Maria Valencia

Csc 154

Lab 12

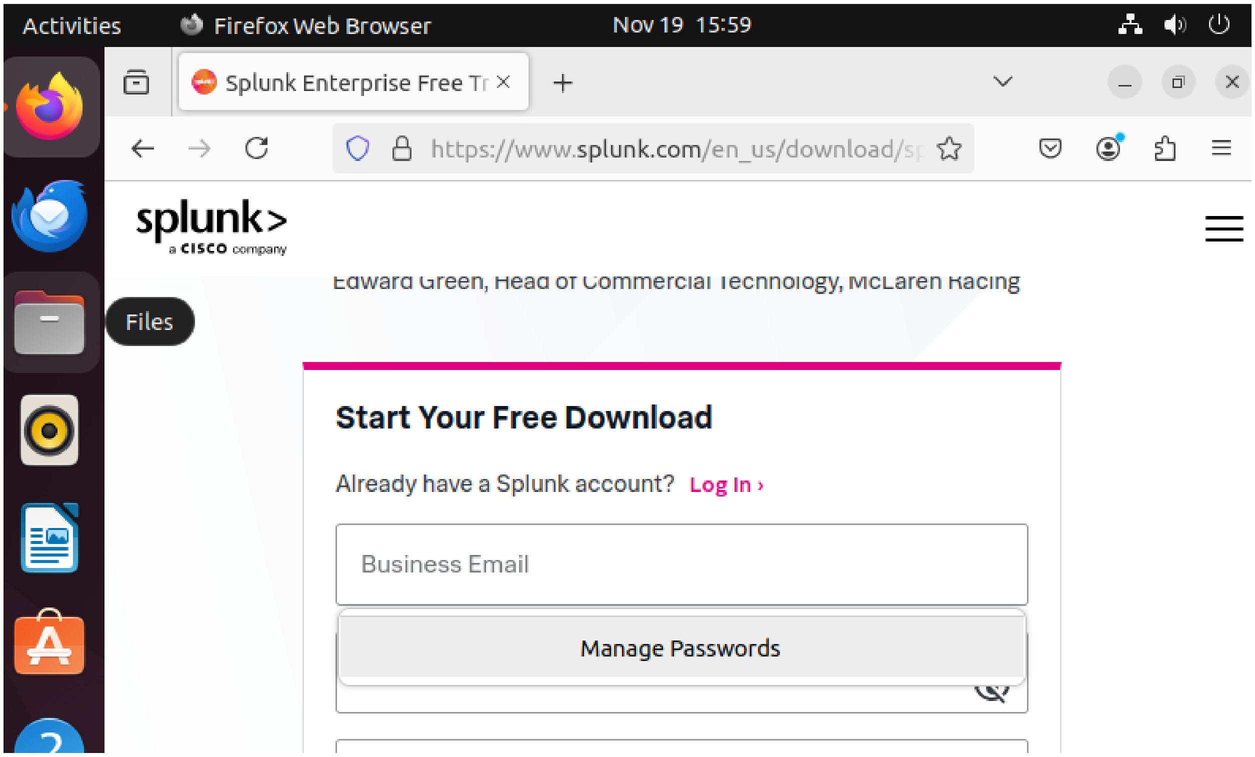
Incident Response

Exercise 12.1 - SIEM Setup

In this task, you will install splunk on your UbuntuVM , import event data, and build queries, reports, and dashboards to analyze events.

Step 1: Install Splunk Enterprise

Using your Ubuntu VM in Bridge Adapter network mode, launch a browser and navigate to https://www.splunk.com/en_us/download/splunk-enterprise.html and fill out the Create Account form with your CSUSemail address.



Edward Green, Head of Commercial Technology, McLaren Racing

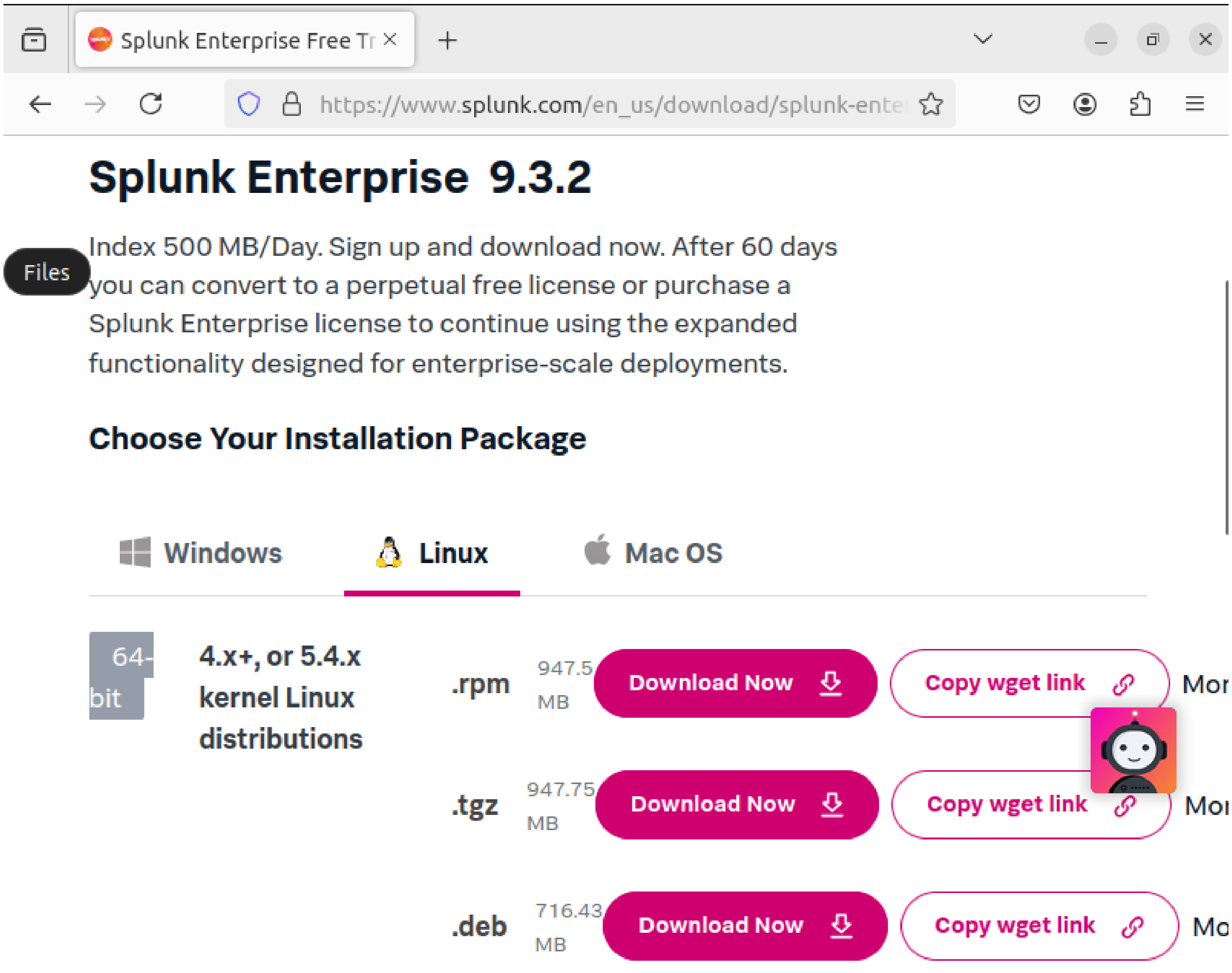
Start Your Free Download

Already have a Splunk account? Log In ›

Business Email

Manage Passwords

Upon login, you should reach the download page. Select Linux and download the ".deb" installer.


Splunk Enterprise Free Tr
https://www.splunk.com/en_us/download/splunk-ente
Files

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

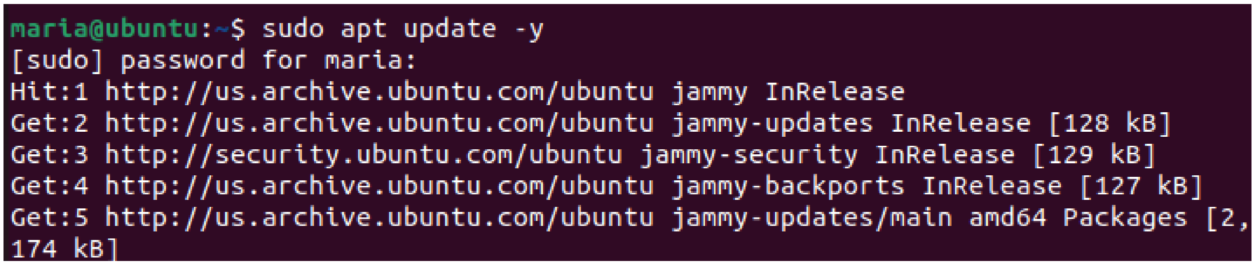
64-bit 4.x+, or 5.4.x kernel Linux distributions

.rpm 947.5 MB Download Now Copy wget link Mor

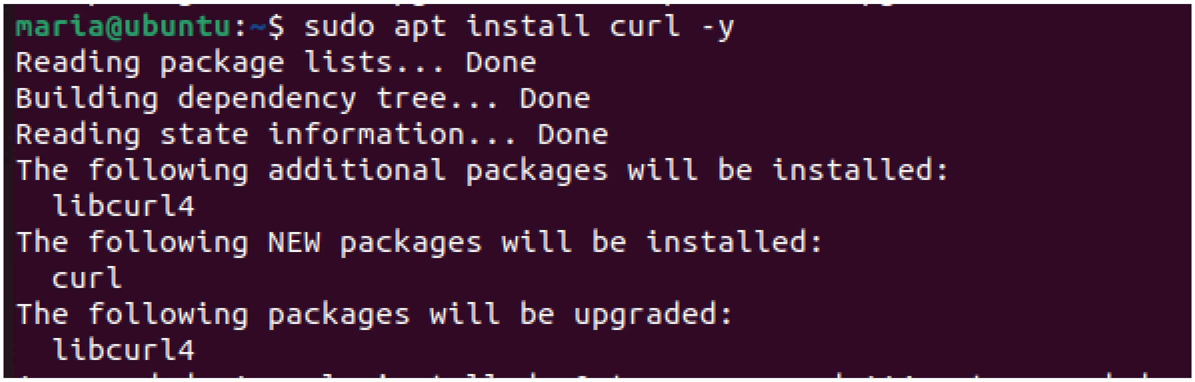
.tgz 947.75 MB Download Now Copy wget link Mor

.deb 716.43 MB Download Now Copy wget link Mo

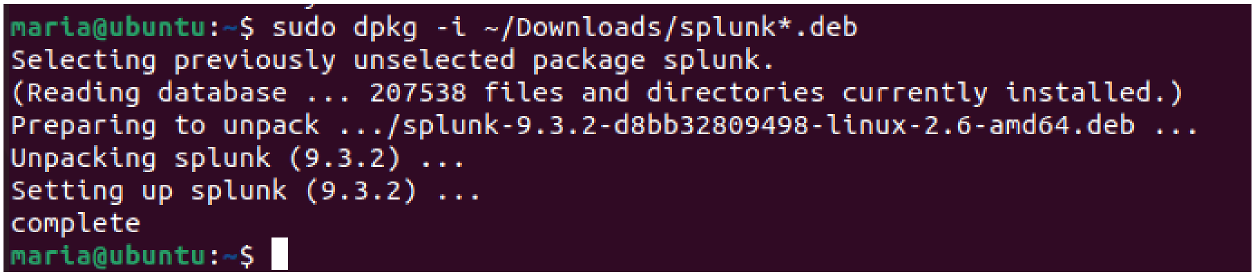
Launch a terminal and install curl and the DEB file to install Splunk Enterprise.



```
maria@ubuntu:~$ sudo apt update -y
[sudo] password for maria:
Hit:1 http://us.archive.ubuntu.com/ubuntu jammy InRelease
Get:2 http://us.archive.ubuntu.com/ubuntu jammy-updates InRelease [128 kB]
Get:3 http://security.ubuntu.com/ubuntu jammy-security InRelease [129 kB]
Get:4 http://us.archive.ubuntu.com/ubuntu jammy-backports InRelease [127 kB]
Get:5 http://us.archive.ubuntu.com/ubuntu jammy-updates/main amd64 Packages [2,
174 kB]
```



```
maria@ubuntu:~$ sudo apt install curl -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libcurl4
The following NEW packages will be installed:
  curl
The following packages will be upgraded:
  libcurl4
```

