

S10-L1

Configurazione modalità Monitora in Splunk

Introduzione

In questa esercitazione ho configurato Splunk utilizzando la **modalità Monitora (Monitor)** per **acquisire eventi da un file di log locale**.

L'obiettivo è dimostrare la **corretta configurazione dell'ingestione dati e verificare che gli eventi vengano indicizzati e visualizzati correttamente nella sezione Search**.

0) Installazione e primo accesso a Splunk

Download del pacchetto

Ho scaricato il pacchetto di installazione di **Splunk Enterprise per Windows (x64)** dalla sezione Download.

Nel percorso **Users > User > Download** è visibile:

- **La cartella compressa tutorialdata** (che utilizzerò successivamente per le esercitazioni)

Nome	Ultima modifica	Tipo	Dimensione
▼ Oggi (4)			
splunkforwarder-10.2.0-d749cb17ea65-wi...	09/02/2026 14:45	Pacchetto di Wind...	193.288 KB
Shadow	09/02/2026 12:13	Cartella compressa	5 KB
tutorialdata	09/02/2026 10:49	Cartella compressa	1.910 KB
splunk-10.2.0-d749cb17ea65-windows-x64	09/02/2026 10:25	Pacchetto di Wind...	1.066.600 KB

Cartella Download con pacchetto Splunk e tutorialdata evidenziati.

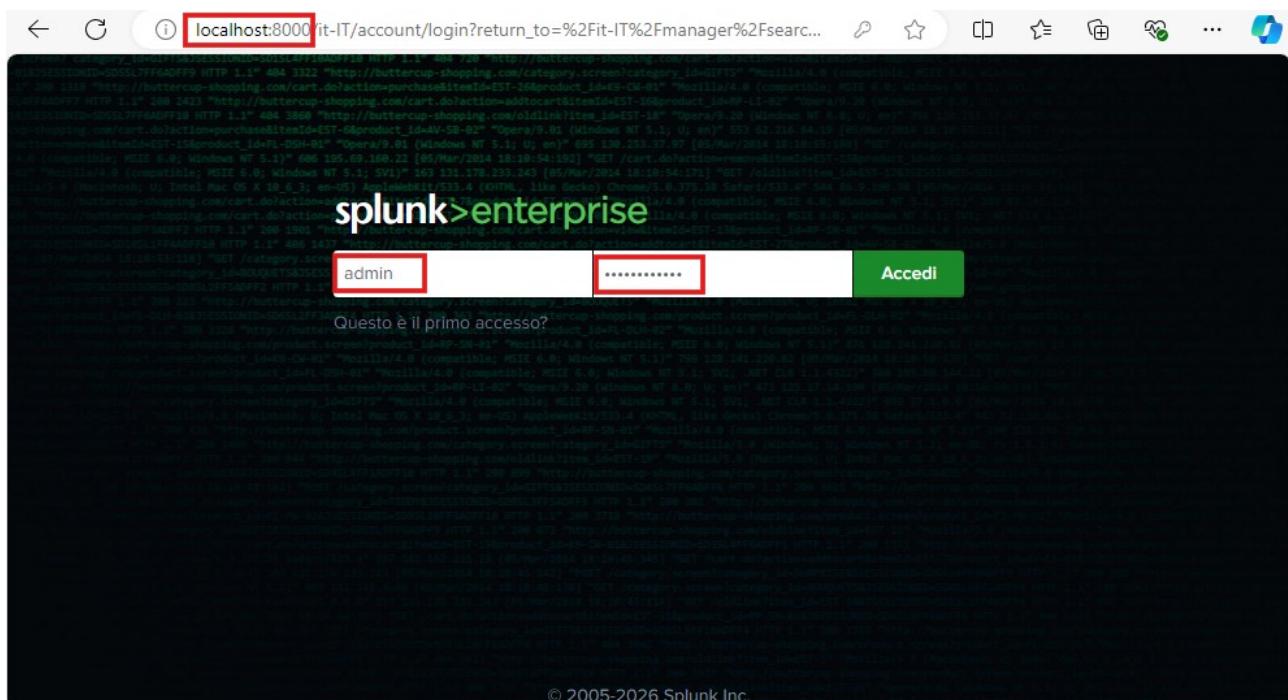
Installazione e avvio

Dopo aver completato l'installazione:

1. Ho avviato Splunk Enterprise.
2. Ho verificato che il servizio fosse in esecuzione.
3. Ho aperto il browser e digitato:

`http://localhost:8000`

Come mostrato nello screenshot a seguire, l'interfaccia web di Splunk è correttamente raggiungibile all'indirizzo **localhost:8000**.



