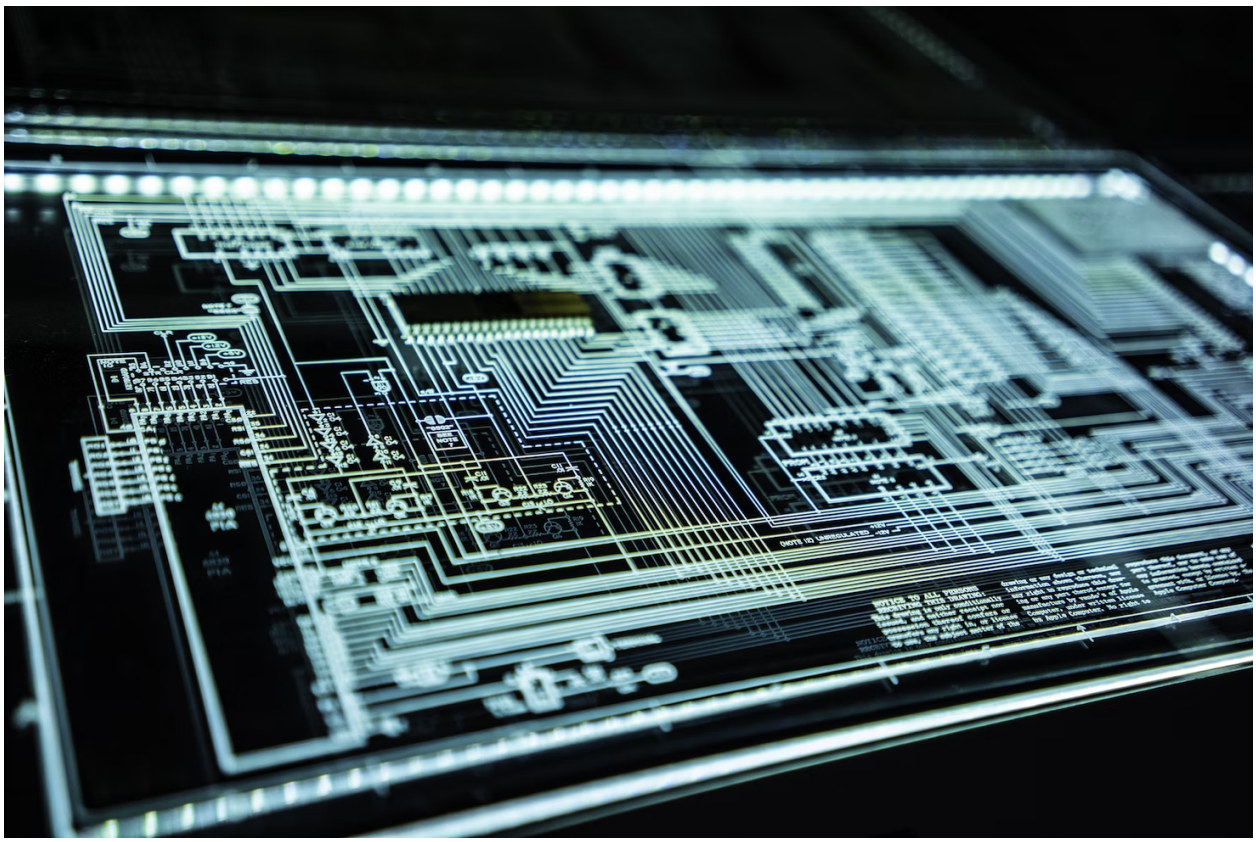
Rafael José

MiniSOC
Documentation

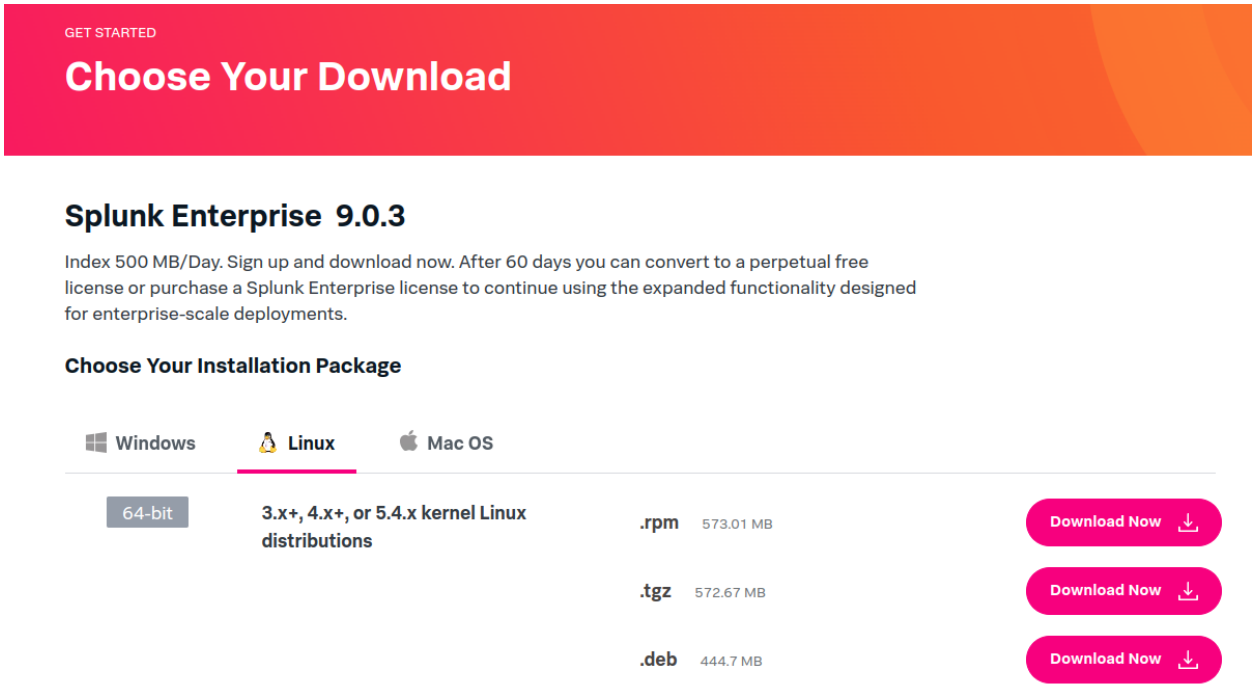


Hi, my name is Rafael. Welcome to my miniSOC documentation!

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.



