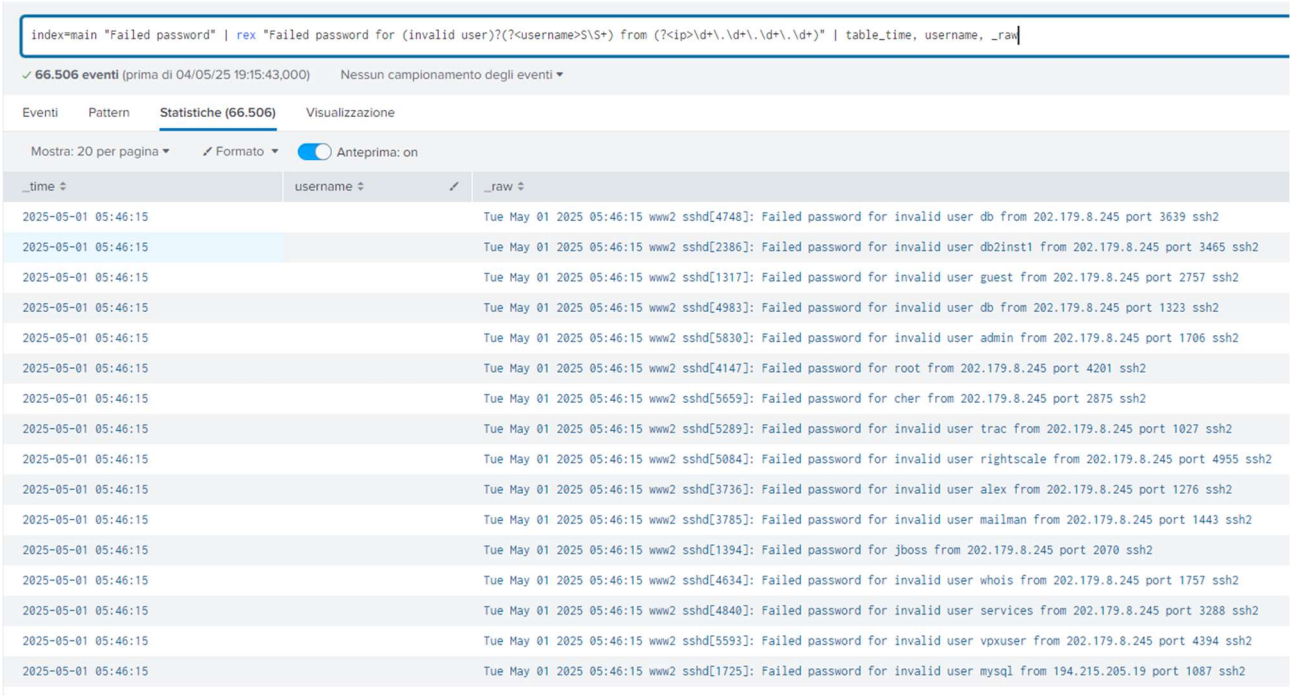
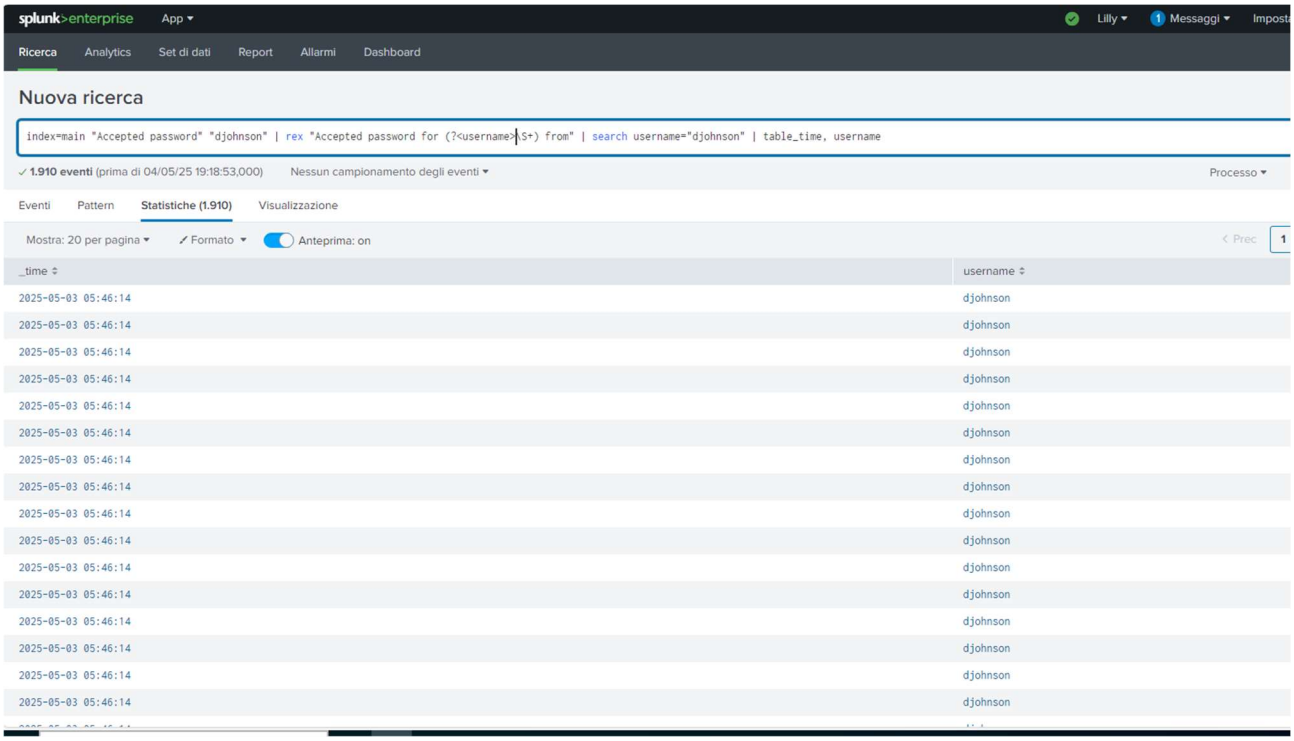
1. Crea una query Splunk per identificare tutti i tentativi di accesso falliti "Failed password". La query dovrebbe mostrare il timestamp, l'indirizzo IP di origine, il nome utente e il motivo del fallimento.