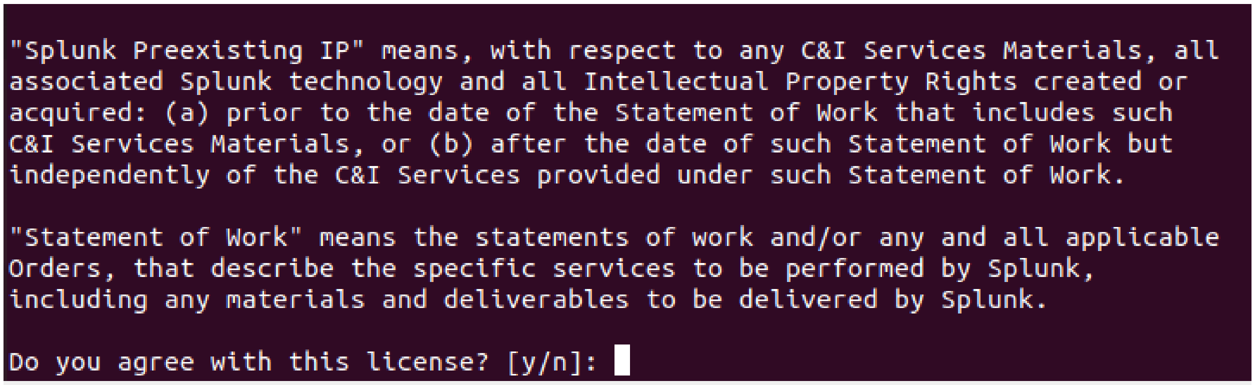


```
maria@ubuntu:~$ sudo dpkg -i ~/Downloads/splunk*.deb
Selecting previously unselected package splunk.
(Reading database ... 207538 files and directories currently installed.)
Preparing to unpack .../splunk-9.3.2-d8bb32809498-linux-2.6-amd64.deb ...
Unpacking splunk (9.3.2) ...
Setting up splunk (9.3.2) ...
complete
maria@ubuntu:~$
```

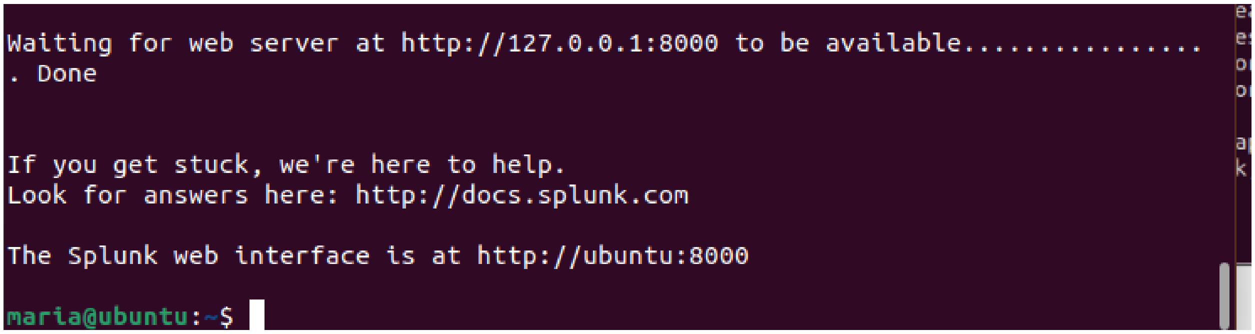
Step 2: Setup Splunk

Start Splunk within your launched Ubuntu VM terminal. When launching for the first time you will be presented with the license agreement. Use the "spacebar" and "y" keys to accept the terms. Follow the CLI questions selecting a username and password.

sudo /opt/splunk/bin/splunk start

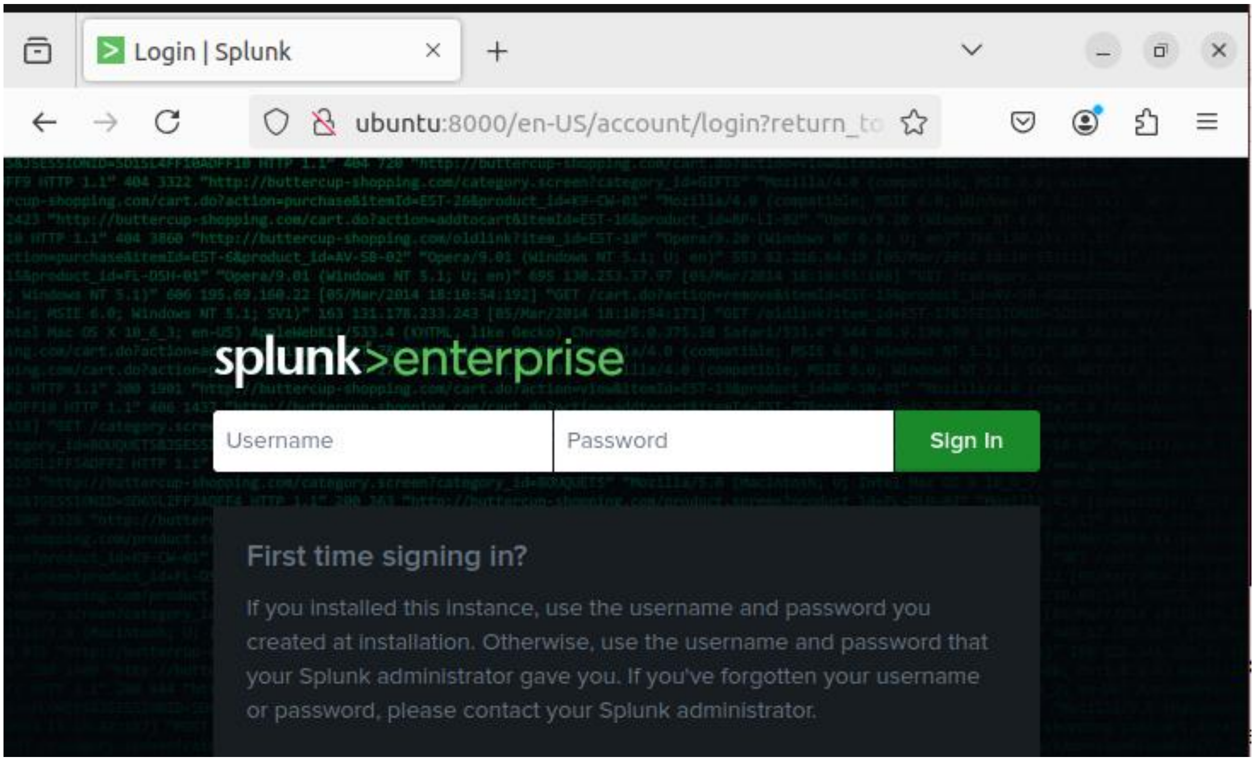


```
"Splunk Preexisting IP" means, with respect to any C&I Services Materials, all
associated Splunk technology and all Intellectual Property Rights created or
acquired: (a) prior to the date of the Statement of Work that includes such
C&I Services Materials, or (b) after the date of such Statement of Work but
independently of the C&I Services provided under such Statement of Work.

"Statement of Work" means the statements of work and/or any and all applicable
Orders, that describe the specific services to be performed by Splunk,
including any materials and deliverables to be delivered by Splunk.

Do you agree with this license? [y/n]:
```



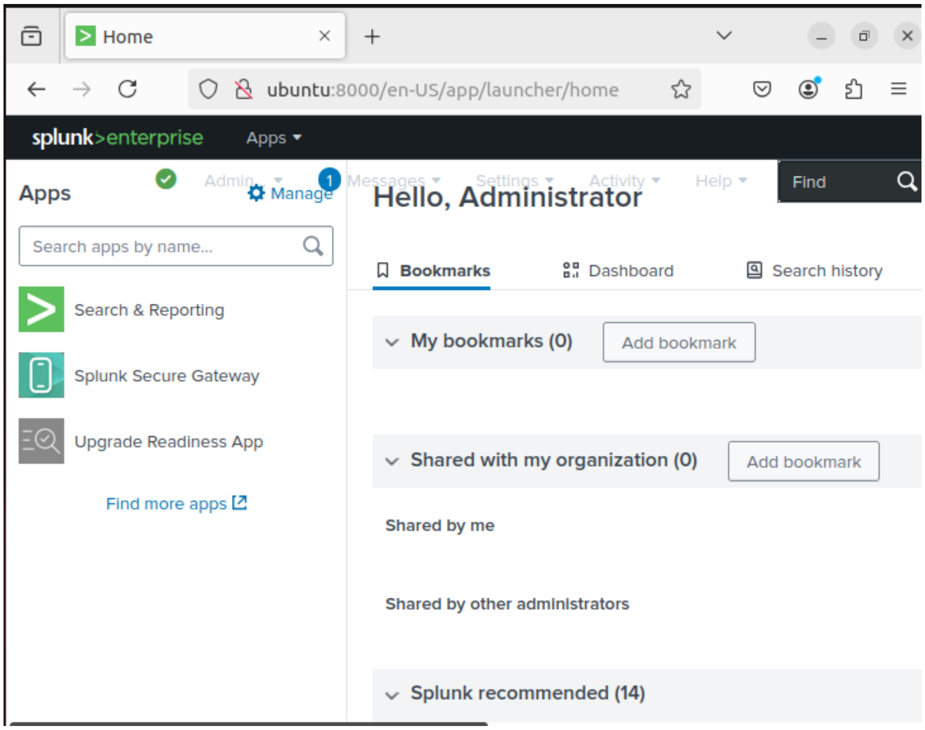
```
Waiting for web server at http://127.0.0.1:8000 to be available...............
. Done


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

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

maria@ubuntu:~$ 
```

Once the setup is complete and Splunk is running, launch a web browser within your Ubuntu VM and navigate to http://ubuntu:8000 or http://127.0.0.1:8000 where you'll be presented with your stand-alone instance of Splunk Enterprise. Login with the credentials you used during the setup.



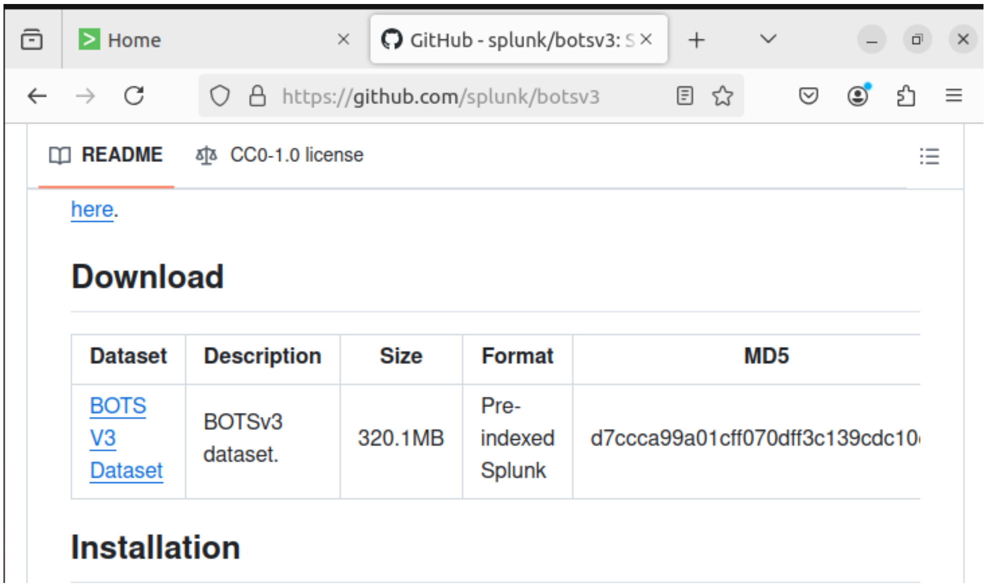
First time signing in?

