

**New Search**

Index-main host-realms fail| root

✓ 692 events before 8/15/24 10:05:17:000 AM No Event Sampling

Jobs | All time | Policy-Based Post | Smart Mode

Events (692) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom In Selection Disabled

1 day per column

Hide Fields	All Fields	List	Format	20 Per Page
<	>	#	Time	Event
SLECTED FIELDS		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
a host 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
a source 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
sourcetype 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
INTERESTING FIELDS		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# date_hour 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# date_minute 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# date_month 2		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# date_second 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# date_weekday 7		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# date_year 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# date_zone 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# index 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# offset 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# purlid 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# splunk_server 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# timestamp 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
# timestamp1 1		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2
+ Extract New Fields		36/23	13/51:00:00 AM	This Mar 06 2023 81:39:51 mailui sshd(1891): failed password for root from 194.8.74.23 port 3788 sxd host=mailv source=tatobaldata.sp.mailbv.securelog sourcetype=secure-2

- **Index** is a repository for data and in this instance, the index is a single dataset containing events from an index named main
- **Host** field specifies the name of the network host from which the event originated. In this instance, we are investigating the events generated by “**mailsv**”
- Source field indicates the file name from which the event originates, in this instance /mailsv/secure.log
- Sourcetype determined how the data is formatted, such as secure-2, in this instance
- We are interested in failed login, so we specify **fail\* root**, where **fail\*** is a keyword with a wildcard that expands the search term to find other terms that contain the word “fail” such as “failure” or “failed.” The keyword root searches for any event that contains the term “**root**”