S10-L1

Configurazione modalità Monitora in Splunk

Introduzione

In questa esercitazione ho configurato Splunk utilizzando la **modalità Monitora (Monitor) per acquisire eventi da un file di log locale.**
L'obiettivo è dimostrare la **corretta configurazione dell'ingestione dati e verificare che gli eventi vengano indicizzati e visualizzati correttamente nella sezione Search.**

---

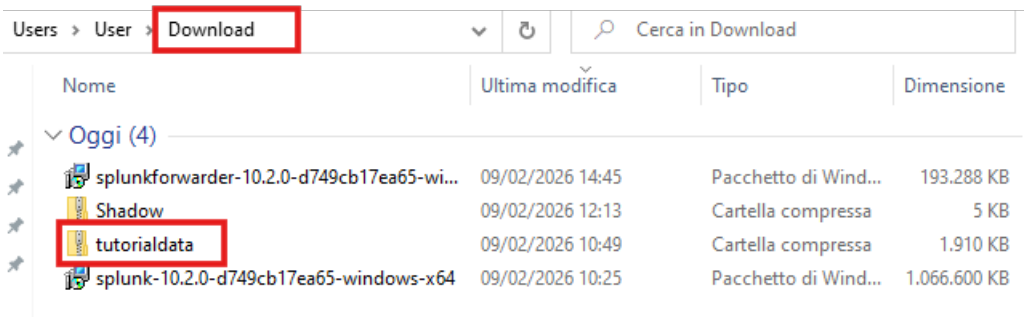
0) Installazione e primo accesso a Splunk

Download del pacchetto

Ho scaricato il pacchetto di installazione di **Splunk Enterprise per Windows (x64)** dalla sezione Download.

Nel percorso `Users > User > Download` è visibile:

- **La cartella compressa `tutorialdata`** (che utilizzerò successivamente per le esercitazioni)



Cartella Download con pacchetto Splunk e tutorialdata evidenziati.

