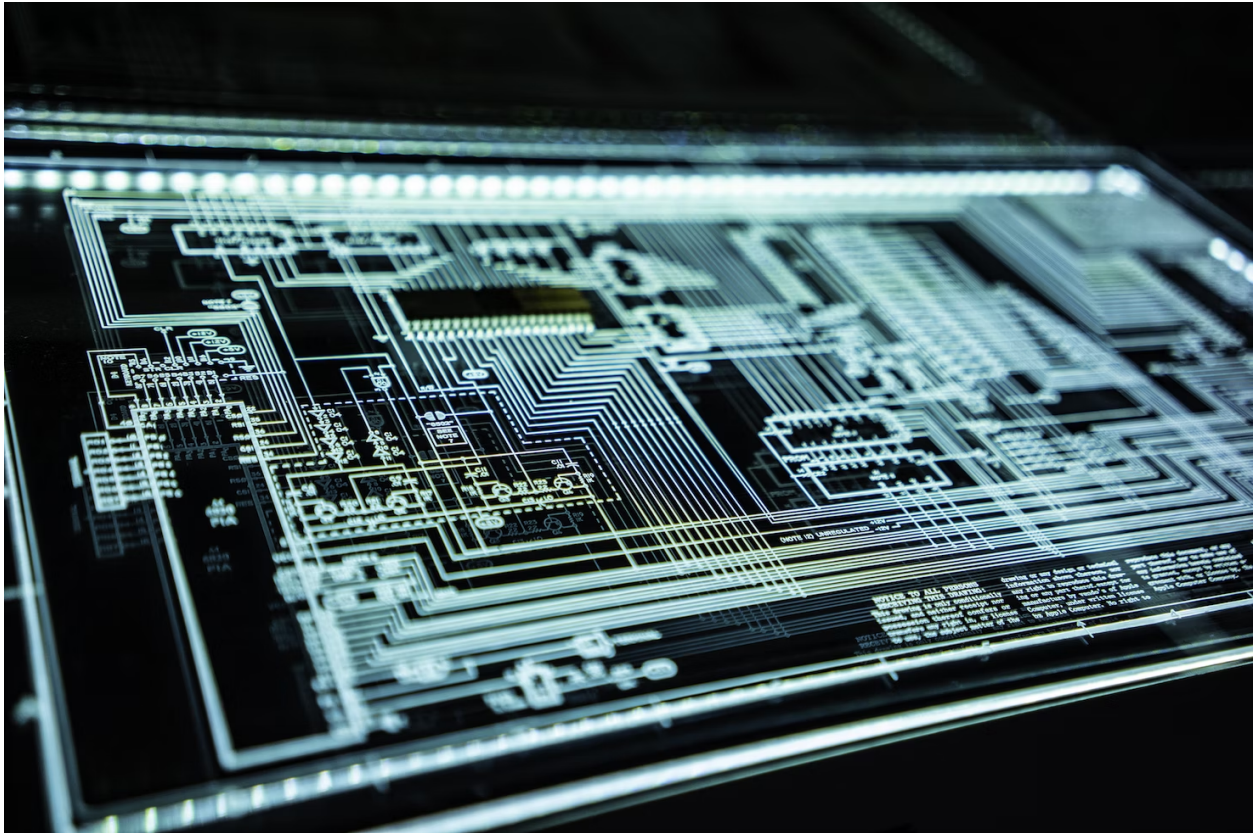


Rafael José

# MiniSOC

## Documentation

---



Hi, my name is Rafael. Welcome to my miniSOC documentation!

## 1. Splunk installation

I decided to choose Splunk for my miniSOC environment. In my case, I will be installing Splunk in Linux.

---

---

We go to the official page of Splunk, log in and download the version that fits our OS.