If you installed this instance, use the username and password you created at installation. Otherwise, use the username and password that your Splunk administrator gave you. If you've forgotten your username or password, please contact your Splunk administrator.



Step 3: Load Data

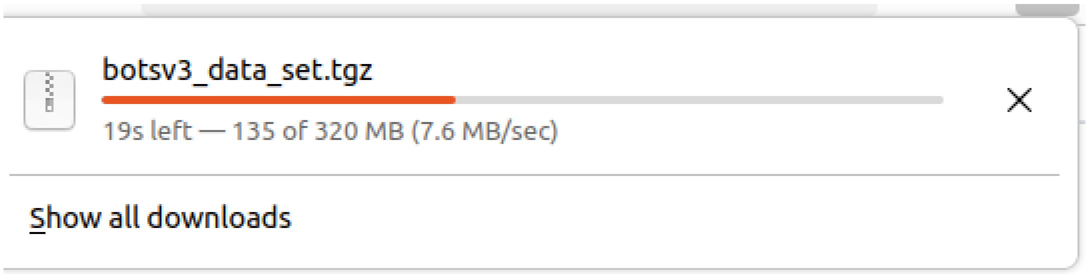
From within your Ubuntu VM, launch a browser and navigate to https://github.com/splunk/botsv3 and download the "BOTS V3 Dataset". It is about 320 MBs which may take a 10 minutes or so to download. This dataset is a curated set of logs used in Splunk's Boss of the SOC CTF challenge.



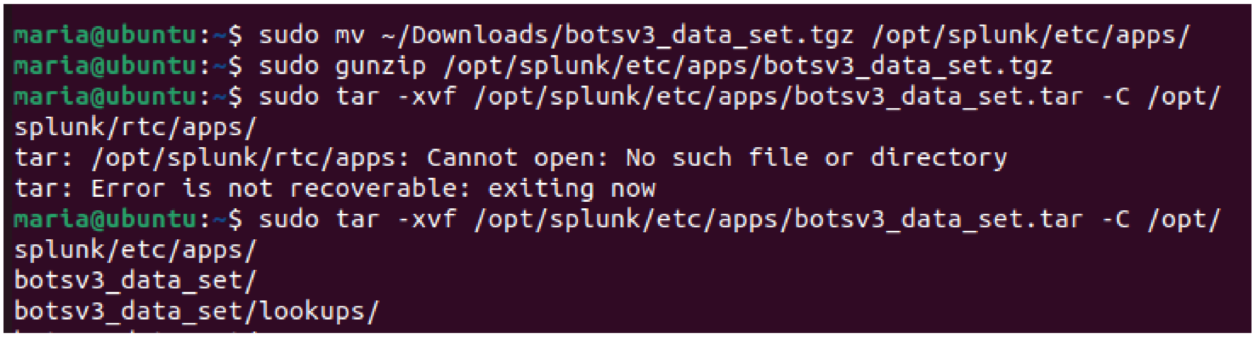
Download

Dataset	Description	Size	Format	MD5
BOTS V3 Dataset	BOTSv3 dataset.	320.1MB	Pre-indexed Splunk	d7ccca99a01cff070dff3c139cdc10

Installation

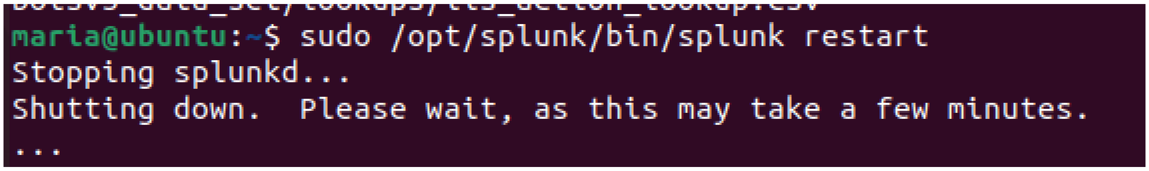


Move the downloaded botsv3 data set to "/opt/splunk/etc/apps/" and unzip the contents using gunzip and tar.



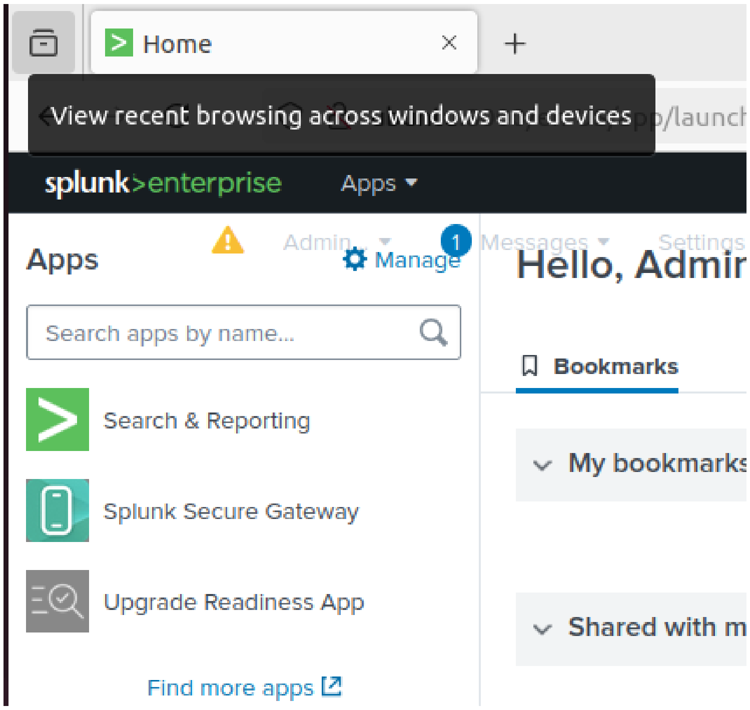
```
maria@ubuntu:~$ sudo mv ~/Downloads/botsv3_data_set.tgz /opt/splunk/etc/apps/
maria@ubuntu:~$ sudo gunzip /opt/splunk/etc/apps/botsv3_data_set.tgz
maria@ubuntu:~$ sudo tar -xvf /opt/splunk/etc/apps/botsv3_data_set.tar -C /opt/
splunk/rtc/apps/
tar: /opt/splunk/rtc/apps: Cannot open: No such file or directory
tar: Error is not recoverable: exiting now
maria@ubuntu:~$ sudo tar -xvf /opt/splunk/etc/apps/botsv3_data_set.tar -C /opt/
splunk/etc/apps/
botsv3_data_set/
botsv3_data_set/lookups/
```

Restart Splunk for the upload botsv3 data set/index to become available.

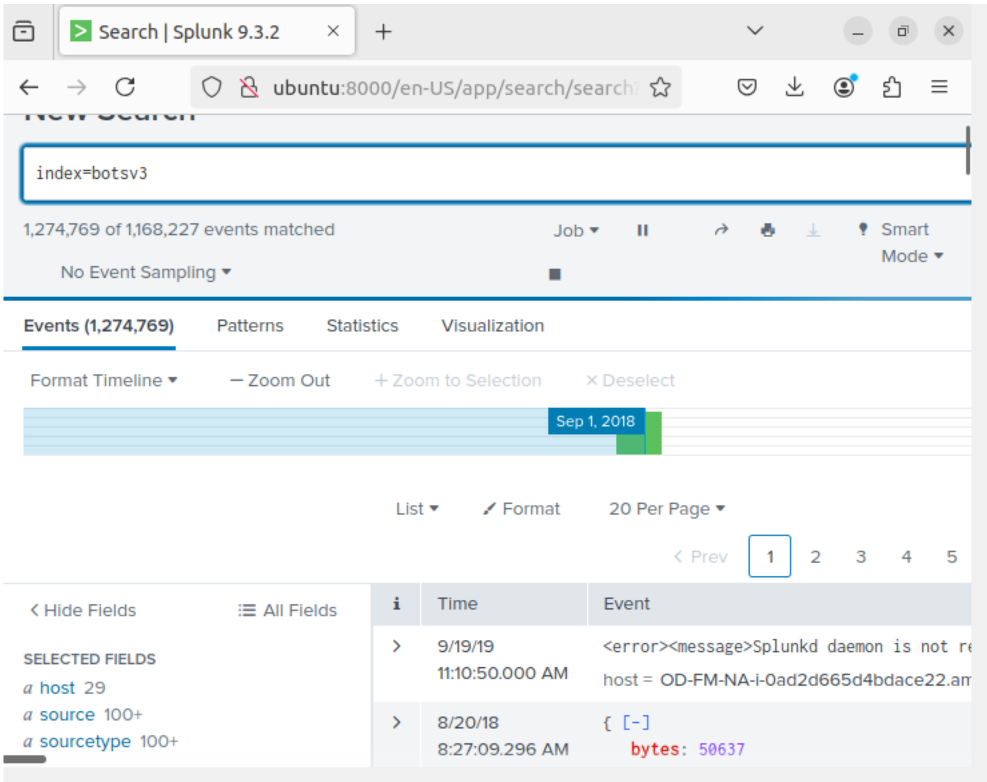


```
botsv3_data_set/lookups/tls_action_lookup.csv
maria@ubuntu:~$ sudo /opt/splunk/bin/splunk restart
Stopping splunkd...
Shutting down.  Please wait, as this may take a few minutes.
...
```

Once restarted navigate to your Splunk instance and select Apps and then "Search & Reporting".



Change the time scope to "All time" and search the term index=botsv3 to discover all available records. Wait a few minutes and observe millions of events loaded.



```
index=botsv3
```

1,274,769 of 1,168,227 events matched

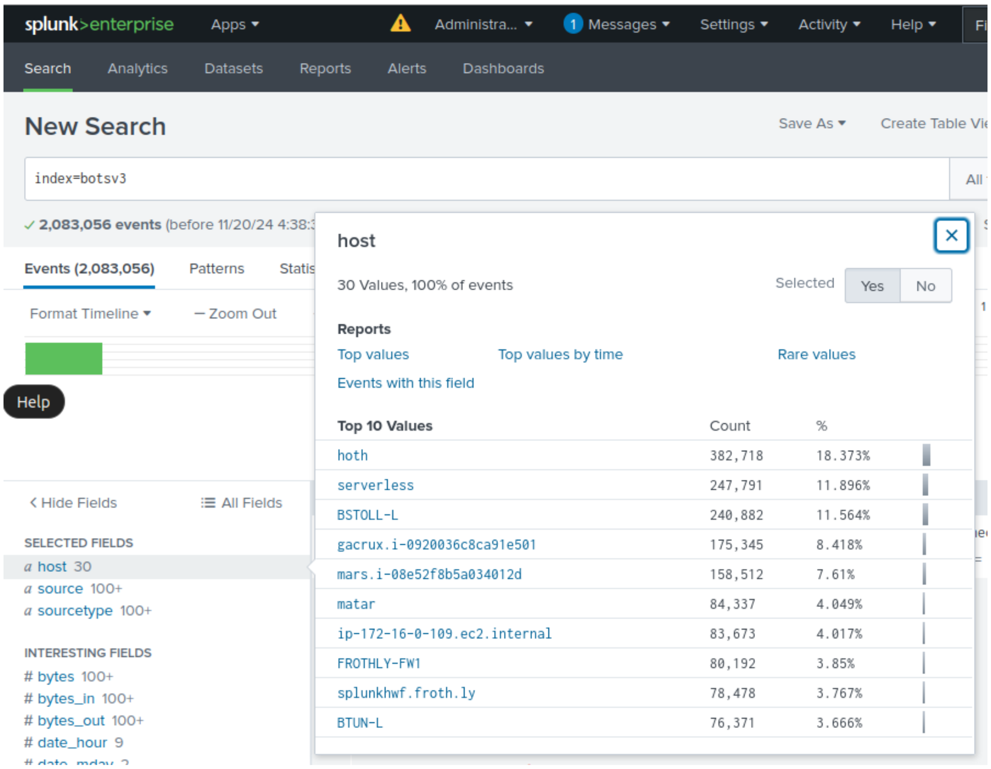
Time	Event

9/19/19 11:10:50.000 AM	`<error><message>Splunkd daemon is not re`
	host = OD-FM-NA-i-0ad2d665d4bdace22.am

8/20/18 8:27:09.296 AM	`{ [-]`
	`bytes: 50637`

Step 4: SPL/Query

With all 2 million events matched in the botsv3 index, scroll down to the Fields navigation on the left pane just below the timeline. Select "host" and chose the "matar" host.



