



Splunk

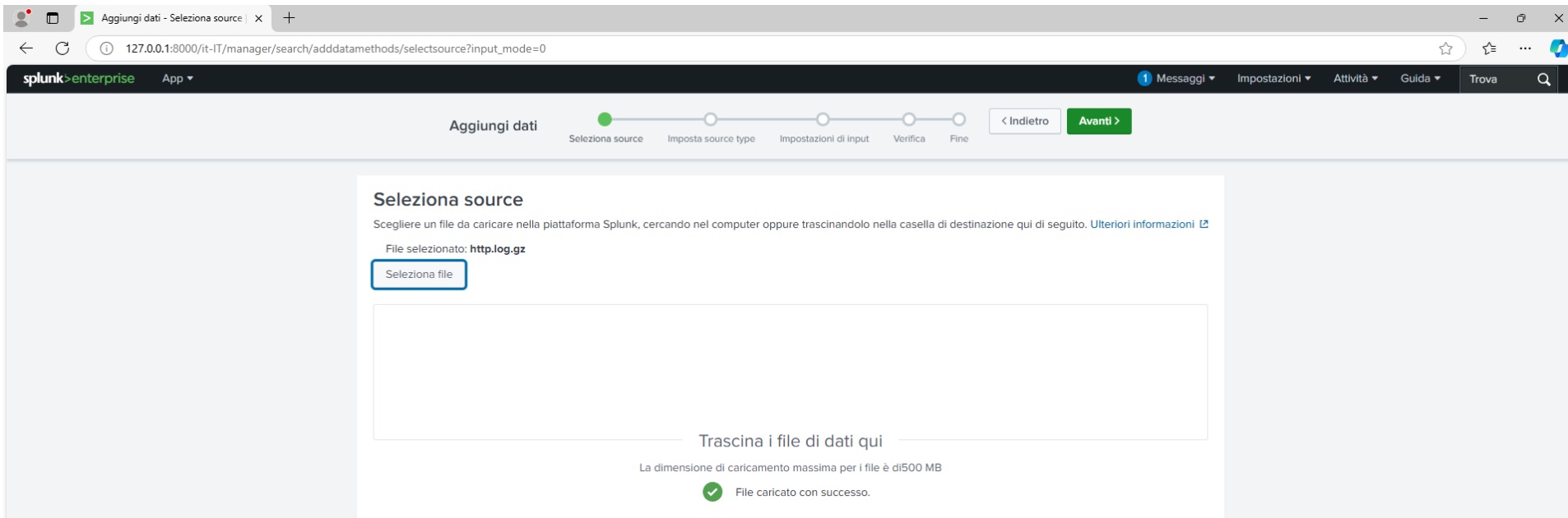
HTTP LOG ANALYSIS

Descrizione del progetto

Prenderemo in esame un log HTTP «raw», vedremo come estrarre dei campi grazie alle funzioni built-in di Splunk, per poi farne una analisi vedendo alcune informazioni che possiamo ricavare.

Caricamento del file di log

Clicchiamo su «aggiungi dati» scegliamo il path dove risiede il file, diamo il nome al source type, confermiamo gli altri campi e carichiamo il file per poter effettuare le ricerche su di esso tramite il modulo Search and Reporting.



Analisi

I campi estratti in automatico risultano essere riduttivi ai fini dell'analisi, per cui possiamo procedere con l'estrazione dei campi associati agli eventi quali: dominio interessato, source e destination ip ecc.

Possiamo fare ciò cliccando su «Estrai nuovi Campi»

< Nascondi campi

☰ Tutti i campi

CAMPI SELEZIONATI

a host 1

a source 1

a sourcetype 1

CAMPI INTERESSANTI

a index 1

linecount 10

a punct 100+

a splunk_server 1

a timestamp 1

11 campi in più

+ Estrai nuovi campi

Estrazione dei campi: selezione di un evento campione.

The screenshot shows the Splunk Field Extractor interface. At the top, a progress bar indicates the current step is 'Seleziona campi', with the 'Avanti >' button circled in red. Below the progress bar, the 'Seleziona evento di esempio' section is active, showing a 'DNS log' source type and a 'Ultima 90 giorni' time range. A sample event is displayed in a blue bar. The 'Eventi' section below shows a list of events with a filter and a table of event details. The table has columns for event ID, source, destination, protocol, port, and various fields. The first row of the table is highlighted.