GET STARTED

## Choose Your Download

### Splunk Enterprise 9.0.3

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	.rpm	573.01 MB	Download Now
		.tgz	572.67 MB	Download Now
		.deb	444.7 MB	Download Now

I downloaded the .deb package. I used dpkg to install it.

```
dpkg -i splunk-9.0.3-dd0128b1f8cd-linux-2.6-amd64.deb
```

## 2. Setting Splunk

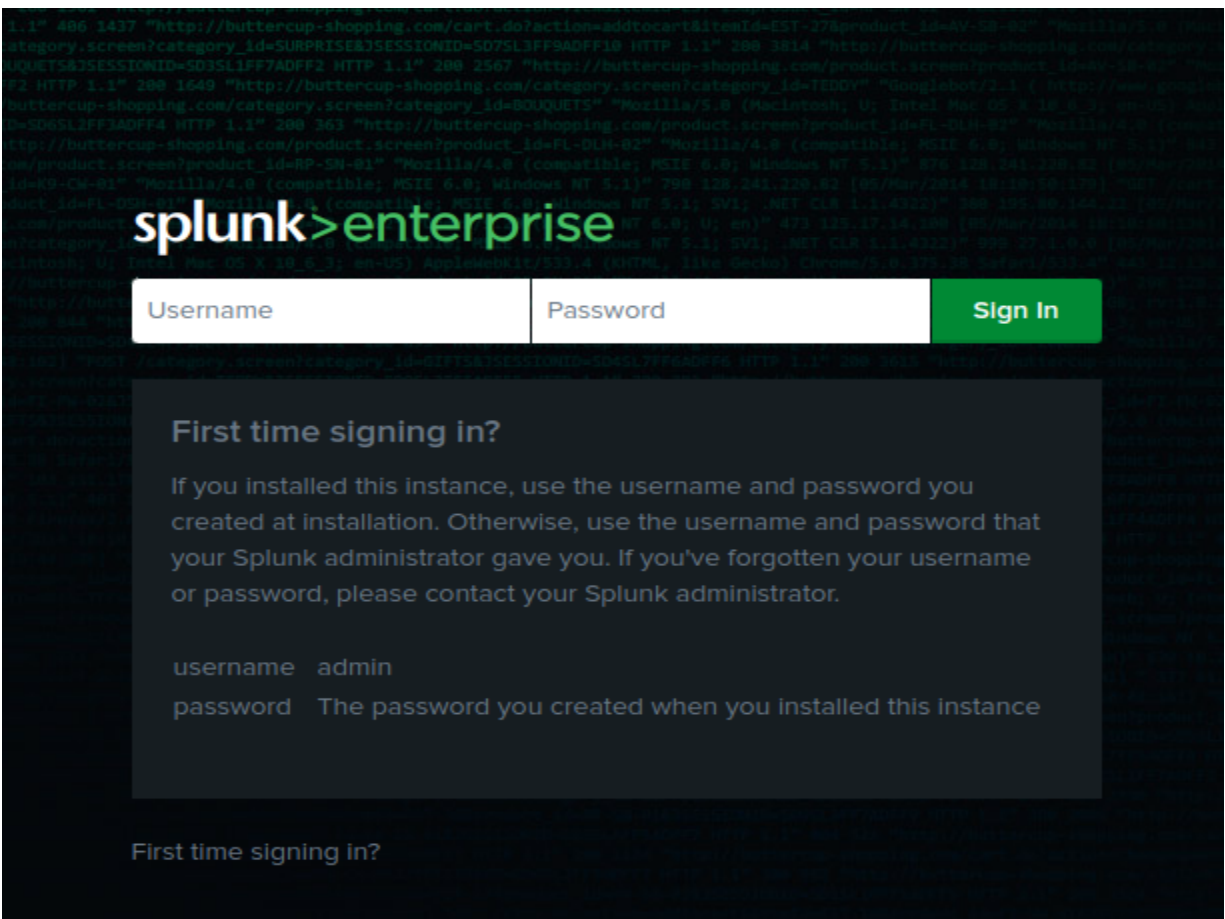
We can choose to start or enable Splunk every time the system starts. I will choose to start it manually every time the system starts.

After the installation, the files were placed into /opt/splunk.

```
sudo /opt/splunk/bin/splunk start
```

