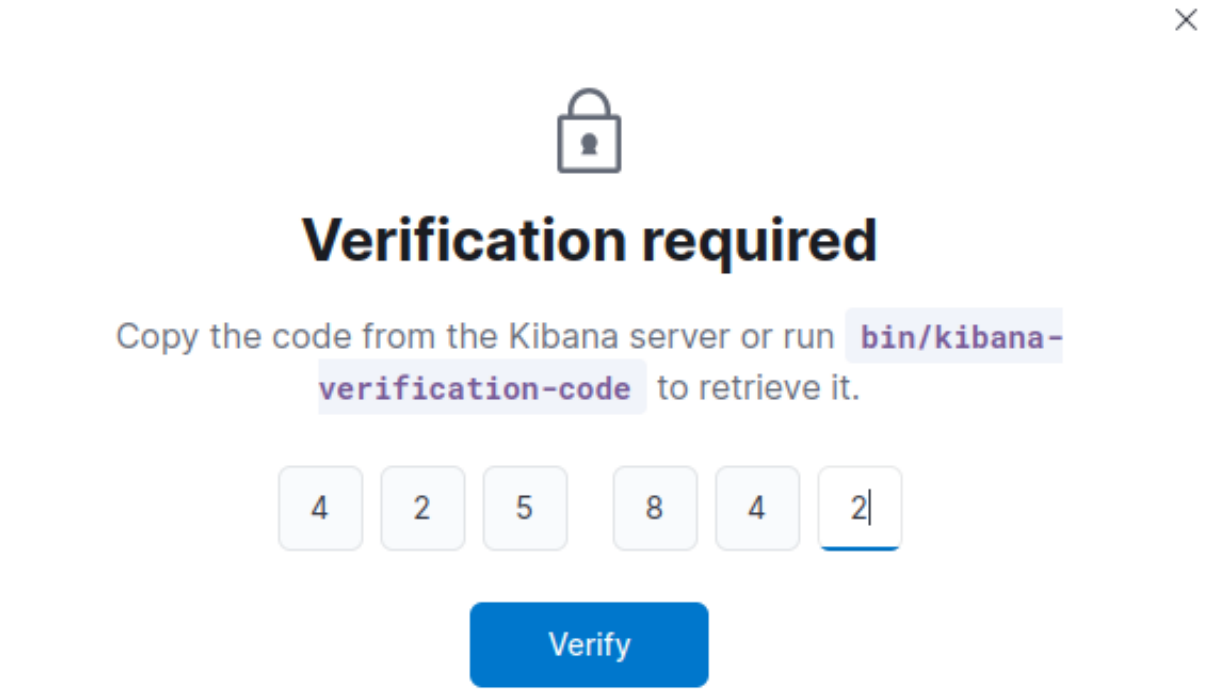

Figura 2.25: Kibana codigo

Y empezará iniciar la cnfiguracion

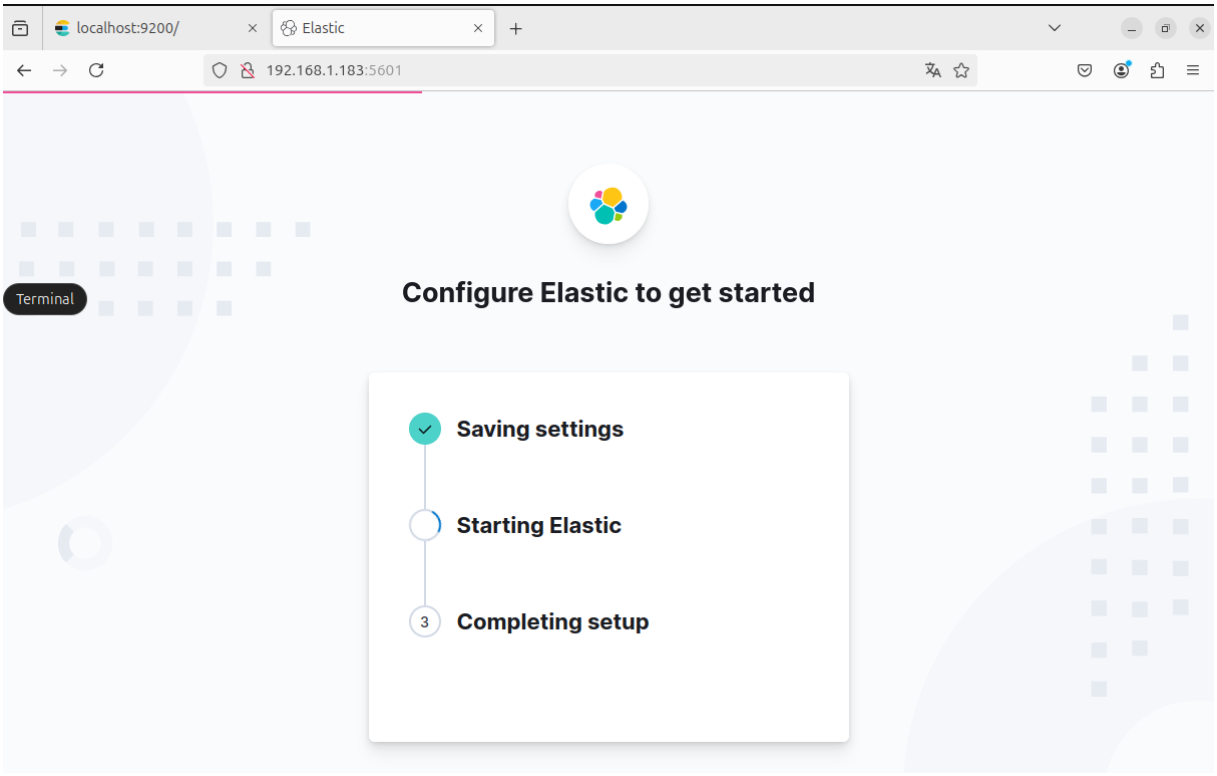

Figura 2.26: Kibana codigo

Después de cargar nos solicitara inicicar de sesión de nuevo esta vez con las credenciales de elastic o crearnos un nuevo usuario.

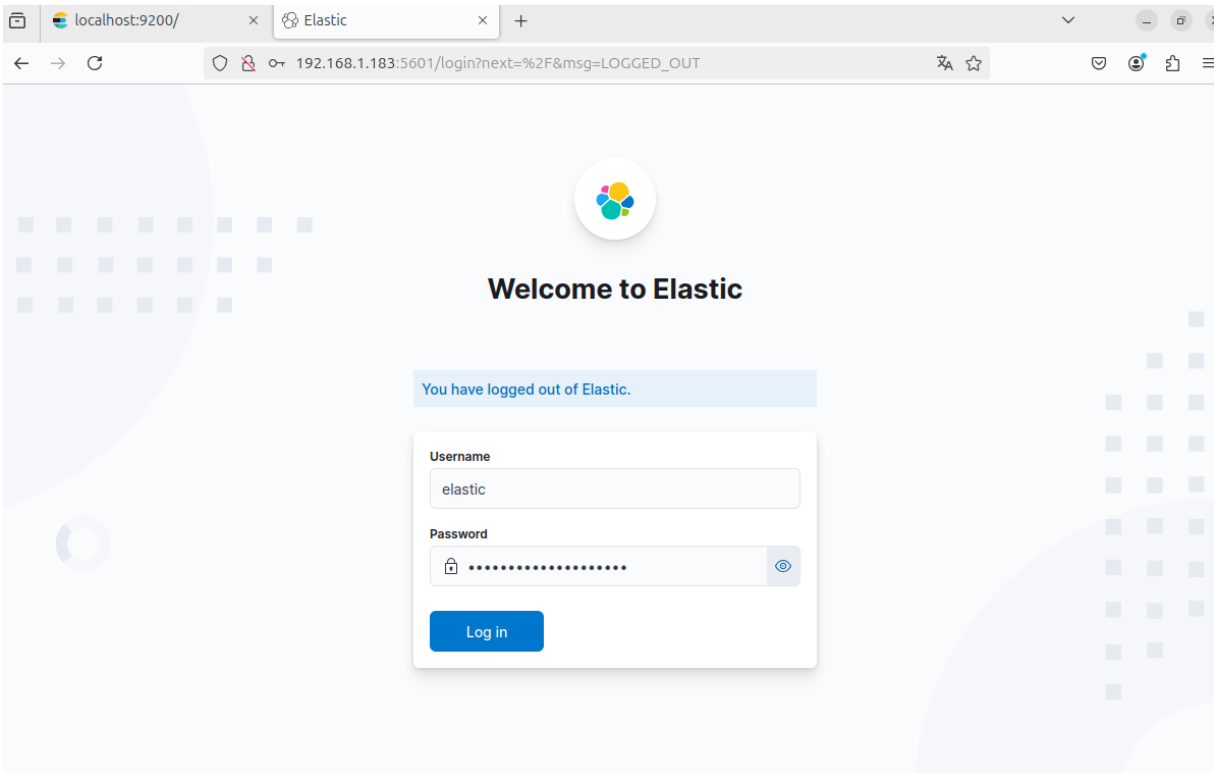

Figura 2.27: Elastic en Kibana

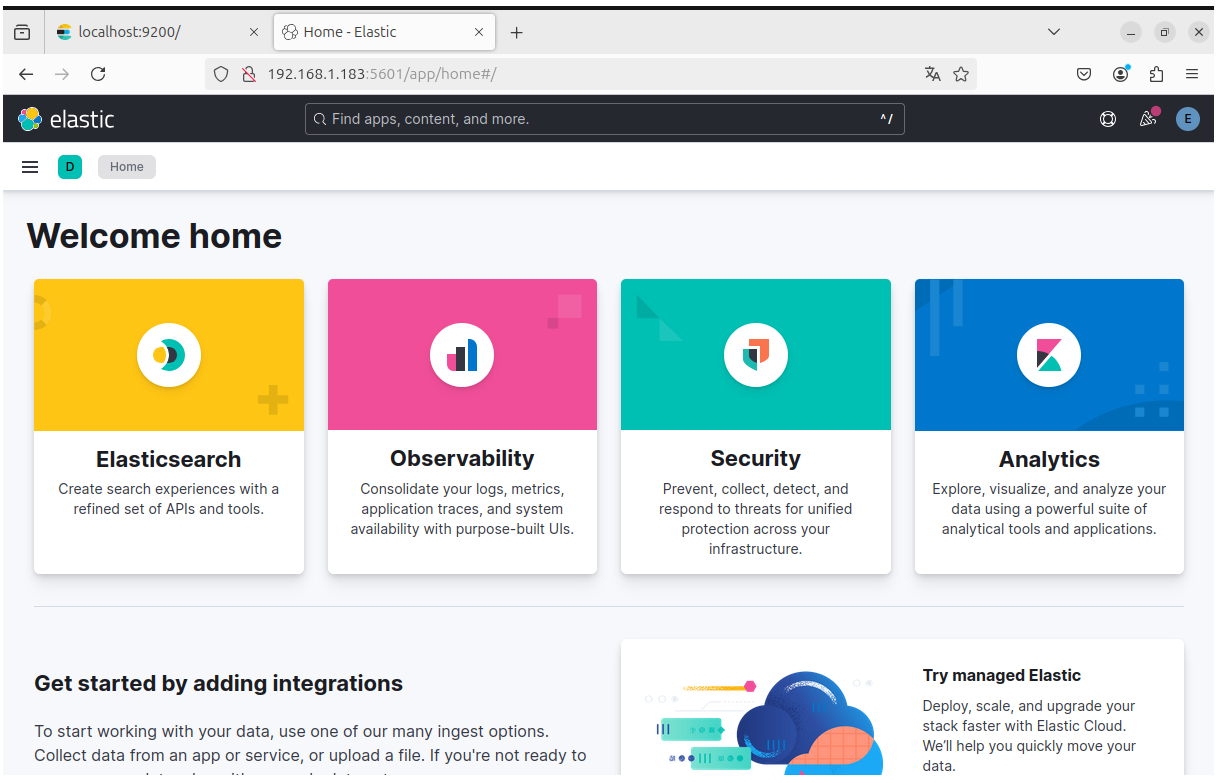

Figura 2.28: Acceso Elastic en Kibana

2.4. Instalación y configuración de Logstash

Logstash es una herramienta para la recolección, procesamiento y envío de logs y eventos. Para instalar Logstash, usaremos el mismo repositorio.

```
sudo apt install logstash
```

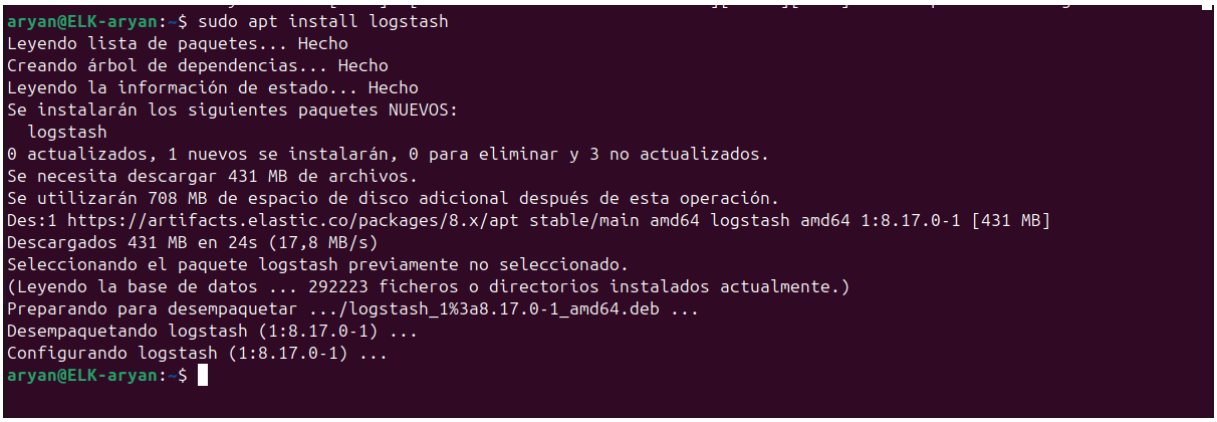

Figura 2.29: Instalación de logstash

2.5. Instalación de Filebeat en nuestras máquinas

Para poder enviar los logs o eventos desde nuestras dos máquinas tenemos que instalar Filebeat en ellas. File beat es un agente ligero que recolecta y envía logs a Logstash.

Vamos a usar la misma arquiectura que anteriormente 1.9.

Vamos a comenzar instalando Filebeat en nuestra máquina ubuntu.

2.5.1. Instalación de Filebeat en ubuntu

Para ello vamos a seguir la guía oficial que nos proporciona elasticsearch.

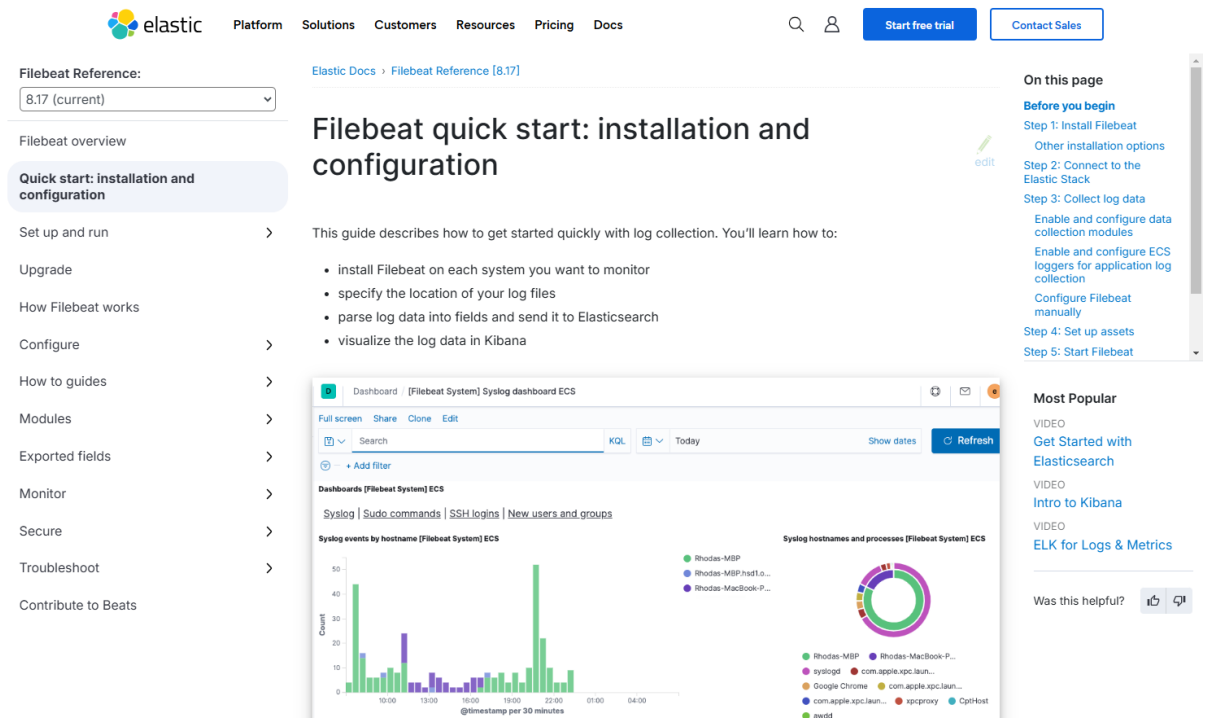

Figura 2.30: Guía Oficial de Filebeat

Para comenzar con la instalación tenemos que lanzar el siguiente comando:

```
curl -L -O
https://artifacts.elastic.co/downloads/beats/
filebeat/filebeat-8.17.0-amd64.deb

sudo dpkg -i filebeat-8.17.0-amd64.deb
```

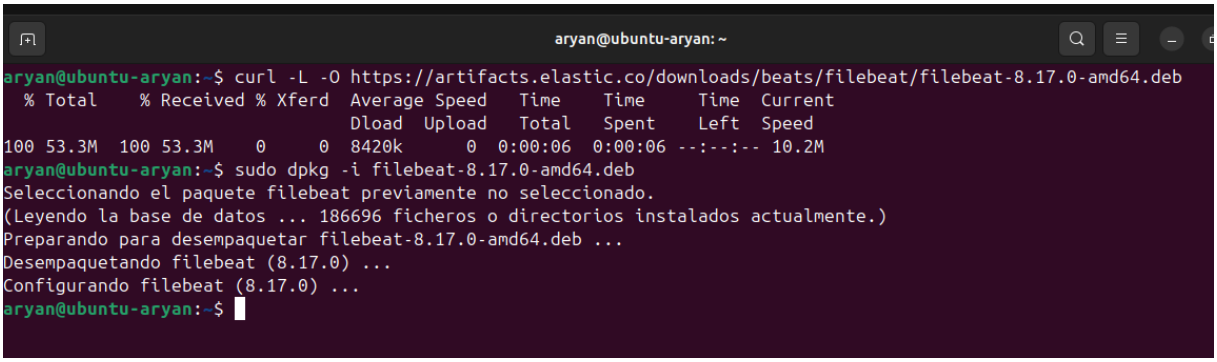

Figura 2.31: Comandos instalación de Filebeat

Antes de iniciar Filebeat tenemos que configurar las conexiones con logstash. Para ello vamos a modificar el archivo de configuración **filebeat.yml**:

```
cd /etc/filebeat
sudo nano filebeat.yml
```

e introducimos lo siguiente:

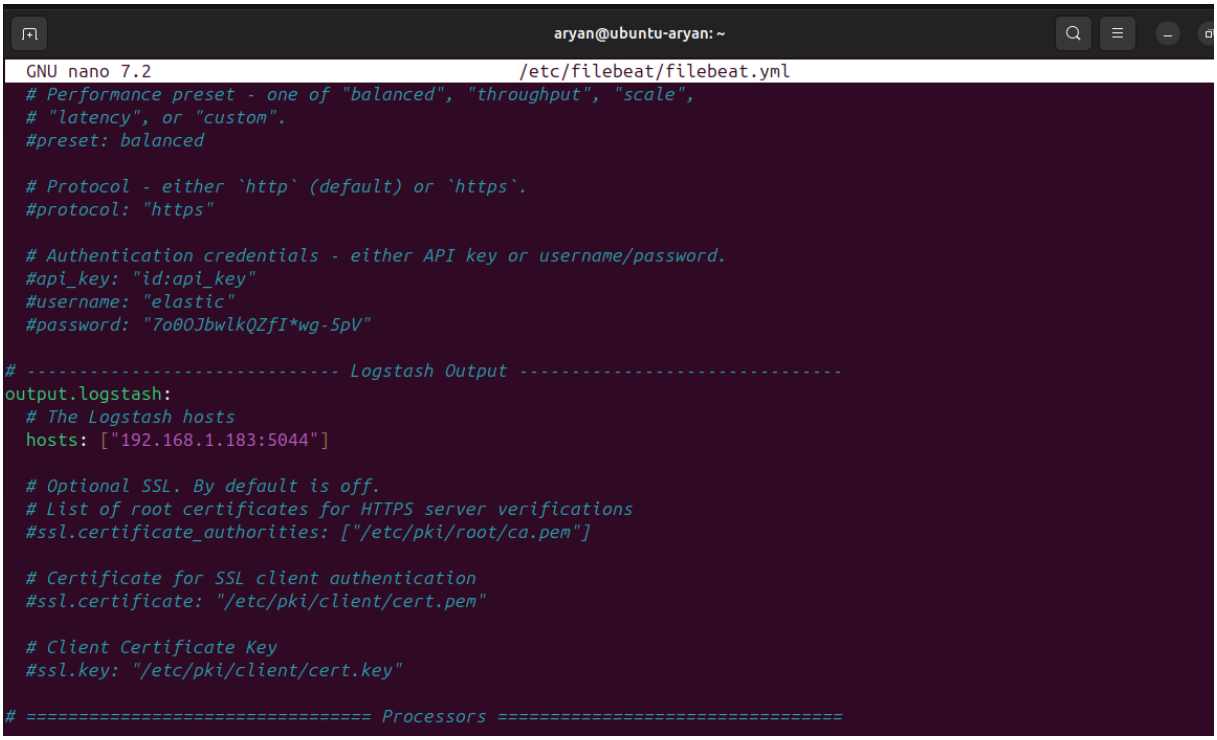

Figura 2.32: Conexión logstash y Filebeat

Además vamos a configurar y habilitar los logs que vamos a enviar. **auth.log**

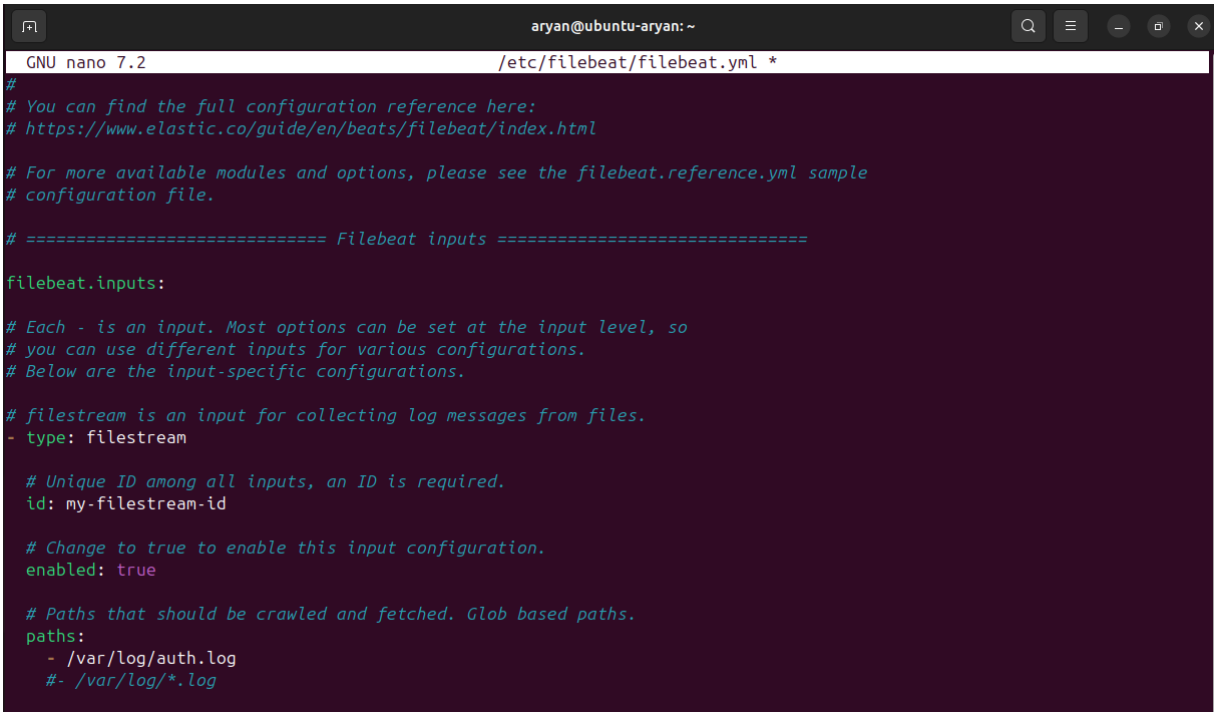

Figura 2.33: Envio de auth.log a elasticsearch

Y una vez terminado ya podemos iniciar filebeat.

```
sudo service filebeat start
sudo service filebeat status
```

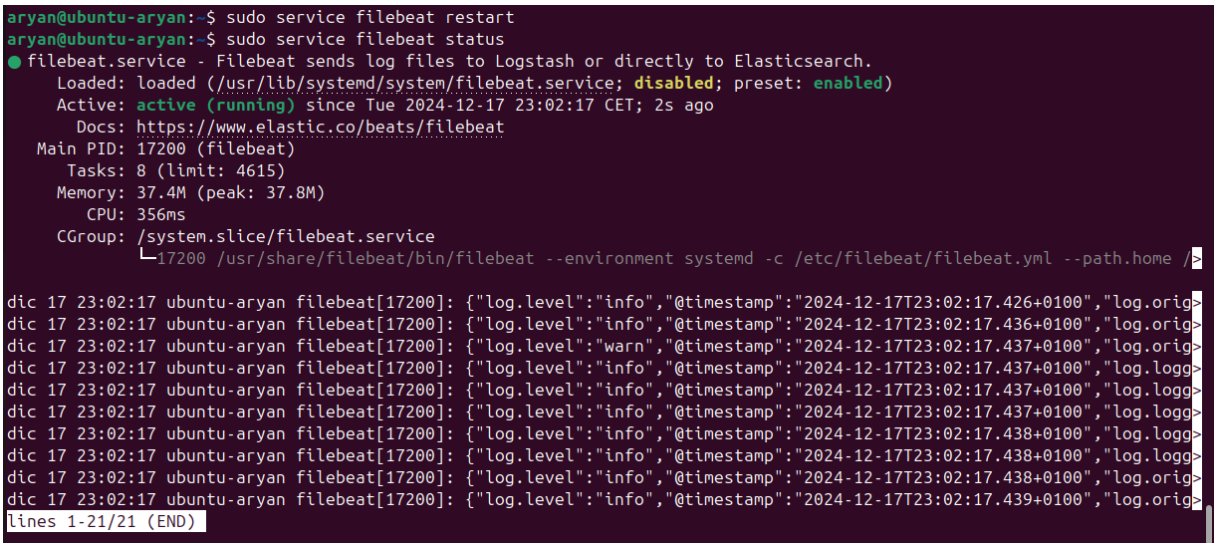

Figura 2.34: Estado del filebeat

2.6. Configurar Logstash para recibir los logs

Para que nuestro servidor reciba los datos vamos a crear un pipeline en logstash para recibir los datos. Para ello creamos una rchivo de configuración:

```
nano /etc/logstash/conf.d/ubuntu.conf
```

E introducimos lo siguiente:

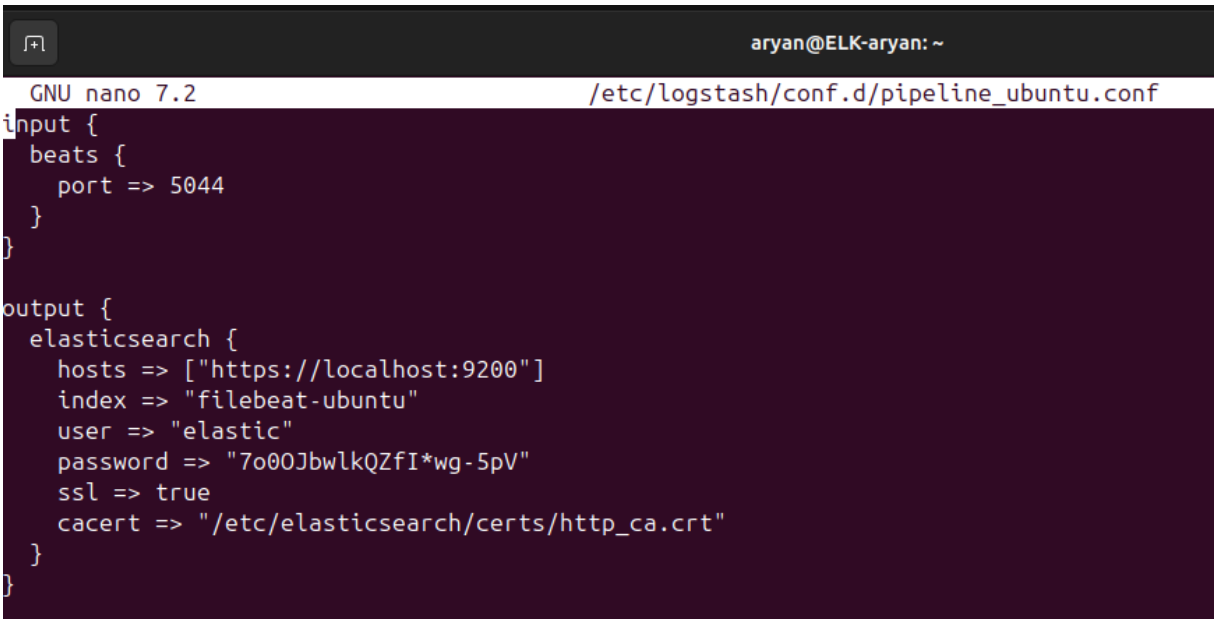

Figura 2.35: Pipeline de logstash

En input introducimos el puerto donde estara escuchando y esperando a que filebeats le envie los datos, como hemos visto en 2.33 Y en output donde estará escuchando elasticsearch.

Por último reiniciaremos el servicio de logstash.

```
sudo systemctl restart logstash
```

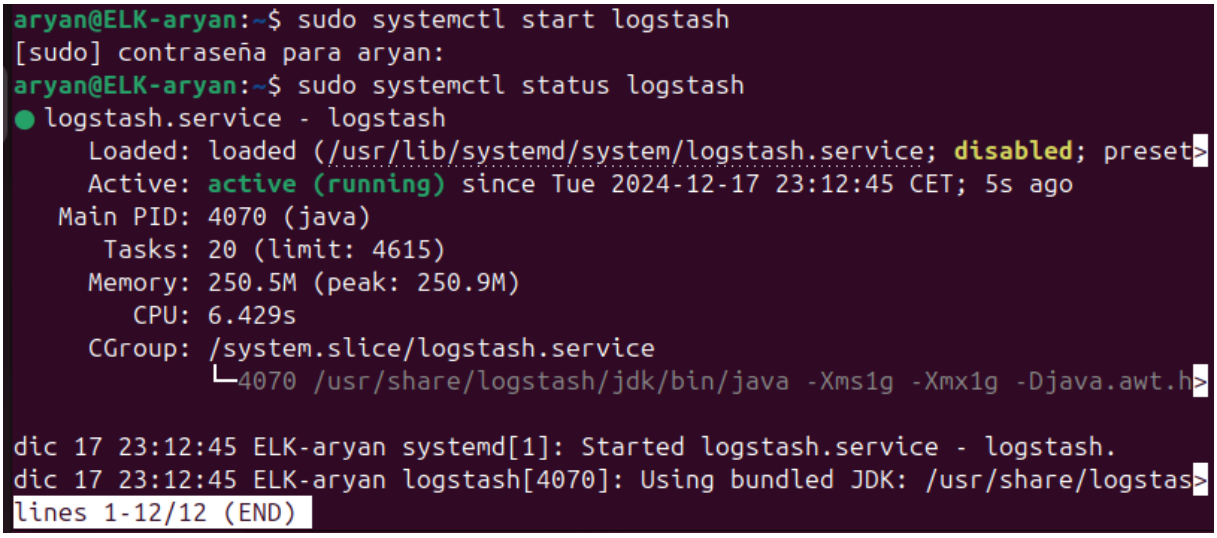

Figura 2.36: Estado de logstash

y con el siguiente comando confirmaremos que la conexion se hace entre filebeat y logstash

```
sudo filebeat test output
```

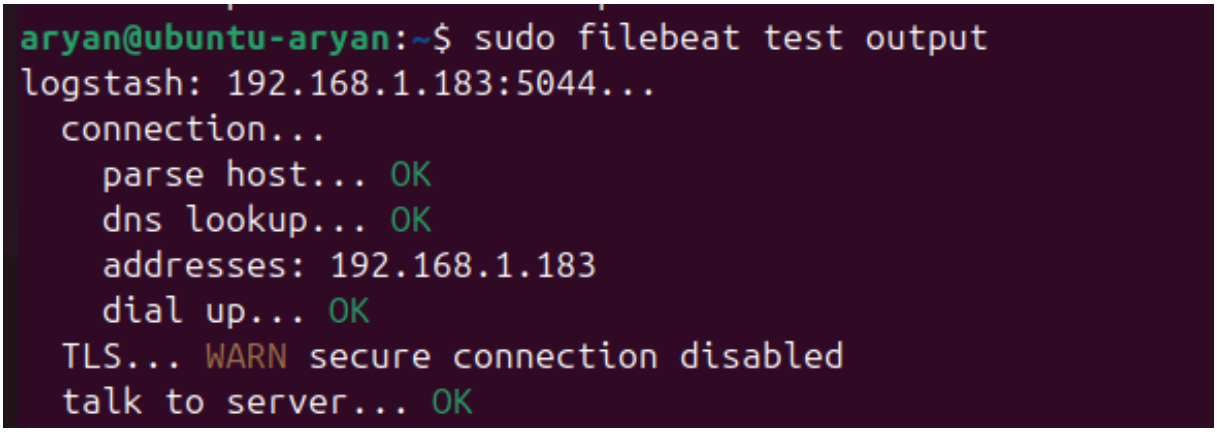

Figura 2.37: Conexion de Filebeat - logstash

2.6.1. Confirmar que los datos llegan

Ahora que tienemos los datos llegando a Logstash, el siguiente paso es asegurarnos de que Elasticsearch esté recibiendo y almacenando esos datos correctamente.

Para ello vamos a hacer uso de este comando

```
curl -u elastic:7o0OJbwlkQZfI*wg-5pV --cacert
/etc/elasticsearch/certs/http_ca.crt
https://localhost:9200/_cat/indices/filebeat-*?v=true
```

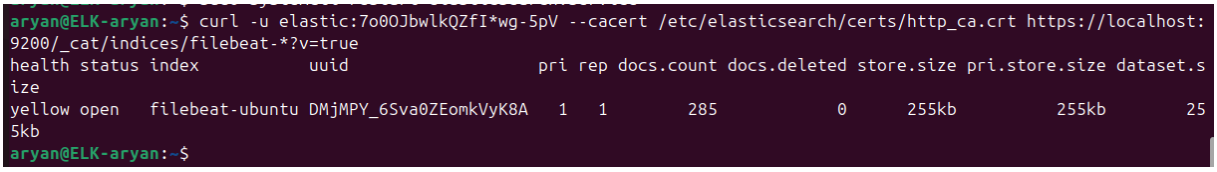

Figura 2.38: Datos en elasticsearch recibidos

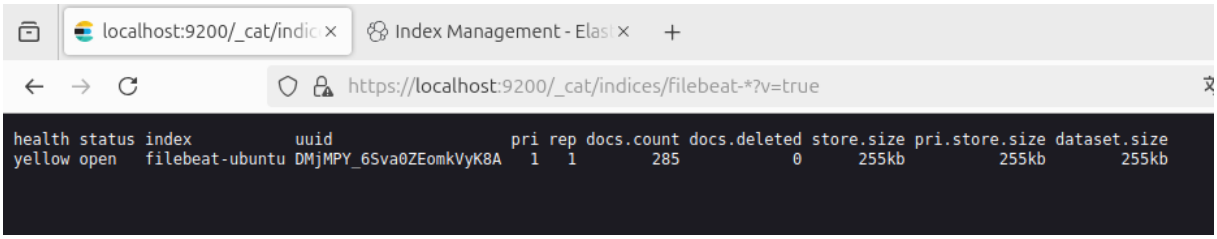

Figura 2.39: Datos en elasticsearch recibidos vistos en el navegador

En estas imagenes podemos ver como la conexión entre Filebeat ->Logstash ->Elasticsearch es correcta. Ya que los datos se han enviado auntomaticamente y los podremos visualizar en Kibana.

2.7. Analizando y visualizando los datos en Kibana

Para poder explorar, visualizar y analizar los datos vamos a usar la herramienta de analytics.

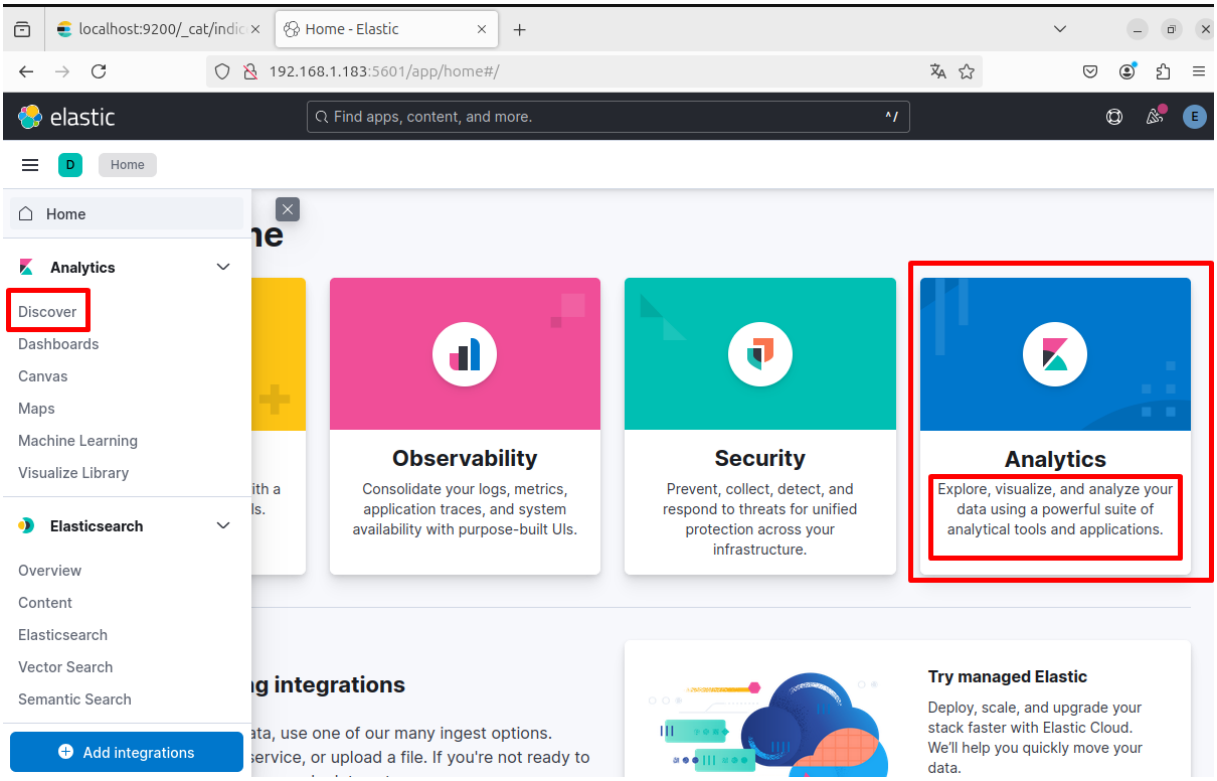

Figura 2.40: Discover

Después le daremos a create data view.

