

# Bootcamp Analista SOC Nivel 1

3° Edición

Módulo IV

## Taller: Implementación de Splunk

**Elaborado por:**

Sheyla Leacock



**COMUNIDAD  
DOJO**

## Objetivos del taller:

- ☐ Crear un HomeLab para el análisis de eventos de seguridad.
- ☐ Implementar el SIEM Splunk Enterprise versión trial free en un entorno local.
- ☐ Realizar la ingesta manual de logs en el SIEM.
- ☐ Relacionarse con las principales funcionalidades ofrecidas por un SIEM.

## Disclaimer:

Este laboratorio se realiza sólomente con fines educativos y de aprendizaje, con el fin de brindar información que permita mejorar las defensas en ciberseguridad.

## Metodología:

1. Se desplegará el SIEM Splunk en una máquina virtual de Ubuntu en VirtualBox y se realizarán las configuraciones necesarias para su funcionamiento.
2. Se realizará la ingesta manual de logs y se habilitará el monitoreo de los logs de la propia instancia.

3. Se visualizarán las capacidades de la herramienta.

## Prerrequisitos:

1. Tener instalado VirtualBox: <https://www.virtualbox.org/wiki/Downloads>
2. Tener una máquina virtual con Ubuntu y / o una máquina virtual con Windows 10.

\*Nota: Tomar de referencia la guía del CyberHomeLab desarrollado en la primera clase:

<https://github.com/WOSEC/AnalistaSOC2022/blob/main/CyberHomeLab/Creando%20tu%20HomeLab.pdf>

## Parte I - Descarga y configuración de Splunk

1. Desde nuestra máquina Ubuntu, ingresamos al sitio oficial de descargas de Splunk Enterprise:  
[https://www.splunk.com/en\\_us/download/splunk-enterprise.html](https://www.splunk.com/en_us/download/splunk-enterprise.html)

GET STARTED

# Splunk Enterprise 9.0.1

Start turning data into insights today. Try Splunk Enterprise free for 60 days. No credit card required.

- ✓ Tackle your hardest Security, IT, and DevOps use cases
- ✓ Stream, collect, and index any data at any scale
- ✓ Search, analyze, and visualize your data with powerful, visually-compelling dashboards



Explore our Splunkbase ecosystem of applications - or develop your own with developer tools at your fingertips!



Flexible environment management for your data no matter the scale with effective tools to administer your Splunk deployment on-premises or with your own cloud license

## Start Your Free Download

Already have a Splunk account? [Login](#)



2. Deberemos ingresar los datos del formulario para crear una cuenta de Splunk o iniciar sesión desde la opción **Login** si ya mantenemos una cuenta.

## Start Your Free Download

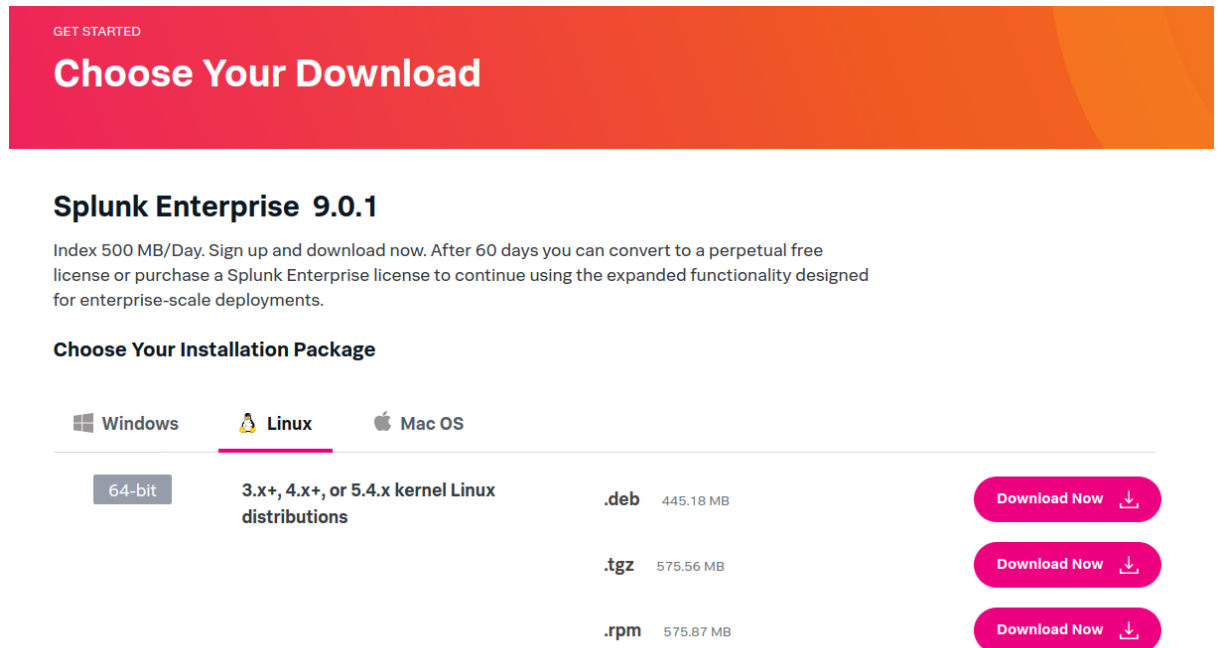
Already have a Splunk account? [Login ›](#)



☐ I agree to the [Splunk Website Terms & Conditions of Use](#), [Splunk Privacy Policy](#) and [Splunk General Terms](#).