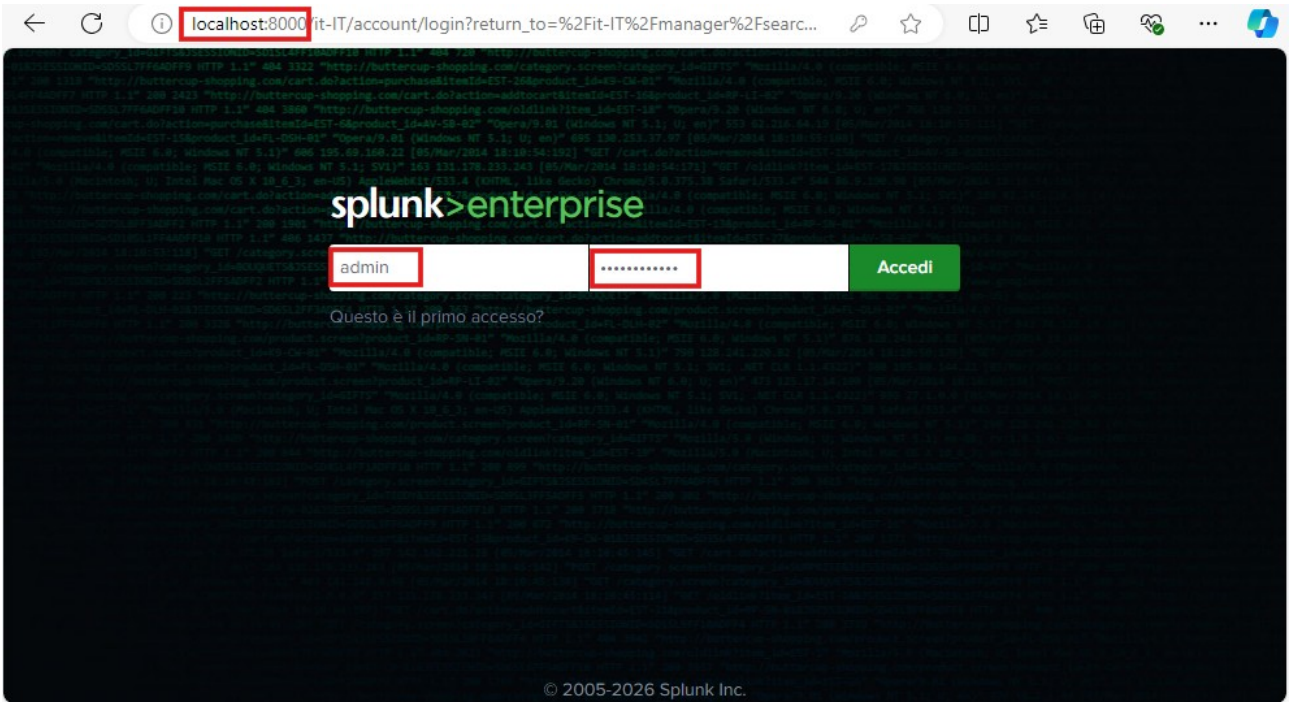
Installazione e avvio

Dopo aver completato l'installazione:

1. Ho avviato Splunk Enterprise.
2. Ho verificato che il servizio fosse in esecuzione.
3. Ho aperto il browser e digitato:

`http://localhost:8000`

Come mostrato nello screenshot a seguire, l'interfaccia web di Splunk è correttamente raggiungibile all'indirizzo **localhost:8000**.



---

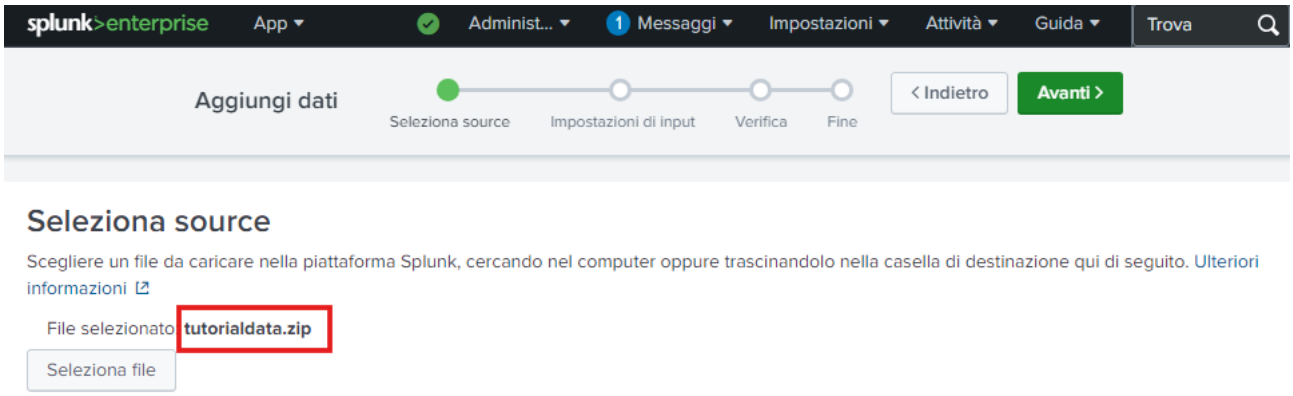
1) Caricamento del file tutorialdata.zip e configurazione input

Selezione della source:

