

```
source="tutorialdata.zip:*" sourcetype="www1/secure" "failed password"
| rex "Failed password for (invalid user )?(?<user>(w+)) from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| stats count by src_ip
| where count > 5
| table src_ip count
```

Sempre ▼

✓ 33.253 eventi (prima di 03/11/24 22:42:27,000) Nessun campionamento degli eventi ▼

Processo ▼ || ▶ 🔍 ⬇️ ! Modalità intelligente ▼

Eventi

Pattern

Statistiche (182)

Visualizzazione

20 per pagina ▼ ✓ Formato Anteprima ▼

< Prec12345678...Avanti >

src_ip ↕	count ↕ ✎
107.3.146.207	281
108.65.113.83	248
109.169.32.135	514
110.138.30.229	163
110.159.208.78	125
111.161.27.20	85
112.111.162.4	118
117.21.246.164	194
118.142.68.222	91
12.130.60.4	227
12.130.60.5	155

Attiva Windows





Nuova ricerca

Salva come ▾ Crea vista tabella Chiudi


source="tutorialdata.zip:\*" sourcetype="www1/secure" "Accepted password" "djohnson" | rex "sshd\[(<session\_id>d+)\]: Accepted password for (<user>\w+)" | where user="djohnson"| eval status="Success" | table \_time user session\_id status

Sempre ▾ 

✓ 955 eventi (prima di 03/11/24 22:31:39,000) Nessun campionamento degli eventi ▾

Processo ▾ ||     Modalità intelligente ▾

Eventi Pattern **Statistiche (955)** Visualizzazione

20 per pagina ▾  Formato Anteprima ▾

< Prec 1 2 3 4 5 6 7 8 ... Avanti >

_time ↕	user ↕	session_id ↕	status ↕
2024-10-30 04:37:04	djohnson	57740	Success
2024-10-30 04:37:04	djohnson	27688	Success
2024-10-30 04:37:04	djohnson	95467	Success
2024-10-30 04:37:04	djohnson	98759	Success
2024-10-30 04:37:04	djohnson	99654	Success
2024-10-30 04:37:04	djohnson	45962	Success
2024-10-30 04:37:04	djohnson	94001	Success
2024-10-30 04:37:04	djohnson	52325	Success
2024-10-30 04:37:04	djohnson	83594	Success
2024-10-30 04:37:04	djohnson	41627	Success
2024-10-30 04:37:04	djohnson	50467	Success
2024-10-30 04:37:04	djohnson	89967	Success
2024-10-30 04:37:04	djohnson	48946	Success
2024-10-30 04:37:04	djohnson	84890	Success
2024 10 30 04:37:04	djohnson	48884	Success

Attiva Windows  
Passa a Impostazioni per attivare Windows.

Nuova ricerca

source="tutorialdata.zip:\*" sourcetype="www1/secure" ("failed password" OR "Accepted password")  
| rex "password for (invalid user )?(?<user>\w+) from (?<src\_ip>86\.212\.199\.60) port (?<port>d+)"  
| eval status=if(searchmatch("failed password"), "Failed", "Success")  
| where src\_ip="86.212.199.60"  
| table \_time src\_ip user port status

Sempre ▾

✓ 158 eventi (prima di 03/11/24 22:38:08,000) Nessun campionamento degli eventi ▾

Processo ▾ || ↶ ↷ ⬇ ⚙ Modalità intelligente ▾

EventiPattern

Statistiche (158)

Visualizzazione

20 per pagina ▾ ✓ Formato Anteprima ▾

< Prec 1 2 3 4 5 6 7 8 Avanti >

_time ↕	src_ip ↕	user ↕	port ↕	status ↕
2024-10-29 04:37:04	86.212.199.60	services	1393	Failed
2024-10-29 04:37:04	86.212.199.60	sync	1695	Failed
2024-10-29 04:37:04	86.212.199.60	admin	3673	Failed
2024-10-29 04:37:04	86.212.199.60	nginx	1582	Failed
2024-10-29 04:37:04	86.212.199.60	whois	1635	Failed
2024-10-29 04:37:04	86.212.199.60	mailman	4339	Failed
2024-10-29 04:37:04	86.212.199.60	mailman	1954	Failed
2024-10-29 04:37:04	86.212.199.60	rdb	2650	Failed
2024-10-28 04:37:04	86.212.199.60	ncsd	4022	Failed
2024-10-28 04:37:04	86.212.199.60	games	1763	Failed
2024-10-28 04:37:04	86.212.199.60	noone	1582	Failed
2024-10-28 04:37:04	86.212.199.60	fpass	3420	Failed