New Search

```
index=botsv3
```

✓ 2,083,056 events (before 11/20/24 4:38:

SELECTED FIELDS
- a host 30
- a source 100+
- a sourcetype 100+

INTERESTING FIELDS
- # bytes 100+
- # bytes_in 100+
- # bytes_out 100+
- # date_hour 9
- # date_mday 2

host

30 Values, 100% of events

Selected Yes No

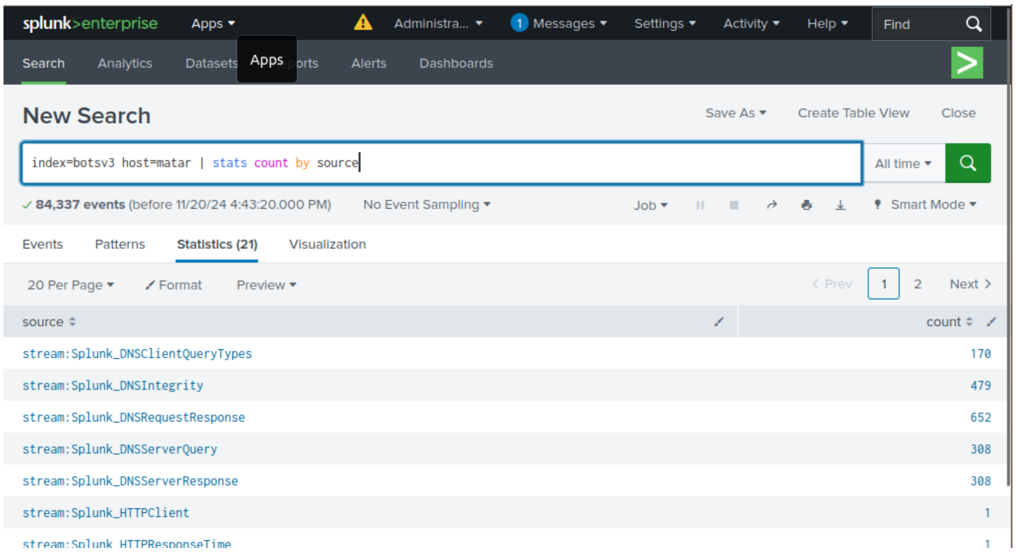
Reports

Top values · Top values by time · Rare values

Events with this field

Top 10 Values	Count	%
hoth	382,718	18.373%
serverless	247,791	11.896%
BSTOLL-L	240,882	11.564%
gacrux.i-0920036c8ca91e501	175,345	8.418%
mars.i-08e52f8b5a034012d	158,512	7.61%
matar	84,337	4.049%
ip-172-16-0-109.ec2.internal	83,673	4.017%
FROTHLY-FW1	80,192	3.85%
splunkhwf.froth.ly	78,478	3.767%
BTUN-L	76,371	3.666%

Once selected, observe the search bar now includes host=matar in the query. Append | stats count by source to the query and hit enter. This query pipes all filtered matar results to the SPL command stats where all sources are counted and displayed in the Statistics tab in the results section.



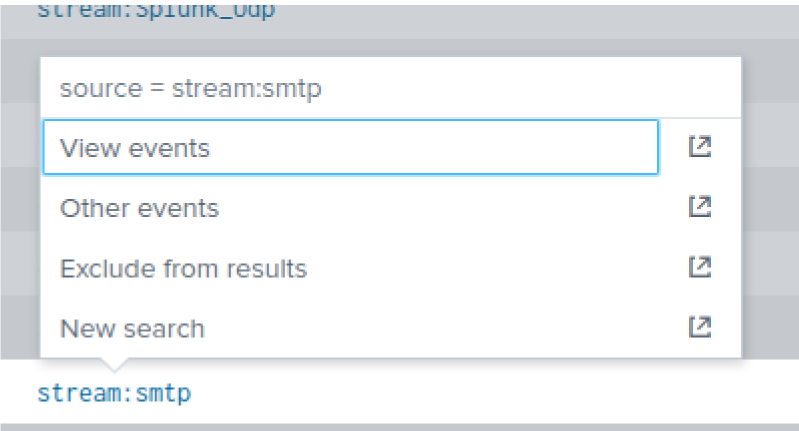
New Search

```
index=botsv3 host=matar | stats count by source
```

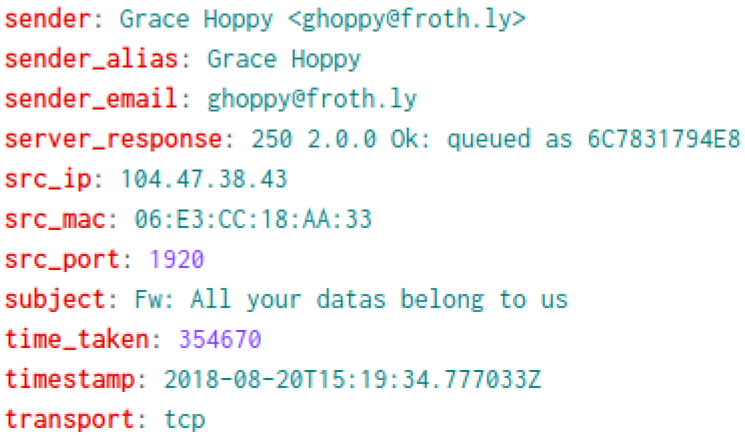
✓ 84,337 events (before 11/20/24 4:43:20.000 PM)

source	count
stream:Splunk_DNSClientQueryTypes	170
stream:Splunk_DNSIntegrity	479
stream:Splunk_DNSRequestResponse	652
stream:Splunk_DNSServerQuery	308
stream:Splunk_DNSServerResponse	308
stream:Splunk_HTTPClient	1
stream:Splunk_HTTPResponseTime	1

Scroll to the bottom of the Statistics page and select the "stream:smtp" and "View Events".

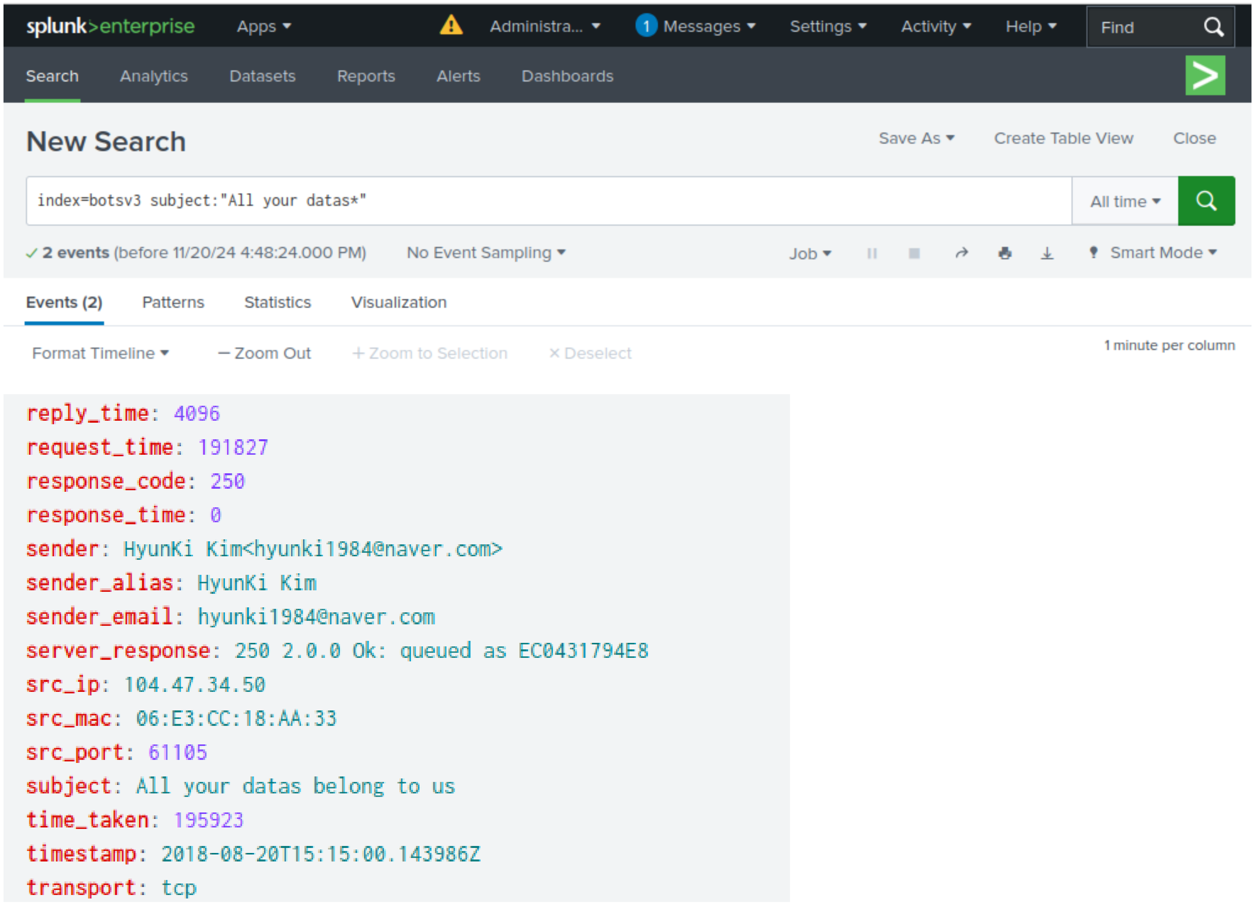


Review the first result in the Events pane. The first event should be an Outlook email from Grace Hoppy with the subject "Fw: All your datas belong to us".



```
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
```

While still using the botsv3 index, query subject:"All your datas*" and observe there are 2 hits. The wildcard * in SPL is a placeholder for any number of characters. Observe the second event is the original email and has a src_ip address of 104.47.34.50.



New Search

```
index=botsv3 subject:"All your datas*"
```

All time

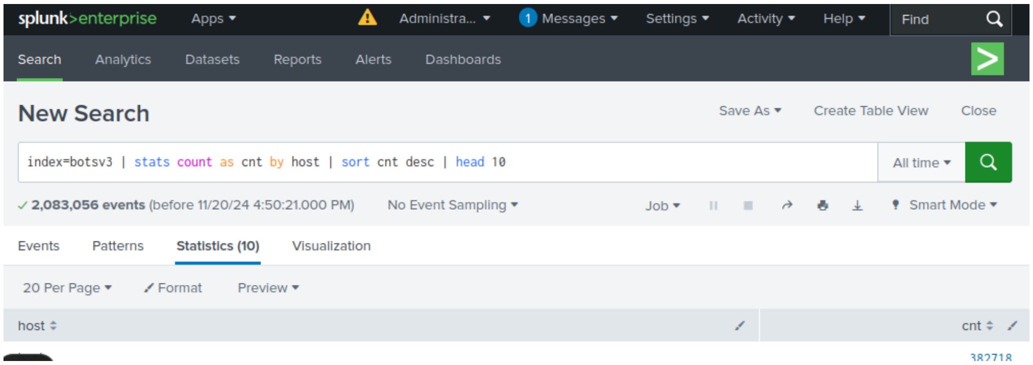
✓ **2 events** (before 11/20/24 4:48:24.000 PM) No Event Sampling

Events (2) | Patterns | Statistics | Visualization

```
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
```

Step 5: Reports

The following query gathers the top 10 source IP addresses with count: index=botsv3 | stats count as cnt by host | sort cnt desc | head 10 . Once the SPL is complete, press the Save As dropdown in the top right corner and select Report.