Create Your Account

Seleccionamos el paquete de instalación para descargar. En este caso, para Ubuntu seleccionaremos Linux y de allí descargamos el paquete comprimido en formato **.tgz**






GET STARTED

## Choose Your Download

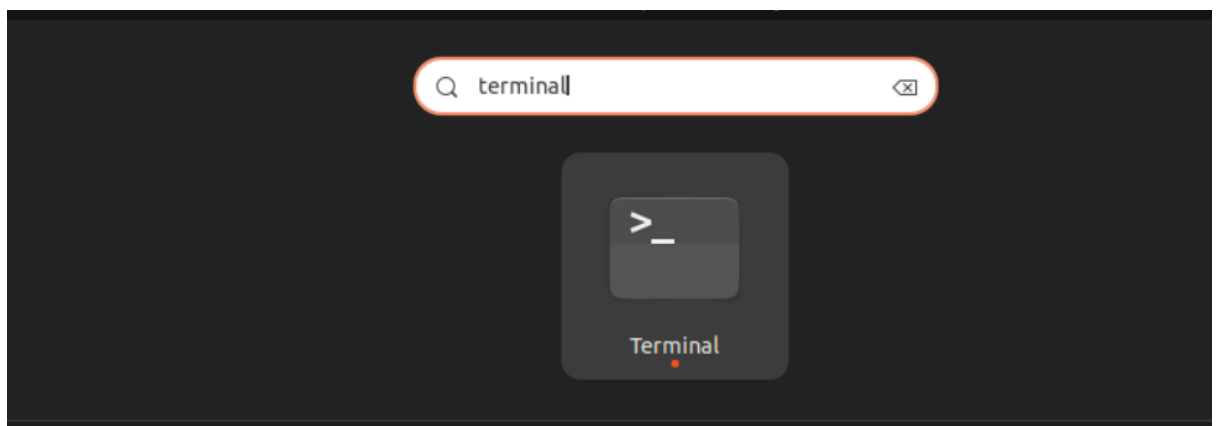
### Splunk Enterprise 9.0.1

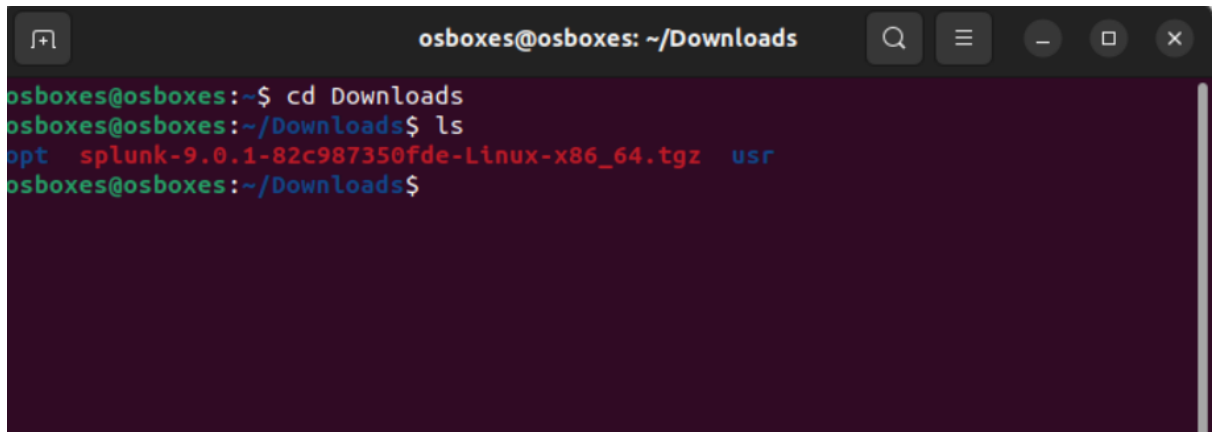
Index 500 MB/Day. Sign up and download now. After 60 days you can convert to a perpetual free license or purchase a Splunk Enterprise license to continue using the expanded functionality designed for enterprise-scale deployments.

#### Choose Your Installation Package

Windows	Linux	Mac OS
64-bit	3.x+, 4.x+, or 5.4.x kernel Linux distributions	
	<b>.deb</b> 445.18 MB	<a href="#">Download Now</a> 
	<b>.tgz</b> 575.56 MB	<a href="#">Download Now</a> 
	<b>.rpm</b> 575.87 MB	<a href="#">Download Now</a> 

- Una vez culmine la descarga, iniciamos la consola (terminal) y nos dirigimos a la carpeta de descargas con el comando: **cd Downloads**

