

Nuova ricerca

```
source="tutorialdata.zip:*" host="Eldia" "sshd:session" "session opened"
| rex "session opened for user (?<user_id>\w+).*uid=(?<uid>\d+)"
| table _time user_id uid
```

Sempre

✓ 12.215 eventi (prima di 21/12/24 01:43:37,000) Nessun campionamento degli eventi

Statistiche (12.215)

_time ↕	user_id ↕	uid ↕
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	nsharp	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	myuan	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	nsharp	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	nsharp	0
2024-12-15 12:43:21	nsharp	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	nsharp	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	nsharp	0
2024-12-15 12:43:21	djohnson	0

_time ↕	user_id ↕		uid ↕	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	myuan		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	myuan		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	myuan		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	

_time ↕	user_id ↕		uid ↕	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	nsharpe		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	myuan		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	
2024-12-15 12:43:21	djohnson		0	

_time ↕	user_id ↕	uid ↕ ✎
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	djohnson	0
2024-12-15 12:43:21	myuan	0