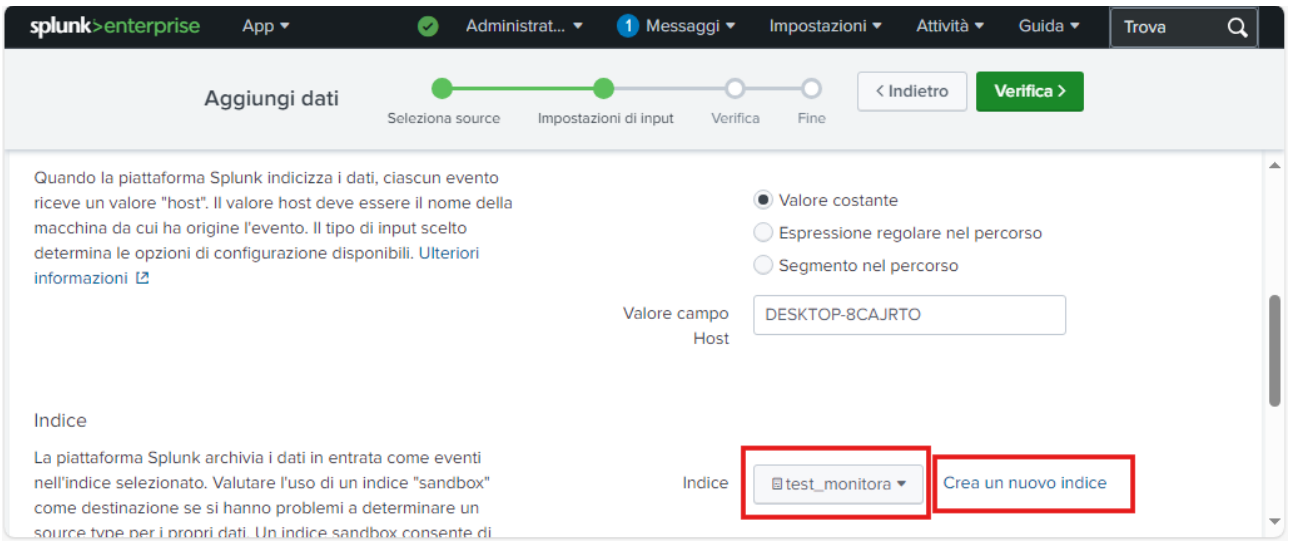
Dalla dashboard di Splunk ho selezionato **Aggiungi dati**.

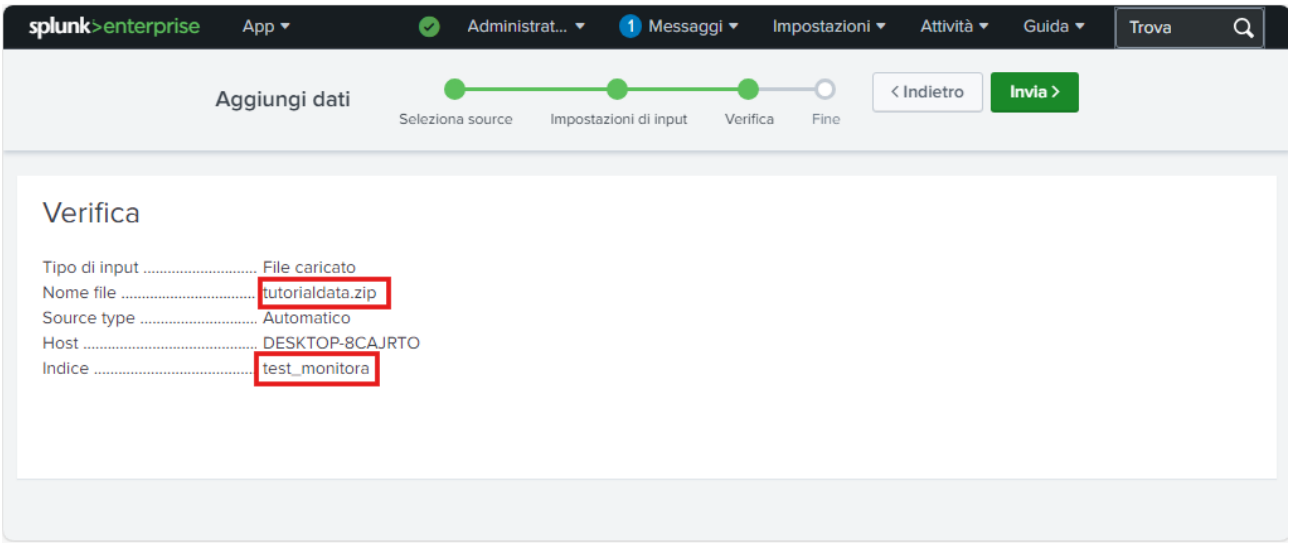
Nella schermata **Seleziona source** ho scelto di caricare un file dal mio computer e ho selezionato:

`tutorialdata.zip`

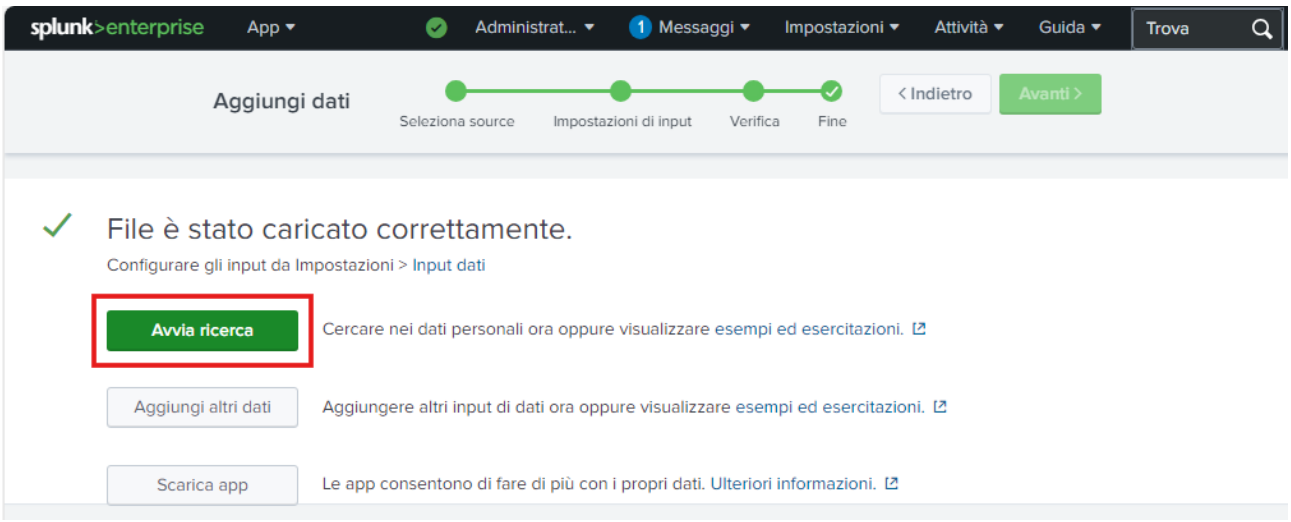


Ho creato un nuovo indice e selezionato Indice: **test_monitora**





Come visibile nello screenshot, il file selezionato è correttamente indicato nella sezione “**Verifica**”.



