

Task 1:

```
timothyd@ubuntu:~$ sudo dpkg -i ~/Downloads/splunk*.deb
Selecting previously unselected package splunk.
(Reading database ... 259129 files and directories currently installed.)
Preparing to unpack .../splunk-9.2.1-78803f08aabb-linux-2.6-amd64.deb ...
Unpacking splunk (9.2.1+78803f08aabb) ...
```

In this step, I have created a splunk account and downloaded the .deb file. Then I installed the DEB through my terminal.

```
timothyd@ubuntu:~$ sudo /opt/splunk/bin/splunk start
SPLUNK GENERAL TERMS

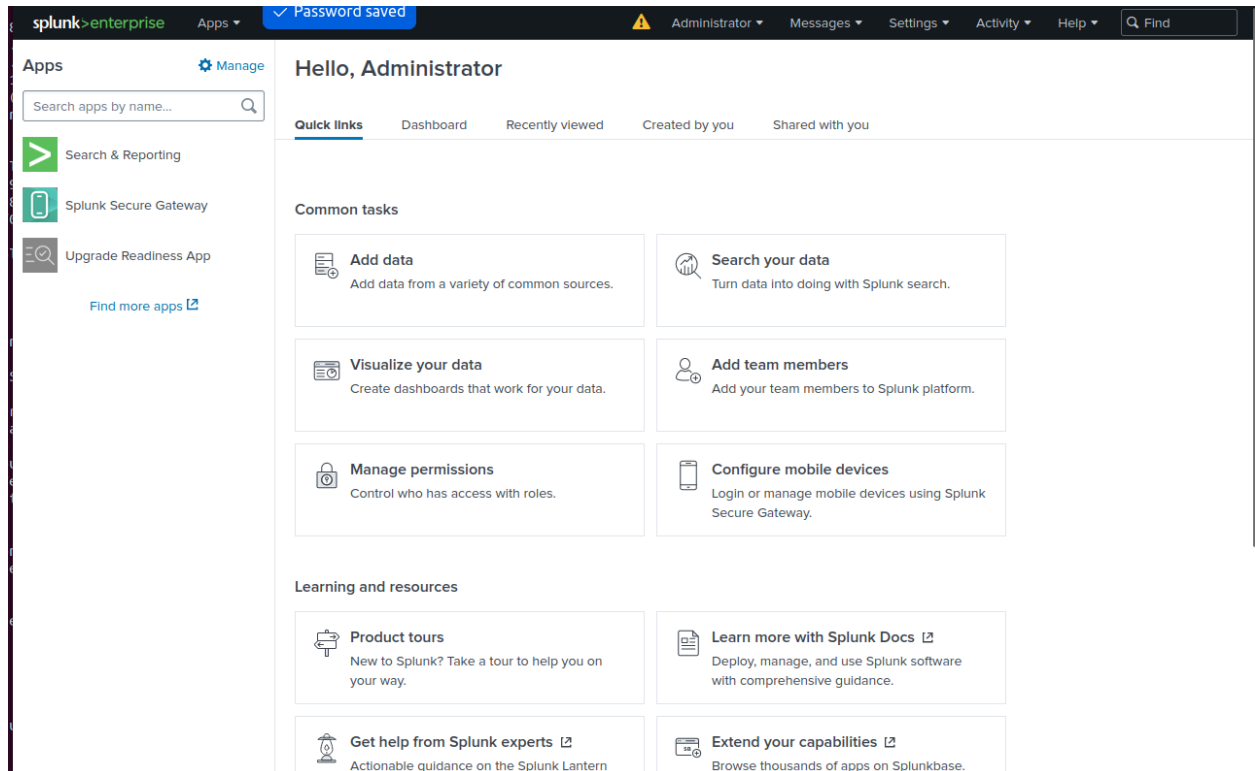
Last Updated: August 12, 2021

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, or by downloading, installing, accessing or using the Offerings, you agree to these General Terms. If you are entering into these General Terms on behalf of Customer, you represent that you have the authority to bind Customer. If you do not agree to these General Terms, or if you are not authorized to accept the General Terms on behalf of the Customer, do not download, install, access, or use any of the Offerings.

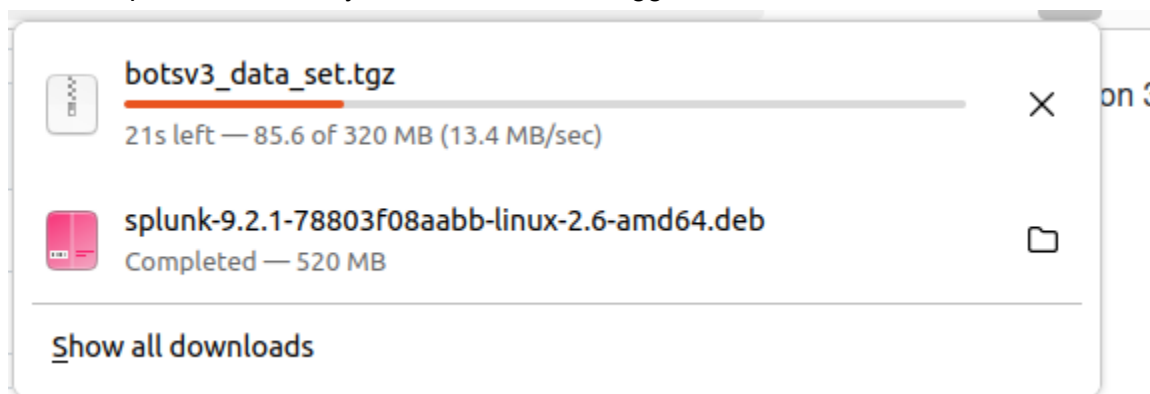
See the General Terms Definitions Exhibit attached for definitions of capitalized terms not defined herein.

1. License Rights
(A) General Rights. You have the nonexclusive, worldwide, nontransferable and nonpublicable right, subject to payment of applicable Fees and compliance
```