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

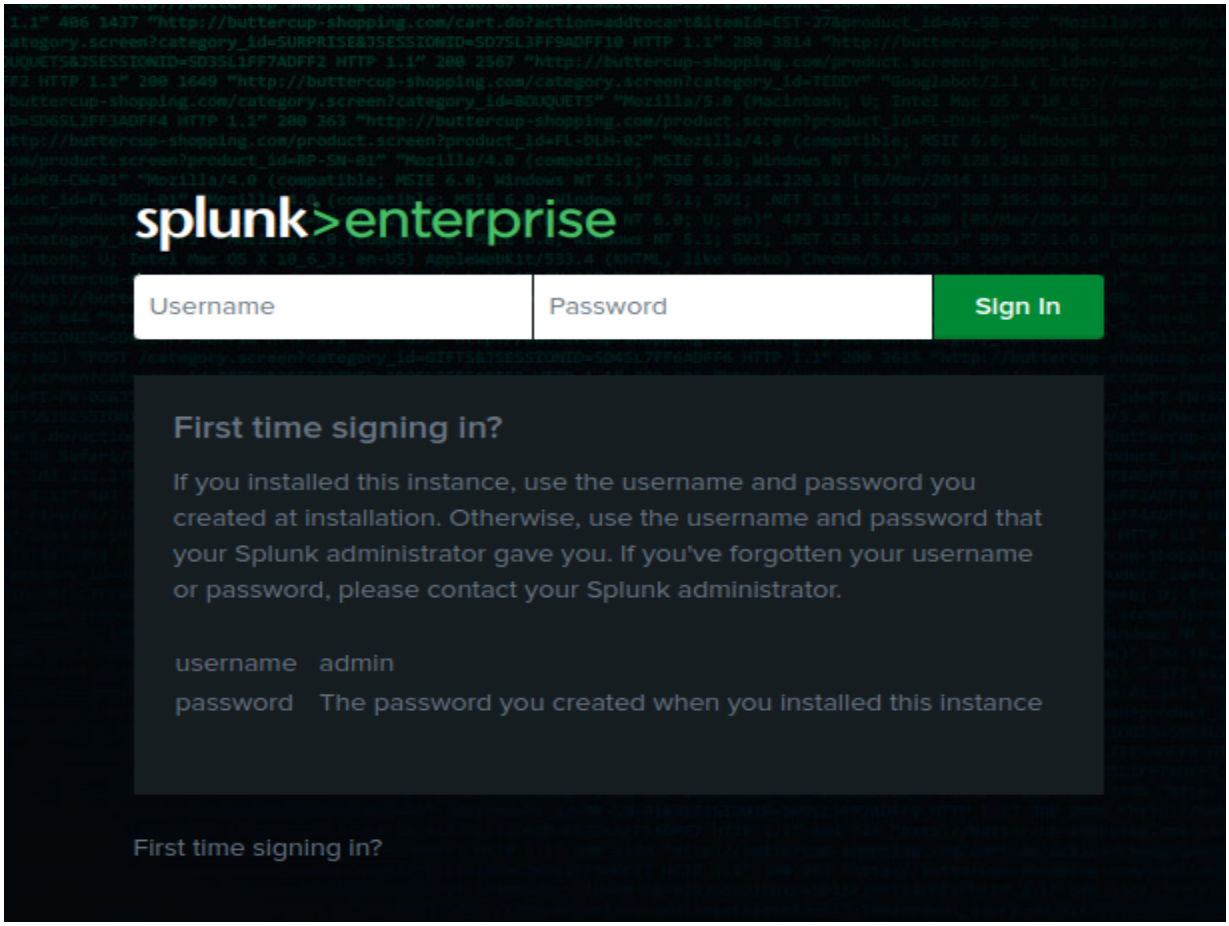
We can choose to start or enable Splunk every time the system starts. I will choose to start it manually every time the system starts.

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

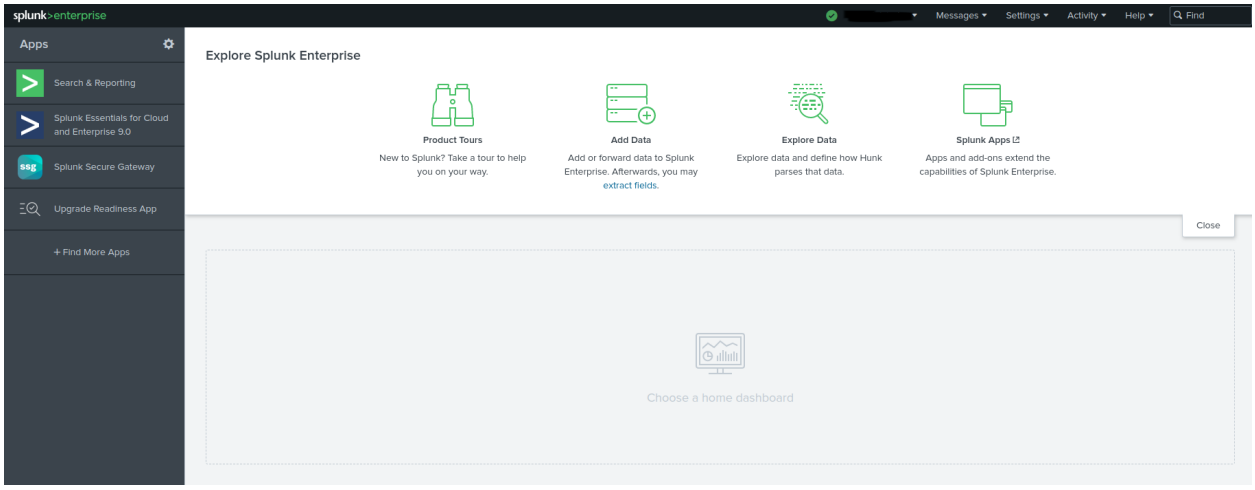
```
sudo /opt/splunk/bin/splunk start
```

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.

