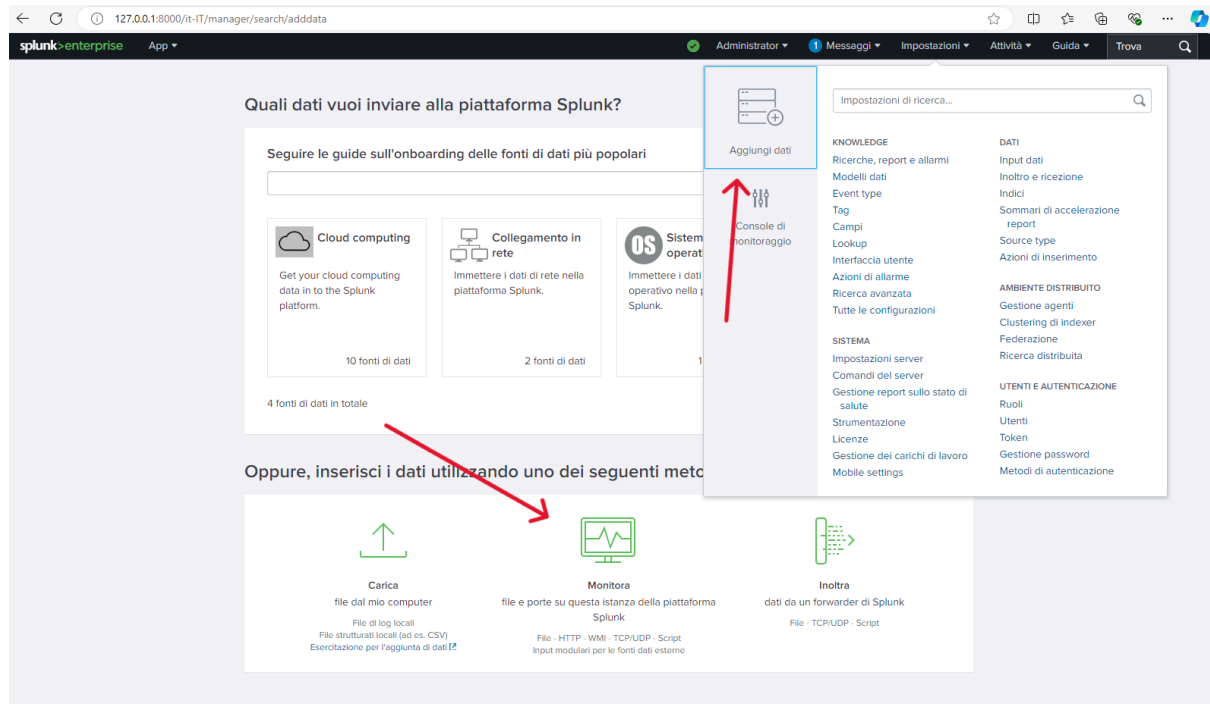


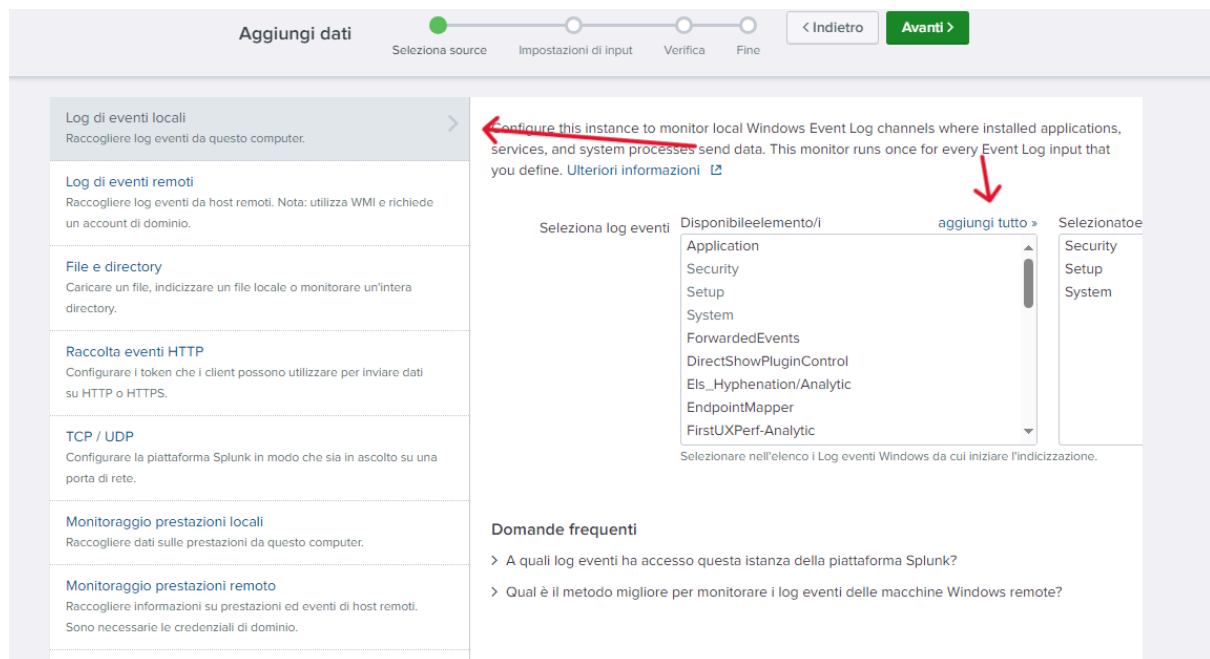
## UNIT3 S10/L1 - Modalità Monitora in Splunk

Il compito di oggi consiste nel configurare la modalità Monitora in Splunk e realizzare degli screenshot che confermino l'avvenuta configurazione.

