Nuova ricerca

```
source="tutorialdata.zip:*" host="Eldia" "Failed password"
| rex field=_raw "Failed password for (?<reason>(invalid user )?(?<username>[^\s]+)) from (?<ip_address
    >[\d\.]+)"
| table _time ip_address username reason
```

Sempre

✓ **199.518 eventi** (prima di 21/12/24 01:26:01,000) Nessun campionamento degli eventi

Statistiche (199.518)

_time	ip_address	username	reason
2024-12-15 12:43:21	194.8.74.23	appserver	invalid user appserver
2024-12-15 12:43:21	194.8.74.23	root	root
2024-12-15 12:43:21	194.8.74.23	testuser	invalid user testuser
2024-12-15 12:43:21	194.8.74.23	apache	apache
2024-12-15 12:43:21	194.8.74.23	mongodb	invalid user mongodb
2024-12-15 12:43:21	194.8.74.23	mail	mail
2024-12-15 12:43:21	194.8.74.23	games	games
2024-12-15 12:43:21	194.8.74.23	desktop	invalid user desktop
2024-12-15 12:43:21	194.8.74.23	nagios	nagios
2024-12-15 12:43:21	194.8.74.23	cyrus	invalid user cyrus
2024-12-15 12:43:21	194.8.74.23	guest	invalid user guest
2024-12-15 12:43:21	194.8.74.23	itmadmin	invalid user itmadmin
2024-12-15 12:43:21	194.8.74.23	inet	invalid user inet
2024-12-15 12:43:21	194.8.74.23	operator	invalid user operator
2024-12-15 12:43:21	194.8.74.23	irc	invalid user irc
2024-12-15 12:43:21	194.8.74.23	harrison	invalid user harrison
2024-12-15 12:43:21	194.8.74.23	local	invalid user local
2024-12-15 12:43:21	194.8.74.23	local	invalid user local
2024-12-15 12:43:21	203.45.206.135	testing	invalid user testing
2024-12-15 12:43:21	203.45.206.135	admin	invalid user admin
2024-12-15 12:43:21	203.45.206.135	demon	invalid user demon
2024-12-15 12:43:21	203.45.206.135	vpxuser	invalid user vpxuser
2024-12-15 12:43:21	203.45.206.135	local	invalid user local
2024-12-15 12:43:21	203.45.206.135	ftp	ftp
2024-12-15 12:43:21	203.45.206.135	nagios	nagios
2024-12-15 12:43:21	203.45.206.135	itmadmin	invalid user itmadmin

_time	ip_address	username	reason
2024-12-15 12:43:21	203.45.206.135	backup	backup
2024-12-15 12:43:21	203.45.206.135	dbase	invalid user dbase
2024-12-15 12:43:21	203.45.206.135	vmware	invalid user vmware
2024-12-15 12:43:21			
2024-12-15 12:43:21	203.45.206.135	nobody	nobody
2024-12-15 12:43:21	203.45.206.135	jabber	invalid user jabber
2024-12-15 12:43:21	203.45.206.135	email	invalid user email
2024-12-15 12:43:21	203.45.206.135	jessica	invalid user jessica
2024-12-15 12:43:21	203.45.206.135	jabber	invalid user jabber
2024-12-15 12:43:21	203.45.206.135	postgres	invalid user postgres
2024-12-15 12:43:21	203.45.206.135	gitolite	invalid user gitolite
2024-12-15 12:43:21	89.106.20.218	irc	invalid user irc
2024-12-15 12:43:21	89.106.20.218	sales	invalid user sales
2024-12-15 12:43:21	89.106.20.218	games	games
2024-12-15 12:43:21			
2024-12-15 12:43:21	89.106.20.218	root	root
2024-12-15 12:43:21	89.106.20.218	hammer	hammer
2024-12-15 12:43:21	89.106.20.218	root	root
2024-12-15 12:43:21	89.106.20.218	news	news
2024-12-15 12:43:21	89.106.20.218	ventrilo	invalid user ventrilo
2024-12-15 12:43:21	89.106.20.218	library	invalid user library
2024-12-15 12:43:21	89.106.20.218	mail	mail
2024-12-15 12:43:21	89.106.20.218	susan	invalid user susan
2024-12-15 12:43:21	89.106.20.218	administrator	invalid user administrator
2024-12-15 12:43:21	89.106.20.218	inet	invalid user inet
2024-12-15 12:43:21	89.106.20.218	email	invalid user email
2024-12-15 12:43:21	69.175.97.11	jira	jira
2024-12-15 12:43:21	69.175.97.11	root	root
2024-12-15 12:43:21	69.175.97.11	appserver	invalid user appserver
2024-12-15 12:43:21	69.175.97.11	admin	invalid user admin
2024-12-15 12:43:21	69.175.97.11	rightscale	invalid user rightscale
2024-12-15 12:43:21	69.175.97.11	games	games
2024-12-15 12:43:21	69.175.97.11	sync	sync
2024-12-15 12:43:21	69.175.97.11	sys	invalid user sys
2024-12-15 12:43:21	69.175.97.11	cyrus	invalid user cyrus