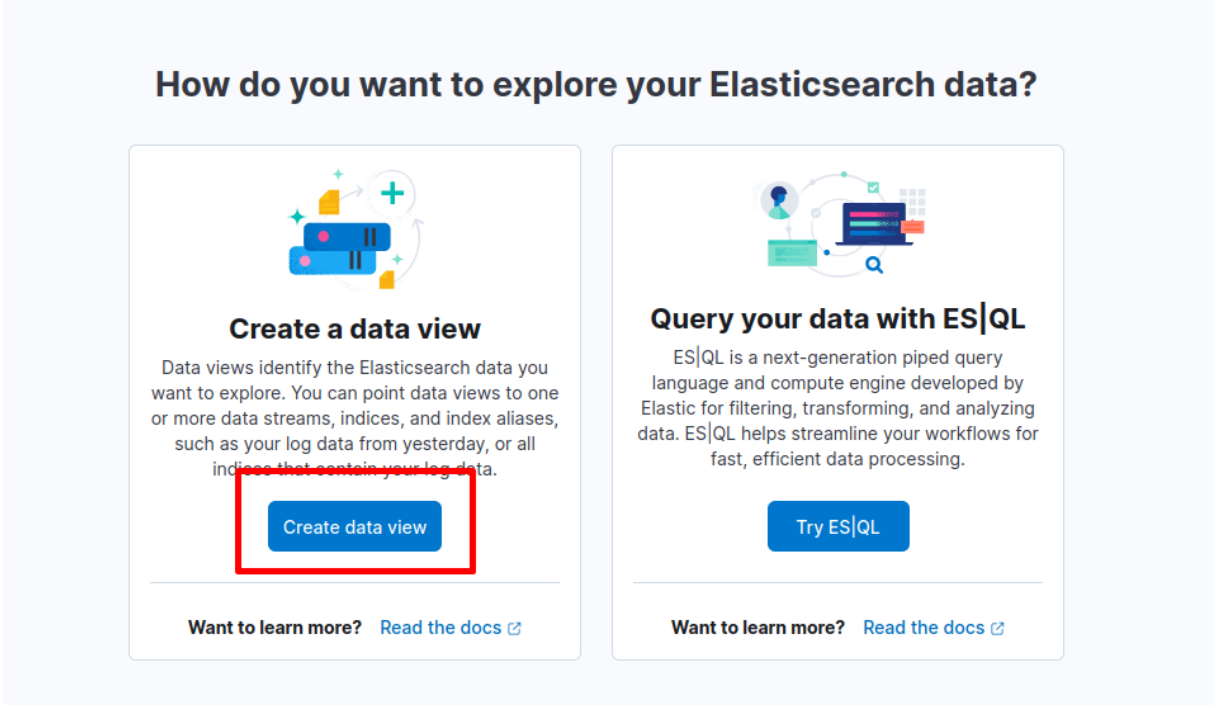

Figura 2.41: Create new dataview

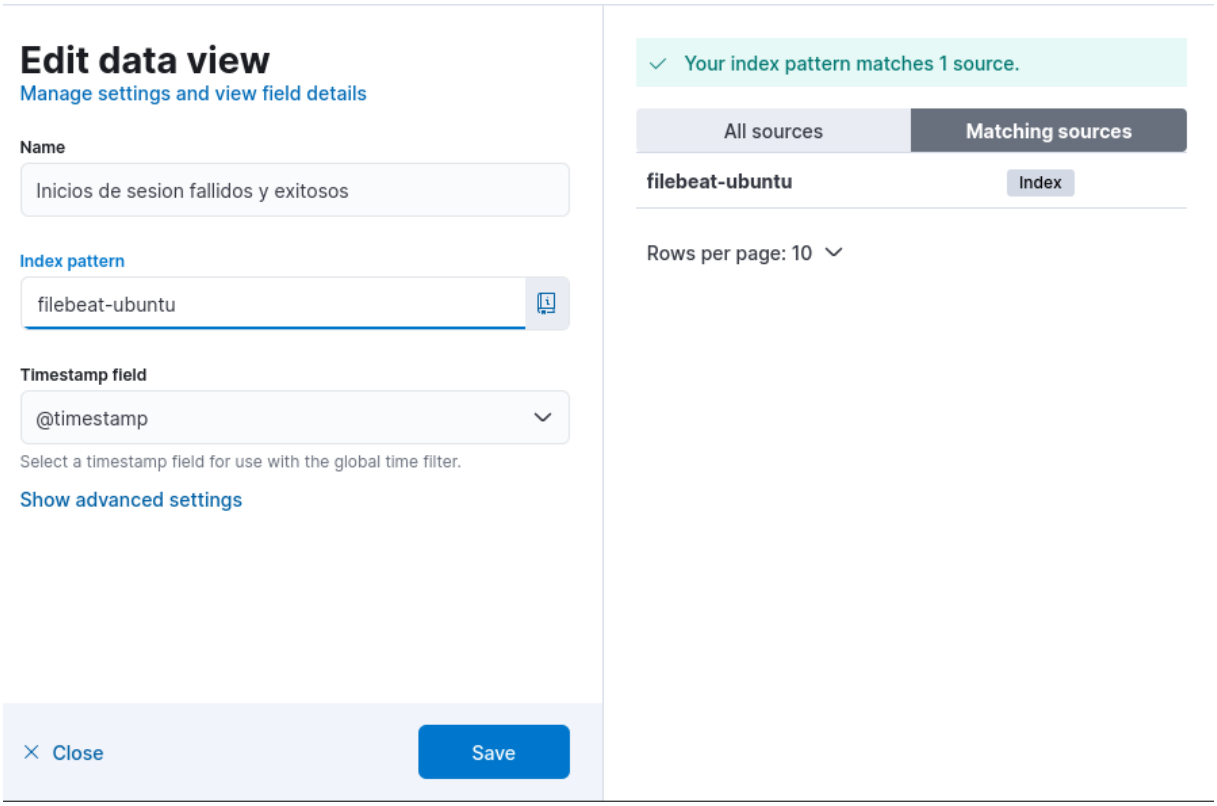

Figura 2.42: Create new dataview

Lo llamaremos inicios de sesion fallidos y exitosos y usaremos el incide filebeat-ubuntu.

Una vez guardado veremos los eventos y los podremos analizar. Encontraremos a mano los campos que aparecen, para poder crear un filtro y poder visualizar los eventos de una mejor forma. Además podremos ampliar la información de los eventos.

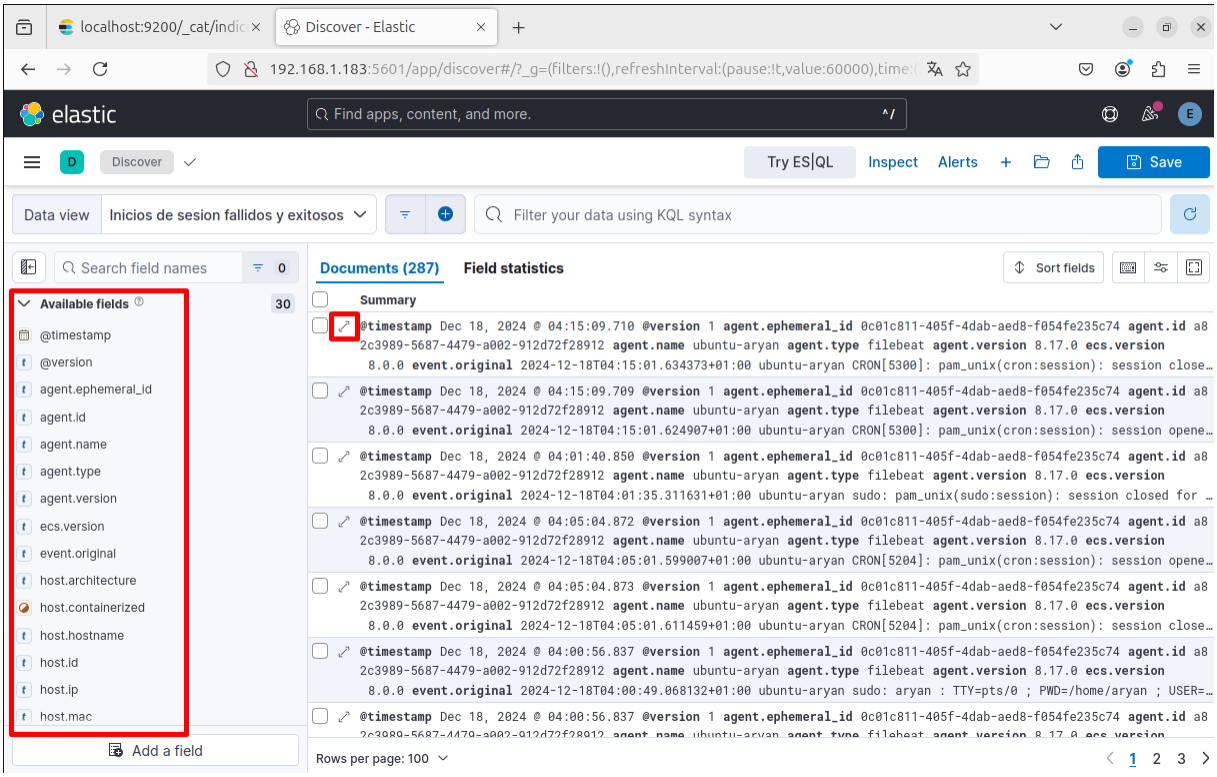

Figura 2.43: Analisis eventos

Si ampliamos podremos ver mucha información de los eventos.

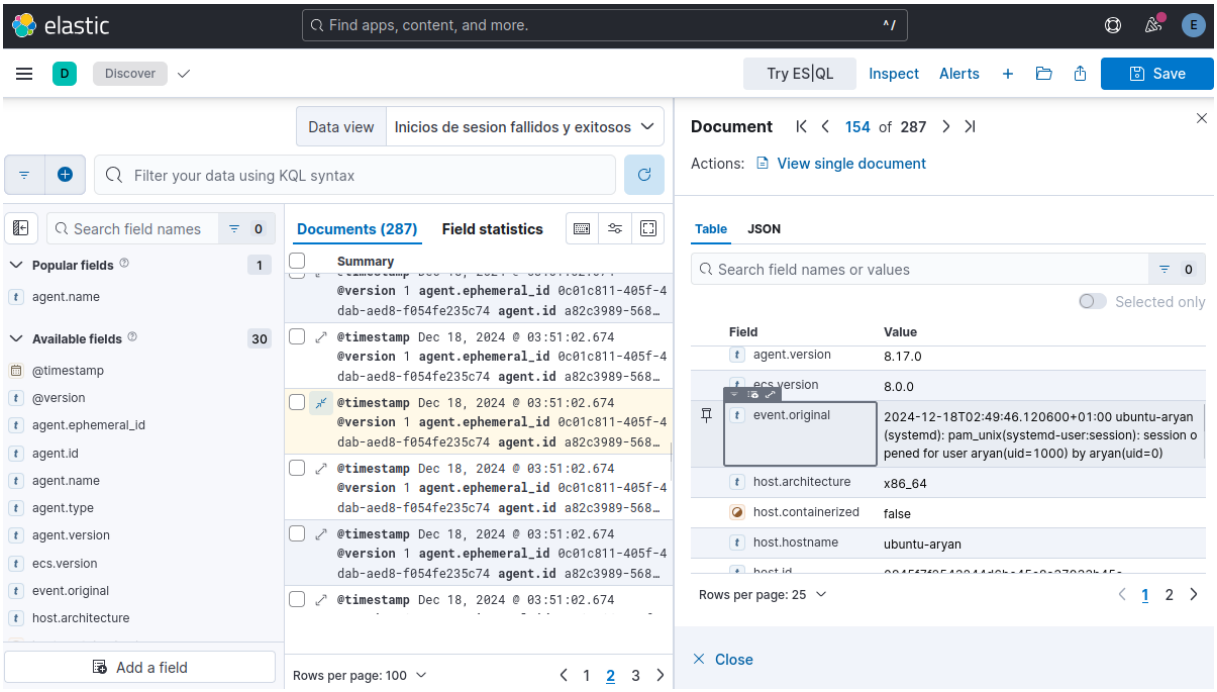

Figura 2.44: Información de Analisis eventos

Ahora vamos a usar los campos que nos interesen para asi poder ver los eventos mas claros.

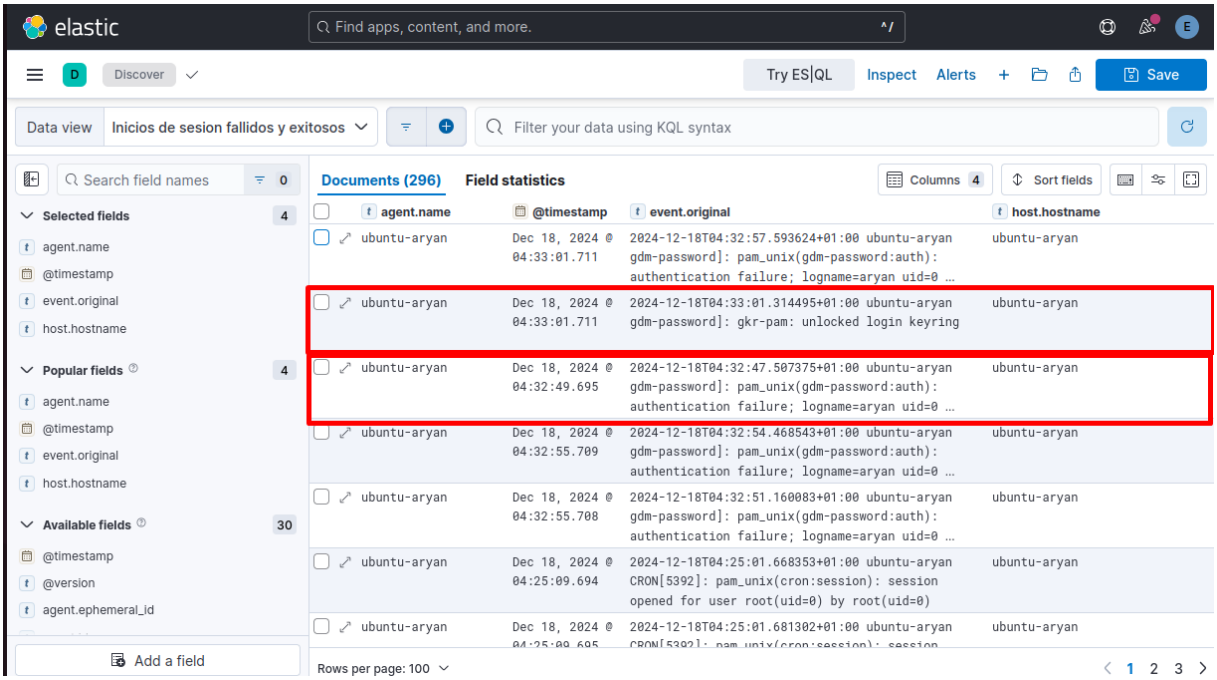

Figura 2.45: Información de Analisis eventos

Antes de poder continuar y visualizar nuestro datos vamos a crear un campo personalizado para separar los eventos de inicios de sesión exitosos, con los fallidos.

Para ello en data view le damos a Add field.

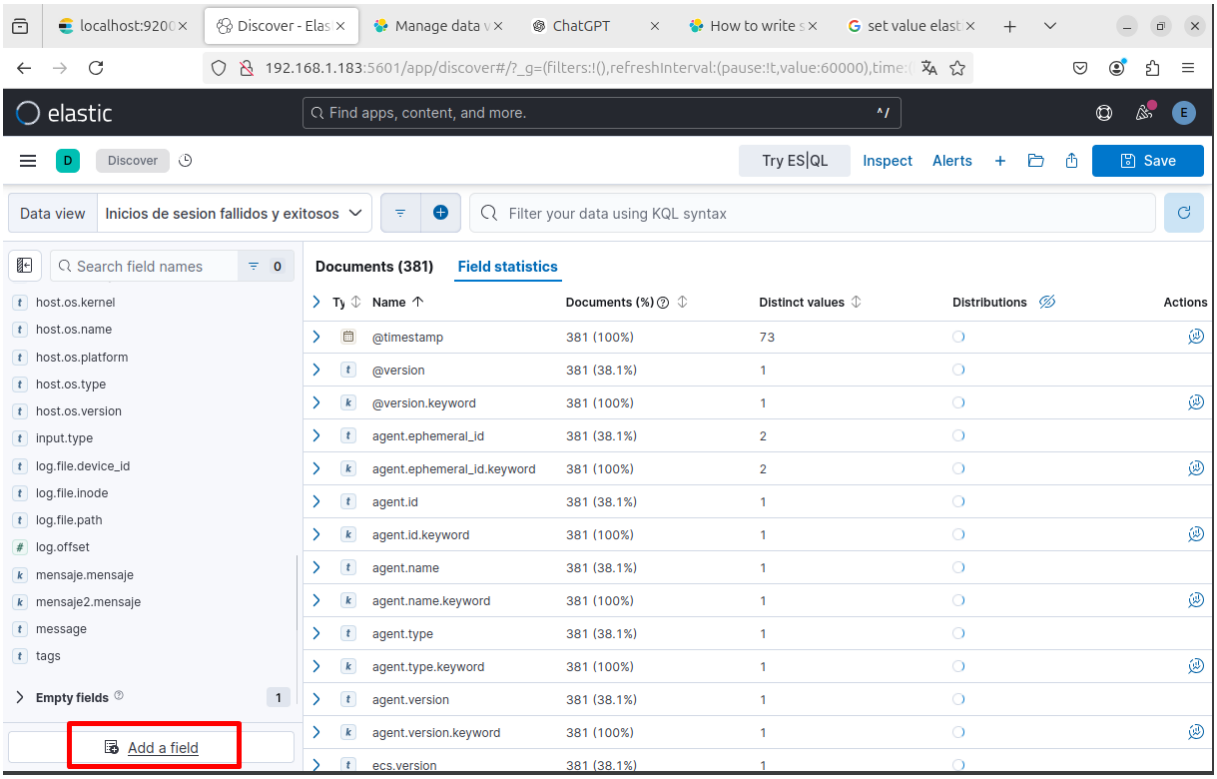

Figura 2.46: Añadir nuevo campo

Y pondremos un nombre a nuestro campo y configuraremos un valor, activanola.

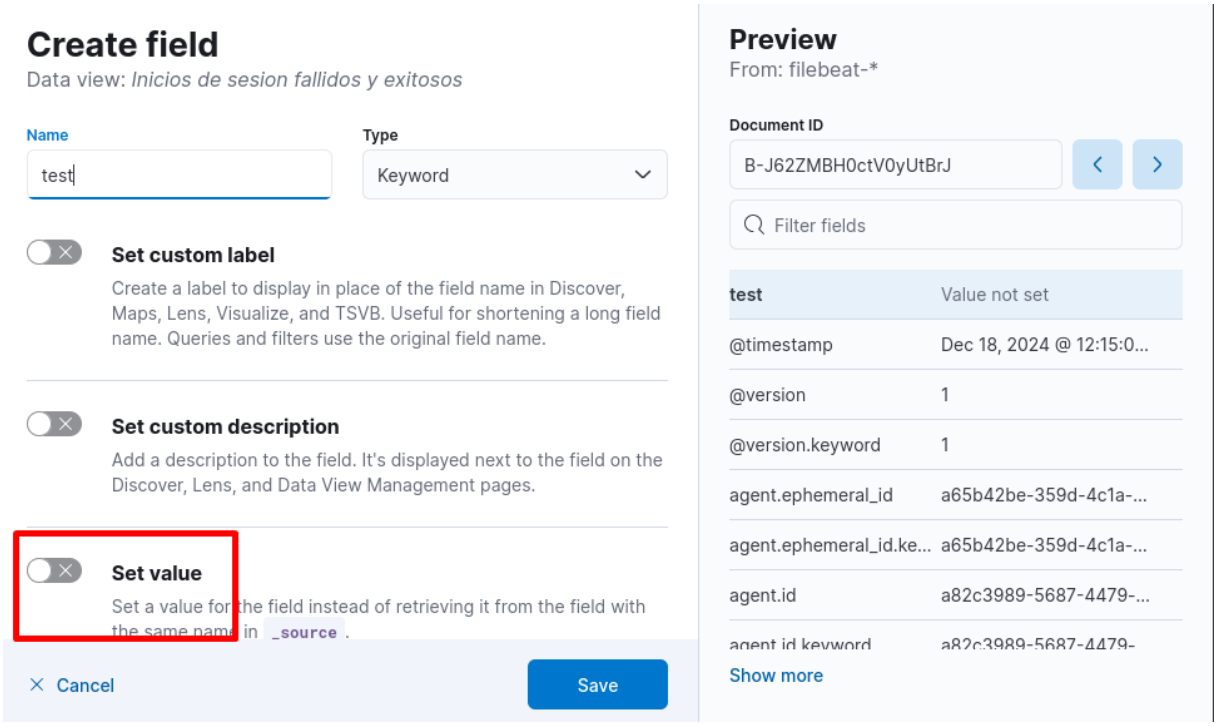

Figura 2.47: Añadir nuevo campo

Tras activar set value deberemos de insertar un script para poder administar el valor del campo.

