S10L1

Splunk

L'obiettivo di oggi è configurare la modalità **"Monitor"** di Splunk, così da poter visualizzare in tempo reale i dati richiesti. Questa configurazione consentirà di acquisire, indicizzare e analizzare i log o i dati specificati non appena vengono generati, garantendo una visione immediata delle informazioni e facilitando il monitoraggio di eventi o anomalie.

Che cosa è Splunk?

Splunk è uno dei migliori SIEM disponibili sul mercato, riconosciuto per la sua straordinaria flessibilità e capacità di scalare in ambienti complessi. La sua potenza risiede nella capacità di adattarsi a diverse esigenze aziendali, offrendo una gestione efficace e scalabile dei dati in tempo reale, rendendolo una scelta ideale per organizzazioni di tutte le dimensioni.

Come funziona Splunk?

1. **Raccolta dei dati:** Splunk acquisisce dati provenienti da una vasta gamma di fonti, tra cui file di log, applicazioni, dispositivi di rete e API.
2. **Indicizzazione dei dati:** I dati raccolti vengono indicizzati, consentendo ricerche rapide ed efficienti. Questo passaggio è fondamentale per gestire grandi volumi di informazioni.
3. **Parsing:** Splunk analizza e trasforma i dati grezzi in un formato strutturato e utilizzabile. Questo processo consente di estrarre significati chiave dai dati in ingresso.
4. **Ricerca e analisi:** Gli utenti possono eseguire ricerche dettagliate sui dati indicizzati utilizzando query personalizzate. Splunk mette a disposizione un linguaggio di ricerca potente e intuitivo.
5. **Visualizzazione dei dati:** I risultati delle analisi possono essere rappresentati visivamente attraverso dashboard, grafici e report, rendendo le informazioni più comprensibili e utili per il processo decisionale.

Componenti principali di Splunk

- **Host:** Rappresenta il sistema o il dispositivo da cui provengono i dati raccolti.
  - **Esempio:** Un server web specifico, un router o un dispositivo di sicurezza.
- **Source:** È il percorso o la posizione esatta da cui Splunk raccoglie i dati. Può essere un file di log, una directory, un protocollo di rete o un comando eseguito.
  - **Esempio:** Un file di log come `/var/log/syslog`, un database o un URL di una API.
- **SourceType:** Indica il formato dei dati raccolti. Questa categorizzazione aiuta Splunk a applicare la logica di parsing corretta e a trattare i dati in modo adeguato.
  - **Esempio:** Formati come JSON, CSV, syslog o Apache access log.

Cos'è il parsing dei dati?

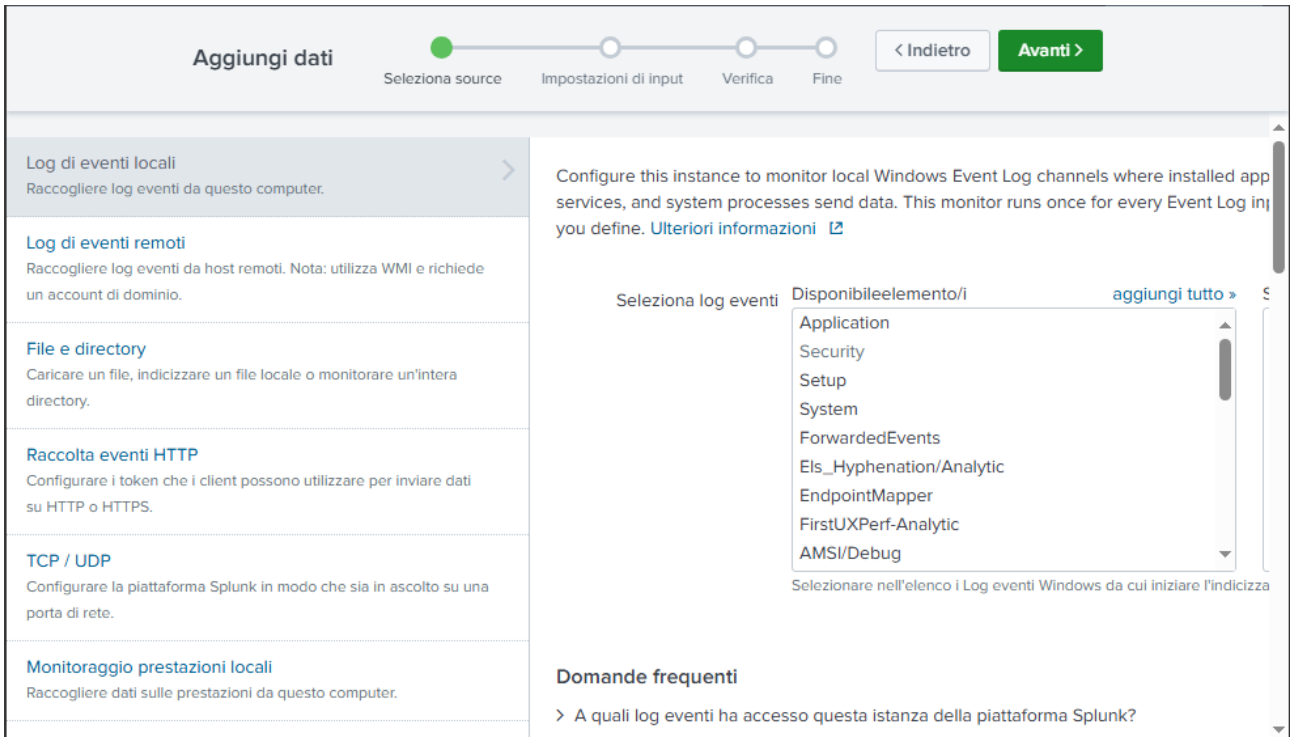
Il parsing è il processo di analisi dei dati grezzi acquisiti per trasformarli in informazioni strutturate e significative. Splunk utilizza il parsing per riconoscere e organizzare i dati in base alla loro origine, formato e contenuto, rendendoli facilmente consultabili e analizzabili.

