





# Configurazione della Modalità Monitora in Splunk

## Obiettivo:

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


monitora

Seguire le guide sull'onboarding delle fonti di dati più popolari


 <b>Cloud computing</b> Get your cloud computing data in to the Splunk platform. 10 fonti di dati	 <b>Collegamento in rete</b> Immettere i dati di rete nella piattaforma Splunk. 2 fonti di dati	 <b>Sistema operativo</b> Immettere i dati del sistema operativo nella piattaforma Splunk. 1 fonte di dati	 <b>Sicurezza</b> 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 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

## Log di eventi locali → Scegliamo l'opzione security

Aggiungi dati

Seleziona source

Impostazioni di input

Verifica

Fine

< Indietro

Avanti >

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.

Monitoraggio prestazioni remoto

Raccogliere informazioni su prestazioni ed eventi di host remoti.

Configura questa istanza per monitorare i canali di log di Windows locali in cui sono installate applicazioni, servizi e processi di sistema che inviano dati. Questo monitor esegue una volta per ogni input di log di eventi che definisci. [Ulteriori informazioni](#)

Seleziona log eventi

Disponibile elemento/i

aggiungi tutto >

Seleziona Security

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

Domande frequenti

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

Qual è il metodo migliore per monitorare i log eventi delle macchine Windows remote?

## Avvia ricerca



### 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](#).

Nuova ricerca

Salva come Crea vista tabella Chiudi

source="WinEventLog:\*" host="DESKTOP-8CAJRT0"

Sempre

Q

✓ 15.082 eventi (prima di 04/06/25 11:34:43.000) Nessun campionamento degli eventi

Processo

Modaltà intelligente

Eventi (15.082) Pattern Statistiche Visualizzazione

Formato timeline Zoom indietro Zoom area selezionata Deselezione

1 mese per colonna

Formato Mostra: 20 per pagina Visualizza: Elenco

Prec 1 2 3 4 5 6 7 8 Avanti

< Nascondi campi

Tutti i campi

CAMPI SELEZIONATI

# host 1

# source 1

# sourcetype 1

CAMPI INTERESSANTI

# ComputerName 2

# date\_hour 10

# date\_minute 5

# date\_second 57

# date\_year 2

# date\_zone 1

# Descrittore\_di\_sicurezza\_originale 3

# Dominio\_account 8

# EventCode 42

# EventType 3

04/06/25 11:33:39.000

06/04/2025 11:33:39 AM

LogName=Security

EventCode=4672

EventType=0

ComputerName=DESKTOP-8CAJRT0

Mostra tutte le 31 righe

host = DESKTOP-8CAJRT0 | source = WinEventLogSecurity | sourcetype = WinEventLogSecurity

>

04/06/25 11:33:39.000

06/04/2025 11:33:39 AM

LogName=Security

EventCode=4624

EventType=0

ComputerName=DESKTOP-8CAJRT0

Mostra tutte le 70 righe

host = DESKTOP-8CAJRT0 | source = WinEventLogSecurity | sourcetype = WinEventLogSecurity

>

04/06/25 11:33:37.000

06/04/2025 11:33:37 AM

LogName=Security

EventCode=4672

EventType=0

Generato il 4 giugno 2025