Here, I have started Splunk in my Ubuntu VM.



In this step, I am now in my browser and have logged in.



Here I am downloading the botsv3 dataset.

```

timothyd@ubuntu:~$ sudo mv ~/Downloads/botsv3_data_set.tgz /opt/splunk/etc/apps/
timothyd@ubuntu:~$ sudo gunzip /opt/splunk/etc/apps/botsv3_data_set.tgz
gzip: /opt/splunk/etc/apps/botsv3_data_set.tgz: No such file or directory
timothyd@ubuntu:~$ sudo gunzip /opt/splunk/etc/apps/botsv3_data_set.tgz
timothyd@ubuntu:~$ sudo tar -xvf /opt/splunk/etc/apps/botsv3_data_set.tar -C /opt/splunk/etc/apps/
botsv3_data_set/
botsv3_data_set/lookups/
botsv3_data_set/LICENSE
botsv3_data_set/bin/
botsv3_data_set/var/
botsv3_data_set/default/
botsv3_data_set/README.txt
botsv3_data_set/default/app.conf
botsv3_data_set/default/indexes.conf
botsv3_data_set/default/tags.conf
botsv3_data_set/default/props.conf
botsv3_data_set/default/data/
botsv3_data_set/default/transforms.conf
botsv3_data_set/default/data/ui/
botsv3_data_set/default/data/ui/nav/
botsv3_data_set/default/data/ui/views/

```

In this step, I have moved the .tgz file and then unzipped it.

```

timothyd@ubuntu:~$ sudo /opt/splunk/bin/splunk restart
Stopping splunkd...
Shutting down. Please wait, as this may take a few minutes.
...
Stopping splunk helpers...

Done.

Splunk> The IT Search Engine.

```

Here, I am restarting splunk.

The screenshot shows the Splunk Enterprise web interface. At the top, there's a navigation bar with 'splunk>enterprise' and various menu items like 'Apps', 'Administrator', 'Messages', 'Settings', 'Activity', and 'Help'. Below this is a 'Search & Reporting' section with a 'New Search' button. The search query 'index=botsv3' is entered in the search bar, and the time scope is set to 'All time'. The results show '452,580 of 417,773 events matched'. The interface includes tabs for 'Events (452,580)', 'Patterns', 'Statistics', and 'Visualization'. At the bottom, there's a pagination bar showing '1' of 8 pages.

In this step, I have navigated to the search page and then changed the time scope to all-time. I am now searching for “index=botsv3”.

