

Universidad de Alcalá Escuela Politécnica Superior

Máster Universitario en
Ciberseguridad



ESCUELA POLITECNICA
Autores:
Aryan Rezaeian Hernández
SUPERIOR

14 de Octubre de 2024



Índice general

1. Configuración de entorno con SIEM	2
1.1. Instalación de Splunk	2
1.2. Primer contacto con Splunk	6
1.3. Configuración inicial de Splunk	8
1.4. Instalación de Splunk Universal Forwarder en Ubuntu	14
1.4.1. Gestión de datos de registro	19
1.4.2. Análisis de eventos	21
1.4.3. Creación de visualizaciones en Splunk	24
1.5. Instalación de Splunk Universal Forwarder en Windows	32
1.5.1. Gestión de datos de registro	42
1.5.2. Análisis de eventos	51
1.5.3. Creación de visualizaciones en Splunk	53
2. Elasticsearch	57
2.1. Instalación y configuración de Elasticsearch	57
2.2. Configuración inicial de Elasticsearch	62
2.3. Instalación y configuración de Kibana	65
2.4. Instalación y configuración de Logstash	76
2.5. Instalación de Filebeat en nuestras máquinas	76
2.5.1. Instalación de Filebeat en ubuntu	76
2.6. Configurar Logstash para recibir los logs	80
2.6.1. Confirmar que los datos llegan	81
2.7. Analizando y visualizando los datos en Kibana	82
2.7.1. Instalación de Filebeat en windows	95
2.8. Configurar Logstash para recibir los logs de windows	99
2.9. Analizando y visualizando los datos en Kibana	101
2.9.1. Instalación y configuración de Winlogbeat	102
3. Conclusiones	115
Bibliografía	116



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](#).

Splunk Enterprise

Download and install Splunk Enterprise trial on your own hardware or cloud instance so you can collect, analyze, visualize and act on all your data — no matter its source. Try indexing up to 500MB/day for 60 days, no credit card required.

[Get My Free Trial](#)[View Product](#)

Figura 1.1: Prueba gratis de splunk enterprise

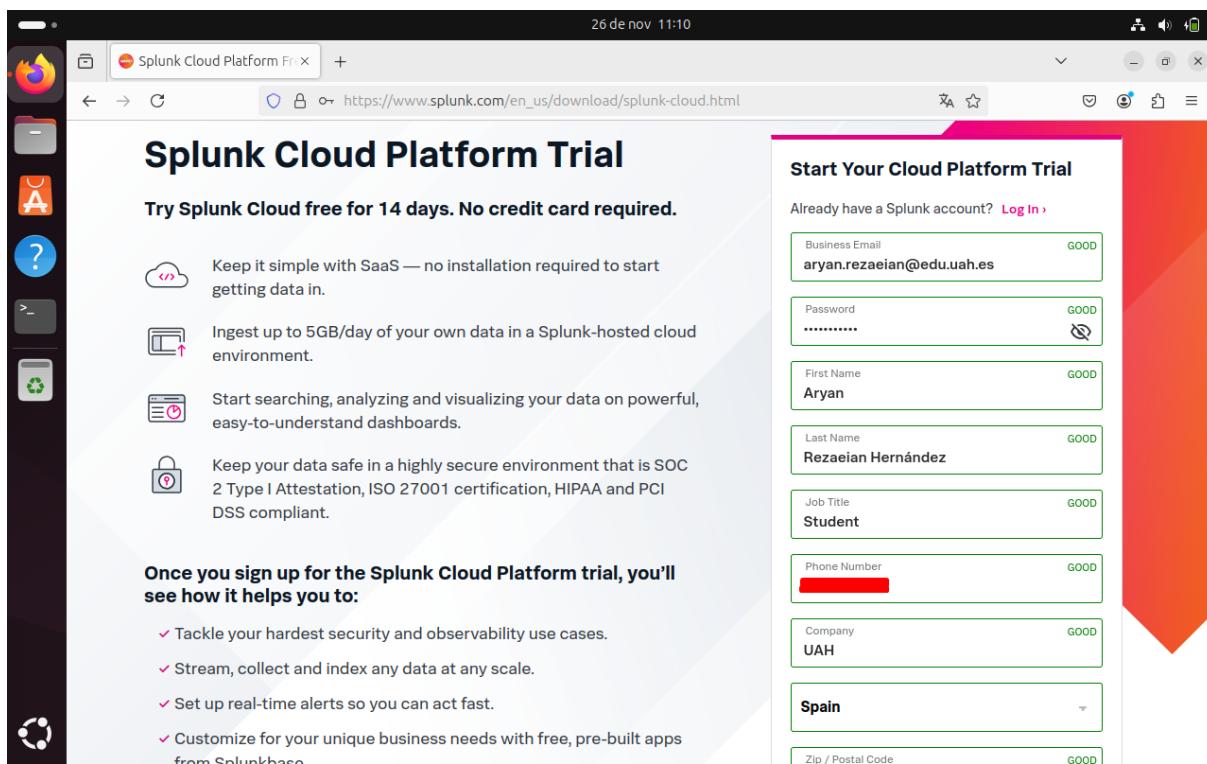


Figura 1.2: Registrarse en splunk

Una vez registrados seleccionamos el producto **Splunk Enterprise** y lo descargamos [1.3.](#)

Splunk Enterprise 9.3.2

Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

Choose Your Installation Package

Platform	Type	File Size	Action	More
Windows				
Linux	4.x+, or 5.4.x kernel Linux distributions	.rpm 947.5 MB tgz 947.75 MB .deb 716.43 MB	Download Now Copy wget link Download Now Copy wget link Download Now Copy wget link	More
Mac OS				

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
```

A screenshot of a terminal window titled "aryan@splunk-aryan: ~/Descargas". The window shows the command "cd Descargas" followed by "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"". The output of the wget command shows the progress of the download, which took 3m 39s at a rate of 8,06MB/s. Finally, the command "tar -xvzf splunk-9.3.2-d8bb32809498-Linux-x86_64.tgz" is run.

Figura 1.4: Descargar y descomprimir splunk

Una vez descargado y descomprimido **Splunk** lo iniciamos [1.5](#).

```
cd ~/Descargas/splunk

sudo ./bin/splunk start
```



```
aryan@splunk-aryan:~/Descargas/splunk$ ls
bin          openssl
copyright.txt opt
etc          quarantined_files
ftr          README-splunk.txt
include      share
lib          splunk-9.3.2-d8bb32809498-linux-2.6-x86_64-manifest
license-eula.txt swidtag
LICENSE.txt

aryan@splunk-aryan:~/Descargas/splunk$ sudo ./bin/splunk start
[sudo] contraseña para aryan:
SPLUNK GENERAL TERMS
```

Last Updated: August 12, 2021

These Splunk General Terms ("General Terms") between Splunk Inc., a Delaware corporation, with its principal place of business at 270 Brannan Street, San Francisco, California 94107, U.S.A ("Splunk" or "we" or "us" or "our") and you ("Customer" or "you" or "your") apply to the purchase of licenses and subscriptions for Splunk's Offerings. By clicking on the appropriate button,

Figura 1.5: Iniciamos Splunk

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



```
aryan@splunk-aryan:~/Descargas/splunk
.....+++++
.....+++++
writing new private key to 'privKeySecure.pem'
-----
Signature ok
subject=/CN=splunk-aryan/O=SplunkUser
Getting CA Private Key
writing RSA key
PYTHONHTTPSVERIFY is set to 0 in splunk-launch.conf disabling certificate validation for the httplib and urllib libraries shipped with the embedded Python interpreter; must be set to "1" for increased security
Done

Waiting for web server at http://127.0.0.1:8000 to be available.....
..... Done

If you get stuck, we're here to help.
Look for answers here: http://docs.splunk.com

The Splunk web interface is at http://splunk-aryan:8000
aryan@splunk-aryan:~/Descargas/splunk$
```

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](#).

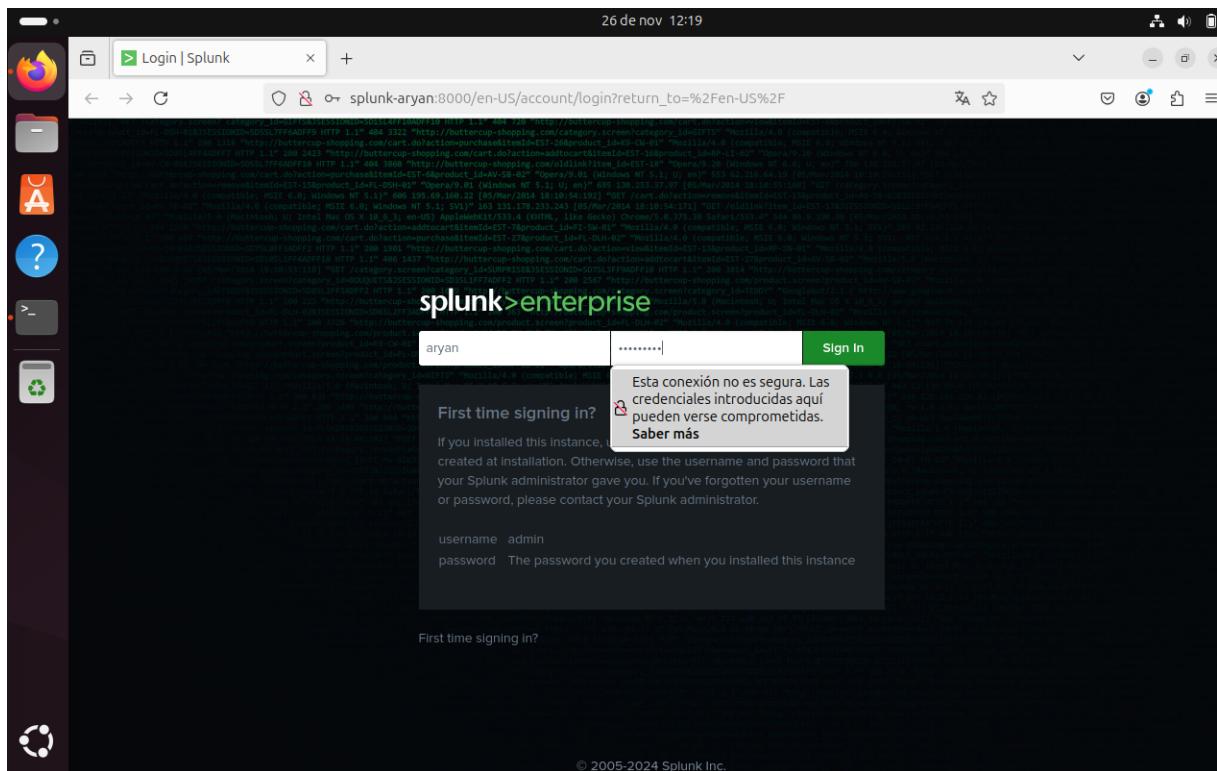


Figura 1.7: Log in Splunk

Introducimos las credenciales que configuramos en la iniciación de **splunk** y accedemos [1.8](#).



The screenshot shows the Splunk Enterprise interface. At the top, there's a header bar with the Splunk logo, a search bar, and various navigation links like 'Messages', 'Settings', 'Activity', 'Help', and 'Find'. Below the header is a sidebar titled 'splunk>enterprise Apps' with a search bar and a list of available apps: 'Search & Reporting', 'Splunk Secure Gateway', and 'Upgrade Readiness App'. There's also a link to 'Find more apps'. The main content area is titled 'Hello, Administrator' and contains sections for 'Bookmarks', 'Dashboard', 'Search history', and 'Recently viewed'. Under 'Bookmarks', there are sections for 'My bookmarks (0)', 'Shared with my organization (0)', and 'Splunk recommended (14)'. The 'Splunk recommended' section includes cards for 'Add data' (which says 'Add data from a variety of common sources.') and 'Search your data' (which says 'Turn data into doing with Splunk search.'). At the bottom left of the sidebar is a button labeled 'Mostrar aplicaciones'.

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.

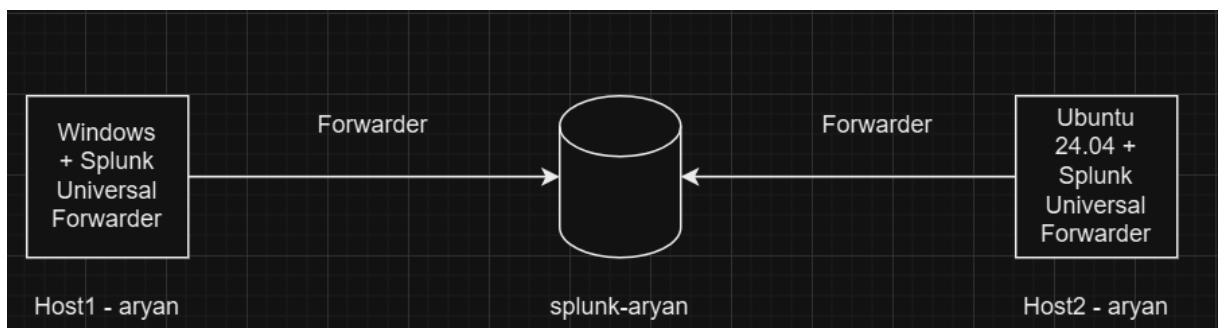


Figura 1.9: Arquitectura

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.



The screenshot shows the Splunk Enterprise home interface. On the left, there's a sidebar with 'Apps' management, search & reporting, secure gateway, and upgrade readiness options. The main area displays 'Hello, Administrator' and sections for 'Bookmarks' (with 'Add Data' highlighted), 'Shared with my organization', and 'Splunk recommended' tasks. On the right, a large navigation menu is open under 'Settings'. The 'DATA' section is expanded, showing 'Forwarding and receiving' (which is also highlighted with a red box). Other visible categories include 'Knowledge', 'Explore Data', 'Monitoring Console', 'System', and 'Distributed Environment'.

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](#)



Screenshot of the Splunk web interface showing the 'Forwarding and receiving' configuration page.

Forward data
Set up forwarding between two or more Splunk instances.

Type	Actions
Forwarding defaults	
Configure forwarding	+ Add new

Receive data
Configure this instance to receive data forwarded from other instances.

Type	Actions
Configure receiving	+ Add new

A red box highlights the '+ Add new' button under the 'Actions' column for the 'Configure receiving' section.

Figura 1.11: Añadir new receiving data a Splunk

E Introducimos el puerto 9997 y hacemos clic en **Save** para guardar la configuración [2.56](#).



Screenshot of the Splunk web interface showing the configuration of a receiving port.

The URL is `splunk-aryan:8000/en-US/manager/launcher/data(inputs/tcp/cooked/_new?action=edit)`.

The page title is "Add new" under "Forwarding and receiving > Receive data".

The "Configure receiving" section contains a field "Listen on this port *" with the value "9997" highlighted by a red box. Below the field is a note: "For example, 9997 will receive data on TCP port 9997." At the bottom right are "Cancel" and "Save" buttons, with "Save" also highlighted by a red box.

A button "Mostrar aplicaciones" is visible at the bottom left.

Figura 1.12: Añadir puerto y guardar ajustes en Splunk

Screenshot of the Splunk web interface showing the list of configured receiving ports.

The URL is `splunk-aryan:8000/en-US/manager/launcher/data(inputs/tcp/cooked?msgid=8425170.783775)`.

The page title is "Receive data" under "Forwarding and receiving > Receive data".

A success message "Successfully saved \"9997\"." is displayed.

The table shows one item:

Listen on this port	Status	Actions
9997	Enabled Disable	Delete

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](#)

The screenshot shows the Splunk Enterprise Settings interface. On the left, under 'Receive data', there is a table with one item: 'Listen on this port' set to '9997' and 'Status' set to 'Enabled'. On the right, the navigation bar has a red box around the 'Indexes' link under the 'Forwarding and receiving' category. Other visible categories include 'Searches, reports, and alerts', 'Data inputs', 'Event types', 'Tags', 'Fields', 'Lookups', 'User interface', 'Alert actions', 'Advanced search', 'All configurations', 'SYSTEM', 'Server settings', 'Server controls', 'Health report manager', 'RapidDiag', 'Instrumentation', 'Licensing', 'Workload management', 'Mobile settings', 'DISTRIBUTED ENVIRONMENT', 'Indexer clustering', 'Forwarder management', 'Federated search', 'Distributed search', 'USERS AND AUTHENTICATION', 'Roles', 'Users', 'Tokens', 'Password management', and 'Authentication methods'.

Figura 1.14: Crear Indexador



Screenshot of the Splunk Enterprise web interface showing the 'Indexes' page. The top navigation bar includes links for 'splunk-aryan:8000/en-US/manager/launcher/data/indexes', 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', 'Find', and a search icon. A red box highlights the green 'New Index' button in the top right corner. The main content area displays a table of 15 indexes, each with columns for Name, Actions, Type, App, Current Size, Max Size, Event Count, Earliest Event, Latest Event, Home Path, and Frozen status. The table rows include: '_audit', '_configtracker', '_dsappevent', '_dsclient', and '_dsphonehome'. The bottom of the table shows summary statistics: 9 MR, 488.28 GB, R4 2K, 2 days ago, a few seconds ago, \$SPLUNK_D/B/_audit/db, N/A; 5 MB, 488.28 GB, 265, 2 days ago, 15 minutes ago, \$SPLUNK_D/B/_configtracker/db, N/A; 1 MB, 488.28 GB, 0, 2 days ago, a few seconds ago, \$SPLUNK_D/B/_dsappevent/db, N/A; 1 MB, 488.28 GB, 0, 2 days ago, a few seconds ago, \$SPLUNK_D/B/_dsclient/db, N/A; 1 MB, 488.28 GB, 0, 2 days ago, a few seconds ago, \$SPLUNK_D/B/_dsphonehome/db, N/A.

Figura 1.15: nuevo Indexador



New Index

X

General Settings

Index Name	Index_aryan	
Set index name (e.g., INDEX_NAME). Search using index=INDEX_NAME.		
Index Data Type	<input checked="" type="radio"/> Events	<input type="radio"/> Metrics
The type of data to store (event-based or metrics).		
Home Path	optional	
Hot/warm db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/db).		
Cold Path	optional	
Cold db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/colddb).		
Thawed Path	optional	
Thawed/resurrected db path. Leave blank for default (\$SPLUNK_DB/INDEX_NAME/thaweddb).		
Data Integrity Check	<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Enable this if you want Splunk to compute hashes on every slice of your data for the purpose of data integrity.		
Max Size of Entire Index	500	GB ▾
Maximum target size of entire index.		
<input type="button" value="Save"/>		<input type="button" value="Cancel"/>

Figura 1.16: Indexador aryan

index_aryan	Edit	Delete	Disable	<input checked="" type="radio"/> Events	search	1 MB	500 GB	0	\$SPLUNK_DB/Index_arya n/db	N/A
-------------	----------------------	------------------------	-------------------------	---	------------------------	------	--------	---	--------------------------------	-----

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](#)



Splunk Universal Forwarder 9.3.2

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

Windows	Linux	Mac OS	Free BSD	Solaris	AIX
 Windows	 Linux	 Mac OS	 Free BSD	 Solaris	 AIX
s390x	4.x+, or 5.x+ kernel Linux distributions	.rpm	30.7 MB	Download Now 	Copy wget link 

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
```



```
aryan@ubuntu-aryan:~$ wget -O splunkforwarder-9.3.2-d8bb32809498-Linux-x86_64.tgz "https://download.splunk.com/products/universalforwarder/releases/9.3.2/linux/splunkforwarder-9.3.2-d8bb32809498-Linux-x86_64.tgz"
--2024-12-07 23:52:48-- https://download.splunk.com/products/universalforwarder/releases/9.3.2/linux/splunkforwarder-9.3.2-d8bb32809498-Linux-x86_64.tgz
Resolviendo download.splunk.com (download.splunk.com)... 52.84.66.112, 52.84.66.41, 52.84.66.10, ...
Conectando con download.splunk.com (download.splunk.com)[52.84.66.112]:443... conectado.
Petición HTTP enviada, esperando respuesta... 200 OK
Longitud: 49486343 (47M) [application/x-tar]
Guardando como: 'splunkforwarder-9.3.2-d8bb32809498-Linux-x86_64.tgz'

splunkforwarder-9.3 100%[=====] 47,19M 13,0MB/s en 4,0s

2024-12-07 23:52:55 (11,8 MB/s) - 'splunkforwarder-9.3.2-d8bb32809498-Linux-x86_64.tgz' guardado [49486343/49486343]

aryan@ubuntu-aryan:~$ tar -xvzf splunkforwarder-9.3.2-d8bb32809498-Linux-x86_64.tgz
```

Figura 1.19: Comandos para la descarga de Splunk Universal Forwarder

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

```
aryan@ubuntu-aryan:~$ cd splunkforwarder/
aryan@ubuntu-aryan:~/splunkforwarder$ sudo ./bin/splunk start --accept-license
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R aryan:arian /home/arian/splunkforwarder"

This appears to be your first time running this version of Splunk.

Splunk software must create an administrator account during startup. Otherwise,
you cannot log in.
Create credentials for the administrator account.
Characters do not appear on the screen when you type in credentials.

Please enter an administrator username: aryan
```

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](#).

```
aryan@ubuntu-aryan:~/splunkforwarder
modules/static/css
    Creating: /home/aryan/splunkforwarder/var/run/splunk/upload
    Creating: /home/aryan/splunkforwarder/var/run/splunk/search_telemetry
    Creating: /home/aryan/splunkforwarder/var/run/splunk/search_log
    Creating: /home/aryan/splunkforwarder/var/spool/splunk
    Creating: /home/aryan/splunkforwarder/var/spool/dirmontcache
    Creating: /home/aryan/splunkforwarder/var/lib/splunk/authDb
    Creating: /home/aryan/splunkforwarder/var/lib/splunk/hashDb
    Creating: /home/aryan/splunkforwarder/var/run/splunk/sessions
New certs have been generated in '/home/aryan/splunkforwarder/etc/auth'.
    Checking conf files for problems...
    Done
    Checking default conf files for edits...
    Validating installed files against hashes from '/home/aryan/splunkforwarder/splunkforwarder-9.3.2-d8bb32809498-linux-2.6-x86_64.manifest'
        All installed files intact.
        Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

aryan@ubuntu-aryan:~/splunkforwarder$
```

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](#).



```
aryan@ubuntu-aryan:~/splunkforwarder$ sudo ./bin/splunk add forward-server 192.168.1.155:9997
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R aryan:aryan /home/aryan/splunkforwarder"
Added forwarding to: 192.168.1.155:9997.
aryan@ubuntu-aryan:~/splunkforwarder$ sudo ./bin/splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R aryan:aryan /home/aryan/splunkforwarder"
Active forwards:
    None
Configured but inactive forwards:
    192.168.1.155:9997
aryan@ubuntu-aryan:~/splunkforwarder$ ls ./etc/system/local/
outputs.conf  README  server.conf
aryan@ubuntu-aryan:~/splunkforwarder$ cat ./etc/system/local/outputs.conf
[tcpout]
defaultGroup = default-autolb-group

[tcpout:default-autolb-group]
server = 192.168.1.155:9997

[tcpout-server://192.168.1.155:9997]
aryan@ubuntu-aryan:~/splunkforwarder$
```

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

```
aryan@ubuntu-aryan:~/splunkforwarder$ ./etc/system/local/outputs.conf
GNU nano 7.2
[tcpout]
defaultGroup = splunk-aryan

[tcpout:splunk-aryan]
server = 192.168.1.155:9997

[tcpout-server://192.168.1.155:9997]
```

Figura 1.23: Archivo Outputs.conf

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



```
aryan@ubuntu-aryan:~/splunkforwarder$ sudo ./bin/splunk restart
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R aryan:ryan /home/ryan/splunkforwarder"
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.

Stopping splunk helpers...

Done.
splunkd.pid doesn't exist...

Splunk> Finding your faults, just like mom.

Checking prerequisites...
    Checking mgmt port [8089]: open
    Checking conf files for problems...
    Done
    Checking default conf files for edits...
    Validating installed files against hashes from '/home/ryan/splunkforwarder/splunkforwarder-9.3.2-d8bb32809498-linux-2.6-x86_64-manifest'
    All installed files intact.
    Done
All preliminary checks passed.

Starting splunk server daemon (splunkd)...
Done

aryan@ubuntu-ryan:~/splunkforwarder$ sudo ./bin/splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R aryan:ryan /home/ryan/splunkforwarder"
Your session is invalid. Please login.
Splunk username: aryan
Password:
Active forwards:
    192.168.1.155:9997
Configured but inactive forwards:
    None
```

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_ryan -sourcetype authlogs
```

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

```
aryan@ubuntu-ryan:~/splunkforwarder$ sudo ./bin/splunk add monitor /var/log/auth.log -index index_ryan -sourcetype authlogs
[sudo] contraseña para aryan:
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R aryan:ryan /home/ryan/splunkforwarder"
Added monitor of '/var/log/auth.log'.
```

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
```

```
aryan@ubuntu-aryan:~/splunkforwarder$ sudo ./bin/splunk list monitor
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R aryan:aryan /home/aryan/splunkforwarder"
Monitored Directories:
$SPLUNK_HOME/var/log/splunk
    /home/aryan/splunkforwarder/var/log/splunk/audit.log
    /home/aryan/splunkforwarder/var/log/splunk/btool.log
    /home/aryan/splunkforwarder/var/log/splunk/conf.log
    /home/aryan/splunkforwarder/var/log/splunk/first_install.log
    /home/aryan/splunkforwarder/var/log/splunk/health.log
    /home/aryan/splunkforwarder/var/log/splunk/license_usage.log
    /home/aryan/splunkforwarder/var/log/splunk/mergebuckets.log
    /home/aryan/splunkforwarder/var/log/splunk/mongod.log
    /home/aryan/splunkforwarder/var/log/splunk/remote_searches.log
    /home/aryan/splunkforwarder/var/log/splunk/scheduler.log
    /home/aryan/splunkforwarder/var/log/splunk/search_messages.log
    /home/aryan/splunkforwarder/var/log/splunk/searchhistory.log
    /home/aryan/splunkforwarder/var/log/splunk/splunkd-utility.log
    /home/aryan/splunkforwarder/var/log/splunk/splunkd_access.log
    /home/aryan/splunkforwarder/var/log/splunk/splunkd_ui_access.log
    /home/aryan/splunkforwarder/var/log/splunk/wlm_monitor.log
$SPLUNK_HOME/var/log/splunk/configuration_change.log
    /home/aryan/splunkforwarder/var/log/splunk/configuration_change.log
$SPLUNK_HOME/var/log/splunk/license_usage_summary.log
    /home/aryan/splunkforwarder/var/log/splunk/license_usage_summary.log
$SPLUNK_HOME/var/log/splunk/metrics.log
    /home/aryan/splunkforwarder/var/log/splunk/metrics.log
$SPLUNK_HOME/var/log/splunk/splunk_instrumentation_cloud.log*
    /home/aryan/splunkforwarder/var/log/splunk/splunk_instrumentation_cloud.log
$SPLUNK_HOME/var/log/splunk/splunkd.log
    /home/aryan/splunkforwarder/var/log/splunk/splunkd.log
$SPLUNK_HOME/var/log/watchdog/watchdog.log*
    /home/aryan/splunkforwarder/var/log/watchdog/watchdog.log
$SPLUNK_HOME/var/run/splunk/search_telemetry/*search_telemetry.json
$SPLUNK_HOME/var/splunk/splunk/tracker.log*
Monitored Files:
$SPLUNK_HOME/etc/splunk.version
/var/log/auth.log
```

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.



splunk-aryan:8000/en-US/manager/launcher/data/indexes#

Administrator 1 Messages Settings Activity Help Find

Indexes

New Index

16 Indexes filter 20 per page ▾

Name	Actions	Type	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Frozen
_Internal	Edit Delete Disable	Events	system	11 MB	488.28 GB	108K	2 days ago	a few seconds ago	\$SPLUNK_D/B/_Internal/db	N/A
_metrics	Edit Delete Disable	Metrics	system	16 MB	488.28 GB	83.2K	2 days ago	a few seconds ago	\$SPLUNK_D/B/_metrics/db	N/A
_audit	Edit Delete Disable	Events	system	4 MB	488.28 GB	14.1K	2 days ago	a few seconds ago	\$SPLUNK_D/B/audit/db	N/A
_introspection	Edit Delete Disable	Events	system	27 MB	488.28 GB	18.8K	2 days ago	a few seconds ago	\$SPLUNK_D/B/_introspection/db	N/A
index_aryan	Edit Delete Disable	Events	search	1 MB	500 GB	307	15 hours ago	3 minutes ago	\$SPLUNK_D/B/Index_arya/n/db	N/A
_configtracker	Edit Delete Disable	Events	system	5 MB	488.28 GB	275	2 days ago	9 minutes ago	\$SPLUNK_D/B/_configtracker/db	N/A
_telemetry	Edit Delete Disable	Events	system	1 MB	488.28 GB	2	41 minutes ago	31 minutes ago	\$SPLUNK_D/B/_telemetry	N/A

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](#)



The screenshot shows the Splunk Enterprise user interface. At the top, there is a navigation bar with links for 'Administrator', 'Messages', 'Settings', 'Activity', 'Help', and a search bar. Below the navigation bar, the main content area is titled 'Hello, Administrator'. It features a sidebar on the left with a 'Search apps by name...' input field and a list of apps: 'Search & Reporting' (highlighted with a red box), 'Splunk Secure Gateway', and 'Upgrade Readiness App'. There is also a link to 'Find more apps'. The main content area is divided into sections: 'My bookmarks (0)', 'Shared with my organization (0)', 'Shared by me', and 'Splunk recommended (14)'. Under 'Common tasks', there are four buttons: 'Add data' (with a description 'Add data from a variety of common sources.'), 'Search your data' (with a description 'Turn data into doing with Splunk search.'), 'Visualize your data' (partially visible), and 'Manage alerts'.

