

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)

Users > User > Download	▼	🔄	🔍 Cerca in Download
Nome	Ultima modifica	Tipo	Dimensione
▼ Oggi (4)			
splunkforwarder-10.2.0-d749cb17ea65-wi...	09/02/2026 14:45	Pacchetto di Wind...	193.288 KB
Shadow	09/02/2026 12:13	Cartella compressa	5 KB
tutorialdata	09/02/2026 10:49	Cartella compressa	1.910 KB
splunk-10.2.0-d749cb17ea65-windows-x64	09/02/2026 10:25	Pacchetto di Wind...	1.066.600 KB

Cartella Download con pacchetto Splunk e tutorialdata evidenziati.

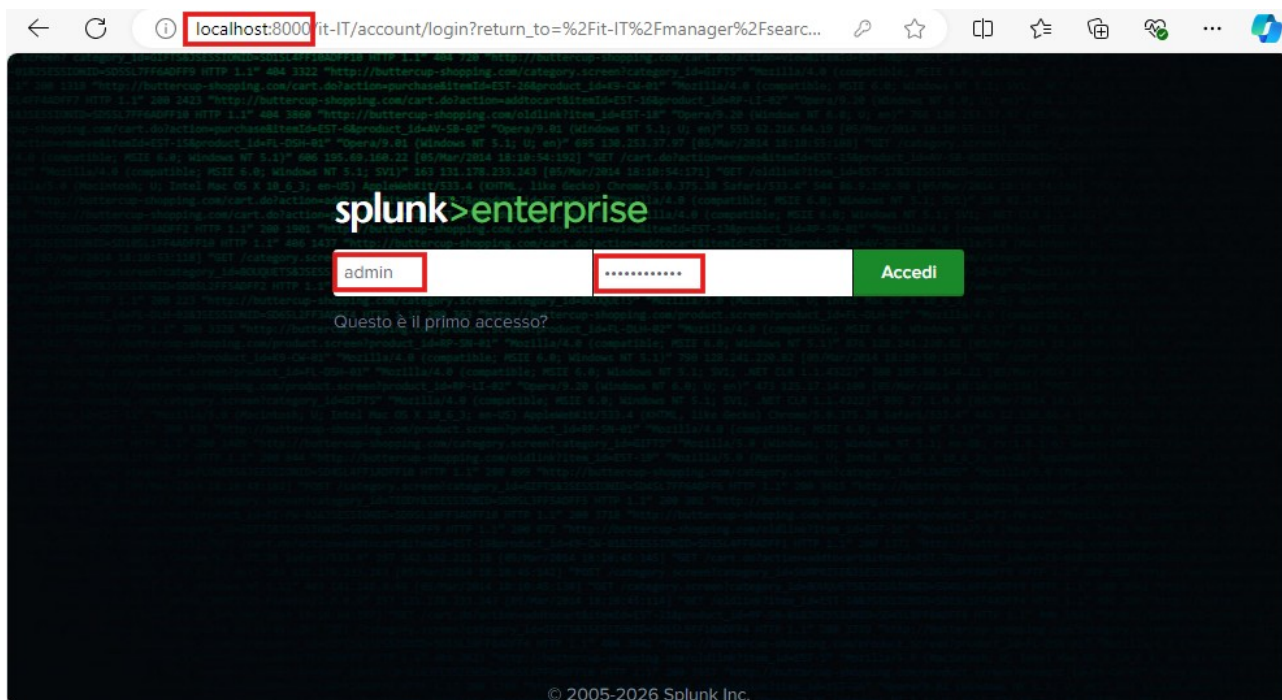
Installazione e avvio

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`

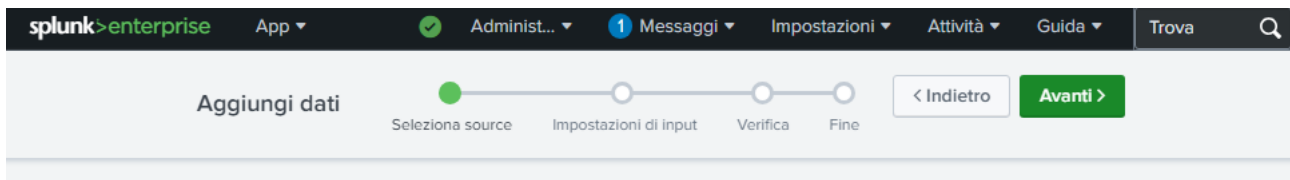
Come mostrato nello screenshot a seguire, l'interfaccia web di Splunk è correttamente raggiungibile all'indirizzo **localhost:8000**.