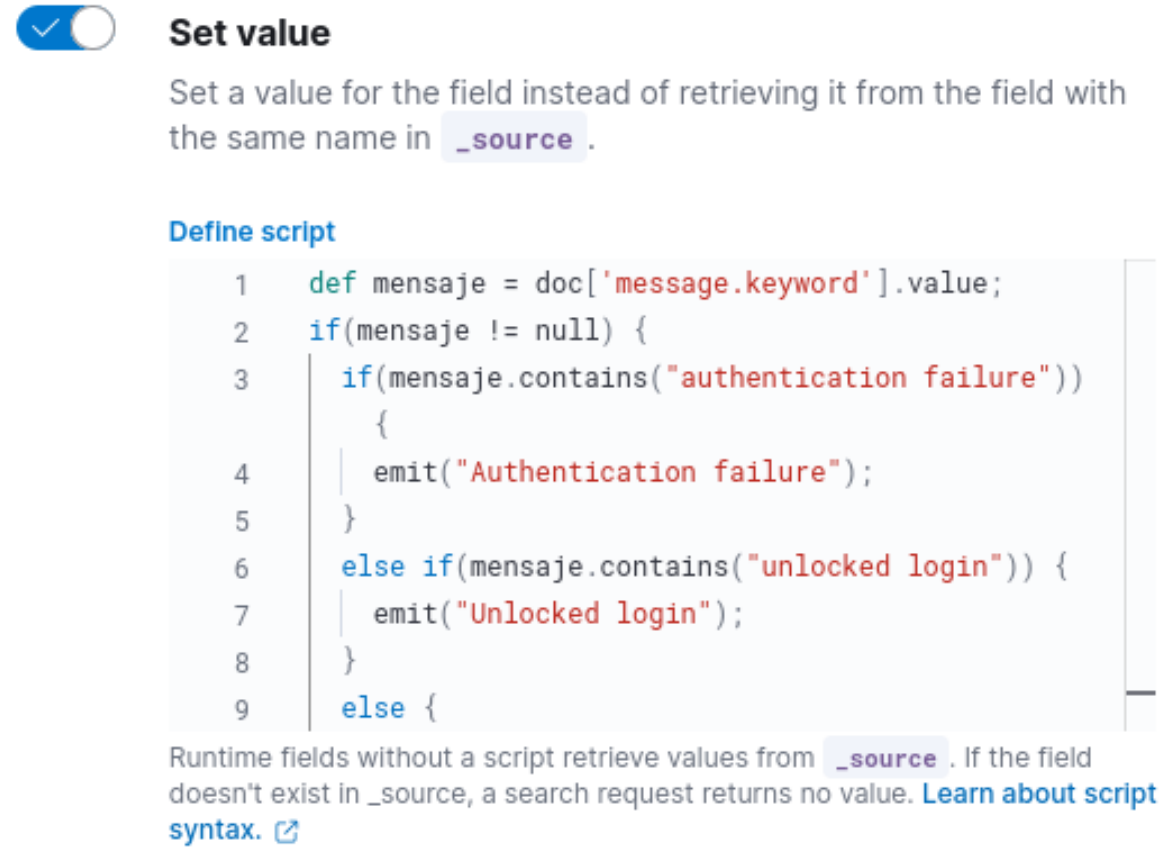

Figura 2.48: Script campo nuevo

El código entero es el siguiente:

```
def mensaje = doc['message.keyword'].value;
if (mensaje != null){
    if (mensaje.contains("authenitcation failure")){
        emit("Authentication failure");
    }
    else if (mensaje.contains("unlocked login")){
        emit("Unlocked login");
    }
    else{
        emit("None");
    }
}
```

Este codigo lo que hace es ver si la variable message no es nula y si contiene authentication

failure o unlocked login, y en caso afirmativo poner ese valor a la variable mensaje. Una vez creado podemos seleccionarlo y darle a visualizar.

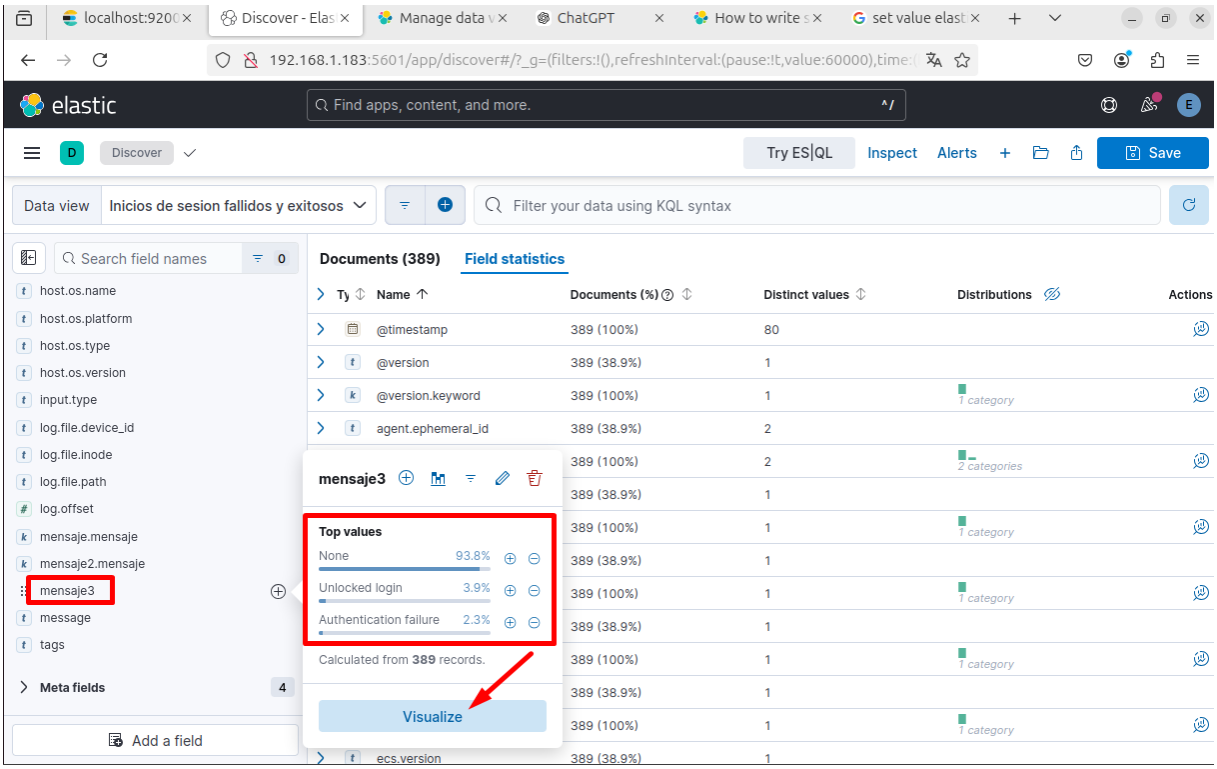

Figura 2.49: visualizar campo nuevo

Y podremos ver en una gráfica los valores.

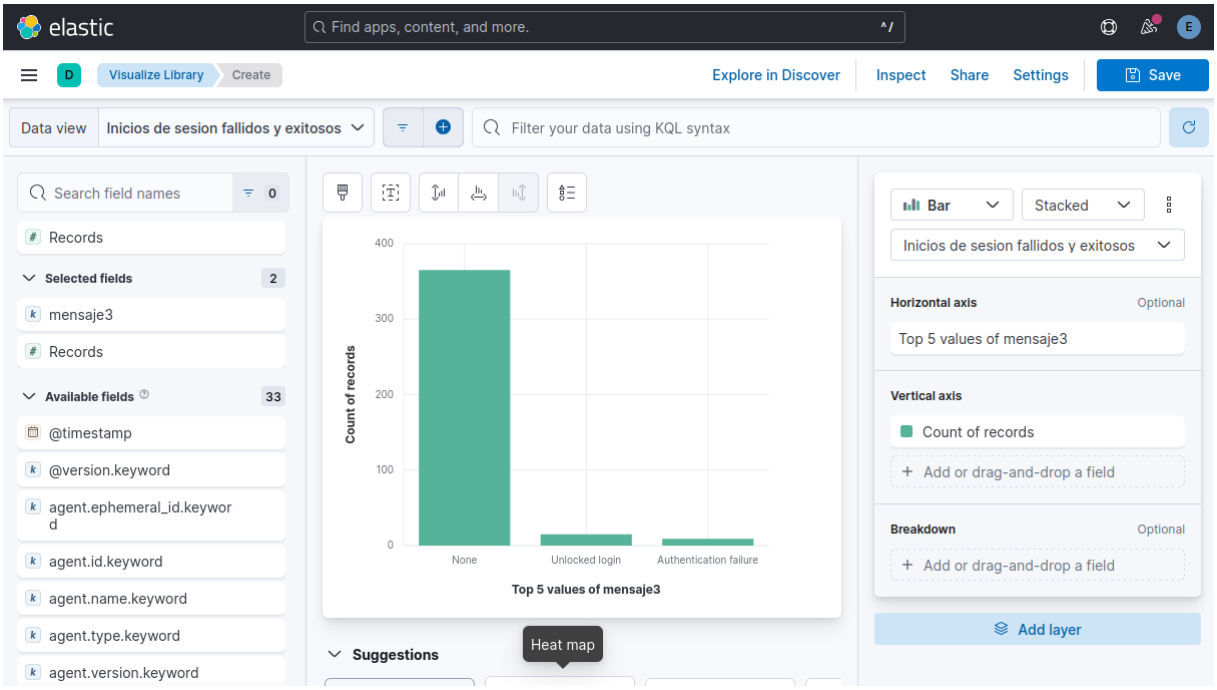

Figura 2.50: visualizar campo nuevo

Pero para que solo nos muestre los inicios de sesion exitosos o fallidos vamos a crear un filtro.

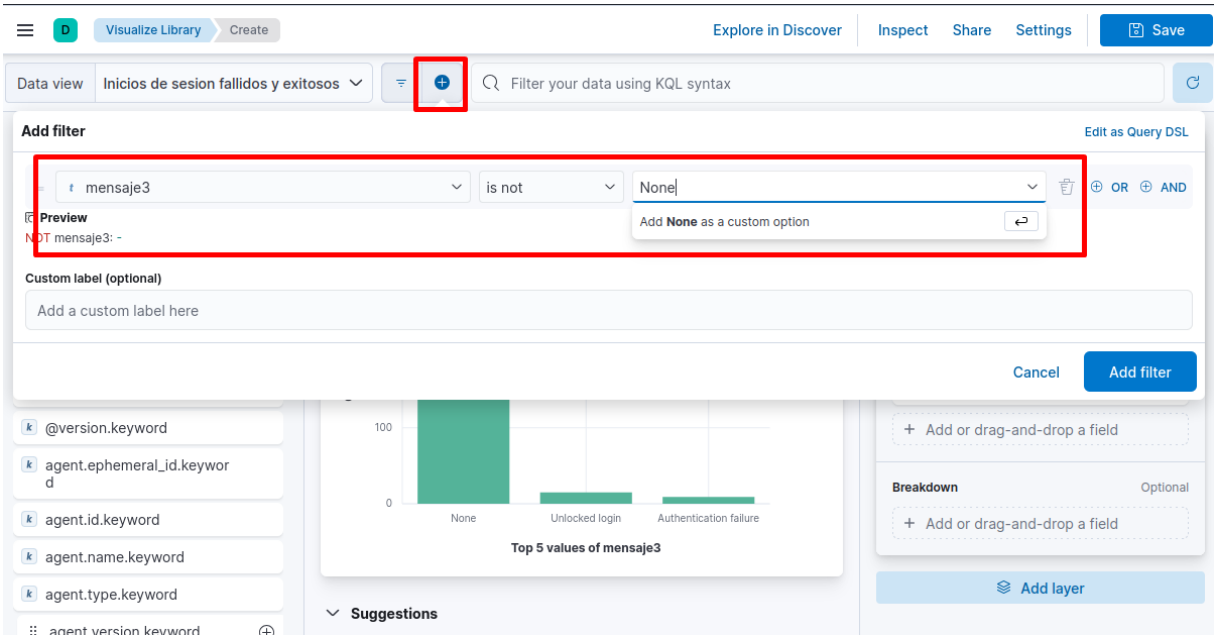

Figura 2.51: visualizar en grafica con filtro

Y una vez aplicado el filtro ya podemos ver la gráfica, más clara.

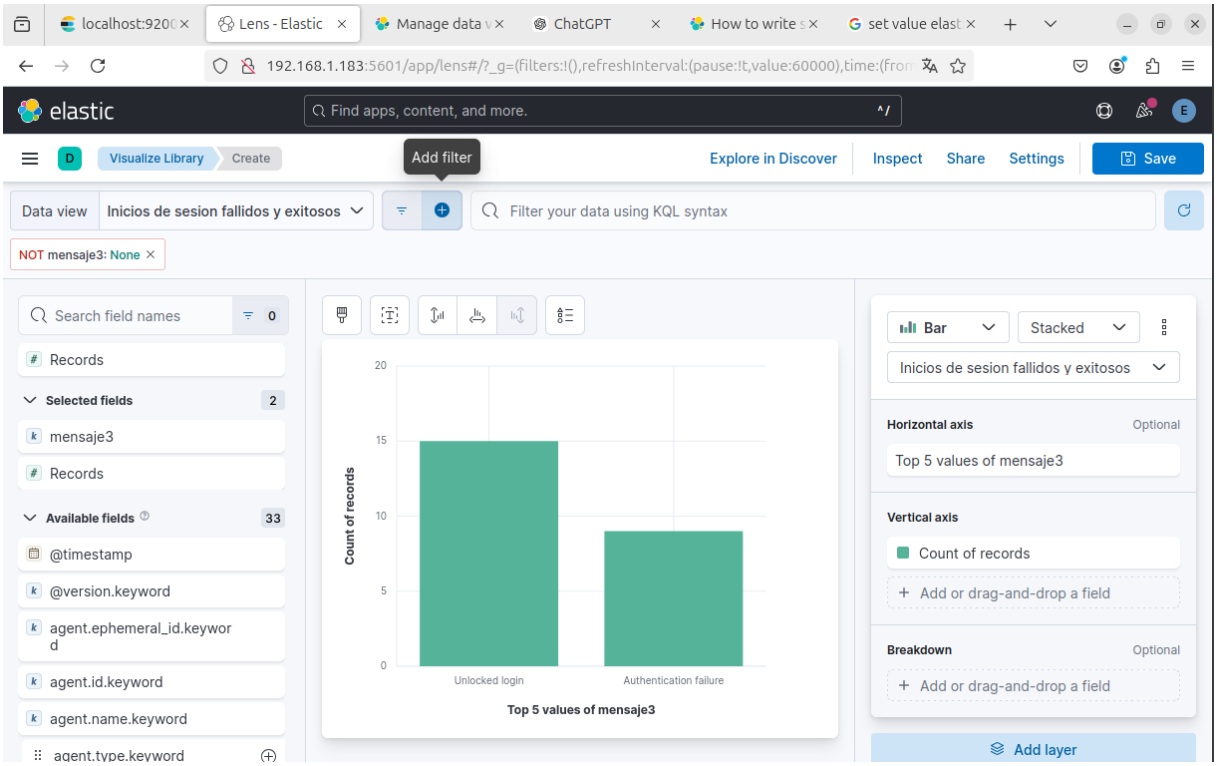

Figura 2.52: visualizar en grafica con filtro

Antes de guardar la gráfica en un dashboard vamos a crear uno.

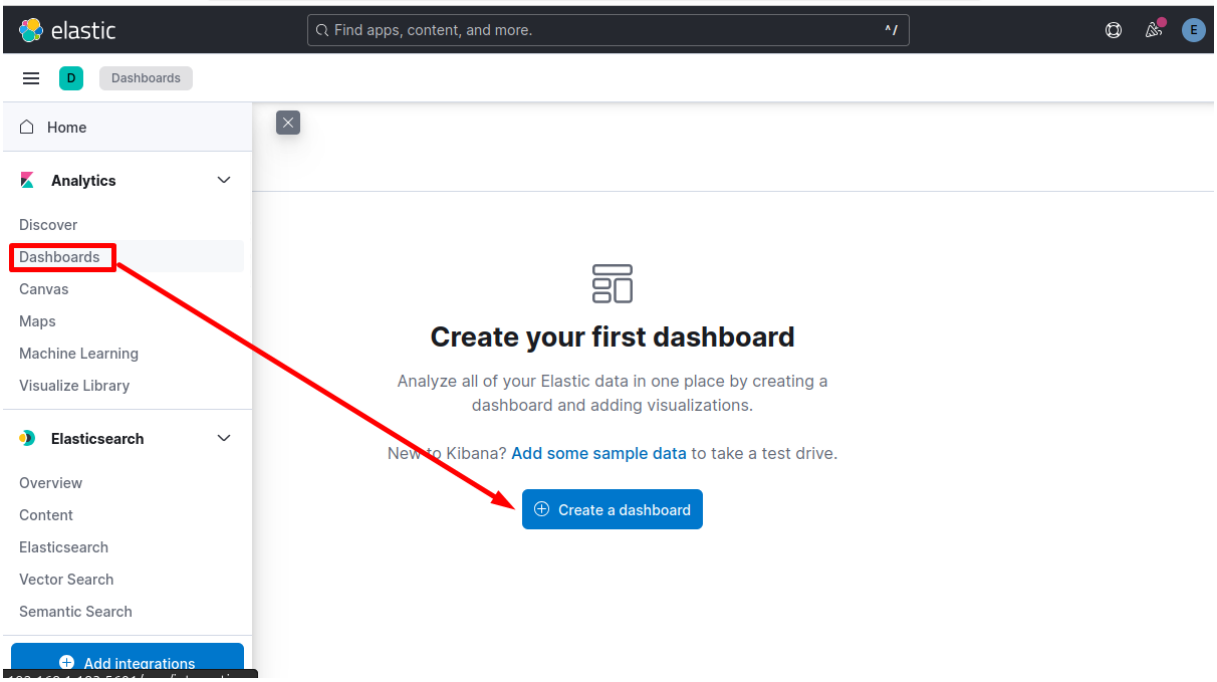

Figura 2.53: Nuevo visualizacion

Y después le daremos a crear nueva visualización.

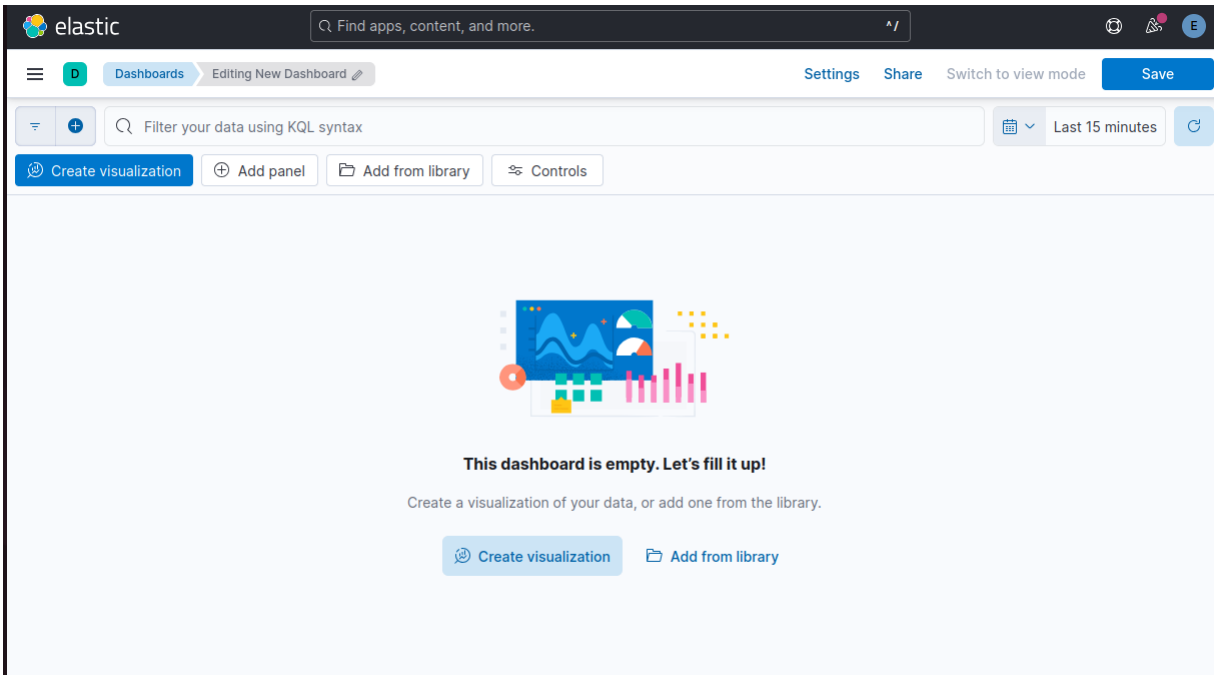

Figura 2.54: Nueva visualizacion dashboard

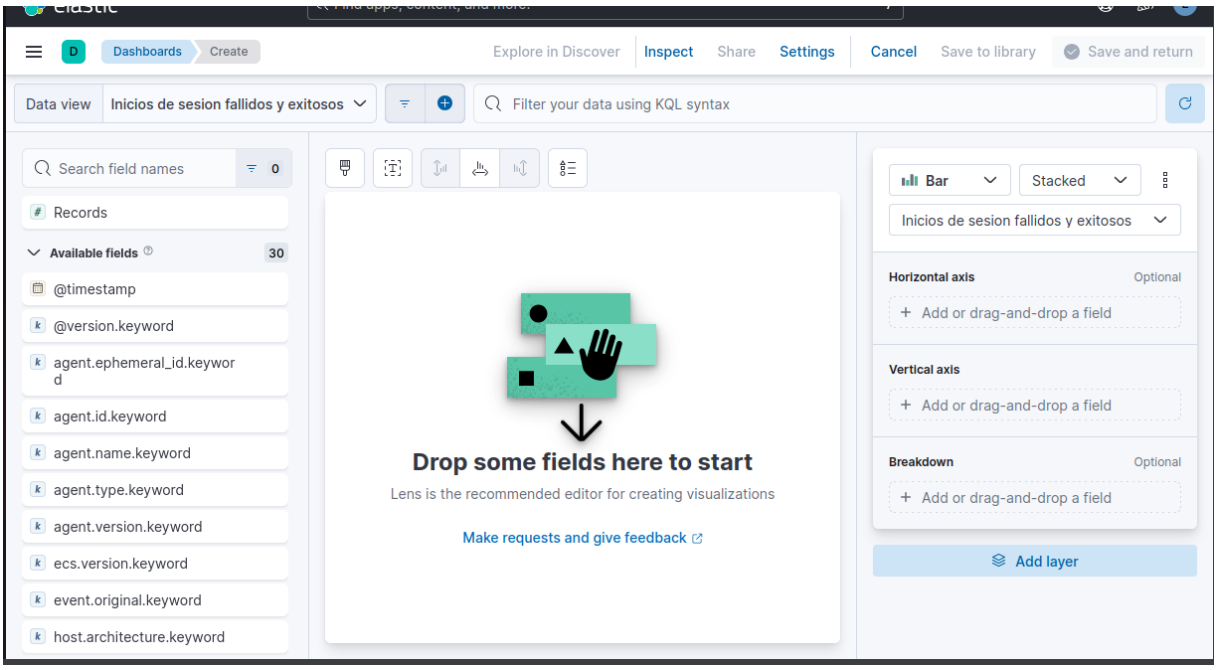

Figura 2.55: Crear visualizacion dashboard

Crearemos la gráfica que hicimos antes 2.52.