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 ??.



New Search

index=index_aryan

Events (5) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection X Deselect

Last 15 minutes ▾

i	Time	Event
>	12/8/24 3:00:30.451 PM	2024-12-08T15:00:30.451485+01:00 ubuntu-aryan gdm-password]: gkr-pam: unlocked login keyring host = ubuntu-aryan : source = /var/log/auth.log : sourcetype = authlogs
>	12/8/24 2:55:01.757 PM	2024-12-08T14:55:01.757239+01:00 ubuntu-aryan CRON[5828]: pam_unix(cron:session): session closed for user root host = ubuntu-aryan : source = /var/log/auth.log : sourcetype = authlogs
>	12/8/24 2:55:01.751 PM	2024-12-08T14:55:01.751822+01:00 ubuntu-aryan CRON[5828]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0) host = ubuntu-aryan : source = /var/log/auth.log : sourcetype = authlogs
>	12/8/24 2:50:55.787 PM	2024-12-08T14:50:55.787662+01:00 ubuntu-aryan sudo: pam_unix(sudo:auth): authentication failure; logname=arnan uid=1000 euid=0 ttv=/dev/pts/0 ruser=arvan rhost= user=arvan

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.

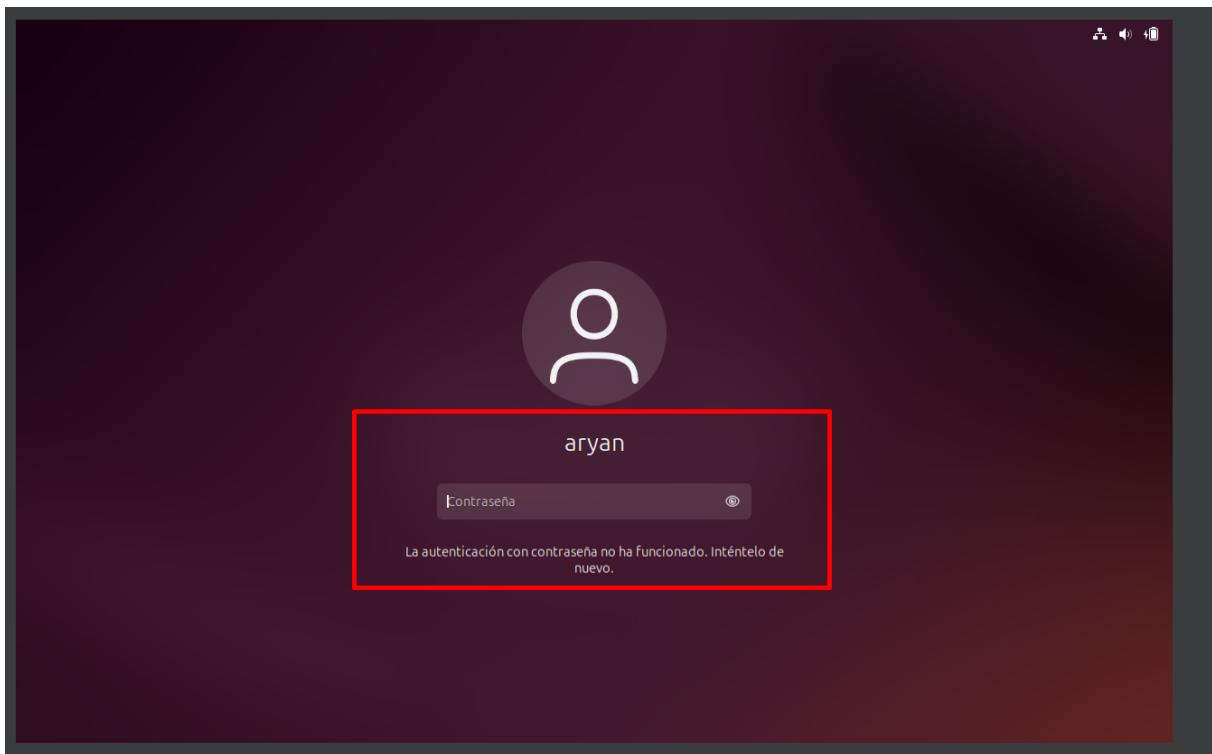


Figura 1.30: Inicio de sesión incorrecto

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



el indexador como iniciamos anteriormente.

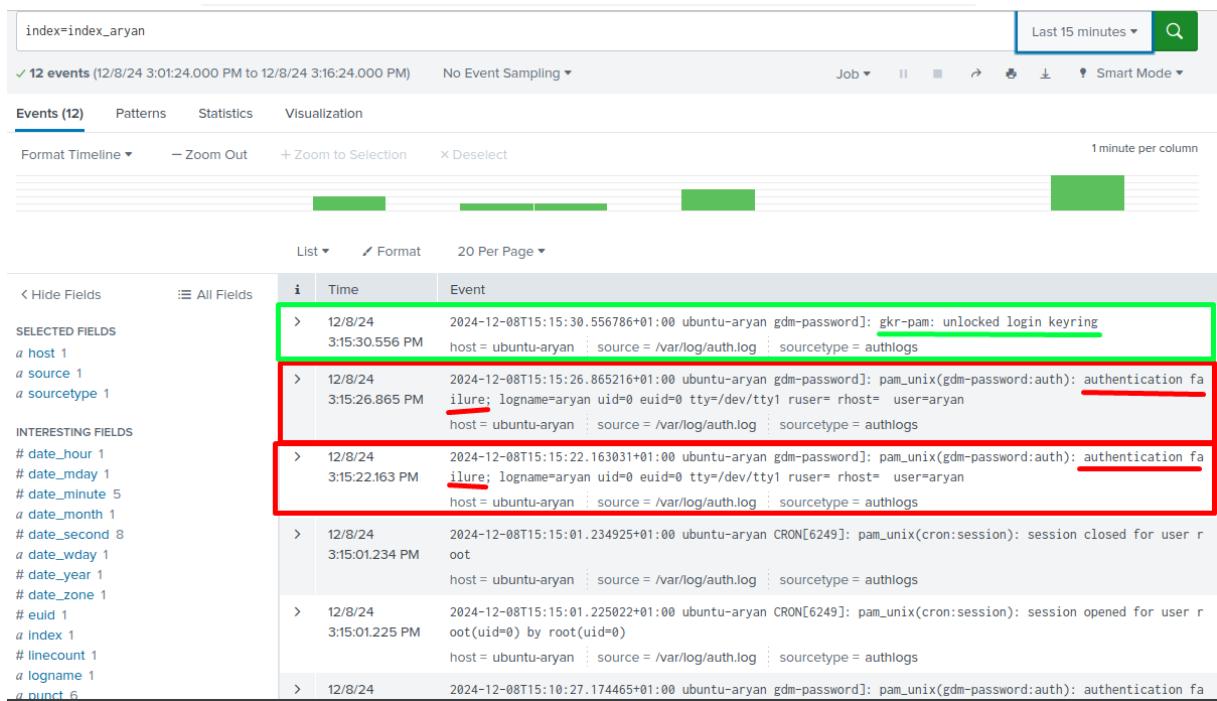


Figura 1.31: Pruebas Inicio de sesión

Como 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 búsqueda para contabilizar los eventos.

```
index="index_aryan" sourcetype="authlogs" source="/var/log/auth.log"
| eval event_type=case(
    like(_raw, "%unlocked login keyring%"), "Unlocked Keyring",
    like(_raw, "%authentication failure%"), "Authentication Failure")
| stats count by event_type
```

Con esta búsqueda lo que hacemos es crear un campo `event_type` que se asigne con base en el contenido de los eventos. Se usa `like` para buscar patrones específicos en el campo `_raw`.



Si el campo `_raw` contiene unlocked login keyring, se marca como Unlocked Keyring y si tiene authentication failure se marca como Authentication Failure.

Y después cuenta cuantos eventos existen para cada tipo. [1.40](#)

Una vez tenemos listados todos los eventos y contado podemos darle a visualización [1.32](#).

The screenshot shows the Splunk Enterprise search interface. The search bar contains the following SPL command:

```
index="index_arian" sourcetype="authlogs" source="/var/log/auth.log"
| eval event_type=case(_raw, "%unlocked login keyring%", "Unlocked Keyring",
    like(_raw, "%authentication failure%"), "Authentication Failure")
| stats count by event_type
```

The results section shows 344 events from 12/7/24 4:00:00.000 PM to 12/8/24 4:23:46.000 PM. The Statistics tab is selected, and the Visualization tab is highlighted with a red box. The visualization table shows two rows:| event_type | count |
| --- | --- |
| Authentication Failure | 5 |
| Unlocked Keyring | 10 |

Figura 1.32: Visualización de eventos

Y podremos ver una grafica en columnas de los eventos [1.33](#).

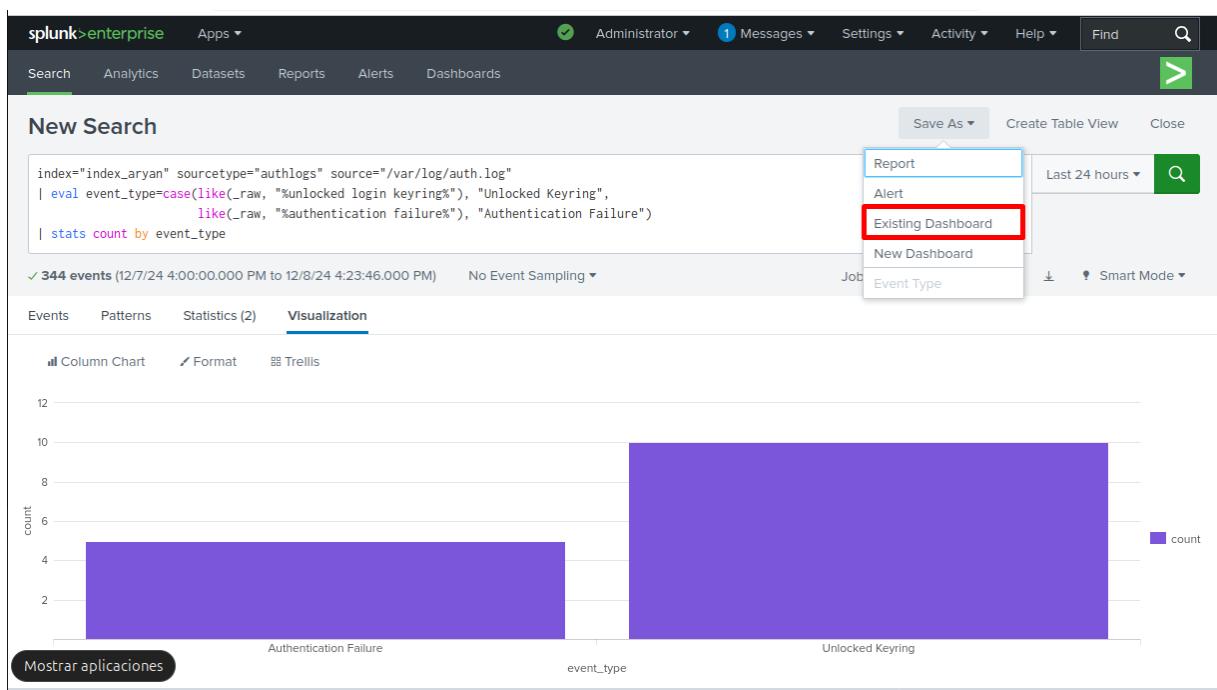


Figura 1.33: Gráfica en columnas

Una vez aquí le damos a Guardar como y elegimos un dashboard existente que ya teníamos creado [1.34](#).



Save Panel to Existing Dashboard

X

Select an Existing Dashboard

Sort: Title (A - Z) ↓

🔍

<input checked="" type="checkbox"/> Inicios de sesión exitosos y fallidos
Integrity Check of Installed Files
Job Details Dashboard
jQuery Upgrade
Orphaned Scheduled Searches, Reports, and Alerts

Panel Title

Optional

Visualization Type

Column Chart

Statistics Table

> Advanced Panel Settings

Cancel

Save to Dashboard

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 él veremos la gráfica de columnas pero lo editamos y elegios la gráfica de barras y ya tendríamos la gráfica y la visualización de ello [1.35](#).

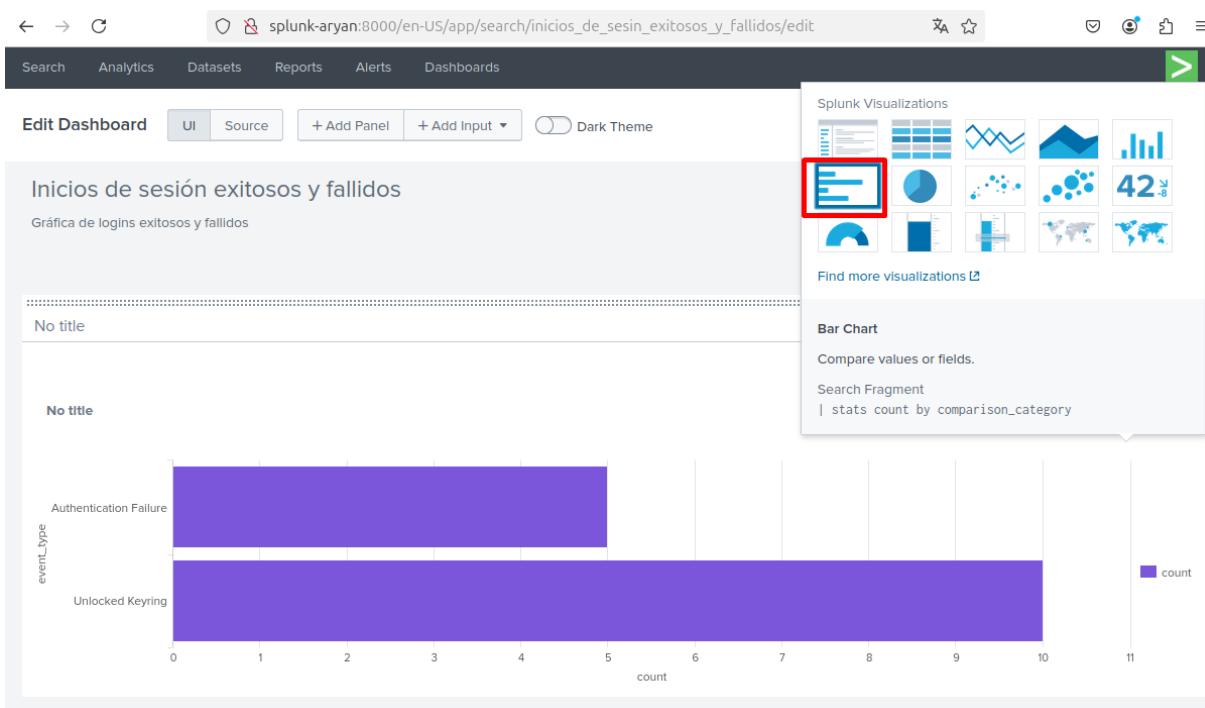


Figura 1.35: Gráfica de barras

Y ya tendremos en el dashboard la gráfica de barras.

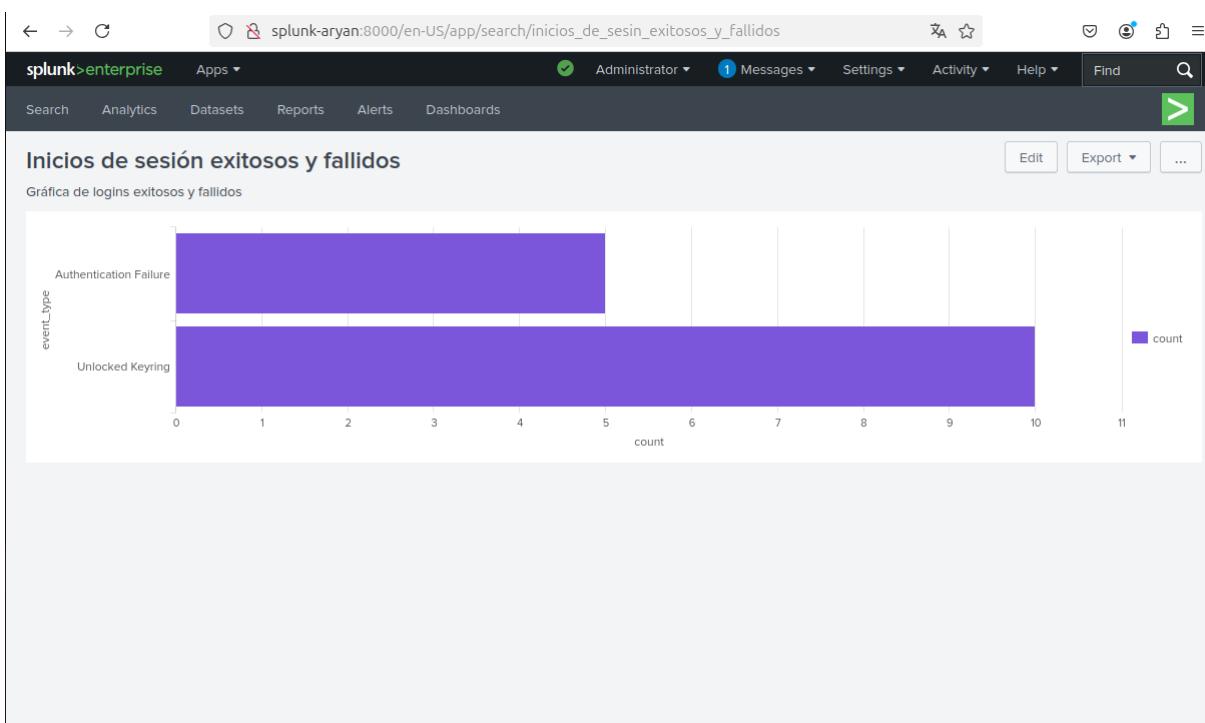


Figura 1.36: Gráfica de barras



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 sitio que en [1.28](#), hacemos clic en Dashboard [1.37](#)

The screenshot shows the Splunk Enterprise web interface. At the top, there is a navigation bar with links for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The 'Dashboards' link is highlighted with a red box. On the right side of the header, there are user status indicators (Administrator, Messages, Settings, Activity, Help) and search/filter tools. Below the header, the main content area has a title 'Dashboards' and a sub-instruction: 'Dashboards include searches, visualizations, and input controls that capture and present available data.' To the right of this text is a green button labeled 'Create New Dashboard' with a red box around it. Underneath, there is a section titled 'Latest Resources' with three cards: 'Examples for Dashboard Studio', 'Intro to Dashboard Studio', and 'Intro to Classic Dashboards'. Below this is a table titled '5 Dashboards' with columns for Title, Actions, Owner, App, Sharing, and Type. The table lists five dashboards: 'Integrity Check of Installed Files', 'Job Details Dashboard', 'jQuery Upgrade', 'Orphaned Scheduled Searches, Reports, and Alerts', and 'Scheduled export is now available for Dashboard Studio'. Each row in the table includes an 'Edit' button and the same set of metadata columns.

Figura 1.37: Nuevo dashboard

Después de seleccionar crear nuevo dashboard [1.38](#) introducimos un nombre y el constructor, en nuestro caso el clásico.



Create New Dashboard

X

Dashboard Title

Inicios de sesión exitosos y fallidos

inicios_de_sesin_exitosos_y_fallidos

Edit ID

Description

Gráfica de logins exitosos y fallidos

Permissions

Shared in App

▼

How do you want to build your dashboard?

[What's this?](#)

Classic Dashboards

The traditional Splunk dashboard builder

Dashboard Studio NEW

A new builder to create visually-rich, customizable dashboards

[Cancel](#)

[Create](#)

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.



splunk-aryan:8000/en-US/app/search/inicios_de_sesin_exitosos_y_fallidos/edit

splunk>enterprise Apps ▾

Administrator 1 Messages Settings

Search Analytics Datasets Reports Alerts Dashboards

Edit Dashboard UI Source + Add Panel + Add Input Dark Theme

Inicios de sesión exitosos y fallidos

Gráfica de logins exitosos y fallidos

! Click Add Panel to start.

Add Panel

New (15)

- Events
- Statistics Table
- Line Chart
- Area Chart
- Column Chart
- Bar Chart
- Pie Chart
- Scatter Chart
- Bubble Chart
- Single Value
- Radial Gauge
- Filler Gauge
- Marker Gauge
- Cluster Map
- Choropleth Map

New from Report (7)

Clone from Dashboard (6)

Add Prebuilt Panel (0)

Figura 1.39: Añadir paneles

Aunque para ello hay que crear una query de búsqueda como en el caso anterior y como vemos en [1.40](#)



The screenshot shows the Splunk Enterprise interface with a modal window titled 'Add Panel'. The modal lists various chart types under the 'Events' category. The 'Events' option is highlighted. To the right of the list, there are fields for 'Content Title' (set to 'optional') and 'Search String' (with placeholder 'enter search here...'). Below the list, there are three additional options: 'New from Report (7)', 'Clone from Dashboard (6)', and 'Add Prebuilt Panel (0)'. At the bottom of the modal, there is a 'Run Search' button.

Figura 1.40: Añadir paneles nuevos, búsqueda

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 instalación 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 nuestra máquina virtual windows.



Personalizar configuración

Personalizar la configuración de cada tipo de red

Puede modificar la configuración del firewall para cada tipo de red que use.

Configuración de red privada

Activar Firewall de Windows Defender
 Bloquear todas las conexiones entrantes, incluidas las de la lista de aplicaciones permitidas
 Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación

Desactivar Firewall de Windows Defender (no recomendado)

Configuración de red pública

Activar Firewall de Windows Defender
 Bloquear todas las conexiones entrantes, incluidas las de la lista de aplicaciones permitidas
 Notificarme cuando Firewall de Windows Defender bloquee una nueva aplicación

Desactivar Firewall de Windows Defender (no recomendado)

Figura 1.42: Desactivar Firewall MV

Y ahora ya nuestras máquinas podran verse.

```
aryan@splunk-aryan:~$ ping -c 3 192.168.1.137
PING 192.168.1.137 (192.168.1.137) 56(84) bytes of data.
64 bytes from 192.168.1.137: icmp_seq=1 ttl=128 time=50.9 ms
64 bytes from 192.168.1.137: icmp_seq=2 ttl=128 time=41.9 ms
64 bytes from 192.168.1.137: icmp_seq=3 ttl=128 time=7.05 ms

--- 192.168.1.137 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2005ms
rtt min/avg/max/mdev = 7.048/33.277/50.889/18.907 ms
```

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](#).



Splunk Universal Forwarder 9.3.2

Universal Forwarders provide reliable, secure data collection from remote sources and forward that data into Splunk software for indexing and consolidation. They can scale to tens of thousands of remote systems, collecting terabytes of data.

Choose Your Installation Package

The screenshot shows the download page for Splunk Universal Forwarder 9.3.2. It lists two main options: 'Windows 10, 11' and 'Windows Server 2019, 2022'. Both are 64-bit packages with '.msi' extensions. The 'Windows 10, 11' package is 129.53 MB and has a 'Download Now' button highlighted with a red box. The 'Windows Server 2019, 2022' package is 65.0 MB and also has a 'Download Now' button. Other platforms listed include Linux, Mac OS, FreeBSD, Solaris, and AIX.

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.

