Nuova ricerca

```
source="tutorialdata.zip:*" | search "failed password" "86.212.199.60"
| rex field=_raw "(?<user>[\w@-]+)\s+from\s+(.*?)"
| rex field=_raw "port (?<port>\d{1,5})"
| sort - _time
| table _time user port
```

Intervallo temporale: Sempre

✓ **1.264 eventi** (prima di 04/01/26 13:28:08,000) Nessun campionamento degli eventi

Statistiche (1.264)

_time	user	port
2025-12-28 06:49:05	agushto	3692
2025-12-28 06:49:05	tomcat	1464
2025-12-28 06:49:05	desktop	3518
2025-12-28 06:49:05	yp	2856
2025-12-28 06:49:05	mail	1054
2025-12-28 06:49:05	apache	2630
2025-12-28 06:49:05	services	4740
2025-12-28 06:49:05	irc	1203
2025-12-28 06:49:05	mysql	4802
2025-12-28 06:49:05	pmuser	1775
2025-12-28 06:49:05	ventrilo	1465
2025-12-28 06:49:05	system	3305
2025-12-28 06:49:05	agushto	3692
2025-12-28 06:49:05	tomcat	1464
2025-12-28 06:49:05	desktop	3518
2025-12-28 06:49:05	yp	2856
2025-12-28 06:49:05	mail	1054
2025-12-28 06:49:05	apache	2630
2025-12-28 06:49:05	services	4740
2025-12-28 06:49:05	irc	1203
2025-12-28 06:49:05	mysql	4802
2025-12-28 06:49:05	pmuser	1775
2025-12-28 06:49:05	ventrilo	1465
2025-12-28 06:49:05	system	3305
2025-12-28 06:49:05	agushto	3692
2025-12-28 06:49:05	tomcat	1464

_time	user	port
2025-12-28 06:49:05	desktop	3518
2025-12-28 06:49:05	yp	2856
2025-12-28 06:49:05	mail	1054
2025-12-28 06:49:05	apache	2630
2025-12-28 06:49:05	services	4740
2025-12-28 06:49:05	irc	1203
2025-12-28 06:49:05	mysql	4802
2025-12-28 06:49:05	pmuser	1775
2025-12-28 06:49:05	ventrilo	1465
2025-12-28 06:49:05	system	3305
2025-12-28 06:49:05	agushto	3692
2025-12-28 06:49:05	tomcat	1464
2025-12-28 06:49:05	desktop	3518
2025-12-28 06:49:05	yp	2856
2025-12-28 06:49:05	mail	1054
2025-12-28 06:49:05	apache	2630
2025-12-28 06:49:05	services	4740
2025-12-28 06:49:05	irc	1203
2025-12-28 06:49:05	mysql	4802
2025-12-28 06:49:05	pmuser	1775
2025-12-28 06:49:05	ventrilo	1465
2025-12-28 06:49:05	system	3305
2025-12-28 06:49:05	agushto	3692
2025-12-28 06:49:05	tomcat	1464
2025-12-28 06:49:05	desktop	3518
2025-12-28 06:49:05	yp	2856
2025-12-28 06:49:05	mail	1054
2025-12-28 06:49:05	apache	2630
2025-12-28 06:49:05	services	4740
2025-12-28 06:49:05	irc	1203
2025-12-28 06:49:05	mysql	4802
2025-12-28 06:49:05	pmuser	1775
2025-12-28 06:49:05	ventrilo	1465
2025-12-28 06:49:05	system	3305
2025-12-28 06:49:05	agushto	3692

_time	user	port
2025-12-28 06:49:05	tomcat	1464
2025-12-28 06:49:05	desktop	3518
2025-12-28 06:49:05	yp	2856
2025-12-28 06:49:05	mail	1054
2025-12-28 06:49:05	apache	2630
2025-12-28 06:49:05	services	4740
2025-12-28 06:49:05	irc	1203
2025-12-28 06:49:05	mysql	4802
2025-12-28 06:49:05	pmuser	1775
2025-12-28 06:49:05	ventrilo	1465
2025-12-28 06:49:05	system	3305
2025-12-28 06:49:05	agushto	3692
2025-12-28 06:49:05	tomcat	1464
2025-12-28 06:49:05	desktop	3518
2025-12-28 06:49:05	yp	2856
2025-12-28 06:49:05	mail	1054
2025-12-28 06:49:05	apache	2630
2025-12-28 06:49:05	services	4740
2025-12-28 06:49:05	irc	1203
2025-12-28 06:49:05	mysql	4802
2025-12-28 06:49:05	pmuser	1775
2025-12-28 06:49:05	ventrilo	1465
2025-12-28 06:49:05	system	3305
2025-12-28 06:49:05	agushto	3692
2025-12-28 06:49:05	tomcat	1464
2025-12-28 06:49:05	desktop	3518
2025-12-28 06:49:05	yp	2856
2025-12-28 06:49:05	mail	1054
2025-12-28 06:49:05	apache	2630
2025-12-28 06:49:05	services	4740
2025-12-28 06:49:05	irc	1203
2025-12-28 06:49:05	mysql	4802
2025-12-28 06:49:05	pmuser	1775
2025-12-28 06:49:05	ventrilo	1465
2025-12-28 06:49:05	system	3305

_time	user	port
2025-12-28 06:49:02	db	2690
2025-12-28 06:49:02	db	2690
2025-12-28 06:49:02	db	2690
2025-12-28 06:49:02	db	2690