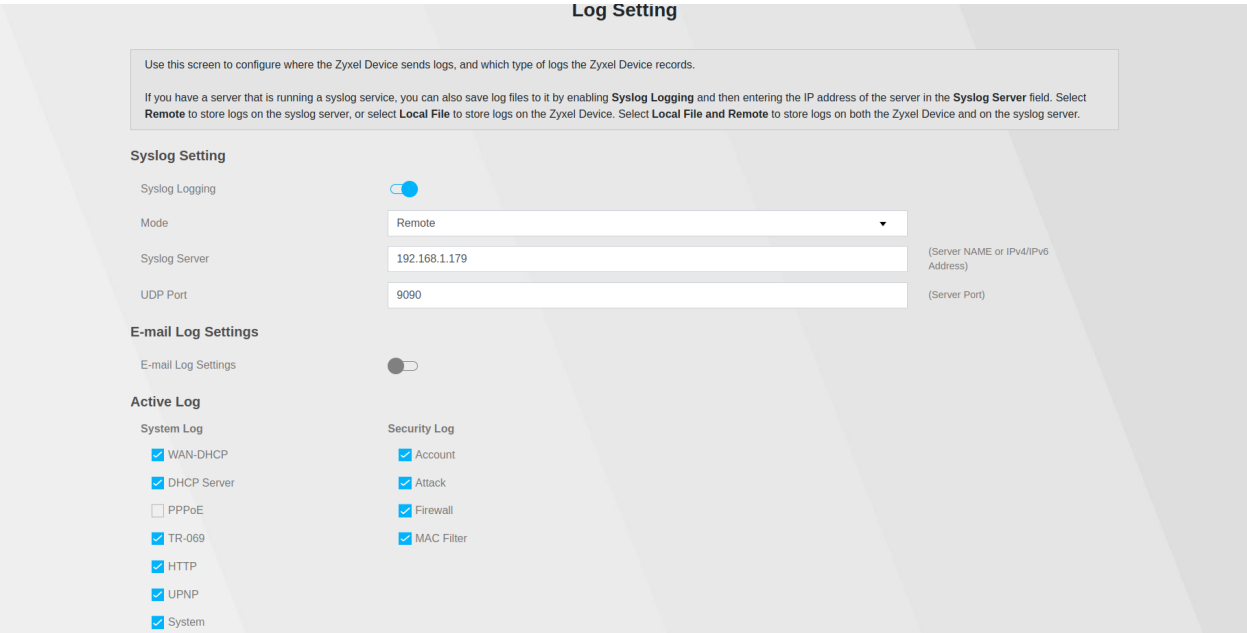


Log in with your credentials.



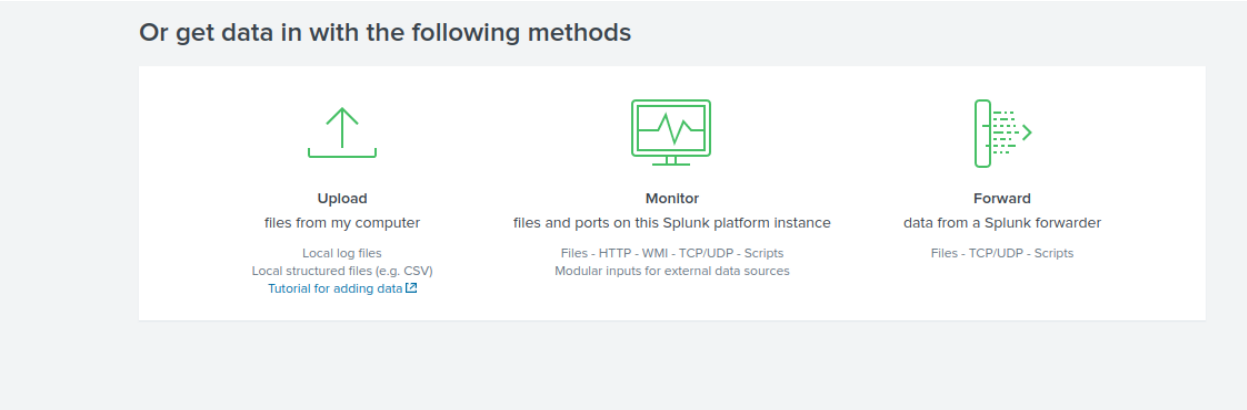
3. Forwarding the logs from my router to splunk

