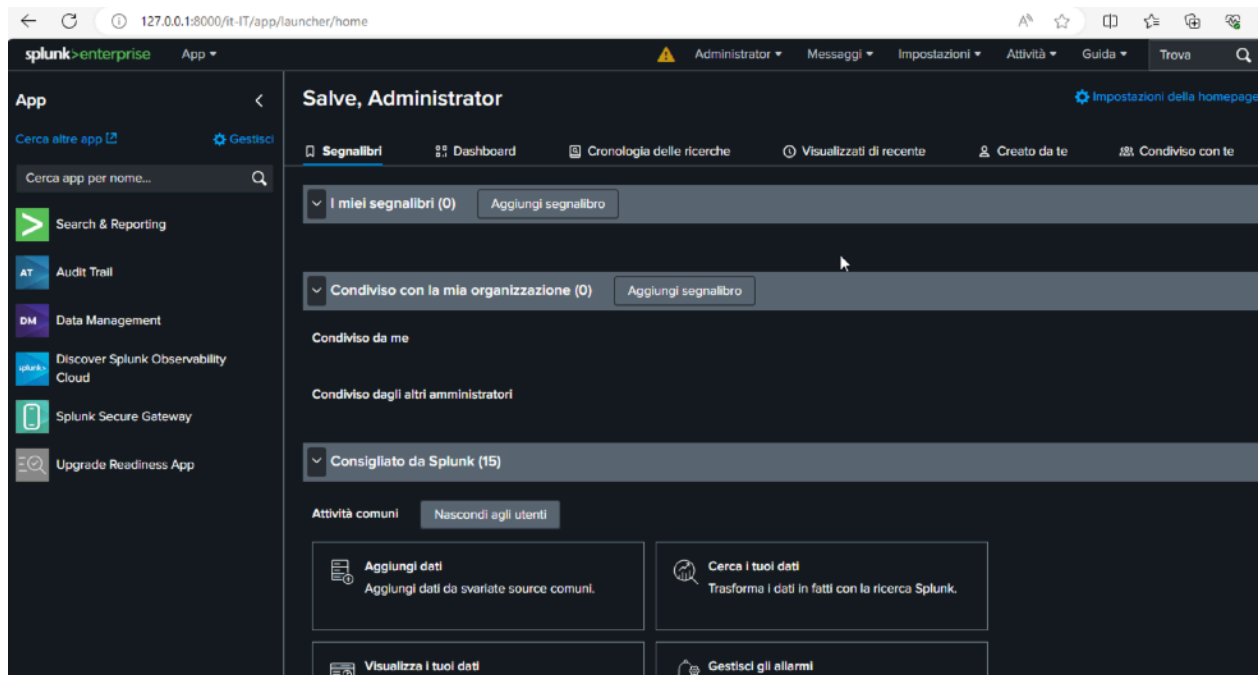


S10L1

Obiettivo: Configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.

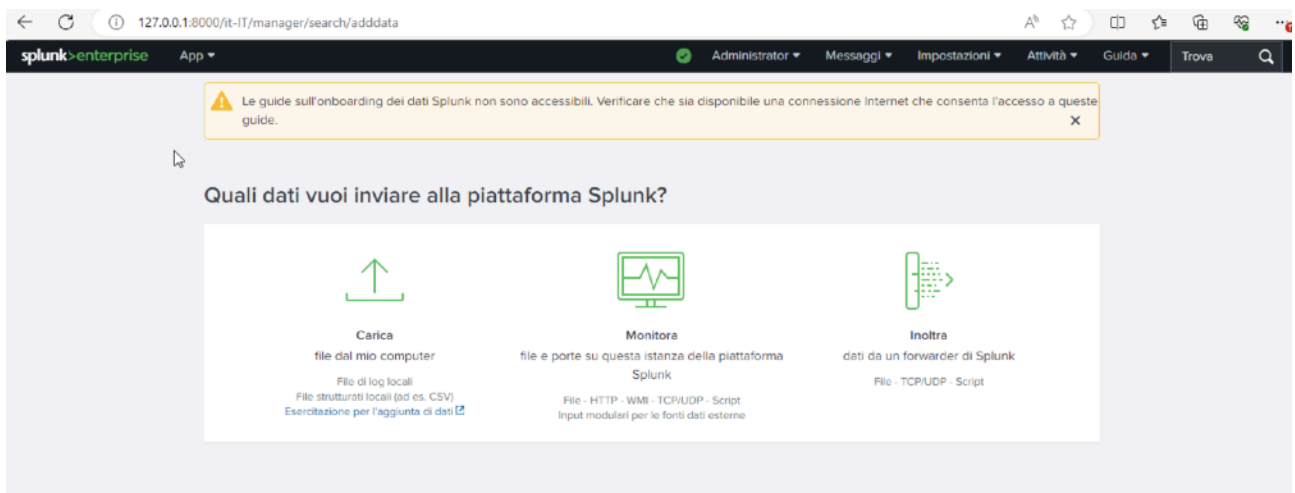
Step1.

