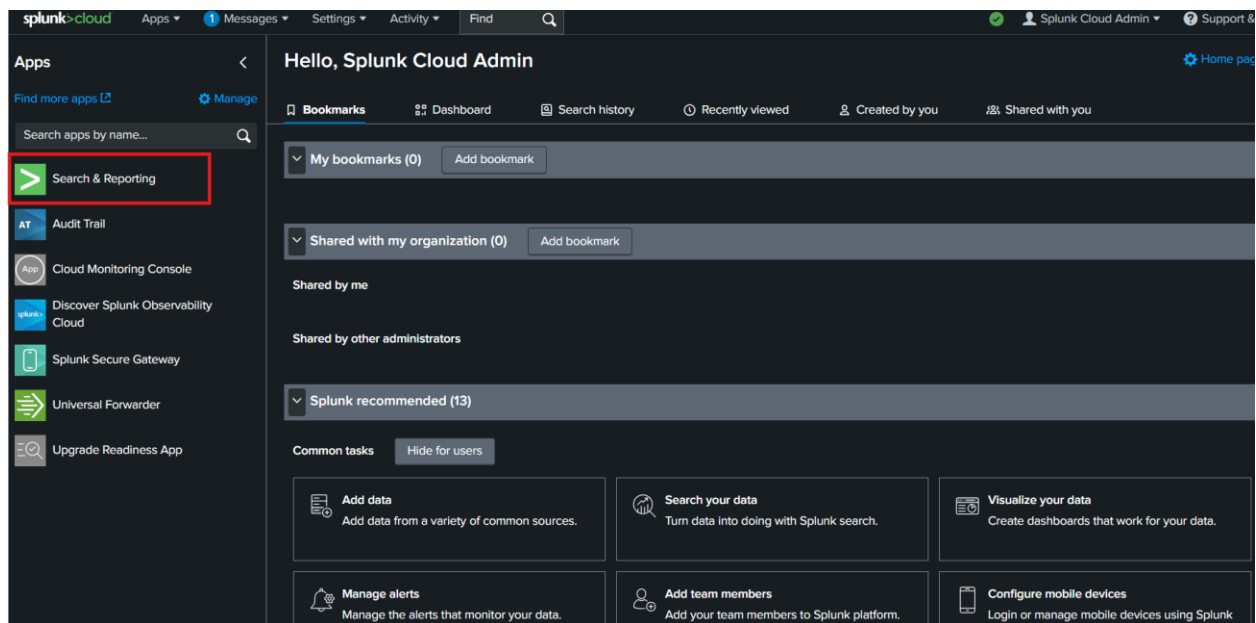


## Querying in Splunk SIEM Tool

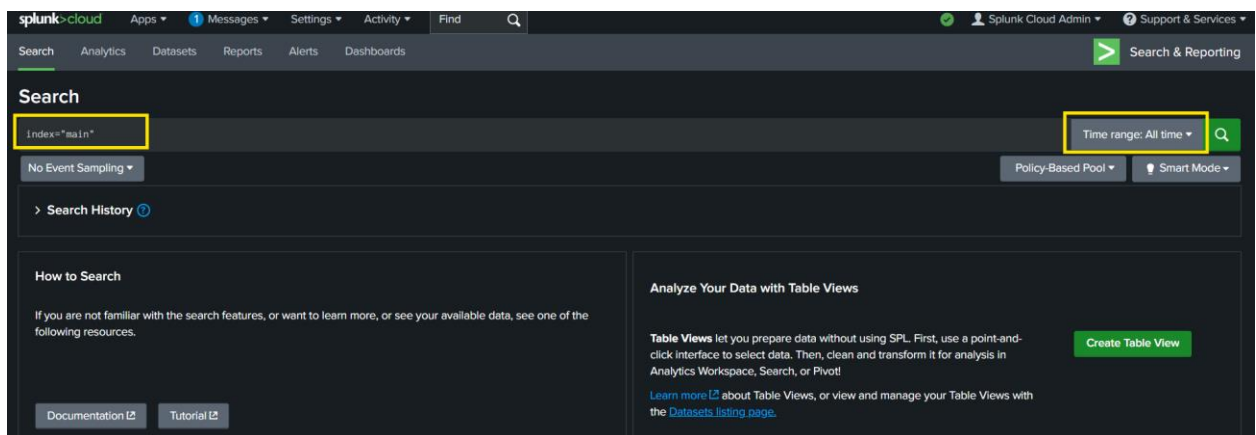
### Project:

In this project I want to identify whether there are any possible security issues with the company's mail server. To do that, I'll need to check for any failed SSH logins for the root acct.