Y ahora si le daremos a guardar.

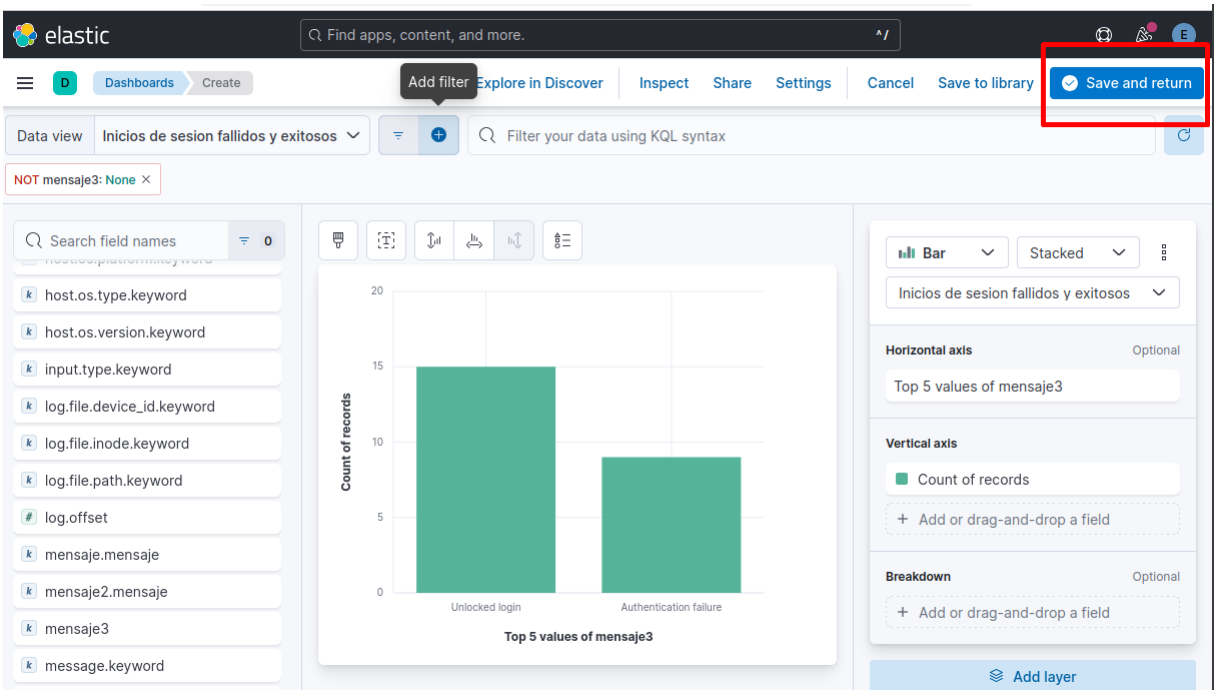

Figura 2.56: Guardar gráfica dashboard

Y ya podriamos visualizar en nuestro dashboard la gráfica de inicios de sesion fallidos y exitosos de la máquina con sistema operativo ubuntu.

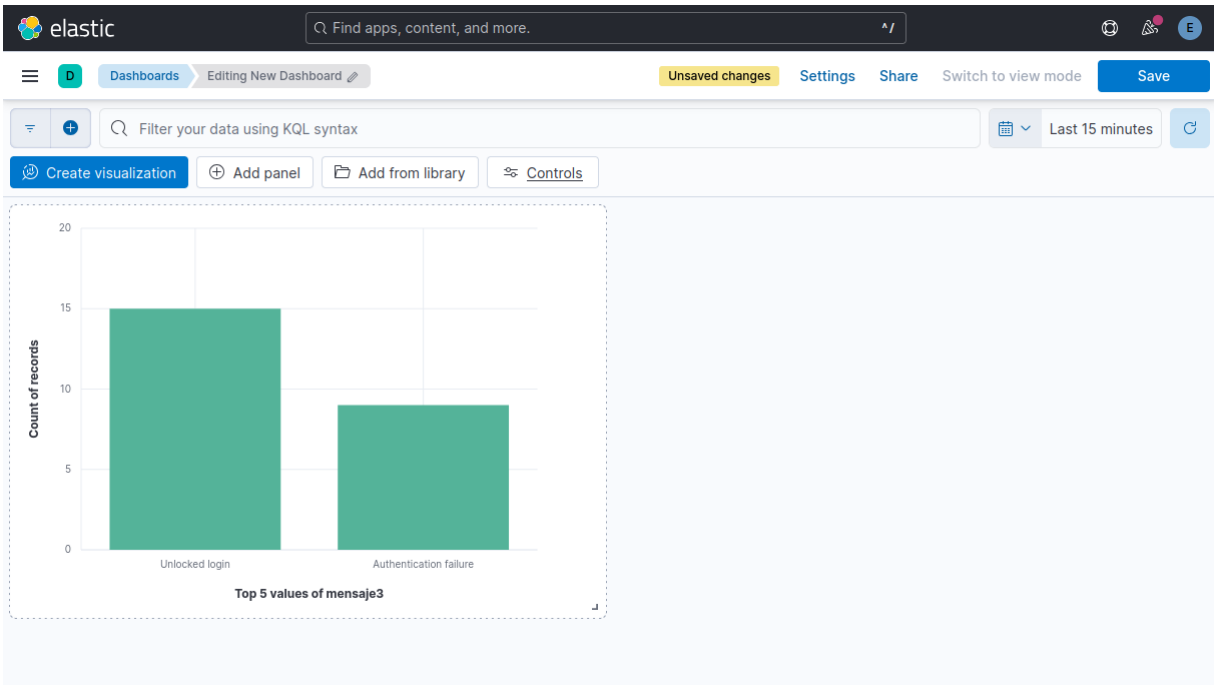

Figura 2.57: Añadida gráfica dashboard

2.7.1. Instalación de Filebeat en windows

Para continuar con la práctica y asi poder visualizar y analizar los logs de inicios de sesión de dos sistemas operativos, vamos a instalar filebeat en una máquina windows.

Para ello vamos a la página de instalación de Filebeat 2.30.

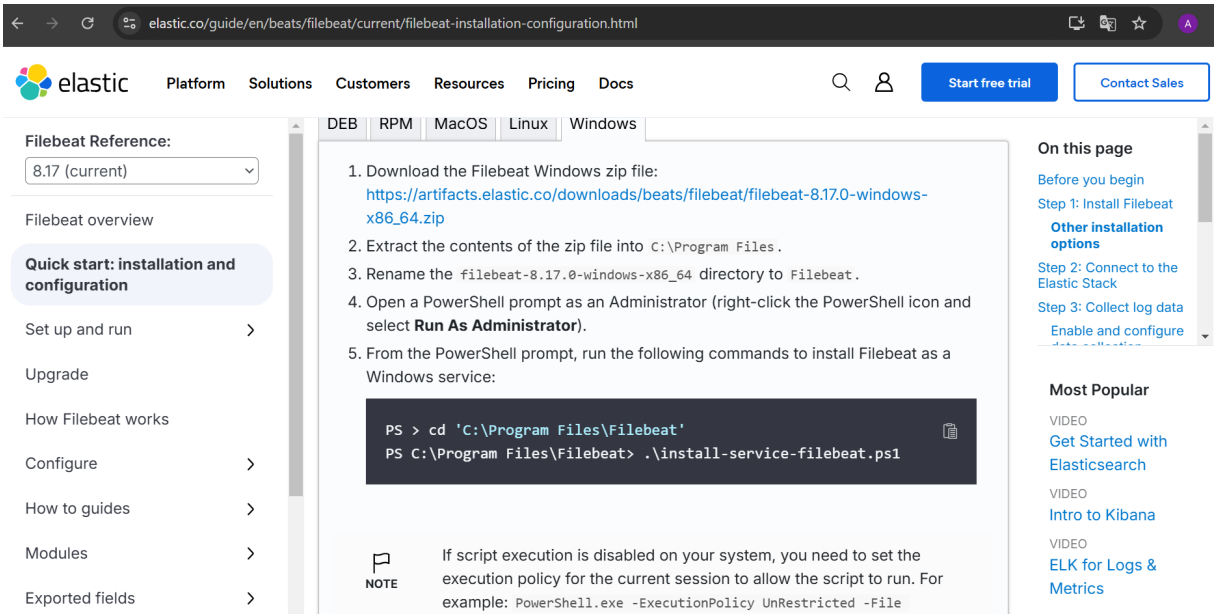

Figura 2.58: Guía instalación Filebeat windows

Nos descargaremos el archivo .zip en nuestra máquina y una vez descargado lo descomprimimos en **D:_Program Files**

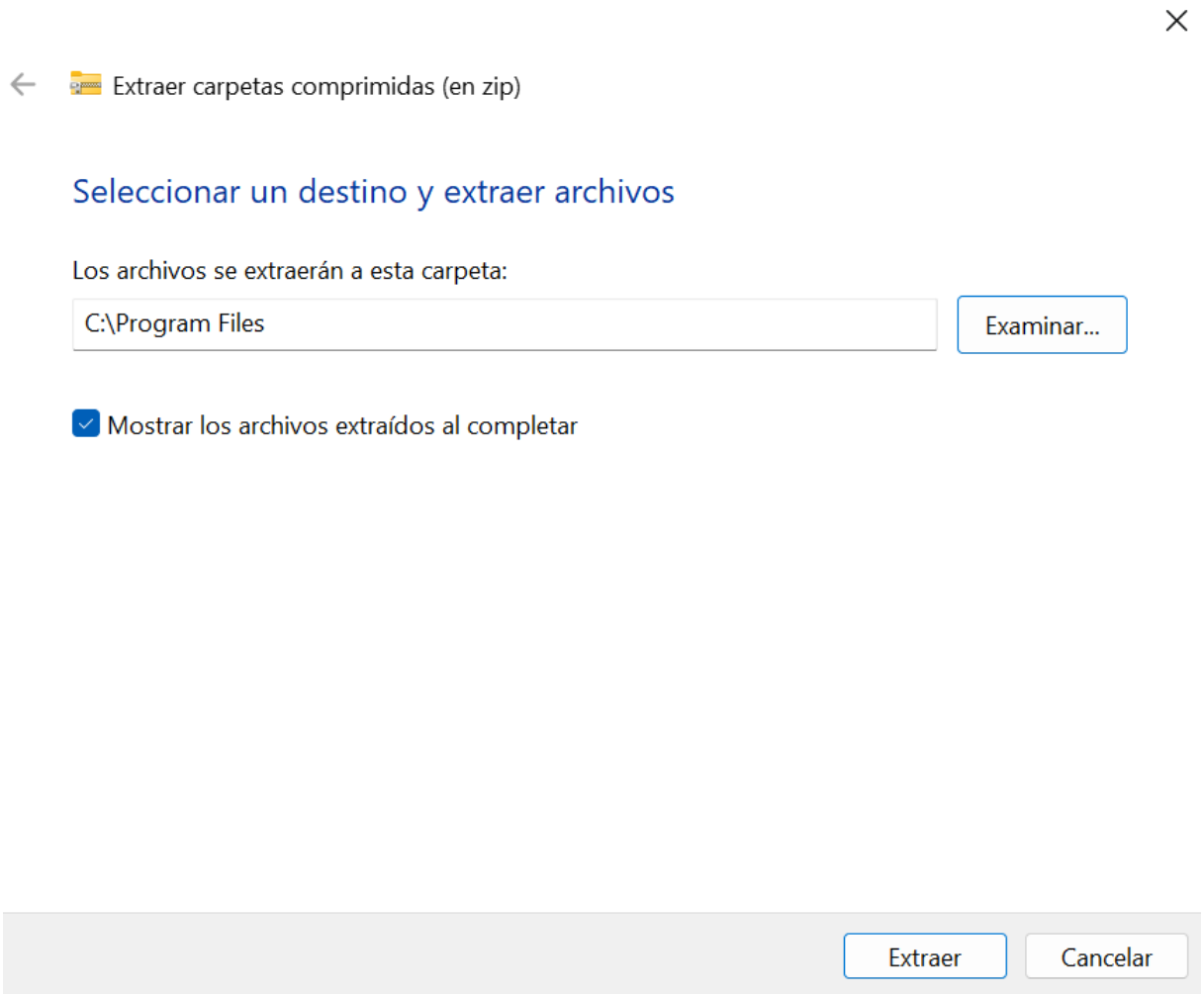

Figura 2.59: Ubicacion de extracción

Una vez extraido vamos a renombrar la carpeta como filebeat. Y abrimos el cmd como administrador.

Y lanzaremos los siguientes comandos:

```
PS > cd 'C:\Program Files\filebeat'
PS C:\Program Files\filebeat> .\install-service-filebeat.ps1
```

Y como nos salta un error ejecutamos

```
PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.ps1
```

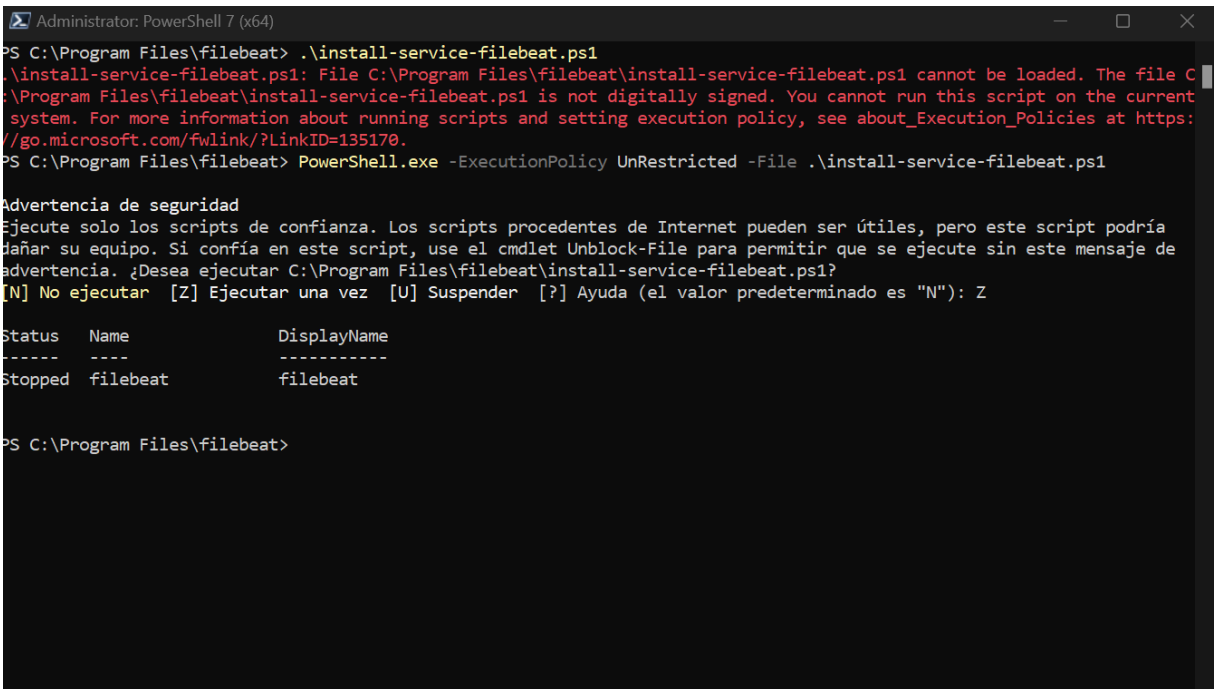

Figura 2.60: Ejecución de comandos

Ahora vamos a editar y modificar el archivo de configuración de filebeat.yml.

```
notepad filebeat.yml
```

Lo primero habilitamos es el envio de logs y especificamos que la ruta de los logs a enviar **C:_Windows_System32_winevt_Logs_Security.evtx**.

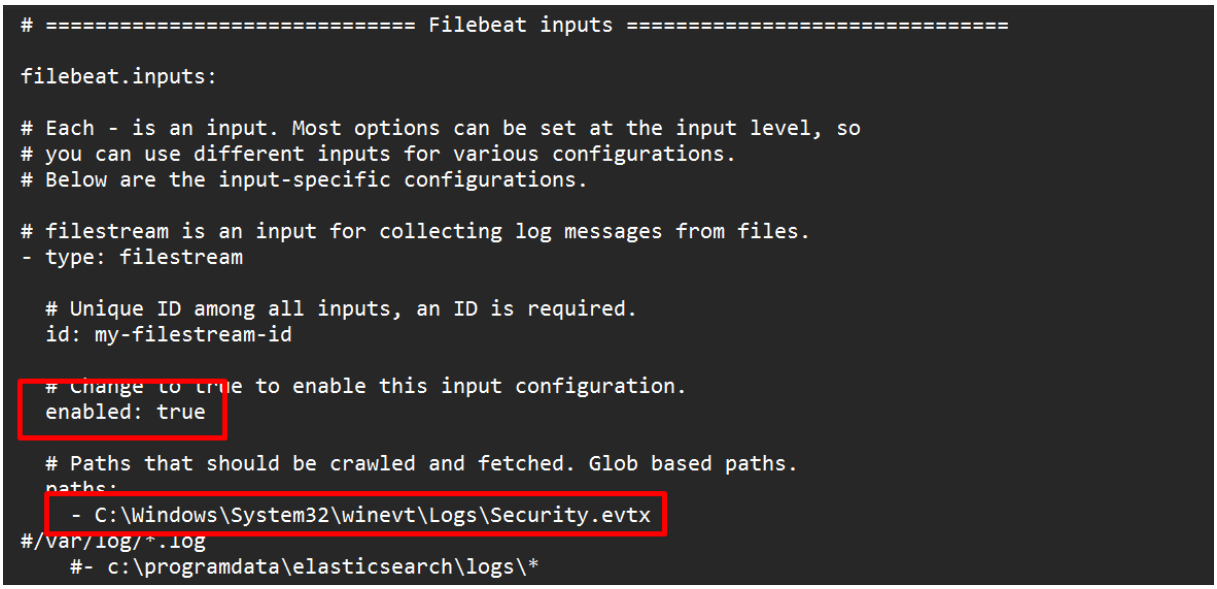

Figura 2.61: Archivo de configuración Filebeat

Después especificaremos donde estará escuchando logstash y comentaremos las líneas referentes a elasticsearch y kibana.

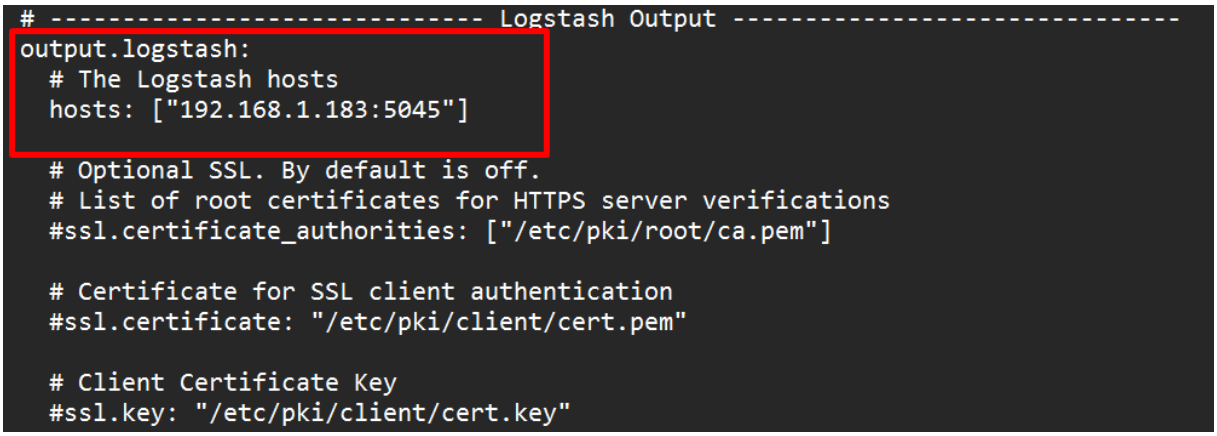

Figura 2.62: Archivo de configuración Filebeat

Una vez guardado el archivo de configuración testeamos que funciona.