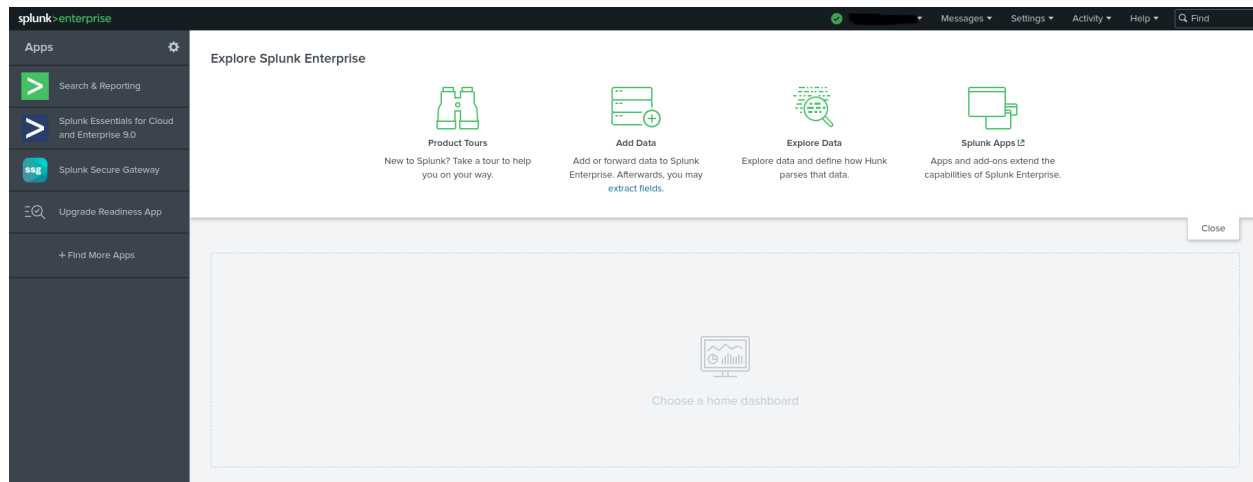
After executing the previous command we will get some output and the port in which Splunk is listening. So we can access it by visiting the localhost address in that port from the web browser.

So visiting the **http://localhost:port** from our web browser, we can see the Splunk panel.



---

Log in with your credentials.



### 3. Forwarding the logs from my router to splunk

To forward the logs from the router to Splunk, you need to enter your router's admin panel. It is important to note that some routers have a limited amount of logging functionalities, so maybe you are not able to forward the logs to Splunk.

### Log Setting

Use this screen to configure where the Zyxel Device sends logs, and which type of logs the Zyxel Device records.

If you have a server that is running a syslog service, you can also save log files to it by enabling **Syslog Logging** and then entering the IP address of the server in the **Syslog Server** field. Select **Remote** to store logs on the syslog server, or select **Local File** to store logs on the Zyxel Device. Select **Local File and Remote** to store logs on both the Zyxel Device and on the syslog server.

---

#### Syslog Setting

Syslog Logging ☒

Mode Remote

Syslog Server 192.168.1.179 (Server NAME or IPv4/IPv6 Address)

UDP Port 9090 (Server Port)

---

#### E-mail Log Settings

E-mail Log Settings ☐

---

#### Active Log

System Log

- ☒ WAN-DHCP
- ☒ DHCP Server
- ☐ PPPoE
- ☒ TR-069
- ☒ HTTP
- ☒ UPNP
- ☒ System


Security Log

- ☒ Account
- ☒ Attack
- ☒ Firewall
- ☒ MAC Filter

In my case, I was using a Zyxel router that had some logging functionalities. I set the syslog server address and the UDP port to send the logging. This address is where my Splunk software is installed. Now we need to configure Splunk to listen on that 9090 UDP port!

So in Splunk, we go to the **Add Data** option.


### Or get data in with the following methods



**Upload**

files from my computer


Local log files  
Local structured files (e.g. CSV)  
[Tutorial for adding data](#)



**Monitor**

files and ports on this Splunk platform instance

Files - HTTP - WMI - TCP/UDP - Scripts  
Modular inputs for external data sources



**Forward**

data from a Splunk forwarder

Files - TCP/UDP - Scripts

Then **Monitor**. And we choose **TCP/UDP**. Set the UDP port.

The screenshot shows the 'TCP / UDP' configuration page in the Splunk interface. On the left is a sidebar with navigation links: 'Files & Directories', 'HTTP Event Collector', 'TCP / UDP' (selected), 'Scripts', and 'Splunk Assist Instance Identifier'. The main content area is titled 'Configure this instance to listen on any TCP or UDP port to capture data sent over the network (such as syslog). Learn More'. It features a toggle switch between 'TCP' and 'UDP', with 'UDP' selected. Below this, there are three input fields: 'Port' with the value '9090' and an example of '514'; 'Source name override' with the value 'optional' and a note 'host:port'; and 'Only accept connection from' with the value 'optional' and an example '10.1.2.3, lbadhost.splunk.com, \*.splunk.com'.