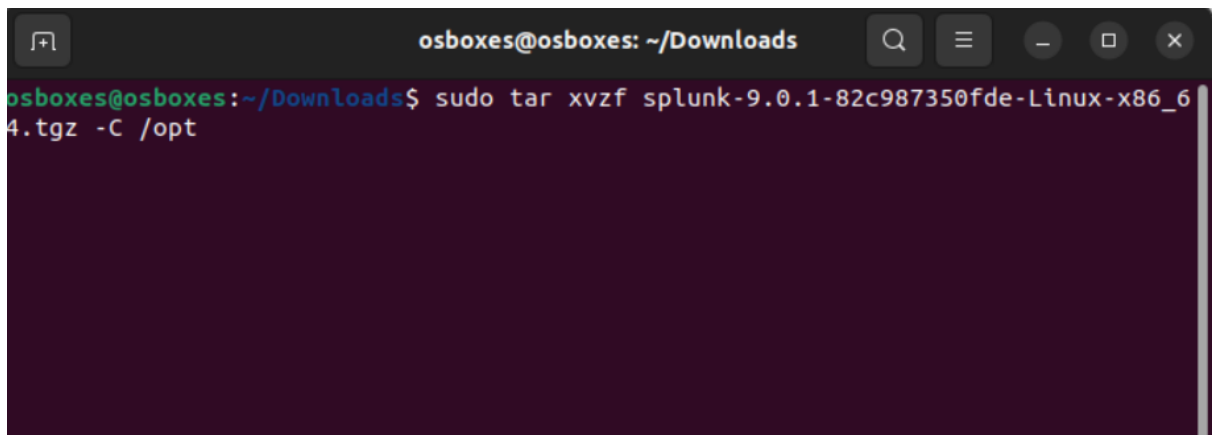




```
osboxes@osboxes: ~/Downloads
osboxes@osboxes:~$ cd Downloads
osboxes@osboxes:~/Downloads$ ls
opt  splunk-9.0.1-82c987350fde-Linux-x86_64.tgz  usr
osboxes@osboxes:~/Downloads$
```

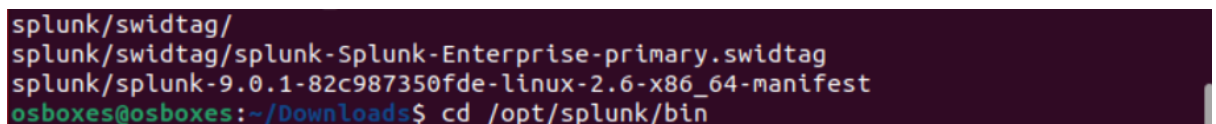
4. Ejecutamos el comando para extraer el archivo comprimido y lo almacenamos en la ruta /opt:

**`sudo tar xvzf splunk-9.0.1-82c987350fde-Linux-x86_x64.tgz -C /opt`**



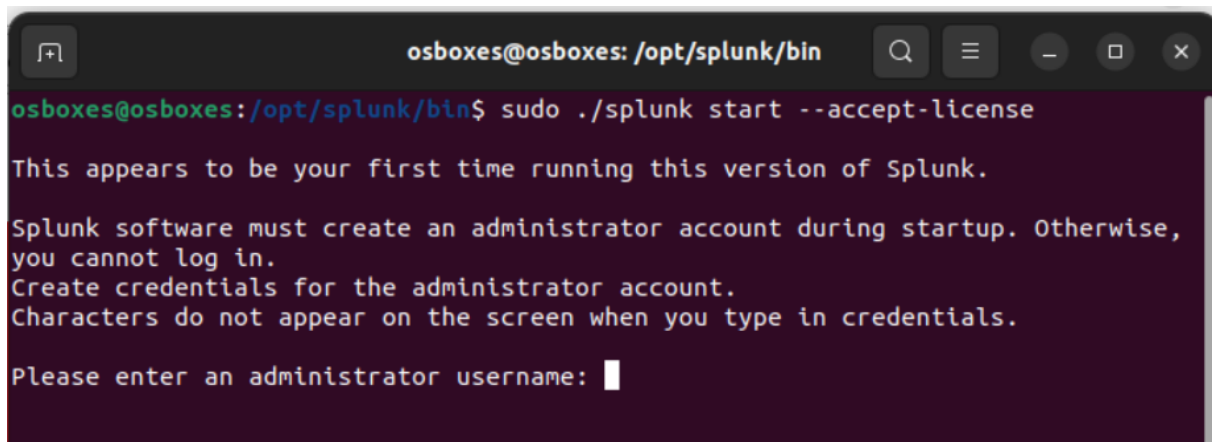
```
osboxes@osboxes:~/Downloads$ sudo tar xvzf splunk-9.0.1-82c987350fde-Linux-x86_64.tgz -C /opt
```

5. Una vez completada la extracción, nos dirigimos a la ruta donde se almacenaron los ejecutables de Splunk: **`cd /opt/splunk/bin`**



```
splunk/swidtag/
splunk/swidtag/splunk-Splunk-Enterprise-primary.swidtag
splunk/splunk-9.0.1-82c987350fde-linux-2.6-x86_64-manifest
osboxes@osboxes:~/Downloads$ cd /opt/splunk/bin
```

6. Ejecutamos el comando **`sudo ./splunk start --accept-license`** para iniciar el servicio de Splunk aceptando automáticamente la licencia.

A terminal window titled 'osboxes@osboxes: /opt/splunk/bin' showing the command 'sudo ./splunk start --accept-license' being executed. The output indicates it's the first time running this version of Splunk and prompts for administrator credentials.