First, by navigating to "Search & Reporting" from the app panel:



I'll enter a query to index the "main" data storage and filter to check for 'all time' to look at **everything** ever captured:



After querying, it returns raw logs or events, which are like time-stamped notes. I'm also able to explore the "Selected Fields" which tells me the number of hosts, sources, & source types:

Index="main" Time range: All time

109,864 events (before 7/27/25 8:48:20.000 PM) No Event Sampling

Events (109,864) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Format Show: 20 Per Page View: List

Hide Fields All Fields

SELECTED FIELDS

- host 5
- source 8
- sourcetype 3

INTERESTING FIELDS

- # AcctID 100+
- # bytes 100+
- a clientip 100+
- a Code 14
- # date\_hour 24
- # date\_mday 8
- # date\_minute 60
- # date\_month 2
- # date\_second 60
- # date\_wday 7
- # date\_year 1
- a date\_zone 1
- a file 14
- a ident 1

Time	Event
3/6/23 6:24:02.000 PM	[06/Mar/2023:18:24:02] VendorID=5036 Code=B AcctID=6024298300471575 host = vendor_sales source = tutorialdata.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:23:46.000 PM	[06/Mar/2023:18:23:46] VendorID=7026 Code=C AcctID=8702194102896748 host = vendor_sales source = tutorialdata.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:23:31.000 PM	[06/Mar/2023:18:23:31] VendorID=1043 Code=B AcctID=2063718909897951 host = vendor_sales source = tutorialdata.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:22:59.000 PM	[06/Mar/2023:18:22:59] VendorID=1243 Code=F AcctID=8768831614147676 host = vendor_sales source = tutorialdata.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:22:48.000 PM	[06/Mar/2023:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740 host = vendor_sales source = tutorialdata.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:22:32.000 PM	[06/Mar/2023:18:22:32] VendorID=7033 Code=E AcctID=4390644811207834 host = vendor_sales source = tutorialdata.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales
3/6/23 6:22:16.000 PM	91.205.189.15 - - [06/Mar/2023:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=S06SL7FF7ADFF53113 HTTP 1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5 159 host = www2 source = tutorialdata.zip./www2/access.log sourcetype = access_combined_wcookie

Selecting the *host* field, all 5 network host are shown (1 sales data, 3 web apps, & 1 mail server)

splunk>cloud Apps Messages Settings Activity Find

Search Analytics Datasets Reports Alerts Dashboards

New Search

Index="main"

109,864 events (before 7/27/25 8:48:20.000 PM) No Event Sampling

Events (109,864) Patterns Statistics Visualization

Timeline format Zoom Out Zoom to Selection Deselect

Hide Fields All Fields

SELECTED FIELDS

- host 5
- source 8
- sourcetype 3

INTERESTING FIELDS

- # AcctID 100+
- # bytes 100+
- a clientip 100+
- a Code 14
- # date\_hour 24
- # date\_mday 8
- # date\_minute 60
- # date\_month 2