New Search

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

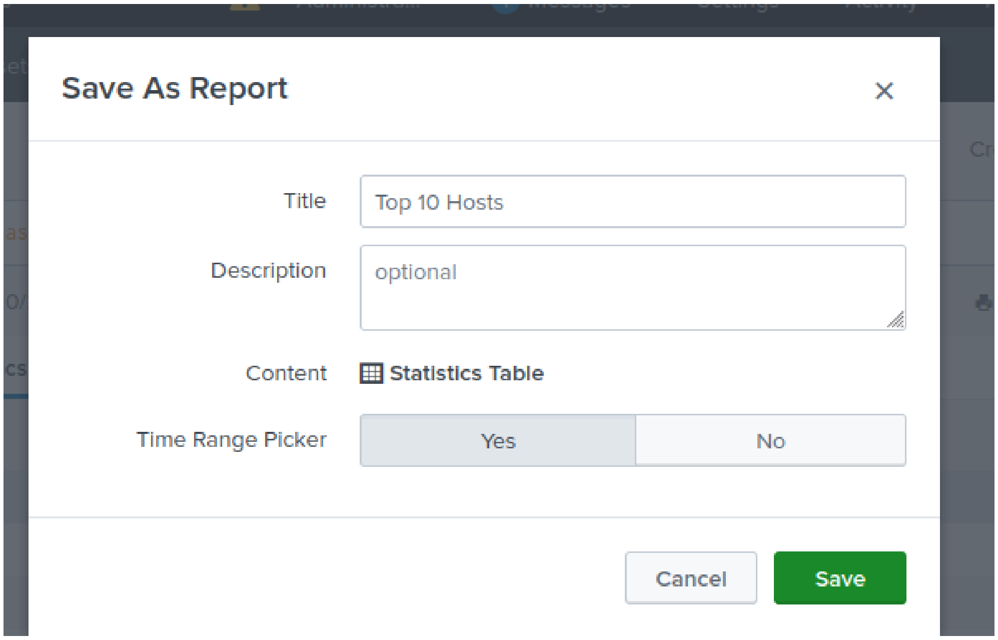
All time

✓ **2,083,056 events** (before 11/20/24 4:50:21.000 PM) No Event Sampling

Events | Patterns | Statistics (10) | Visualization

host	cnt
[redacted]	382718

Title the report "Top 10 Hosts", Time Range Picker as Yes, and hit Save.



Save As Report

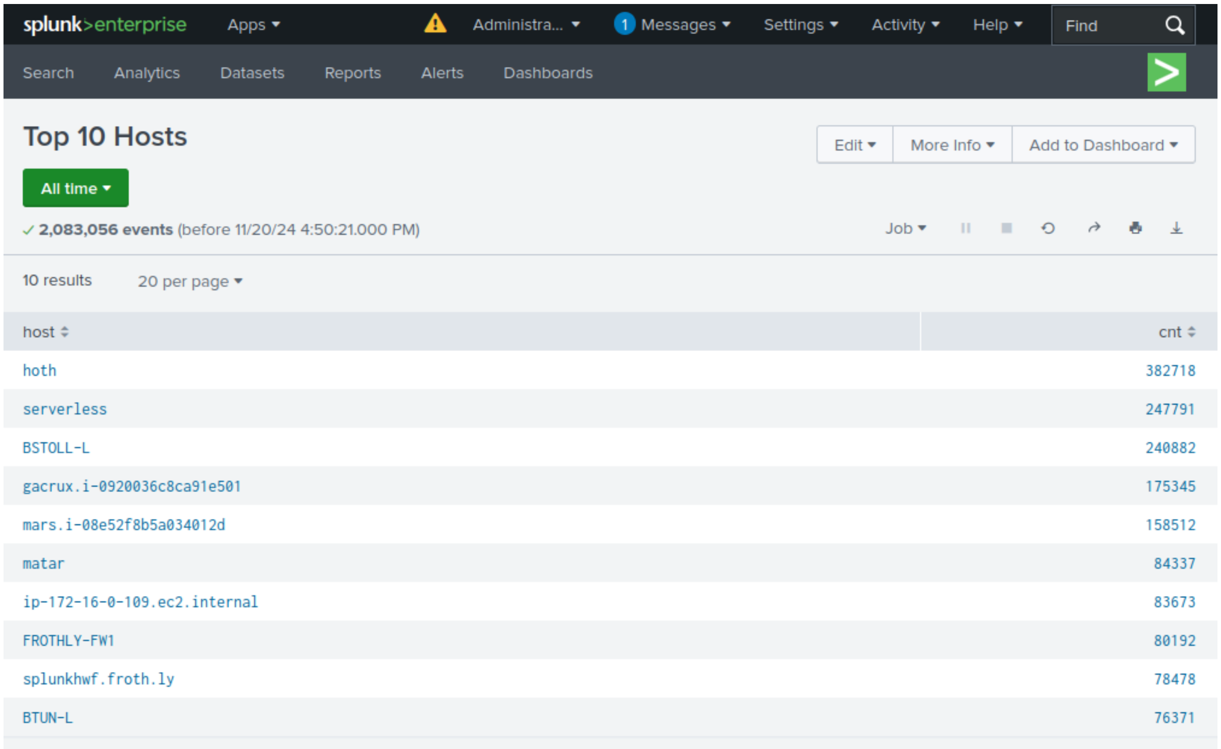
Title: Top 10 Hosts

Description: optional

Content: Statistics Table

Time Range Picker: Yes | No

Once the report is created, press the View button.



Top 10 Hosts

All time

✓ 2,083,056 events (before 11/20/24 4:50:21.000 PM)

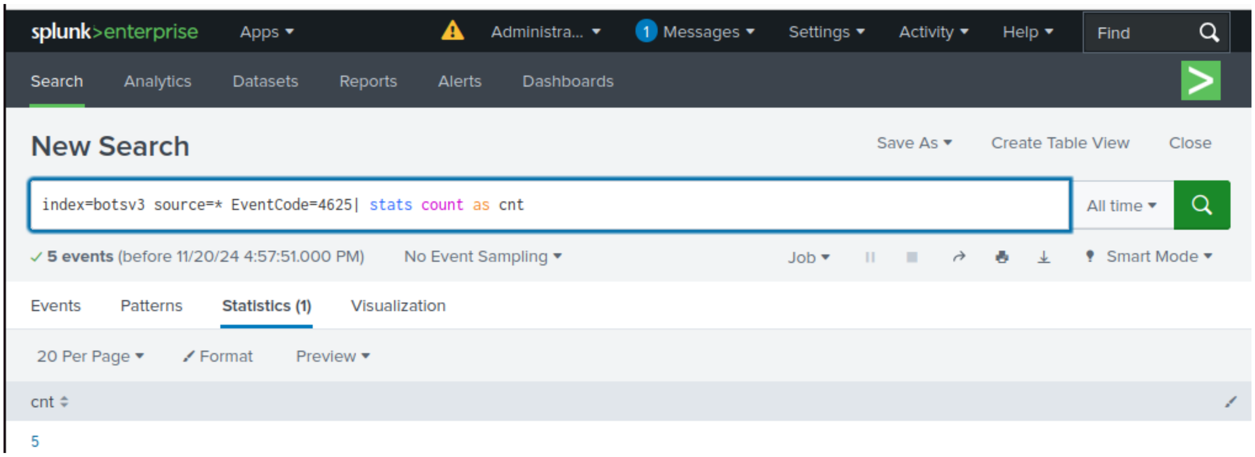
10 results 20 per page

host	cnt
hoth	382718
serverless	247791
BSTOLL-L	240882
gacrux.i-0920036c8ca91e501	175345
mars.i-08e52f8b5a034012d	158512
matar	84337
ip-172-16-0-109.ec2.internal	83673
FROTHLY-FW1	80192
splunkhwf.froth.ly	78478
BTUN-L	76371

Review the report and observe that it can be refreshed and exported at any time for reference. (top right)

Step 6: Visualizations and Dashboards

In this step you will develop a radial gauge visualization to enhance our dashboard. Create a new query that counts the number of failed Windows logon attempts which could identify bruteforce attacks.



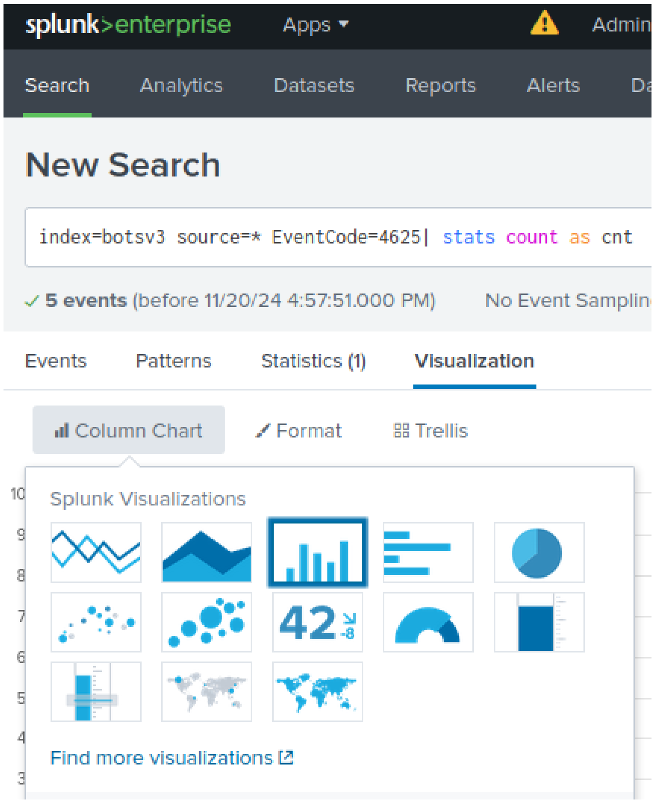
New Search

```
index=botsv3 source=* EventCode=4625| stats count as cnt
```

✓ 5 events (before 11/20/24 4:57:51.000 PM) No Event Sampling

cnt
5

Once the query is entered, select the Visualization subtab and choose the radial gauge type.

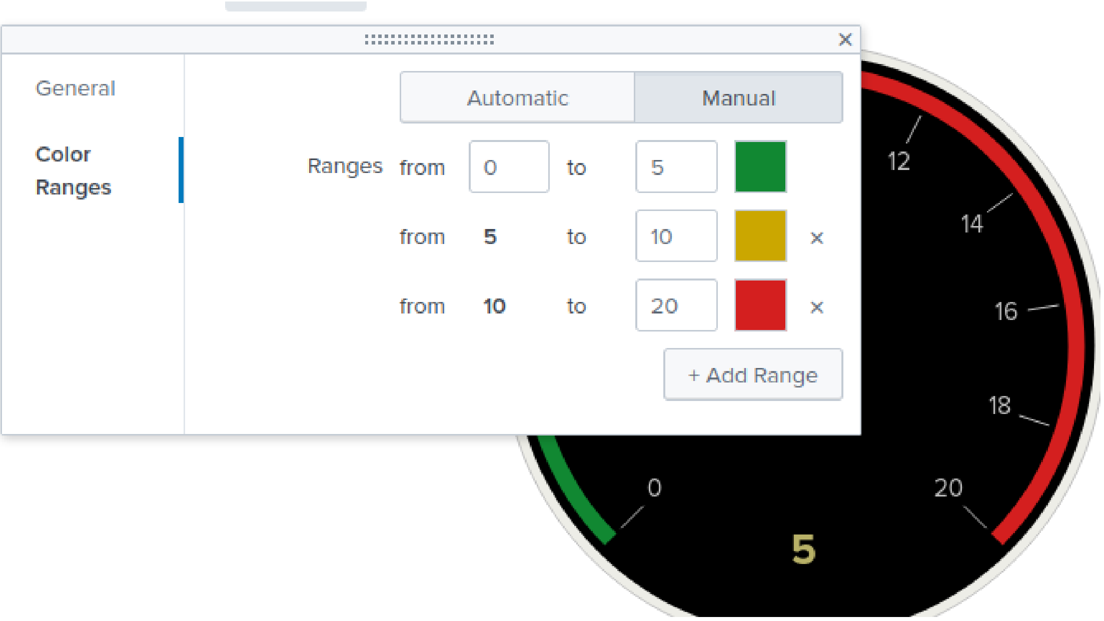


New Search

```
index=botsv3 source=* EventCode=4625| stats count as cnt
```

✓ 5 events (before 11/20/24 4:57:51.000 PM) No Event Samplin

With the Radial gauge selected, choose Format, Color Ranges, and change the green range to 0-5, yellow range to 6-10, and red range to 11-20. These thresholds would typically be based off normal or expected behavior over time.