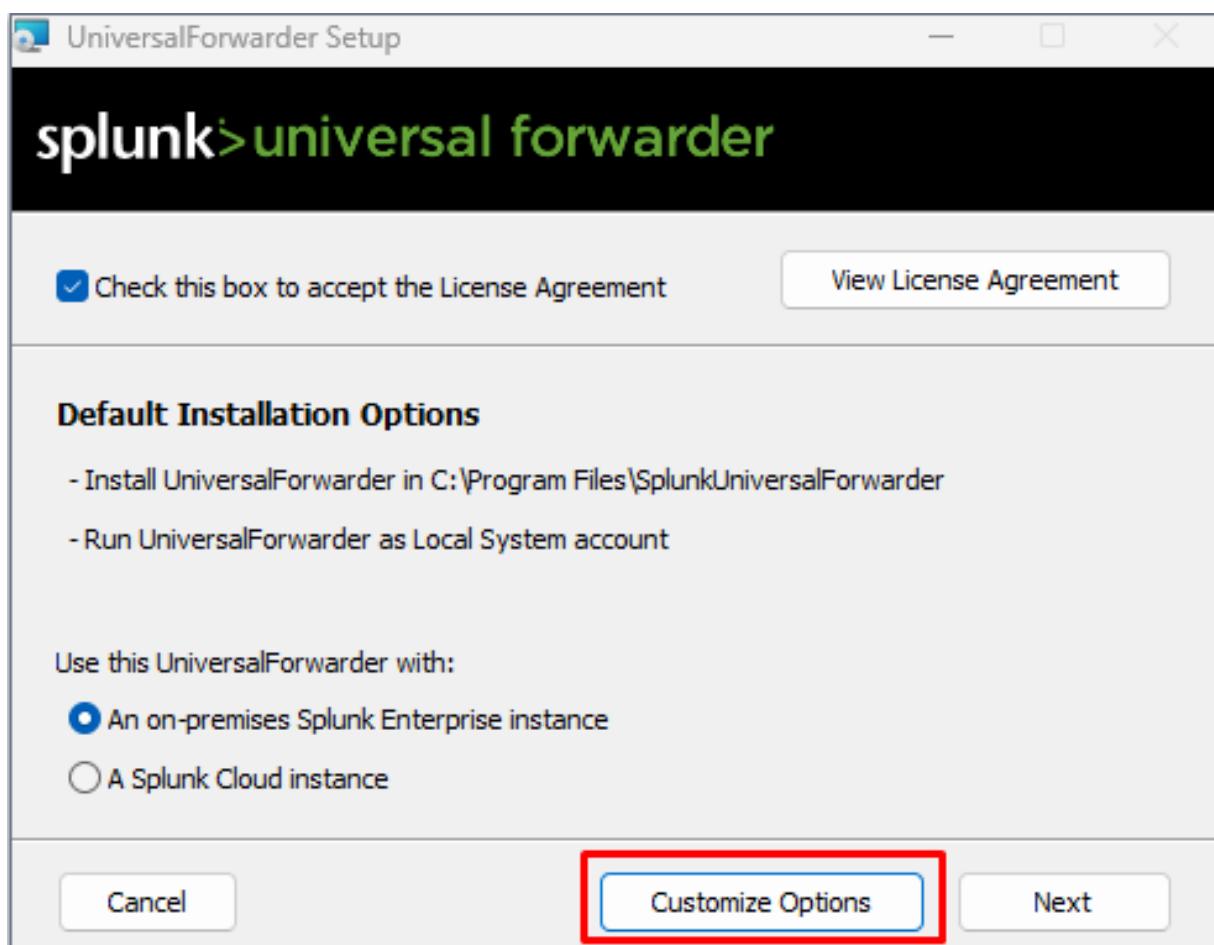


Figura 1.45: Licencia windows



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

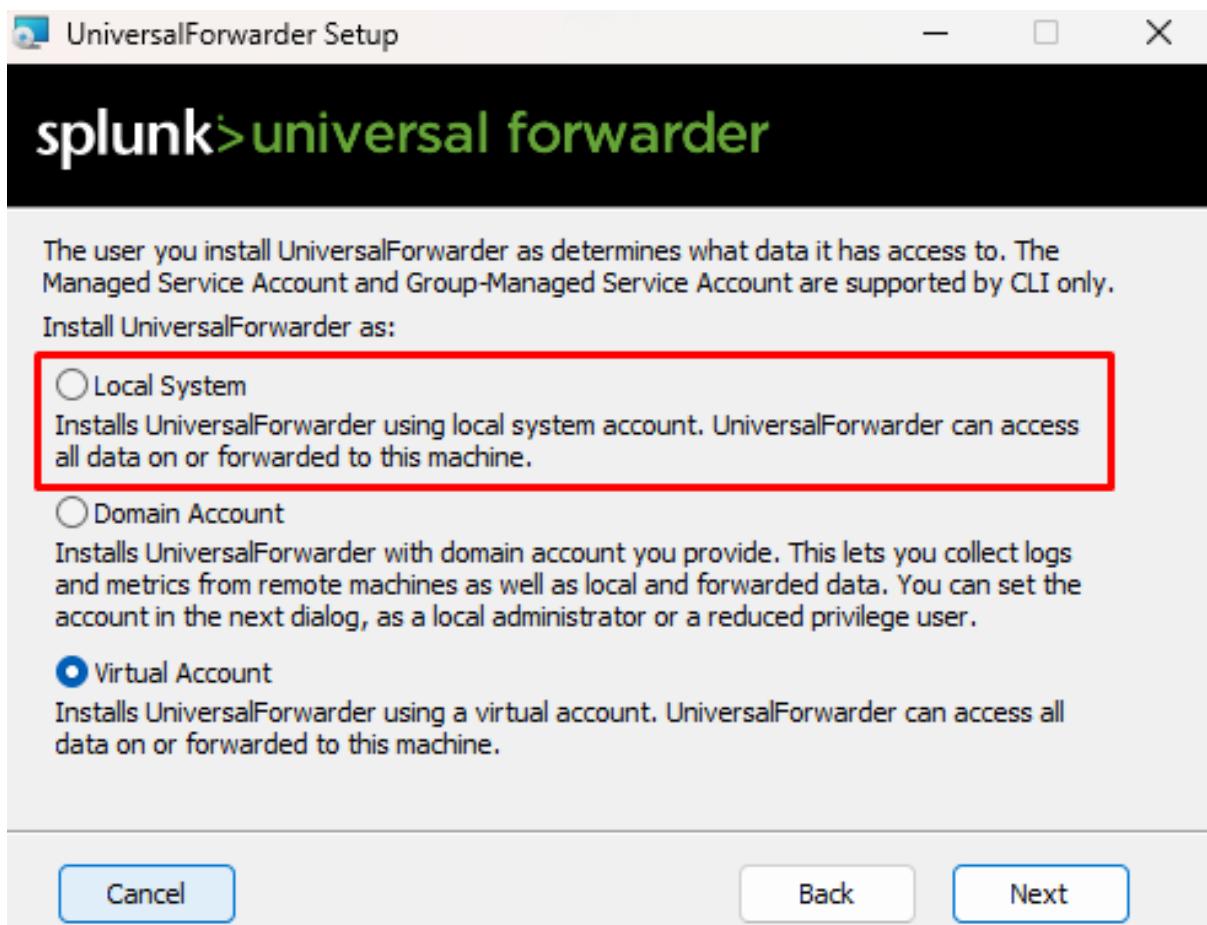


Figura 1.46: Local System

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

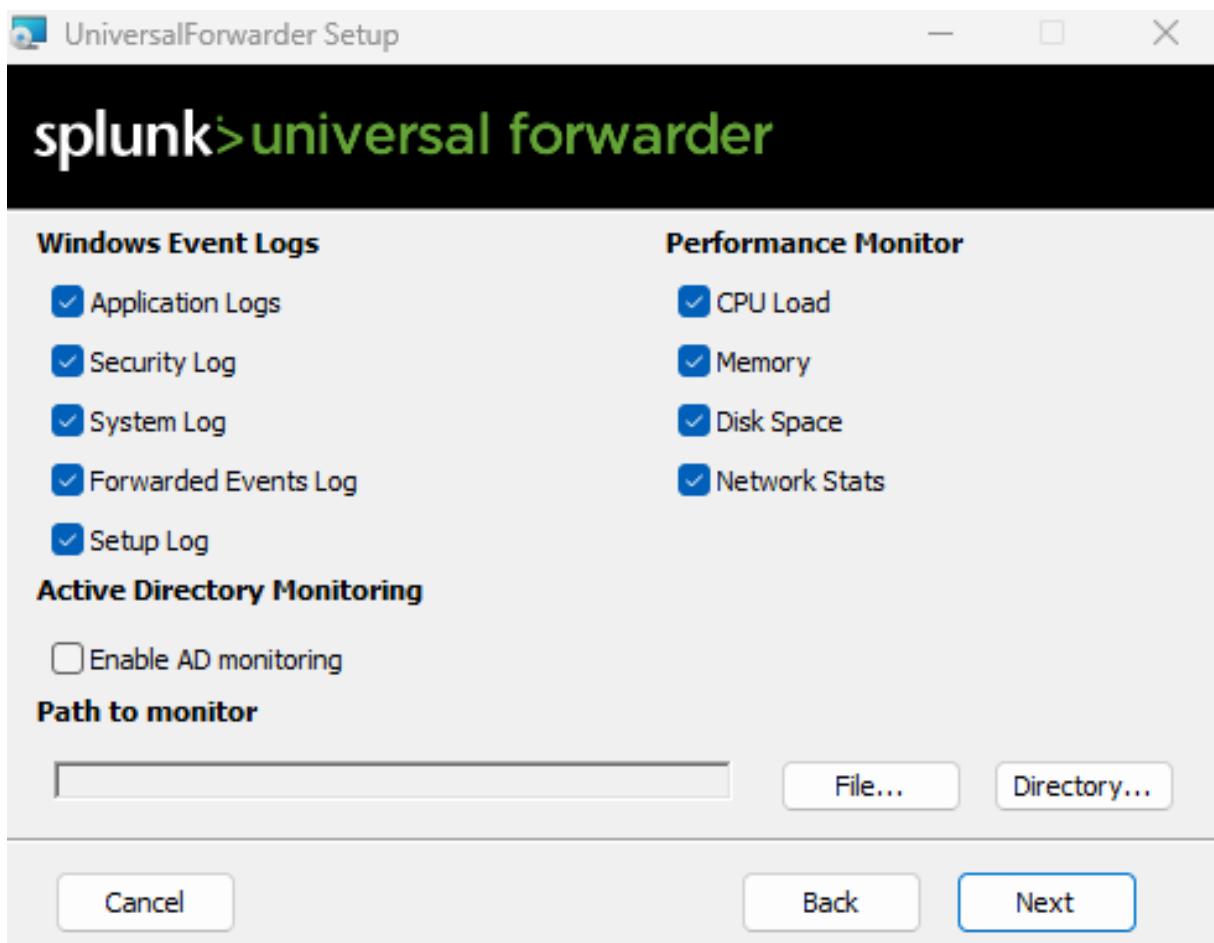


Figura 1.47: Ip deployment server

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

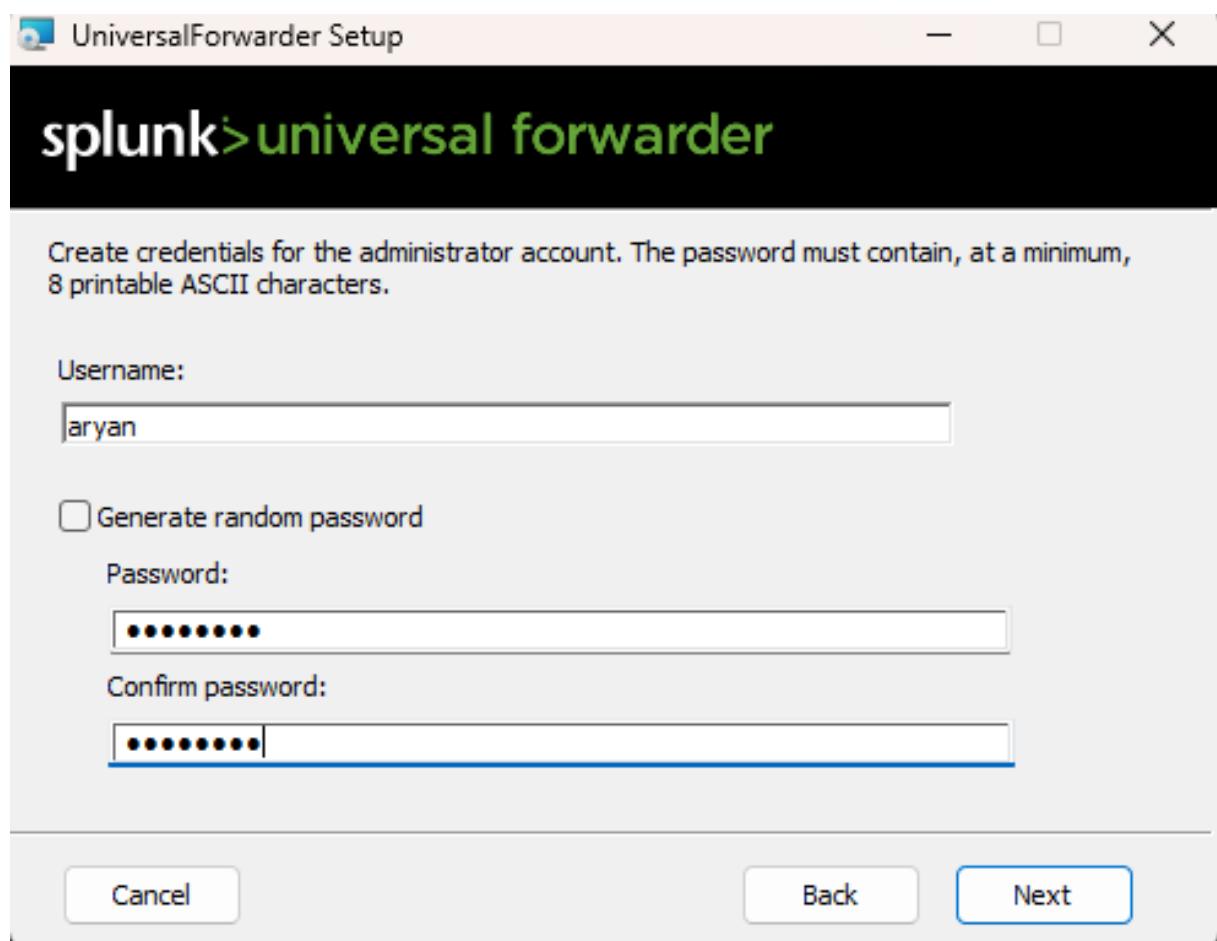


Figura 1.48: Credenciales

Ahora vamos a introducir 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](#)).

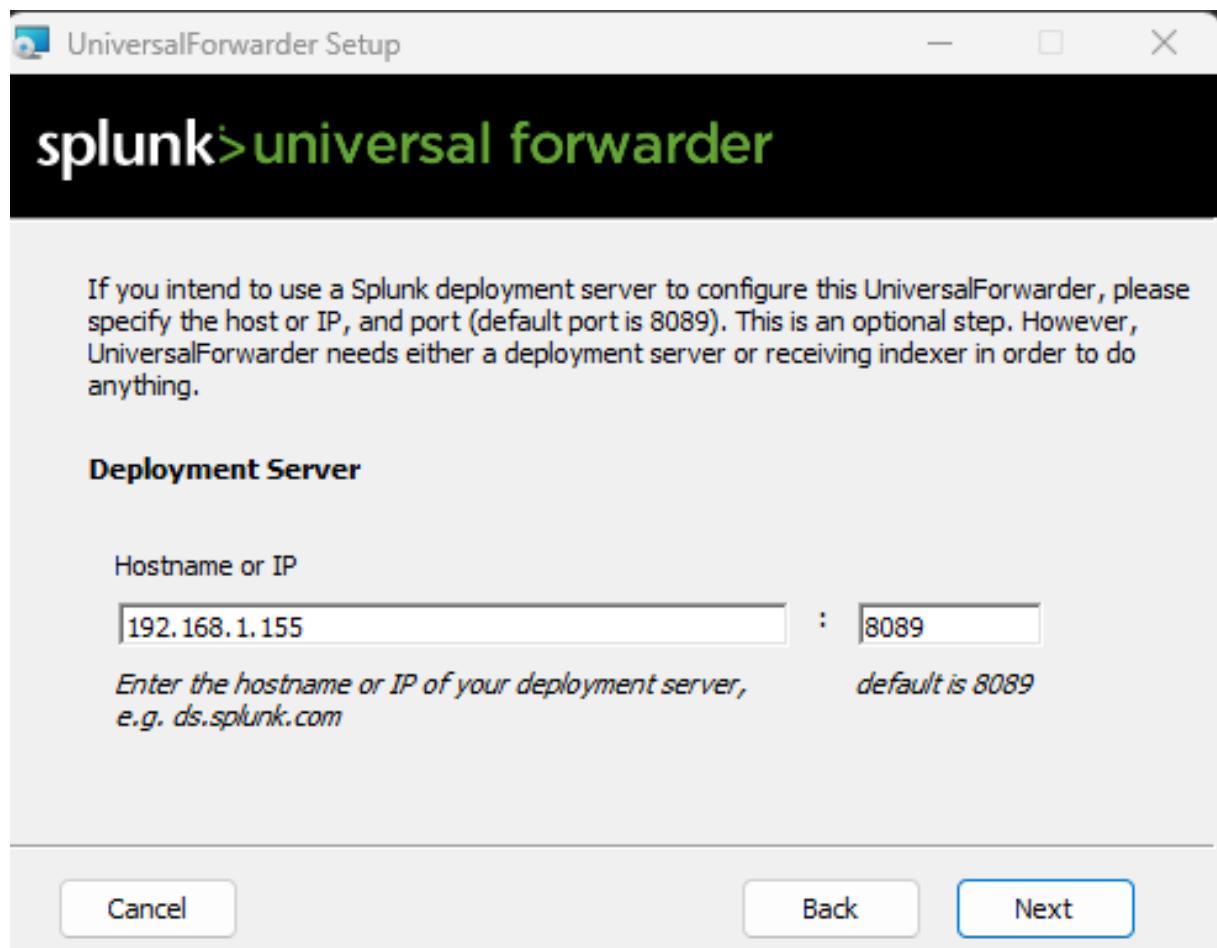


Figura 1.49: IP deployment server

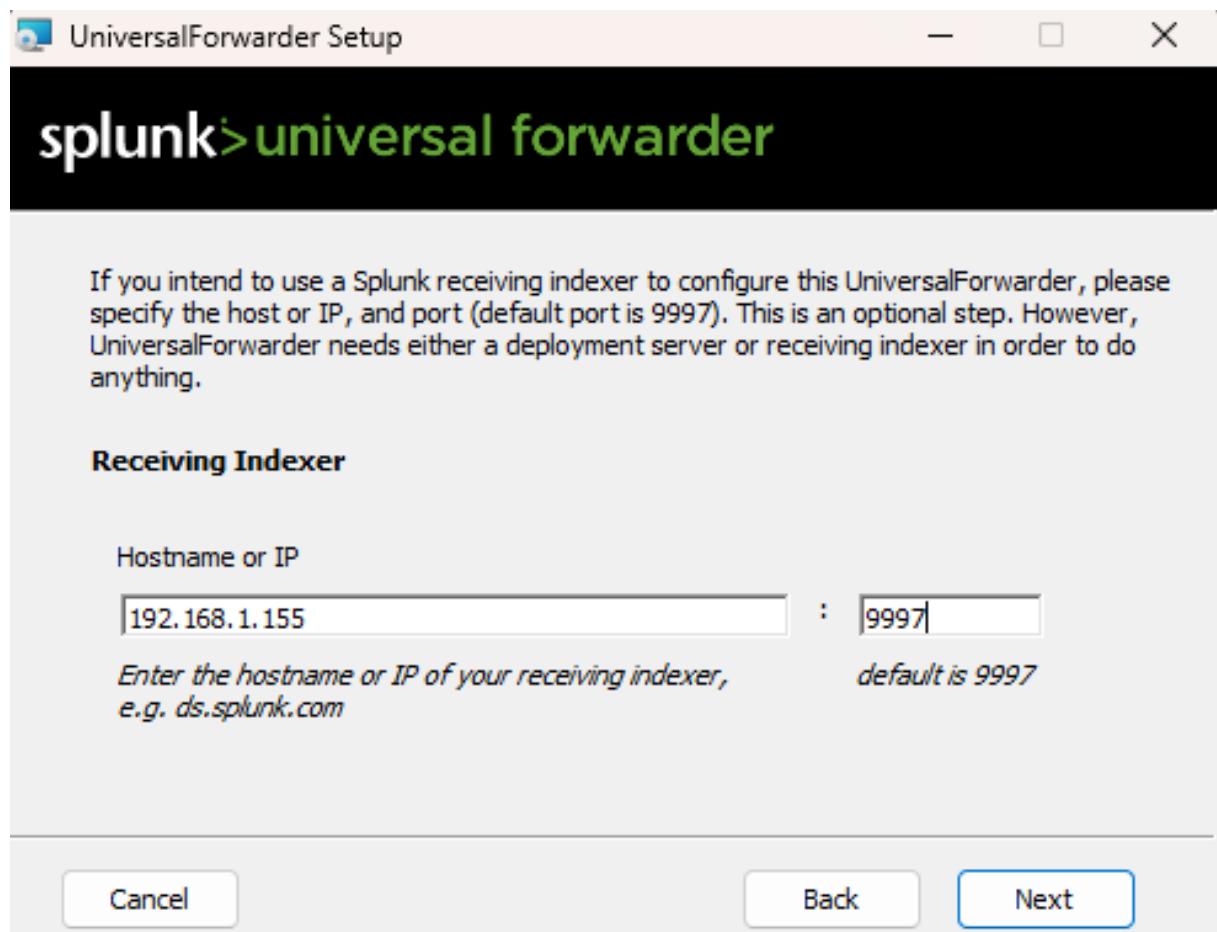


Figura 1.50: IP indexador

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

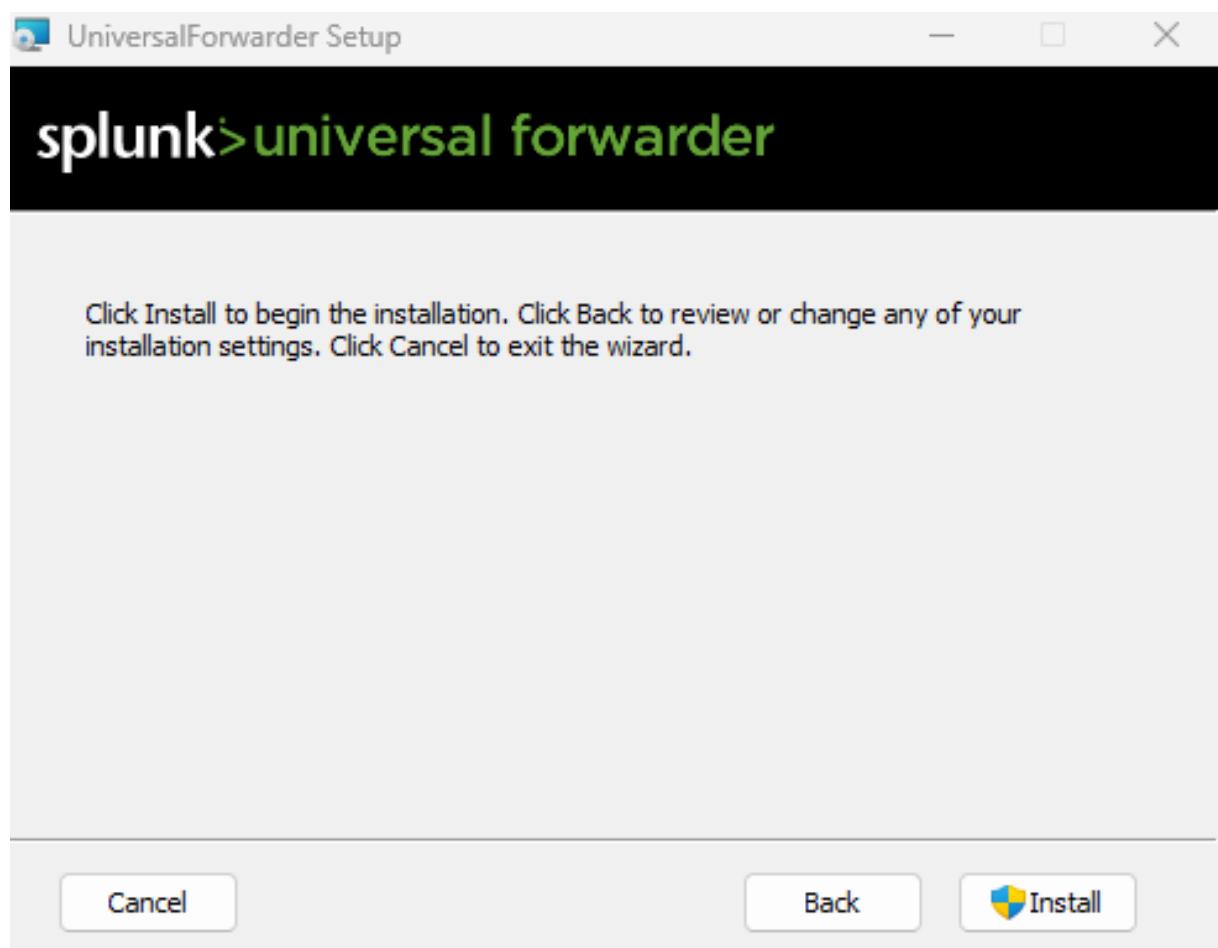


Figura 1.51: Instalar

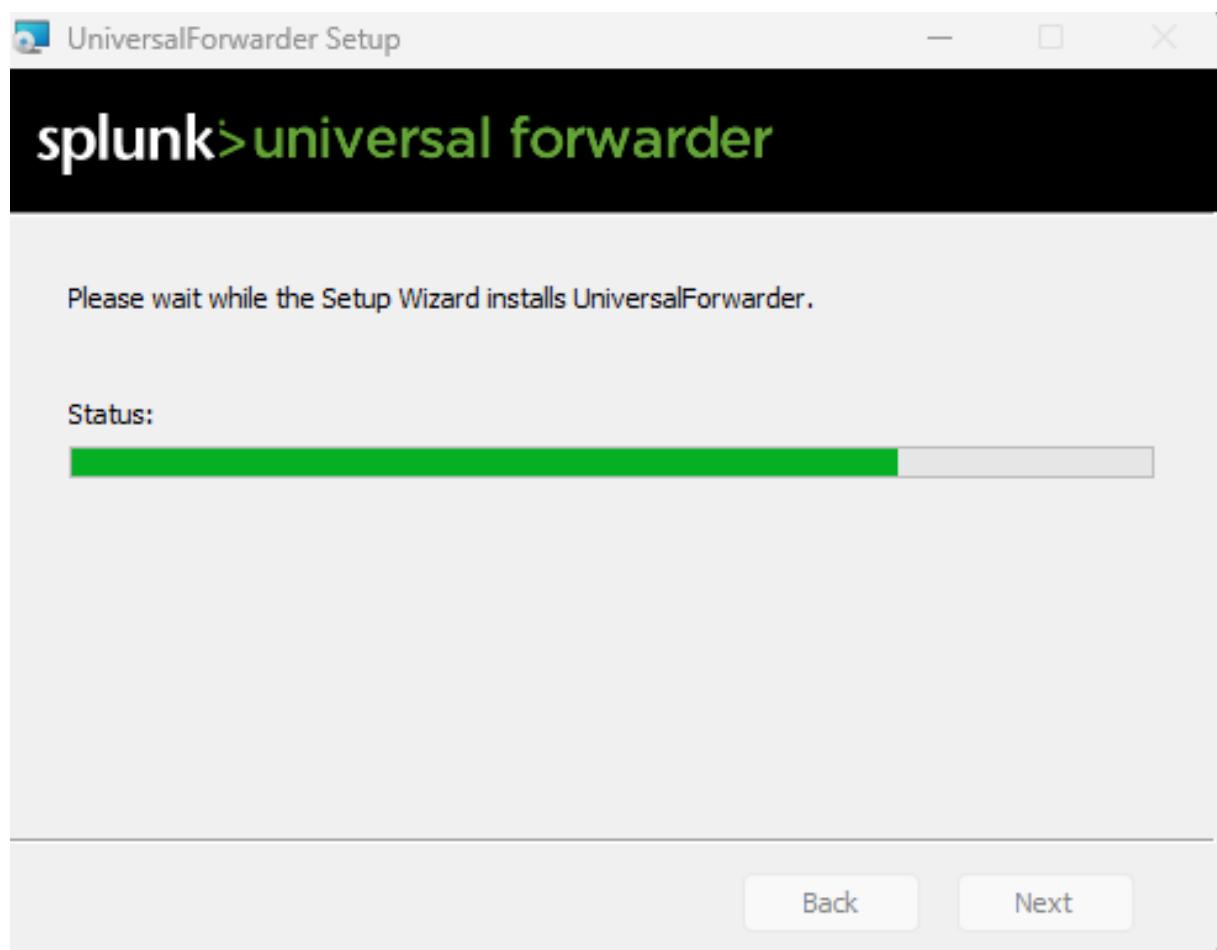


Figura 1.52: Status de la instalación

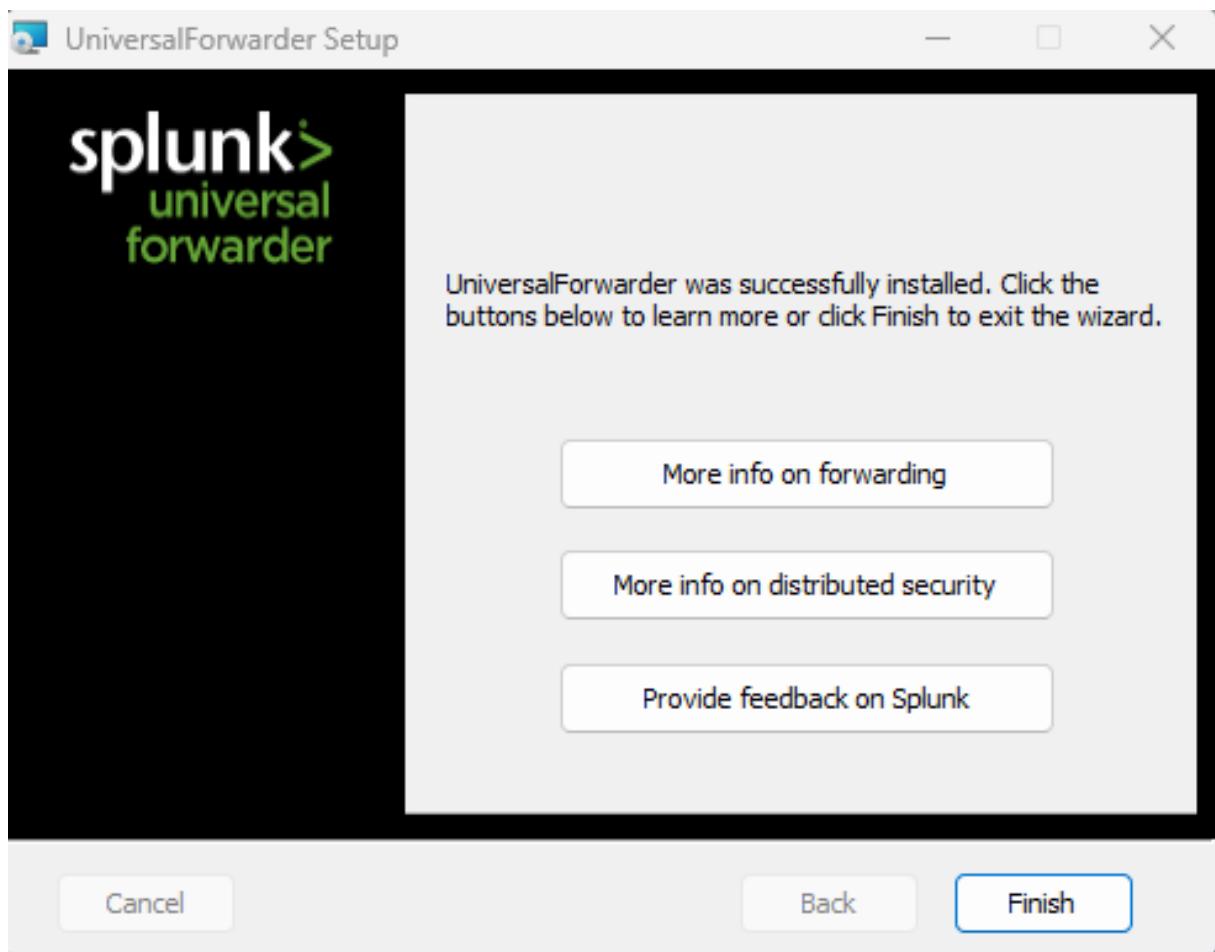


Figura 1.53: Fin de instalación de Universal forwarder

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.

index_aryan	Edit	Delete	Disable	Events	search	1 MB	500 GB	364	4 days ago	3 days ago	\$SPLUNK_D B/Index_arya n/db
index_aryan_windows	Edit	Delete	Disable	Events	search	1 MB	500 GB	0			\$SPLUNK_D B/Index_arya n_windows/ db

Figura 1.54: Indexador para windows

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



Add Data

Explore Data

Monitoring Console

KNOWLEDGE

[Searches, reports, and alerts](#)

[Data models](#)

[Event types](#)

[Tags](#)

[Fields](#)

[Lookups](#)

[User interface](#)

[Alert actions](#)

[Advanced search](#)

[All configurations](#)

DATA

[Data inputs](#)

[Forwarding and receiving](#)

[Indexes](#)

[Report acceleration summaries](#)

[Virtual indexes](#)

[Source types](#)

[Ingest actions](#)

DISTRIBUTED ENVIRONMENT

[Indexer clustering](#)

Forwarder management

[Federated search](#)

[Distributed search](#)

SYSTEM

[Server settings](#)

[Server controls](#)

[Health report manager](#)

[RapidDiag](#)

[Instrumentation](#)

[Licensing](#)

[Workload management](#)

[Mobile settings](#)

USERS AND AUTHENTICATION

[Roles](#)

[Users](#)

[Tokens](#)

[Password management](#)

[Authentication methods](#)

Figura 1.55: Forward Management

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

Clients (1)								
Phone Home: All ▾		All Clients ▾		filter				
1 Clients		10 Per Page ▾						
i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	DESKTOP-RMJL9A2	977894BC-6201-4C98-930B-968F87EE8D0B	DESKTOP-RMJL9A2	192.168.1.137	Delete Record	windows-x64	0 deployed	a few seconds ago

Figura 1.56: Cliente 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.