_time	ip_address	username	reason
2024-12-15 12:43:21	69.175.97.11	sys	invalid user sys
2024-12-15 12:43:21	212.58.253.71	jabber	invalid user jabber
2024-12-15 12:43:21	212.58.253.71	britany	britany
2024-12-15 12:43:21	212.58.253.71	db4	invalid user db4
2024-12-15 12:43:21	212.58.253.71	sys	invalid user sys
2024-12-15 12:43:21	212.58.253.71	rdb	invalid user rdb
2024-12-15 12:43:21	212.58.253.71	administrator	invalid user administrator
2024-12-15 12:43:21	212.58.253.71	irc	invalid user irc
2024-12-15 12:43:21	212.58.253.71	ubuntu	invalid user ubuntu
2024-12-15 12:43:21	212.58.253.71	mailman	invalid user mailman
2024-12-15 12:43:21	212.58.253.71	system	invalid user system
2024-12-15 12:43:21	212.58.253.71	jabber	invalid user jabber
2024-12-15 12:43:21	109.169.32.135	amanda	invalid user amanda
2024-12-15 12:43:21	109.169.32.135	admin	invalid user admin
2024-12-15 12:43:21	109.169.32.135	services	invalid user services
2024-12-15 12:43:21	109.169.32.135	ubuntu	invalid user ubuntu
2024-12-15 12:43:21	109.169.32.135	root	root
2024-12-15 12:43:21	109.169.32.135	whois	invalid user whois
2024-12-15 12:43:21	109.169.32.135	itmuser	invalid user itmuser
2024-12-15 12:43:21	109.169.32.135	perl	invalid user perl
2024-12-15 12:43:21	109.169.32.135	system	invalid user system
2024-12-15 12:43:21	109.169.32.135	email	invalid user email
2024-12-15 12:43:21	109.169.32.135	inet	invalid user inet
2024-12-15 12:43:21	109.169.32.135	itmuser	invalid user itmuser
2024-12-15 12:43:21	95.130.170.231	ftpuser	ftpuser
2024-12-15 12:43:21	95.130.170.231	administrator	invalid user administrator
2024-12-15 12:43:21	95.130.170.231	operator	invalid user operator
2024-12-15 12:43:21	95.130.170.231	squid	squid
2024-12-15 12:43:21	95.130.170.231	apache	apache
2024-12-15 12:43:21	95.130.170.231	informix	invalid user informix
2024-12-15 12:43:21	95.130.170.231	admin	invalid user admin
2024-12-15 12:43:21	95.130.170.231	helpdesk	invalid user helpdesk
2024-12-15 12:43:21	95.130.170.231	ftpuser	ftpuser
2024-12-15 12:43:21	95.130.170.231	edmond	invalid user edmond
2024-12-15 12:43:21	95.130.170.231	postgres	invalid user postgres

_time	ip_address	username	reason
2024-12-15 12:43:21	95.130.170.231	dba	invalid user dba
2024-12-15 12:43:21	95.130.170.231	sysadmin	invalid user sysadmin
2024-12-15 12:43:21	217.197.192.20	carrie	invalid user carrie
2024-12-15 12:43:21	217.197.192.20	susan	invalid user susan