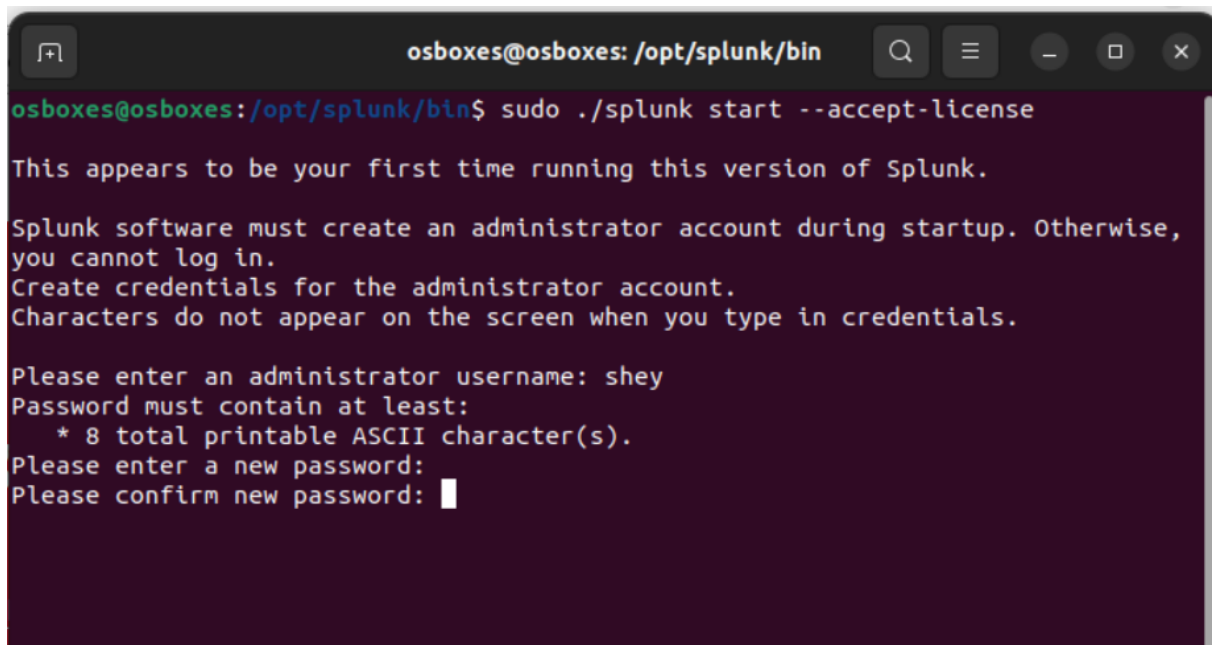
```
osboxes@osboxes: /opt/splunk/bin$ sudo ./splunk start --accept-license

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: 
```

7. Se nos mostrará en la pantalla la opción de ingresar un usuario administrador para poder utilizar splunk. Ingresamos el usuario, contraseña y confirmación de contraseña para continuar.

A terminal window titled 'osboxes@osboxes: /opt/splunk/bin' showing the same command as before. The output now prompts for a password and its confirmation.

```
osboxes@osboxes: /opt/splunk/bin$ sudo ./splunk start --accept-license

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: shey
Password must contain at least:
  * 8 total printable ASCII character(s).
Please enter a new password:
Please confirm new password: 
```

8. Una vez se complete la configuración se nos mostrará la URL para acceder a la interfaz web.



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

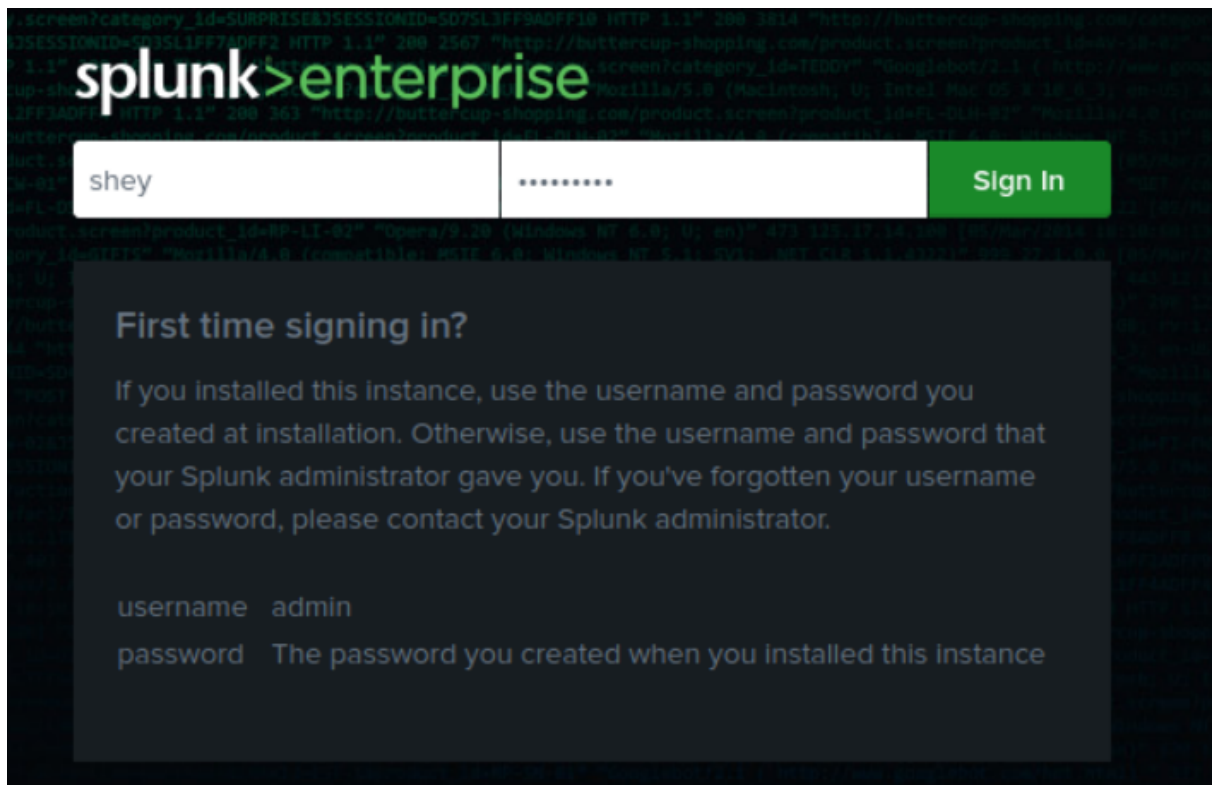
Waiting for web server at http://127.0.0.1:8000 to be available.....
..... Done