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.

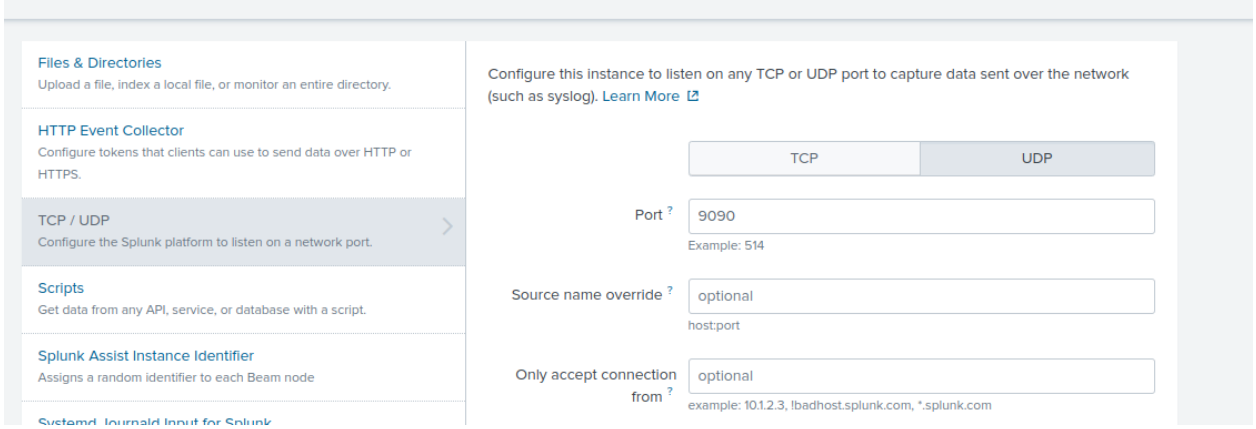


In my case, I was using a Zyxel router that had some logging functionalities. I set the syslog server address and the UDP port to send the logging. This address is were my Splunk software is installed. Now we need to configure Splunk to listen on that 9090 UDP port!