The screenshot shows a navigation bar with three items: 'Apps (0)', 'Server Classes (0)', and 'Clients (1)'. The 'Server Classes (0)' item is highlighted with a blue border. Below the navigation bar, there is a message: 'No server classes. Learn more. ↗ or [create one](#)' with a red box around the 'create one' link.

Figura 1.57: Crear server class

The screenshot shows a dialog box titled 'New Server Class' with a close button 'X' in the top right corner. It has a single input field labeled 'Name' containing the value 'windows-aryan'. At the bottom of the dialog are two buttons: 'Cancel' and a green 'Save' button.

Figura 1.58: Server class windows

Como vemos en [1.58](#) lo nombramos windows-aryan. Una vez creado tenemos que añadir el cliente.



Server Class: windows-aryan

[Edit](#) [Documentation](#)

You haven't added any apps

[Add Apps](#)

You haven't added any clients

[Add Clients](#)

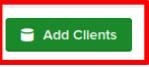


Figura 1.59: Añadir cliente

Edit Clients

Server Class: windows-aryan

[Documentation](#)

Include (includeList)

Required

Can be client name, host name, IP address, or DNS name.
Examples: 185.2.3.*., fwdr~*

[Learn more](#)

Exclude (excludelist)

Optional

Can be client name, host name, IP address, or DNS name.
Examples: ronnie, rarity

[Learn more](#)

Filter by Machine Type (machineTypesFilter)

Optional

[+](#)

[Cancel](#) [Preview](#) [Save](#)

All Matched Unmatched filter

1 10 Per Page ▾

Matched	Host Name	DNS Name	Client Name	Instance Name	IP Address	Machine Type	Phone Home
	DESKTOP-RMJL9A2	192.168.1.137	977894BC-6201-4C98-930B-968F87EE8D0B	DESKTOP-RMJL9A2	192.168.1.137	windows-x64	a minute ago



Figura 1.60: Añadir cliente

Y una vez agregado lo guardamos.



Edit Clients

Server Class: windows-aryan

Include (includelist)
DESKTOP-RM JL9A2

Exclude (excludelist)
Optional

Filter by Machine Type (machineTypesFilter)
Optional

Can be client name, host name, IP address, or DNS name.
Examples: 185.2.3.* , fwdr-*
[Learn more](#)

Can be client name, host name, IP address, or DNS name.
Examples: ronnie, rarity
[Learn more](#)

[Cancel](#) [Preview](#) **Save**

All Matched Unmatched filter

1 10 Per Page ▾

Matched	Host Name	DNS Name	Client Name	Instance Name	IP Address	Machine Type	Phone Home
	DESKTOP-RM JL9A2	192.168.1.137	977894BC-6201-4C98-930B-968F87EE8D0B	DESKTOP-RM JL9A2	192.168.1.137	windows-x64	a minute ago

Figura 1.61: Guardar cliente en el server class

Server Class: windows-aryan

[Edit](#) [Documentation](#)

[Back to Forwarder Management](#)

You haven't added any apps

[Add Apps](#)

Clients [Edit](#)

Phone Home: All ▾ All Clients ▾ filter

1 Clients 10 Per Page ▾

i	Host Name	Client Name	Instance Name	IP Address	Actions	Machine Type	Deployed Apps	Phone Home
>	DESKTOP-RM JL9A2	977894BC-6201-4C98-930B-968F87EE8D0B	DESKTOP-RM JL9A2	192.168.1.137	Delete Record	windows-x64	0 deployed	a few seconds ago

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.





Add Data



Explore Data



Monitoring
Console

Search settings...

🔍

<p>KNOWLEDGE</p> <p>Searches, reports, and alerts</p> <p>Data models</p> <p>Event types</p> <p>Tags</p> <p>Fields</p> <p>Lookups</p> <p>User interface</p> <p>Alert actions</p> <p>Advanced search</p> <p>All configurations</p>	<p>DATA</p> <p>Data inputs</p> <p>Forwarding and receiving</p> <p>Indexes</p> <p>Report acceleration summaries</p> <p>Virtual indexes</p> <p>Source types</p> <p>Ingest actions</p>
<p>DISTRIBUTED ENVIRONMENT</p> <p>Indexer clustering</p> <p>Forwarder management</p> <p>Federated search</p> <p>Distributed search</p>	
<p>SYSTEM</p> <p>Server settings</p> <p>Server controls</p> <p>Health report manager</p> <p>RapidDiag</p> <p>Instrumentation</p> <p>Licensing</p> <p>Workload management</p> <p>Mobile settings</p>	
<p>USERS AND AUTHENTICATION</p> <p>Roles</p> <p>Users</p> <p>Tokens</p> <p>Password management</p> <p>Authentication methods</p>	

Figura 1.63: Añadir datos

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



Cloud computing

Networking

Operating System

Security

4 data sources in total

Or get data in with the following methods

Upload files from my computer

Monitor files and ports on this Splunk platform instance

Forward data from a Splunk forwarder

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.

Add Data

Select Forwarders

Select Source

Input Settings

Review

Done

Next >

Select Forwarders

Create or select a server class for data inputs. Use this page only in a single-instance Splunk environment.

To enable forwarding of data from deployment clients to this instance, set the output configurations on your forwarders. [Learn More](#)

Select Server Class: New Existing

Server Class: windows-aryan

List of Forwarders: WINDOWS | DESKTOP-RMUL9A2

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.



Add Data

Select Forwarders Select Source Input Settings Review Done < Back Next >

Local Event Logs
Collect event logs from this machine.

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Local Performance Monitoring
Collect performance data from this machine.

Scripts
Get data from any API, service, or database with a script.

Splunk Assist Instance Identifier
Assigns a random identifier to every node

Systemd Journald Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.

Configure selected Splunk Universal Forwarders to monitor local Windows event log channels, which contain log data published by installed applications, services, and system processes. The event log monitor runs once for every event log input defined in the Splunk platform. [Learn More](#)

Select Event Logs Available item(s) add all > Selected item

Application
ForwardedEvents
Security
Setup
System

Select the Windows Event Logs you want to index from the list.

FAQ

> What event logs does this Splunk platform instance have access to?
> What is the best method for monitoring event logs of remote Windows machines?

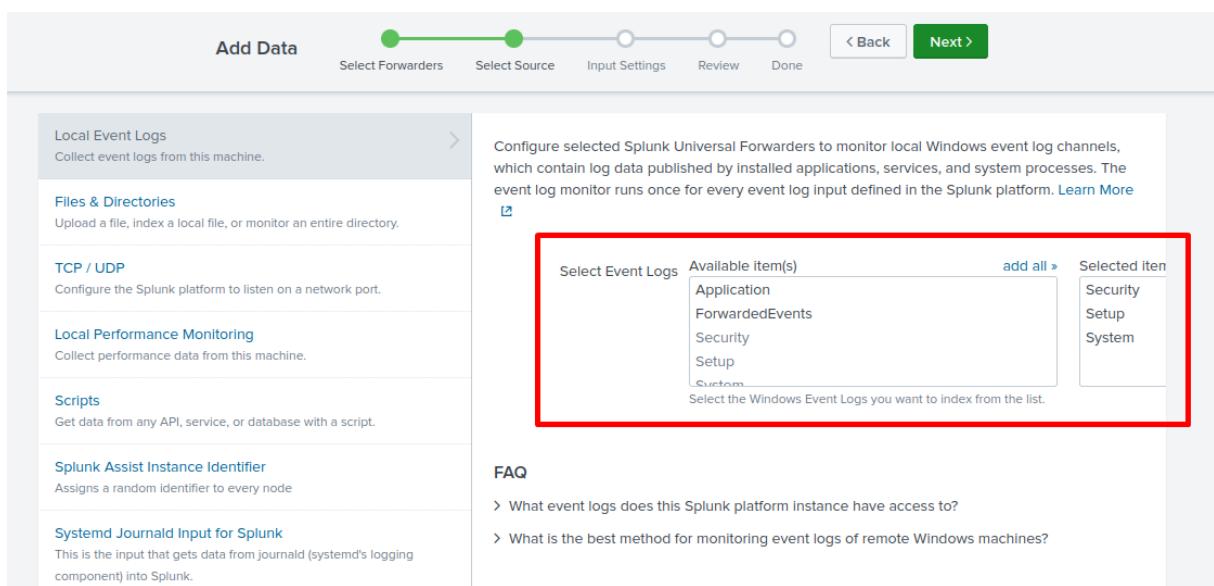


Figura 1.66: Elegir eventos para enviar

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.

Add Data

Select Forwarders Select Source Input Settings Review Done < Back Review >

Input Settings

Optionally set additional input parameters for this data input as follows:

Index

The Splunk platform stores incoming data as events in the selected Index. Consider using a "sandbox" index as a destination if you have problems determining a source type for your data. A sandbox index lets you troubleshoot your configuration without impacting production indexes. You can always change this setting later. [Learn More](#)

Index Create a new index

FAQ

> How do indexes work?
> How do I know when to create or use multiple indexes?

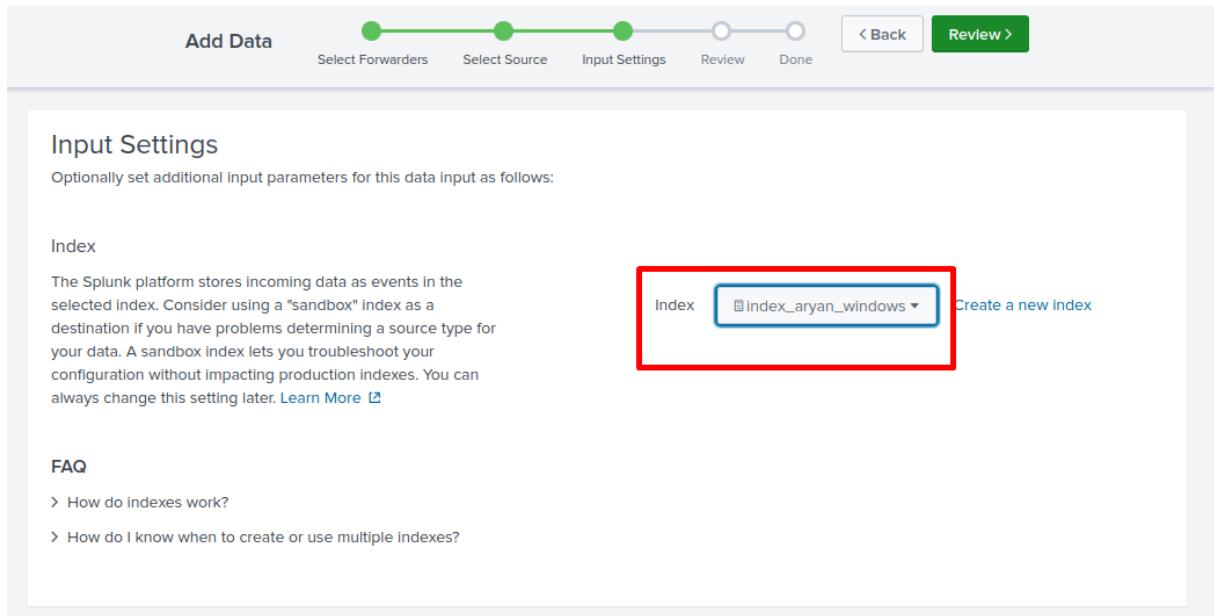


Figura 1.67: Elegir indexador para los eventos windows

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



Add Data

Review

Server Class Name windows-aryan
List of Forwarders WINDOWS | DESKTOP-RM JL9A2

Collection Name localhost
Input Type Windows Event Logs
Event Logs Security
Setup
System

Index index_aryan_windows

[Submit >](#)

Figura 1.68: Review

Add Data

Review

✓ Local event logs input has been created successfully.
Configure your inputs by going to Settings > [Data Inputs](#)

[Start Searching](#) Search your data now or see [examples and tutorials.](#)

[Add More Data](#) Add more data inputs now or see [examples and tutorials.](#)

[Download Apps](#) Apps help you do more with your data. [Learn more.](#)

[Build Dashboards](#) Visualize your searches. [Learn more.](#)

[Next >](#)

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.



index_aryan_windows	Edit	Delete	Disable	Events	search	1 MB	500 GB	1.07K	19 minutes ago	In 13 minutes	\$SPLUNK_DB/index_arya_n_windows/db	N/A
---------------------	------	--------	---------	--------	--------	------	--------	-------	----------------	---------------	-------------------------------------	-----

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 aquí ponemos en el buscador:

The screenshot shows the Splunk interface for a new search. The search bar contains the query `index=index_aryan_windows`. Below the search bar, it says `✓ 1,526 events (12/11/24 12:00:00.000 AM to 12/12/24 12:14:40.000 AM)`. The results table has a header row with columns `i`, `Time`, and `Event`. The first event listed is from 12/11/24 at 10:29:32.000 PM, with fields: host=DESKTOP-RMJL9A2, LogName=Security, EventCode=5379, EventType=0, ComputerName=DESKTOP-RMJL9A2, and source=WinEventLog:Security. The second event listed is also from 12/11/24 at 10:29:32.000 PM, with similar fields. The sidebar on the left shows selected fields like `host`, `source`, and `sourcetype`, and interesting fields like `ComputerName`, `Domino_de_la_cuenta`, `EventCode`, `EventType`, and `Id. de inicio de sesión`.

Figura 1.71: Eventos windows

Con esta búsqueda 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.



index="index_aryan_windows" EventCode=4624

Last 24 hours Search

✓ 97 events (12/11/24 12:00:00.000 AM to 12/12/24 12:16:57.000 AM) No Event Sampling ▾ Job ▾ II ■ ▾ Smart Mode ▾

Events (97) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection X Deselect 1 hour per column

List ▾ Format 20 Per Page ▾ 1 2 3 4 5 Next >

Time	Event
12/11/24 10:28:55 PM 10:28:55.000 PM	<p>LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-RMJL9A2 SourceName=Microsoft Windows security auditing. Type=Información RecordNumber=1740321 Keywords=Auditoría correcta TaskCategory=Logon OpCode=Información Message=Se INICIO sesion correctamente en una cuenta.</p> <p>Firmante: Id. de seguridad: S-1-5-18 Nombre de cuenta: DESKTOP-RMJL9A2\$ Dominio de cuenta: WORKGROUP Id. de inicio de sesión: 0x3E7</p>

Figura 1.72: Eventos login exitoso

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



```
Token elevado:           Sí
Nivel de suplantación:  Suplantación
Nuevo inicio de sesión:
  Id. de seguridad:      S-1-5-18
  Nombre de cuenta:       SYSTEM
  Dominio de cuenta:     NT AUTHORITY
  Id. de inicio de sesión: 0x3E7
  Inicio de sesión vinculado: 0x0
  Nombre de cuenta de red:   -
  Dominio de cuenta de red:  -
  GUID de inicio de sesión: {00000000-0000-0000-0000-000000000000}

Información de proceso:
  Id. de proceso:        0x2a4
  Nombre de proceso:     C:\Windows\System32\services.exe

Información de red:
  Nombre de estación de trabajo: -
  Dirección de red de origen:   -
  Puerto de origen:            -

Información de autenticación detallada:
  Proceso de inicio de sesión:  Advapi
  Paquete de autenticación:    Negotiate
  Servicios transitados:      -
  Nombre de paquete (solo NTLM): -
  Longitud de clave:          0
```

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 búsqueda 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 búsqueda lo que hacemos es filtrar los dos códigos de eventos y si es 4624 lo nombramos como exitoso y si no como fallido y los contamos.



New Search

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

✓ 82 events (12/10/24 10:00:00.000 PM to 12/11/24 10:08:44.000 PM) No Event Sampling ▾ Job ▾ II ■ ▶ 🔍 ⌂ Smart Mode ▾

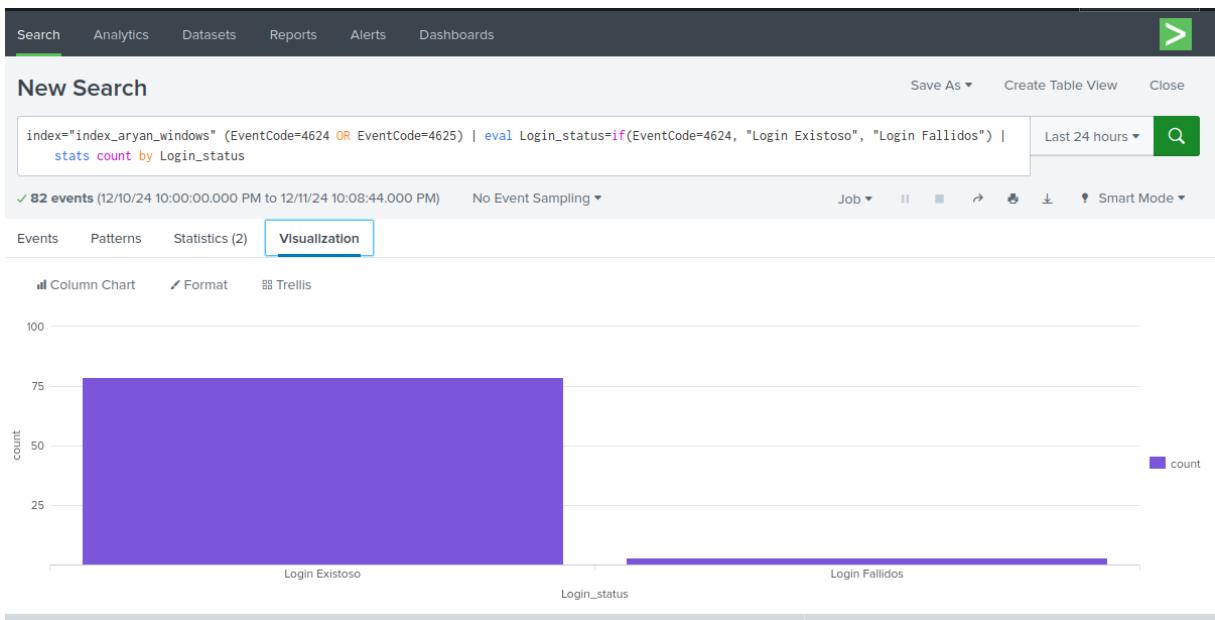
Events Patterns Statistics (2) Visualization

20 Per Page ▾ Format Preview ▾

Login_status	count
Login Existoso	79
Login Fallidos	3

Figura 1.74: Busqueda de los eventos

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



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

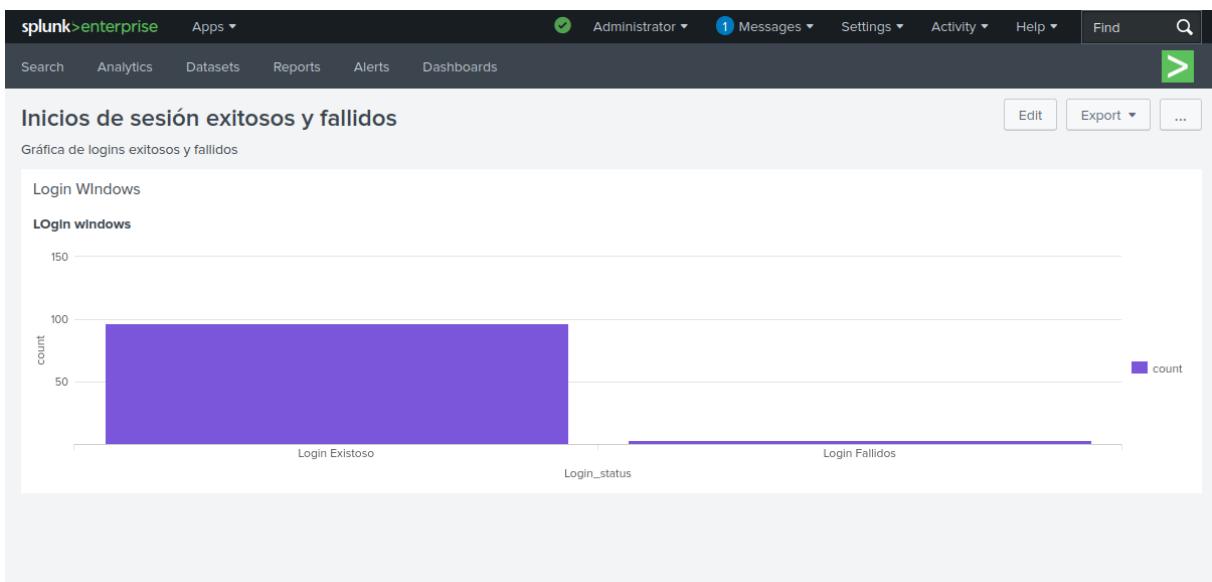


Figura 1.76: Eventos en grafica columnas windows en el dashboard

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

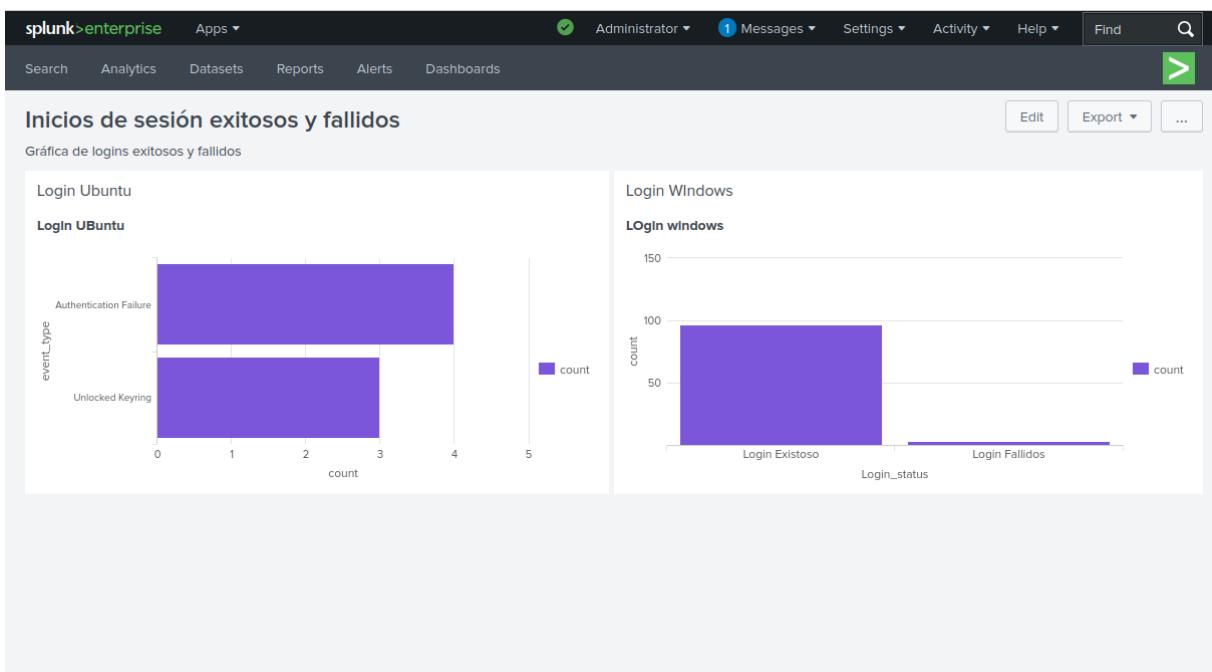


Figura 1.77: Eventos de los dos SO en el dashboard

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 así 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 envía datos entrantes a ElasticSearch.
- **Kibana:** Es una interfaz web para buscar y visualizar los registros.
- **Beats:** Es un transportador de datos ligeros de uso único que pueden enviar datos a cientos o miles de máquinas 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 ello 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.



Screenshot of the official Elasticsearch download page (<https://www.elastic.co/es/downloads/elasticsearch>) showing the "Download and unzip Elasticsearch" section.

1 Download and unzip Elasticsearch

Choose platform: Linux x86_64

Package managers: yum, dnf, or zypper, apt-get

Containers: Docker

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

License: Elastic License 2.0
[Elastic License 2.0](#)

Supported OS/JVM/Browser:
[Support Matrix](#)

Notes:
Running on Kubernetes? Try [Elastic Cloud on Kubernetes](#).
This default distribution is governed by the Elastic License, and includes the [full set of free features](#).

Want it hosted? Deploy on Elastic Cloud.

Figura 2.3: Pagina oficial ElasticSearch

Y seguiremos los pasos de la documentación oficial de Elasticsearch.



Screenshot of the official Elasticsearch documentation page for Debian package installation.

The page title is "Install Elasticsearch with Debian Package". It includes a note about bundled OpenJDK and Java version requirements. A sidebar on the left lists various Elasticsearch setup options, and a sidebar on the right provides links for importing PGP keys and managing clusters.