Seleziona evento di esempio

Scegliere una source o un source type, selezionare un evento campione e fare clic su Avanti per continuare con il passaggio successivo. L'estrattore di campi userà l'evento per estrarre i campi. [Ulteriori informazioni](#)

Preferisco scrivere lo stesso l'espressione regolare >

Source type
DNS log

Intervallo temporale
Ultima 90 giorni

1332017991.970000 Cw500TGmBFF5z1Rc9 192.168.202.122 137 192.168.202.255 137 udp 33707 LABADMIN-641491 1 C_INTERNET 32 NB - - F F T F 1 - - F

Eventi

✓ 1.000 evento (04/06/24 00:00:00,000 - 02/09/24 19:17:12,000) 20 per pagina < Prec 1 2 3 4 5 6 7 8 ... Avanti >

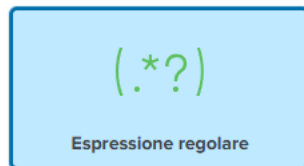
filto Esempio: 1.000 eventi Tutti gli eventi

_raw	...																			
1332017991.970000	Cw500TGmBFF5z1Rc9	192.168.202.122 137	192.168.202.255 137	udp	33707	LABADMIN-641491 1	C_INTERNET	32	NB	-	-	F	F	T	F	1	-	-	F	
1332017979.080000	CQnrcF1yLbtvjQbS8	192.168.202.83	45561	192.168.207.4	53	udp	12572	44.206.168.192.in-addr.arpa	1	C_INTERNET	12	PTR	3	NXDOMAIN	F	F	T	F	0	-
1332017959.830000	C4zDh93z81GYT1dq2k	192.168.202.88	60538	192.168.206.44	53	udp	36843	dr._dns-sd._udp.0.48.16.172.in-addr.arpa	1	C_INTERNET	12	PTR	5	REFUSED F	F	T	F	0	-	
1332017959.830000	CGBRgg3GyzwSH1wkB7	192.168.202.88	58547	192.168.206.44	53	udp	30842	dr._dns-sd._udp.0.202.168.192.in-addr.arpa	1	C_INTERNET	12	PTR	5	REFUSED F	F	T	F	0	-	
1332017959.830000	C1ZL144oVCIMvJgqb	192.168.202.88	58045	192.168.206.44	53	udp	28561	b._dns-sd._udp.0.48.16.172.in-addr.arpa	1	C_INTERNET	12	PTR	5	REFUSED F	F	T	F	0	-	
1332017959.830000	C0n0E3NUMg9TxJRsd	192.168.202.88	65208	192.168.206.44	53	udp	50791	1b._dns-sd._udp.0.48.16.172.in-addr.arpa	1	C_INTERNET	12	PTR	5	REFUSED F	F	T	F	0	-	

Estrazione dei campi

In base e grazie all'evento campione effettuiamo un «parsing» sul file di log, logicamente conoscendo la struttura di questi logs e i pattern che seguono.

Qui sotto riportiamo un esempio individuando il source ip, lo faremo anche per altri campi sullo stesso log e nella stessa sessione; sarebbe buona pratica estrarre però un campo per volta.



Splunk Enterprise estrarrà i campi usando un'espressione regolare.

`x|y|z`

Delimitatori

Splunk Enterprise estrarrà i campi utilizzando un delimitatore (come ad es. virgole, spazi o caratteri). Usare questo metodo per i dati delimitati, come i valori separati da virgola (file CSV).

Seleziona campi

Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare il testo che fa già parte di un'estrazione esistente, disabilitare prima le e

1332017991.970000 CwS00TGmBFF5z1Rc9 192.168.202.122 137

Anteprima

Se di seguito appaiono dei risultati non cor

Eventi

✓ 1.000 evento (04/06/24 00:00:00,000 - C

Estrai

Richiedi

Nome campo

Valore di esempio

192.168.202.122

Add Extraction

Estrazione dei campi

Estrattore di campi | Splunk 9.3.1

127.0.0.1:8000/it-IT/app/search/field_extractor?sid=1730990282.121

splunk>enterprise

App

1 MessaggiImpostazioniAttivitàGuidaTrova

Estrai campi

Seleziona campione

Seleziona metodo

Seleziona campi

Salva

< IndietroAvanti >

Campi esistenti >

Seleziona metodo

Indicare il metodo che si intende utilizzare per estrarre i campi. [Ulteriori informazioni](#)

[Preferisco scrivere io stesso l'espressione regolare >](#)

Source type
dhcn

Seleziona campi

Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare un valore come obbligatorio, il che significa che deve esistere in un evento per fare in modo che l'espressione regolare vi corrisponda. Fare clic sui valori evidenziati nell'evento di esempio per modificarli. Per evidenziare il testo che fa già parte di un'estrazione esistente, disabilitare prima le estrazioni esistenti. [Ulteriori informazioni](#)