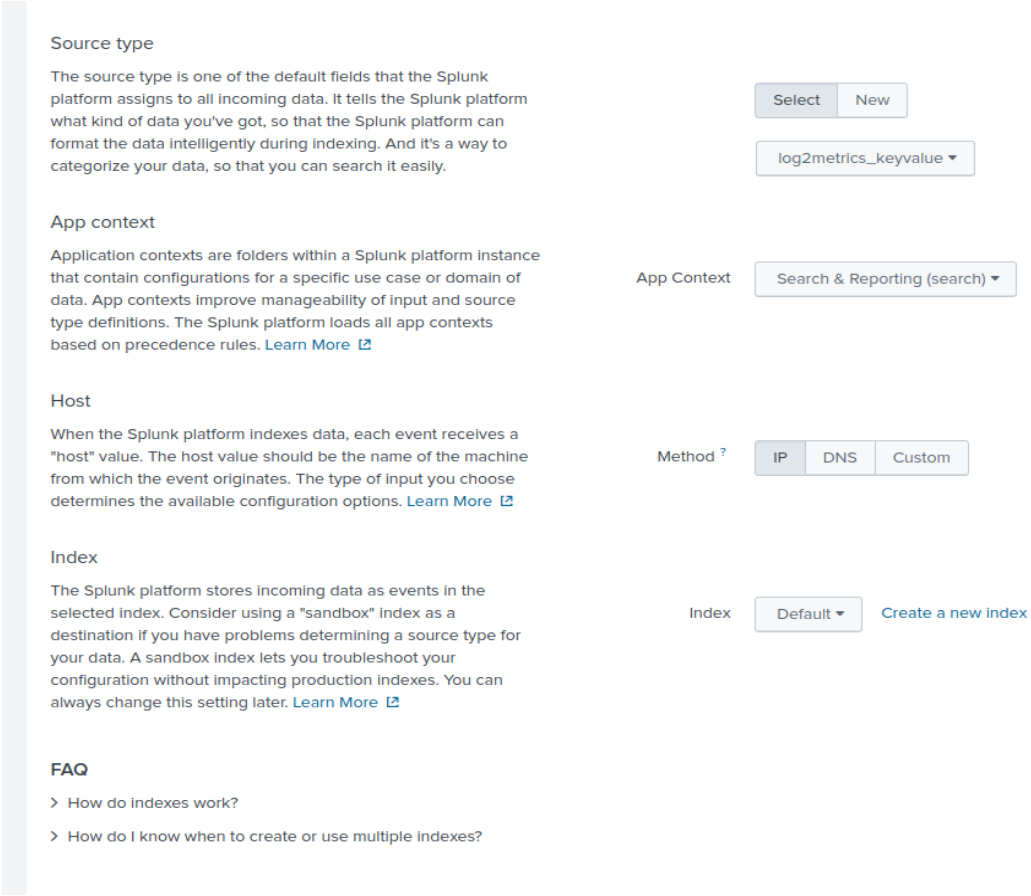
So in Splunk, we go to the **Add Data** option.