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**



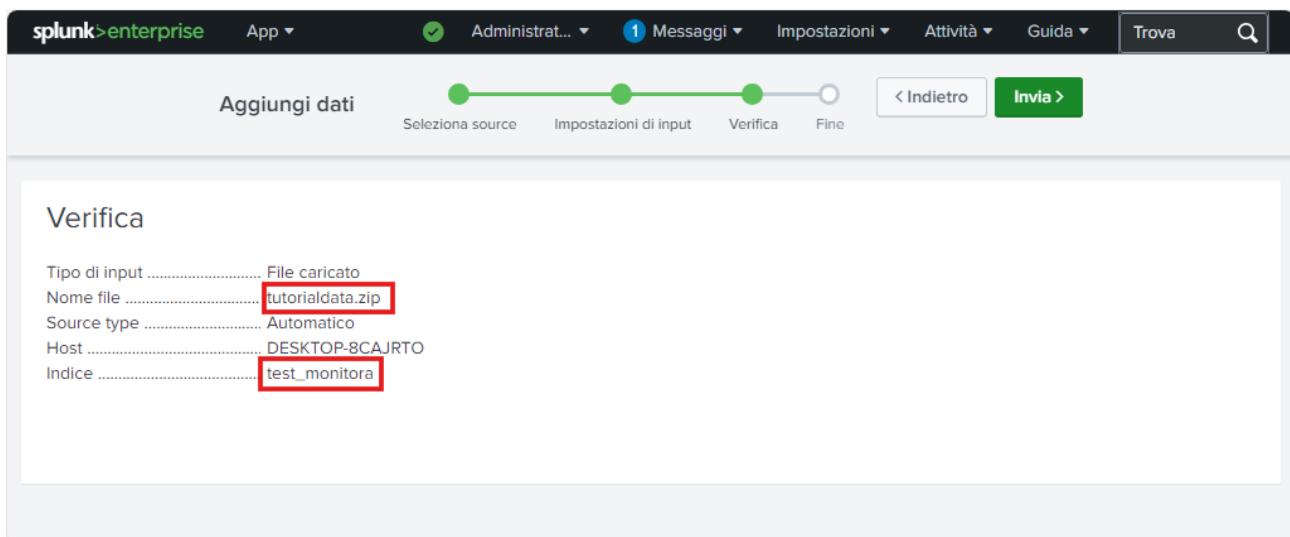
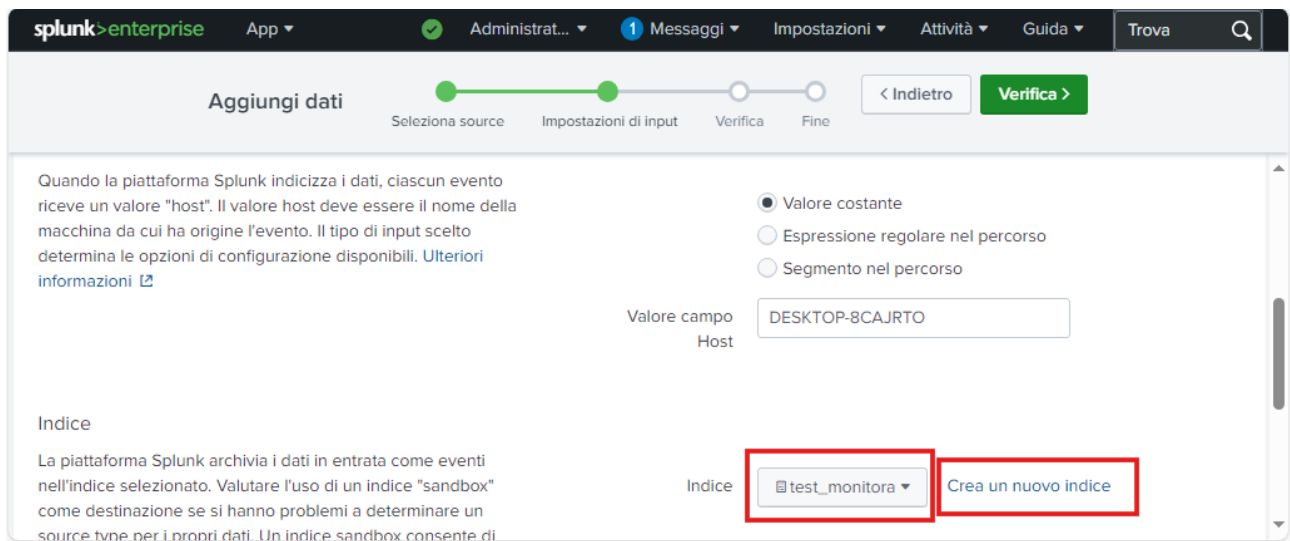
Seleziona source