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

The Splunk web interface is at http://osboxes:8000

osboxes@osboxes: /opt/splunk/bin$
```

9. Ingresamos a dicha URL desde el navegador web e ingresamos con los datos del usuario administrador previamente creado.



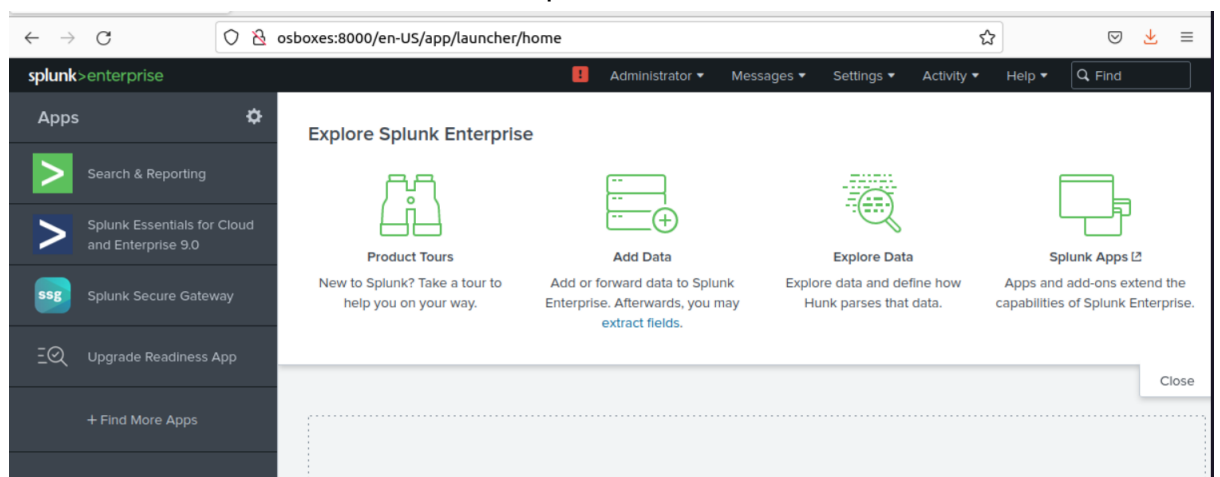
\*Nota: Podemos configurar el inicio de Splunk automático al encender el sistema con el siguiente comando:

***sudo ./splunk enable boot-start -user <usuariodelamaquina>***