1) Caricamento del file **tutorialdata.zip** e configurazione input

Selezione della source:

Dalla dashboard di Splunk ho selezionato **Aggiungi dati**.

Nella schermata **Seleziona source** ho scelto di caricare un file dal mio computer e ho selezionato: **tutorialdata.zip**

splunk>enterprise App ▾ Administ... 1 Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova 🔍

Aggiungi dati

Selezione source Impostazioni di input Verifica Fine

< Indietro Avanti >

File selezionato **tutorialdata.zip**

Selezione file

Ho creato un nuovo indice e selezionato Indice: **test_monitora**

splunk>enterprise App ▾ Administ... 1 Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova 🔍

Aggiungi dati

Selezione source Impostazioni di input Verifica Fine

< Indietro Verifica >

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 costante
 Espressione regolare nel percorso
 Segmento nel percorso

Valore campo Host **DESKTOP-8CAJRT0**

Indice **test_monitora** Crea un nuovo indice

splunk>enterprise App ▾ Administ... 1 Messaggi ▾ Impostazioni ▾ Attività ▾ Guida ▾ Trova 🔍

Aggiungi dati

Selezione source Impostazioni di input Verifica Fine

< Indietro Invia >

Verifica

Tipo di input File caricato
Nome file **tutorialdata.zip**
Source type Automatico
Host DESKTOP-8CAJRT0
Indice **test_monitora**

Come visibile nello screenshot, il file selezionato è correttamente indicato nella sezione “**Verifica**”.

✓ File è stato caricato correttamente.
Configurare gli input da Impostazioni > Input dati

Avvia ricerca

Cercare nei dati personali 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. ↗

2) Configurazione della modalità “Monitora” in Splunk

2) Accesso alla modalità Monitora

Dalla schermata principale di Splunk ho cliccato su **Aggiungi dati (Add Data)**.

Successivamente ho selezionato l’opzione **Monitora (Monitor)**, che consente di acquisire dati in tempo reale da file o directory presenti nel sistema.

Cloud computing
Get your cloud computing data in to the Splunk platform.
10 fonti di dati

Collegamento in rete
Immettere i dati di rete nella piattaforma Splunk.
2 fonti di dati

Sistema operativo
Immettere i dati del sistema operativo nella piattaforma Splunk.
1 fonte di dati

Sicurezza
Immettere i dati di sicurezza nella piattaforma Splunk.
3 fonti di dati

4 fonti di dati in totale

Oppure, inserisci i dati utilizzando uno dei seguenti metodi

Carica file dal mio computer
file log locali
file strutturati locali (ad es. CSV)
Esercitazione per l’aggiunta dei 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

Output schermata “Aggiungi dati” con opzione **Monitora** selezionata.

Dalla schermata **Aggiungi dati** ho selezionato l’opzione **Monitora**, che consente di acquisire dati in tempo reale da file, directory o porte locali della piattaforma Splunk.

Questa modalità permette di configurare il monitoraggio continuo delle fonti dati presenti sul sistema.

3) Selezione della fonte da monitorare

Ho selezionato l'opzione **Log di eventi locali** nella schermata di configurazione della modalità Monitora.

Questa opzione consente di acquisire direttamente i registri eventi del sistema operativo Windows, come:

- Security
- Application
- System

Ho scelto di monitorare il registro **Security**, in quanto **contiene eventi relativi ad accessi, autenticazioni e attività di sicurezza del sistema**.

In questo modo Splunk acquisisce in tempo reale gli eventi generati dal sistema operativo, indicizzandoli automaticamente nell'indice configurato.