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-https paquete 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
```



```
aryan@ELK-aryan: $ wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo gpg --dearmor -o /usr/share/keyrings/elasticsearch-keyring.gpg
[sudo] contraseña para aryan:
aryan@ELK-aryan: $ sudo apt-get install apt-transport-https
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  apt-transport-https
  0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 3.974 B de archivos.
Se utilizarán 35,8 kB de espacio de disco adicional después de esta operación.
Des:1 http://es.archive.ubuntu.com/ubuntu noble/universe amd64 apt-transport-https all 2.7.14build2 [3.974 B]
Descargados 3.974 B en 0s (20,0 kB/s)
Seleccionando el paquete apt-transport-https previamente no seleccionado.
(Leyendo la base de datos ... 187760 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../apt-transport-https_2.7.14build2_all.deb ...
Desempaquetando apt-transport-https (2.7.14build2) ...
Configurando apt-transport-https (2.7.14build2) ...
aryan@ELK-aryan: $ 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
deb [signed-by=/usr/share/keyrings/elasticsearch-keyring.gpg] https://artifacts.elastic.co/packages/8.x/apt stable main
```

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
```

```
aryan@ELK-aryan:~$ sudo apt update && sudo apt upgrade -y
Obj:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Obj:2 https://artifacts.elastic.co/packages/8.x/apt stable InRelease
Obj:3 http://es.archive.ubuntu.com/ubuntu noble InRelease
Obj:4 http://es.archive.ubuntu.com/ubuntu noble-updates InRelease
Obj:5 http://es.archive.ubuntu.com/ubuntu noble-backports InRelease
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se pueden actualizar 3 paquetes. Ejecute «apt list --upgradable» para verlos.
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Calculando la actualización... Hecho
The following upgrades have been deferred due to phasing:
  python3-distupgrade ubuntu-release-upgrader-core ubuntu-release-upgrader-gtk
  0 actualizados, 0 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
```

Figura 2.6: Actualización de repositorios

Y ahora podremos instalar elasticsearch mediante apt install.

```
sudo apt install elasticsearch
```



```
aryan@ELK-aryan:~$ sudo apt install elasticsearch
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  elasticsearch
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 636 MB de archivos.
Se utilizarán 1.210 MB de espacio adicional después de esta operación.
Des:1 https://artifacts.elastic.co/packages/8.x/apt/stable/main amd64 elasticsearch amd64 8.17.0 [636 MB]
Descargados 636 MB en 30s (20,9 MB/s)
Seleccionando el paquete elasticsearch previamente no seleccionado.
(Leyendo la base de datos ... 187764 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../elasticsearch_8.17.0_amd64.deb ...
Creating elasticsearch group... OK
Creating elasticsearch user... OK
Desempaquetando elasticsearch (8.17.0) ...
Configurando elasticsearch (8.17.0) ...
Warning: The unit file, source configuration file or drop-ins of systemd-sysctl.service changed on disk. Run 'systemctl daemon-reload' to reload units.
----- Security autoconfiguration information -----
Authentication and authorization are enabled.
TLS for the transport and HTTP layers is enabled and configured.

The generated password for the elastic built-in superuser is : 7o00JbwIkQZfI*wg-5pV

If this node should join an existing cluster, you can reconfigure this with
'/usr/share/elasticsearch/bin/elasticsearch-reconfigure-node --enrollment-token <token-here>'
after creating an enrollment token on your existing cluster.

You can complete the following actions at any time:
```

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/
```

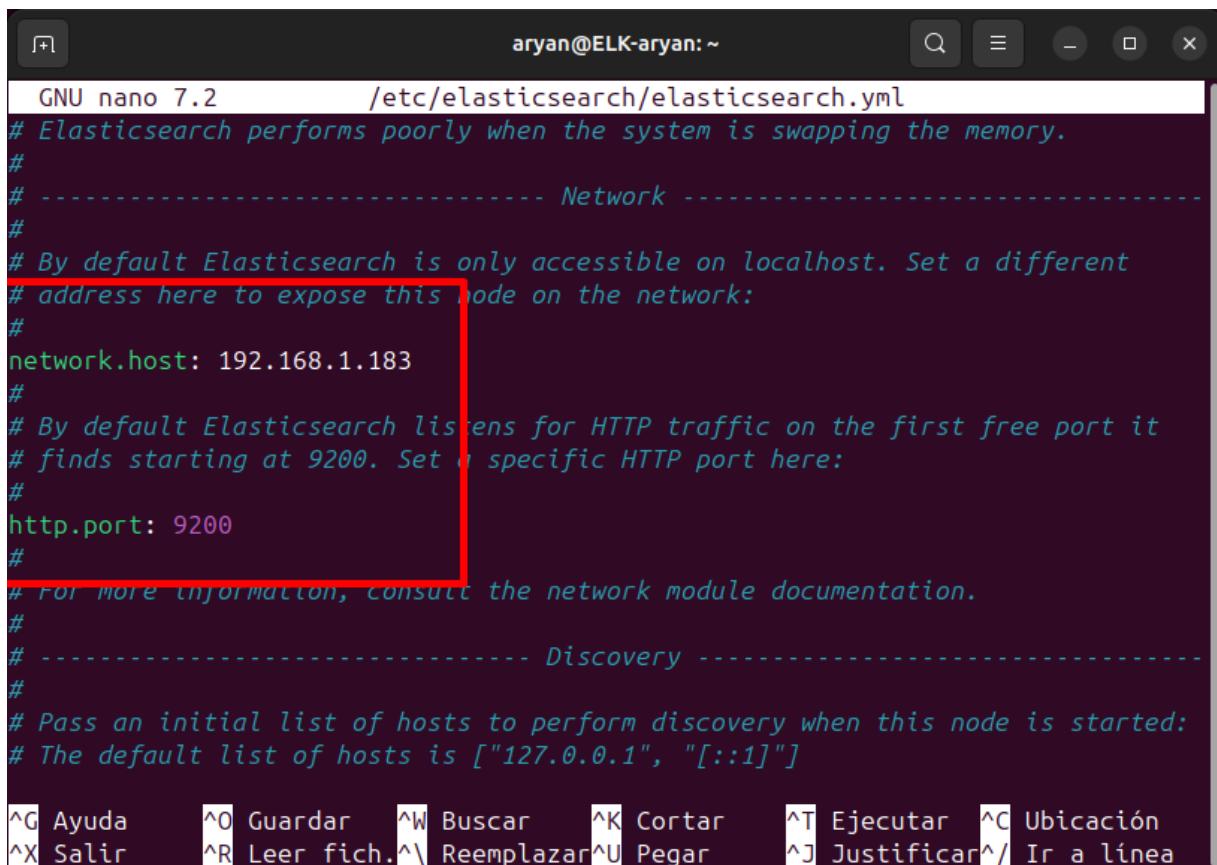
```
aryan@ELK-aryan:/etc/elasticsearch$ ls
certs          elasticsearch-plugins.example.yml    jvm.options      log4j2.properties  roles.yml   users_roles
elasticsearch.keystore  elasticsearch.yml           jvm.options.d    role_mapping.yml  users
aryan@ELK-aryan:/etc/elasticsearch$
```

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
```



```
aryan@ELK-aryan:~
```

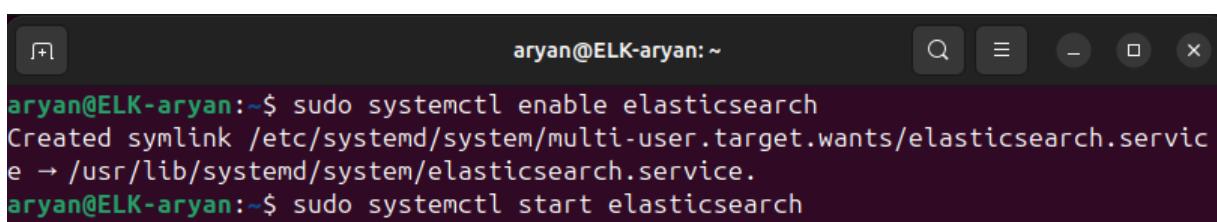
```
GNU nano 7.2          /etc/elasticsearch/elasticsearch.yml
# Elasticsearch performs poorly when the system is swapping the memory.
#
# ----- Network -----
#
# By default Elasticsearch is only accessible on localhost. Set a different
# address here to expose this node on the network:
#
network.host: 192.168.1.183
#
# By default Elasticsearch listens for HTTP traffic on the first free port it
# finds starting at 9200. Set a specific HTTP port here:
#
http.port: 9200
#
# For more information, consult the network module documentation.
#
# ----- Discovery -----
#
# Pass an initial list of hosts to perform discovery when this node is started:
# The default list of hosts is ["127.0.0.1", "[::1]"]

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

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
```



```
aryan@ELK-aryan:~$ sudo systemctl enable elasticsearch
Created symlink /etc/systemd/system/multi-user.target.wants/elasticsearch.service → /usr/lib/systemd/system/elasticsearch.service.
aryan@ELK-aryan:~$ 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
```

```
aryan@ELK-aryan:~$ sudo systemctl status elasticsearch.service
● elasticsearch.service - Elasticsearch
  Loaded: loaded (/usr/lib/systemd/system/elasticsearch.service; enabled; pr>
  Active: active (running) since Mon 2024-12-16 20:28:25 CET; 1min 34s ago
    Docs: https://www.elastic.co
   Main PID: 3144 (java)
     Tasks: 90 (limit: 4615)
    Memory: 2.4G (peak: 2.4G)
       CPU: 1min 43.635s
      CGroup: /system.slice/elasticsearch.service
              └─3144 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+U>
                ├ 3202 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.c>
                └─3225 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x>

dic 16 20:27:32 ELK-aryan systemd[1]: Starting elasticsearch.service - Elastics>
dic 16 20:27:46 ELK-aryan systemd-entrypoint[3202]: CompileCommand: dontinline >
dic 16 20:27:46 ELK-aryan systemd-entrypoint[3202]: CompileCommand: dontinline >
dic 16 20:28:25 ELK-aryan systemd[1]: Started elasticsearch.service - Elasticse>
lines 1-17/17 (END)
```

Figura 2.11: Estado de elasticsearch

```
aryan@ELK-aryan:~$ curl --cacert /etc/elasticsearch/certs/http_ca.crt -u elastic:7o00JbwIkQZfI*wg-5pV https://localhost:9200
{
  "name" : "ELK-aryan",
  "cluster_name" : "elasticsearch",
  "cluster_uuid" : "RsyjBKJPTxaLOJVUjQIW4A",
  "version" : {
    "number" : "8.17.0",
    "build_flavor" : "default",
    "build_type" : "deb",
    "build_hash" : "2b6a7fed44faa321997703718f07ee0420804b41",
    "build_date" : "2024-12-11T12:08:05.663969764Z",
    "build_snapshot" : false,
    "lucene_version" : "9.12.0",
    "minimum_wire_compatibility_version" : "7.17.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "You Know, for Search"
}
```

Figura 2.12: Elasticsearch

Introducinedo esta url podremos acceder desde le navegador.



```
https://elastic:7o00JbwIkQZfI*wg-5pV@localhost:9200
```

A screenshot of a web browser window displaying the Elasticsearch cluster state in JSON format. The URL in the address bar is https://localhost:9200. The browser interface includes a header with tabs for 'JSON', 'Datos sin procesar', and 'Cabeceras', and buttons for 'Guardar', 'Copiar', 'Contraer todo', 'Expandir todo', and 'Filtrar JSON'. The main content area shows the following JSON data:

```
name: "ELK-aryan"
cluster_name: "elasticsearch"
cluster_uuid: "RsyjBKJPTxaLOJVUjQIW4A"
version:
  number: "8.17.0"
  build_flavor: "default"
  build_type: "deb"
  build_hash: "2b6a7fed44faa321997703718f07ee0420804b41"
  build_date: "2024-12-11T12:08:05.663969764Z"
  build_snapshot: false
  lucene_version: "9.12.0"
  minimum_wire_compatibility_version: "7.17.0"
  minimum_index_compatibility_version: "7.0.0"
tagline: "You Know, for Search"
```

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
```



```
aryan@ELK-aryan:~$ sudo apt install kibana
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se actualizan los siguientes paquetes:
  kibana
1 actualizados, 0 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
1 no instalados del todo o eliminados.
Se necesita descargar 0 B/345 MB de archivos.
Se utilizarán 1.037 MB de espacio de disco adicional después de esta operación.
(Leyendo la base de datos ... 189288 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../kibana_8.17.0_amd64.deb ...
Desempaquetando kibana (8.17.0) sobre (8.17.0) ...
Configurando kibana (8.17.0) ...
Creating kibana group... OK
Creating kibana user... OK
Kibana is currently running with legacy OpenSSL providers enabled! For details and instructions on how to disable see https://www.elastic.co/guide/en/kibana/8.17/production.html#openssl-legacy-provider
Created Kibana keystore in /etc/kibana/kibana.keystore
aryan@ELK-aryan:~$
```

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
```

```
aryan@ELK-aryan:~$ sudo systemctl enable kibana
[sudo] contraseña para aryan:
Created symlink /etc/systemd/system/multi-user.target.wants/kibana.service → /usr/lib/systemd/system/kibana.service.
aryan@ELK-aryan:~$ sudo systemctl start kibana
aryan@ELK-aryan:~$ sudo systemctl status kibana
● kibana.service - Kibana
   Loaded: loaded (/usr/lib/systemd/system/kibana.service; enabled; preset: enabled)
   Active: active (running) since Mon 2024-12-16 21:05:48 CET; 15s ago
     Docs: https://www.elastic.co
 Main PID: 3466 (node)
    Tasks: 11 (limit: 4615)
   Memory: 229.3M (peak: 260.4M)
      CPU: 12.923s
     CGroup: /system.slice/kibana.service
             └─3466 /usr/share/kibana/bin/../node/glibc-217/bin/node /usr/share/kibana/bin/../src/cli/dist

dic 16 21:05:48 ELK-aryan systemd[1]: Started kibana.service - Kibana.
dic 16 21:05:48 ELK-aryan kibana[3466]: Kibana is currently running with legacy OpenSSL providers enabled! For details >
dic 16 21:05:50 ELK-aryan kibana[3466]: {"log.level": "info", "@timestamp": "2024-12-16T20:05:50.898Z", "log.logger": "elast>
dic 16 21:05:51 ELK-aryan kibana[3466]: Native global console methods have been overridden in production environment.
dic 16 21:05:56 ELK-aryan kibana[3466]: [2024-12-16T21:05:56.677+01:00][INFO ][root] Kibana is starting
dic 16 21:05:56 ELK-aryan kibana[3466]: [2024-12-16T21:05:56.755+01:00][INFO ][node] Kibana process configured with rol>
lines 1-17/17 (END)
```

Figura 2.15: Arranque y Estado de Kibana

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



```
aryan@ELK-aryan:~
```

```
GNU nano 7.2 /etc/kibana/kibana.yml
# For more configuration options see the configuration guide for Kibana in
# https://www.elastic.co/guide/index.html

# ===== System: Kibana Server =====
# Kibana is served by a back end server. This setting specifies the port to use.
server.port: 5601

# Specifies the address to which the Kibana server will bind. IP addresses and host names are both valid values.
# The default is 'localhost', which usually means remote machines will not be able to connect.
# To allow connections from remote users, set this parameter to a non-loopback address.
server.host: "192.168.1.183"
```

Figura 2.16: Archivo de configuración de Kibana

```
aryan@ELK-aryan:~
```

```
GNU nano 7.2 /etc/kibana/kibana.yml
#server.rewriteBasePath: false

# Specifies the public URL at which Kibana is available for end users. If
# 'server.basePath' is configured this URL should end with the same basePath.
#server.publicBaseUrl: ""

# The maximum payload size in bytes for incoming server requests.
#server.maxPayload: 1048576

# The Kibana server's name. This is used for display purposes.
#server.name: "your-hostname"

# ===== System: Kibana Server (Optional) =====
# Enables SSL and paths to the PEM-format SSL certificate and SSL key files, respectively.
# These settings enable SSL for outgoing requests from the Kibana server to the browser.
#server.ssl.enabled: false
#server.ssl.certificate: /path/to/your/server.crt
#server.ssl.key: /path/to/your/server.key

# ===== System: Elasticsearch =====
# The URLs of the Elasticsearch instances to use for all your queries.
elasticsearch.hosts: ["http://localhost:9200"]

# If your Elasticsearch is protected with basic authentication, these settings provide
```

Figura 2.17: Archivo de configuración de Kibana

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

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

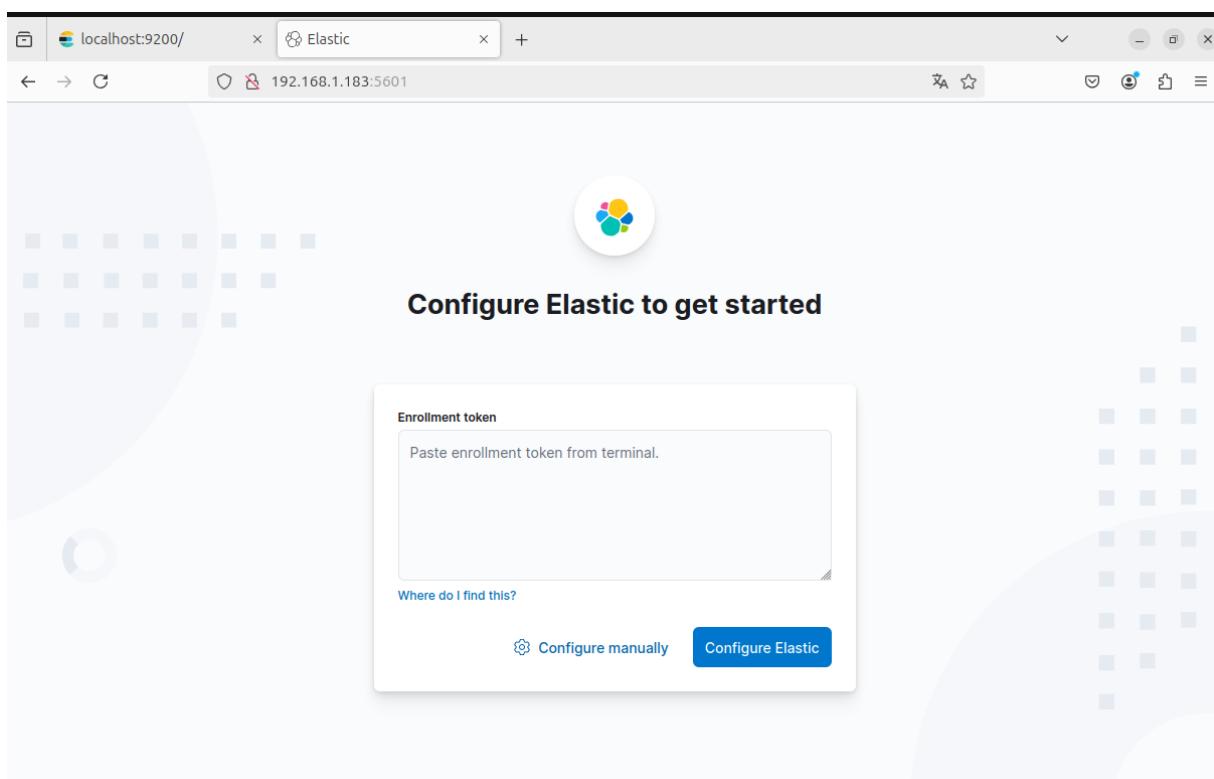


Figura 2.18: Kibana desde el navegador

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.

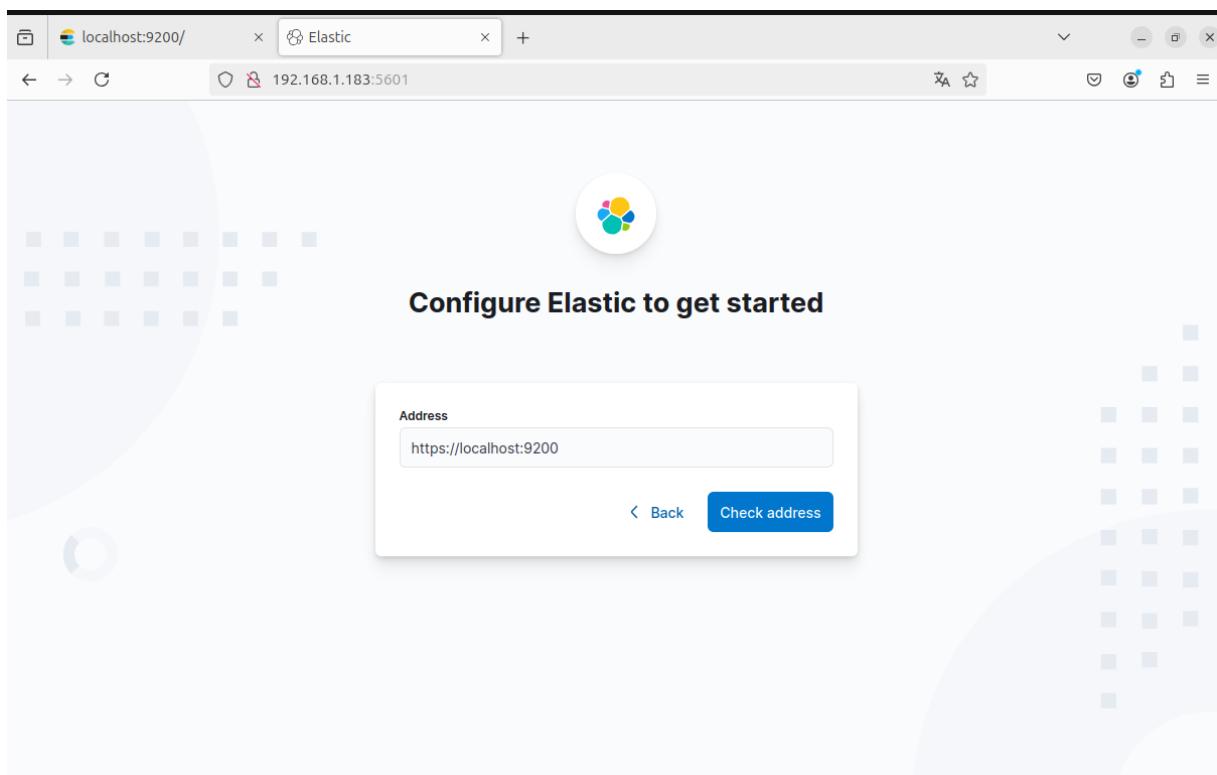


Figura 2.19: Kibana web paso dos

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

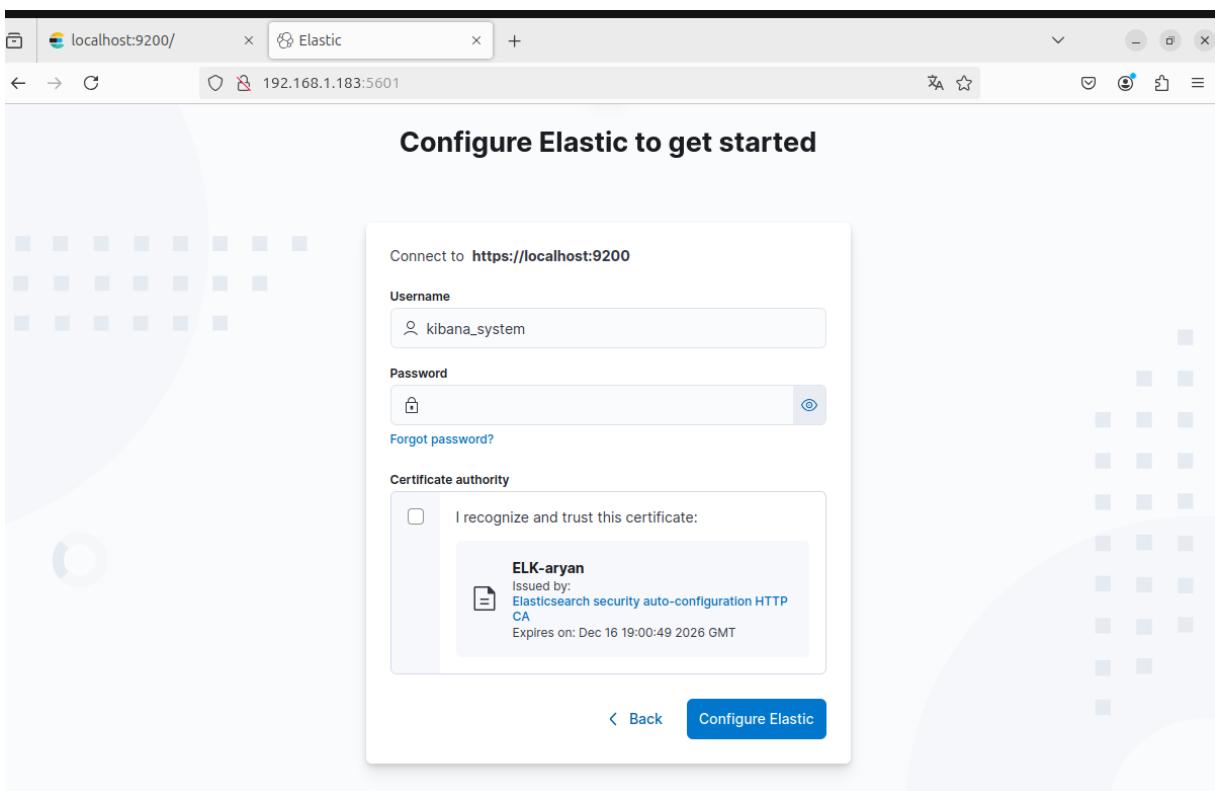


Figura 2.20: Kibana login

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
```

```
aryan@ELK-aryan:~$ sudo /usr/share/elasticsearch/bin/elasticsearch-reset-password -u kibana_system --url https://localhost:9200 -f  
This tool will reset the password of the [kibana_system] user to an autogenerated value.  
The password will be printed in the console.  
Please confirm that you would like to continue [y/N]Y  
  
Password for the [kibana_system] user successfully reset.  
New value: E00iyUc75T2FJoQ0pwZu  
aryan@ELK-aryan:~$
```

Figura 2.21: Kibana password

Luego marcaremos el certificado y haremos clic sobre Configure Elastic.

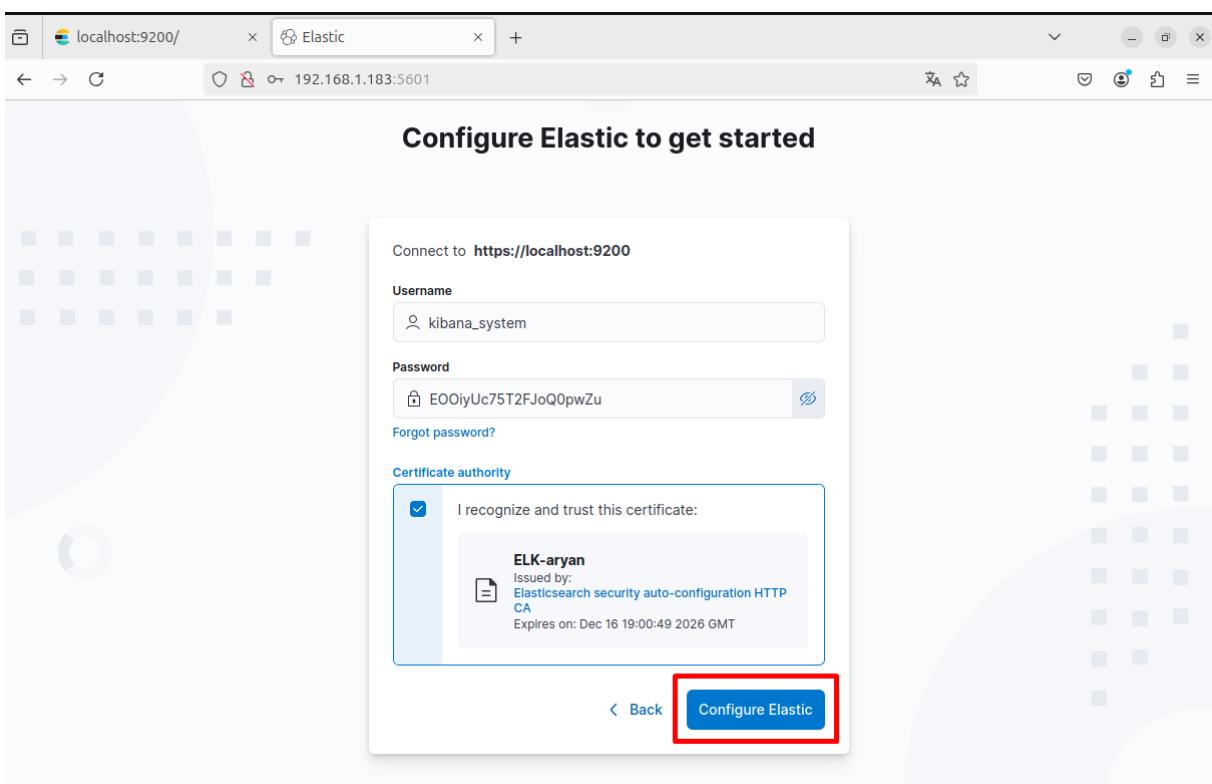


Figura 2.22: Kibana

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



X



Verification required

Copy the code from the Kibana server or run `bin/kibana-verification-code` to retrieve it.

Figura 2.23: Kibana codigo

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