New Search

Save As

Create Table View

Close

index=btosv3 host=matar | stats count by source

All time

✓ 84,337 events (before 4/22/24 10:32:22.000 PM)

No Event Sampling

Job

In this step, we were able to change the search to “index=btosv3 host=matar | stats count by source”.

```

}
reply_time: 4676
request_time: 349994
response_code: 250
response_time: 0
sender: Grace Hoppy <ghoppy@froth.ly>
sender_alias: Grace Hoppy
sender_email: ghoppy@froth.ly
server_response: 250 2.0.0 Ok: queued as 6C7831794E8
src_ip: 104.47.38.43
src_mac: 06:E3:CC:18:AA:33
src_port: 1920
subject: Fw: All your datas belong to us
time_taken: 354670
timestamp: 2018-08-20T15:19:34.777033Z
transport: tcp
}

```

Show as raw text

host = matar | source = stream:smtp | sourcetype = stream:smtp

After selecting “stream:smtp” and the “View Events” I am able to see this email from Grace Hoppy with the subject saying “All your datas belong to us”.

```
receiver_type: [ [ ] ]
reply_time: 4096
request_time: 191827
response_code: 250
response_time: 0
sender: HyunKi Kim<hyunki1984@naver.com>
sender_alias: HyunKi Kim
sender_email: hyunki1984@naver.com
server_response: 250 2.0.0 Ok: queued as EC0431794E8
src_ip: 104.47.34.50
src_mac: 06:E3:CC:18:AA:33
src_port: 61105
subject: All your datas belong to us
time_taken: 195923
timestamp: 2018-08-20T15:15:00.143986Z
transport: tcp
}
```

Show as raw text

After adding “subject:All your datas*”, we were able to find this email with the ip 10.47.34.50.

index=botsv3 | stats count as cnt by host | sort cnt desc | head 10

✓ 2,083,056 events (before 4/22/24 10:38:26.000 PM) No Event Sampling

Events Patterns **Statistics (10)** Visualization

20 Per Page Format Preview

host	cnt
hoth	382718
serverless	247791
BSTOLL-L	240882
gacruх.1-0920036c8ca91e501	175345
nars.1-08e52f8b5a034012d	158512
natar	84337
ip-172-16-0-109.ec2.internal	83673
FROTHLY-FW1	80192
splunkhvf.froth.ly	78478
BTUN-L	76371

Here I have made a new query to get the top 10 source IP addresses. I am going to save this report.