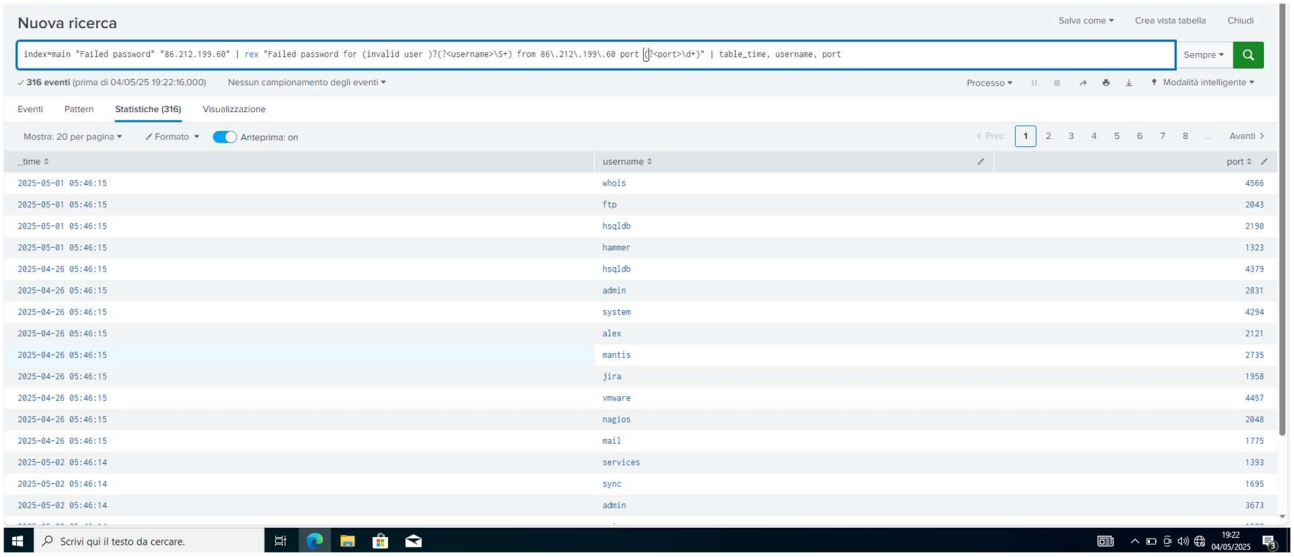


2. Scrivi una query Splunk per trovare tutte le sessioni SSH aperte con successo. La query dovrebbe filtrare per l'utente “djohnson” e mostrare il timestamp e l'ID utente.