Esercitazione pratica

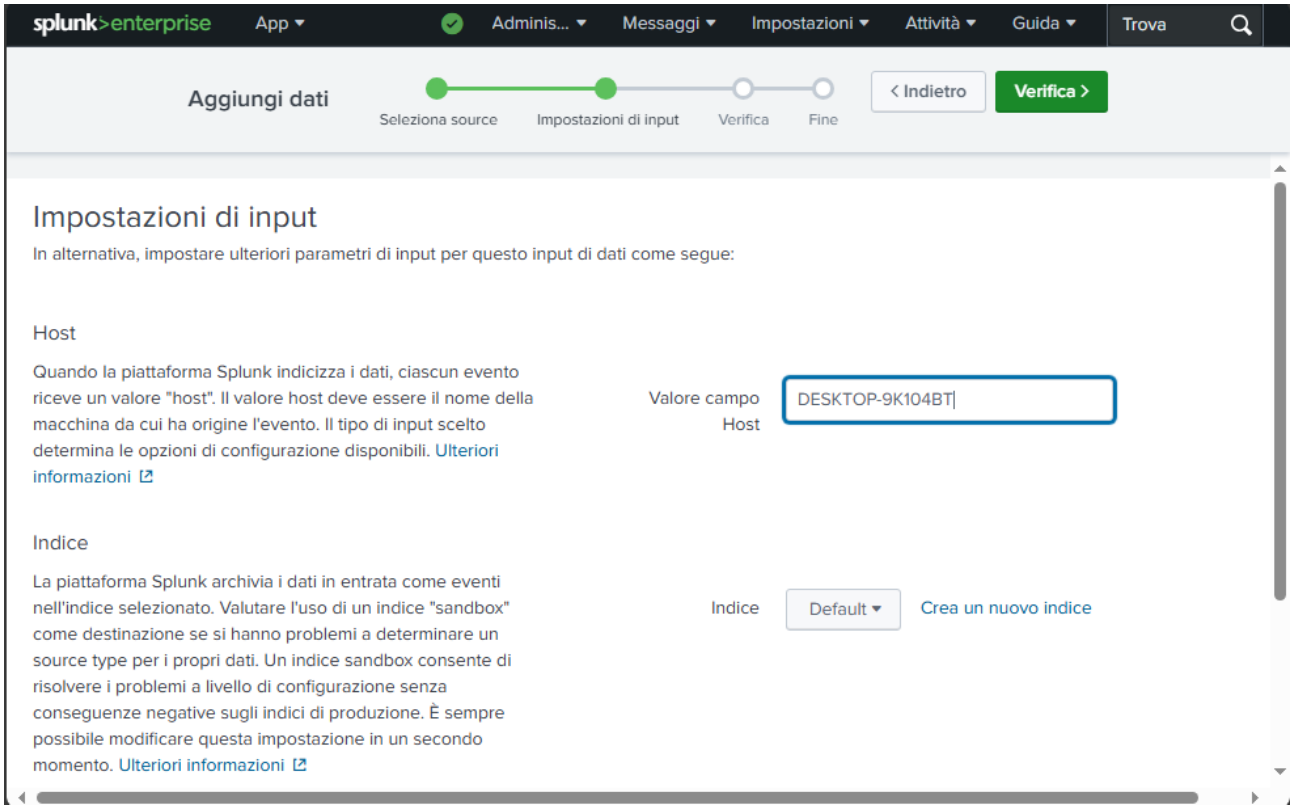
Per andare a configurare la modalità monitor bisogna seguire una serie di passaggi.