```
aryan@ELK-aryan:/usr/share/kibana/bin$ sudo ./kibana-verification-code
Your verification code is: 425 842
```

Figura 2.24: Kibana codigo

Y ahora accederemos después de introducir el código de verificación.



X



Verification required

Copy the code from the Kibana server or run `bin/kibana-verification-code` to retrieve it.

4

2

5

8

4

2|

Verify

Figura 2.25: Kibana codigo

Y empezará iniciar la cnfiguracion

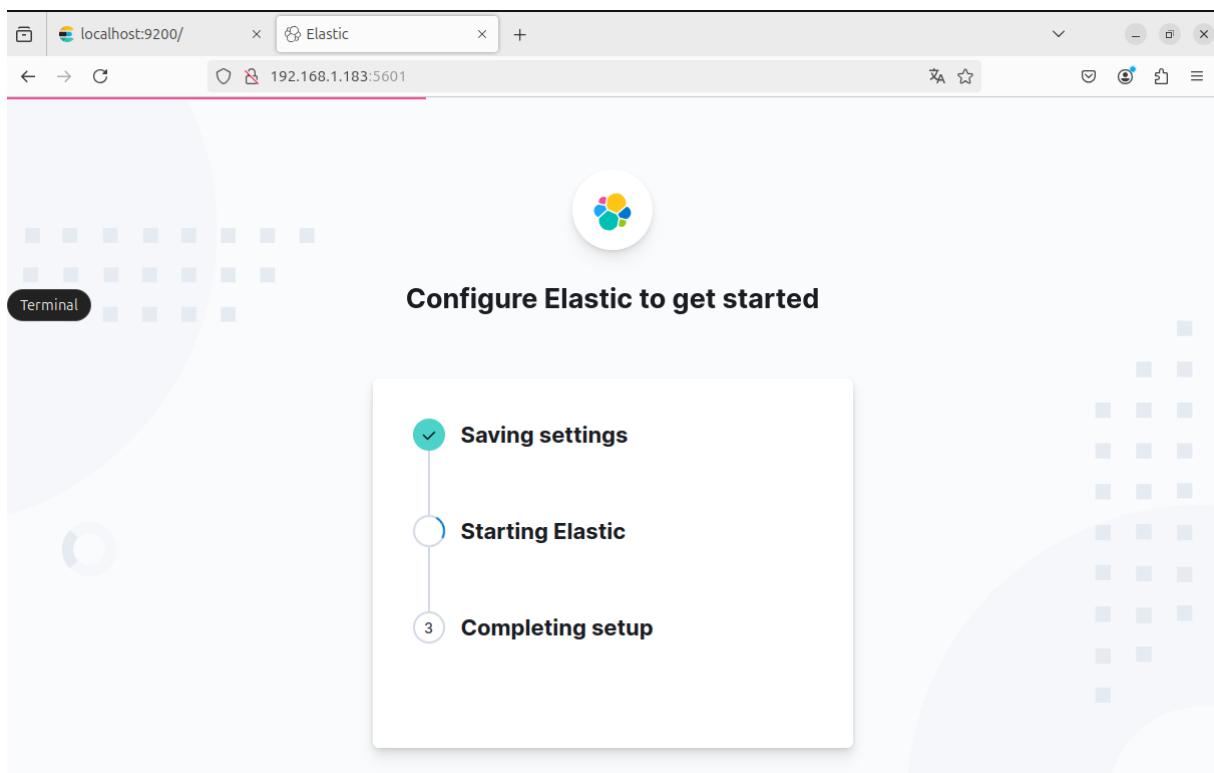


Figura 2.26: Kibana código

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

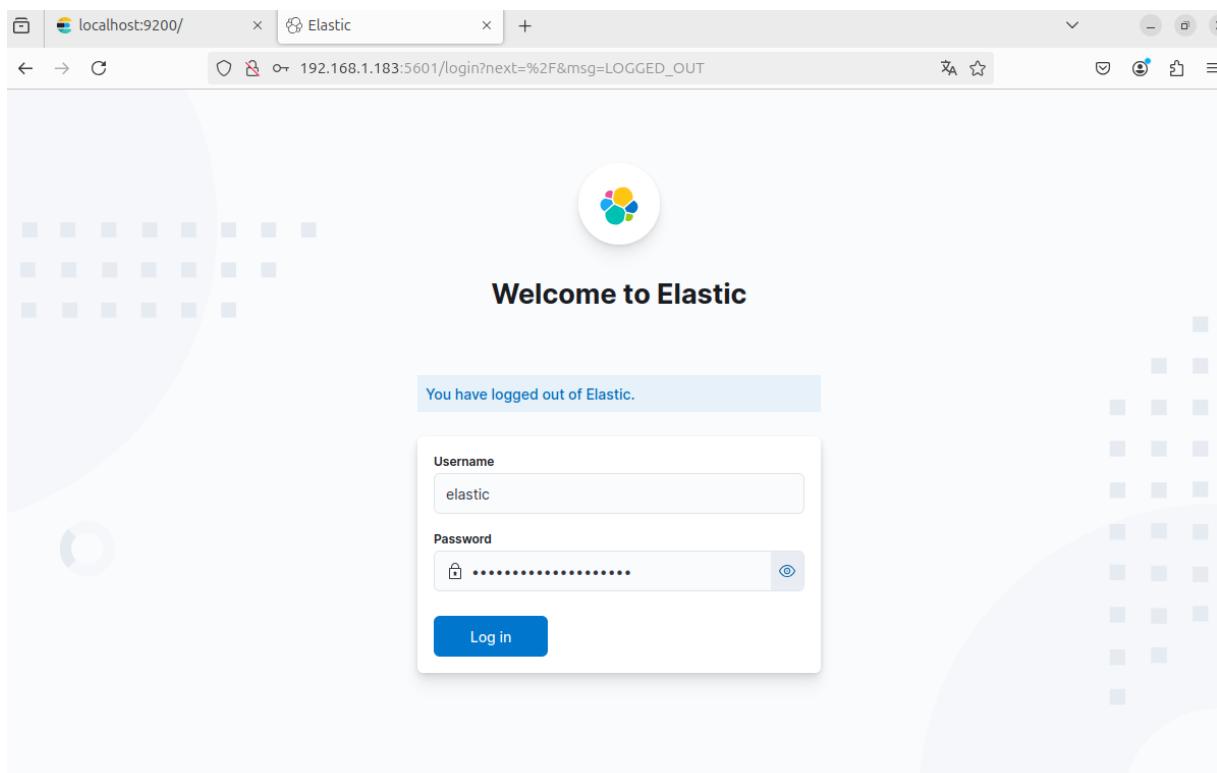


Figura 2.27: Elastic en Kibana

Welcome home

Elasticsearch
Create search experiences with a refined set of APIs and tools.

Observability
Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security
Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

Analytics
Explore, visualize, and analyze your data using a powerful suite of analytical tools and applications.

Get started by adding integrations
To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to

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

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
```

```
aryan@ELK-aryan:~$ sudo apt install logstash
Leyendo lista de paquetes... Hecho
Creando árbol de dependencias... Hecho
Leyendo la información de estado... Hecho
Se instalarán los siguientes paquetes NUEVOS:
  logstash
0 actualizados, 1 nuevos se instalarán, 0 para eliminar y 3 no actualizados.
Se necesita descargar 431 MB de archivos.
Se utilizarán 708 MB de espacio de disco adicional después de esta operación.
Des:1 https://artifacts.elastic.co/packages/8.x/apt/stable/main amd64 logstash amd64 1:8.17.0-1 [431 MB]
Descargados 431 MB en 24s (17,8 MB/s)
Seleccionando el paquete logstash previamente no seleccionado.
(Leyendo la base de datos ... 292223 ficheros o directorios instalados actualmente.)
Preparando para desempaquetar .../logstash_1%3a8.17.0-1_amd64.deb ...
Desempaquetando logstash (1:8.17.0-1) ...
Configurando logstash (1:8.17.0-1) ...
aryan@ELK-aryan:~$
```

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 arquitectura 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.



Filebeat Reference: [8.17 \(current\)](#)

Elastic Docs > Filebeat Reference [8.17]

Filebeat quick start: installation and configuration

This guide describes how to get started quickly with log collection. You'll learn how to:

- install Filebeat on each system you want to monitor
- specify the location of your log files
- parse log data into fields and send it to Elasticsearch
- visualize the log data in Kibana

On this page

- Before you begin
 - Step 1: Install Filebeat
 - Other installation options
- Step 2: Connect to the Elastic Stack
- Step 3: Collect log data
 - Enable and configure data collection modules
 - Enable and configure ECS loggers for application log collection
 - Configure Filebeat manually
- Step 4: Set up assets
- Step 5: Start Filebeat

Most Popular

VIDEO [Get Started with Elasticsearch](#)

VIDEO [Intro to Kibana](#)

VIDEO [ELK for Logs & Metrics](#)

Was this helpful? [Upvote](#) [Downvote](#)

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
```

```
aryan@ubuntu-aryan:~$ curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.17.0-amd64.deb  
% Total    % Received % Xferd  Average Speed   Time      Time     Current  
          Dload  Upload   Total Spent  Left  Speed  
100 53.3M  100 53.3M    0     0  8420k      0:00:06  0:00:06  ---:--- 10.2M  
aryan@ubuntu-aryan:~$ sudo dpkg -i filebeat-8.17.0-amd64.deb  
Seleccionando el paquete filebeat previamente no seleccionado.  
(Leyendo la base de datos ... 186696 ficheros o directorios instalados actualmente.)  
Preparando para desempaquetar filebeat-8.17.0-amd64.deb ...  
Desempaquetando filebeat (8.17.0) ...  
Configurando filebeat (8.17.0) ...  
aryan@ubuntu-aryan:~$
```

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:

```
aryan@ubuntu-aryan:~  
GNU nano 7.2 /etc/filebeat/filebeat.yml  
# Performance preset - one of "balanced", "throughput", "scale",  
# "latency", or "custom".  
#preset: balanced  
  
# Protocol - either `http` (default) or `https`.  
#protocol: "https"  
  
# Authentication credentials - either API key or username/password.  
#api_key: "id:api_key"  
#username: "elastic"  
#password: "7o00JbwIkQZfI*wg-5pV"  
  
# ----- Logstash Output -----  
output.logstash:  
  # The Logstash hosts  
  hosts: ["192.168.1.183:5044"]  
  
  # Optional SSL. By default is off.  
  # List of root certificates for HTTPS server verifications  
  #ssl.certificateAuthorities: ["/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"  
  
# ===== Processors =====
```

Figura 2.32: Conexión logstash y Filebeat

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



```
aryan@ubuntu-aryan:~
```

```
GNU nano 7.2
```

```
/etc/filebeat/filebeat.yml *
```

```
# You can find the full configuration reference here:  
# https://www.elastic.co/guide/en/beats/filebeat/index.html
```

```
# For more available modules and options, please see the filebeat.reference.yml sample  
# configuration file.
```

```
# ===== Filebeat inputs =====
```

```
filebeat.inputs:
```

```
# Each - is an input. Most options can be set at the input level, so  
# you can use different inputs for various configurations.  
# Below are the input-specific configurations.
```

```
# filestream is an input for collecting log messages from files.  
- type: filestream
```

```
# Unique ID among all inputs, an ID is required.  
id: my-filestream-id
```

```
# Change to true to enable this input configuration.  
enabled: true
```

```
# Paths that should be crawled and fetched. Glob based paths.  
paths:  
- /var/log/auth.log  
#- /var/log/*.*.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
```

```
aryan@ubuntu-aryan:~$ sudo service filebeat restart  
aryan@ubuntu-aryan:~$ sudo service filebeat status
```

```
● filebeat.service - Filebeat sends log files to Logstash or directly to Elasticsearch.  
  Loaded: loaded (/usr/lib/systemd/system/filebeat.service; disabled; preset: enabled)  
  Active: active (running) since Tue 2024-12-17 23:02:17 CET; 2s ago  
    Docs: https://www.elastic.co/beats/filebeat  
   Main PID: 17200 (filebeat)  
     Tasks: 8 (limit: 4615)  
    Memory: 37.4M (peak: 37.8M)  
      CPU: 356ms  
     CGroup: /system.slice/filebeat.service  
             └─17200 /usr/share/filebeat/bin/filebeat --environment systemd -c /etc/filebeat/filebeat.yml --path.home />
```

```
dic 17 23:02:17 ubuntu-aryan filebeat[17200]: {"log.level":"info","@timestamp":"2024-12-17T23:02:17.426+0100","log.orig>  
dic 17 23:02:17 ubuntu-aryan filebeat[17200]: {"log.level":"info","@timestamp":"2024-12-17T23:02:17.436+0100","log.orig>  
dic 17 23:02:17 ubuntu-aryan filebeat[17200]: {"log.level":"warn","@timestamp":"2024-12-17T23:02:17.437+0100","log.orig>  
dic 17 23:02:17 ubuntu-aryan filebeat[17200]: {"log.level":"info","@timestamp":"2024-12-17T23:02:17.437+0100","log.logg>  
dic 17 23:02:17 ubuntu-aryan filebeat[17200]: {"log.level":"info","@timestamp":"2024-12-17T23:02:17.437+0100","log.logg>  
dic 17 23:02:17 ubuntu-aryan filebeat[17200]: {"log.level":"info","@timestamp":"2024-12-17T23:02:17.437+0100","log.logg>  
dic 17 23:02:17 ubuntu-aryan filebeat[17200]: {"log.level":"info","@timestamp":"2024-12-17T23:02:17.438+0100","log.logg>  
dic 17 23:02:17 ubuntu-aryan filebeat[17200]: {"log.level":"info","@timestamp":"2024-12-17T23:02:17.438+0100","log.orig>  
dic 17 23:02:17 ubuntu-aryan filebeat[17200]: {"log.level":"info","@timestamp":"2024-12-17T23:02:17.439+0100","log.orig>
```

```
[lines 1-21/21 (END)]
```

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 archivo de configuración:

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

E introducimos lo siguiente:

```
aryan@ELK-aryan:~
```

```
GNU nano 7.2
```

```
/etc/logstash/conf.d/pipeline_ubuntu.conf
```

```
input {  
  beats {  
    port => 5044  
  }  
}  
  
output {  
  elasticsearch {  
    hosts => ["https://localhost:9200"]  
    index => "filebeat-ubuntu"  
    user => "elastic"  
    password => "7o00JbwIkQZfI*wg-5pV"  
    ssl => true  
    cacert => "/etc/elasticsearch/certs/http_ca.crt"  
  }  
}
```

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
```



```
aryan@ELK-aryan:~$ sudo systemctl start logstash
[sudo] contraseña para aryan:
aryan@ELK-aryan:~$ sudo systemctl status logstash
● logstash.service - logstash
   Loaded: loaded (/usr/lib/systemd/system/logstash.service; disabled; preset>
   Active: active (running) since Tue 2024-12-17 23:12:45 CET; 5s ago
     Main PID: 4070 (java)
        Tasks: 20 (limit: 4615)
       Memory: 250.5M (peak: 250.9M)
          CPU: 6.429s
         CGroup: /system.slice/logstash.service
                   └─4070 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.h>

dic 17 23:12:45 ELK-aryan systemd[1]: Started logstash.service - logstash.
dic 17 23:12:45 ELK-aryan logstash[4070]: Using bundled JDK: /usr/share/logstas>
lines 1-12/12 (END)
```

Figura 2.36: Estado de logstash

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

```
sudo filebeat test output
```

```
aryan@ubuntu-aryan:~$ sudo filebeat test output
logstash: 192.168.1.183:5044...
connection...
  parse host... OK
  dns lookup... OK
  addresses: 192.168.1.183
  dial up... OK
  TLS... WARN secure connection disabled
  talk to server... OK
```

Figura 2.37: Conexión de Filebeat - logstash

2.6.1. Confirmar que los datos llegan

Ahora que tenemos 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:7o00JbwIkQZfI*wg-5pV --cacert  
/etc/elasticsearch/certs/http_ca.crt  
https://localhost:9200/\_cat/indices/filebeat-\*?v=true
```

```
aryan@ELK-aryan:~$ curl -u elastic:7o00JbwIkQZfI*wg-5pV --cacert /etc/elasticsearch/certs/http_ca.crt https://localhost:  
9200/_cat/indices/filebeat-*?v=true  
health status index          uuid                           pri rep docs.count docs.deleted store.size pri.store.size dataset.size  
yellow open   filebeat-ubuntu DMjMPY_6Sva0ZEomkVyK8A 1 1      285      0    255kb      255kb      25  
5kb  
aryan@ELK-aryan:~$
```

Figura 2.38: Datos en elasticsearch recibidos

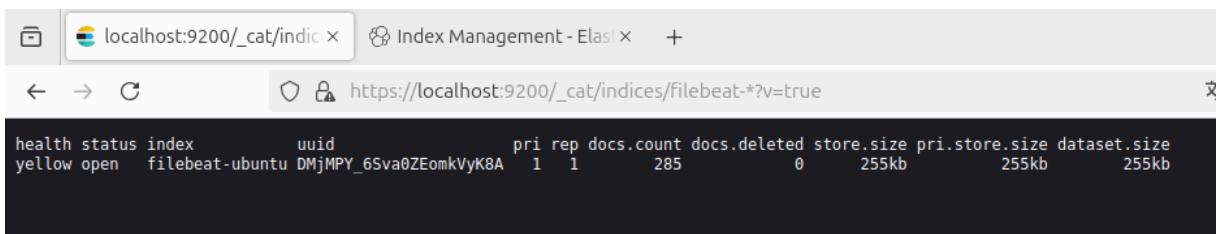


Figura 2.39: Datos en elasticsearch recibidos vistos en el navegador

En estas imágenes podemos ver como la conexión entre Filebeat ->Logstash ->Elasticsearch es correcta. Ya que los datos se han enviado automaticamente 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.



The screenshot shows the Elastic Stack interface at `localhost:9200/_cat/indices`. The left sidebar has sections for Analytics (Discover, Dashboards, Canvas, Maps, Machine Learning, Visualize Library) and Elasticsearch (Overview, Content, Elasticsearch, Vector Search, Semantic Search). A red box highlights the 'Discover' link. The main area features cards for Observability, Security, and Analytics. The 'Analytics' card is also highlighted with a red box. A callout box points to the 'Discover' link in the sidebar.

Figura 2.40: Discover

Después le daremos a create data view.

The screenshot shows a section titled 'How do you want to explore your Elasticsearch data?'. It contains two main options: 'Create a data view' and 'Query your data with ES|QL'. The 'Create a data view' section includes a description of what data views are and a 'Create data view' button, which is highlighted with a red box. The 'Query your data with ES|QL' section includes a description of the ES|QL language and a 'Try ES|QL' button. Both sections have 'Want to learn more? Read the docs' links.

Figura 2.41: Create new dataview



Edit data view
Manage settings and view field details

Name
Inicios de sesion fallidos y exitosos

Index pattern
filebeat-ubuntu

Timestamp field
@timestamp

Select a timestamp field for use with the global time filter.

Show advanced settings

✓ Your index pattern matches 1 source.

All sources Matching sources

filebeat-ubuntu Index

Rows per page: 10

X Close Save

Figura 2.42: Create new dataview

Lo llamaremos inicios de sesion fallidos y exitosos y usaremos el indice 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.



Screenshot of the Elasticsearch Discover interface showing a list of 287 events. The left sidebar shows available fields like @timestamp, @version, agent.id, etc. A red box highlights the 'Available fields' section. The main area shows event details with a checkbox for each entry. One specific event is selected, indicated by a red box around its timestamp.

Figura 2.43: Análisis eventos

Si ampliamos podremos ver mucha información de los eventos.

Screenshot of the Elasticsearch Discover interface showing a detailed view of an event. The left sidebar shows popular and available fields. The main area shows the selected event's details in JSON format. The 'event.original' field is highlighted with a red box, showing the raw log entry.

Field	Value
agent.version	8.17.0
ecs.version	8.0.0
event.original	2024-12-18T02:49:46.120600+01:00 ubuntu-arian (systemd): pam_unix(systemd-user:session): session opened for user aryan(uid=1000) by aryan(uid=0)
host.architecture	x86_64
host.containerized	false
host.hostname	ubuntu-arian
host.id	0c01c811-405f-4dab-aed8-f054fe235c74

Figura 2.44: Información de Análisis eventos



Ahora vamos a usar los campos que nos interesen para así poder ver los eventos más claros.

checkbox	host.hostname	@timestamp	event.original	host.hostname
<input type="checkbox"/>	ubuntu-aryan	Dec 18, 2024 04:33:01.711	2024-12-18T04:32:57.593624+01:00 ubuntu-aryan gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname=aryan uid=0 ...	ubuntu-aryan
<input type="checkbox"/>	ubuntu-aryan	Dec 18, 2024 04:33:01.711	2024-12-18T04:33:01.314495+01:00 ubuntu-aryan gdm-password]: gkr-pam: unlocked login keyring	ubuntu-aryan
<input type="checkbox"/>	ubuntu-aryan	Dec 18, 2024 04:32:49.695	2024-12-18T04:32:47.507375+01:00 ubuntu-aryan gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname=aryan uid=0 ...	ubuntu-aryan
<input type="checkbox"/>	ubuntu-aryan	Dec 18, 2024 04:32:55.709	2024-12-18T04:32:54.468543+01:00 ubuntu-aryan gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname=aryan uid=0 ...	ubuntu-aryan
<input type="checkbox"/>	ubuntu-aryan	Dec 18, 2024 04:32:55.708	2024-12-18T04:32:51.160083+01:00 ubuntu-aryan gdm-password]: pam_unix(gdm-password:auth): authentication failure; logname=aryan uid=0 ...	ubuntu-aryan
<input type="checkbox"/>	ubuntu-aryan	Dec 18, 2024 04:25:09.694	2024-12-18T04:25:01.668353+01:00 ubuntu-aryan CRON[5392]: pam_unix(cron:session): session opened for user root(uid=0) by root(uid=0)	ubuntu-aryan
<input type="checkbox"/>	ubuntu-aryan	Dec 18, 2024 04:25:00.605	2024-12-18T04:25:01.681302+01:00 ubuntu-aryan CRON[5392]: pam_unix(cron:session): session	ubuntu-aryan

Figura 2.45: Información de Análisis de 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.



The screenshot shows the Elasticsearch Discover interface with the following details:

- Header:** Shows the URL as `localhost:9200/_search/_discover` and the page title as "Discover - Elasticsearch".
- Search Bar:** Contains the placeholder "Find apps, content, and more...".
- Toolbar:** Includes "Try ES|QL", "Inspect", "Alerts", "Save", and other navigation icons.
- Data View:** Set to "Inicios de sesion fallidos y exitosos".
- Filter Bar:** Shows a search input "Filter your data using KQL syntax".
- Left Panel:** A sidebar titled "Search field names" lists various fields like host.os.kernel, host.os.name, etc., with some entries under "Empty fields". A red box highlights the "Add a field" button at the bottom of this panel.
- Table:** Titled "Field statistics" (381 documents), showing the following data:

Name	Documents (%)	Distinct values	Distributions	Actions
@timestamp	381 (100%)	73	○	edit
@version	381 (38.1%)	1	○	edit
@version.keyword	381 (100%)	1	○	edit
agent.ephemeral_id	381 (38.1%)	2	○	edit
agent.ephemeral_id.keyword	381 (100%)	2	○	edit
agent.id	381 (38.1%)	1	○	edit
agent.id.keyword	381 (100%)	1	○	edit
agent.name	381 (38.1%)	1	○	edit
agent.name.keyword	381 (100%)	1	○	edit
agent.type	381 (38.1%)	1	○	edit
agent.type.keyword	381 (100%)	1	○	edit
agent.version	381 (38.1%)	1	○	edit
agent.version.keyword	381 (100%)	1	○	edit
ecs.version	381 (38.1%)	1	○	edit

Figura 2.46: Añadir nuevo campo

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



Create field

Data view: Inicios de sesion fallidos y exitosos

Name Type

Set custom label
Create a label to display in place of the field name in Discover, Maps, Lens, Visualize, and TSVB. Useful for shortening a long field name. Queries and filters use the original field name.

Set custom description
Add a description to the field. It's displayed next to the field on the Discover, Lens, and Data View Management pages.

Set value
Set a value for the field instead of retrieving it from the field with the same name in `_source`.

[Cancel](#) [Save](#)

Preview

From: filebeat-*

Document ID

B-J62ZMBH0ctV0yUtBrJ



Filter fields

test	Value not set
@timestamp	Dec 18, 2024 @ 12:15:0...
@version	1
@version.keyword	1
agent.ephemeral_id	a65b42be-359d-4c1a...
agent.ephemeral_id.ke...	a65b42be-359d-4c1a...
agent.id	a82c3989-5687-4479...
agent.id.keyword	a82c3989-5687-4479-

[Show more](#)

Figura 2.47: Añadir nuevo campo

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



Set value

Set a value for the field instead of retrieving it from the field with the same name in `_source`.

Define script