```
osboxes@osboxes:/opt/splunk/bin$ sudo ./splunk enable boot-start -user osboxes
Warning: cannot create "/opt/splunk/var/log/splunk"
Warning: cannot create "/opt/splunk/var/log/introspection"
Warning: cannot create "/opt/splunk/var/log/watchdog"
Init script installed at /etc/init.d/splunk.
Init script is configured to run at boot.
osboxes@osboxes:/opt/splunk/bin$
```

Cuando queramos reiniciar el servicio de Splunk podemos utilizar el comando: ***sudo ./splunk restart***, para detenerlo: ***sudo ./splunk stop*** y para ver la ayuda: ***sudo ./splunk help***

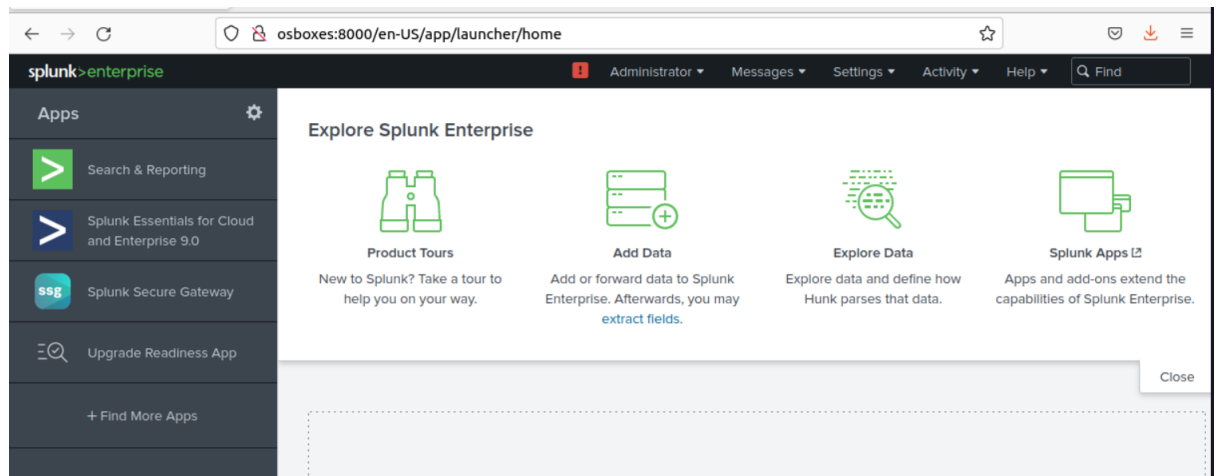
10. Una vez iniciemos se nos mostrará el panel inicial



# Parte II - Ingesta de logs

## Opción 1: Monitoreo de logs de la propia instancia

1. Desde el apartado inicial, seleccionamos la opción **Add Data**



2. En la siguiente pantalla seleccionamos la opción Monitor para agregar la data de nuestro propio dispositivo.

The screenshot shows the 'Add Data' wizard in Splunk. At the top, there are four categories of data sources: Cloud computing (10 data sources), Networking (2 data sources), Operating System (1 data source), and Security (3 data sources). Below these, it states '4 data sources in total'. Under the heading 'Or get data in with the following methods', there are three options: Upload (files from my computer), Monitor (files and ports on this Splunk platform instance), and Forward (data from a Splunk forwarder). The 'Monitor' option is highlighted, showing details about monitoring files, ports, and scripts.

3. Seleccionamos la opción **Files & Directories**, se nos mostrarán entonces las opciones para configurar las rutas donde se almacenan nuestros logs, ingresamos la ruta **/var/log**, directorio bajo el cual se almacenan los logs en Ubuntu.

The screenshot shows the 'Add Data' wizard in Splunk, specifically the 'Files & Directories' step. The left sidebar lists several options: HTTP Event Collector, TCP / UDP, Scripts, Splunk Assist Instance Identifier, and Systemd Journal Input for Splunk. The main area shows the configuration for monitoring files and directories. It includes a 'File or Directory' field with the value '/var/log' and a 'Browse' button. Below this, there are fields for 'Includelist' and 'Excludelist', both set to 'optional'. A note indicates that data preview will be skipped for directories.

4. Damos **Next** para pasar a la siguiente pantalla donde seleccionamos la opción de entrada de los datos. Mantenemos todas las opciones como vienen marcadas por defecto:

Source type: **Automatic**

App context: **Search & Reporting (search)**

Host: Constant Value: **osboxes**

Index: **default**

Add Data

Select Source

Input Settings

Review

Done

< Back

