

# MONITORA SPLUNK



# Configurare la modalità "Monitora" in Splunk per raccogliere eventi dai registri di Windows e verificare l'avvenuta configurazione attraverso degli screenshot.

The screenshot shows the Splunk Enterprise web interface. The top navigation bar includes icons for user profile, dashboard, and search, followed by the title 'Impostazioni | Splunk'. Below the title is a search bar with the URL '127.0.0.1:8000/it-IT/manager/launcher/data/inputs/tcp/cooked'. The main menu bar contains links for 'splunk>enterprise', 'App ▾', 'Administra... ▾' (with a green checkmark), 'Messaggi ▾', 'Impostazioni ▾' (highlighted in blue), 'Attività ▾', 'Guida ▾', 'Trova', and a search icon. On the left, a sidebar titled 'Ricevi dati' shows the path 'Inoltro e ricezione ▾ > Ricevi dati'. It includes a 'Nuova porta di ricezione' button. Below this are sections for 'Visualizzazione 1-1 di 1 elemento', 'filtro' with a search icon, and '25 per pagina ▾'. A table lists a single input configuration: 'In ascolto su questa porta ▾' (9997), 'Stato ▾' (Abilitato | Disabilita), and 'Azioni' (Elimina). The overall theme is dark with blue and orange highlights.



## Procedura Seguita:

### 1. Accesso a Splunk:

- Ho avviato l'interfaccia web di Splunk utilizzando l'indirizzo 127.0.0.1:8000.
- La schermata mostra la ricerca personalizzata che utilizza come sorgente i log di eventi di Windows (WinEventLog).

### Configurazione della Modalità Monitora:

- La modalità "Monitora" in Splunk è stata configurata per acquisire i log relativi alla sicurezza del sistema operativo Windows.
- Questo è evidente dalla query eseguita: source="WinEventLog:\*" host="WinServer". Essa indica che Splunk è stato configurato per monitorare tutti i registri di eventi di Windows provenienti dal server denominato WinServer.

## Raccolta dei Dati:

- **Splunk ha correttamente acquisito 1.028 eventi, come indicato dai risultati della query.**
- **Tra le informazioni visibili nel pannello:**
  - **Il source è WinEventLog:Security, che conferma che Splunk sta monitorando gli eventi di sicurezza.**
  - **Il sourcetype è WinEventLog, una categorizzazione standard di Splunk per i registri di eventi di Windows.**
  - **L'host è correttamente configurato come WinServer.**

## Validazione e Visualizzazione dei Dati:

- **Gli eventi sono stati visualizzati nella sezione Eventi di Splunk, con dettagli completi, inclusa l'ora e il contenuto degli eventi di sicurezza acquisiti.**
- **Nello screenshot si nota chiaramente una timeline che mostra la distribuzione temporale degli eventi, confermando che la raccolta è in tempo reale e continua.**

The screenshot shows the Splunk search interface with the following details:

- Search Bar:** Ricerca | Splunk 9.3.2
- Search Query:** source="WinEventLog\*" host="WinServer" windows
- Results Summary:** 1.028 eventi (prima di 02/12/24 15:26:40,000)
- Event Timeline:** A horizontal timeline at the bottom showing event distribution over time.
- Event List:** A table showing the first few events with columns: Ora (Time), Evento (Event), and additional context.

Ora	Evento
02/12/24 15:26:24,000	12/02/2024 03:26:24 PM ... 2 lines omitted ... EventType=0 ComputerName=WinServer SourceName=Microsoft Windows security auditing. Type=Informazioni Mostra tutte le 31 righe
02/12/24 15:26:24,000	host = WINSERVER   source = WinEventLog:Security sourcetype = WinEventLog:Security ... 4 lines omitted ... ComputerName=WinServer SourceName=Microsoft Windows security auditing.

- Left Panel:** Shows selected fields (host 1, source 1, sourcetype 1) and interesting fields (ComputerName, date\_hour, date\_mday, date\_minute, date\_month, date\_second).

i	Ora	Evento
>	02/12/24 15:26:24,000	12/02/2024 03:26:24 PM LogName=Security EventCode=4672 EventType=0 ComputerName=WinServer SourceName=Microsoft Windows security auditing. Type=Informazioni RecordNumber=1028 Keywords=Controllo riuscito TaskCategory=Special Logon OpCode=Informazioni Message=Privilegi speciali assegnati a nuovo accesso.  Soggetto: ID sicurezza: S-1-5-18 Nome account: SYSTEM Dominio account: NT AUTHORITY ID accesso: 0x3E7  Privilegi: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeIncreaseQuotaPrivilege



**Conclusioni:**  
**Splunk è stato configurato per monitorare gli eventi di sicurezza generati dal sistema operativo Windows in modalità Monitora. La query utilizzata dimostra che i dati sono stati acquisiti correttamente e sono pronti per essere analizzati. La modalità Monitora è uno strumento potente di Splunk che consente di raccogliere eventi in tempo reale, offrendo una soluzione efficace per il monitoraggio della sicurezza e la diagnostica dei sistemi.**