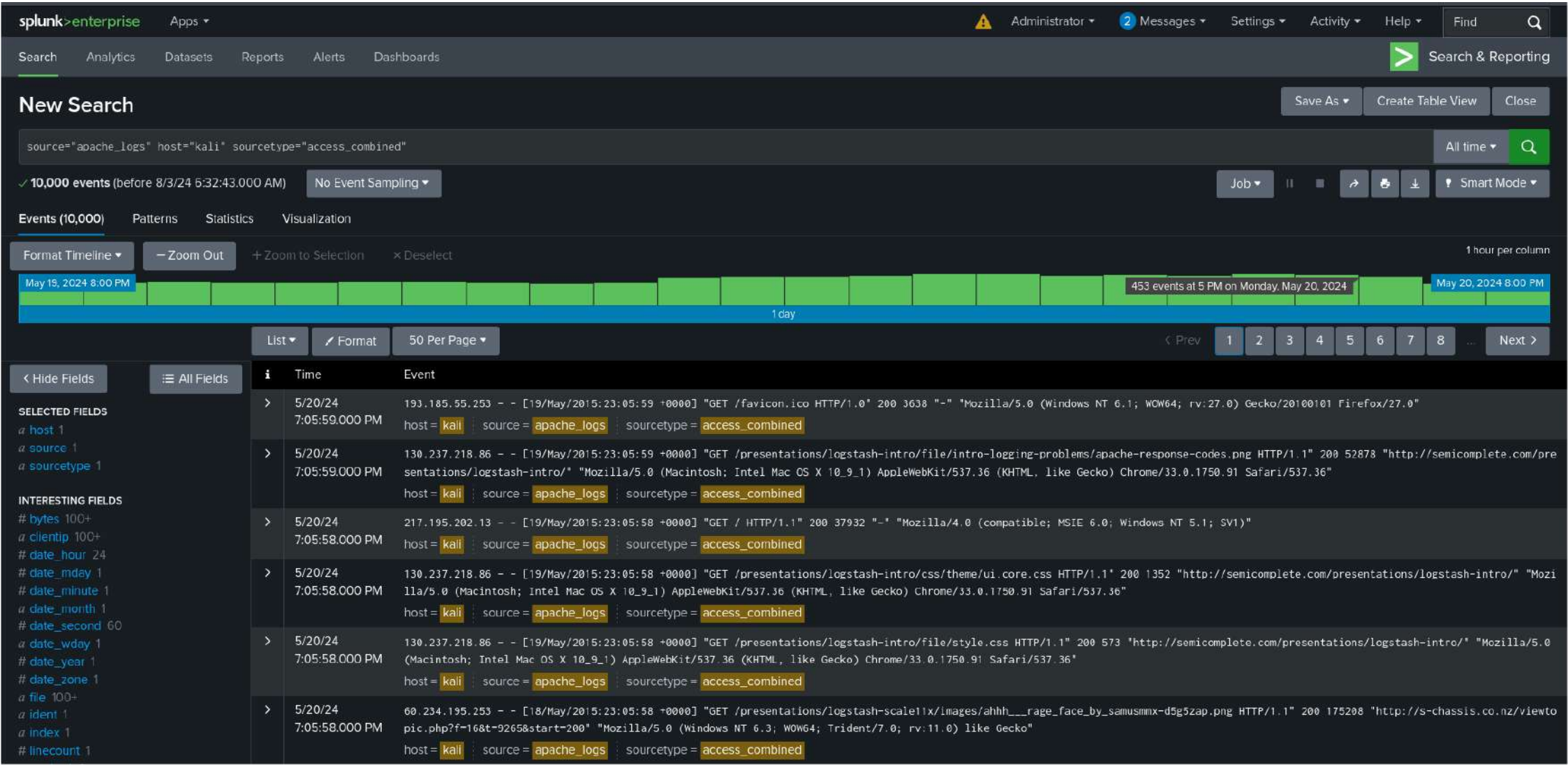
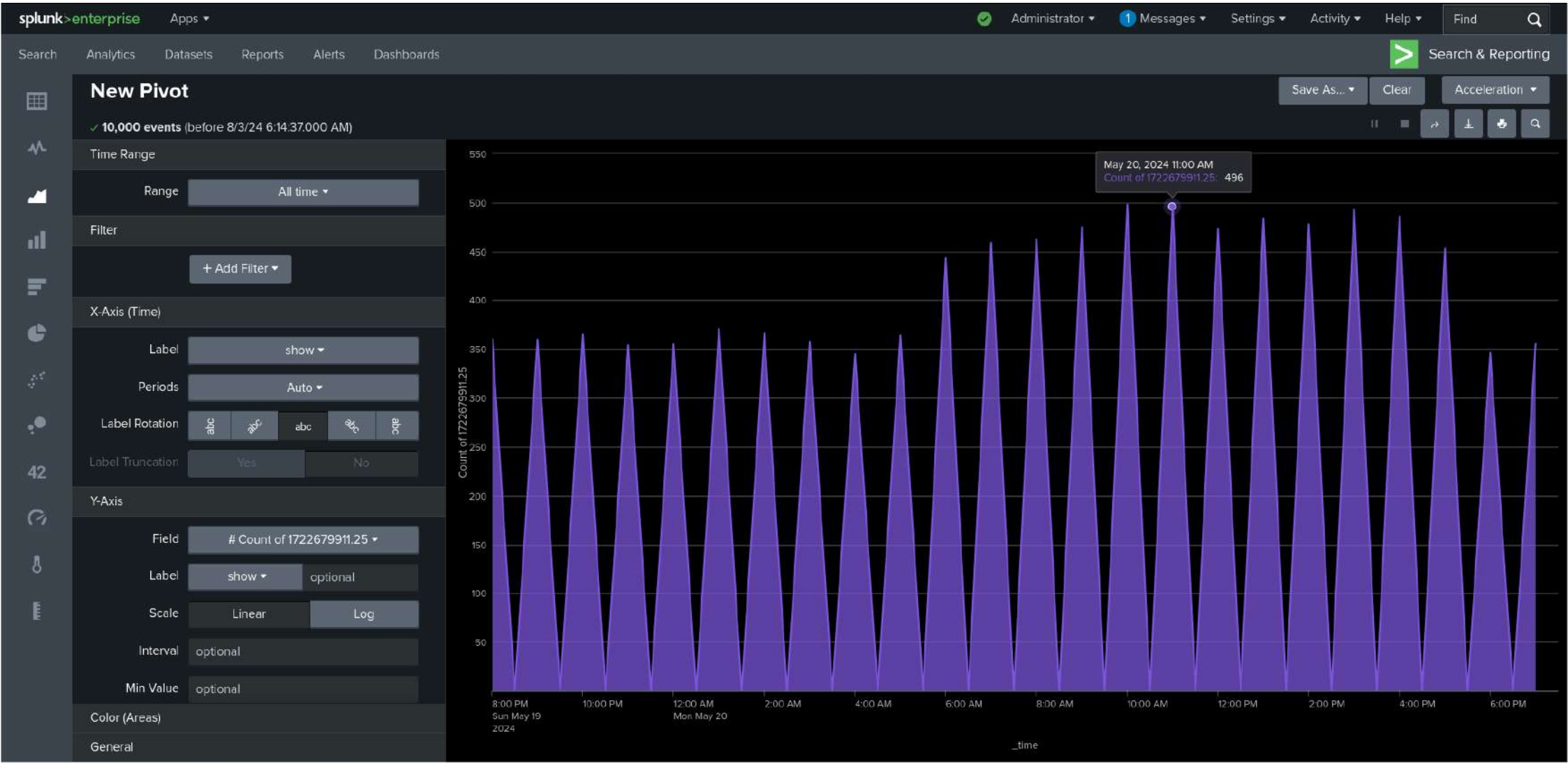
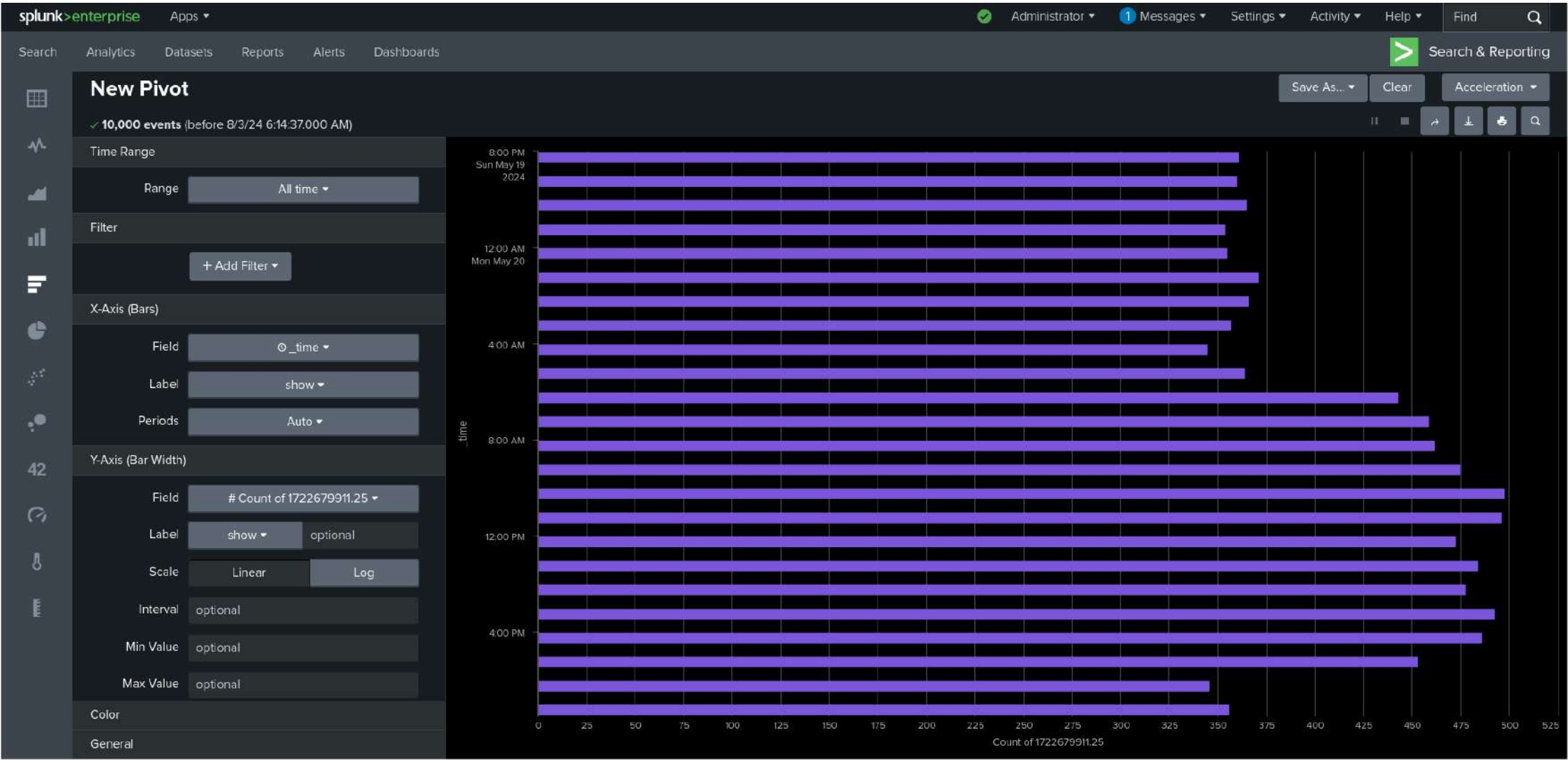
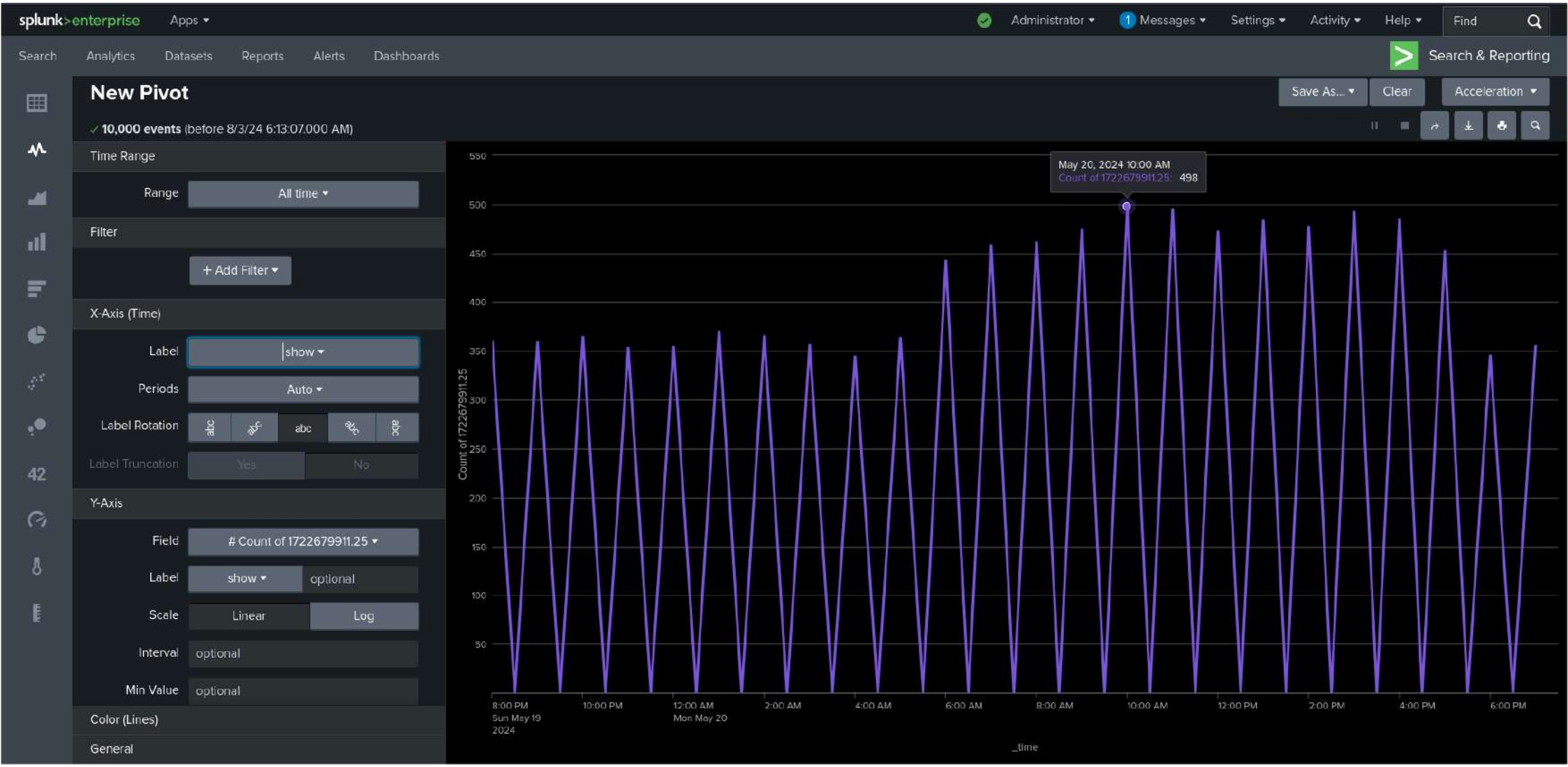
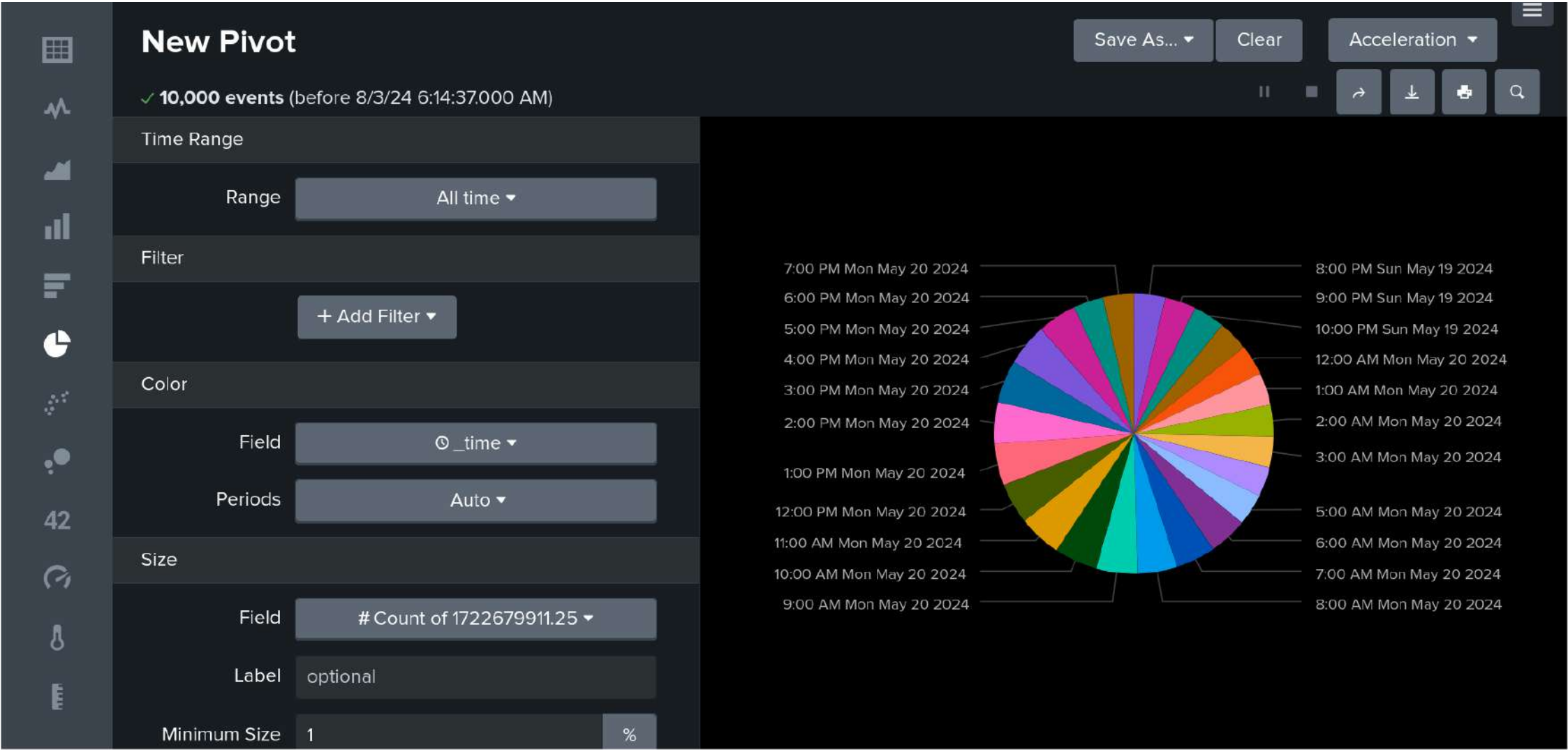

splunk>enterprise
Apps
Administrator
2 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Search
Save As
Create Table View
Close
source="apache_logs" host="kali" sourcetype="access_combined"
All time
10,000 events (before 8/3/24 6:32:43.000 AM)
No Event Sampling
Job
Smart Mode
Events (10,000)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
May 19, 2024 8:00 PM