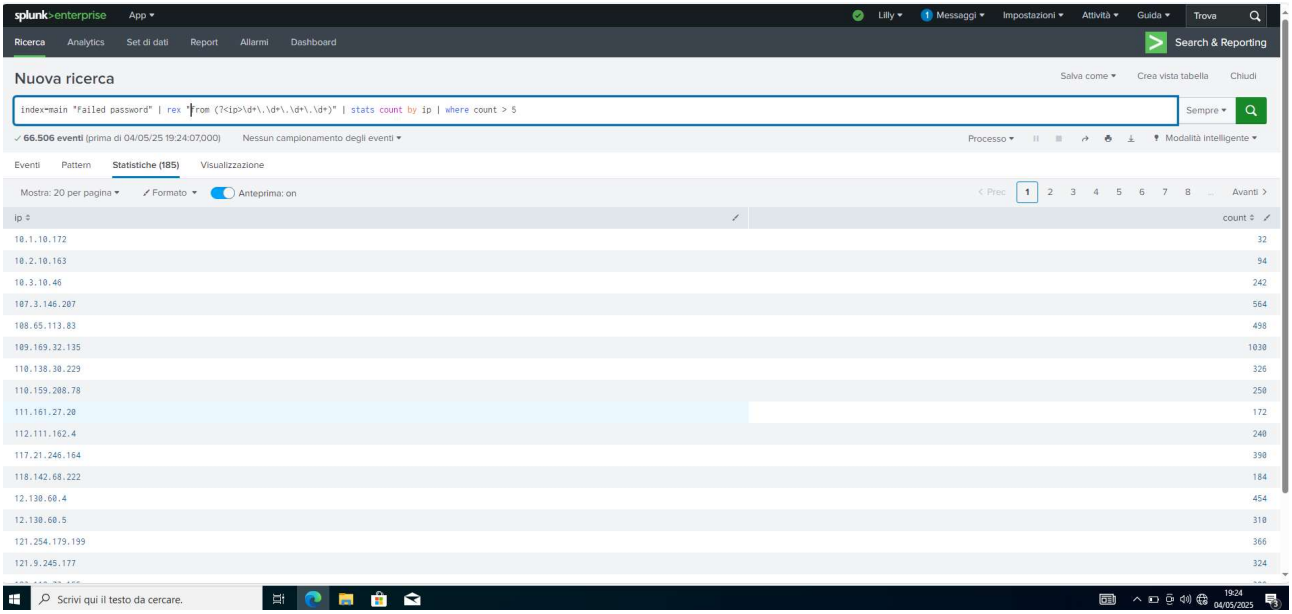


Scrivi una query Splunk per trovare tutti i tentativi di accesso falliti provenienti dall'indirizzo IP “86.212.199.60”. La query dovrebbe mostrare il timestamp, il nome utente e il numero di

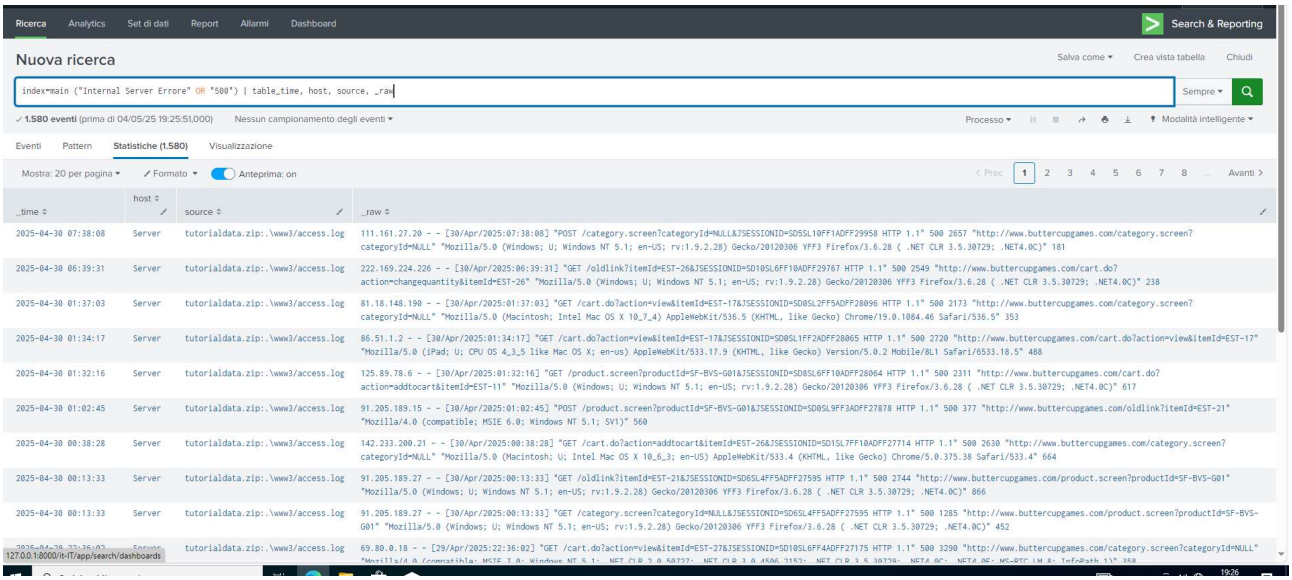
porta.