General

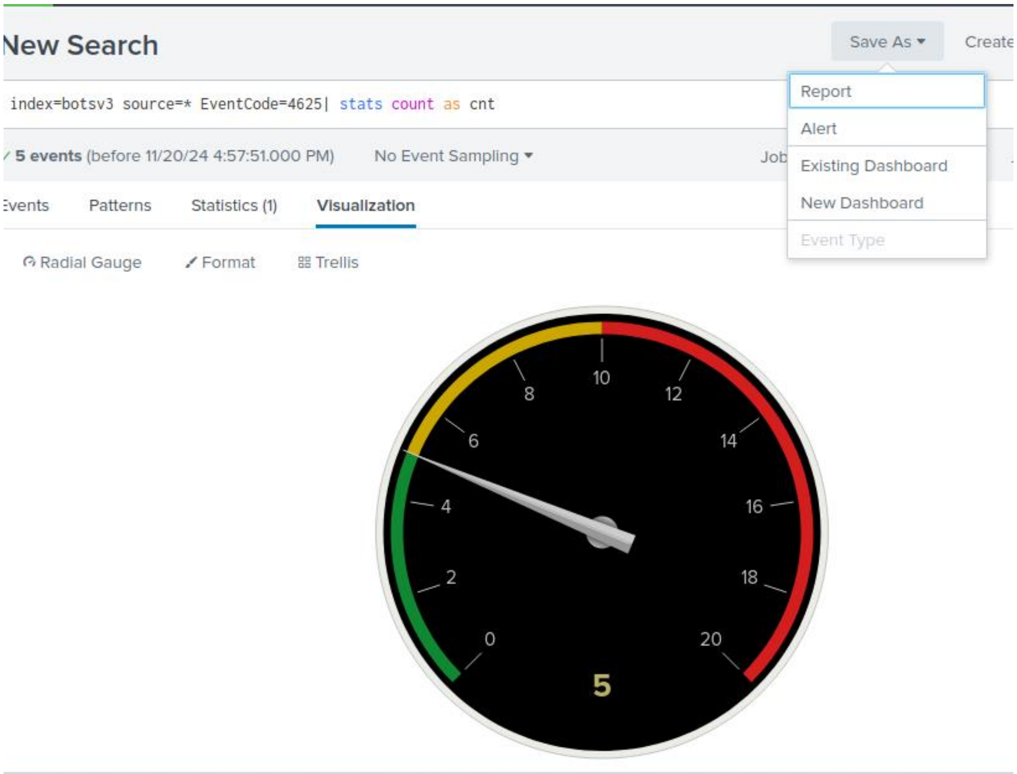
Color Ranges

Automatic | Manual

Ranges	from	0	to	5	🟩	
	from	5	to	10	🟨	×
	from	10	to	20	🟥	×

+ Add Range

Now that the gauge is configured with our thresholds, select the Save As and New Dashboard.



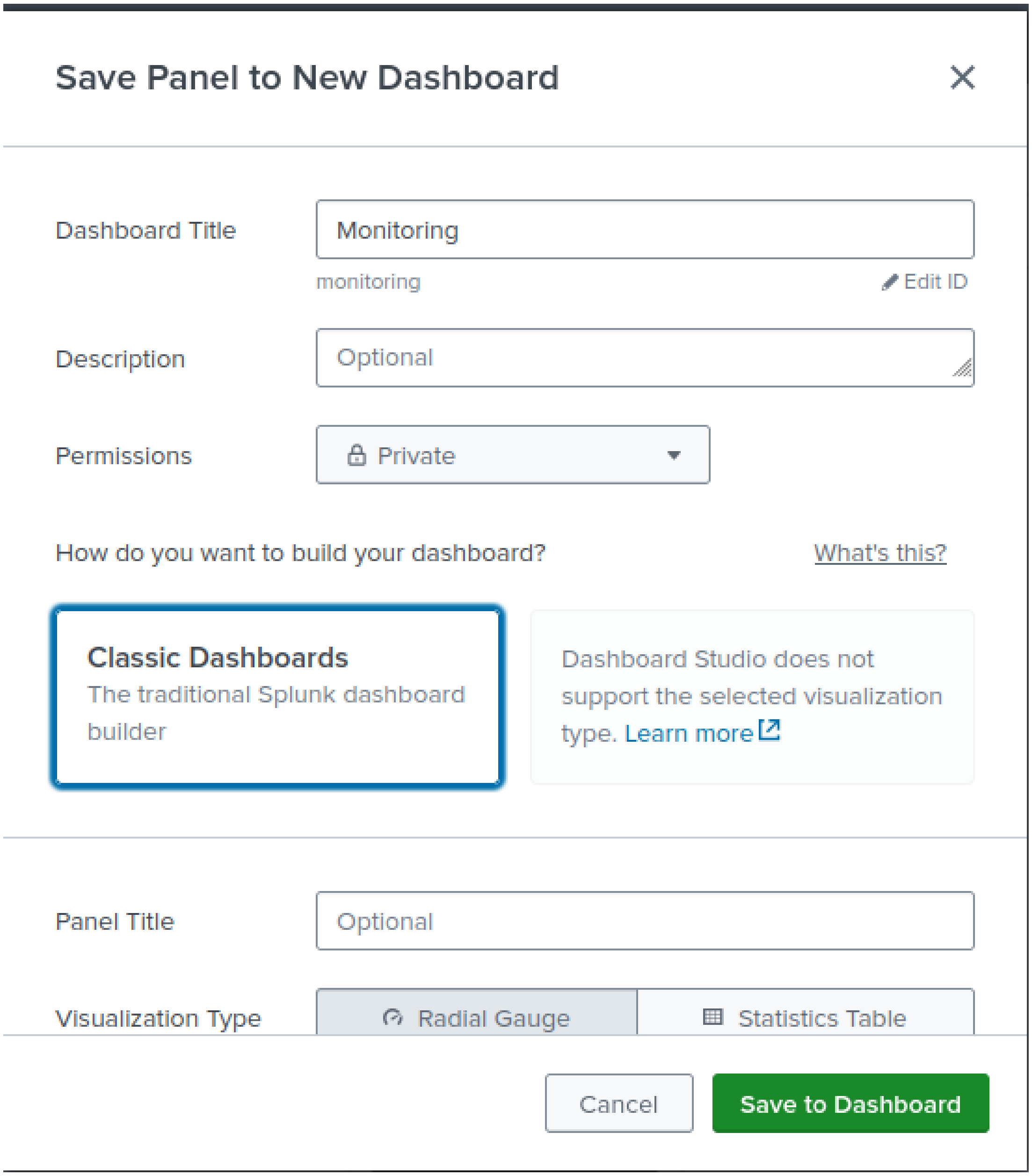
New Search

```
index=botsv3 source=* EventCode=4625| stats count as cnt
```

✓ 5 events (before 11/20/24 4:57:51.000 PM) No Event Sampling ▾ Job

Events Patterns Statistics (1) **Visualization**

Enter the Dashboard Title as "Monitoring", select "Classic Dashboards" and press Save to Dashboard



Save Panel to New Dashboard

Dashboard Title: Monitoring

monitoring

Description: Optional

Permissions: Private

How do you want to build your dashboard?

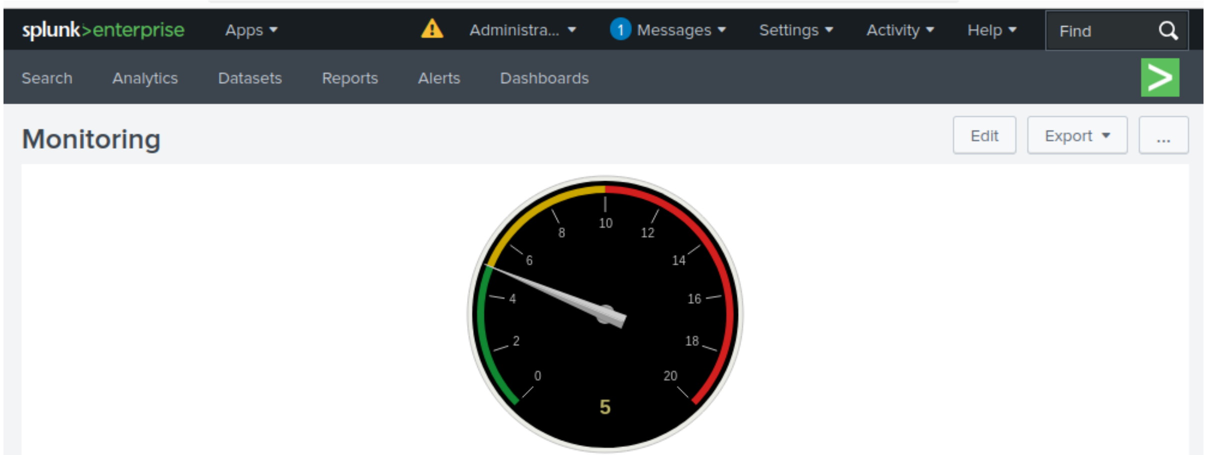
Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio does not support the selected visualization type. Learn more

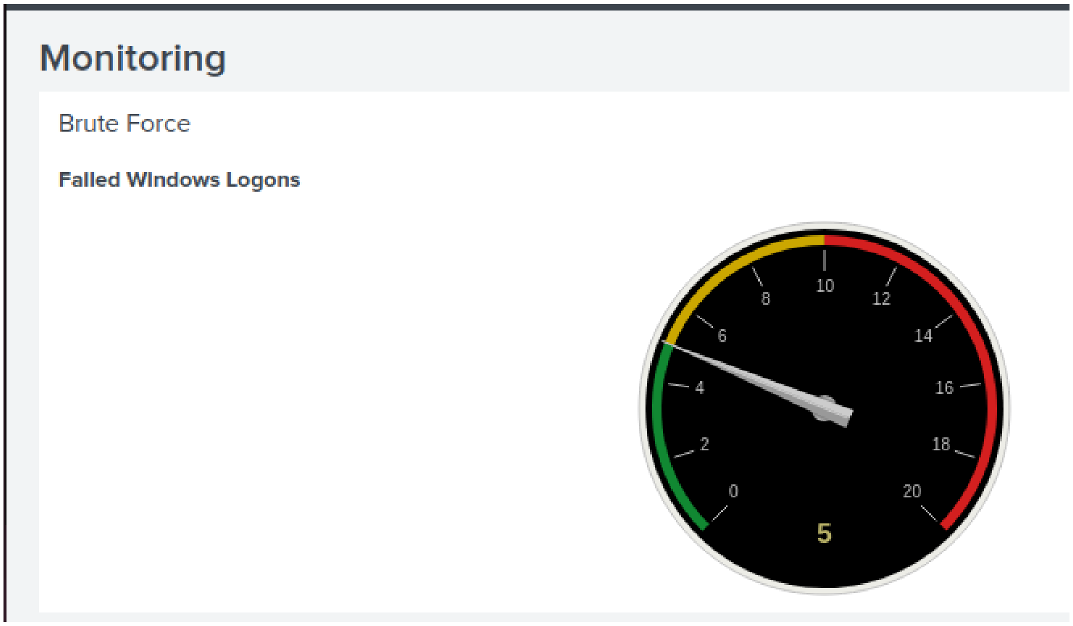
Panel Title: Optional

Visualization Type: Radial Gauge | Statistics Table

Select the View Dashboard button and observe our Monitoring Dashboard has the radial gauge, but it excludes a title and/or context. Press the Edit button in the upper right corner and name the section "Brute Force" and name the widget "Failed Windows Logons" then hit Save.