```
1  def mensaje = doc['message.keyword'].value;
2  if(mensaje != null) {
3      if(mensaje.contains("authentication failure"))
4          {
5              emit("Authentication failure");
6          }
7      else if(mensaje.contains("unlocked login")) {
8          emit("Unlocked login");
9      }
10     else {
```

Runtime fields without a script retrieve values from `_source`. If the field doesn't exist in `_source`, a search request returns no value. [Learn about script syntax.](#)

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 código 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.

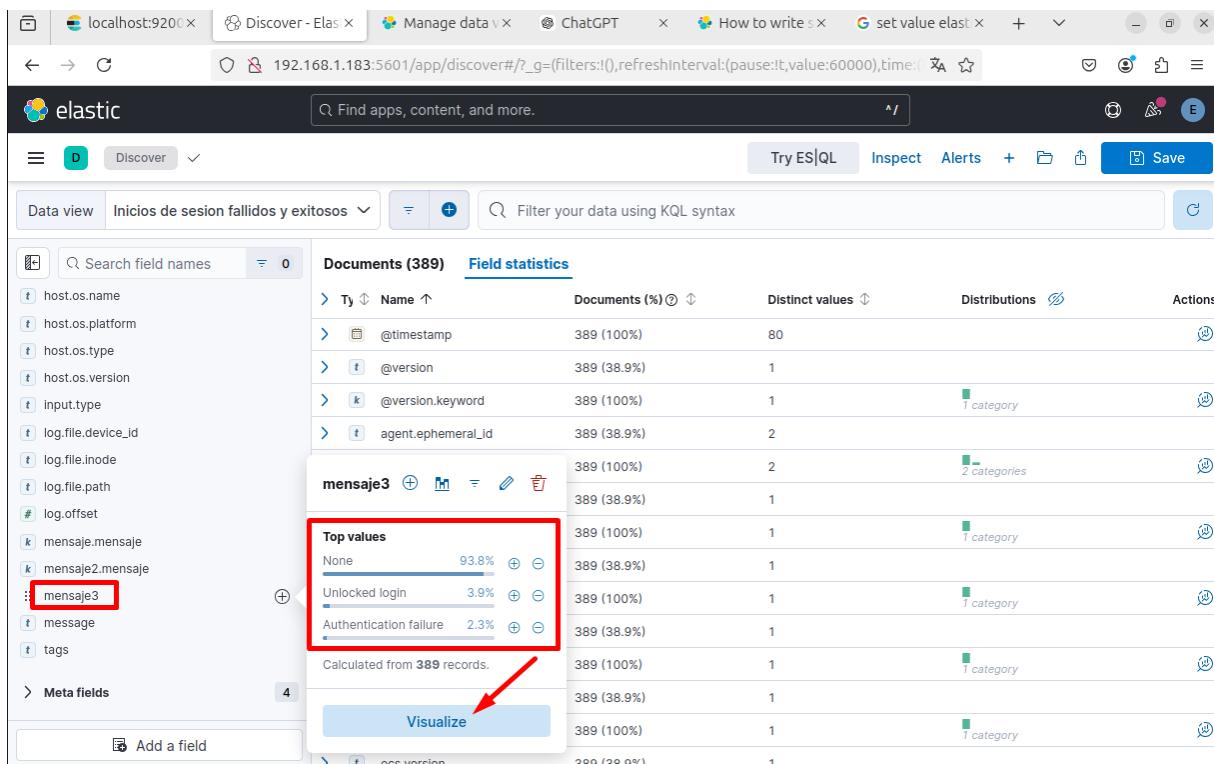


Figura 2.49: visualizar campo nuevo

Y podremos ver en una gráfica los valores.

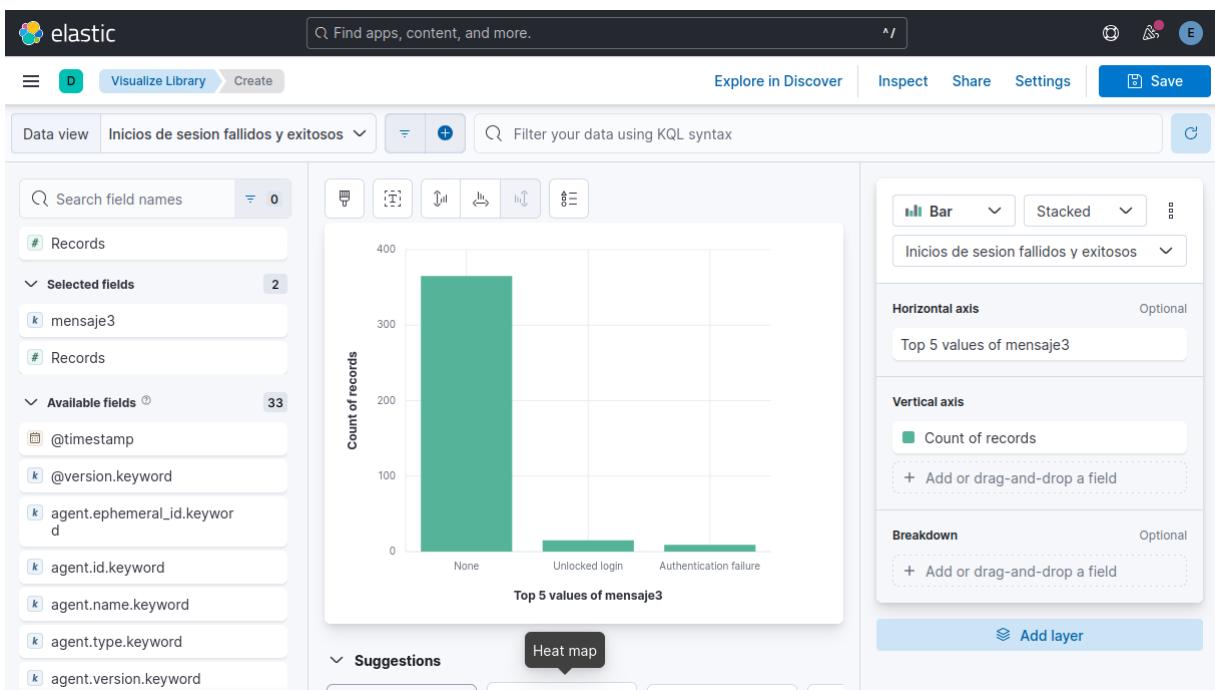


Figura 2.50: visualizar campo nuevo

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

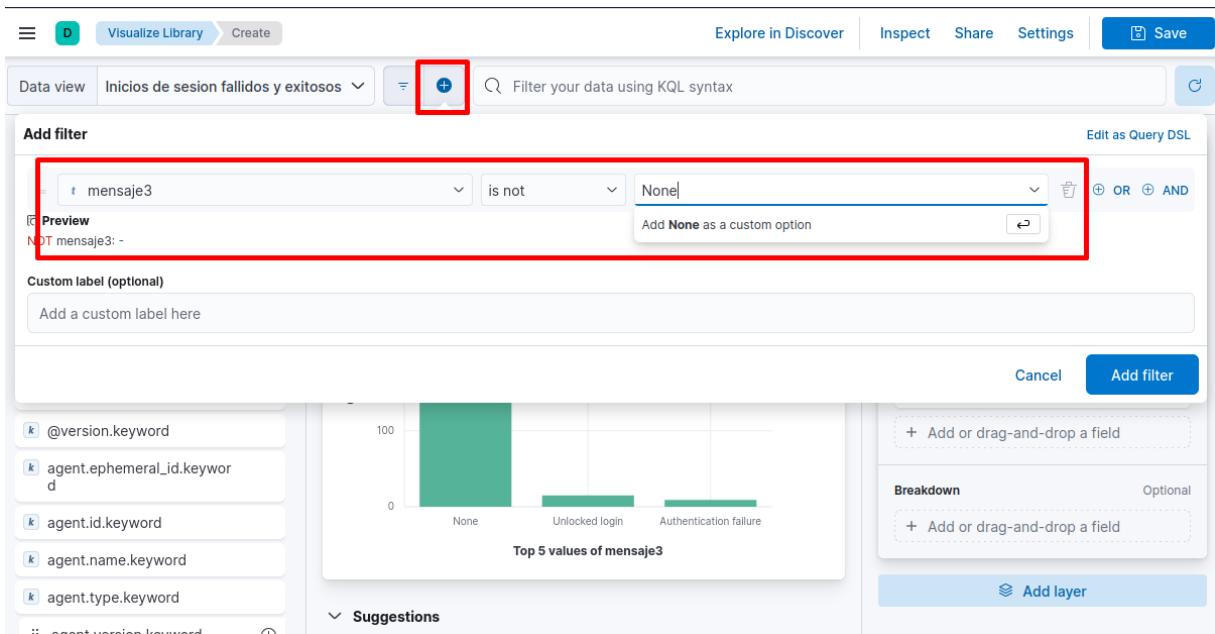


Figura 2.51: visualizar en grafica con filtro

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

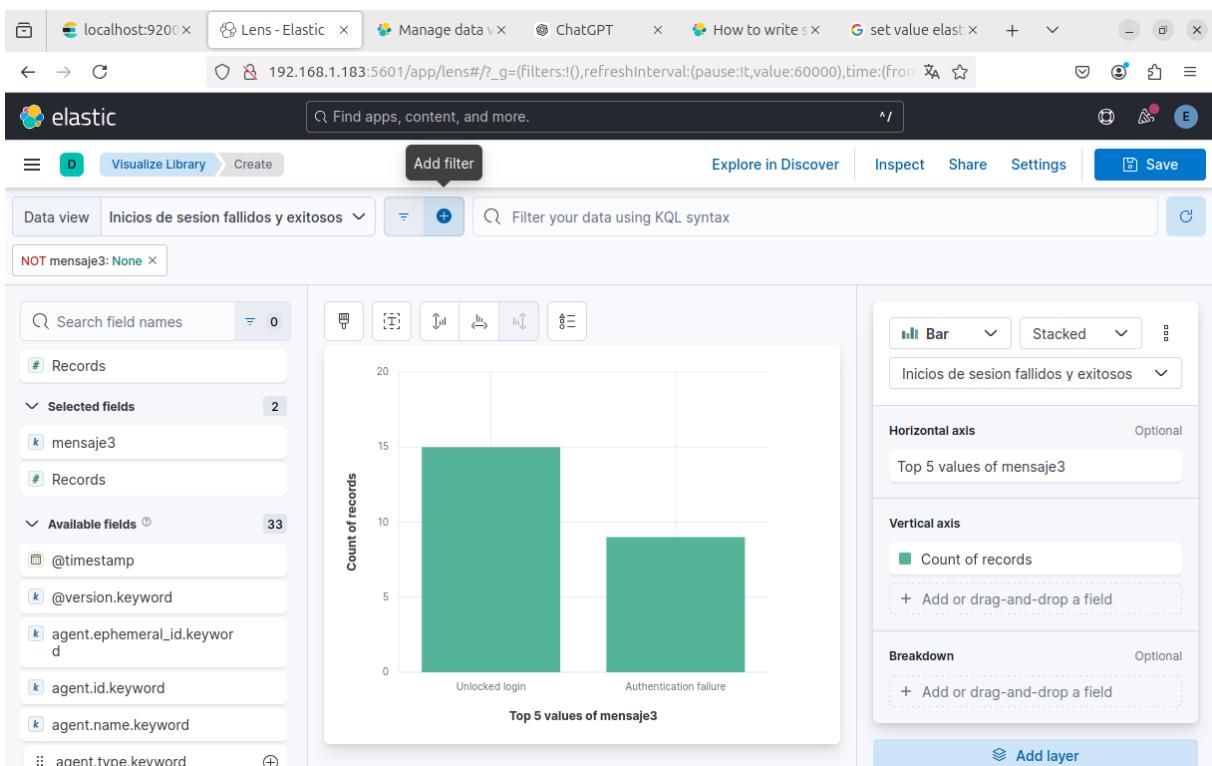


Figura 2.52: visualizar en grafica con filtro

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

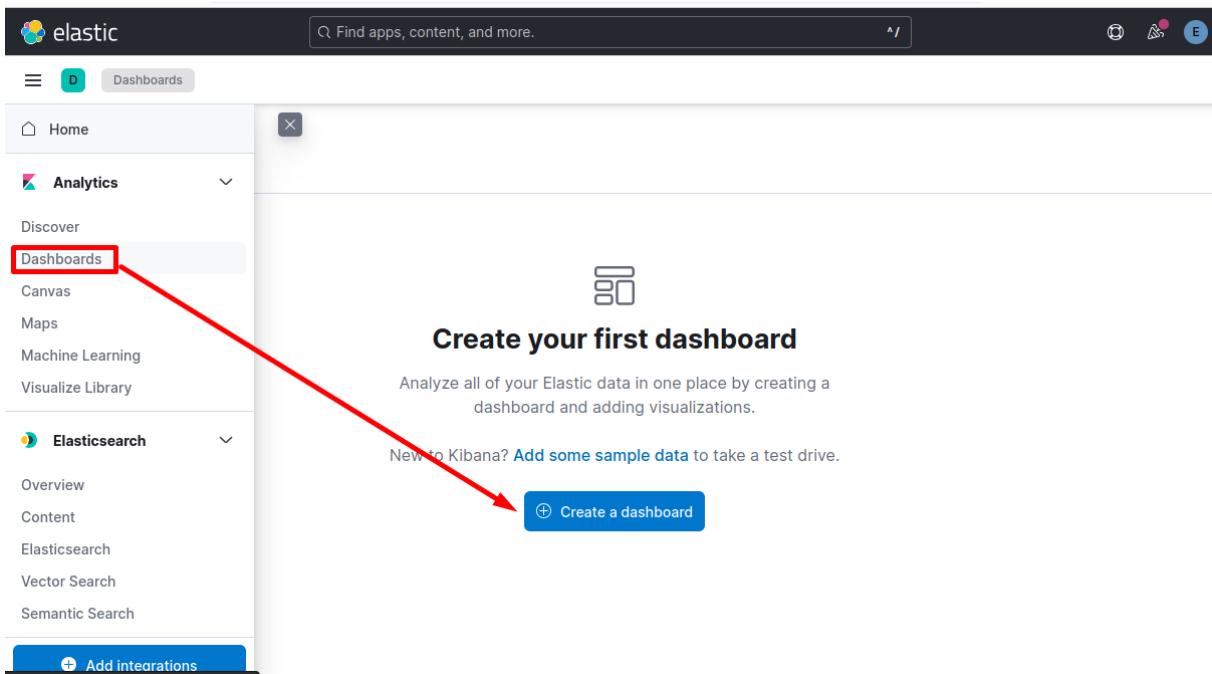


Figura 2.53: Nuevo visualizacion



Y después le daremos a crear nueva visualización.

The screenshot shows the Elastic Dashboards interface. At the top, there's a search bar with the placeholder "Find apps, content, and more." and a "Save" button. Below the header, there are buttons for "Create visualization", "Add panel", "Add from library", and "Controls". A message in the center says "This dashboard is empty. Let's fill it up!" with a sub-instruction "Create a visualization of your data, or add one from the library." There are also "Create visualization" and "Add from library" buttons at the bottom of this section.

Figura 2.54: Nueva visualizacion dashboard

The screenshot shows the "Create" tab in the Elastic Dashboards interface. On the left, there's a sidebar with a search bar for "Search field names" and a list of "Available fields" including @timestamp, @version.keyword, agent.ephemeral_id.keyword, agent.id.keyword, agent.name.keyword, agent.type.keyword, agent.version.keyword, ecs.version.keyword, event.original.keyword, and host.architecture.keyword. In the center, there's a large area with a hand icon and the text "Drop some fields here to start". Below this, it says "Lens is the recommended editor for creating visualizations" and "Make requests and give feedback". On the right, there are sections for "Horizontal axis" (with a "Bar" dropdown), "Vertical axis" (with a "Stacked" dropdown), and "Breakdown" (with a dropdown menu set to "Inicios de sesión fallidos y exitosos"). There are also "Optional" labels and "Add or drag-and-drop a field" buttons. At the bottom right, there's a blue "Add layer" button.

Figura 2.55: Crear visualizacion dashboard

Crearemos la gráfica que hicimos antes [2.52](#).

Y ahora si le daremos a guardar.

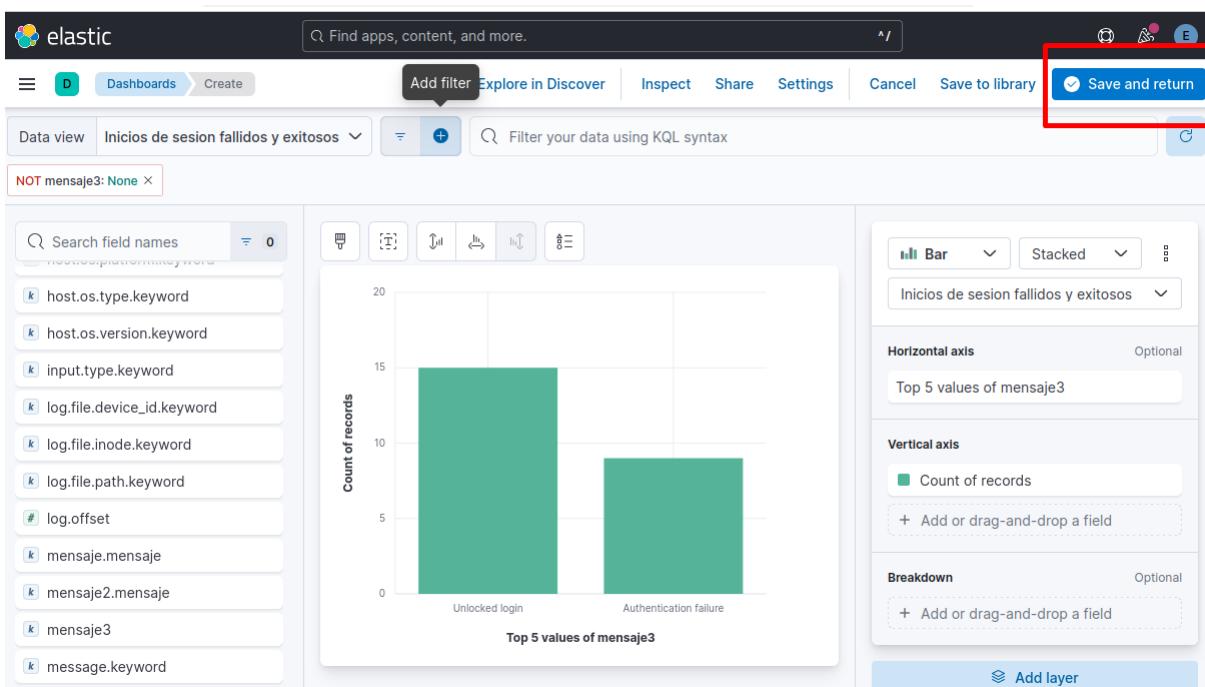


Figura 2.56: Guardar gráfica dashboard

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

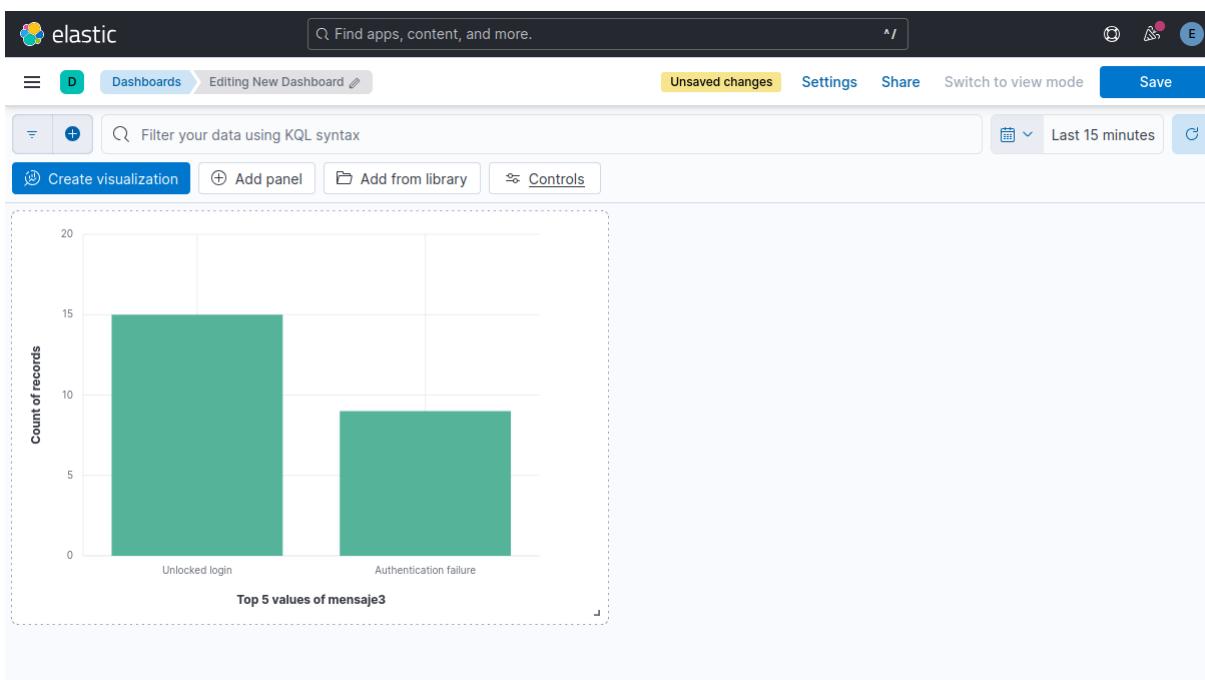


Figura 2.57: Añadida gráfica dashboard



2.7.1. Instalación de Filebeat en windows

Para continuar con la práctica y así 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](#).

The screenshot shows a web browser displaying the Elastic Filebeat installation guide for Windows. The URL in the address bar is elastic.co/guide/en/beats/filebeat/current/filebeat-installation-configuration.html. The page has a navigation menu on the left with sections like 'Filebeat Reference:', 'Filebeat overview', 'Quick start: installation and configuration' (which is currently selected), 'Set up and run', 'Upgrade', 'How Filebeat works', 'Configure', 'How to guides', 'Modules', and 'Exported fields'. The main content area shows steps for installing Filebeat on Windows:

- Download the Filebeat Windows zip file: https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-8.17.0-windows-x86_64.zip
- Extract the contents of the zip file into C:\Program Files.
- Rename the filebeat-8.17.0-windows-x86_64 directory to Filebeat.
- Open a PowerShell prompt as an Administrator (right-click the PowerShell icon and select Run As Administrator).
- From the PowerShell prompt, run the following commands to install Filebeat as a Windows service:

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

A note at the bottom of the steps says: "If script execution is disabled on your system, you need to set the execution policy for the current session to allow the script to run. For example: PowerShell.exe -ExecutionPolicy Unrestricted -File". On the right side of the page, there's a sidebar titled "On this page" with links to other sections of the guide, and a "Most Popular" section with links to related content like "Get Started with Elasticsearch" and "Intro to Kibana".

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**

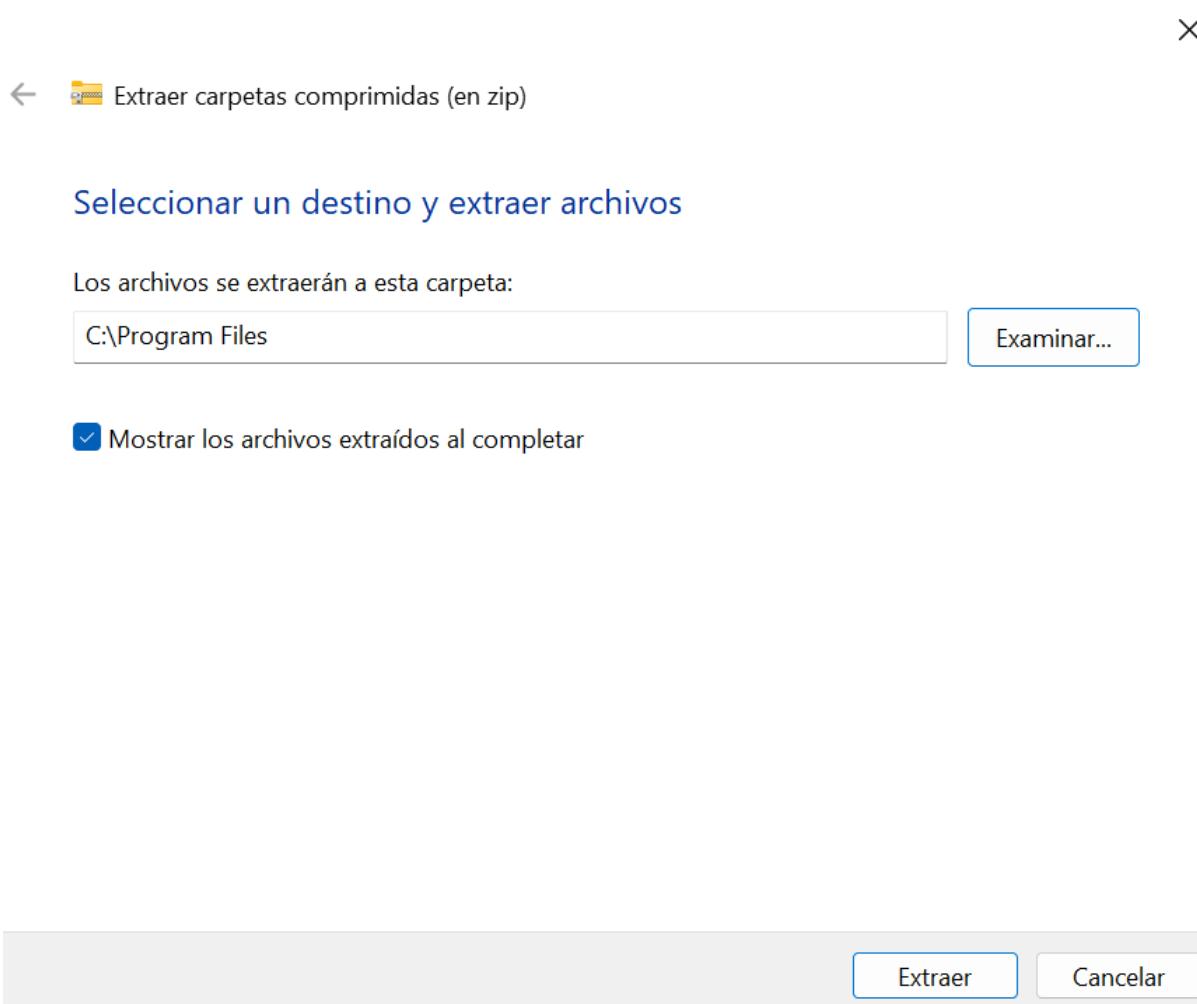


Figura 2.59: Ubicacion de extracción

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
```

The screenshot shows a Windows PowerShell window titled "Administrator: PowerShell 7 (x64)". The command entered is "PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.ps1". The output shows a warning about running unsigned scripts and a security prompt asking if the user wants to run the script. The command then lists the status of the "filebeat" service, which is currently stopped.

```
PS C:\Program Files\filebeat> .\install-service-filebeat.ps1
.\install-service-filebeat.ps1: File C:\Program Files\filebeat\install-service-filebeat.ps1 cannot be loaded. The file C:\Program Files\filebeat\install-service-filebeat.ps1 is not digitally signed. You cannot run this script on the 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\filebeat> PowerShell.exe -ExecutionPolicy UnRestricted -File .\install-service-filebeat.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\filebeat\install-service-filebeat.ps1?
[N] No ejecutar [Z] Ejecutar una vez [U] Suspender [?] Ayuda (el valor predeterminado es "N"): Z

Status     Name           DisplayName
-----     --          -----
Stopped   filebeat       filebeat

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

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 envío de logs y especificamos que la ruta de los logs a enviar C:_Windows_System32_winevt_Logs_Security.evtx.



```
# ===== Filebeat inputs =====

filebeat.inputs:

# Each - is an input. Most options can be set at the input level, so
# you can use different inputs for various configurations.
# Below are the input-specific configurations.

# filestream is an input for collecting log messages from files.
- type: filestream

  # Unique ID among all inputs, an ID is required.
  id: my-filestream-id

  # Change to true to enable this input configuration.
  enabled: true

  # Paths that should be crawled and fetched. Glob based paths.
  paths:
    - C:\Windows\System32\winevt\Logs\Security.evtx
#/var/log/*.log
#- c:\programdata\elasticsearch\logs\*
```

Figura 2.61: Archivo de configuración Filebeat

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

```
# ----- Logstash Output -----
output.logstash:
  # The Logstash hosts
  hosts: ["192.168.1.183:5045"]

  # Optional SSL. By default is off.
  # List of root certificates for HTTPS server verifications
  #ssl.certificateAuthorities: ["/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 2.62: Archivo de configuración Filebeat

Una vez guardado el archivo de configuración testeamos que funciona.

```
PS C:\Program Files\filebeat> .\filebeat.exe test config
Config OK
PS C:\Program Files\filebeat>
```

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](#)

The terminal window shows the configuration file for Logstash at /etc/logstash/conf.d/pipeline_windows.conf. The file contains the following code:

```
GNU nano 7.2      /etc/logstash/conf.d/pipeline_windows.conf
input {
  beats {
    port => 5045
  }
}

output {
  elasticsearch {
    hosts => ["https://localhost:9200"]
    index => "filebeat-windows"
    user => "elastic"
    password => "7o0OJbwIkQZfI*wg-5pV"
    ssl => true
    cacert => "/etc/elasticsearch/certs/http_ca.crt"
  }
}
```

Figura 2.64: Pipeline de logstash para windows

Y reseteamos el servicio de logsatash.