3. Crea una query Splunk per identificare gli indirizzi IP che hanno tentato di accedere ("Failed password") al sistema più di 5 volte. La query dovrebbe mostrare l'indirizzo IP e il numero di tentativi.



4. Crea una query Splunk per trovare tutti gli Internal Server Error.


Ricerca
Analytics
Set di dati
Report
Allarmi
Dashboard
Search & Reporting
Nuova ricerca
Salva come
Crea vista tabella
Chiudi
index=main ("Internal Server Errore" OR "500") | table_time, host, source, _raw
Sempre
1.580 eventi (prima di 04/05/25 19:25:51,000)
Nessun campionamento degli eventi
Processo
Modalità intelligente
Eventi
Pattern
Statistiche (1.580)
Visualizzazione
Mostra: 20 per pagina
Formato
Anteprima: on
< Prec
1
2
3
4
5
6
7
8
Avanti >
_time
host
source
_raw
2025-04-30 07:38:08 Server tutorialdata.zip:.\www3/access.log 111.161.27.20 - - [30/Apr/2025:07:38:08] "POST /category.screen?categoryId=NULL&JSESSIONID=SD5SL10FF1ADFF29958 HTTP 1.1" 500 2657 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 181
2025-04-30 06:39:31 Server tutorialdata.zip:.\www3/access.log 222.169.224.226 - - [30/Apr/2025:06:39:31] "GET /oldlink?itemId=EST-26&JSESSIONID=SD10SL6FF10ADFF29767 HTTP 1.1" 500 2549 "http://www.buttercupgames.com/cart.do?action=changequantity&itemId=EST-26" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 238
2025-04-30 01:37:03 Server tutorialdata.zip:.\www3/access.log 81.18.148.190 - - [30/Apr/2025:01:37:03] "GET /cart.do?action=view&itemId=EST-17&JSESSIONID=SD0SL2FF5ADFF28096 HTTP 1.1" 500 2173 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 353
2025-04-30 01:34:17 Server tutorialdata.zip:.\www3/access.log 86.51.1.2 - - [30/Apr/2025:01:34:17] "GET /cart.do?action=view&itemId=EST-17&JSESSIONID=SD0SL1FF2ADFF28065 HTTP 1.1" 500 2720 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-17" "Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5" 488
2025-04-30 01:32:16 Server tutorialdata.zip:.\www3/access.log 125.89.78.6 - - [30/Apr/2025:01:32:16] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD8SL6FF10ADFF28064 HTTP 1.1" 500 2311 "http://www.buttercupgames.com/cart.do?action=addtocart&itemId=EST-11" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 617
2025-04-30 01:02:45 Server tutorialdata.zip:.\www3/access.log 91.205.189.15 - - [30/Apr/2025:01:02:45] "POST /product.screen?productId=SF-BVS-G01&JSESSIONID=SD0SL9FF3ADFF27878 HTTP 1.1" 500 377 "http://www.buttercupgames.com/oldlink?itemId=EST-21" "Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.1; SV1)" 560
2025-04-30 00:38:28 Server tutorialdata.zip:.\www3/access.log 142.233.200.21 - - [30/Apr/2025:00:38:28] "GET /cart.do?action=addtocart&itemId=EST-26&JSESSIONID=SD1SL7FF10ADFF27714 HTTP 1.1" 500 2630 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Macintosh; U; Intel Mac OS X 10_6_3; en-US) AppleWebKit/533.4 (KHTML, like Gecko) Chrome/5.0.375.38 Safari/533.4" 664
2025-04-30 00:13:33 Server tutorialdata.zip:.\www3/access.log 91.205.189.27 - - [30/Apr/2025:00:13:33] "GET /oldlink?itemId=EST-21&JSESSIONID=SD6SL4FF5ADFF27595 HTTP 1.1" 500 2744 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 866
2025-04-30 00:13:33 Server tutorialdata.zip:.\www3/access.log 91.205.189.27 - - [30/Apr/2025:00:13:33] "GET /category.screen?categoryId=NULL&JSESSIONID=SD6SL4FF5ADFF27595 HTTP 1.1" 500 1285 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 452
Server tutorialdata.zip:.\www3/access.log 69.80.0.18 - - [29/Apr/2025:22:36:02] "GET /cart.do?action=view&itemId=EST-27&JSESSIONID=SD10SL6FF4ADFF27175 HTTP 1.1" 500 3290 "http://www.buttercupgames.com/category.screen?categoryId=NULL"
127.0.0.1:8000/it-IT/app/search/dashboards
19:26