Nuova ricerca

```
index=m6 "Failed password"
| rex "Failed password for (invalid user )?(?<username>\S+) from (?<src_ip>\d{1,3}(?:\.\d{1,3}){3}) port
    (?<port>\d+)"
| table _time, src_ip, username, port, _raw
```

Sempre

✓ **33.253 eventi** (prima di 05/05/25 08:33:10,000) Nessun campionamento degli eventi

Statistiche (33.253)

_time	src_ip	username	port	_raw
2025-05-02 05:46:19	123.30.108.208	jabber	1454	Tue May 02 2025 05:46:19 www3 sshd[4732]: Failed password for invalid user jabber from 123.30.108.208 port 1454 ssh2
2025-05-02 05:46:19	123.30.108.208	mailman	4980	Tue May 02 2025 05:46:19 www3 sshd[4875]: Failed password for invalid user mailman from 123.30.108.208 port 4980 ssh2
2025-05-02 05:46:19	123.30.108.208	henri	2359	Tue May 02 2025 05:46:19 www3 sshd[1664]: Failed password for invalid user henri from 123.30.108.208 port 2359 ssh2
2025-05-02 05:46:19	123.30.108.208	root	2295	Tue May 02 2025 05:46:19 www3 sshd[2221]: Failed password for root from 123.30.108.208 port 2295 ssh2
2025-05-02 05:46:19	128.241.220.82	helpdesk	3210	Tue May 02 2025 05:46:19 www3 sshd[3917]: Failed password for invalid user helpdesk from 128.241.220.82 port 3210 ssh2
2025-05-02 05:46:19	128.241.220.82	root	3117	Tue May 02 2025 05:46:19 www3 sshd[1448]: Failed password for root from 128.241.220.82 port 3117 ssh2
2025-05-02 05:46:19	128.241.220.82	irc	3428	Tue May 02 2025 05:46:19 www3 sshd[1613]: Failed password for invalid user irc from 128.241.220.82 port 3428 ssh2
2025-05-02 05:46:19	128.241.220.82	services	2361	Tue May 02 2025 05:46:19 www3 sshd[5892]: Failed password for invalid user services from 128.241.220.82 port 2361 ssh2
2025-05-02 05:46:19	128.241.220.82	prince	2481	Tue May 02 2025 05:46:19 www3 sshd[2594]: Failed password for prince from 128.241.220.82 port 2481 ssh2
2025-05-02 05:46:19	128.241.220.82	root	1070	Tue May 02 2025 05:46:19 www3 sshd[3786]: Failed password for root from 128.241.220.82 port 1070 ssh2
2025-05-02 05:46:19	128.241.220.82	sys	2687	Tue May 02 2025 05:46:19 www3 sshd[2388]: Failed password for invalid user sys from 128.241.220.82 port 2687 ssh2

_time	src_ip	username	port	_raw
2025-05-02 05:46:19	128.241.220.82	sunny	4350	Tue May 02 2025 05:46:19 www3 sshd[4767]: Failed password for invalid user sunny from 128.241.220.82 port 4350 ssh2
2025-05-02 05:46:19	128.241.220.82	icinga	1547	Tue May 02 2025 05:46:19 www3 sshd[5981]: Failed password for invalid user icinga from 128.241.220.82 port 1547 ssh2
2025-05-02 05:46:19	128.241.220.82	email	2794	Tue May 02 2025 05:46:19 www3 sshd[3713]: Failed password for invalid user email from 128.241.220.82 port 2794 ssh2
2025-05-02 05:46:19	128.241.220.82	harrison	4813	Tue May 02 2025 05:46:19 www3 sshd[4345]: Failed password for invalid user harrison from 128.241.220.82 port 4813 ssh2
2025-05-02 05:46:19	128.241.220.82	desktop	1954	Tue May 02 2025 05:46:19 www3 sshd[3951]: Failed password for invalid user desktop from 128.241.220.82 port 1954 ssh2
2025-05-02 05:46:19	128.241.220.82	operator	1811	Tue May 02 2025 05:46:19 www3 sshd[3302]: Failed password for invalid user operator from 128.241.220.82 port 1811 ssh2
2025-05-02 05:46:19	128.241.220.82	noone	1522	Tue May 02 2025 05:46:19 www3 sshd[5759]: Failed password for invalid user noone from 128.241.220.82 port 1522 ssh2
2025-05-02 05:46:19	128.241.220.82	administrator	1141	Tue May 02 2025 05:46:19 www3 sshd[1907]: Failed password for invalid user administrator from 128.241.220.82 port 1141 ssh2
2025-05-02 05:46:19	128.241.220.82	informix	2723	Tue May 02 2025 05:46:19 www3 sshd[4131]: Failed password for invalid user informix from 128.241.220.82 port 2723 ssh2