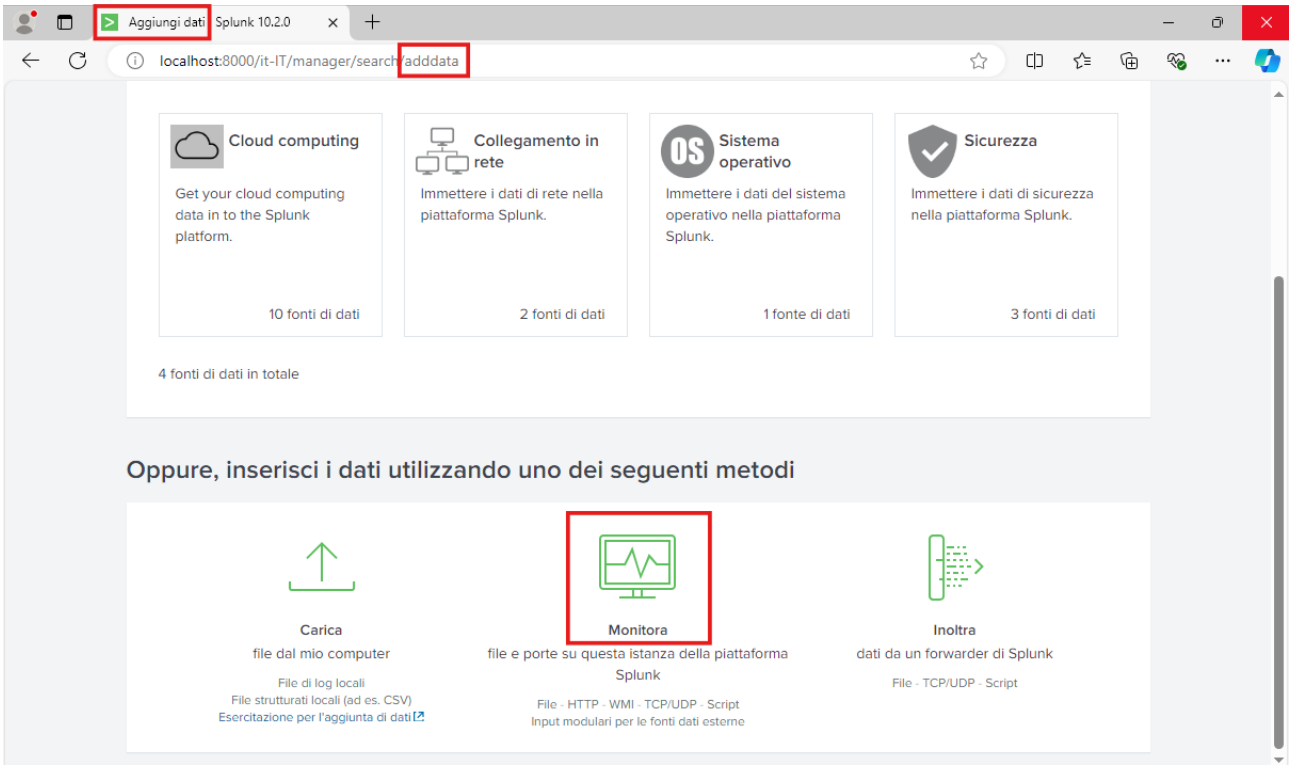
2) Configurazione della modalità “Monitora” in Splunk

---

2) Accesso alla modalità Monitora

Dalla schermata principale di Splunk ho cliccato su **Aggiungi dati (Add Data)**.

Successivamente ho selezionato l’opzione **Monitora (Monitor)**, che consente di acquisire dati in tempo reale da file o directory presenti nel sistema.



Output schermata “Aggiungi dati” con opzione **Monitora** selezionata.

Dalla schermata **Aggiungi dati** ho selezionato l’opzione **Monitora**, che consente di acquisire dati in tempo reale da file, directory o porte locali della piattaforma Splunk.

Questa modalità permette di configurare il monitoraggio continuo delle fonti dati presenti sul sistema.