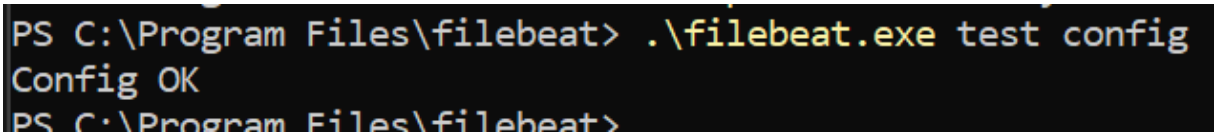

Figura 2.63: Test Archivo de configuración Filebeat

2.8. Configurar Logstash para recibir los logs de windows

Una vez configurado el Filebeat ahora vamos a crear un pipeline en logstash para que este escuchando en el puerto que especificamos anteriormente y lo realizaremos como explicamos anteriormente. 2.62

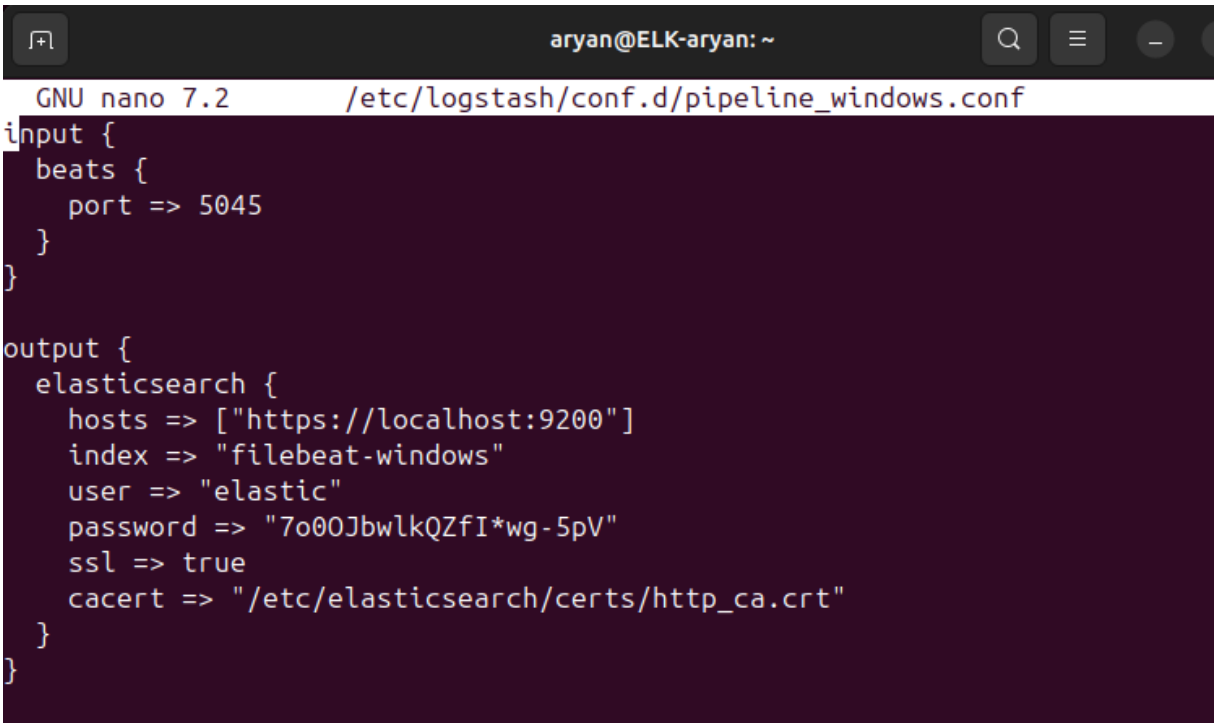

Figura 2.64: Pipeline de logstash para windows

Y reseteamos el servicio de logsatash.

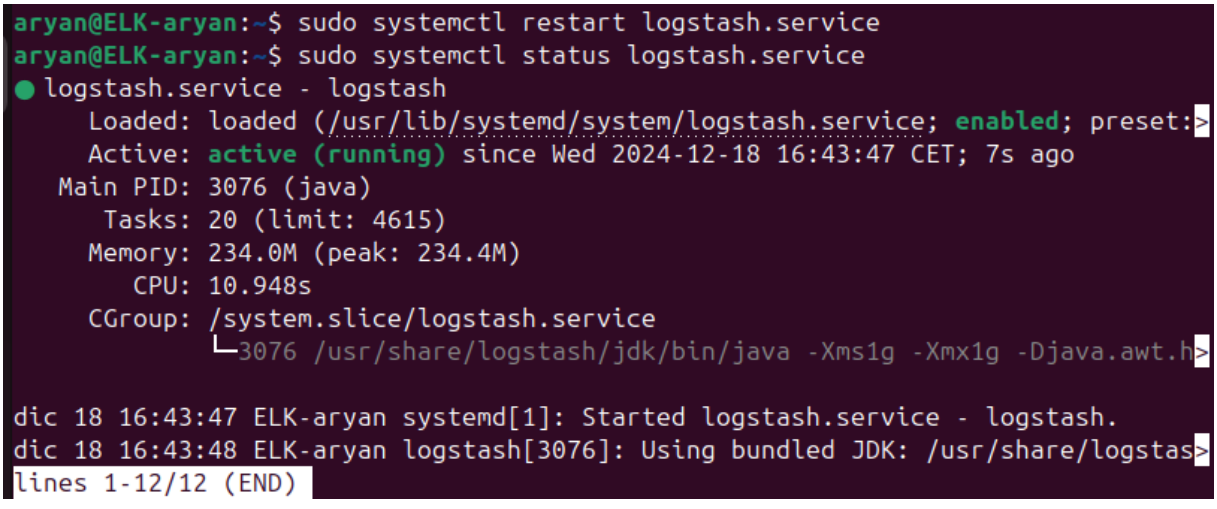

Figura 2.65: reinicio y estado de logstash

Y comprobamos que se comunica nuestro filebeat de windows con el logstash, para eso usamos este comando en nuestra máquina windows.

```
    .\filebeat.exe test output
```

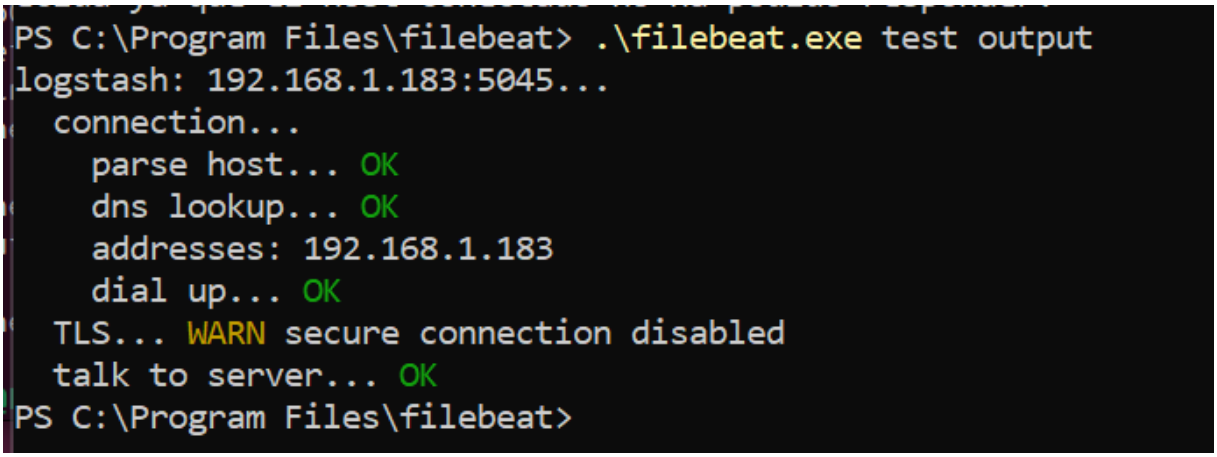

Figura 2.66: Test de conexión entre filebeat y logstash

Una vez comprobado que se envian los datos a logstash, vamos a comprobar que se envie a elasticsearch.

```
    curl -u elastic:7o0OJbwlkQZfI*wg-5pV --cacert
    /etc/elasticsearch/certs/http_ca.crt
    https://localhost:9200/_cat/indices/filebeat-*?v=true
```

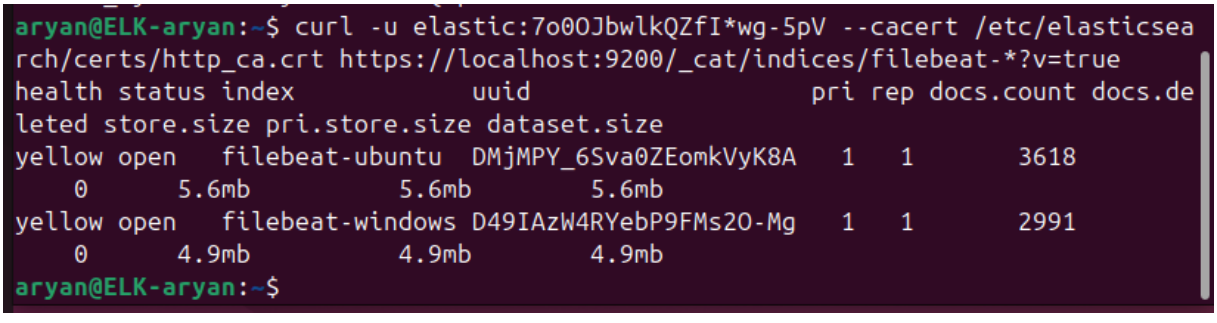

Figura 2.67: Envio de datos a elasticsearch

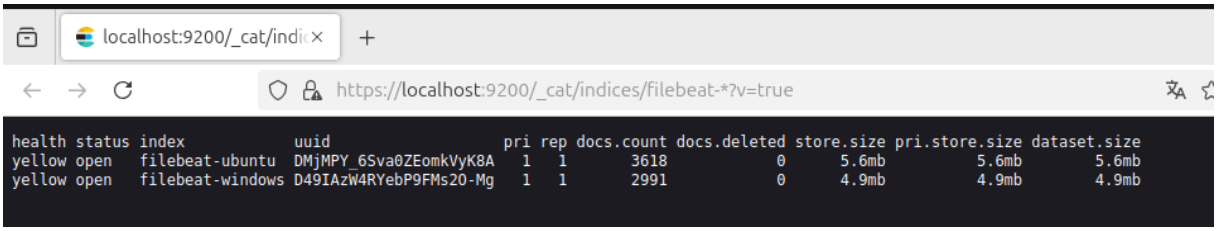

Figura 2.68: Envio de datos a elasticsearch y revisión en el navegador

En estas imagenes podemos ver como la conexión entre Filebeat ->Logstash ->Elasticsearch es correcta. Ya que los datos se han enviado auntomaticamente y los podremos visualizar en Kibana.

2.9. Analizando y visualizando los datos en Kibana

Como hemos explicado anteriormente en 2.7 Vamos a analizar los datos enviados. Para ello vamos a crear un data view como hicimos antes.

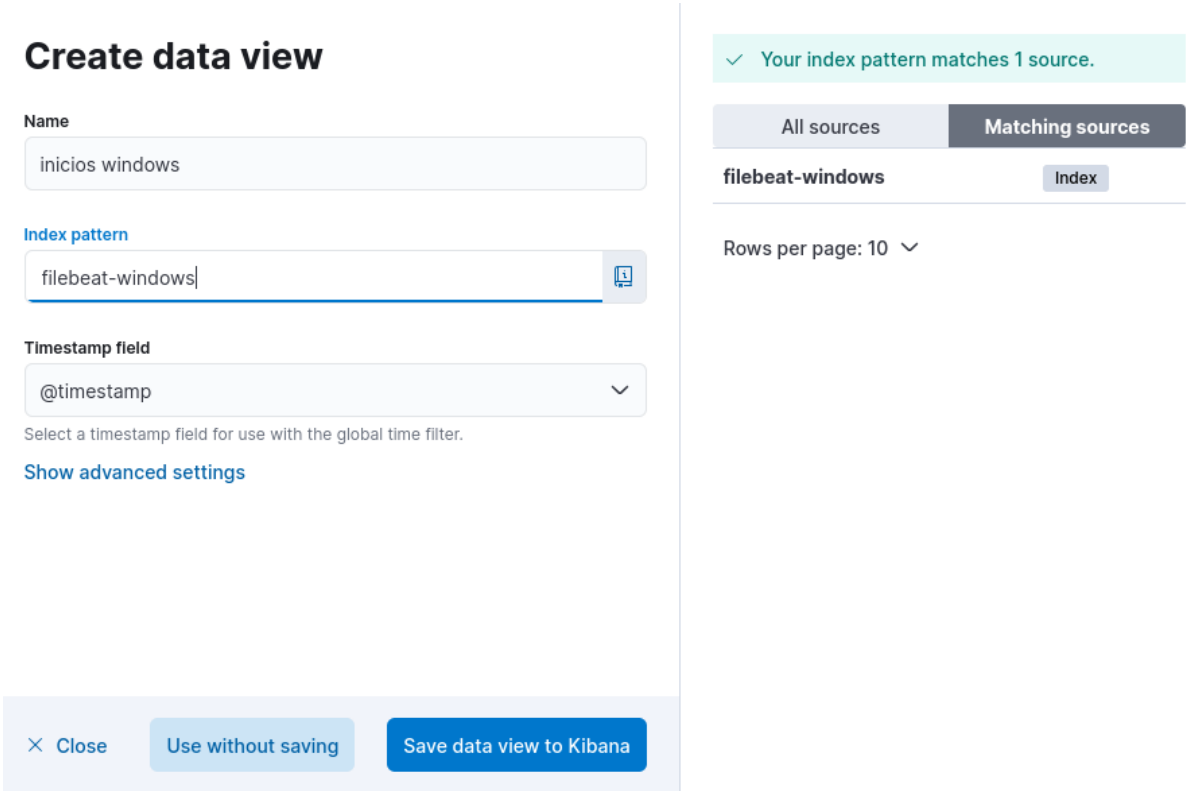

Figura 2.69: Creación de data view de datos de windows

Analizando los datos vemos que nos llegan los datos cifrados

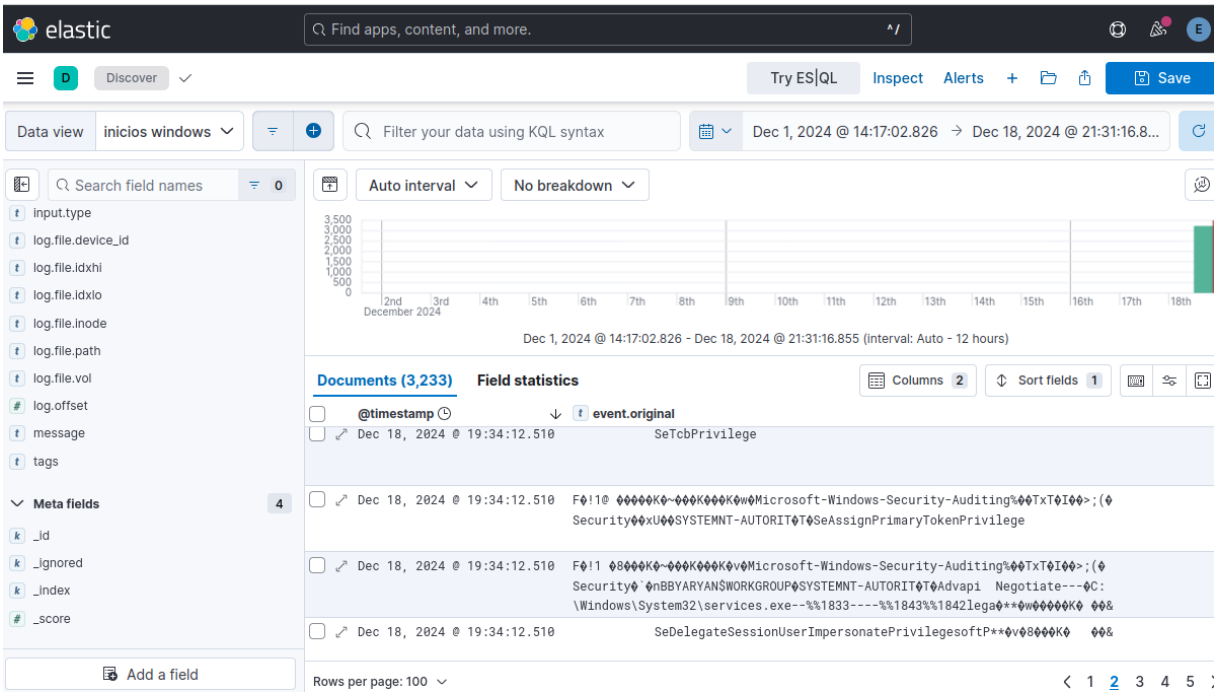

Figura 2.70: Datos cifrados de los eventos

Asi que en vez de usar filebeat vamos a usar, winlogbeat.

2.9.1. Instalación y configuración de Winlogbeat

Para comenzar con la instalación vamos a seguir la guía que nos ofrecen en la pagina oficial de elastic.

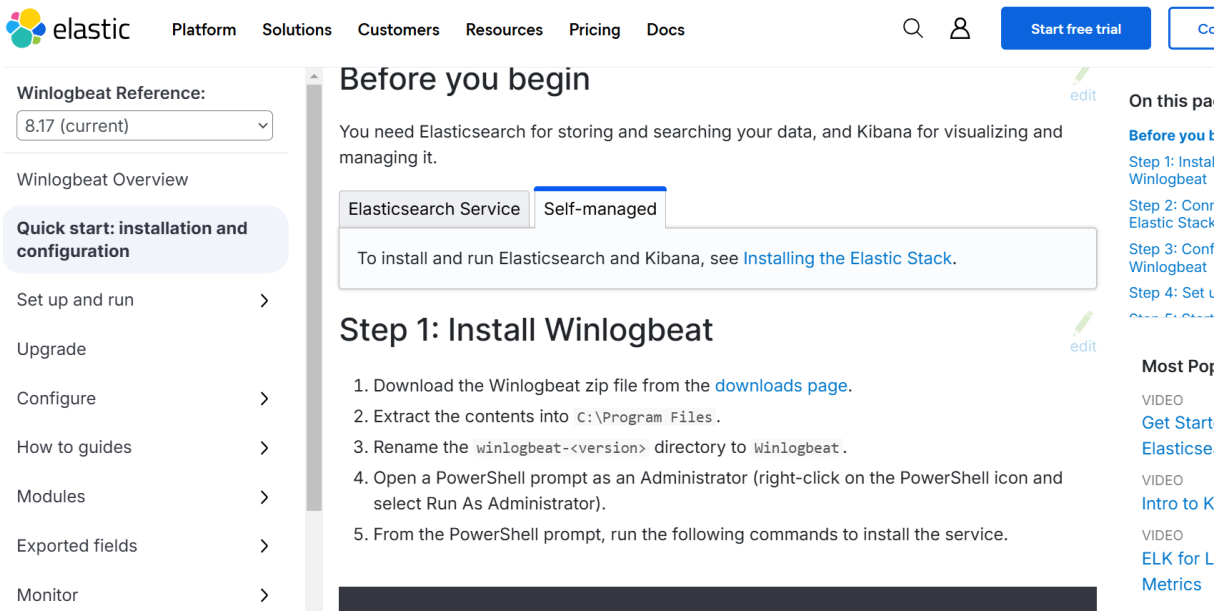

Figura 2.71: Guía Winlogbeat

Descargamos el archivo .zip y descomprimios el archivo .zip. Lo extraemos todo a la ubicación C:_Program Files Y renombramos la carpeta a winlogbeat.