splunk>enterprise Apps

Administrator Messages Settings Activity Help Find

Search Analytics Datasets Reports Alerts Dashboards

Search & Reporting

Top 10 Hosts

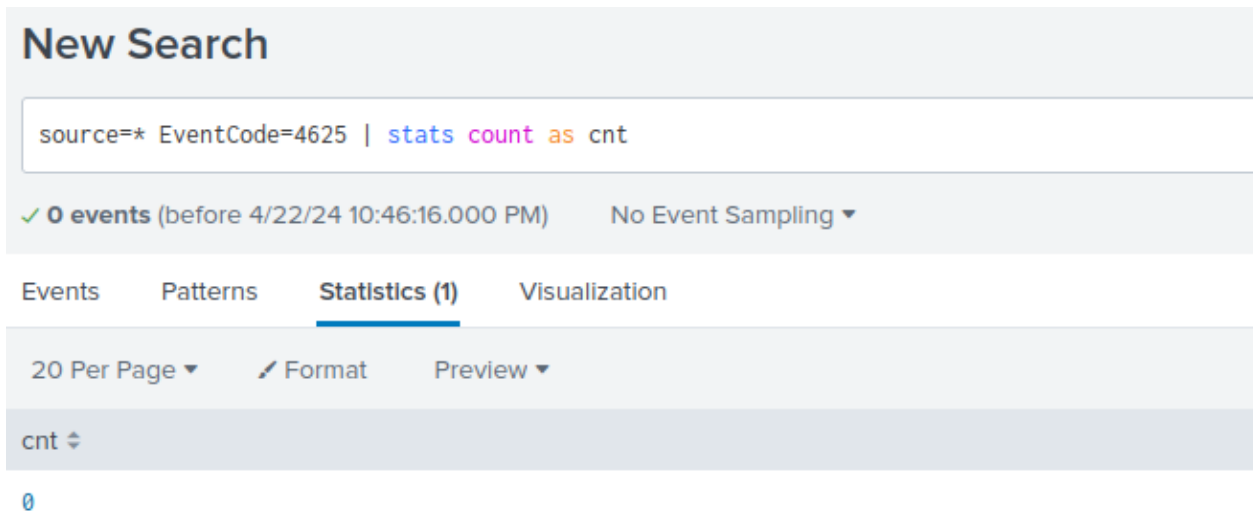
All time

✓ 2,083,056 events (before 4/22/24 10:38:26.000 PM)

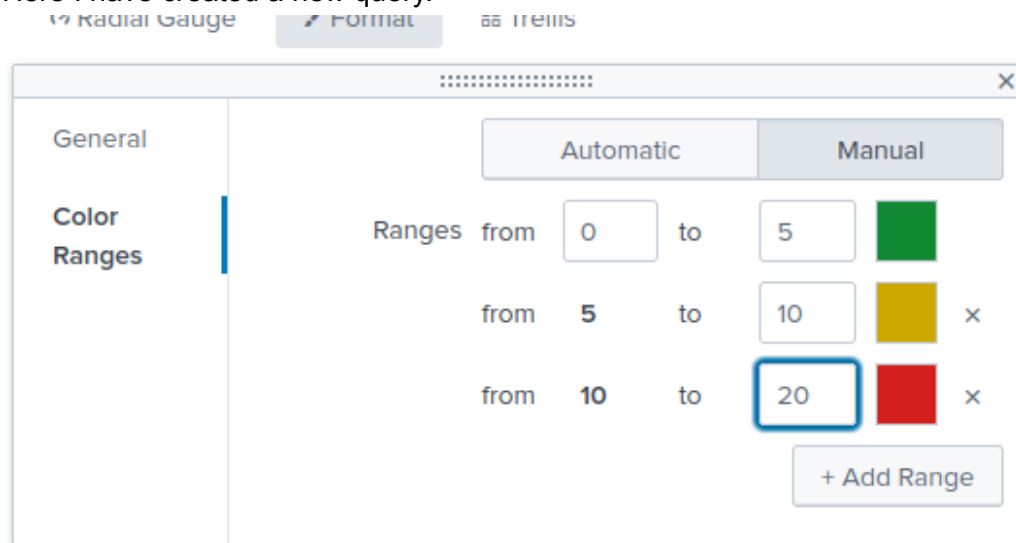
10 results 20 per page

host	cnt
hoth	382718
serverless	247791
BSTOLL-L	240882
gacruх.1-0920036c8ca91e501	175345
nars.1-08e52f8b5a034012d	158512
natar	84337
ip-172-16-0-109.ec2.internal	83673
FROTHLY-FW1	80192
splunkhvf.froth.ly	78478
BTUN-L	76371

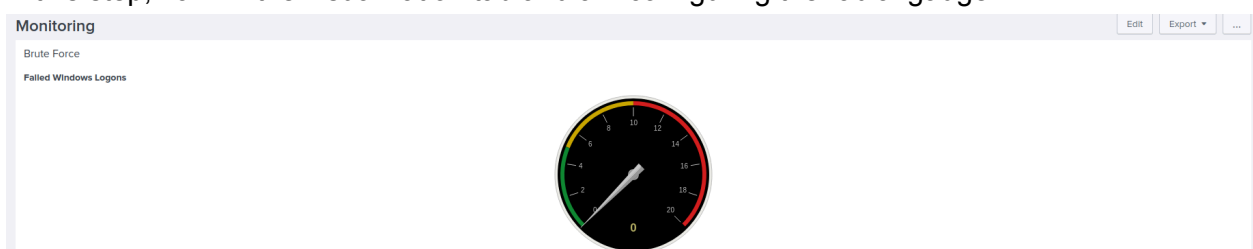
Here is the report and it can be refreshed and exported at any time.



Here I have created a new query.



In this step, I am in the visualization tab and am configuring the radial gauge.



Here I have saved it as a new dashboard and added a title and description. The query is returning 0 for some reason which is why the gauge is at 0. I have followed the steps and my query is correct, but it is still resulting in 0 returned.