453 events at 5 PM on Monday, May 20, 2024
May 20, 2024 8:00 PM
1 day
List
Format
50 Per Page
Prev
1 2 3 4 5 6 7 8 ...
Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 1
a sourcetype 1
INTERESTING FIELDS
bytes 100+
a clientip 100+
date_hour 24
date_mday 1
date_minute 1
a date_month 1
date_second 60
a date_wday 1
date_year 1
date_zone 1
a file 100+
a ident 1
a index 1
linecount 1
Time
Event
5/20/24 7:05:59.000 PM
193.185.55.253 - - [19/May/2015:23:05:59 +0000] "GET /favicon.ico HTTP/1.0" 200 3638 "-" "Mozilla/5.0 (Windows NT 6.1; WOW64; rv:27.0) Gecko/20100101 Firefox/27.0"
host = kali source = apache_logs sourcetype = access_combined
5/20/24 7:05:59.000 PM
130.237.218.86 - - [19/May/2015:23:05:59 +0000] "GET /presentations/logstash-intro/file/intro-logging-problems/apache-response-codes.png HTTP/1.1" 200 52878 "http://semicomplete.com/presentations/logstash-intro/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36"
host = kali source = apache_logs sourcetype = access_combined
5/20/24 7:05:58.000 PM
217.195.202.13 - - [19/May/2015:23:05:58 +0000] "GET / HTTP/1.1" 200 37932 "-" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)"
host = kali source = apache_logs sourcetype = access_combined
5/20/24 7:05:58.000 PM
130.237.218.86 - - [19/May/2015:23:05:58 +0000] "GET /presentations/logstash-intro/css/theme/ui.core.css HTTP/1.1" 200 1352 "http://semicomplete.com/presentations/logstash-intro/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36"
host = kali source = apache_logs sourcetype = access_combined
5/20/24 7:05:58.000 PM
130.237.218.86 - - [19/May/2015:23:05:58 +0000] "GET /presentations/logstash-intro/file/style.css HTTP/1.1" 200 573 "http://semicomplete.com/presentations/logstash-intro/" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_9_1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/33.0.1750.91 Safari/537.36"
host = kali source = apache_logs sourcetype = access_combined
5/20/24 7:05:58.000 PM
60.234.195.253 - - [18/May/2015:23:05:58 +0000] "GET /presentations/logstash-scale11x/images/ahhh___rage_face_by_samusmmx-d5g5zap.png HTTP/1.1" 200 175208 "http://s-chassis.co.nz/viewtopic.php?f=16&t=9265&start=200" "Mozilla/5.0 (Windows NT 6.3; WOW64; Trident/7.0; rv:11.0) like Gecko"
host = kali source = apache_logs sourcetype = access_combined


splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Pivot
Save As...