---

3) Selezione della fonte da monitorare

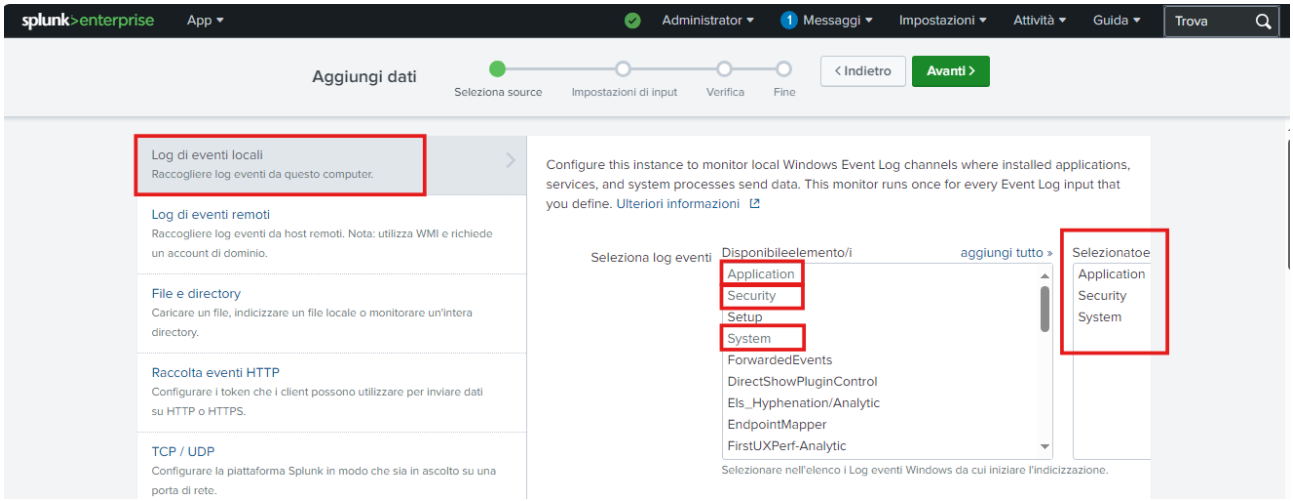
Ho selezionato l'opzione **Log di eventi locali** nella schermata di configurazione della modalità Monitora.

Questa opzione consente di acquisire direttamente i registri eventi del sistema operativo Windows, come:

- Security
- Application
- System

Ho scelto di monitorare il registro **Security**, in quanto **contiene eventi relativi ad accessi, autenticazioni e attività di sicurezza del sistema.**

In questo modo Splunk acquisisce in tempo reale gli eventi generati dal sistema operativo, indicizzandoli automaticamente nell'indice configurato.



Output "Log di eventi locali" con registri selezionati.

---

4) Configurazione dell'indice e completamento della modalità Monitora

Ho proceduto alla configurazione dei parametri di indicizzazione.

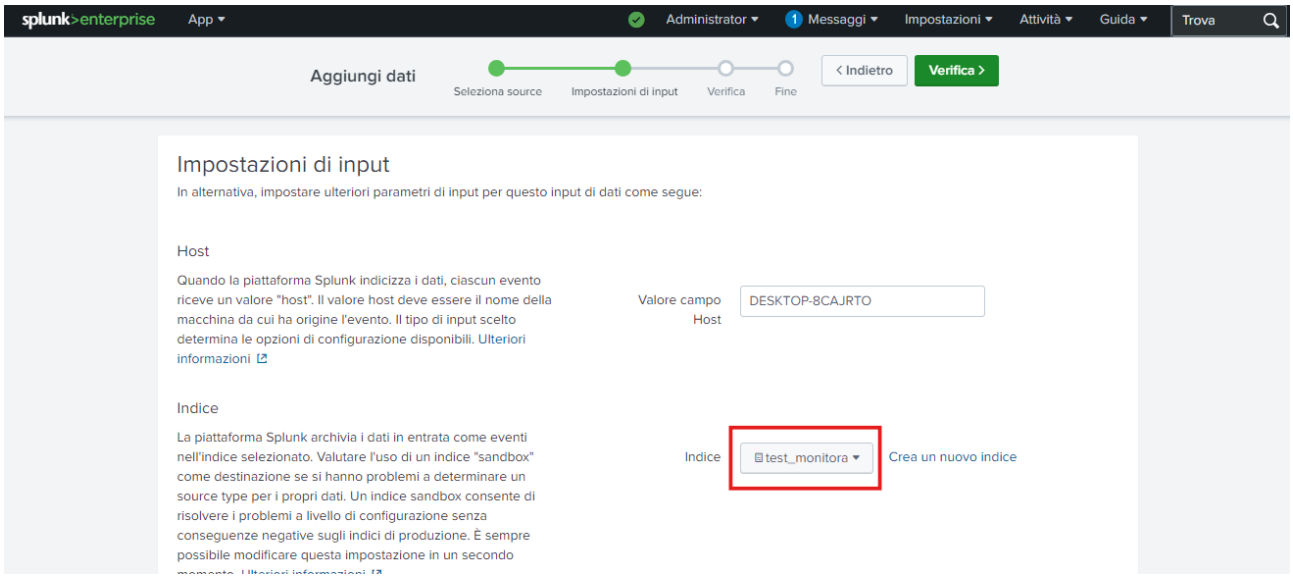
Nella schermata **Impostazioni di input**:

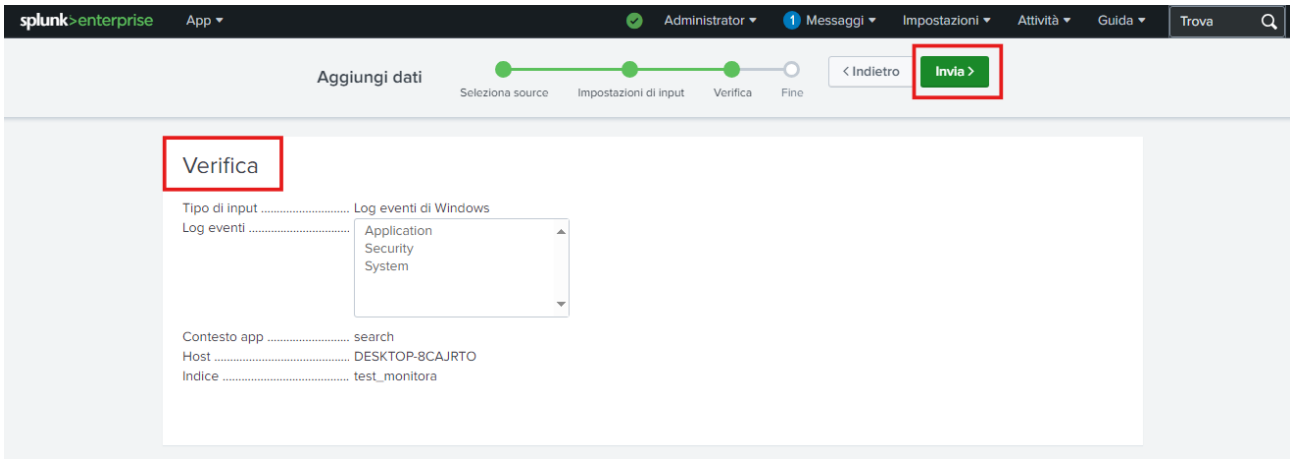
- Ho lasciato il valore **Host** impostato automaticamente (nome della macchina locale).
- Ho selezionato come **Indice**:

`test_monitora`

Ho verificato che il tipo di input fosse relativo al registro eventi di Windows e ho cliccato su **Verifica**, controllando la correttezza dei parametri configurati.

Successivamente ho cliccato su **Invia per completare la configurazione della modalità Monitora.**





Output schermata di configurazione con registri selezionati e indice `test_monitora`.

Conferma configurazione

Nella schermata di riepilogo ho controllato:

- Tipo di input: Monitoraggio file/directory
- Percorso configurato
- Host

- Indice test_monitora

Ho quindi cliccato su **Invia** per completare la configurazione.

---

5) Verifica del corretto funzionamento della modalità Monitora

Dopo aver completato la configurazione, ho verificato l'effettiva acquisizione degli eventi accedendo alla sezione **Search & Reporting**.

