

Report di Analisi: Raccolta e Monitoraggio Log con Splunk Enterprise

Questo report illustra le attività svolte per la configurazione di Splunk Enterprise, l'importazione dei dati dai log di eventi di Windows e l'analisi degli eventi di sicurezza raccolti. L'obiettivo è stato quello di configurare correttamente una pipeline di monitoraggio degli eventi e fornire una panoramica dei principali dati ottenuti.

1. Configurazione dell'ambiente Splunk

Splunk è stato installato in locale ed è stato configurato per ascoltare sulla porta predefinita 8000. L'accesso è avvenuto tramite browser, come mostrato nella prima immagine (Figura 1). La configurazione è stata eseguita in un ambiente virtualizzato tramite Oracle VirtualBox, utilizzando una macchina Windows 10 Debloated.

2. Aggiunta dei dati e configurazione input

È stato selezionato il metodo di input per i log di eventi locali (Windows Event Logs). Nella Figura 2, possiamo osservare l'interfaccia che consente di scegliere i canali di log da monitorare. In questo caso, è stato selezionato il canale di sicurezza, che contiene informazioni rilevanti su login, tentativi di accesso falliti e attività di sistema.

Nella schermata successiva (Figura 3), sono state impostate le informazioni di input: l'host è stato nominato 'splunk-server' e i dati sono stati indicizzati nell'indice di default. Una volta completata la configurazione, è stata confermata la creazione dell'input per i log eventi locali (Figura 4).

3. Analisi dei log

Dopo aver completato la configurazione, è stato possibile effettuare una ricerca all'interno degli eventi raccolti (Figura 5). Sono stati rilevati 2.297 eventi di sicurezza, tutti appartenenti al tipo di sorgente 'WinEventLog:Security' (Figura 6).

Analizzando i campi, si osservano tre valori distinti per il campo 'ComputerName' (Figura 7):

- DESKTOP-8CAJRT0: 2.091 eventi (91%)
- WIN-55L622JBHP6: 194 eventi (8%)
- splunk-server: 12 eventi (0,5%)

Gli eventi analizzati (Figura 8 e Figura 9) includono codici evento significativi come:

- EventCode 4672: 'Special privileges assigned to new logon', utile per identificare accessi

con privilegi elevati.

- EventCode 4624: 'An account was successfully logged on', che indica autenticazioni riuscite.

4. Conclusioni

La configurazione di Splunk ha permesso di centralizzare e analizzare i log di sicurezza generati dal sistema Windows. L'identificazione dei codici evento 4672 e 4624 consente di avere visibilità su attività critiche e login effettuati. Il sistema è ora pronto per essere utilizzato per monitoraggi in tempo reale, creazione di dashboard e generazione di alert di sicurezza.

5. Screenshot dell'analisi

Le immagini seguenti mostrano passo passo la configurazione di Splunk, l'aggiunta dei dati e i risultati delle analisi eseguite.

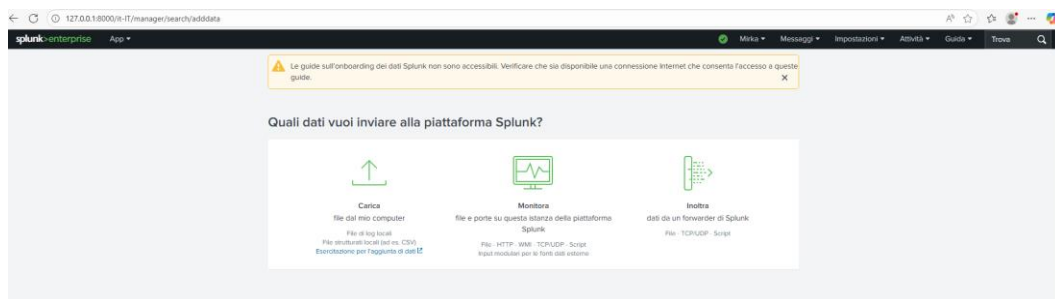


Figura 1: Interfaccia iniziale di Splunk Enterprise per l'aggiunta dati.

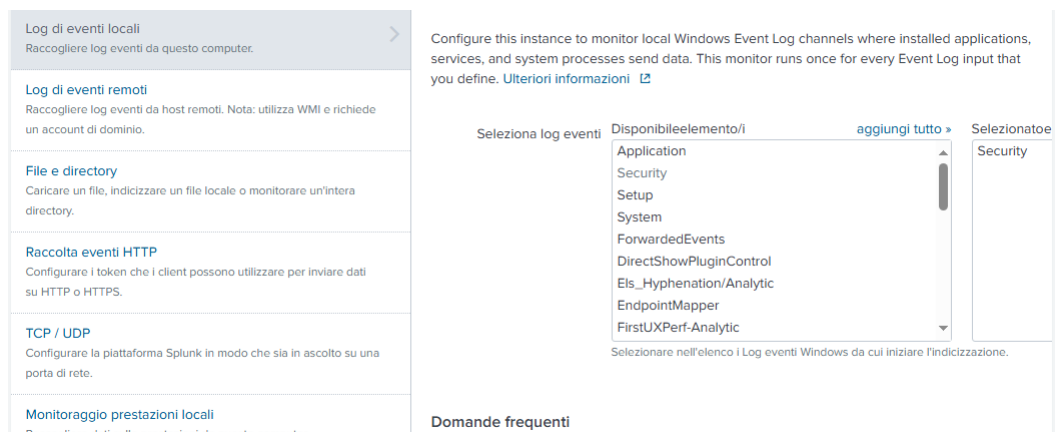


Figura 2: Scelta dei log di eventi locali di Windows.

