

S10L1

Esercizio di oggi: Configurazione della Modalità Monitora in Splunk

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.

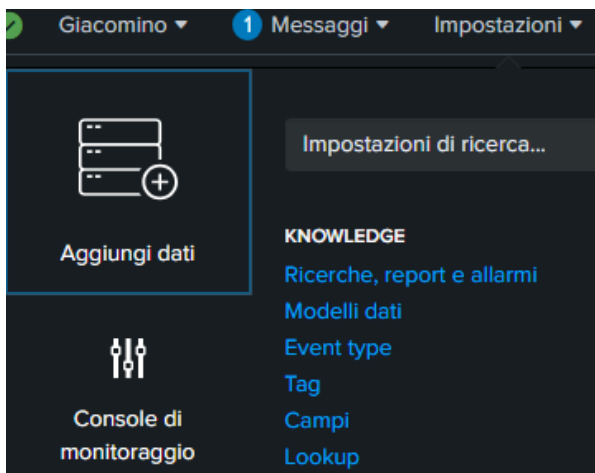
In breve: Lo studente dovrà configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.

L'obiettivo di questo esercizio è **configurare la modalità "Monitora" in Splunk** e dimostrarne il funzionamento attraverso degli screenshot. Splunk offre diverse funzionalità, ma in questo caso, ci concentriamo sulla capacità di monitorare dati in tempo reale. Questo processo ci permette di raccogliere e analizzare log da diverse fonti, come ad esempio i log degli eventi di Windows.

La prima fase consiste nell'accedere alla schermata principale di **Splunk** e selezionare l'opzione

Aggiungi dati

Questa è la porta d'accesso per iniziare a importare qualsiasi tipo di dato nella piattaforma.



Una volta nella schermata di aggiunta dati, si presentano diverse opzioni. Scegliamo

Monitora

Questa modalità è ideale per l'acquisizione continua di dati da file, porte o script, rendendola perfetta per il monitoraggio in tempo reale.



Successivamente, il sistema ci chiede di specificare la fonte dei dati da monitorare. Abbiamo selezionato **"Log di eventi locali"** per raccogliere i log degli eventi di Windows del computer. Per questo esercizio, abbiamo scelto di aggiungere tutti i log disponibili (Application, Security, Setup, System) per una dimostrazione completa.

The screenshot shows the 'Log di eventi locali' configuration page. On the left, there are four options: 'Log di eventi locali' (selected), 'Log di eventi remoti', 'File e directory', and 'Raccolta eventi HTTP'. Below these is a 'TCP / UDP' section. The main area on the right is titled '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 the text, there is a table with two columns: 'Seleziona log eventi' and 'Disponibile elemento/i'. The 'Disponibile elemento/i' column contains a list of event log channels: Application, Security, Setup, System, ForwardedEvents, DirectShowPluginControl, Els_Hyphenation/Analytic, EndpointMapper, and FirstUXPerf-Analytic. To the right of this list is a 'Seleziona' column with a list of the same channels. A 'aggiungi tutto >' link is located between the two columns.

Nella fase di configurazione successiva, abbiamo impostato i parametri di input. Il valore

"Host" è stato lasciato come **SplunkServer** per identificare la macchina di origine dei dati, mentre l'**"Indice"** è stato mantenuto come **default**. Questo indice è il contenitore predefinito dove Splunk archiverà i dati in ingresso.

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

SplunkServer

Prima di finalizzare, Splunk mostra un riepilogo delle configurazioni scelte per la verifica. Dopo aver confermato che tutte le impostazioni sono corrette, il processo di configurazione è stato completato con successo. Un messaggio di conferma indica che l'input dei log eventi locali è stato creato.

The screenshot shows a progress bar with four steps: 'Seleziona source', 'Impostazioni di input', 'Verifica', and 'Fine'. The 'Verifica' step is currently active, indicated by a green dot. To the right of the progress bar are two buttons: '< Indietro' and 'Invia >'. Above the progress bar, the text 'Aggiungi dati' is displayed.

Verifica

Tipo di input Log eventi di Windows

Log eventi
Application
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
ForwardedEvents

Contesto app search

Host SplunkServer

Indice default



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](#). [↗](#)

Infine, abbiamo avviato la ricerca per visualizzare i dati appena acquisiti. Lo screenshot mostra la schermata di **Splunk** con i log degli eventi visualizzati, confermando che la configurazione è stata eseguita correttamente e che il monitoraggio è attivo.

I dati sono ora pronti per essere analizzati, visualizzando informazioni dettagliate come l'ora, il tipo di evento e l'host di provenienza.

The screenshot displays the Splunk search results page. At the top, the search bar contains the query `source="WinEventLog:*" host="splunkserver"`. Below the search bar, the results are shown in a table format. The table has columns for time, event type, and event details. The first event is a "LogName: System" event with EventCode=1614, occurring on 09/15/2025 at 13:56:10.000. The second event is a "LogName: System" event with EventCode=1614, occurring on 09/15/2025 at 13:51:08.000. The third event is a "LogName: Security" event with EventCode=4672, occurring on 09/15/2025 at 13:51:04.000. The fourth event is a "LogName: Security" event with EventCode=4624, occurring on 09/15/2025 at 13:51:04.000. The fifth event is a "LogName: Security" event with EventCode=4672, occurring on 09/15/2025 at 13:51:03.000. The interface includes various navigation and filtering options on the left and top.

L'esito finale della ricerca ha confermato che la configurazione è stata completata correttamente, permettendo di visualizzare i dati in una dashboard intuitiva. Questo processo non solo valida la comprensione delle funzionalità di Splunk, ma sottolinea anche l'importanza di monitorare continuamente i log per mantenere la sicurezza e l'integrità dei sistemi.