Una volta eseguito l'accesso su splunk



si clicca dal menù a tendina "impostazioni" → "aggiungi dati" → "monitora"



si sceglie quali log inserire (in questo caso solo event log locali) selezionando tutti gli eventi.

**Aggiungi dati**

Seleziona source   Impostazioni di input   Verifica   Fine


< Indietro   **Verifica >**

### 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](#)

**Domande frequenti**

- > Come funzionano gli indici?
- > Come faccio a sapere quando creare o utilizzare più indici?

si deve definire nel “valore campo host” il nome del pc (in questo caso SPLUNK-Server)

**Aggiungi dati**

Seleziona source   Impostazioni di input   Verifica   Fine

< Indietro   **Invia >**

### Verifica

Tipo di input ..... Log eventi di Windows

Log eventi .....

Contesto app ..... search

Host ..... SPLUNK-Server

Indice ..... default

finestra di verifica prima dell'avvio della ricerca

Aggiungi dati

< Indietro

Avanti >

✓

Log eventi locali (input) è stato creato correttamente.

Configurare gli input da Impostazioni > Input dati

Avvia ricerca

Eseguire una ricerca tra i dati ora oppure visualizzare esempi ed esercitazioni. [↗](#)

Aggiungi altri dati

Aggiungere altri input di dati ora oppure visualizzare esempi ed esercitazioni. [↗](#)

Scarica app

Le app consentono di fare di più con i propri dati. Ulteriori informazioni. [↗](#)

Crea dashboard

Visualizza le ricerche. Ulteriori informazioni. [↗](#)

clickare sul tasto verde per far partire la ricerca

Nuova ricerca

Salva come ▾ Crea vista tabella Chiudi

source="WinEventLog:\*" host="SPLUNK-Server"

Intervallo temporale: Sempre 🔍

✓ 22.458 eventi (prima di 24/11/25 14:15:59,000) Nessun campionamento degli eventi ▾

Processo ▾ ⏏ 🔄 📄 📌 Modalità intelligente ▾

Eventi (22.458) Pattern Statistiche Visualizzazione

✓ Formato timeline ▾ — Zoom indietro + Zoom area selezionata × Deselezione

1 mese per colonna

< Nascondi campi ⌵ Tutti i campi

CAMPI SELEZIONATI  
# host 1  
# source 5  
# sourcetype 5

CAMPI INTERESSANTI  
# ComputerName 3  
# date\_hour 9  
# date\_mday 2  
# date\_minute 56  
# date\_month 2  
# date\_second 60  
# date\_wday 2  
# date\_year 2  
# date\_zone 1  
# Descrittore\_di\_sicurezza\_originale 3  
# Domain\_account 9  
# EventCode 100+  
# EventType 5  
# ID\_accesso 100+  
# ID\_handle 100+  
# ID\_processo 100+  
# ID\_sicurezza 38  
# Index 1  
# Keywords 9  
# linecount 34  
# LogName 5  
# Message 100+  
# Name\_account 31  
# Nome\_oggetto 100+  
# Nome\_processo 20  
# Nuovo\_descrittore\_di\_sicurezza 5

sourcetype

5 Valori, 100% di eventi

Selezionato Si No

Report

Primi valori Primi valori nel tempo Valori rari

Eventi con questo campo

Valori

	Conteggio	%
WinEventLog:Security	19,383	85,952%
WinEventLog:Application	2,881	9,266%
WinEventLog:System	1,849	4,671%
WinEventLog:Setup	18	0,08%
WinEventLog:Windows PowerShell	7	0,031%

Mostra tutte le 15 righe

host = SPLUNK-Server | source = WinEventLog:System | sourcetype = WinEventLog:System

> 24/11/25 11/24/2025 02:09:50.360 PM LogName=Security EventCode=4672 EventType=0 ComputerName=SPLUNK-Server Mostra tutte le 31 righe host = SPLUNK-Server | source = WinEventLog:Security | sourcetype = WinEventLog:Security

> 24/11/25 11/24/2025 02:09:50.360 PM LogName=Security EventCode=4624 EventType=0 ComputerName=SPLUNK-Server Mostra tutte le 70 righe host = SPLUNK-Server | source = WinEventLog:Security | sourcetype = WinEventLog:Security

> 24/11/25 11/24/2025 02:07:50.716 PM

abbiamo come output l'intera lista di log con la possibilità di filtrare in base al campo che preferiamo