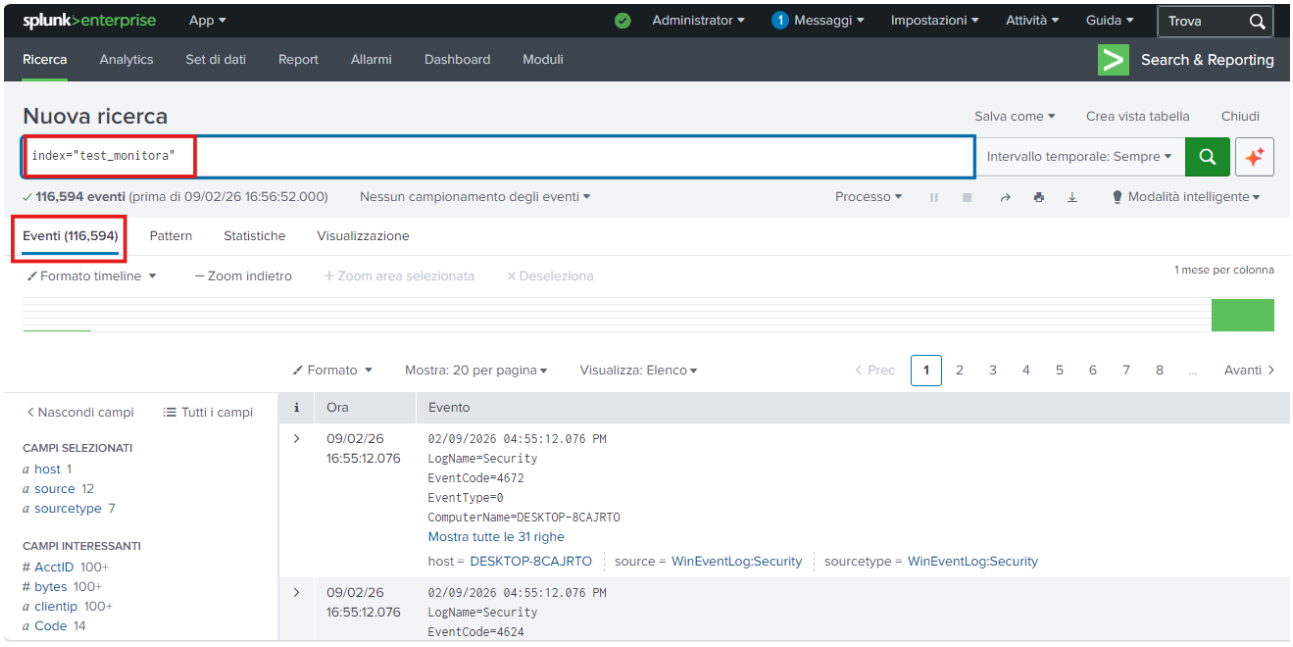
Ho eseguito la seguente query:

```
index="test_monitora"
```

Tra i risultati sono visibili eventi con:

- sourcetype = **WinEventLog:Security**
- **EventCode relativi ad attività di sicurezza** (es. 4624, 4672)
- Host = **DESKTOP-8CAJRTO**

La presenza degli eventi conferma che la modalità **Monitora** è stata configurata correttamente e che Splunk sta acquisendo i log in tempo reale.



La ricerca ha restituito oltre 116.000 eventi, provenienti dai registri locali di Windows.

Conclusioni:

Attraverso la modalità Monitora, **ho configurato correttamente l’acquisizione dei Log di eventi locali di Windows in Splunk**.

Ho verificato che:

- **I registri Application, Security e System vengono monitorati in tempo reale.**
- **Gli eventi vengono indicizzati correttamente nell’indice configurato.**
- **I dati risultano correttamente ricercabili nella sezione Search & Reporting.**

L’obiettivo dimostra la comprensione del processo di configurazione, indicizzazione e verifica dell’acquisizione dati tramite modalità Monitora in Splunk.