Then I set some options like the source type, Host, and App context.

The screenshot shows the configuration page for 'Source type', 'App context', 'Host', and 'Index'. On the left is a sidebar with sections: 'Source type', 'App context', 'Host', 'Index', and 'FAQ'. The main content area has four sections: 1. 'Source type' with a description and a 'Select' button showing 'log2metrics\_keyvalue'. 2. 'App context' with a description and a dropdown menu showing 'Search & Reporting (search)'. 3. 'Host' with a description and a 'Method' dropdown menu showing 'IP'. 4. 'Index' with a description and a dropdown menu showing 'Default', with a link 'Create a new index'.

After that we click review, we check everything is ok and then we are done! Let's see how the logging looks like!

## 4. Searching

We click the option **Search & Reporting** on the home page, and we can start to perform some searches on the logs that we have!

The first thing I did was to log in into the router once again to see how the events look like

### New Search

host="192.168.1.1" login

✓ 2 events (22/01/2023 11:00:00.000 to 23/01/2023 11:28:17.000) No Event Sampling ▼

Events (2) Patterns Statistics Visualization

Format Timeline ▼ — Zoom Out + Zoom to Selection × Deselect

List ▼ ✓ Format 50 Per Page ▼

< Hide Fields

≡ All Fields

SELECTED FIELDS

a host 1

a source 1

a sourcetype 1

INTERESTING FIELDS

# date\_hour 1

# date\_mday 1

# date\_minute 1

a date\_month 1

# date\_second 1

a date\_wday 1

# date\_year 1

a date\_zone 1

a index 1

# linecount 1

a punct 1

a splunk\_server 1

# timeendpos 1

# timestartpos 1

+ Extract New Fields

i	Time	Event
>	23/01/2023 11:27:12.000	Jan 23 11:27:12 user.info zHttpd: Account: User [REDACTED] 'login' from the host(192.168.1.179). host = 192.168.1.1 source = udp:9090 sourcetype = log2metrics_keyvalue
>	23/01/2023 11:27:12.000	Jan 23 11:27:12 user.info zHttpd: Account: User [REDACTED] 'login' from the host(192.168.1.179). host = 192.168.1.1 source = udp:9090 sourcetype = log2metrics_keyvalue

---

Nice! So, we will receive many events from the router. Now we can make searches and start to gain some hands-on experience with Splunk!

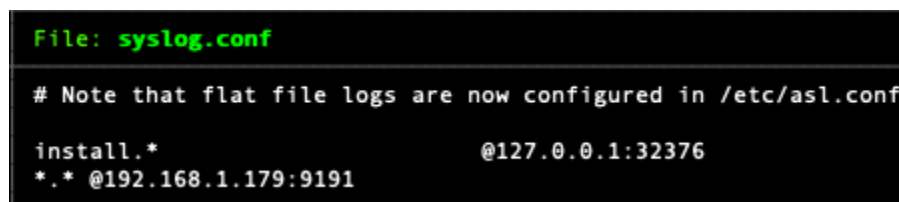
The next step is going to be to add more logs from other sources to Splunk.

## 5. Forwarding the logs from my computer to splunk

In this case I will send the syslogs from a macOS to Splunk. For this purpose we need to modify the **syslog.conf** file that lives in /etc.

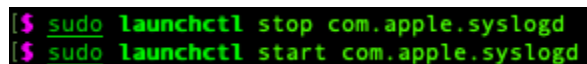
We need to add the following line: **\*.\*@ip:port**

The IP address is the IP address of the computer where you have splunk installed. And the port is the port that you will listen on Splunk to receive the logs.



```
File: syslog.conf
# Note that flat file logs are now configured in /etc/asl.conf
install.* @127.0.0.1:32376
*.* @192.168.1.179:9191
```

Then we need to execute these commands to restart the syslogd daemon



```
$ sudo launchctl stop com.apple.syslogd
$ sudo launchctl start com.apple.syslogd
```

Finally, we need to configure Splunk to listen on the port that we specified on the syslog.conf to listen. Like we did when forwarding the router logs.

Now we can see the logs from our mac computer!