Nuova ricerca

Salva come ▾ Crea vista tabella Chiudi

```
source="tutorialdata.zip:*" sourcetype="www1/secure" "failed password"
| rex "Failed password for (invalid user )?(?<user>\w+) from (?<src_ip>\d+\.\d+\.\d+\.\d+)"
| eval failure_reason=if(match(_raw, "invalid user"), "Invalid User", "Incorrect Password")
| table _time src_ip user failure_reason
```

✓ 66.506 eventi (prima di 03/11/24 22:25:59,000) Nessun campionamento degli eventi ▾

Processo ▾ || ↻ 🗑️ ⬇️ ! Modalità intelligente ▾

Eventi Pattern **Statistiche (66.506)** Visualizzazione

20 per pagina ▾ ↗ Formato Anteprima ▾ < Prec 1 2 3 4 5 6 7 8 ... Avanti >

_time ↕	src_ip ↕	user ↕	failure_reason ↕
2024-10-28 04:37:05	194.215.205.19	desktop	Invalid User
2024-10-28 04:37:05	194.215.205.19	rdb	Invalid User
2024-10-28 04:37:05	194.215.205.19	games	Incorrect Password
2024-10-28 04:37:05	194.215.205.19	library	Invalid User
2024-10-28 04:37:05	87.194.216.51	nagios	Incorrect Password
2024-10-28 04:37:05	87.194.216.51	helpdesk	Invalid User
2024-10-28 04:37:05	87.194.216.51	fpass	Invalid User
2024-10-28 04:37:05	87.194.216.51	vpuser	Invalid User
2024-10-28 04:37:05	87.194.216.51	uni	Invalid User
2024-10-28 04:37:05	87.194.216.51	sys	Invalid User
2024-10-28 04:37:05	87.194.216.51	mysql	Invalid User
2024-10-28 04:37:05	87.194.216.51	system	Invalid User
2024-10-28 04:37:05	87.194.216.51	vmware	Invalid User

Attiva Windows  
Passa a Impostazioni per attivare Windows.

Nuova ricerca

Salva come   Crea vista tabella   Chiudi

```
source="tutorialdata.zip:*" sourcetype="access_combined_wcookie"
("Internal Server Error" OR "500")
| eval status="Internal Server Error"
| table _time src_ip status_code error_message status
```

Sempre

✓ 781 eventi (prima di 03/11/24 22:47:39,000)   Nessun campionamento degli eventi   Processo   ||   ➔   ⌵   ⌴   ⚡ Modalità intelligente

Eventi   Pattern   **Statistiche (781)**   Visualizzazione

20 per pagina   Formato   Anteprima   < Prec   1   2   3   4   5   6   7   8   ...   Avanti >

_time	src_ip	status_code	error_message	status
2024-10-27 07:38:08				Internal Server Error
2024-10-27 06:39:31				Internal Server Error
2024-10-27 01:37:03				Internal Server Error
2024-10-27 01:34:17				Internal Server Error
2024-10-27 01:32:16				Internal Server Error
2024-10-27 01:02:45				Internal Server Error
2024-10-27 00:38:28				Internal Server Error
2024-10-27 00:13:33				Internal Server Error
2024-10-27 00:13:33				Internal Server Error
2024-10-26 22:36:02				Internal Server Error
2024-10-26 21:54:50				Internal Server Error
2024-10-26 19:26:28				Internal Server Error
2024-10-26 18:50:51				Internal Server Error

Attiva Windows  
Passa a Impostazioni per attivare Windows.

