

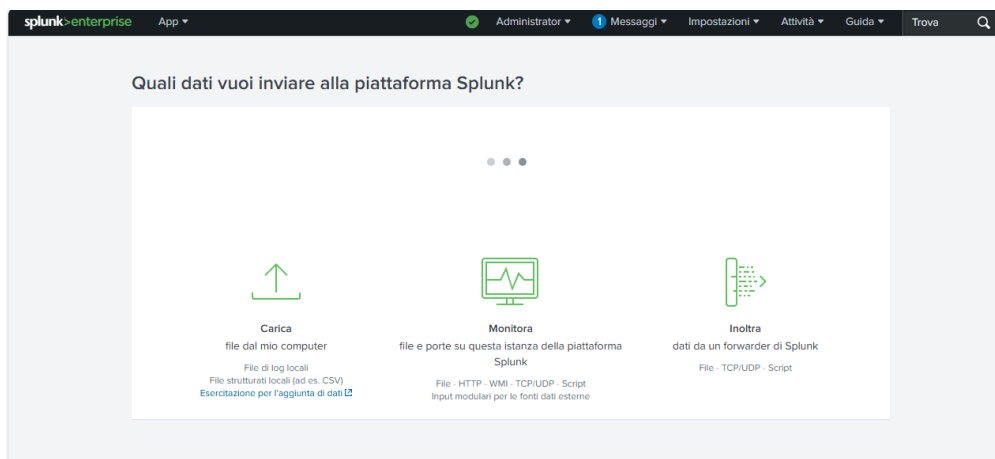
Esercizio.

Obiettivo: configurare la modalità monitora su Splunk e recuperare screen dell'avvenuta configurazione.

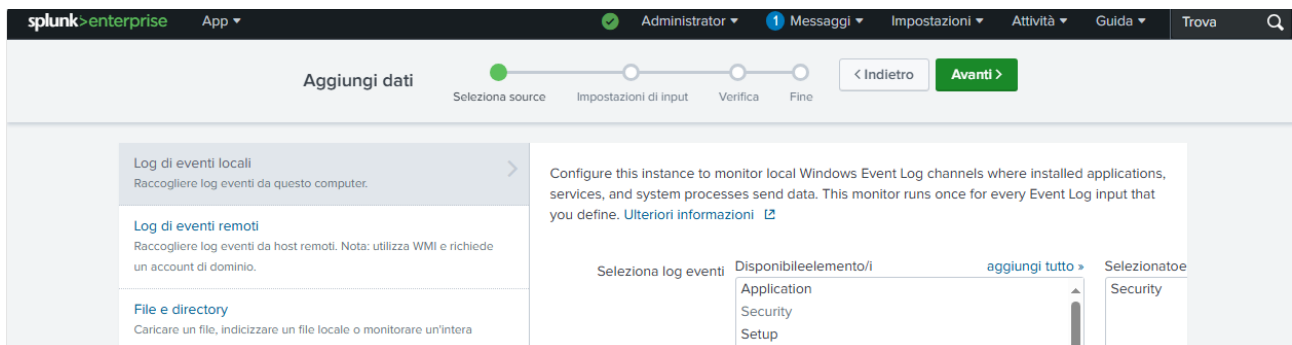
Apri e accedi Splunk Enterprise e clicco su aggiungi dati



Vado su monitora:



clicco su log ed eventi locali scelgo come impostazione: Security e clicco su avanti:



Imposto come valore campo host: DESKTOP-8CAJRTO

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

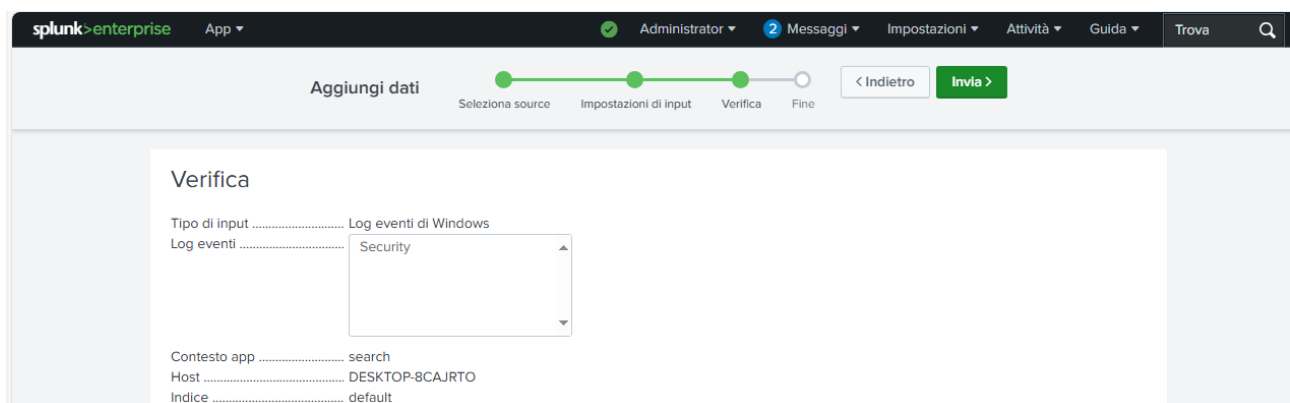
La piattaforma Splunk archivia i dati in entrata come eventi nell'indice selezionato. Valutare l'uso di un indice "sandbox" come destinazione se si hanno problemi a determinare un

Indice

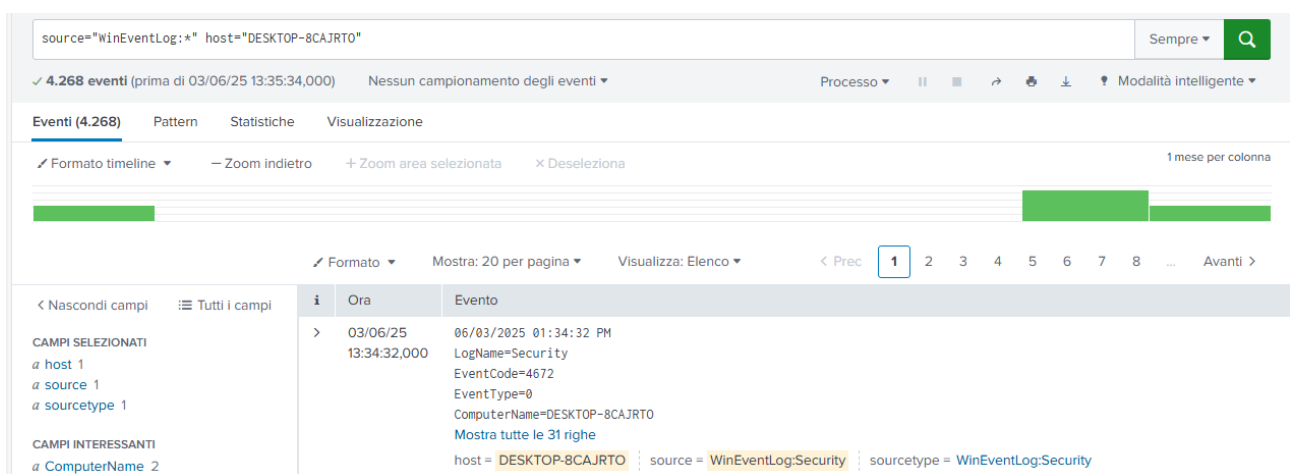
Default ▾

[Crea un nuovo indice](#)

Clicco su verifica → invia



Clicco su avvia la ricerca



Ora posso vedere tutti gli eventi che sono avvenuti e che avverranno sul pc DESKTOP-8CAJRTO.