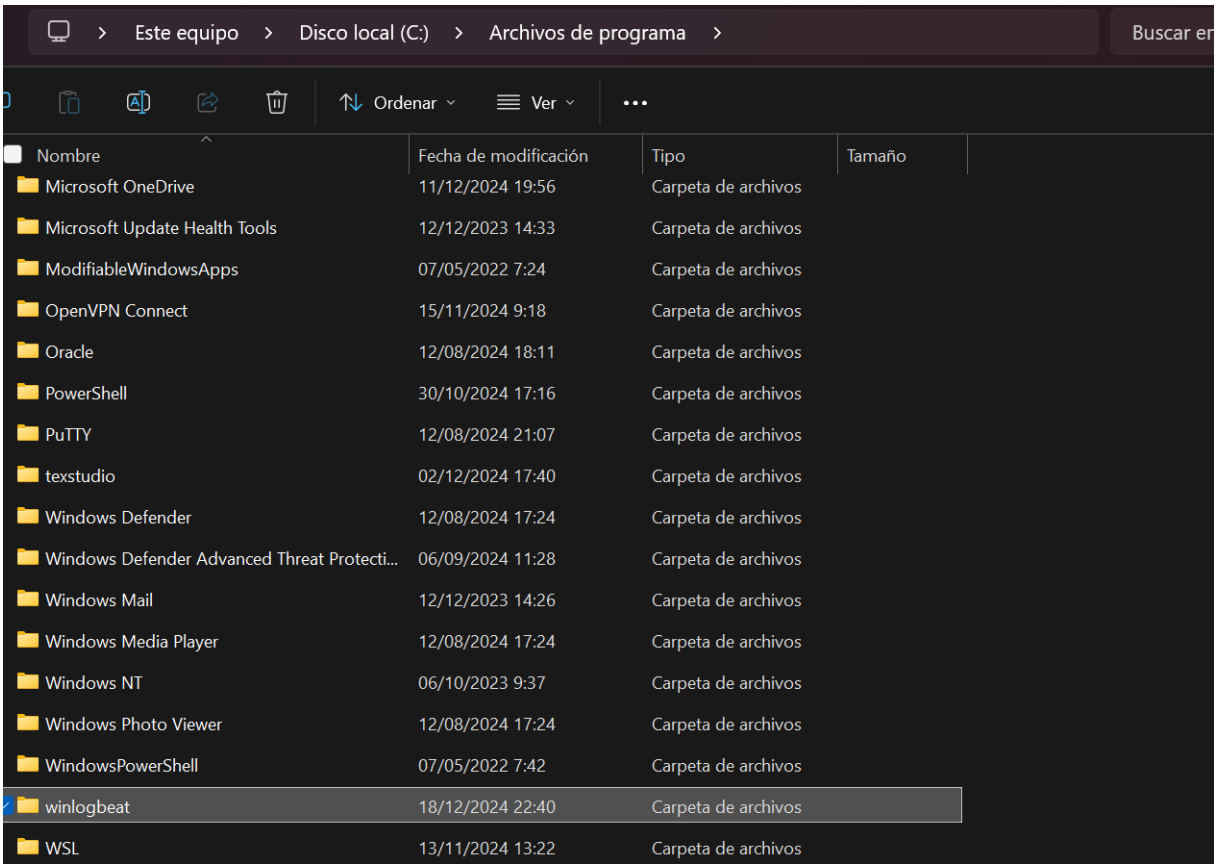

Figura 2.72: Winlogbeat

Utilizamos estos comandos para iniciar el servicio

```
PS > cd 'C:\Program Files\winlogbeat'
PS C:\Program Files\winlogbeat> .\install-service-winlogbeat.ps1
```

Y como nos salta un error ejecutamos

```
PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1
```

```
PS C:\Users\aryan> cd ..
PS C:\Users> cd ..
PS C:\> cd '.\Program Files\winlogbeat\'
PS C:\Program Files\winlogbeat> .\install-service-winlogbeat.ps1
.\install-service-winlogbeat.ps1: File C:\Program Files\winlogbeat\install-service-winlogbeat.ps1 cannot be loaded. The
file C:\Program Files\winlogbeat\install-service-winlogbeat.ps1 is not digitally signed. You cannot run this script on t
he current system. For more information about running scripts and setting execution policy, see about_Execution_Policies
 at https://go.microsoft.com/fwlink/?LinkID=135170.
PS C:\Program Files\winlogbeat> PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-winlogbeat.ps1

Advertencia de seguridad
Ejecute solo los scripts de confianza. Los scripts procedentes de Internet pueden ser útiles, pero este script podría
dañar su equipo. Si confía en este script, use el cmdlet Unblock-File para permitir que se ejecute sin este mensaje de
advertencia. ¿Desea ejecutar C:\Program Files\winlogbeat\install-service-winlogbeat.ps1?
[N] No ejecutar  [Z] Ejecutar una vez  [U] Suspender  [?] Ayuda (el valor predeterminado es "N"): Z

Status   Name               DisplayName
------   ----               -----------
Stopped  winlogbeat         winlogbeat


PS C:\Program Files\winlogbeat>
```

Figura 2.73: Winlogbeat comandos

Ahora editaremos el archivo de configuración de winlogbeat. **winlogbeats.yml**

Y comentaremos las líneas referentes a kibana y elasticsearch y descomentaremos las de logstash. Y lo configuraremos para especificar la IP donde esta escuchando logstash y el puerto.

```
# ------------------------------ Logstash Output -------------------------------
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.1.183:5046"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificate_authorities: ["/etc/pki/root/ca.pem"]

  # Certificate for SSL client authentication
  #ssl.certificate: "/etc/pki/client/cert.pem"

  # Client Certificate Key
  #ssl.key: "/etc/pki/client/cert.key"
```

Figura 2.74: Winlogbeat.yml logstash

Y en esta imagen veremos como se ha configurado los archivos de los logs, el que nos importa es el de Security el resto los comentamos.

```
winlogbeat.event_logs:
#  - name: Application
#    ignore_older: 72h

#  - name: System

  - name: Security

#  - name: Microsoft-Windows-Sysmon/Operational

#  - name: Windows PowerShell
#    event_id: 400, 403, 600, 800

#  - name: Microsoft-Windows-PowerShell/Operational
#    event_id: 4103, 4104, 4105, 4106

#  - name: ForwardedEvents
#    tags: [forwarded]
```

Figura 2.75: Winlogbeat.yml logstash

Ahora crearemos otro pipeline para que este escuchando en el puerto que hemos especificado en el archivo de configuración.

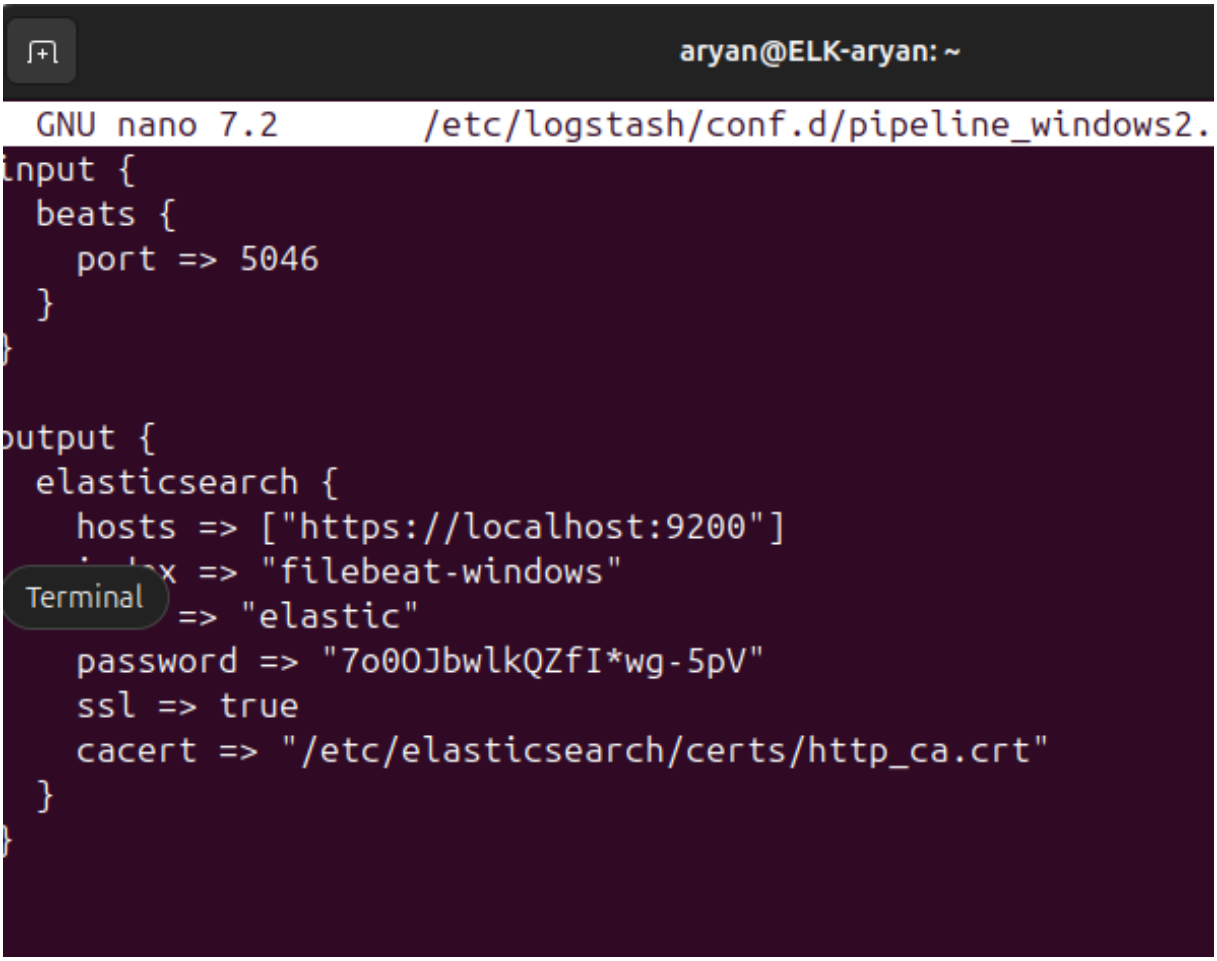

Figura 2.76: Pipeline nuevo

Y reseteamos el servicio como antes.

Ahora vamos a hacer los test para comprobar que nuestro winlogbeat esta bien configurado y que nuestro logstash recibe los datos.

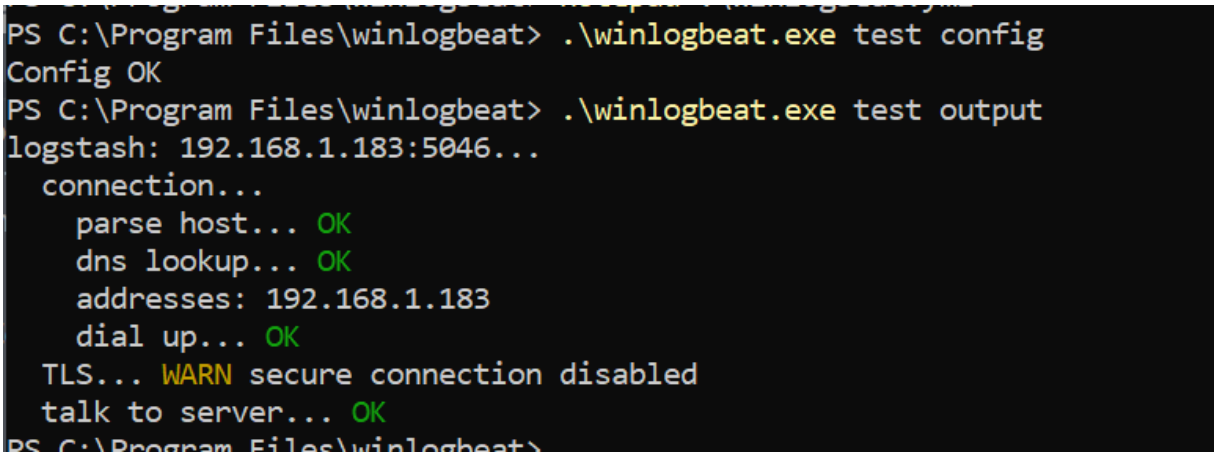

Figura 2.77: Tests

Y comprobaremos que los datos se reciben en elasticsearch.

```
curl -u elastic:7o0OJbwlkQZfI*wg-5pV --cacert
/etc/elasticsearch/certs/http_ca.crt
https://localhost:9200/_cat/indices/filebeat-*?v=true
```

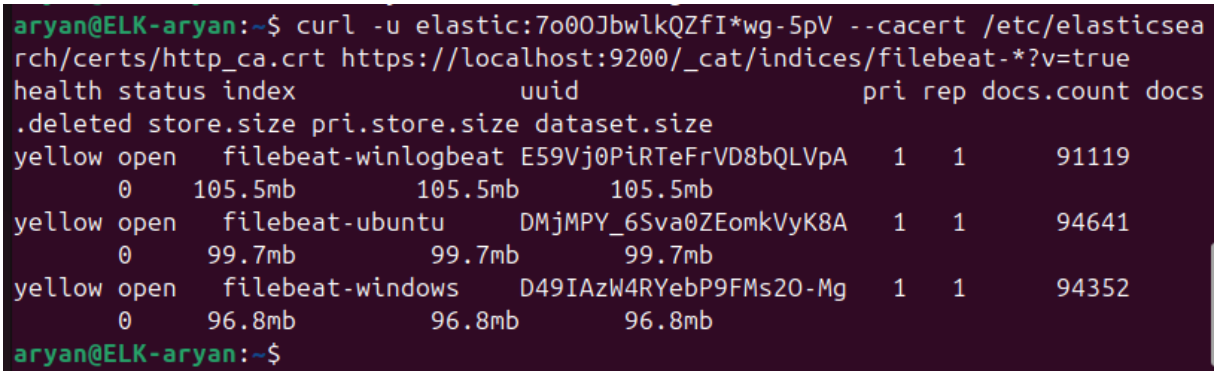

Figura 2.78: datos winlogbeats

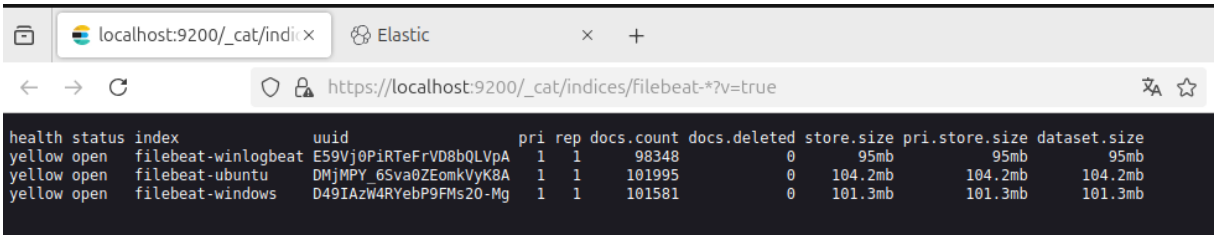

Figura 2.79: datos winlogbeats

Y ya podemos ver el indice nuevo como aparece en elastic search por lo que ahora vamos a visualizarlos.

Creamos un data view como hicimos anteriormente.

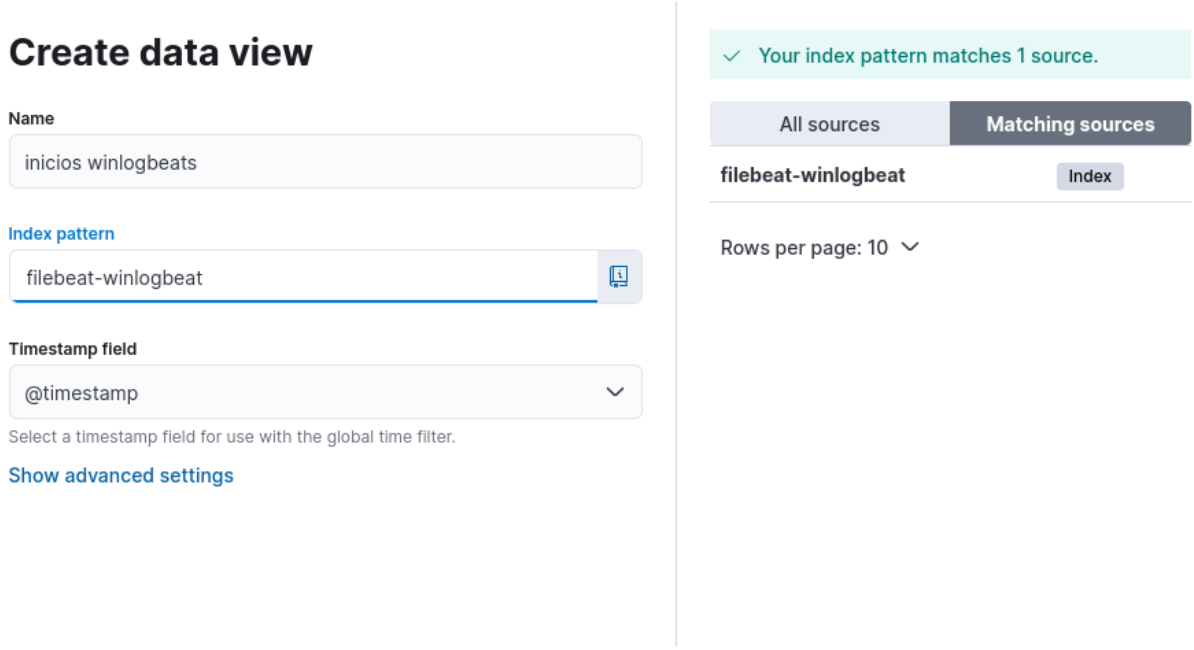

Figura 2.80: Creación data view

Y ya podremos ver los datos (Sale en aleman porque mi ordenador es reacondicionado y fue comprado alli)

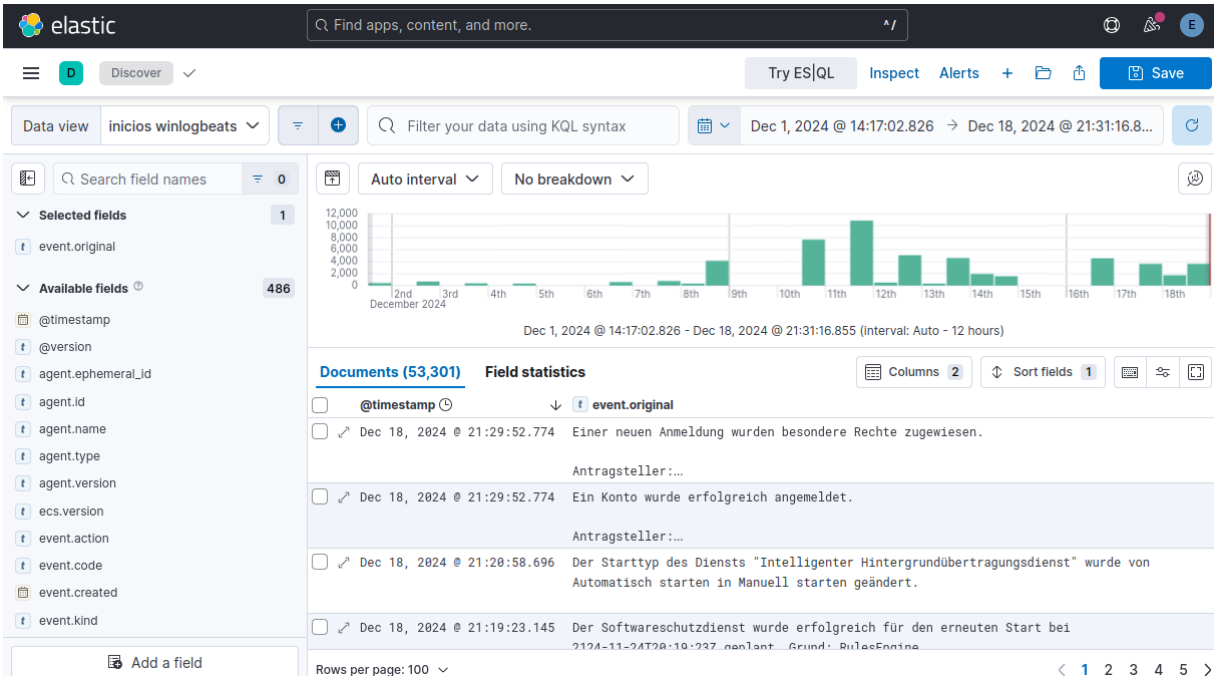

Figura 2.81: Visualización de data

Analizamos los datos y vemos que hay un campo Event.Code asi que vamos a crear un filtro para que nos muestre solo los eventos de inicio de sesión exitosos (4624) y fallidos (4625).

