

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.

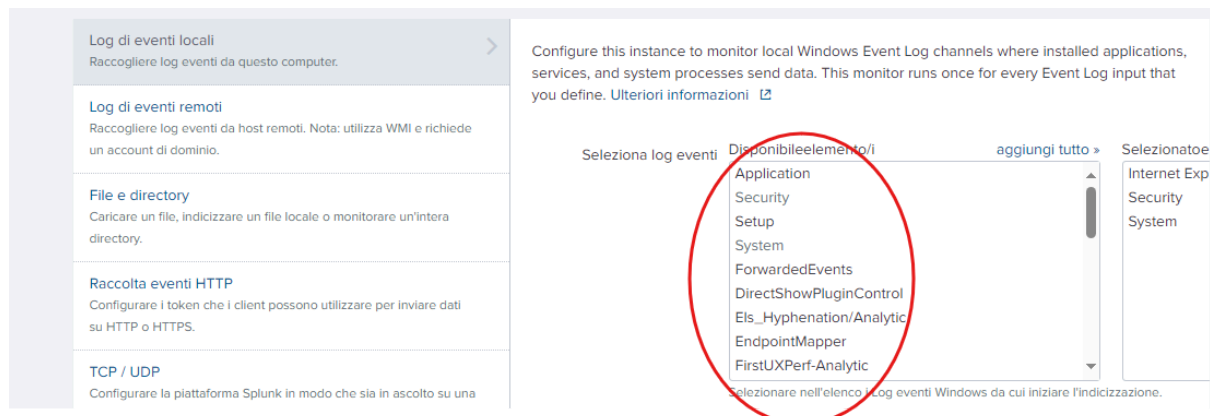
Svolgimento

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"**.

Impostazioni di input

In alternativa, impostare ulteriori parametri di input per questo input di dati come segue:

Host

Quando la piattaforma Splunk indicizza i dati, ciascun evento riceve un valore "host". Il valore host deve essere il nome della macchina da cui ha origine l'evento. Il tipo di input scelto determina le opzioni di configurazione disponibili. [Ulteriori informazioni](#)

Valore campo Host

Indice

La piattaforma Splunk archivia i dati in entrata come eventi nell'indice selezionato. Valutare l'uso di un indice "sandbox" come destinazione se si hanno problemi a determinare un source type per i propri dati. Un indice sandbox consente di risolvere i problemi a livello di configurazione senza conseguenze negative sugli indici di produzione. È sempre possibile modificare questa impostazione in un secondo momento. [Ulteriori informazioni](#)

Indice [Crea un nuovo indice](#)

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:

Nuova ricerca

source="WinEventLog:*" host="DESKTOP-8CAJRT0" index="main"

✓ **17.254 eventi** (prima di 15/09/25 14:44:08,000) Nessun campionamento degli eventi ▼

Eventi (17.254) Pattern Statistiche Visualizzazione

Formato timeline ▼ Zoom indietro Zoom area selezionata Deseleziona

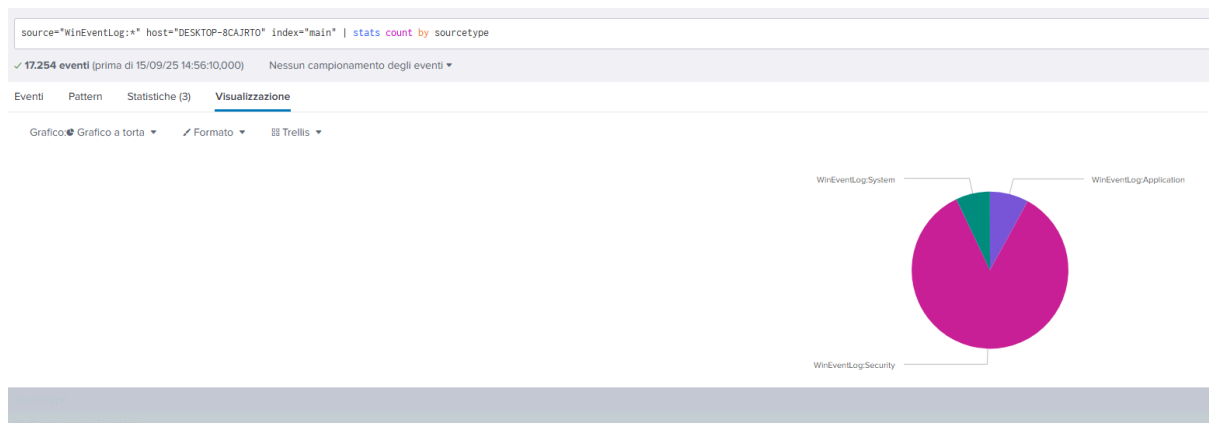
Formato ▼ Mostra: 20 per pagina ▼ Visualizza: Elenco ▼

| < Nascondi campi Tutti i campi | | i | Ora | Evento |
|--|--|---|--------------|--|
| CAMPI SELEZIONATI | | > | 15/09/25 | 09/15/2025 02:38:07 PM |
| a host 1 | | | 14:38:07,000 | LogName=Security |
| a source 3 | | | | EventCode=4907 |
| a sourcetype 3 | | | | EventType=0 |
| CAMPI INTERESSANTI | | | | ComputerName=DESKTOP-8CAJRT0 |
| a ComputerName 2 | | | | Mostra tutte le 32 righe |
| # date_hour 7 | | | | host = DESKTOP-8CAJRT0 source = WinEventLog:Security sourcetype = WinEventLog:Security |
| # date_mday 3 | | > | 15/09/25 | 09/15/2025 02:37:54 PM |
| # date_minute 57 | | | 14:37:54,000 | LogName=Security |
| a date_month 2 | | | | EventCode=4907 |
| # date_second 60 | | | | EventType=0 |
| a date_wday 3 | | | | ComputerName=DESKTOP-8CAJRT0 |
| # date_year 2 | | | | Mostra tutte le 32 righe |
| a date_zone 1 | | | | host = DESKTOP-8CAJRT0 source = WinEventLog:Security sourcetype = WinEventLog:Security |
| a Descrittore_di_sicurezza_originale 3 | | > | 15/09/25 | 09/15/2025 02:37:54 PM |

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.