host

5 Values, 100% of events

Reports

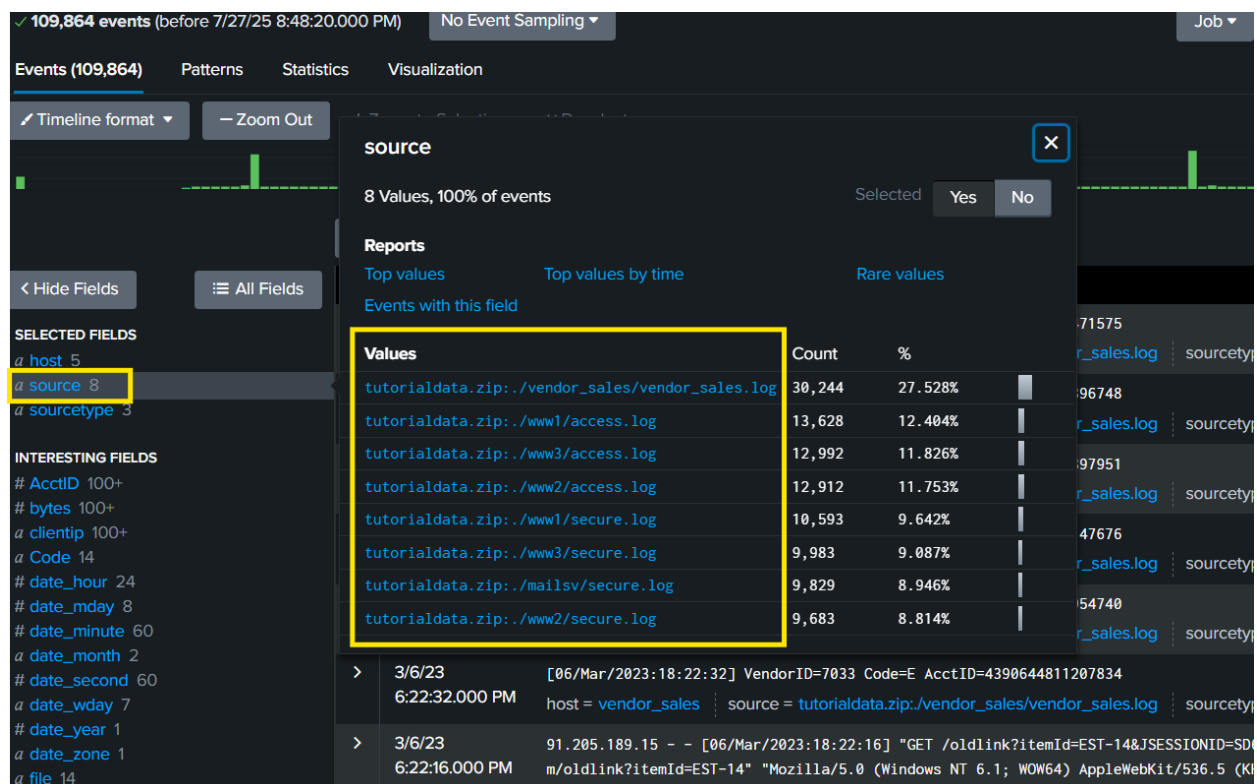
- Top values
- Top values by time
- Rare values

Events with this field

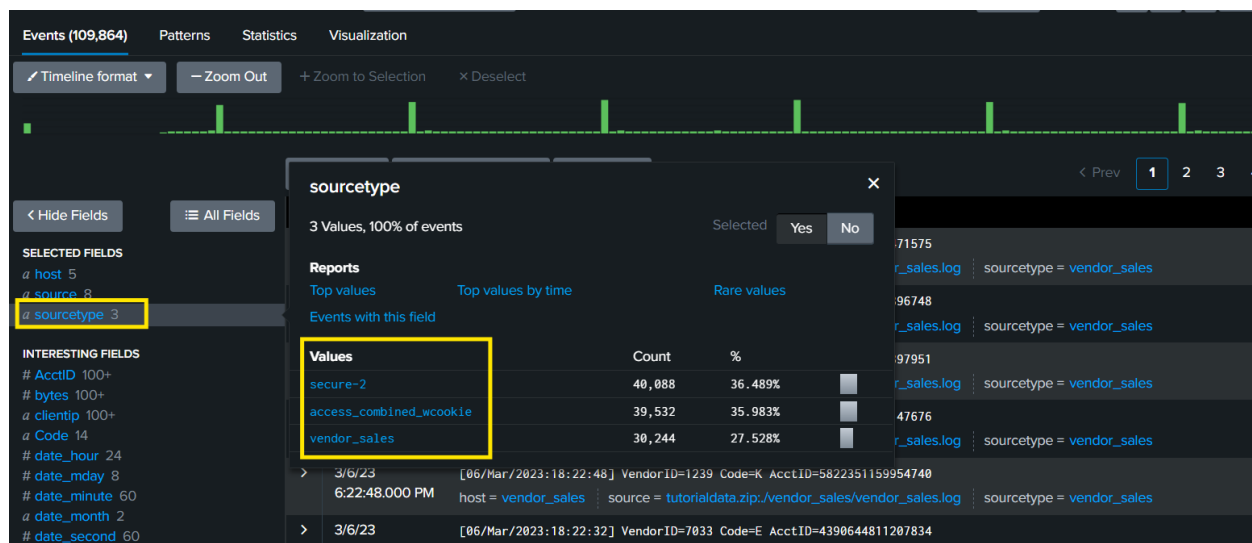
Values	Count	%
vendor_sales	30,244	27.528%
www1	24,221	22.046%
www3	22,975	20.912%
www2	22,595	20.566%
mailsv	9,829	8.946%