New Search

Save AsCreate Table ViewClose

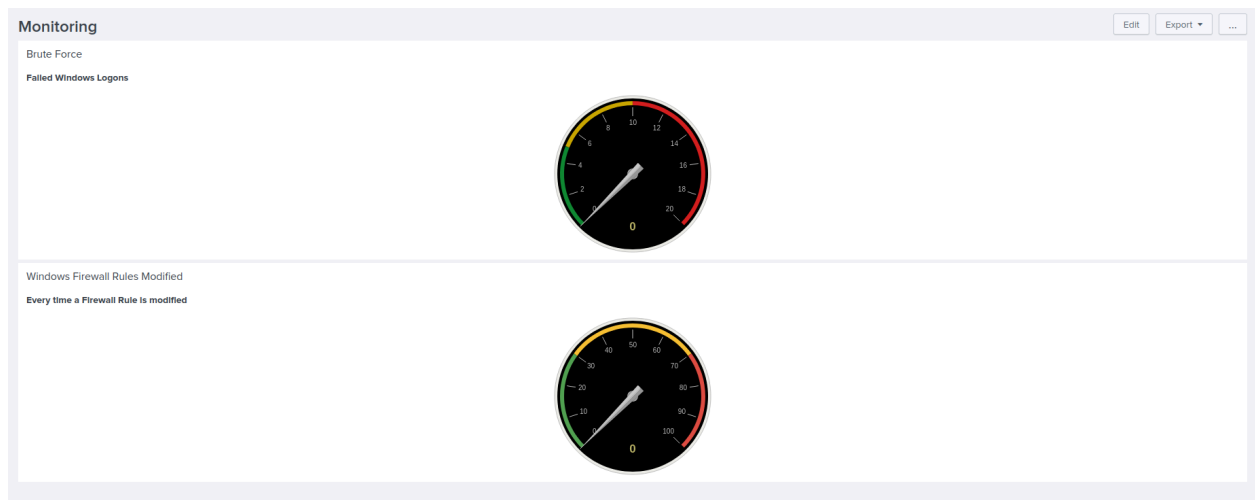
source= EventCode=4947 stats count as cntAll time

0 events (before 4/24/24 11:36:12.000 PM)No Event SamplingJob

EventsPatternsStatistics (1)Visualization

20 Per PageFormatPreview


This is a new query that I have made. This will check for all the times that a Windows Firewall exception rule was modified. This is important to track because admins should understand what firewall rules are being implemented. If somebody is trying to change a rule, it should go through an approval process first so that it doesn't cause any future vulnerabilities. If there are many rules being modified, then an admin should go in and review these rules to ensure that they are still allowing for best security practices.



Here is the visualization. Still running into the issue where the queries are returning 0, but I have everything set up.

Task 2:

[< Back](#)



Introduction to Enterprise Security (eLearning)

Class | Course ID: EDU-1010

In Progress Registered on: 23-APR-2024

[CONTINUE](#)

Progress and Activities







Overview & Other Information

History

English | eLearning | Class ID: EDU-1010 0 USD

Total duration: 00:40 Hrs

Activities

 Introduction to Enterprise Security Videos Expires on: 24-APR-2025 at 12:00 AM  	Not evaluated	LAUNCH
 Introduction to Enterprise Security Quiz Expires on: 24-APR-2025 at 12:00 AM  	Not evaluated	LAUNCH

Overview

Here, I have logged into splunk and enrolled into the course.



Introduction to Enterprise Security (eLearning)



Course | ID: EDU-1010

Successful

Completed on: 23-APR-2024

EXPORT CERTIFICATE

PRINT CERTIFICATE

Progress and Activities

Overview & Other Information

History

English | eLearning | Class ID: EDU-1010

0 USD

Total duration: 00:40 Hrs

BUY NOW



Activities

Introduction to Enterprise Security Videos

Completed

VIEW RESULTS



Expires on: 24-APR-2025 at 12:00 AM

Completed on: 23-APR-2024



Introduction to Enterprise Security Quiz

Completed

VIEW RESULTS



Expires on: 24-APR-2025 at 12:00 AM

Completed on: 23-APR-2024





In this step, I have completed the course.