

Monitora Splunk

S10L1

Traccia:

Abbiamo esplorato diverse funzionalità offerte da Splunk. Oggi ci concentreremo sulla modalità "Monitora".

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

In breve: Lo studente dovrà configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.

1) Obiettivo

L'obiettivo dell'esercizio è configurare Splunk Enterprise in modalità "Monitor" per raccogliere e analizzare in tempo reale i log di sistema (Windows Event Logs) dalla macchina locale.

2) Procedura di configurazione

Passo 1: selezione della sorgente dati

Dalla home di Splunk, ho selezionato "Aggiungi dati" e successivamente la modalità **monitor**.

Nella sezione "Log di eventi locali" (Local Event Logs), ho selezionato la tipologia di log da monitorare.

Come mostrato nello screenshot sottostante, ho scelto di monitorare il canale **security** per analizzare gli eventi relativi alla sicurezza del sistema.

The screenshot shows the 'Aggiungi dati' (Add Data) wizard in progress. The current step is 'Impostazioni di input' (Input Settings). A sidebar on the left lists five options: 'Log di eventi locali' (selected), 'Log di eventi remoti', 'File e directory', 'Raccolta eventi HTTP', and 'TCP / UDP'. On the right, a configuration panel for 'Log di eventi locali' is displayed. It includes a table where 'Security' is checked under 'Selezionato' (Selected). Other items listed in the table are 'Application', 'Security', 'Setup', 'System', 'ForwardedEvents', 'DirectShowPluginControl', 'Els_Hyphenation/Analytic', 'EndpointMapper', and 'FirstUXPerf-Analytic'. A note at the bottom says 'Selezionare nell'elenco i Log eventi Windows da cui iniziare l'indicizzazione.'

Passo 2: impostazione dell'input

Durante la configurazione, ho personalizzato il nome dell'**host** per identificare univocamente la macchina sorgente.

Al termine della procedura guidata, Splunk ha confermato la corretta creazione dell'input dati.

The screenshot shows the 'Aggiungi dati' (Add Data) wizard in Step 4: 'Verifica' (Verification). A green checkmark is displayed next to the message 'Log eventi locali (input) è stato creato correttamente.' (Local log events (input) was created successfully). Below this, there are several buttons: 'Avvia ricerca' (Run search), 'Aggiungi altri dati' (Add other data), 'Scarica app' (Download app), 'Crea dashboard' (Create dashboard), and 'Visualizza le ricerche' (View searches).

3) Verifica e risultati

Per confermare che la configurazione fosse operativa, ho avviato una ricerca sui dati indicizzati.

Analisi dei risultati:

- **Source: WinEventLog:Security**
- **Host: DESKTOP-8CAJRT0**
- **Esito:** la ricerca ha restituito **5.675 eventi**, confermando che Splunk sta ricevendo e indicizzando i dati in tempo reale.

The screenshot shows the Splunk Enterprise search interface. The search bar contains the query "source='WinEventLog:Security' host='DESKTOP-8CAJRT0'". The results panel shows 5,675 events found, with the first event being a security log entry from November 24, 2025, at 16:49:41.460 PM. The event details include LogName=Security, EventCode=5061, EventType=0, and ComputerName=DESKTOP-8CAJRT0. The interface also shows various navigation and visualization options.

4) Conclusione

La configurazione della modalità Monitor è avvenuta con successo, il sistema è ora attivo e sta collezionando i log di sicurezza locali, permettendo future analisi di security monitoring e incident response.