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



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

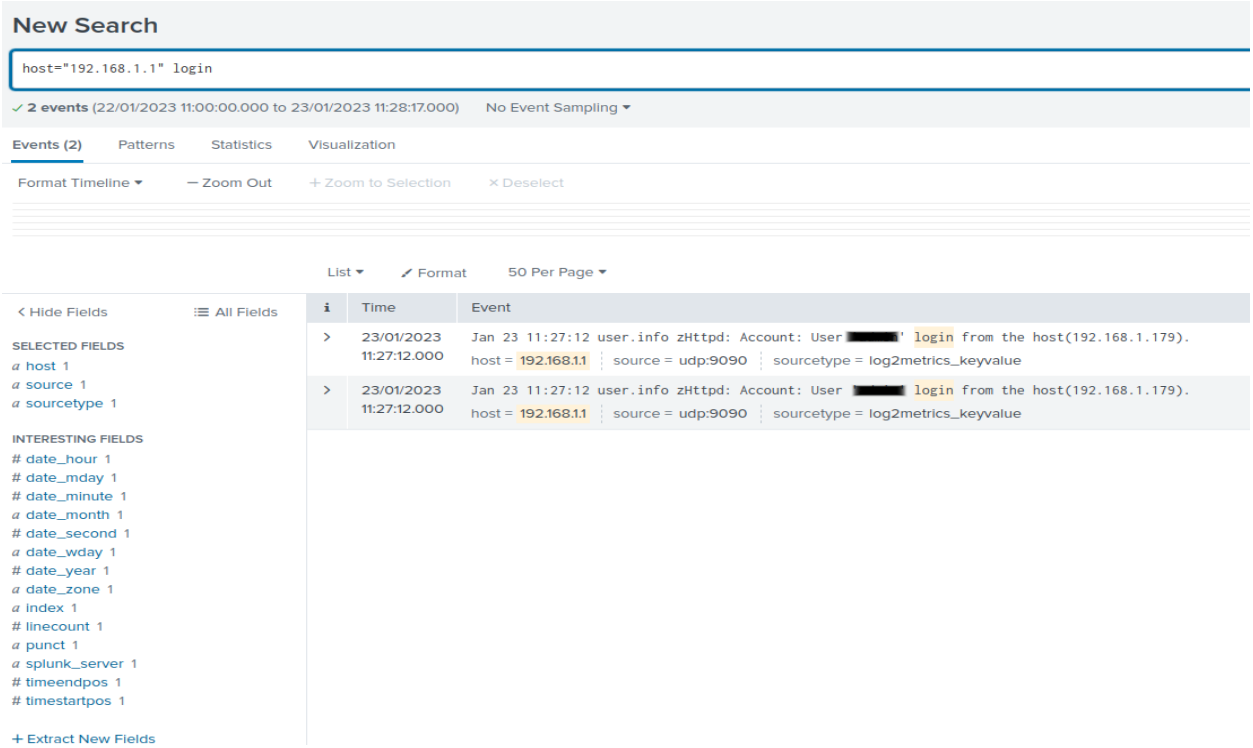


After that we click review, we check everything is ok and then we are done! Let's see how the logging looks like!

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



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.

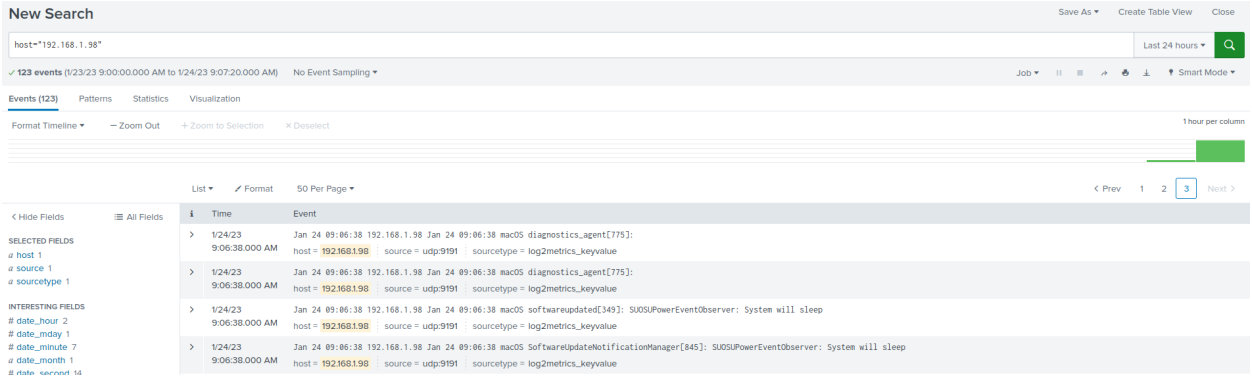
```
File: syslog.conf

# 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!


New Search
Save As
Create Table View
Close
host="192.168.1.98"
Last 24 hours
123 events (1/23/23 9:00:00.000 AM to 1/24/23 9:07:20.000 AM)
No Event Sampling
Job
Smart Mode
Events (123)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
List
Format
50 Per Page
Prev
1
2
3
Next
Hide Fields
All Fields
SELECTED FIELDS
host 1
source 1
sourcetype 1
INTERESTING FIELDS
date_hour 2
date_mday 1
date_minute 7
date_month 1
Time
Event
1/24/23 9:06:38.000 AM
Jan 24 09:06:38 192.168.1.98 Jan 24 09:06:38 macOS diagnostics_agent[775]:
host = 192.168.1.98 source = udp:9191 sourcetype = log2metrics_keyvalue
1/24/23 9:06:38.000 AM
Jan 24 09:06:38 192.168.1.98 Jan 24 09:06:38 macOS diagnostics_agent[775]:
host = 192.168.1.98 source = udp:9191 sourcetype = log2metrics_keyvalue
1/24/23 9:06:38.000 AM
Jan 24 09:06:38 192.168.1.98 Jan 24 09:06:38 macOS softwareupdated[349]: SUOSUPowerEventObserver: System will sleep
host = 192.168.1.98 source = udp:9191 sourcetype = log2metrics_keyvalue
1/24/23 9:06:38.000 AM
Jan 24 09:06:38 192.168.1.98 Jan 24 09:06:38 macOS SoftwareUpdateNotificationManager[845]: SUOSUPowerEventObserver: System will sleep
host = 192.168.1.98 source = udp:9191 sourcetype = log2metrics_keyvalue