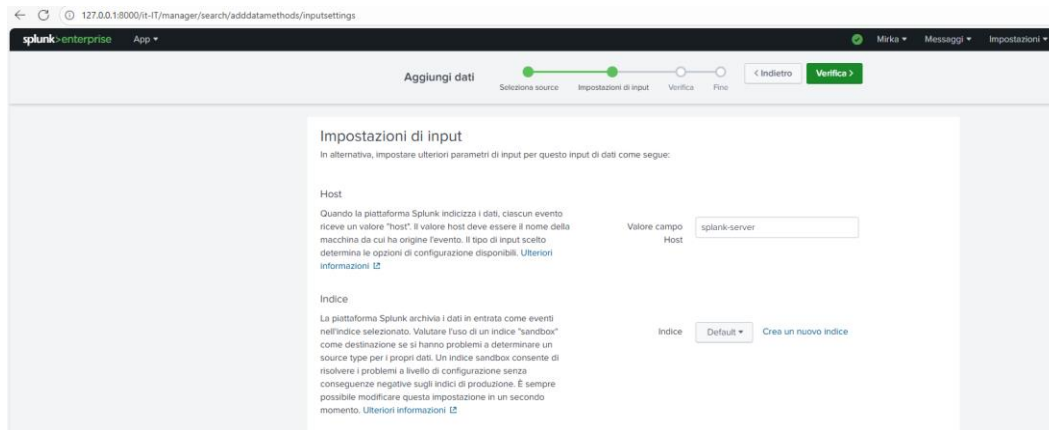


Figura 3: Impostazioni di input per host e indice.

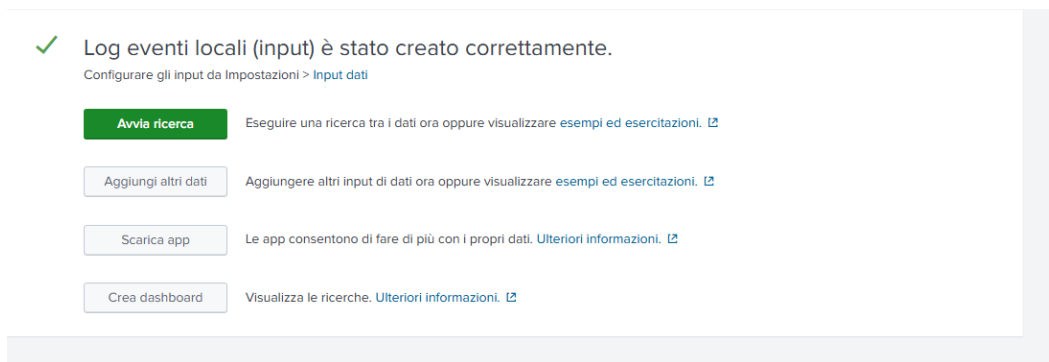


Figura 4: Conferma creazione input per log eventi locali.

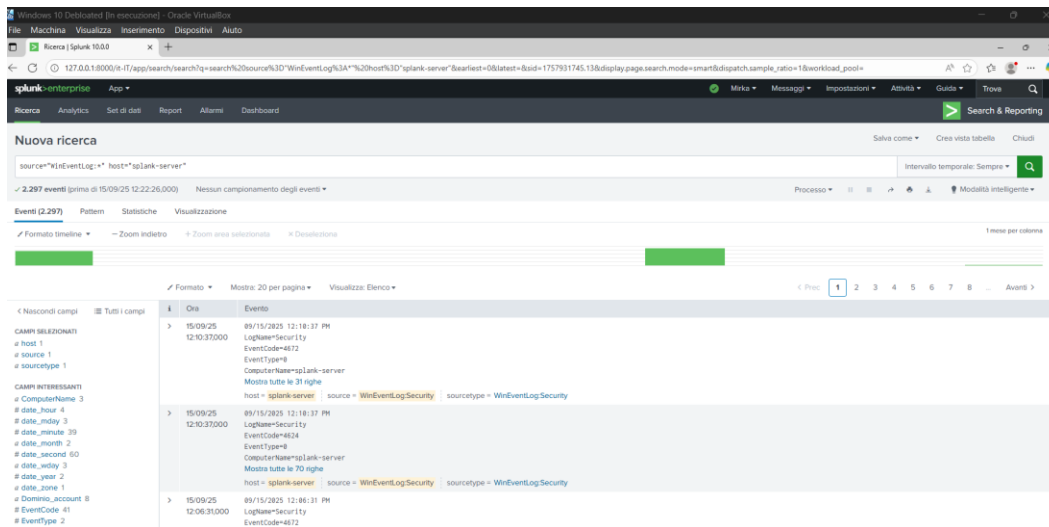


Figura 5: Ricerca eventi raccolti con Splunk.

