Esercizio_S9_L1_Splunk_Monitor

Consegna

Abbiamo esplorato diverse funzionalità offerte da Splunk.

Oggi ci concentreremo sulla modalità "Monitora".

Il compito di oggi consiste nel configurare la modalità Monitora in Splunk e realizzare degli screenshot che ne confermino l'avvenuta configurazione.

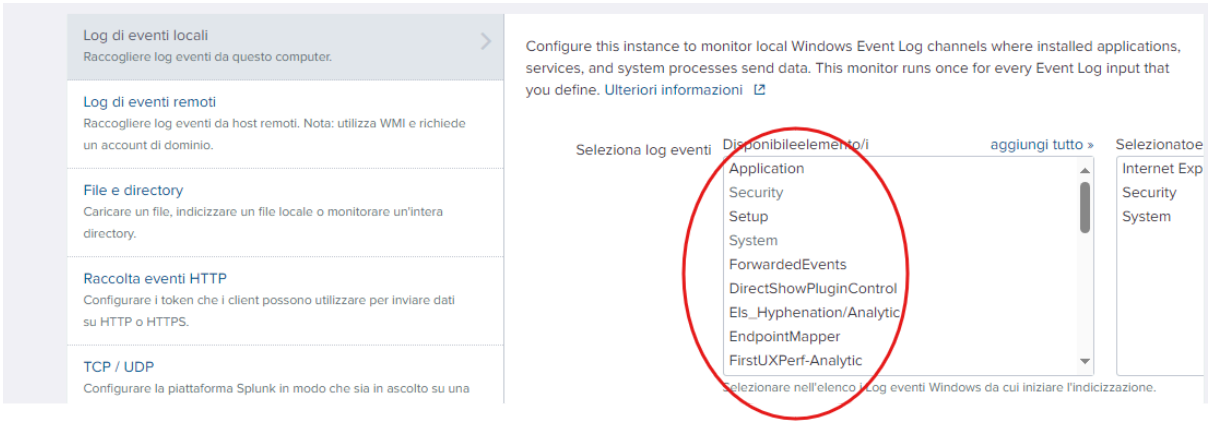
In breve: Lo studente dovrà configurare la modalità Monitora in Splunk e realizzare degli screenshot che ne mostrino l'esecuzione.

Svolgimento

Ho iniziato aprendo la dashboard di splunk tramite browser in localhost sulla porta 8000.

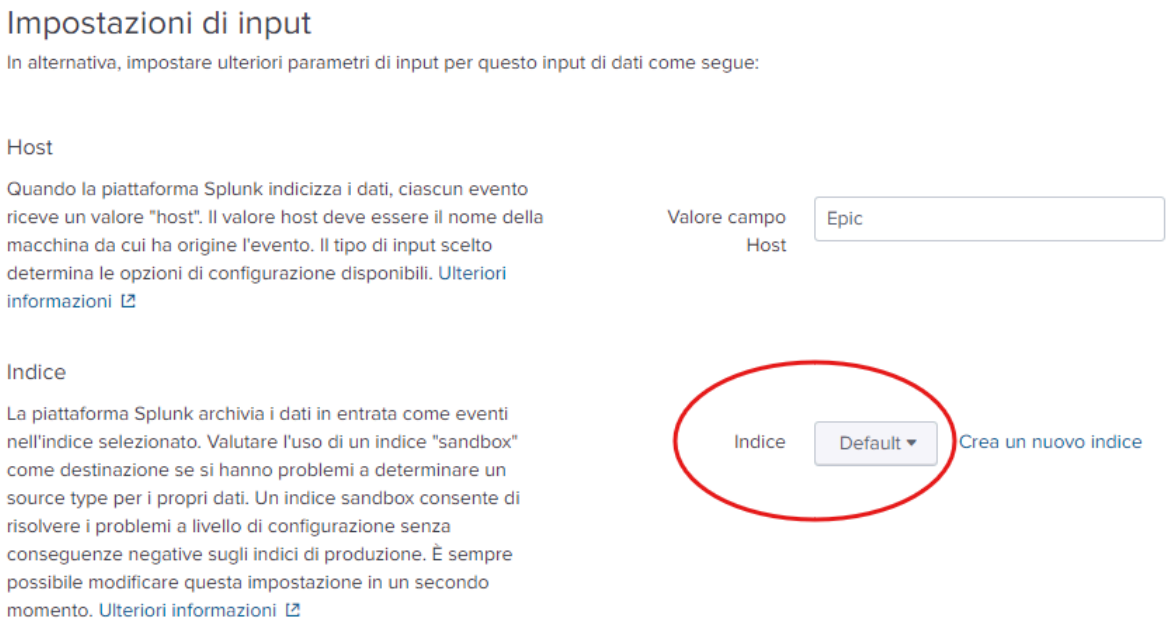
Una volta effettuato il login mi sono diretto verso la sezione per l'aggiunta di dati, data input, ed una volta proposti i metodi di integrazione dati, ho selezionato Monitora.

A seguire, ho deciso di procedere con l'integrazione dei log locali; ho quindi selezionato la sezione log di eventi locali ed ho optato per assimilare i log inerenti a Security, Application e System.