Review >

### Input Settings

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

**Source type**

The source type is one of the default fields that the Splunk platform assigns to all incoming data. It tells the Splunk platform what kind of data you've got, so that the Splunk platform can format the data intelligently during indexing. And it's a way to categorize your data, so that you can search it easily.

Automatic

Select

New

**App context**

Application contexts are folders within a Splunk platform instance that contain configurations for a specific use case or domain of data. App contexts improve manageability of input and source type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

App Context

Search & Reporting (search) ▼

type definitions. The Splunk platform loads all app contexts based on precedence rules. [Learn More](#)

**Host**

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

Constant value

Regular expression on path

Segment in path

Host field value

osboxes

**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

Default ▼

Create a new index

5. Damos click a **review** y de allí a **Submit** para finalizar

Add Data

Select Source

Input Settings

Review

Done

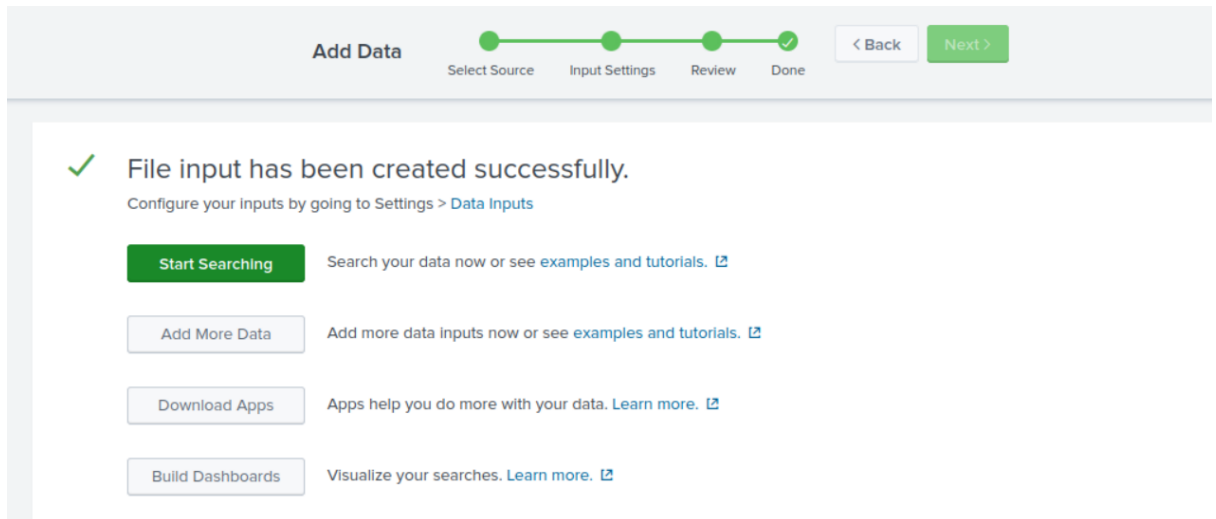
< Back

Submit >

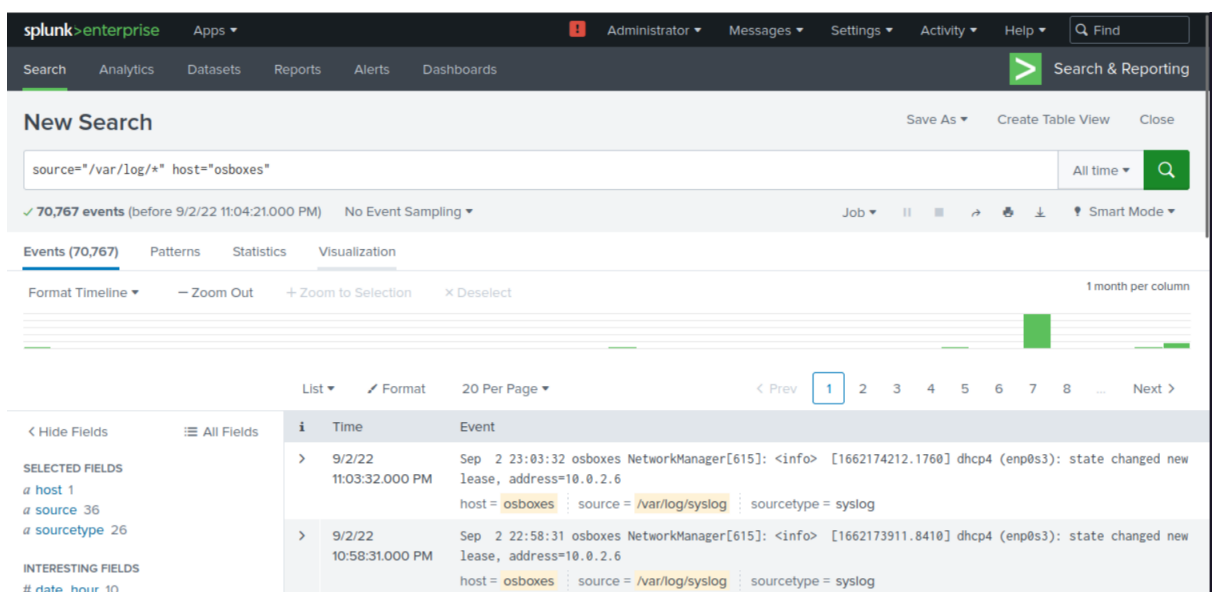
### Review

Input Type .....	Directory Monitor
Source Path .....	/var/log
Includelist .....	N/A
Excludelist .....	N/A
Source Type .....	Automatic
App Context .....	search
Host .....	osboxes
Index .....	default

- En la siguiente pantalla damos click a **Start Searching** para empezar a revisar la data recolectada.



- Ahora se nos muestra el apartado de nuevas búsquedas para empezar a navegar sobre los eventos registrados

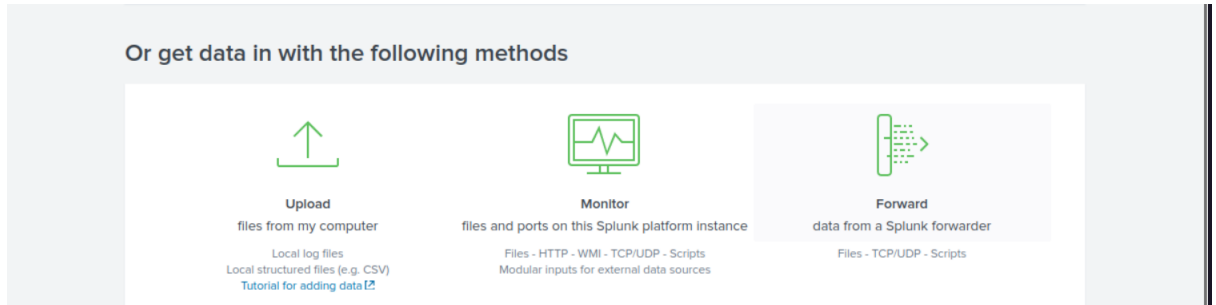


## Opción 2: Mediante ingesta manual de archivos

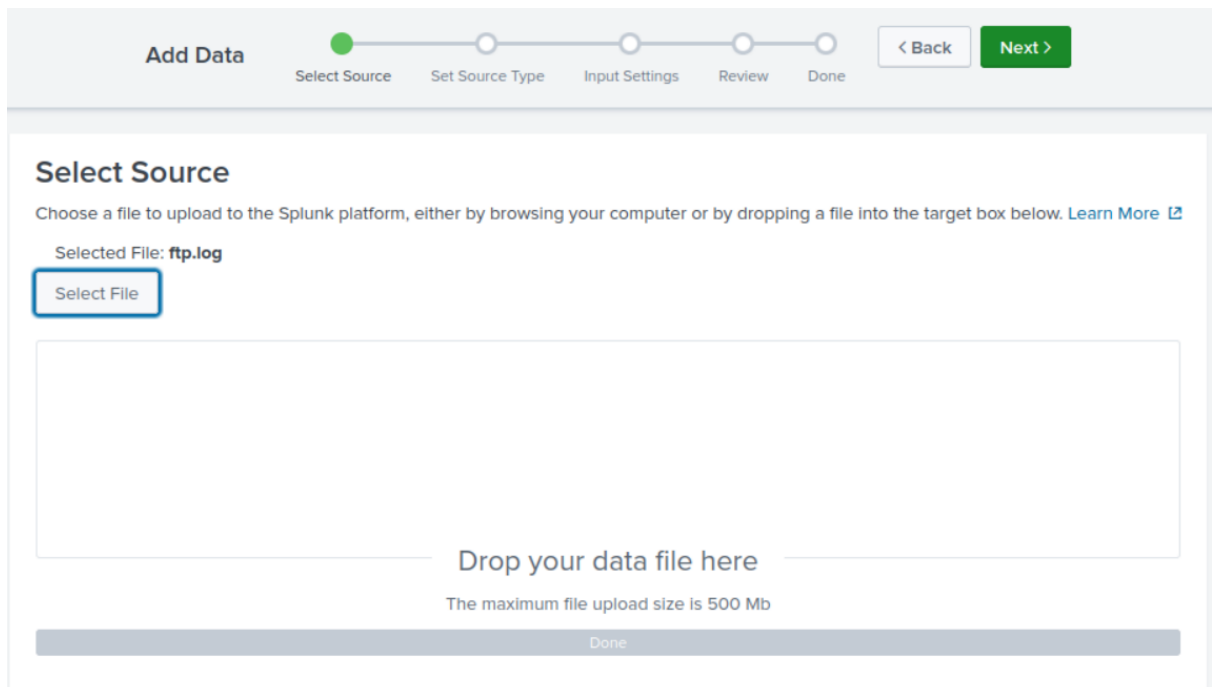
- Podemos descargar algunas muestras de logs de los siguientes sitios:  
<https://www.secrepo.com/maccdc2012/ftp.log.gz>

<https://github.com/sbousseaden/EVTX-ATTACK-SAMPLES/tree/master/AutomatedTestingTools>

- Una vez descargadas, volvemos a la interfaz web de Splunk y desde el apartado inicial, seleccionamos la opción **Add Data** y luego la opción **Upload**



- Seleccionamos el archivo de log a importar



- Damos click en **Next** para pre visualizar cómo Splunk interpretará la fuente de datos

**Add Data**

Select Source   Set Source Type   Input Settings   Review   Done

< Back   Next >

### Set Source Type

This page lets you see how the Splunk platform sees your data before indexing. If the events look correct and have the right timestamps, click "Next" to proceed. If not, use the options below to define proper event breaks and timestamps. If you cannot find an appropriate source type for your data, create a new one by clicking "Save As".