Monitoring



Monitoring

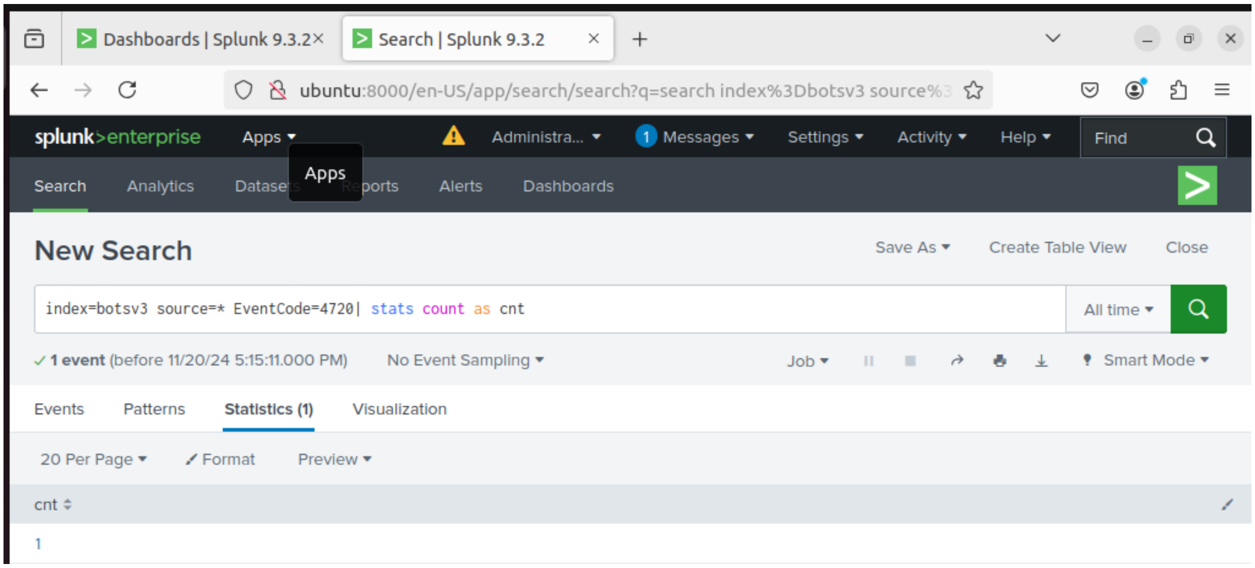
Brute Force

Failed Windows Logons

Step 7: Challenge

Find at least one other event worth monitoring from a security context. It doesn't have to be a Windows Event, but you can use https://www.xplg.com/windows-server-security-events-list/ for inspiration. Create a query and a Visualization (your choice on type). Configure the visualization and add it to the Monitoring Dashboard with an
appropriate title.

4720: A user account was created



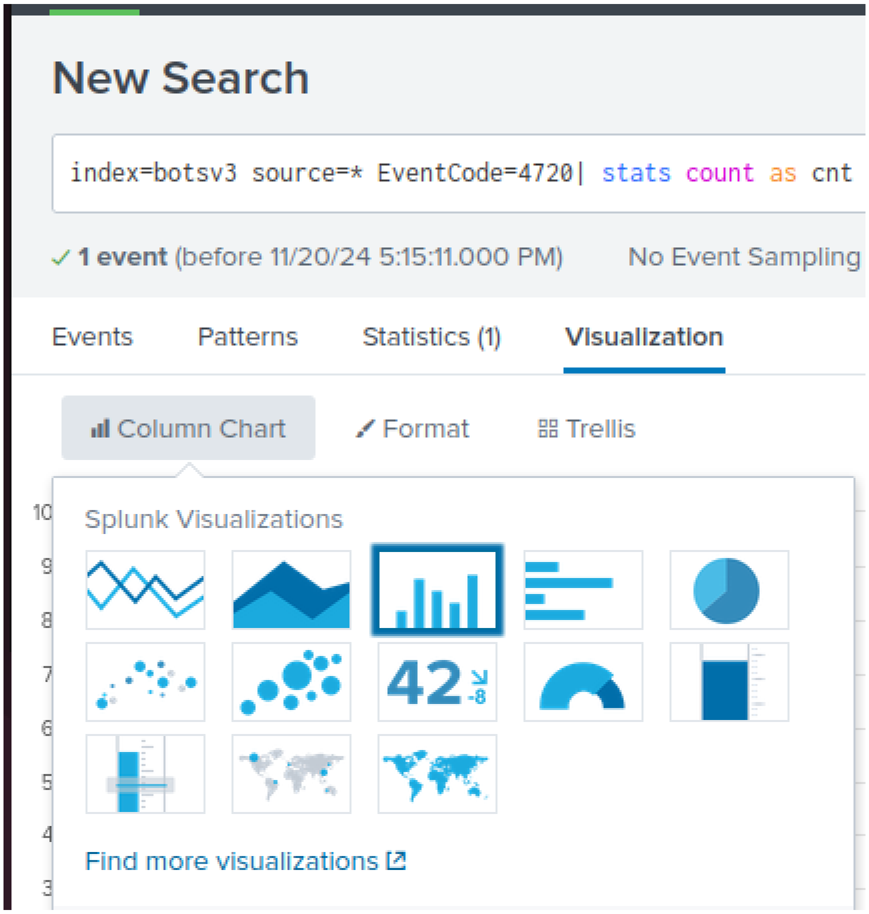
ubuntu:8000/en-US/app/search/search?q=search index%3Dbotsv3 source%3

New Search

```
index=botsv3 source=* EventCode=4720| stats count as cnt
```

✓ 1 event (before 11/20/24 5:15:11.000 PM)

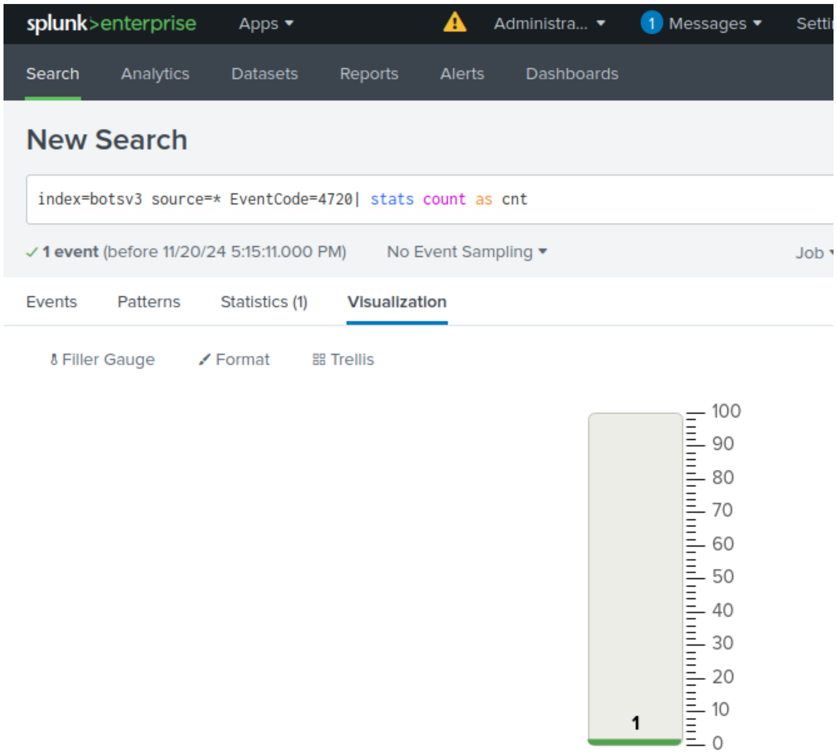
cnt
1



New Search

```
index=botsv3 source=* EventCode=4720| stats count as cnt
```

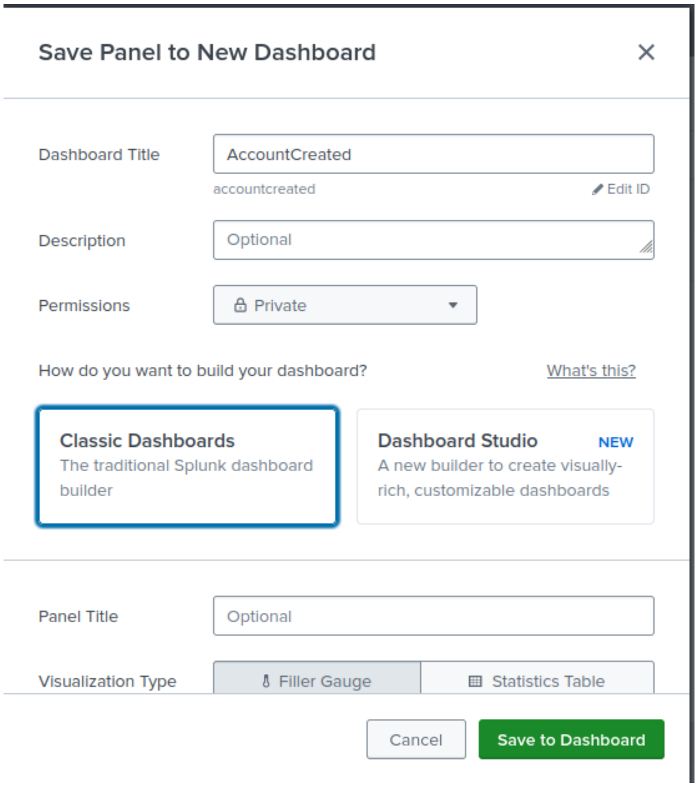
✓ 1 event (before 11/20/24 5:15:11.000 PM) No Event Sampling



New Search

```
index=botsv3 source=* EventCode=4720| stats count as cnt
```

✓ 1 event (before 11/20/24 5:15:11.000 PM)   No Event Sampling



Save Panel to New Dashboard

Dashboard Title: AccountCreated
accountcreated

Description: Optional

Permissions: Private

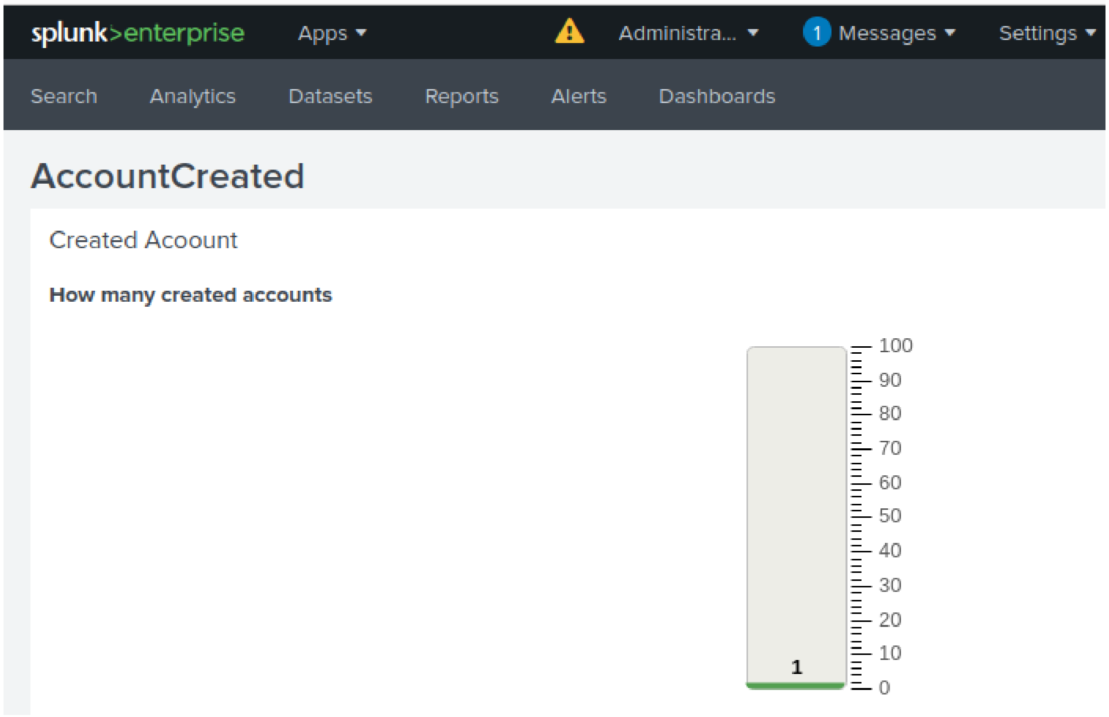
How do you want to build your dashboard?