The screenshot shows the 'Aggiungi dati' (Add Data) wizard. The first step, 'Selezione source' (Select source), is active. A red box highlights the 'Log di eventi locali' (Local Log Events) option, which is selected. To its right, a detailed configuration panel is shown. It explains that this instance monitors local Windows Event Log channels where installed applications, services, and system processes send data. It runs once for every Event Log input defined. A link to 'Ulteriori informazioni' (More information) is provided. Below this, there are two columns: 'Disponibile/elemento/i' (Available/item/s) and 'aggiungi tutto' (Add all). A red box highlights the 'Security' item under 'Disponibile/elemento/i'. Another red box highlights the 'Selezionato' (Selected) column, which contains 'Application', 'Security', and 'System'. Other items listed include 'ForwardedEvents', 'DirectShowPluginControl', 'Els_Hyphenation/Analytic', 'EndpointMapper', and 'FirstUXPerf-Analytic'. At the bottom of the panel, a note says 'Selezionare nell'elenco i Log eventi Windows da cui iniziare l'indicizzazione.'

Output "Log di eventi locali" con registri selezionati.

4) Configurazione dell'indice e completamento della modalità Monitora

Ho proceduto alla configurazione dei parametri di indicizzazione.

Nella schermata **Impostazioni di input**:

- Ho lasciato il valore **Host** impostato automaticamente (nome della macchina locale).
- Ho selezionato come **Indice**:

test_monitora

Ho verificato che il tipo di input fosse relativo al registro eventi di Windows e ho cliccato su **Verifica**, controllando la correttezza dei parametri configurati.

Successivamente ho cliccato su **Invia** per completare la configurazione della modalità **Monitora**.

The screenshot shows the Splunk interface with the following steps completed:

- Step 1: **Aggiungi dati** → **Selezione source** (green dot)
- Step 2: **Impostazioni di input** (green dot)
- Step 3: **Verifica** (green dot)
- Step 4: **Fine** (white dot)

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: DESKTOP-8CAJRTO

Indice: **Indice**: **test_monitora** (highlighted with a red box) | Crea un nuovo indice

Verifica: **Invia >** (highlighted with a red box)

Verifica details:
Tipo di input Log eventi di Windows
Log eventi Application
Contesto app search
Host DESKTOP-8CAJRTO
Indice test_monitora

Output schermata di configurazione con registri selezionati e indice **test_monitora**.

Conferma configurazione

Nella schermata di riepilogo ho controllato:

- Tipo di input: Monitoraggio file/directory
- Percorso configurato
- Host

- Indice test_monitora

Ho quindi cliccato su **Invia** per completare la configurazione.

5) Verifica del corretto funzionamento della modalità Monitora

Dopo aver completato la configurazione, ho verificato l'effettiva acquisizione degli eventi accedendo alla sezione **Search & Reporting**.

Ho eseguito la seguente query:

```
index="test_monitora"
```

Tra i risultati sono visibili eventi con:

- sourcetype = **WinEventLog:Security**
- **EventCode relativi ad attività di sicurezza** (es. 4624, 4672)
- Host = **DESKTOP-8CAJRT0**

La presenza degli eventi conferma che la modalità **Monitora** è stata configurata correttamente e che Splunk sta acquisendo i log in tempo reale.

Ora	Evento
09/02/26 16:55:12.076	02/09/2026 04:55:12.076 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-8CAJRT0 Mostra tutte le 31 righe
09/02/26 16:55:12.076	02/09/2026 04:55:12.076 PM LogName=Security EventCode=4624

La ricerca ha restituito oltre 116.000 eventi, provenienti dai registri locali di Windows.

Conclusioni:

Attraverso la modalità Monitora, **ho configurato correttamente l'acquisizione dei Log di eventi locali di Windows in Splunk.**

Ho verificato che:

- **I registri Application, Security e System vengono monitorati in tempo reale.**
- **Gli eventi vengono indicizzati correttamente nell'indice configurato.**
- **I dati risultano correttamente ricercabili nella sezione Search & Reporting.**

L'obiettivo dimostra la comprensione del processo di configurazione, indicizzazione e verifica dell'acquisizione dati tramite modalità Monitora in Splunk.