1332014025.890000	CB0BGv2cvrebRwbJy8	192.168.202.150	50201	192.168.25.202	80	5	GET	192.168.25.202	/stylesheet.php?version=1332014220	http://192.168.25.202/main.php?stuff=1330755826	Mozilla/5.0 (X11; Linux	
i686; rv:10.0.2)	Gecko/20100101	Firefox/10.0.2	0	11805	200	OK	-	-	-	-	FyxEjX2vNhphAgn47	text/plain

[Mostra espressione regolare >](#)

[Visualizza in Ricerca](#)

Anteprima

Se di seguito appaiono dei risultati non corretti, fare clic su un evento aggiuntivo per aggiungerlo al set degli eventi di esempio. Evidenziarne i valori per migliorare l'estrazione. È possibile rimuovere i valori non corretti nel prossimo passaggio.

Eventi

Timestamp

src_ip

src_port

dst_ip

dst_port

Request_Method

URL

User_agent

Response_code

Response

Estrazione dei campi: nuovi campi interessanti

In automatico in base ai campi selezionati viene elaborata la regular expression corrispondente, fatto ciò potremo visualizzare i nuovi campi generati come in basso a destra.

Salva

Assegnare un nome all'estrazione e impostare le autorizzazioni.

Nome estrazioni **EXTRACT-**

Proprietario **splunktest**

App **search**

Autorizzazioni ☒ Proprietario ☐ App ☐ Tutte le app

Source type **DNS log**

Evento di esempio 1332017979.080000 CQnrcF1yLbtvjQbS8 192.168.202.83 45561 192.168.207.4 53 udp
12572 44.206.168.192.in-addr.arpa 1 C_INTERNET 12 PTR 3 NXDOMAIN F
F T F 0 - - F

Campi **src_ip,src_port,dst_ip,dst_port,Domain**

Espressione regolare **^(?:[^\t\n]*\t){2}(?P<src_ip>[^\t+])\t(?P<src_port>\d+)\t(?P<dst_ip>[^\t+])\t(?P<dst_port>[^\t+])\t[w+]\t\d+\t(?P<Domain>[^\t+])**

CAMPI SELEZIONATI

a host 1
a source 1
a sourcetype 1

CAMPI INTERESSANTI

a Domain 100+
a dst_ip 100+
dst_port 4
a index 1
linecount 10
a punct 100+
a splunk_server 1
a src_ip 100+
src_port 100+
a timestamp 1

11 campi in più

+ Estrai nuovi campi

Analisi del log

Per l'analisi del log la prima richiesta è di determinare la distribuzione dei metodi di richiesta (GET, POST, ecc.) per comprendere i modelli di traffico web.

Nuova ricerca

Salva come ▼

Crea vista tabella

Chiudi

1 index=_* OR index=* sourcetype=dhcp source="http.zip:.\http.log" Request_Method="*" | stats count by Request_Method

Sempre ▼



✓ 6.680 eventi (prima di 08/11/24 09:23:03,000)

Nessun campionamento degli eventi ▼

Processo ▼



Modalità intelligente ▼

Eventi

Pattern

Statistiche (3)