Scegliere un file da caricare nella piattaforma Splunk, cercando nel computer oppure trascinandolo nella casella di destinazione qui di seguito. [Ulteriori informazioni](#)

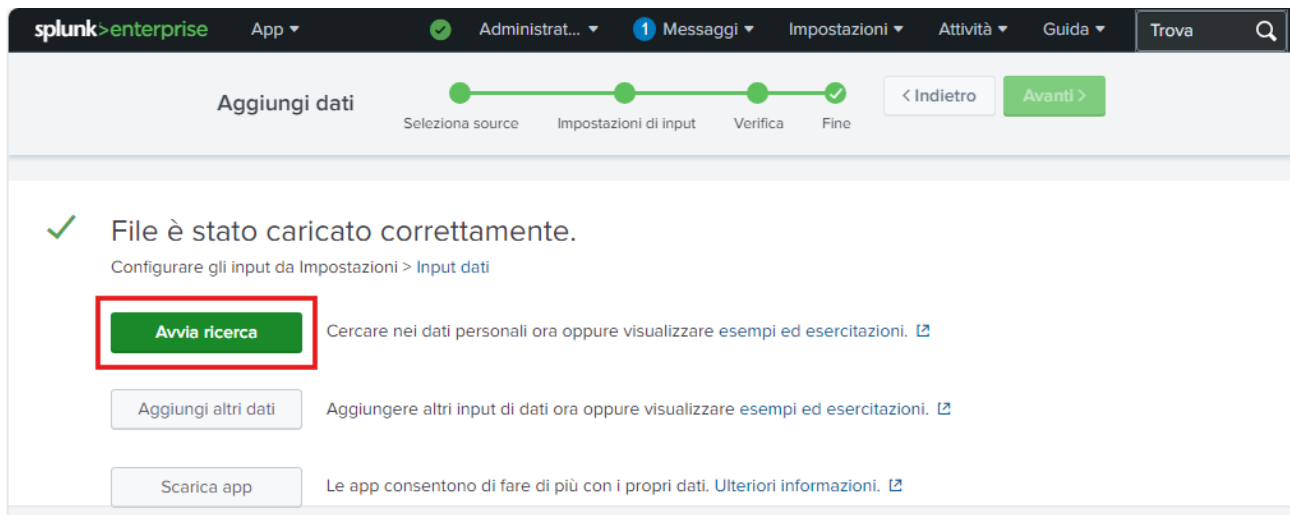
File selezionato **tutorialdata.zip**

Seleziona file

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



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

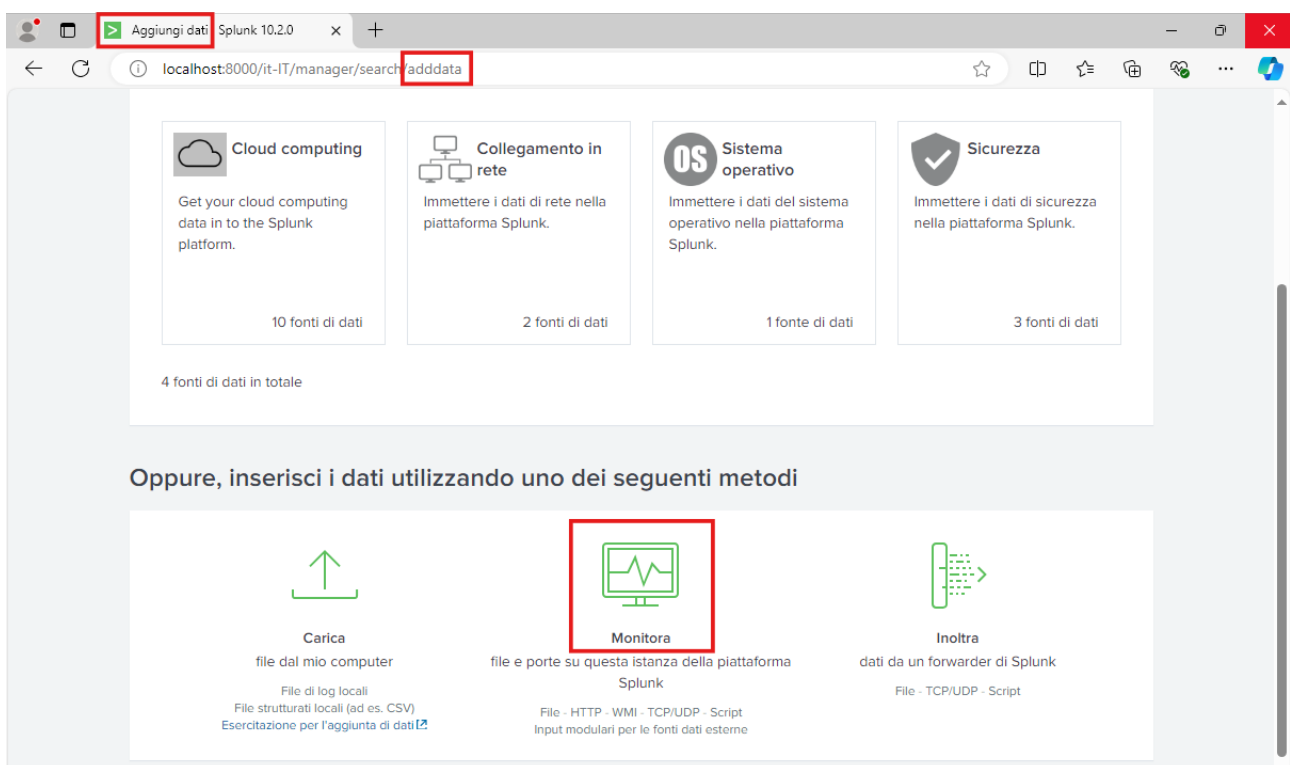


2) Configurazione della modalità “Monitora” in Splunk

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

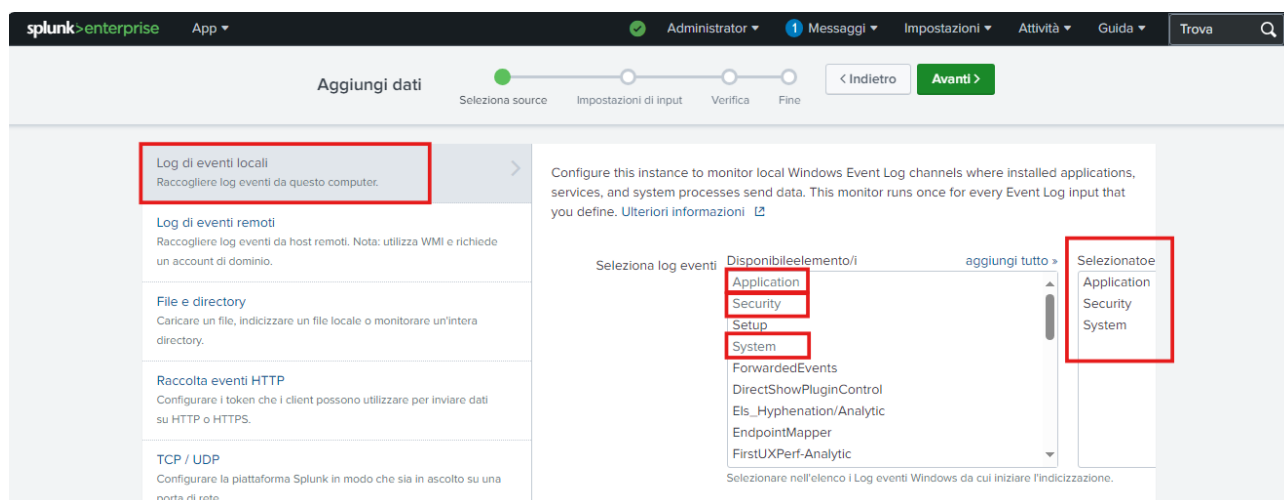
Ho selezionato l'opzione **Log di eventi locali** nella schermata di configurazione della modalità Monitora.

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**.

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: test_monitora [Crea un nuovo indice](#)

Verifica

Verifica

Tipo di input Log eventi di Windows

Log eventi Application
Security
System

Contesto app search

Host DESKTOP-8CAJRTO

Indice test_monitora

Invia

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.

The screenshot shows the Splunk Search & Reporting interface. At the top, the search bar contains the query `index="test_monitora"`. Below the search bar, it indicates that 116,594 events were found. The interface shows a list of events with columns for time, source, and event details. The first event is from 09/02/26 at 16:55:12.076, with LogName=Security, EventCode=4672, and ComputerName=DESKTOP-8CAJRTO. The second event is from 09/02/26 at 16:55:12.076, with LogName=Security and EventCode=4624. The interface also shows a sidebar with filters for host, source, and sourcetype.

i	Ora	Evento
>	09/02/26 16:55:12.076	02/09/2026 04:55:12.076 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-8CAJRTO Mostra tutte le 31 righe host = DESKTOP-8CAJRTO source = WinEventLog:Security sourcetype = WinEventLog:Security
>	09/02/26 16:55:12.076	02/09/2026 04:55:12.076 PM LogName=Security EventCode=4624

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.