

# S10L1

## Splunk

L'obiettivo di oggi è configurare la modalità "**Monitor**" di Splunk, così da poter visualizzare in tempo reale i dati richiesti. Questa configurazione consentirà di acquisire, indicizzare e analizzare i log o i dati specificati non appena vengono generati, garantendo una visione immediata delle informazioni e facilitando il monitoraggio di eventi o anomalie.

## Che cosa è Splunk?

Splunk è uno dei migliori SIEM disponibili sul mercato, riconosciuto per la sua straordinaria flessibilità e capacità di scalare in ambienti complessi. La sua potenza risiede nella capacità di adattarsi a diverse esigenze aziendali, offrendo una gestione efficace e scalabile dei dati in tempo reale, rendendolo una scelta ideale per organizzazioni di tutte le dimensioni.

## Come funziona Splunk?

1. **Raccolta dei dati:** Splunk acquisisce dati provenienti da una vasta gamma di fonti, tra cui file di log, applicazioni, dispositivi di rete e API.
2. **Indicizzazione dei dati:** I dati raccolti vengono indicizzati, consentendo ricerche rapide ed efficienti. Questo passaggio è fondamentale per gestire grandi volumi di informazioni.
3. **Parsing:** Splunk analizza e trasforma i dati grezzi in un formato strutturato e utilizzabile. Questo processo consente di estrarre significati chiave dai dati in ingresso.
4. **Ricerca e analisi:** Gli utenti possono eseguire ricerche dettagliate sui dati indicizzati utilizzando query personalizzate. Splunk mette a disposizione un linguaggio di ricerca potente e intuitivo.
5. **Visualizzazione dei dati:** I risultati delle analisi possono essere rappresentati visivamente attraverso dashboard, grafici e report, rendendo le informazioni più comprensibili e utili per il processo decisionale.

## Componenti principali di Splunk

- **Host:** Rappresenta il sistema o il dispositivo da cui provengono i dati raccolti.
  - **Esempio:** Un server web specifico, un router o un dispositivo di sicurezza.
- **Source:** È il percorso o la posizione esatta da cui Splunk raccoglie i dati. Può essere un file di log, una directory, un protocollo di rete o un comando eseguito.
  - **Esempio:** Un file di log come `/var/log/syslog`, un database o un URL di una API.
- **SourceType:** Indica il formato dei dati raccolti. Questa categorizzazione aiuta Splunk a applicare la logica di parsing corretta e a trattare i dati in modo adeguato.
  - **Esempio:** Formati come JSON, CSV, syslog o Apache access log.

## Cos'è il parsing dei dati?

Il parsing è il processo di analisi dei dati grezzi acquisiti per trasformarli in informazioni strutturate e significative. Splunk utilizza il parsing per riconoscere e organizzare i dati in base alla loro origine, formato e contenuto, rendendoli facilmente consultabili e analizzabili.

## Esercitazione pratica

Per andare a configurare la modalità monitor bisogna seguire una serie di passaggi.

### Passaggio 1

Andare nella sezione 'monitora' di splunk



Carica

file dal mio computer

File di log locali

File strutturati locali (ad es. CSV)

Esercitazione per l'aggiunta di dati [?](#)



Monitora

file e porte su questa istanza della piattaforma

Splunk

File - HTTP - WMI - TCP/UDP - Script  
Input modulari per le fonti dati esterne



Inoltra

dati da un forwarder di Splunk

File - TCP/UDP - Script

## Passaggio 2

Successivamente nella sezione 'log di eventi locali' selezionare la voce 'security' dal menù a tendina sulla destra. Dopodiché procedere con il tasto **'avanti'**

**Aggiungi dati**

Seleziona source   Impostazioni di input   Verifica   Fine

**Log di eventi locali**  
Raccogliere log eventi da questo computer.

**Log di eventi remoti**  
Raccogliere log eventi da host remoti. Nota: utilizza WMI e richiede un account di dominio.

**File e directory**  
Caricare un file, indicizzare un file locale o monitorare un'intera directory.

**Raccolta eventi HTTP**  
Configurare i token che i client possono utilizzare per inviare dati su HTTP o HTTPS.

**TCP / UDP**  
Configurare la piattaforma Splunk in modo che sia in ascolto su una porta di rete.

**Monitoraggio prestazioni locali**  
Raccogliere dati sulle prestazioni da questo computer.

Configure this instance to monitor local Windows Event Log channels where installed app services, and system processes send data. This monitor runs once for every Event Log in you define. [Ulteriori informazioni](#)

Seleziona log eventi   Disponibile elemento/i   [aggiungi tutto >](#)

Application  
Security  
Setup  
System  
ForwardedEvents  
Els\_Hyphenation/Analytic  
EndpointMapper  
FirstUXPerf-Analytic  
AMSI/Debug

Selezionare nell'elenco i Log eventi Windows da cui iniziare l'indicizzazione

**Domande frequenti**

> A quali log eventi ha accesso questa istanza della piattaforma Splunk?

## Passaggio 3

Come terzo passaggio bisogna selezionare l'host che decidiamo di tenere sotto controllo. Dopo aver dichiarato il nome dell'host pigiare sul tasto **'verifica'**

**splunk>enterprise**   App   Adminis...   Messaggi   Impostazioni   Attività   Guida   Trova

**Aggiungi dati**

Seleziona source   Impostazioni di input   Verifica   Fine

**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  

**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      [Crea un nuovo indice](#)

## Passaggio 4

Splunk come quarta schermata mostra un recap della richiesta che stiamo per attuare. Se tutto è continuare pigiando sul testo **‘invia’**

The screenshot shows the 'Verifica' (Verify) step in the Splunk data ingestion process. At the top, there is a progress bar with four stages: 'Seleziona source', 'Impostazioni di input', 'Verifica', and 'Fine'. The 'Verifica' stage is currently active. Below the progress bar, there are two buttons: '< Indietro' (Previous) and 'Invia >' (Next). The main content area is titled 'Verifica' and contains the following fields:

- Tipo di input ..... Log eventi di Windows
- Log eventi ..... Security
- Contesto app ..... search
- Host ..... WindowsServerIT
- Indice ..... default

## Passaggio 5

L'ultima schermata mostra come la richiesta sia stata creata correttamente ora bisogna andare su **‘avvia ricerca’**.

The screenshot shows the 'Avvia ricerca' (Run search) screen in Splunk. At the top, there is a green checkmark and the text: 'Log eventi locali (input) è stato creato correttamente.' Below this, there is a link: 'Configurare gli input da Impostazioni > Input dati'. There are four main buttons with descriptions:

- Avvia ricerca**: Esegui 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](#).

## Fase di monitoraggio

Ora saremo in grado di monitorare tutti i dati richiesti e, grazie all'uso di query personalizzate, potremo definire con precisione la quantità e il tipo di informazioni da visualizzare, rendendo l'analisi dei dati più mirata ed efficace.

The screenshot shows the Splunk search results interface. At the top, there is a search bar with the query: 'source="WinEventLog:\*" host="desktop-9k104bt"'. Below the search bar, there is a status bar indicating '127.427 eventi (prima di 02/12/24 16:05:40,000)'. There are buttons for 'Processo', 'Modalità intelligente', and 'Zoom indietro'. The main content area shows a list of events with columns for 'Ora' (Time) and 'Evento' (Event). The first event is from 02/12/24 16:08:29,000, with LogName=Security, EventCode=4798, EventType=0, ComputerName=DESKTOP-9K104BT, and source=WinEventLog:Security. The second event is from 02/12/24 16:08:29,000, with LogName=Security.