Time	Event
3/6/23 6:22:48.000 PM	[06/Mar/2023:18:22:48] VendorID=1239 Code=K AcctID=5822351159954740 host = vendor_sales source = tutorialdata.zip./vendor_sales/vendor_sales.log sourcetype = vendor_sales

Alternately, selecting the *source* field, it indicates the file name from which the event originates:



Same goes for *sourcetype*, which determines how data is formatted:



But for this project, I'm focusing on exploring failed SSH login for the mail server, so I'll populate the *mailsv* host and notice that a new term has been added to the search bar and the number of events have significantly decreased to just over 9k:

**New Search**

index="main" host=mailsv

Time range: All time

✓ 9,829 events (before 7/27/25 9:13:46.000 PM) No Event Sampling

Events (9,829) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection x Deselect

Format Show: 20 Per Page View: List

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- # date\_hour 1
- # date\_mday 8
- # date\_minute 1
- # date\_month 2
- # date\_second 1
- # date\_wday 7
- # date\_year 1
- # date\_zone 1
- # index 1
- # linecount 1
- # punct 9

i	Time	Event
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[5276]: Failed password for invalid user appserver from 194.8.74.23 port 3351 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[1039]: Failed password for root from 194.8.74.23 port 3768 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[5258]: Failed password for invalid user testuser from 194.8.74.23 port 3626 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[21881]: pam_unix(sshd:session): session closed for user nsarhe by (uid=0) host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[1165]: Failed password for apache from 194.8.74.23 port 4684 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[3760]: Failed password for invalid user mongodb from 194.8.74.23 port 2472 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[4998]: Failed password for mail from 194.8.74.23 port 1552 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2

Now to query for failed logins from the host *mailsv* that's attached to word *root*, which returns less than 350 events, and shows all failed attempts:

**New Search**

index=main host=mailsv fail\* root

Time range

✓ 346 events (before 7/27/25 9:19:30.000 PM) No Event Sampling

Events (346) Patterns Statistics Visualization

Timeline format Zoom Out + Zoom to Selection x Deselect

Format Show: 20 Per Page View: List

SELECTED FIELDS

- host 1
- source 1
- sourcetype 1

INTERESTING FIELDS

- # date\_hour 1
- # date\_mday 8
- # date\_minute 1
- # date\_month 2
- # date\_second 1
- # date\_wday 7
- # date\_year 1
- # date\_zone 1
- # index 1
- # linecount 1
- # punct 1
- # splunk\_server 1

i	Time	Event
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[1039]: failed password for root from 194.8.74.23 port 3768 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[2426]: failed password for root from 89.106.20.218 port 1392 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[1712]: failed password for root from 89.106.20.218 port 1347 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[1345]: failed password for root from 69.175.97.11 port 1823 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[3912]: failed password for root from 109.169.32.135 port 4253 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[5838]: failed password for root from 223.205.219.67 port 3230 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2
>	3/6/23 1:39:51.000 AM	Thu Mar 06 2023 01:39:51 mailsv sshd[1151]: failed password for root from 175.44.1.122 port 1202 ssh2 host = mailsv source = tutorialdata.zip./mailsv/secure.log sourcetype = secure-2

After reviewing all 18 pages, I have concluded that there were over 300 failed SSH logins for the root account