Source: **ftp.log** [View Event Summary](#)

Source type: Select Source Type ▼ **Save As**

- > Event Breaks
- > Timestamp
- > Advanced

List ▼	Format	20 Per Page ▼	< Prev	1	2	3	4	5	6	7	8	...	Next >
1	▲	9/2/22 11:29:40.000 PM	1331903558.160000	CNfo204HUpVHDn1qt2	192.168.203.45	34433	19						
			2.168.21.101	21	anonymous	IEUser@ PASV	-	-	-	-	-	-	-
			227	Entering Passive Mode (192,168,21,101,219,204).	T	19							
			2.168.203.45	192.168.21.101	56268	-							
			timestamp = none										
2	▲	9/2/22 11:29:40.000 PM	1331903560.090000	CyHkLo2YfhjddpbSV1	192.168.203.45	56158	19						
			2.168.21.103	21	anonymous	IEUser@ PASV	-	-	-	-	-	-	-
			227	Entering Passive Mode (192,168,21,103,192,28)	T	19							
			2.168.203.45	192.168.21.103	49180	-							
			timestamp = none										

5. Damos **Next** y en la siguiente pantalla ingresamos un nombre, descripción, categoría y aplicación para almacenar el tipo de fuente de logs.

### Save Source Type

Name:

Description:

Category:

App:

Cancel   Save

6. Damos click en **Save** y pasamos a la siguiente pantalla donde ingresamos el valor **ftpsamples** para el host y mantendremos el indexador por defecto.



Add Data

Select Source

Set Source Type

Input Settings

Review

Done

< Back

Review >

### Input Settings

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

#### Host

When the Splunk platform indexes data, each event receives a "host" value. The host value should be the name of the machine from which the event originates. The type of input you choose determines the available configuration options. [Learn More](#)

☒ Constant value

☐ Regular expression on path

☐ Segment in path

Host field value

#### 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

Default ▾

Create a new index

7. Damos click a **Review** y luego a **Submit** para finalizar la ingesta manual.

Add Data

Select Source

Set Source Type

Input Settings

Review

Done

< Back

Submit

### Review

Input Type ..... Uploaded File  
File Name ..... ftp.log  
Source Type ..... FTP logs  
Host ..... ftpsamples  
Index ..... Default

Add Data

Select Source

Set Source Type

Input Settings

Review

Done

< Back

Next >



File has been uploaded successfully.

Configure your inputs by going to [Settings > Data Inputs](#)

Start Searching

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

Extract Fields

Create search-time field extractions. [Learn more about fields](#).

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](#).

8. Damos click en **Start Searching** para volver a la pantalla de búsqueda y analizar los eventos registrados.

[illegible]