Apro su splunk e vado su aggiungi dati



Step 2.

Vado su monitora



Seleziono Log di eventi locali e poi security

The screenshot shows the 'Log di eventi locali' configuration page. On the left, there's a sidebar with options: 'Log di eventi locali' (selected), 'Log di eventi remoti', 'File e directory', 'Raccolta eventi HTTP', 'TCP / UDP', and 'Monitoraggio prestazioni locali'. The main area has a heading 'Configura questa istanza per monitorare i canali di log di Windows locali in cui le applicazioni, i servizi e i processi del sistema inviano dati. Questo monitor si esegue una volta per ogni input di log di eventi che definisci. [Ulteriori informazioni](#)

. Below this is a table with columns 'Seleziona log eventi' and 'Disponibile elemento/i'. The 'Disponibile elemento/i' column lists: Application, Security, Setup, System, ForwardedEvents, Els_Hyphenation/Analytic, EndpointMapper, FirstUXPerf-Analytic, and AMSI/Debug. There's an 'aggiungi tutto >' button and a 'Seleziona' column. Below the table, it says 'Selezionare nell'elenco i Log eventi Windows da cui iniziare l'indicizzazione.' and a 'Domande frequenti' link.

A questo punto faccio verifica-invio-Avvia ricerca

The screenshot shows the 'Aggiungi dati' wizard in the 'Verifica' step. The progress bar shows four steps: 'Seleziona source' (completed), 'Impostazioni di input' (completed), 'Verifica' (current step), and 'Fine' (pending). The 'Verifica' step has a 'Verifica >' button. Below the progress bar, there's a section titled 'Log eventi locali (input) è stato creato correttamente.' with a green checkmark. It says 'Configurare gli input da Impostazioni > Input dati'. There are four buttons: 'Avvia ricerca' (green), 'Aggiungi altri dati', 'Scarica app', and 'Crea dashboard'. Each button has a description: 'Eseguire una ricerca tra i dati ora oppure visualizzare esempi ed esercitazioni.', 'Aggiungere altri input di dati ora oppure visualizzare esempi ed esercitazioni.', 'Le app consentono di fare di più con i propri dati. Ulteriori informazioni.', and 'Visualizza le ricerche. Ulteriori informazioni.' respectively.

Step3.

La scansione è stata fatta ora posso navigare per vedere tutti i dettagli.

The screenshot displays the Splunk Enterprise Search & Reporting interface. The search bar at the top contains the query: `source="WinEventLog:*" host="Splunk-Server"`. The search results show 3,010 events. The interface is in Italian, with the search bar labeled "Nuova ricerca". The search results are displayed in a table format, showing the event details for the selected time range.

Search Query: `source="WinEventLog:*" host="Splunk-Server"`

Results: 3.010 eventi (prima di 15/09/25 17:58:30,000)

Event Details:

Ora	Evento
15/09/25 10:57:51,000	09/15/2025 10:57:51 AM LogName=Security EventCode=1100 EventType=4 ComputerName=WIN-39AQM68JP3H Mostra tutte le 12 righe host = Splunk-Server source = WinEventLog:Security sourcetype = WinEventLog:Security
15/09/25 10:57:34,000	09/15/2025 10:57:34 AM LogName=Security EventCode=4672 EventType=8 ComputerName=WIN-39AQM68JP3H Mostra tutte le 31 righe host = Splunk-Server source = WinEventLog:Security sourcetype = WinEventLog:Security

Left Panel (CAMPIONI SELEZIONATI):

- host 1
- source 1
- sourcetype 1

Left Panel (CAMPIONI INTERESSANTI):

- ComputerName 3
- date_hour 3
- date_mday 2
- date_minute 53
- date_month 2
- date_second 60
- date_wday 2
- date_year 1
- date_zone 1

Right Panel: Attiva Windows. Passa a Impostazioni per attivare Windows.