## Conclusioni Basate sui Log Analizzati

Dall'analisi eseguita con le query Splunk, sono emerse diverse informazioni utili riguardo alle attività e agli errori di sistema presenti nei log. Questi risultati ci permettono di identificare potenziali minacce e aree di miglioramento per la sicurezza del sistema. Di seguito sono riportate le principali osservazioni:

### 1. **Tentativi di Accesso Falliti :**

- Numerosi tentativi di accesso falliti, indicati da "Failed password", sono stati rilevati nei log. Questo potrebbe suggerire:
  - **Attività di forza bruta** : Indirizzi IP che tentano ripetutamente di accedere possono rappresentare tentativi di indovinare credenziali.
  - **Esposizione di account sensibili** : La presenza di nomi utente specifici nei tentativi di accesso potrebbe indicare che gli aggressori stanno cercando di compromettere account privilegiati. È consigliabile monitorare tali account per identificare tempestivamente possibili minacce.

### 2. **Accesso SSH di Successo per Utenti Specifici :**

- Le sessioni SSH aperte con successo per utenti privilegiati non sono emerse nei dati analizzati, ma è comunque importante:
  - **Implementare il monitoraggio continuo** : Gli accessi SSH per utenti con privilegi elevati dovrebbero essere monitorati costantemente, in particolare per l'utente **djohnson**, per prevenire abusi o accessi non autorizzati da IP sospetti.
  - **Abilitare notifiche per accessi anomali** : L'invio di notifiche in caso di accessi fuori orario o da indirizzi IP insoliti potrebbe migliorare la sicurezza del sistema.

### 3. Tentativi di accesso da IP specifici :

- Non sono stati rilevati tentativi di accesso falliti dall'indirizzo IP **86.212.199.60**, suggerendo che questo IP non è stato utilizzato in tentativi sospetti. Tuttavia, per la sicurezza:
- **mantenere una lista di controllo** : Si consiglia di mantenere un elenco di IP in considerazione a rischio e monitorare eventuali tentativi di accesso futuri a questi indirizzi.

### 4. Indirizzi IP con più di 3 Tentativi di Accesso Falliti :

- Non è stato possibile identificare indirizzi IP specifici con più di 3 tentativi falliti a causa della mancanza di estrazione automatica del campo **src\_ip**. Per migliorare il monitoraggio:
  - **Configurare estrazioni personalizzate** : È consigliato configurare Splunk per estrarre correttamente il campo **src\_ip**, in modo da facilitare l'identificazione dell'IP potenzialmente ostile e il blocco preventivo delle attività sospette.

### 5. Errori di tipo "Errore interno del server" (500) :

- Gli errori "Internal Server Error" sono stati rilevati in numero significativo, suggerendo potenziali problemi di configurazione o destinazione nelle applicazioni web.
  - **Possibile debolezza del sistema** : Gli errori interni del server possono essere causati da input imprevisti che mettono alla prova i sistemi. Gli attaccanti potrebbero sfruttare queste vulnerabilità per lanciare attacchi più sofisticati.
  - **Necessità di revisione del codice** : Questi errori dovrebbero essere esaminati dal team di sviluppo per identificare problemi nel codice e ridurre il rischio di exploit.

## Raccomandazioni

- **Implementare un sistema di rilevamento delle intrusioni (IDS)** : Un IDS può monitorare e bloccare in modo proattivo i tentativi di accesso non autorizzati, migliorando la sicurezza del sistema.
- **Automatizzare l'analisi dei log** : configurare report automatici per identificare in tempo reale tentativi di accesso ripetuti o errori critici può migliorare la risposta a potenziali minacce.
- **Controllo degli errori del server** : Ridurre la frequenza degli errori "500" è fondamentale per prevenire gli exploit. Effettuare un'analisi approfondita del codice delle applicazioni può ridurre la probabilità di vulnerabilità.
- **Abilitare il rate limiting** : Limitare il numero di tentativi di accesso consentiti da un singolo IP in un breve periodo è una misura efficace per mitigare gli attacchi di forza bruta.

Questi interventi, insieme a una supervisione continua e a tecniche di rilevamento avanzate, possono contribuire in modo significativo a migliorare la sicurezza del sistema, prevenendo accessi non autorizzati e riducendo il rischio di interruzioni del servizio.