Classic Dashboards
The traditional Splunk dashboard builder

Dashboard Studio NEW
A new builder to create visually-rich, customizable dashboards

Panel Title: Optional

Visualization Type: Filler Gauge | Statistics Table



AccountCreated

Created Acoount

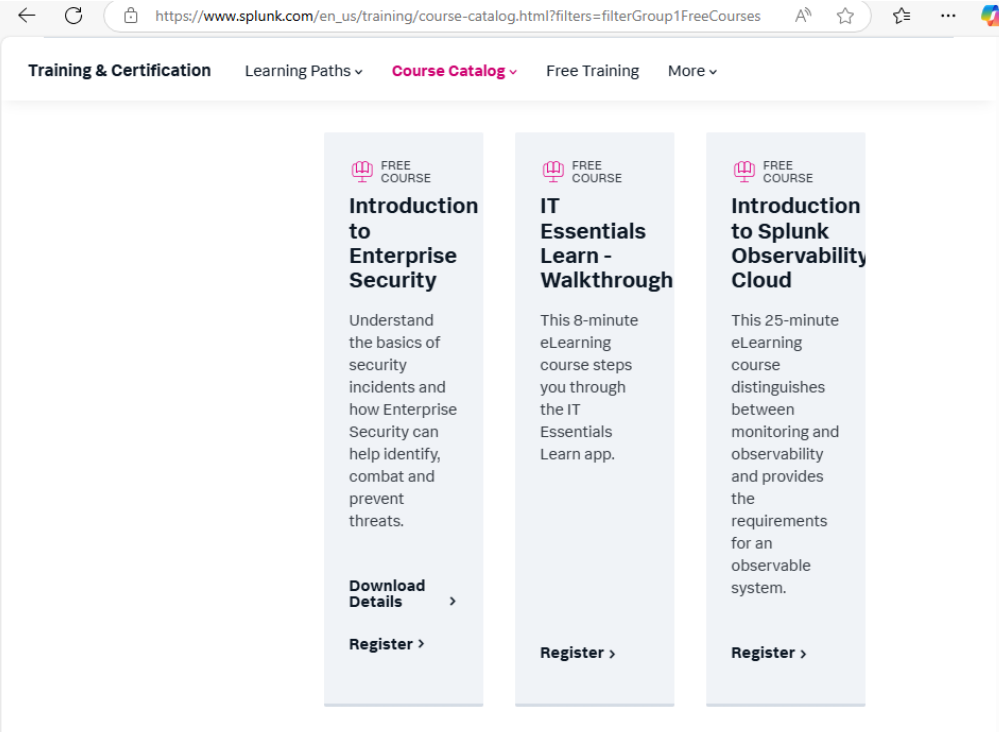
How many created accounts

Exercise 12.2 - Splunk Enterprise Security

In this task you will register and complete Splunk's free eLearning course "Introduction to Enterprise Security". Splunk is one of the most popular SIEM tools in the industry. Evidencing your completion of the course is a great resume builder while expanding your knowledge in security.

Step 1: Register for Course

Navigate to https://www.splunk.com/en_us/training/course-catalog.html?filters=filterGroup1FreeCourses and find the "Introduction to Enterprise Security" course.
Press the Register link and then press the ENROLL button. Log in to Splunk using your existing account (or create one if you don't have one).



https://www.splunk.com/en_us/training/course-catalog.html?filters=filterGroup1FreeCourses

FREE COURSE

Introduction to Enterprise Security

Understand the basics of security incidents and how Enterprise Security can help identify, combat and prevent threats.

Download Details ›

Register ›

FREE COURSE

IT Essentials Learn - Walkthrough

This 8-minute eLearning course steps you through the IT Essentials Learn app.

Register ›

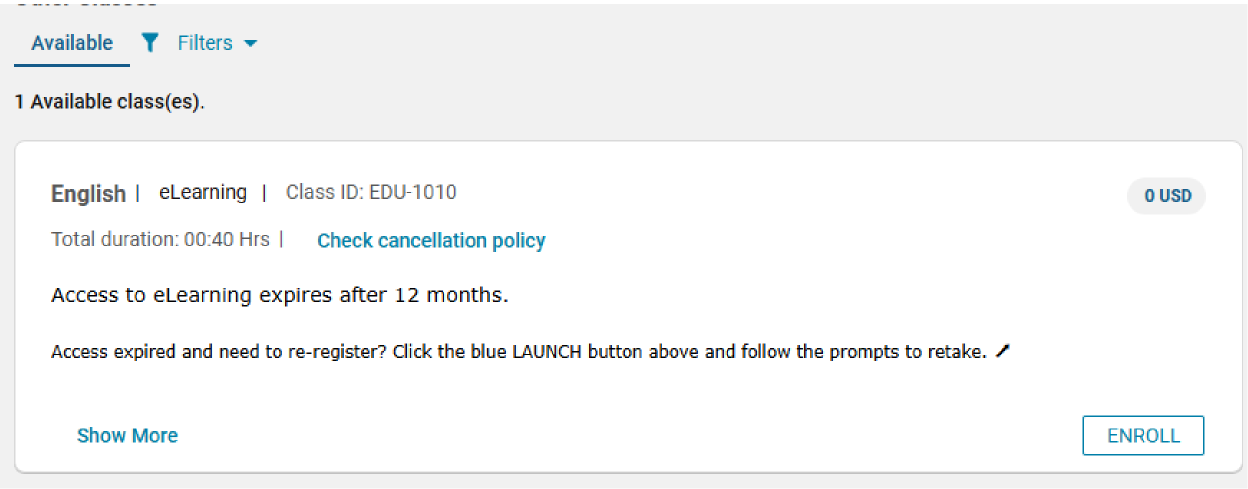
FREE COURSE

Introduction to Splunk Observability Cloud

This 25-minute eLearning course distinguishes between monitoring and observability and provides the requirements for an observable system.

Register ›

Press the Register link and then press the ENROLL button.



1 Available class(es).

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

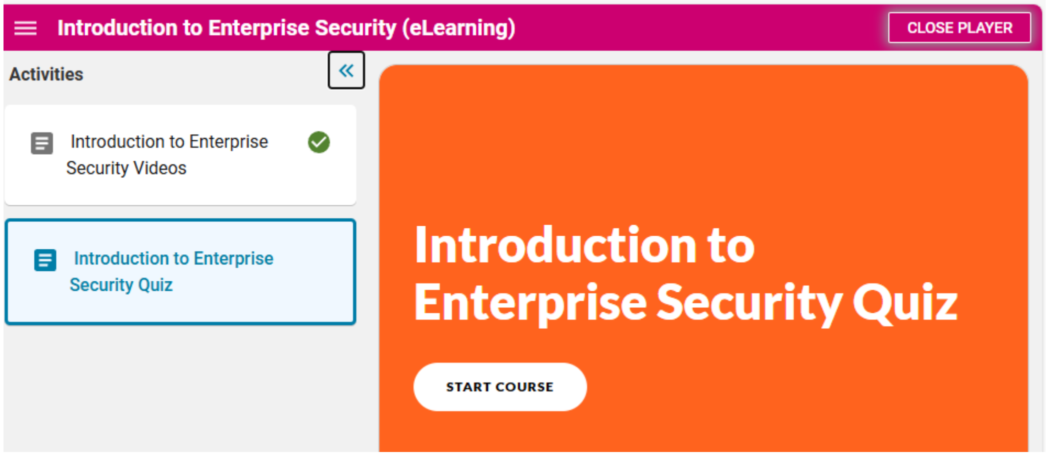
Total duration: 00:40 Hrs | Check cancellation policy

Access to eLearning expires after 12 months.

Access expired and need to re-register? Click the blue LAUNCH button above and follow the prompts to retake.

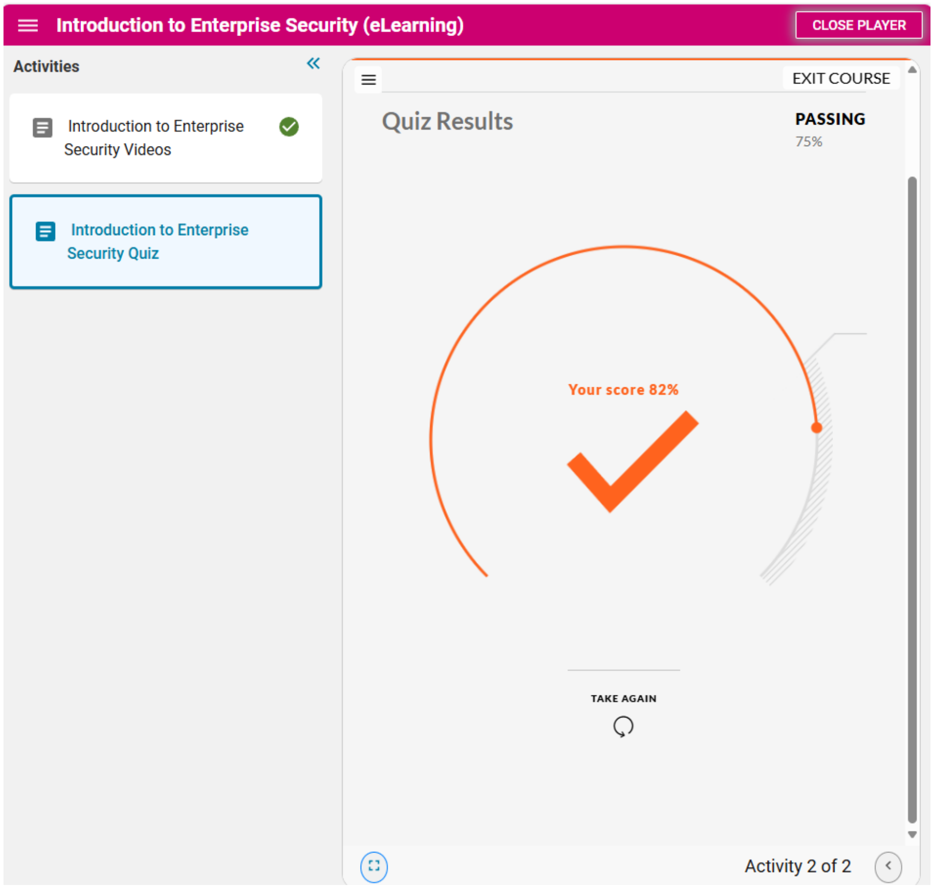
Step 2: Watch the Assigned Videos

Once you've enrolled in the eLearning course, you may start the Video coursework. Watch the videos and take notes! You can re-watch the videos at any time as many times as you'd like.


Introduction to Enterprise Security (eLearning)
CLOSE PLAYER
Activities
Introduction to Enterprise Security Videos
Introduction to Enterprise Security Quiz
Introduction to Enterprise Security Quiz
START COURSE

Step 3: Take the Quiz

Once you've studied the videos you should be ready for the quiz. There are 11 multiple choice questions that are untimed and can be retaken as many times as you need. You must achieve a score of 75% or greater to pass the course


Introduction to Enterprise Security (eLearning)
CLOSE PLAYER
Activities
Introduction to Enterprise Security Videos
Introduction to Enterprise Security Quiz
EXIT COURSE
Quiz Results
PASSING
75%
Your score 82%
TAKE AGAIN
Activity 2 of 2