Clear
Acceleration
10,000 events (before 8/3/24 6:14:37.000 AM)
Time Range
Range
All time
Filter
+ Add Filter
X-Axis (Time)
Label
show
Periods
Auto
Label Rotation
Label Truncation
Yes
No
Y-Axis
Field
Count of 1722679911.25
Label
show
optional
Scale
Linear
Log
Interval
optional
Min Value
optional
Color (Areas)
General
May 20, 2024 11:00 AM
Count of 1722679911.25: 496
Count of 1722679911.25
550
500
450
400
350
300
250
200
150
100
50
8:00 PM
Sun May 19
2024
10:00 PM
12:00 AM
Mon May 20
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
_time


splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Pivot
Save As...
Clear
Acceleration
10,000 events (before 8/3/24 6:14:37.000 AM)
Time Range
Range
All time
Filter
+ Add Filter
X-Axis (Bars)
Field
_time
Label
show
Periods
Auto
Y-Axis (Bar Width)
Field
Count of 1722679911.25
Label
show
optional
Scale
Linear
Log
Interval
optional
Min Value
optional
Max Value
optional
Color
General
8:00 PM
Sun May 19
2024
12:00 AM
Mon May 20
4:00 AM
8:00 AM
12:00 PM
4:00 PM
_time
0
25
50
75
100
125
150
175
200
225
250
275
300
325
350
375
400
425
450
475
500
525
Count of 1722679911.25


splunk>enterprise
Apps
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
New Pivot
Save As...
Clear
Acceleration
10,000 events (before 8/3/24 6:13:07.000 AM)
Time Range
Range
All time
Filter
+ Add Filter
X-Axis (Time)
Label
show
Periods
Auto
Label Rotation
Label Truncation
Yes
No
Y-Axis
Field
Count of 1722679911.25
Label
show
optional
Scale
Linear
Log
Interval
optional
Min Value
optional
Color (Lines)
General
May 20, 2024 10:00 AM
Count of 1722679911.25: 498
Count of 1722679911.25
550
500
450
400
350
300
250
200
150
100
50
8:00 PM
Sun May 19
2024
10:00 PM
12:00 AM
Mon May 20
2:00 AM
4:00 AM
6:00 AM
8:00 AM
10:00 AM
12:00 PM
2:00 PM
4:00 PM
6:00 PM
_time


New Pivot
Save As...
Clear
Acceleration
10,000 events (before 8/3/24 6:14:37.000 AM)
Time Range
Range
All time
Filter
+ Add Filter
Color
Field
_time
Periods
Auto
Size
Field
Count of 1722679911.25
Label
optional
Minimum Size
1
%
7:00 PM Mon May 20 2024
6:00 PM Mon May 20 2024
5:00 PM Mon May 20 2024
4:00 PM Mon May 20 2024
3:00 PM Mon May 20 2024
2:00 PM Mon May 20 2024
1:00 PM Mon May 20 2024
12:00 PM Mon May 20 2024
11:00 AM Mon May 20 2024
10:00 AM Mon May 20 2024
9:00 AM Mon May 20 2024
8:00 PM Sun May 19 2024
9:00 PM Sun May 19 2024
10:00 PM Sun May 19 2024
12:00 AM Mon May 20 2024
1:00 AM Mon May 20 2024
2:00 AM Mon May 20 2024
3:00 AM Mon May 20 2024
5:00 AM Mon May 20 2024
6:00 AM Mon May 20 2024
7:00 AM Mon May 20 2024
8:00 AM Mon May 20 2024