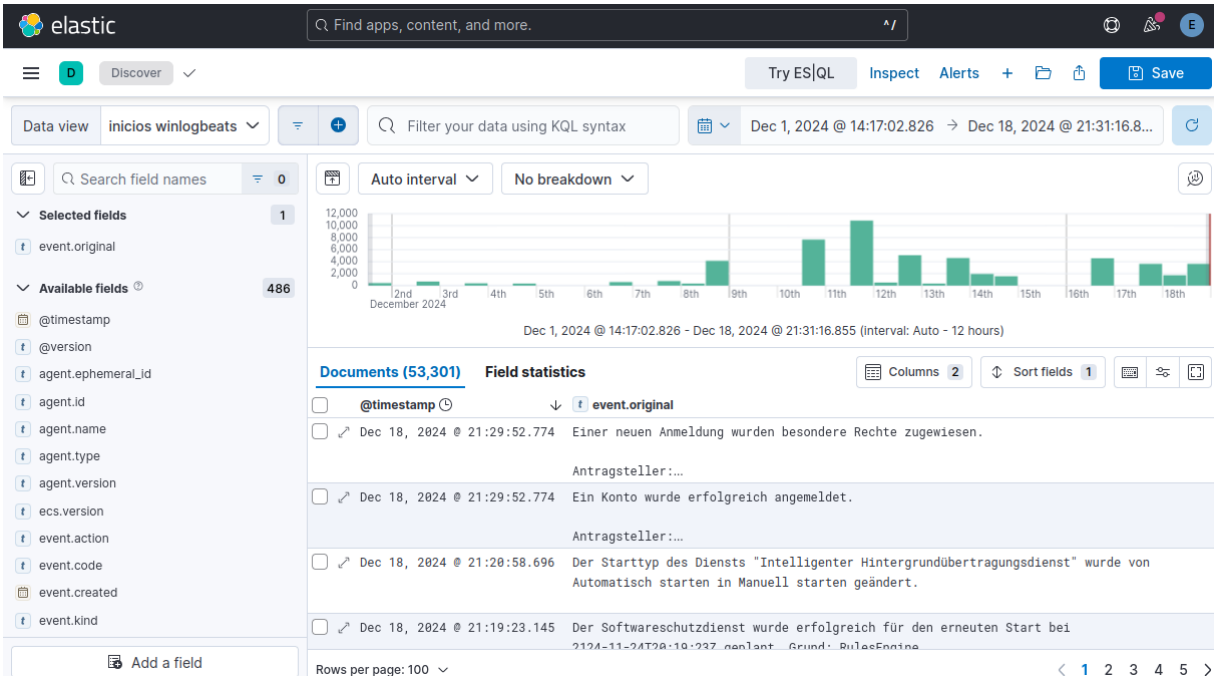

Figura 2.82: Analisis de datos

Para crear el filtro como hicimos anteriormente.

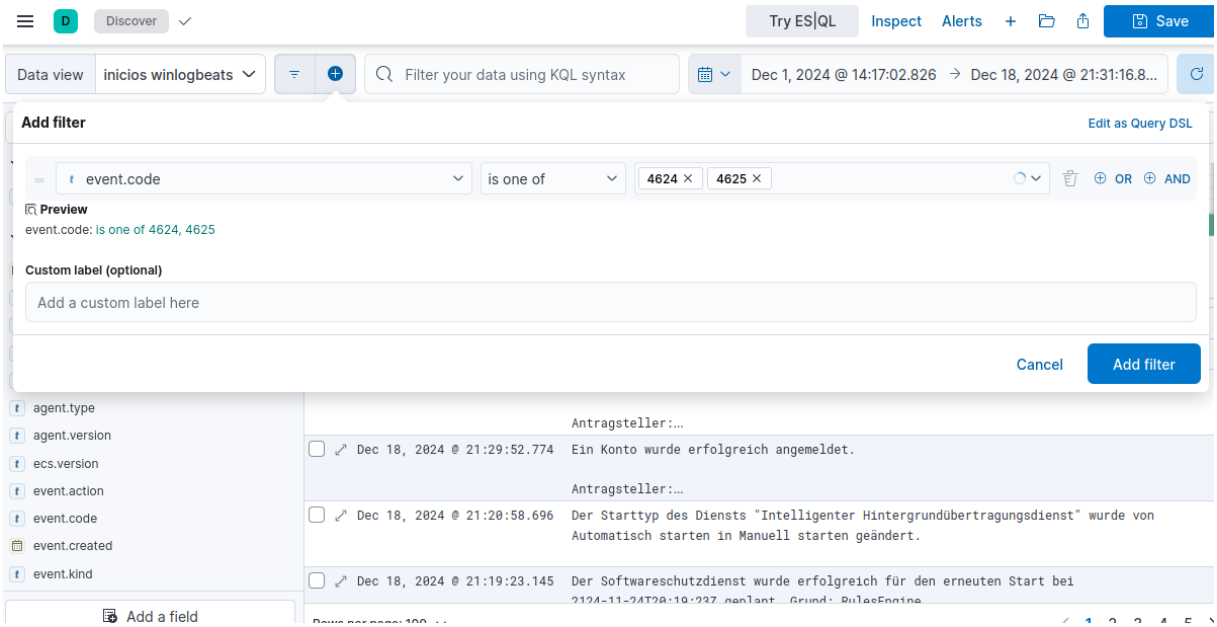

Figura 2.83: Filtro

Y ya solo nos apareceran los eventos que hemos especificado en el filtro.

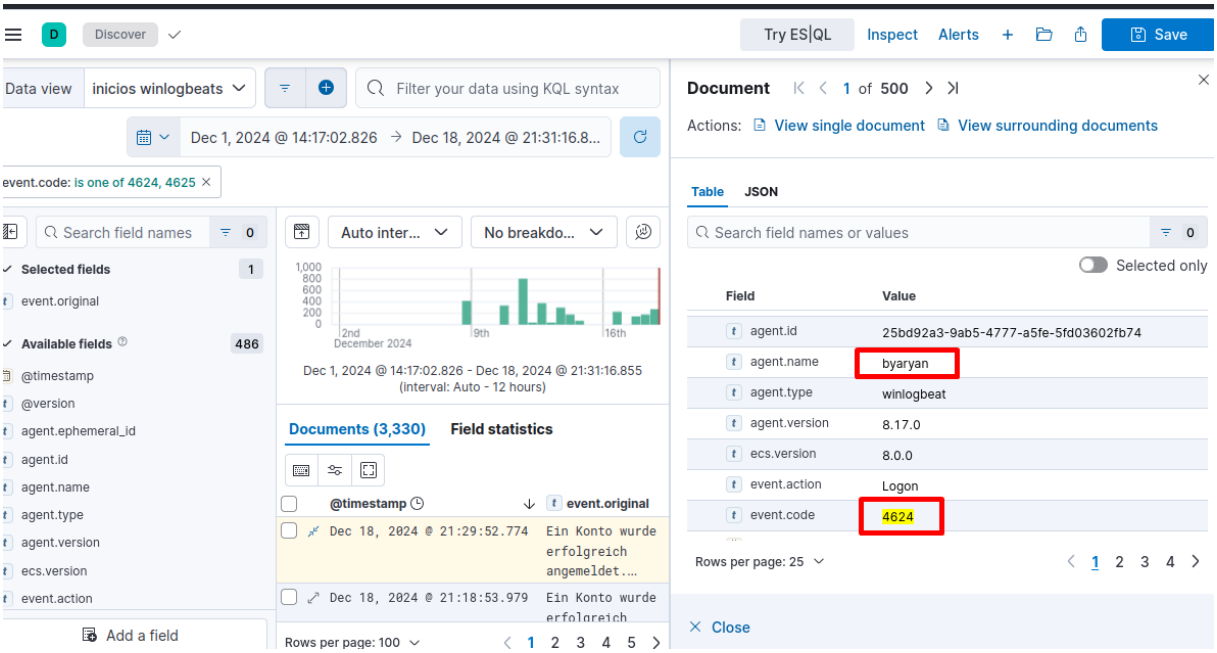

Figura 2.84: Eventos fltrados

Ahora lo guardaremos.

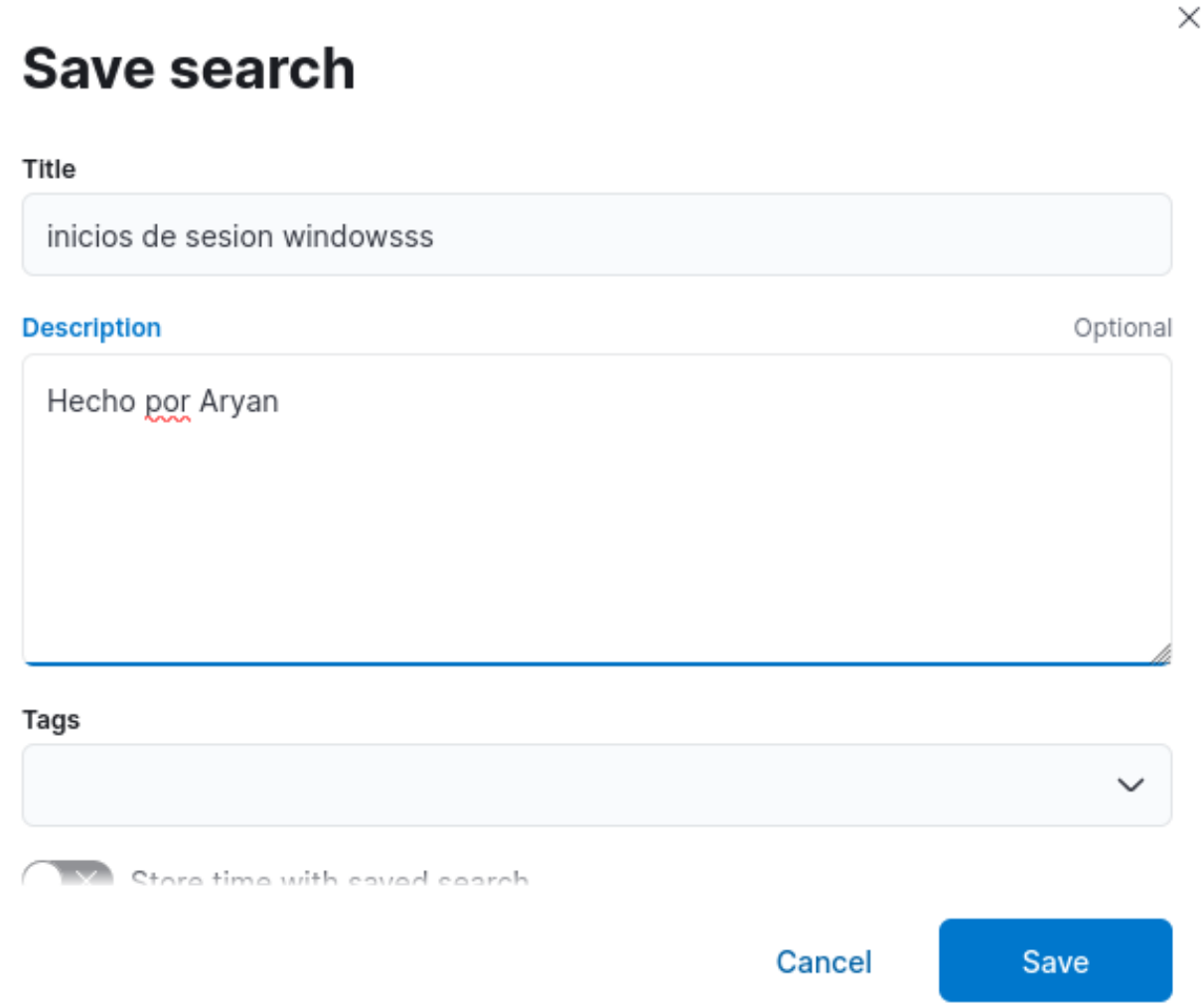

Figura 2.85: Guardar eventos

Vamos a crear un dashboard y asi visualizamos los datos de los últimos 30 días.

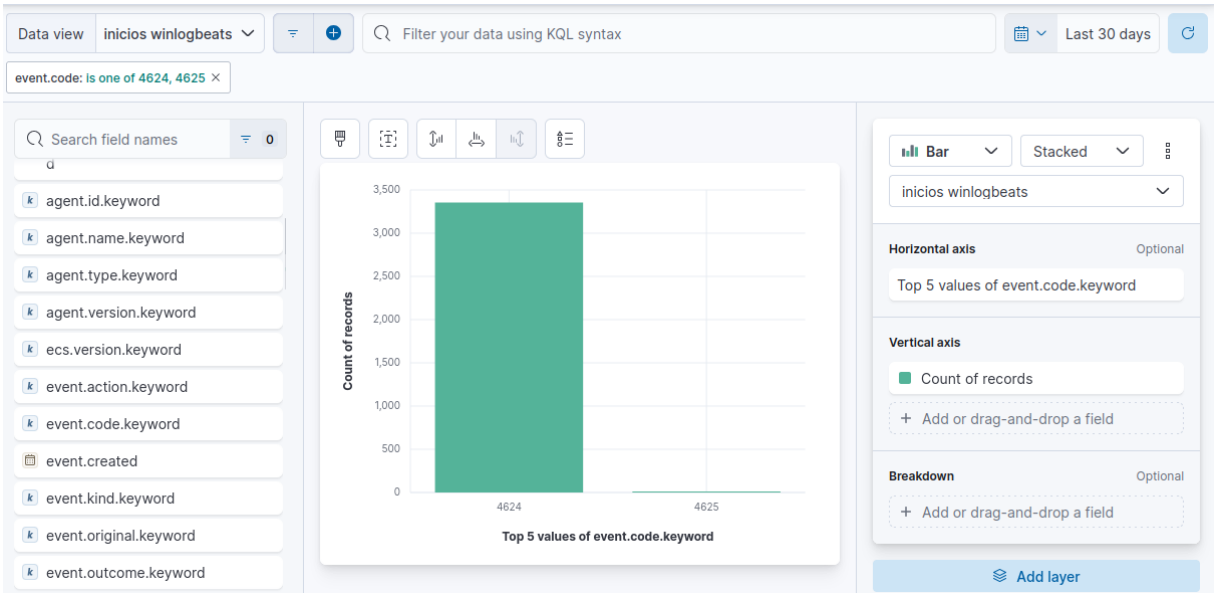

Figura 2.86: Grafica de eventos

Y lo guardamos y automaticamente se nos añade al dashboard.

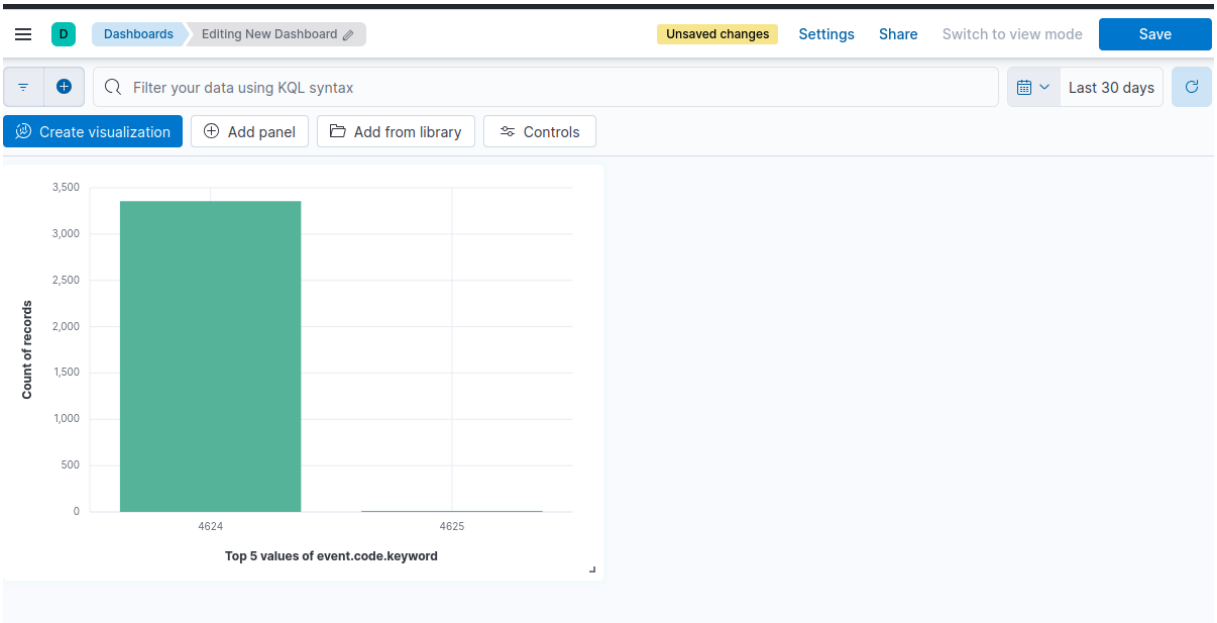

Figura 2.87: Gráfica añadida al dashboard

Ahora vamos a hacer que en el mismo dashboard se muestren las gráficas de ambos sistemas operativos.

Para ello le volvemos a dar a Crear visualizacion y esta vez escogeremos el incide de ubuntu. y lo añadimos al dashboard.

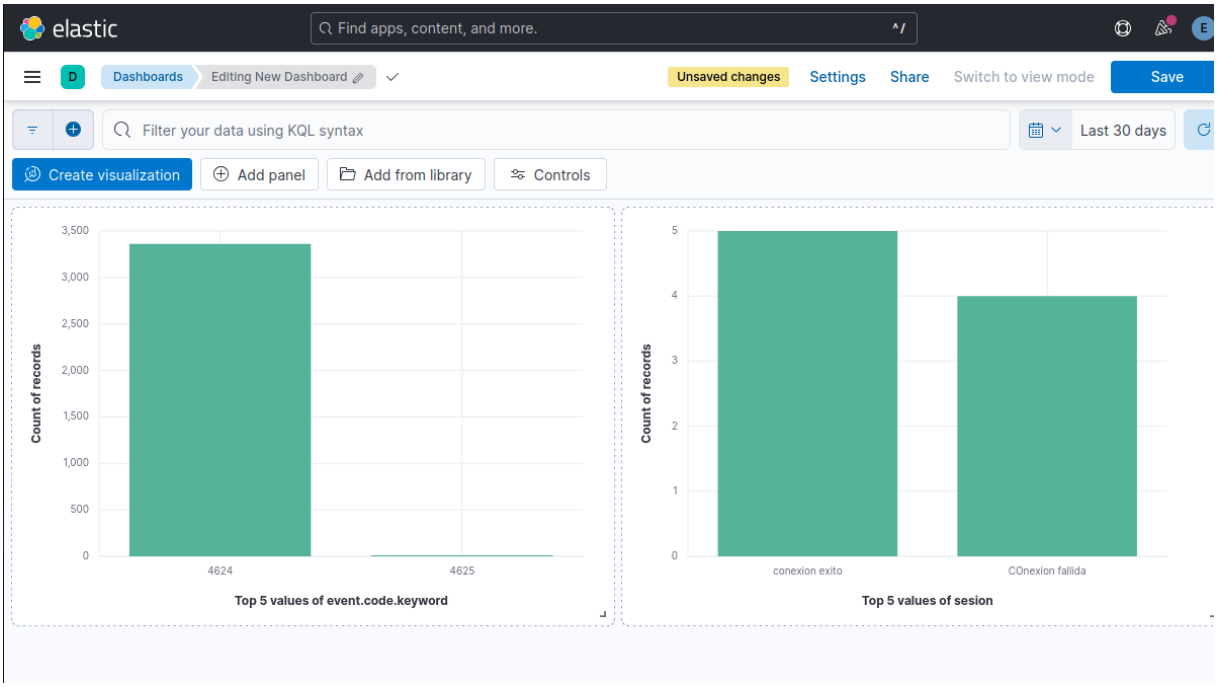

Figura 2.88: Gráficas añadidas al dashboard

La gráfica de la izquierda es la de windows y la de la derecha la de ubuntu.

Capítulo 3

Conclusiones

En esta práctica, hemos comparado el uso de Elasticsearch y Splunk como plataformas para la gestión de información y eventos de seguridad (SIEM). Ambas herramientas tienen puntos fuertes y desafíos únicos, lo que permite apreciar sus capacidades en escenarios específicos.

La elección entre Elasticsearch y Splunk como SIEM depende del caso de uso, presupuesto y necesidades de la organización:

Splunk es ideal para entornos donde la rapidez, facilidad de uso y análisis avanzado son prioritarios, especialmente si el presupuesto no es un limitante. Elasticsearch, en cambio, es una solución más flexible y económica para organizaciones con conocimientos técnicos sólidos, que buscan personalizar su infraestructura y manejar grandes volúmenes de datos. Ambas plataformas son poderosas, pero requieren enfoques distintos para sacarles el máximo provecho. En esta práctica, Elasticsearch destacó por su escalabilidad y costo, mientras que Splunk impresionó por su simplicidad y capacidades nativas de análisis.

Bibliografía

[1] Splunk Community, "How do i configure a splunk forwarder on linux?," 2024.

[2] elastic, "Winlogbeat quick start: installation and configuration," 2024.

[3] elastic, "Repositories for apt and yum," 2024.

[4] elastic, "Install elasticsearch with debian package," 2024.

[5] elastic, "Filebeat quick start: installation and configuration," 2024.