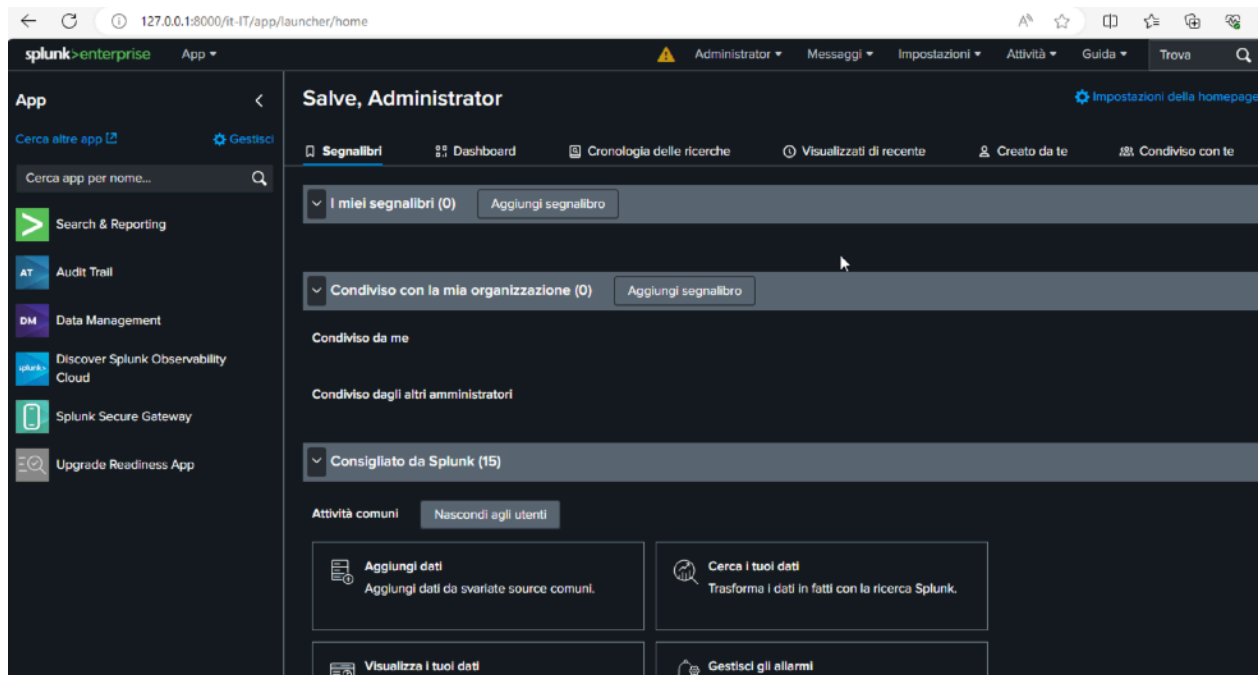


Splunk

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

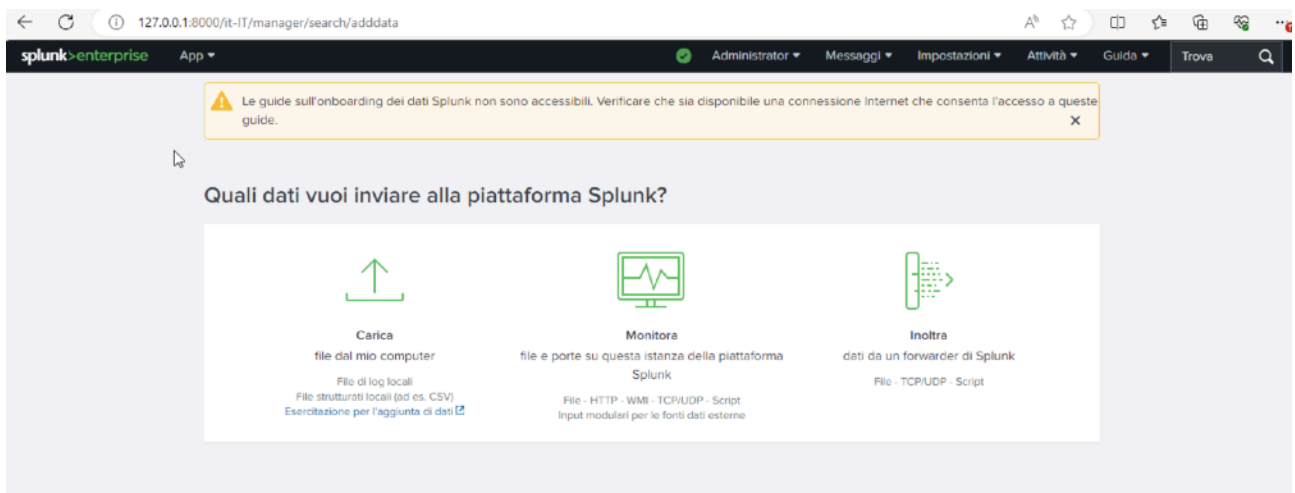
Step1.

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' (Local Event Logs) configuration page in Splunk. 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 dei log di eventi locali di Windows 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 on the right. 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' (Add Data) wizard in Splunk. The progress bar at the top shows four steps: 'Seleziona source', 'Impostazioni di input', 'Verifica', and 'Fine'. The 'Verifica' step is currently active. Below the progress bar, there are three rows of the wizard, each with a 'Verifica' button. The first row has a 'Verifica >' button. The second row has an 'Invia >' button. The third row has an 'Avanti >' button. Below the wizard, there's a green checkmark and the text 'Log eventi locali (input) è stato creato correttamente.' followed by 'Configurare gli input da Impostazioni > Input dati'. There are four buttons: 'Avvia ricerca' (with a description 'Eseguire una ricerca tra i dati ora oppure visualizzare esempi ed esercitazioni. [?](#)'), 'Aggiungi altri dati' (with a description 'Aggiungere altri input di dati ora oppure visualizzare esempi ed esercitazioni. [?](#)'), 'Scarica app' (with a description 'Le app consentono di fare di più con i propri dati. Ulteriori informazioni. [?](#)'), and 'Crea dashboard' (with a description 'Visualizza le ricerche. Ulteriori informazioni. [?](#)').

Step3.

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

The screenshot displays the Splunk Enterprise search interface. The search bar at the top contains the query `source="WinEventLog:*" host="Splunk-Server"`. Below the search bar, a notification indicates that 3,010 events were found. The interface is set to 'Visualizzazione' (Visualization) mode, showing a list of events. The left sidebar contains a list of fields under 'CAMPI SELEZIONATI' and 'CAMPI INTERESSANTI'. The main panel shows a table of search results with columns for 'i', 'Ora', and 'Evento'. The first event is dated 15/09/25 at 10:57:51 AM, with LogName=Security, EventCode=1100, and EventType=4. The second event is dated 15/09/25 at 10:57:34 AM, with LogName=Security, EventCode=4672, and EventType=8. The interface also includes a 'Processo' button and a 'Modalità intelligente' dropdown.

source="WinEventLog:*" host="Splunk-Server"

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

Abilita il campionamento degli eventi per eseguire la ricerca e restituire un insieme casuale di eventi.

Processo

Formato timeline Zoom indietro

Formato Mostra: 20 per pagina Visualizza: Elenco

i	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

Attiva Windows
Passa a Impostazioni per attivare Windows