Nuova ricerca

```
source="tutorialdata.zip:*" | search "Failed password"
| rex field=_raw "from (?<ip>\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3})"
| rex field=_raw "(?<user>[\w@-]+) from" |rex field=_raw "(?<motivo>invalid user)"
| eval fallimento = if(isnull(motivo), "Failed password for valid user", "Failed password for invalid user"
    )
| sort - _time
| table _time ip user fallimento
```

Intervallo temporale: Sempre

✓ **10.000 eventi** (prima di 04/01/26 13:25:47,000) Nessun campionamento degli eventi

Statistiche (10.000)

_time	ip	user	fallimento
2025-12-28 06:49:05	194.8.74.23	appserver	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	appserver	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	appserver	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	appserver	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	root	Failed password for valid user
2025-12-28 06:49:05	194.8.74.23	testuser	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	apache	Failed password for valid user
2025-12-28 06:49:05	194.8.74.23	mongodb	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	mail	Failed password for valid user
2025-12-28 06:49:05	194.8.74.23	games	Failed password for valid user
2025-12-28 06:49:05	194.8.74.23	desktop	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	nagios	Failed password for valid user
2025-12-28 06:49:05	194.8.74.23	cyrus	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	guest	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	itmadmin	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	inet	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	operator	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	irc	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	harrison	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	local	Failed password for invalid user
2025-12-28 06:49:05	194.8.74.23	local	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	testing	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	admin	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	demon	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	vpxuser	Failed password for invalid user

_time	ip	user	fallimento
2025-12-28 06:49:05	203.45.206.135	local	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	ftp	Failed password for valid user
2025-12-28 06:49:05	203.45.206.135	nagios	Failed password for valid user
2025-12-28 06:49:05	203.45.206.135	itmadmin	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	backup	Failed password for valid user
2025-12-28 06:49:05	203.45.206.135	dbase	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	vmware	Failed password for invalid user
2025-12-28 06:49:05	10.1.10.172	myuan	Failed password for valid user
2025-12-28 06:49:05	203.45.206.135	nobody	Failed password for valid user
2025-12-28 06:49:05	203.45.206.135	jabber	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	email	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	jessica	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	jabber	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	postgres	Failed password for invalid user
2025-12-28 06:49:05	203.45.206.135	gitolite	Failed password for invalid user
2025-12-28 06:49:05	89.106.20.218	irc	Failed password for invalid user
2025-12-28 06:49:05	89.106.20.218	sales	Failed password for invalid user
2025-12-28 06:49:05	89.106.20.218	games	Failed password for valid user
2025-12-28 06:49:05	10.2.10.163	nsharpe	Failed password for valid user
2025-12-28 06:49:05	89.106.20.218	root	Failed password for valid user
2025-12-28 06:49:05	89.106.20.218	hammer	Failed password for valid user
2025-12-28 06:49:05	89.106.20.218	root	Failed password for valid user
2025-12-28 06:49:05	89.106.20.218	news	Failed password for valid user
2025-12-28 06:49:05	89.106.20.218	ventrilo	Failed password for invalid user
2025-12-28 06:49:05	89.106.20.218	library	Failed password for invalid user
2025-12-28 06:49:05	89.106.20.218	mail	Failed password for valid user
2025-12-28 06:49:05	89.106.20.218	susan	Failed password for invalid user
2025-12-28 06:49:05	89.106.20.218	administrator	Failed password for invalid user
2025-12-28 06:49:05	89.106.20.218	inet	Failed password for invalid user
2025-12-28 06:49:05	89.106.20.218	email	Failed password for invalid user
2025-12-28 06:49:05	69.175.97.11	jira	Failed password for valid user
2025-12-28 06:49:05	69.175.97.11	root	Failed password for valid user
2025-12-28 06:49:05	69.175.97.11	appserver	Failed password for invalid user
2025-12-28 06:49:05	69.175.97.11	admin	Failed password for invalid user
2025-12-28 06:49:05	69.175.97.11	rightscale	Failed password for invalid user

_time	ip	user	fallimento
2025-12-28 06:49:05	69.175.97.11	games	Failed password for valid user
2025-12-28 06:49:05	69.175.97.11	sync	Failed password for valid user
2025-12-28 06:49:05	69.175.97.11	sys	Failed password for invalid user
2025-12-28 06:49:05	69.175.97.11	cyrus	Failed password for invalid user
2025-12-28 06:49:05	69.175.97.11	sys	Failed password for invalid user
2025-12-28 06:49:05	212.58.253.71	jabber	Failed password for invalid user
2025-12-28 06:49:05	212.58.253.71	britany	Failed password for valid user
2025-12-28 06:49:05	212.58.253.71	db4	Failed password for invalid user
2025-12-28 06:49:05	212.58.253.71	sys	Failed password for invalid user
2025-12-28 06:49:05	212.58.253.71	rdb	Failed password for invalid user
2025-12-28 06:49:05	212.58.253.71	administrator	Failed password for invalid user
2025-12-28 06:49:05	212.58.253.71	irc	Failed password for invalid user
2025-12-28 06:49:05	212.58.253.71	ubuntu	Failed password for invalid user
2025-12-28 06:49:05	212.58.253.71	mailman	Failed password for invalid user
2025-12-28 06:49:05	212.58.253.71	system	Failed password for invalid user
2025-12-28 06:49:05	212.58.253.71	jabber	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	amanda	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	admin	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	services	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	ubuntu	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	root	Failed password for valid user
2025-12-28 06:49:05	109.169.32.135	whois	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	itmuser	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	perl	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	system	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	email	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	inet	Failed password for invalid user
2025-12-28 06:49:05	109.169.32.135	itmuser	Failed password for invalid user
2025-12-28 06:49:05	95.130.170.231	ftpuser	Failed password for valid user
2025-12-28 06:49:05	95.130.170.231	administrator	Failed password for invalid user
2025-12-28 06:49:05	95.130.170.231	operator	Failed password for invalid user
2025-12-28 06:49:05	95.130.170.231	squid	Failed password for valid user
2025-12-28 06:49:05	95.130.170.231	apache	Failed password for valid user
2025-12-28 06:49:05	95.130.170.231	informix	Failed password for invalid user
2025-12-28 06:49:05	95.130.170.231	admin	Failed password for invalid user

_time	ip	user	fallimento
2025-12-28 06:49:05	95.130.170.231	helpdesk	Failed password for invalid user
2025-12-28 06:49:05	95.130.170.231	ftpuser	Failed password for valid user
2025-12-28 06:49:05	95.130.170.231	edmond	Failed password for invalid user
2025-12-28 06:49:05	95.130.170.231	postgres	Failed password for invalid user
2025-12-28 06:49:05	95.130.170.231	dba	Failed password for invalid user