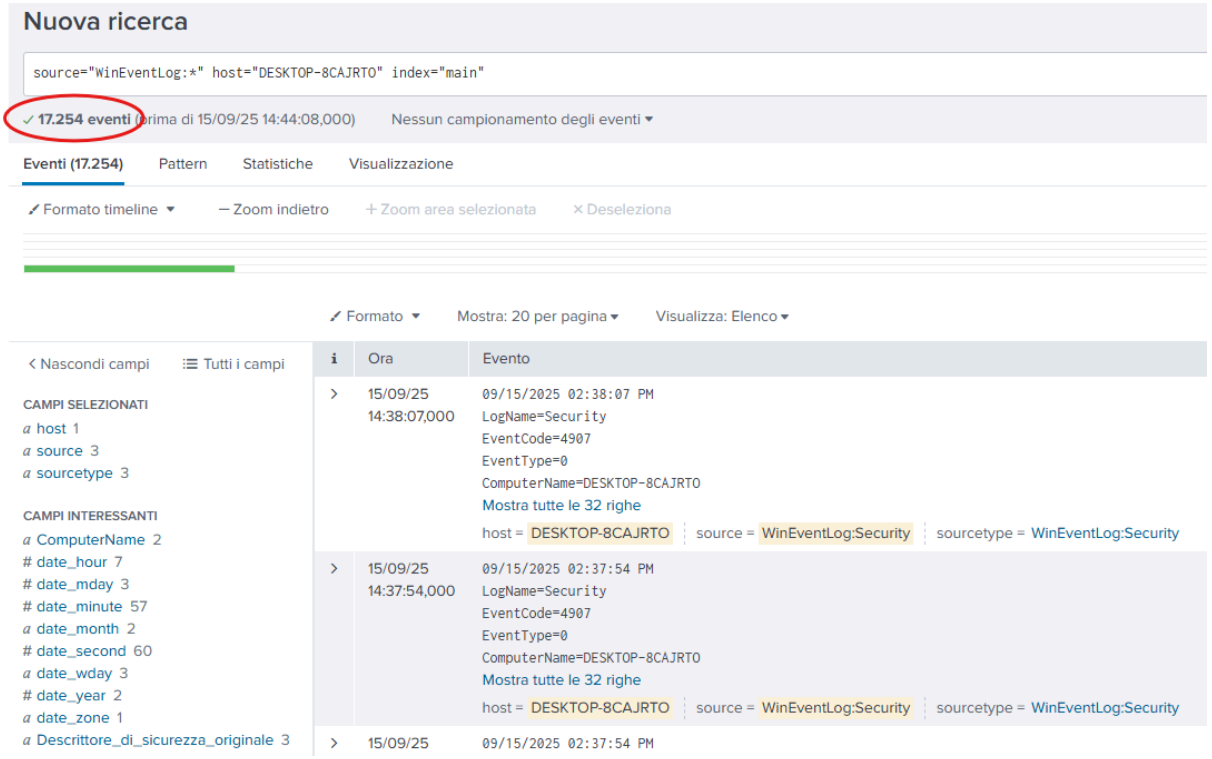
- Application
- Security
- System

A seguito della decisione ci viene chiesto in che indice li si voglia catalogare; per comodità ho lasciato le impostazioni di default in modo da poterli richiamare filtrando con index="main".



Una volta avviata la ricerca possiamo notare che SPLUNK ha integrato correttamente i log richiesti, tutti accuratamente elencati per timestamp.

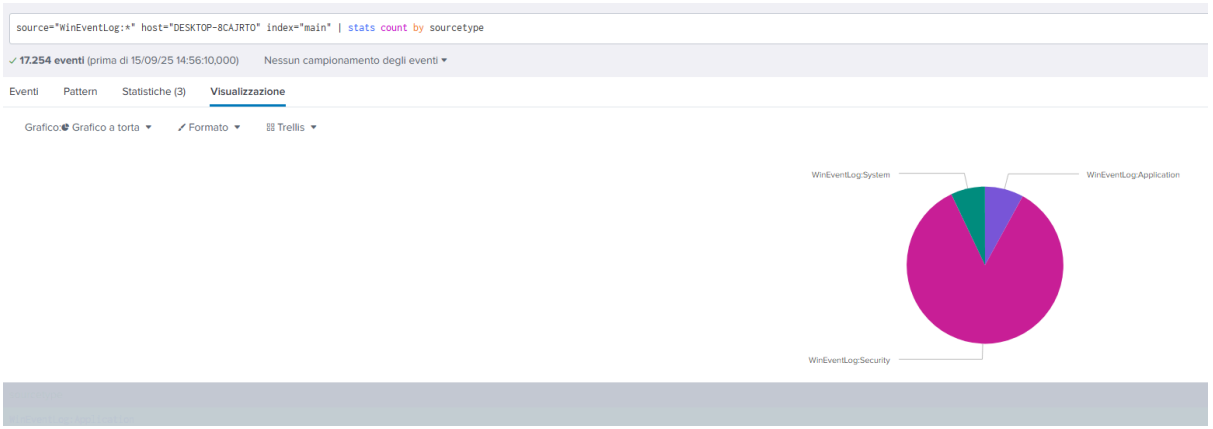
Possiamo osservare la presenza di 17254 eventi:



Possiamo poi trarre delle statistiche utilizzando la funzione stats.

In questo caso ho raggruppato gli eventi per sourcetype:

... | stats count by sourcetype



Questa query restituisce una tabella riepilogativa che può essere trasformata in un grafico (a barre o a torta) tramite la scheda Visualization.

Conclusioni

L'esercizio ha mostrato come configurare con successo la modalità **Monitora** di Splunk, selezionando log di sistema Windows, impostando l'host e l'indice, e verificando l'arrivo degli eventi in tempo reale.
Gli screenshot prodotti durante i vari passaggi (configurazione, ricerca e grafici) dimostrano l'avvenuta esecuzione e possono essere allegati come prova della configurazione.