

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

The screenshot shows the Splunk Manager interface at the URL 127.0.0.1:8000/it-IT/manager/search/adddata. The main panel displays options for adding data to the Splunk platform, including 'Cloud computing', 'Collegamento in rete', and 'Sistemi operativi'. Below these, there's a section for 'Oppure, inserisci i dati utilizzando uno dei seguenti metodi' with three icons: 'Carica' (Upload), 'Monitora' (Monitor), and 'Inoltra' (Forward). To the right, a sidebar titled 'Impostazioni' (Settings) is open, showing various categories like KNOWLEDGE, DATI, AMBIENTE DISTRIBUITO, and UTENTI E AUTENTICAZIONE. Red arrows highlight the 'Monitora' icons in both the main interface and the settings sidebar.

si clicca dal menù a tendina “impostazioni” → “aggiungi dati” → “monitora”

The screenshot shows the 'Aggiungi dati' (Add Data) configuration page. It has a progress bar at the top with steps: 'Selezione source', 'Impostazioni di input', 'Verifica', and 'Fine'. The 'Impostazioni di input' step is active. On the left, there are several configuration sections: 'Log di eventi locali', 'Log di eventi remoti', 'File e directory', 'Raccolta eventi HTTP', 'TCP / UDP', 'Monitoraggio prestazioni locali', and 'Monitoraggio prestazioni remoto'. The 'Log di eventi locali' section is expanded, showing instructions to monitor local Windows Event Log channels. On the right, there's a 'Selezione log eventi' (Select log events) section with a list of available event types: Application, Security, Setup, System, ForwardedEvents, DirectShowPluginControl, Els_Hyphenation/Analytic, EndpointMapper, and FirstUXPerf-Analytic. A 'aggiungi tutto' (Add all) button is present. A red arrow highlights the 'Monitora' icon in the 'Impostazioni di input' section, and another red arrow highlights the 'Monitora' icon in the 'Disponibile/elemento/i' list.

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

Aggiungi dati

In alternativa, impostare ulteriori parametri di input per questo input di dati come segue:

Host

Quando la piattaforma Splunk indica 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: SPLUNK-Server

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: Default ▾ 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)

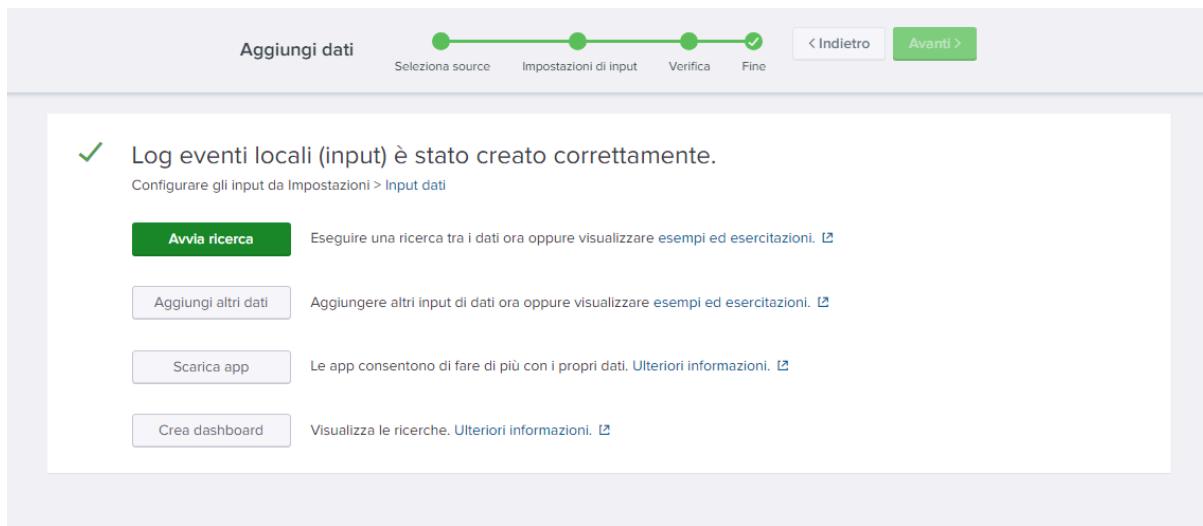
Aggiungi dati

Verifica

Tipo di input Log eventi di Windows
 Log eventi Application
 DirectShowPluginControl
 Els_Hyphenation/Analytic
 EndpointMapper
 FirstUXPerf-Analytic

Contesto app search
 Host SPLUNK-Server
 Indice default

finestra di verifica prima dell'avvio della ricerca



cliccare sul tasto verde per far partire la ricerca

The screenshot shows the Splunk search interface with a search bar containing 'source="WinEventLog:*" host="SPLUNK-Server"'. The results section shows '2.458 eventi (prima di 24/11/25 14:15:59,000)' and 'Nessun campionamento degli eventi'. The 'Eventi' tab is selected. A modal dialog is open over the search results, titled 'sourcetype'. It displays a table of values: WinEventLog:Security (19,393, 85,952%), WinEventLog:Application (2,081, 9,266%), WinEventLog:System (1,049, 4,671%), WinEventLog:Setup (18, 0,08%), and WinEventLog:Windows PowerShell (7, 0,031%). The 'Report' section includes tabs for 'Primi valori', 'Primi valori nel tempo', and 'Valori rari'. The bottom of the dialog shows a preview of log entries for WinEventLog:Security and WinEventLog:System.

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