Visualizzazione

20 per pagina ▼

Formato

Anteprima ▼

Request_Method ↕

count ↕

GET

5524

HEAD

6

POST

1150

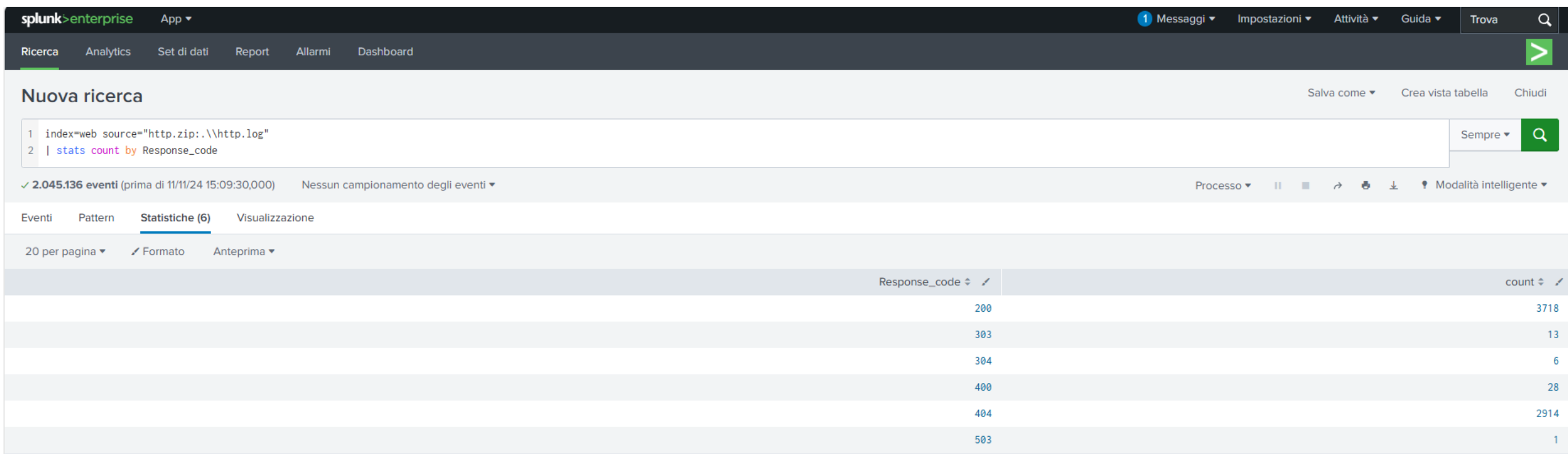
Analisi del log

Identificare gli URL o gli endpoint più accessibili dagli utenti.

<pre>1 index=web source="http.zip:\\http.log" 2 top limit=10 URL</pre>		Sempre	
✓ 2.045.136 eventi (prima di 11/11/24 15:03:01,000) Nessun campionamento degli eventi		Processo	Modalità intelligente
Eventi Pattern Statistiche (10) Visualizzazione			
20 per pagina Formato Anteprima			
URL	count	percent	
-	1783	26.556449	
/phpScheduleIt/reserve.php	1134	16.890080	
http://192.168.27.202/index.php	994	14.804885	
http://192.168.23.202/	432	6.434316	
http://192.168.28.202/	383	5.704498	
http://192.168.22.202/	357	5.317248	
http://192.168.26.202/	318	4.736372	
http://192.168.26.202/top.php?stuff=1861731255	188	2.800119	
http://192.168.23.202/top.php?stuff=2040844887	188	2.800119	
http://192.168.22.202/top.php?stuff=1417058040	164	2.442657	

Analisi del log

Analizzare i codici di risposta per identificare errori o richieste riuscite.



The screenshot displays the Splunk Enterprise web interface. At the top, the navigation bar includes the 'splunk>enterprise' logo, an 'App' dropdown, and links for 'Messaggi', 'Impostazioni', 'Attività', 'Guida', 'Trova', and a search icon. Below this, a secondary navigation bar contains 'Ricerca', 'Analytics', 'Set di dati', 'Report', 'Allarmi', and 'Dashboard'. The main content area is titled 'Nuova ricerca' and shows a search query: `1 index=web source="http.zip:\\http.log"` and `2 | stats count by Response_code`. The search results indicate 2,045,136 events. The 'Statistiche (6)' tab is selected, showing a table of response codes and their counts.

Response_code	count
200	3718
303	13
304	6
400	28
404	2914
503	1

Analisi del log

Possiamo fare una ricerca di attività sospette partendo dai codici di errore:

The screenshot shows a web interface for log analysis. At the top, there's a navigation bar with tabs: Ricerca, Analytics, Set di dati, Report, Allarmi, and Dashboard. Below this, a section titled 'Nuova ricerca' contains a search query editor. The query is: `1 index=*_* OR index=web source="http.zip:\\http.log"`, `2 | where Response_code=401`, and `3 | top limit=10 src_ip`. To the right of the query editor are buttons for 'Salva come', 'Crea vista tabella', and 'Chiudi'. Below the query editor, it shows '✓ 2.341 eventi (prima di 12/11/24 07:50:32,000)' and 'Nessun campionamento degli eventi'. There are also icons for 'Processo', a pause button, a refresh button, a download button, and a 'Modalità intelligente' toggle. Below the search section, there's a tab bar with 'Eventi', 'Pattern', 'Statistiche (10)', and 'Visualizzazione'. The 'Statistiche (10)' tab is selected. Below the tab bar, there's a table with columns: 'src_ip', 'count', and 'percent'. The table shows the top 10 IP addresses by count of 401 errors.

src_ip	count	percent
192.168.202.110	1699	72.575822
192.168.202.79	390	16.659547
192.168.202.138	82	3.502777
192.168.202.140	27	1.153353
192.168.202.112	26	1.110636
192.168.202.102	22	0.939769
192.168.202.136	17	0.726185
192.168.202.100	14	0.599255