Passaggio 1
Andare nella sezione 'monitora' di splunk

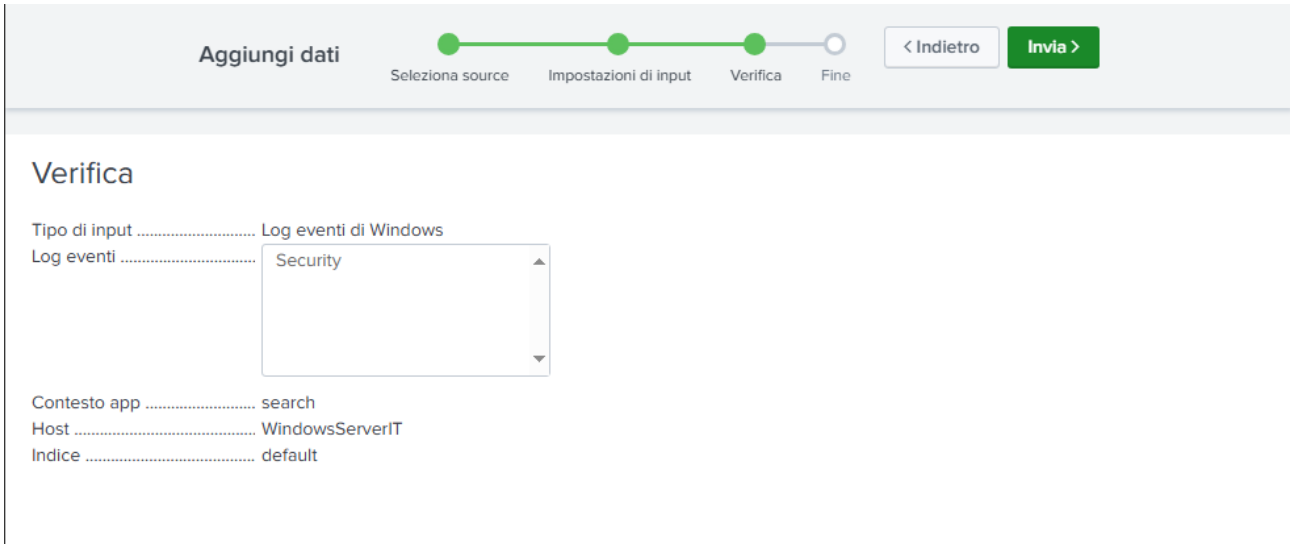
Passaggio 2
Successivamente nella sezione ‘log di eventi locali’ selezionare la voce ‘security’ dal menù a tendina sulla destra. Dopodiché procedere con il tasto **‘avanti’**



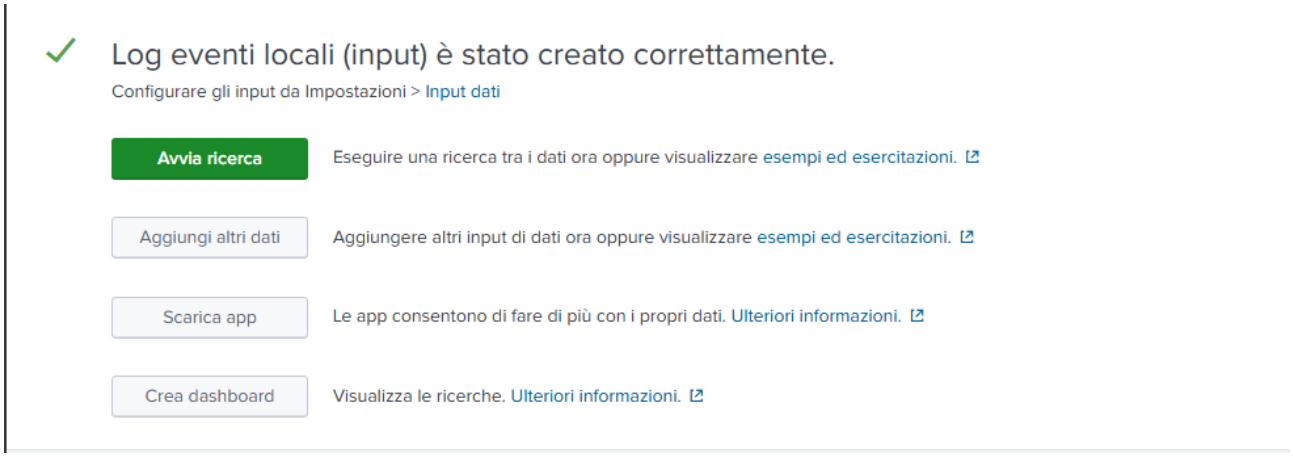
Passaggio 3
Come terzo passaggio bisogna selezionare l’host che decidiamo di tenere sotto controllo. Dopo aver dichiarato il nome dell’host pigiare sul tasto **‘verifica’**



Passaggio 4
Splunk come quarta schermata mostra un recap della richiesta che stiamo per attuare. Se tutto è continuare pigiando sul testo **'invia'**



Passaggio 5
L'ultima schermata mostra come la richiesta sia stata creata correttamente ora bisogna andare su **'avvia ricerca'.**



Fase di monitoraggio
Ora saremo in grado di monitorare tutti i dati richiesti e, grazie all'uso di query personalizzate, potremo definire con precisione la quantità e il tipo di informazioni da visualizzare, rendendo l'analisi dei dati più mirata ed efficace.