The terminal window shows the status and restart of the logstash service:

```
aryan@ELK-aryan:~$ sudo systemctl restart logstash.service
aryan@ELK-aryan:~$ sudo systemctl status logstash.service
● logstash.service - logstash
   Loaded: loaded (/usr/lib/systemd/system/logstash.service; enabled; preset:>)
   Active: active (running) since Wed 2024-12-18 16:43:47 CET; 7s ago
     Main PID: 3076 (java)
        Tasks: 20 (limit: 4615)
       Memory: 234.0M (peak: 234.4M)
          CPU: 10.948s
        CGroup: /system.slice/logstash.service
                  └─3076 /usr/share/logstash/jdk/bin/java -Xms1g -Xmx1g -Djava.awt.h>

dic 18 16:43:47 ELK-aryan systemd[1]: Started logstash.service - logstash.
dic 18 16:43:48 ELK-aryan logstash[3076]: Using bundled JDK: /usr/share/logstas>
lines 1-12/12 (END)
```

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
```

```
PS C:\Program Files\filebeat> .\filebeat.exe test output
logstash: 192.168.1.183:5045...
  connection...
    parse host... OK
    dns lookup... OK
    addresses: 192.168.1.183
    dial up... OK
  TLS... WARN secure connection disabled
  talk to server... OK
PS C:\Program Files\filebeat>
```

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:7o00JbwIkQZfI*wg-5pV --cacert
/etc/elasticsearch/certs/http_ca.crt
https://localhost:9200/_cat/indices/filebeat-*?v=true
```

```
aryan@ELK-aryan:~$ curl -u elastic:7o00JbwIkQZfI*wg-5pV --cacert /etc/elasticsearch/certs/http_ca.crt https://localhost:9200/_cat/indices/filebeat-*?v=true
health status index      uuid                                     pri rep docs.count docs.deleted store.size pri.store.size dataset.size
yellow open   filebeat-ubuntu  DMjMPY_6Sva0ZEomkVyK8A     1   1        3618
          0      5.6mb        5.6mb        5.6mb
yellow open   filebeat-windows D49IAzW4RYebP9FMs20-Mg     1   1        2991
          0      4.9mb        4.9mb        4.9mb
aryan@ELK-aryan:~$
```

Figura 2.67: Envio de datos a elasticsearch



health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size	dataset.size
yellow	open	filebeat-ubuntu	DMjMPY_6Sva0ZEomkVyK8A	1	1	3618	0	5.6mb	5.6mb	5.6mb
yellow	open	filebeat-windows	D49IAzW4RYebP9FMs20-Mg	1	1	2991	0	4.9mb	4.9mb	4.9mb

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 automaticamente 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.

Create data view

Name
inicios windows

Index pattern
filebeat-windows

Timestamp field
@timestamp

Your index pattern matches 1 source.

All sources Matching sources

filebeat-windows

Rows per page: 10

Close Use without saving Save data view to Kibana

Figura 2.69: Creación de data view de datos de windows

Analizando los datos vemos que nos llegan los datos cifrados

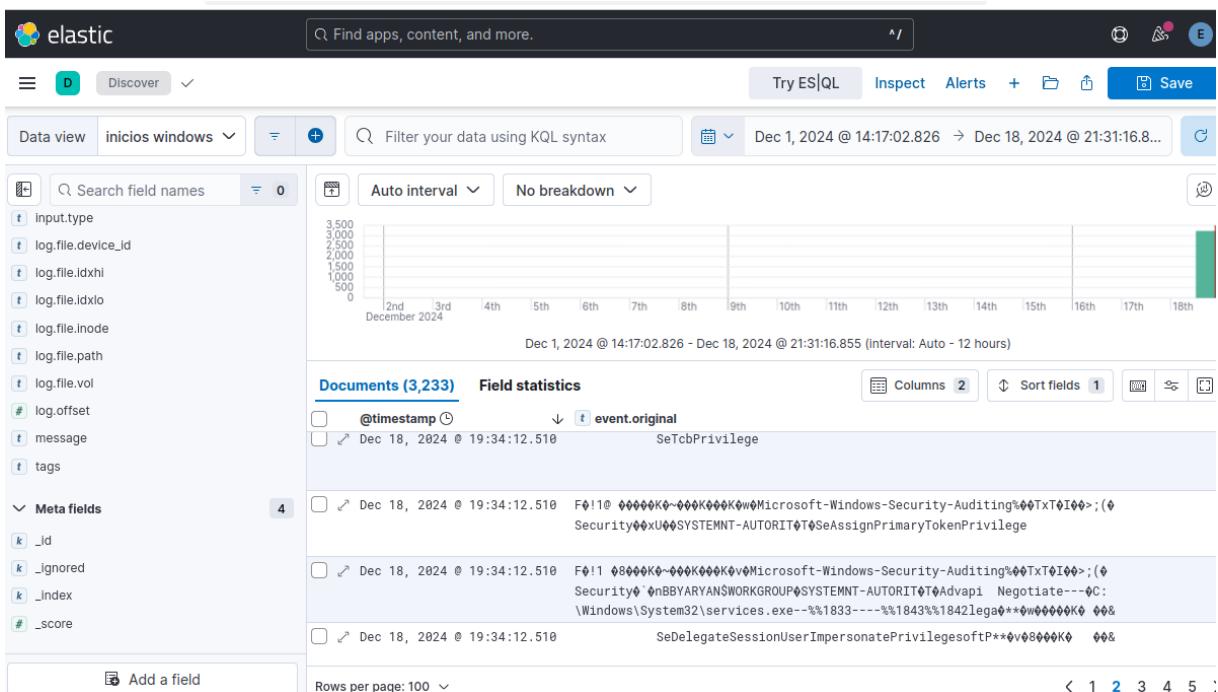


Figura 2.70: Datos cifrados de los eventos

Así 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 página oficial de elastic.



elasticsearch

Platform Solutions Customers Resources Pricing Docs

Start free trial

On this page

Before you begin

You need Elasticsearch for storing and searching your data, and Kibana for visualizing and managing it.

Elasticsearch Service Self-managed

To install and run Elasticsearch and Kibana, see [Installing the Elastic Stack](#).

Quick start: installation and configuration

Set up and run >

Upgrade

Configure >

How to guides >

Modules >

Exported fields >

Monitor >

edit

Most Popular

VIDEO Get Started with Elasticsearch

VIDEO Intro to Kibana

VIDEO ELK for Logstash Metrics

Figura 2.71: Guía Winlogbeat

Descargamos el archivo .zip y descomprimimos el archivo .zip. Lo extraemos todo a la ubicación C:_ Program Files Y renombramos la carpeta a winlogbeat.



Nombre	Fecha de modificación	Tipo	Tamaño
Microsoft OneDrive	11/12/2024 19:56	Carpeta de archivos	
Microsoft Update Health Tools	12/12/2023 14:33	Carpeta de archivos	
ModifiableWindowsApps	07/05/2022 7:24	Carpeta de archivos	
OpenVPN Connect	15/11/2024 9:18	Carpeta de archivos	
Oracle	12/08/2024 18:11	Carpeta de archivos	
PowerShell	30/10/2024 17:16	Carpeta de archivos	
PuTTY	12/08/2024 21:07	Carpeta de archivos	
texstudio	02/12/2024 17:40	Carpeta de archivos	
Windows Defender	12/08/2024 17:24	Carpeta de archivos	
Windows Defender Advanced Threat Protecti...	06/09/2024 11:28	Carpeta de archivos	
Windows Mail	12/12/2023 14:26	Carpeta de archivos	
Windows Media Player	12/08/2024 17:24	Carpeta de archivos	
Windows NT	06/10/2023 9:37	Carpeta de archivos	
Windows Photo Viewer	12/08/2024 17:24	Carpeta de archivos	
WindowsPowerShell	07/05/2022 7:42	Carpeta de archivos	
winlogbeat	18/12/2024 22:40	Carpeta de archivos	
WSL	13/11/2024 13:22	Carpeta de archivos	

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.certificateAuthorities: ["/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.



```
GNU nano 7.2          /etc/logstash/conf.d/pipeline_windows2.  
input {  
    beats {  
        port => 5046  
    }  
}  
  
output {  
    elasticsearch {  
        hosts => ["https://localhost:9200"]  
        'x => "filebeat-windows"  
Terminal => "elastic"  
        password => "7o00JbwIkQZfI*wg-5pV"  
        ssl => true  
        cacert => "/etc/elasticsearch/certs/http_ca.crt"  
    }  
}
```

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.



```
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test config
Config OK
PS C:\Program Files\winlogbeat> .\winlogbeat.exe test output
logstash: 192.168.1.183:5046...
    connection...
        parse host... OK
        dns lookup... OK
        addresses: 192.168.1.183
        dial up... OK
    TLS... WARN secure connection disabled
    talk to server... OK
PS C:\Program Files\winlogbeat>
```

Figura 2.77: Tests

Y comprobaremos que los datos se reciben en elasticsearch.

```
curl -u elastic:7o00JbwIkQZfI*wg-5pV --cacert
/etc/elasticsearch/certs/http_ca.crt
https://localhost:9200/_cat/indices/filebeat-*?v=true
```

```
aryan@ELK-aryan:~$ curl -u elastic:7o00JbwIkQZfI*wg-5pV --cacert /etc/elasticsearch/certs/http_ca.crt https://localhost:9200/_cat/indices/filebeat-*?v=true
health status index          uuid                               pri rep docs.count docs.deleted store.size pri.store.size dataset.size
yellow open   filebeat-winlogbeat E59Vj0PiRTeFrVD8bQLVpA   1   1      91119           0       95mb       95mb       95mb
yellow open   filebeat-ubuntu   DMjMPY_6Sva0ZEomkVyK8A   1   1      94641           0      104.2mb     104.2mb     104.2mb
yellow open   filebeat-windows D49IAzW4RYebP9FMs20-Mg   1   1      94352           0      101.3mb     101.3mb     101.3mb
aryan@ELK-aryan:~$
```

Figura 2.78: datos winlogbeats

health	status	index	uuid	pri	rep	docs.count	docs.deleted	store.size	pri.store.size	dataset.size
yellow	open	filebeat-winlogbeat	E59Vj0PiRTeFrVD8bQLVpA	1	1	98348	0	95mb	95mb	95mb
yellow	open	filebeat-ubuntu	DMjMPY_6Sva0ZEomkVyK8A	1	1	101995	0	104.2mb	104.2mb	104.2mb
yellow	open	filebeat-windows	D49IAzW4RYebP9FMs20-Mg	1	1	101581	0	101.3mb	101.3mb	101.3mb

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.

Create data view

Name
inicios winlogbeats

Index pattern
filebeat-winlogbeat

Timestamp field
@timestamp

Select a timestamp field for use with the global time filter.

Show advanced settings

✓ Your index pattern matches 1 source.

All sources

Matching sources

filebeat-winlogbeat

Index

Rows per page: 10

Figura 2.80: Creación data view

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

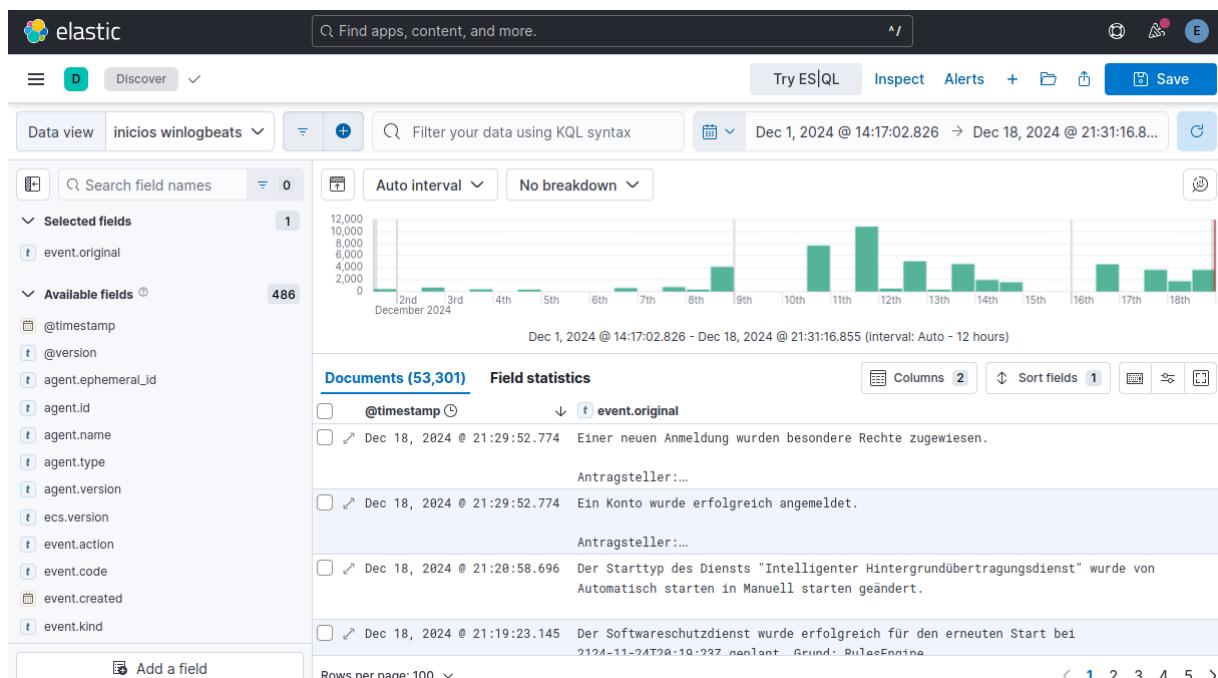


Figura 2.81: Visualización de data



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).

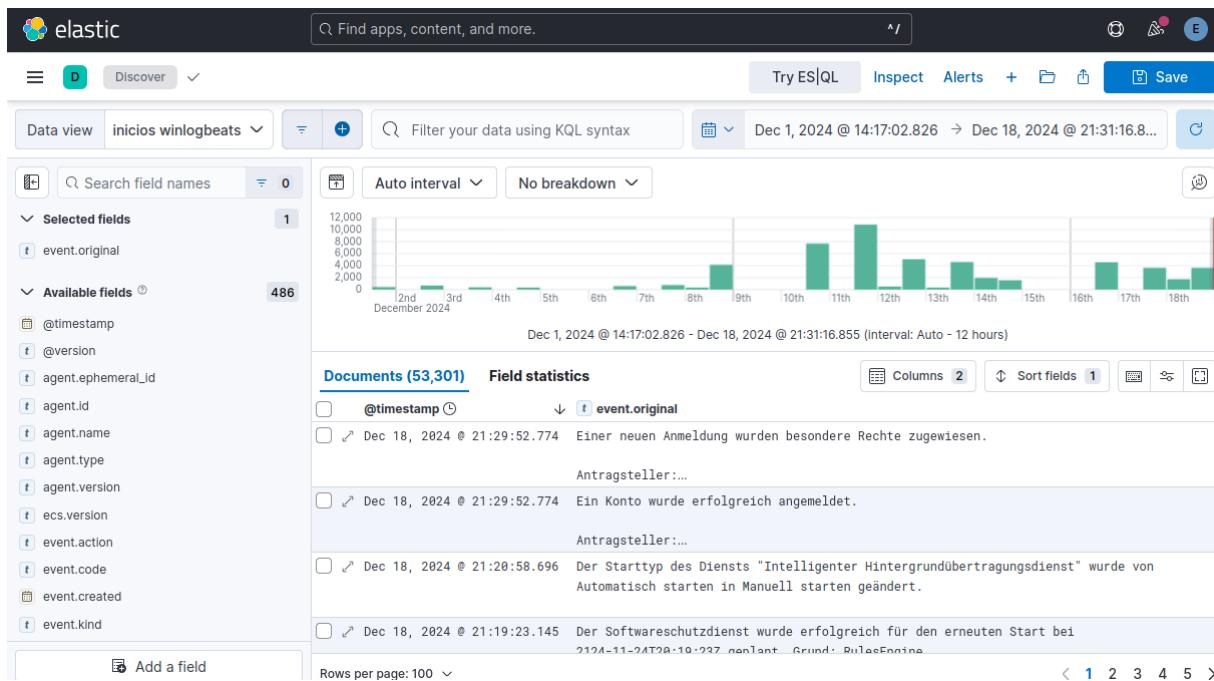


Figura 2.82: Analisis de datos

Para crear el filtro como hicimos anteriormente.

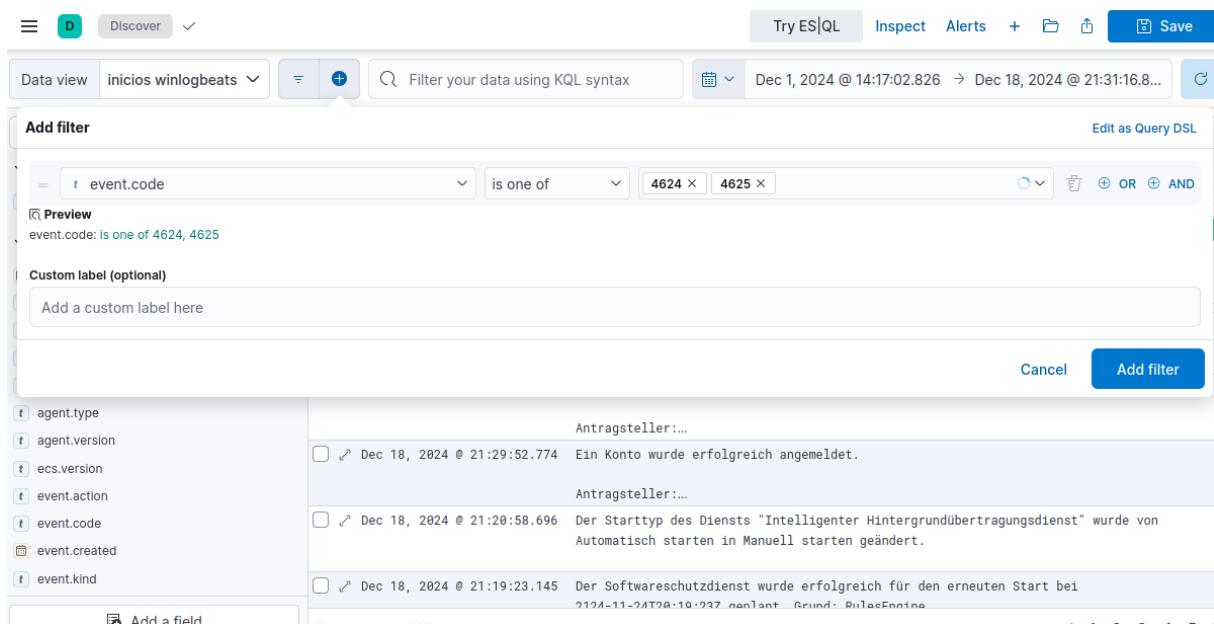


Figura 2.83: Filtro

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

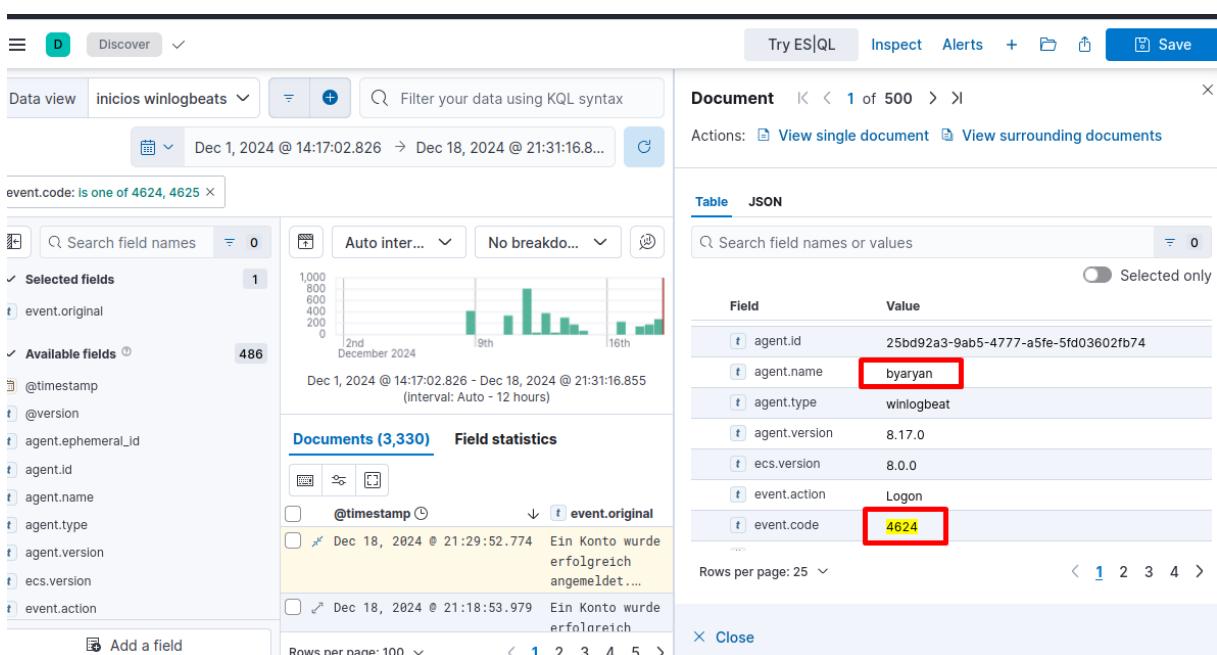


Figura 2.84: Eventos filtrados

Ahora lo guardaremos.



X

Save search

Title

inicios de sesion windowsss

Description

Optional

Hecho por Aryan

Tags



Store time with saved search

Cancel

Save

Figura 2.85: Guardar eventos

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

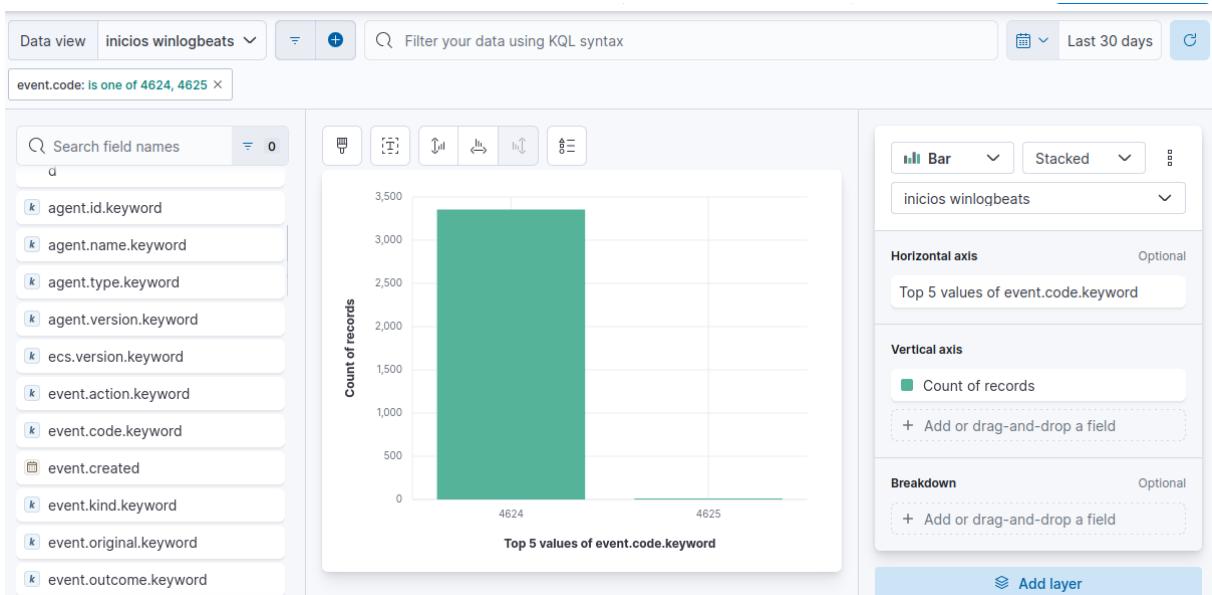


Figura 2.86: Grafica de eventos

Y lo guardamos y automaticamente se nos añade al dashboard.

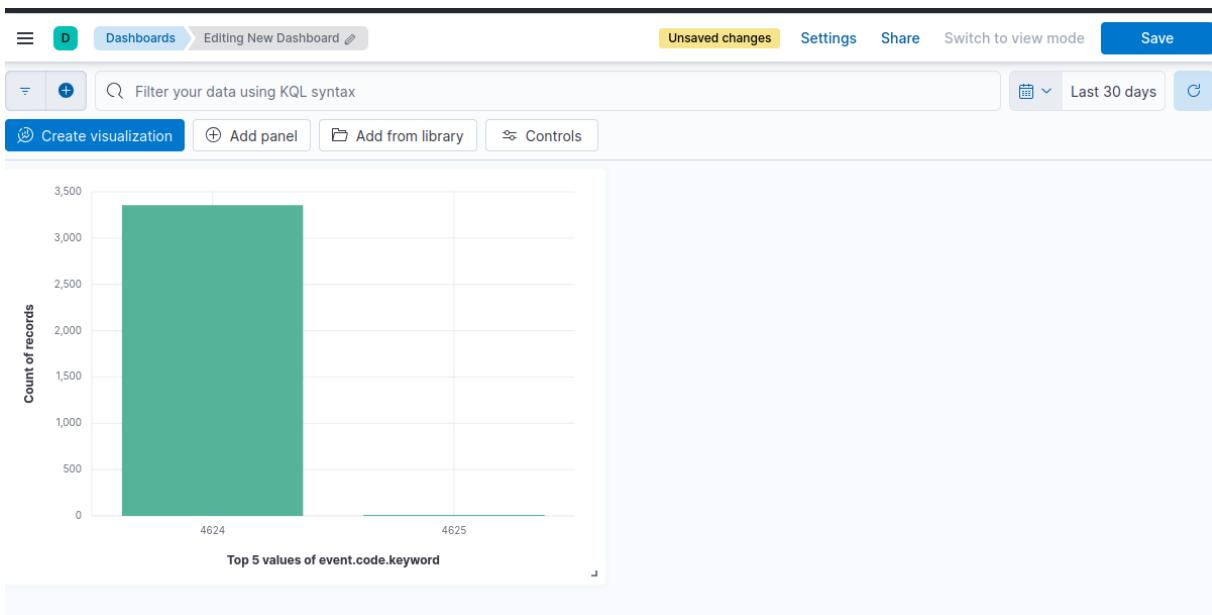


Figura 2.87: Gráfica añadida al dashboard

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.

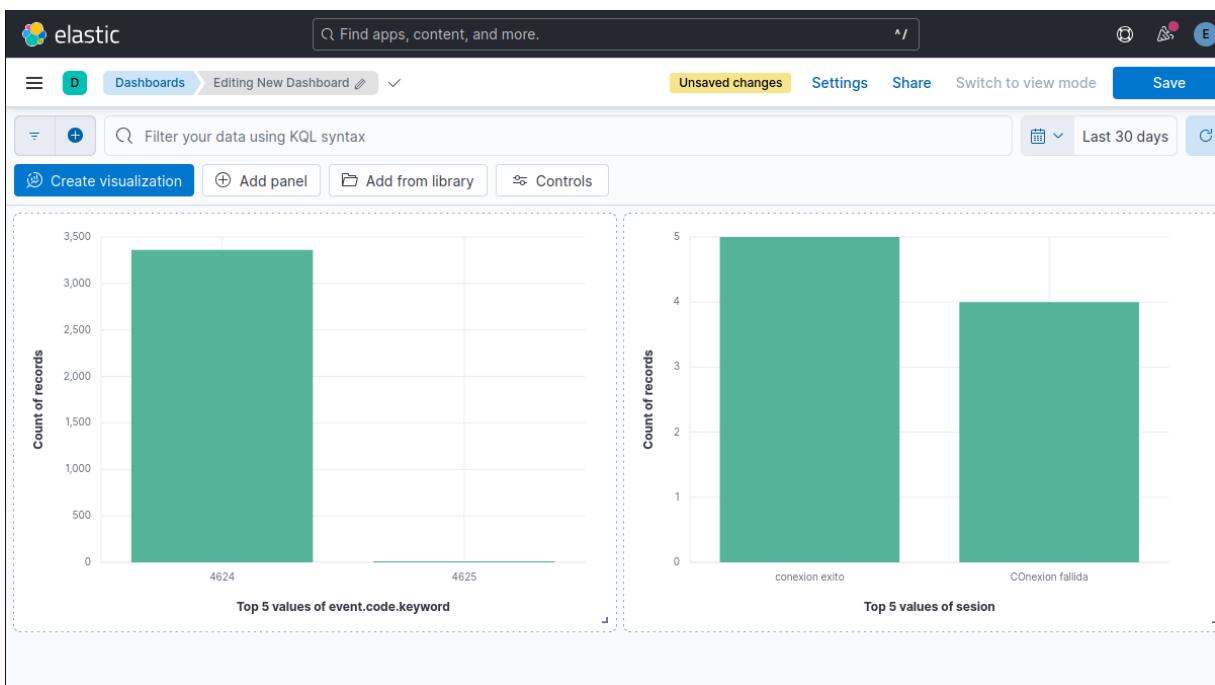


Figura 2.88: Gráficas añadidas al dashboard

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.