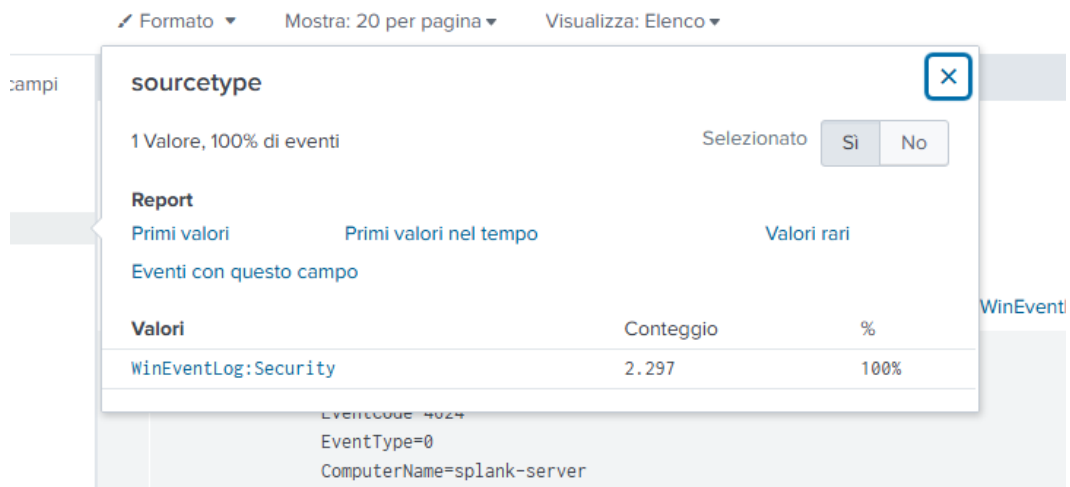


Figura 6: Tipologia di sorgente evento 'WinEventLog:Security'.

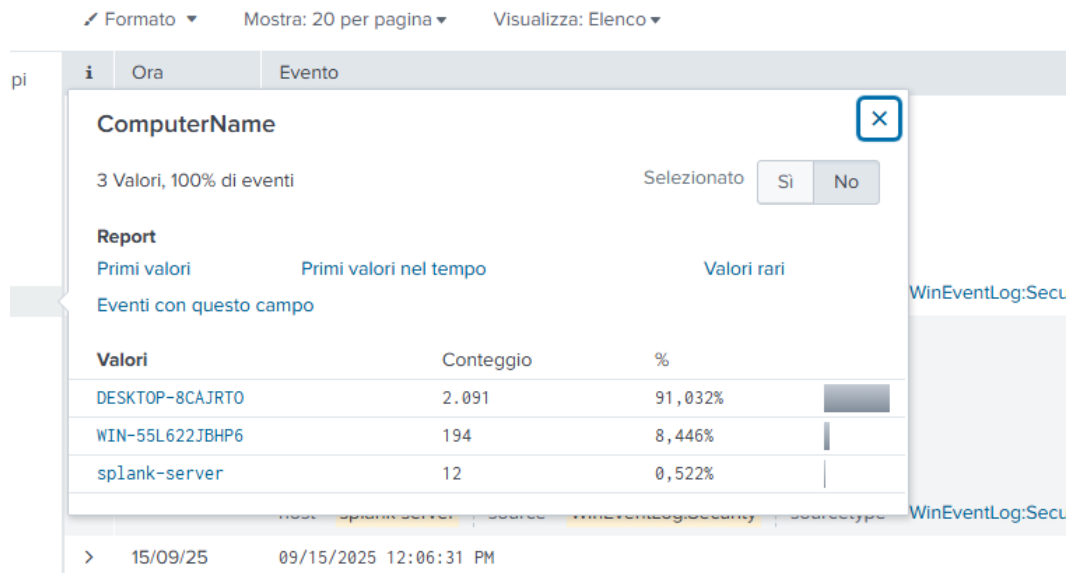


Figura 7: Analisi del campo ComputerName.

Formato ▼ Mostra: 20 per pagina ▼ Visualizza: Dati non elaborati ▼

i	Evento
>	09/15/2025 12:10:37 PM LogName=Security EventCode=4672 EventType=0 ComputerName=splank-server Mostra tutte le 31 righe
>	09/15/2025 12:10:37 PM LogName=Security EventCode=4624 EventType=0 ComputerName=splank-server Mostra tutte le 70 righe

Figura 8: Visualizzazione eventi grezzi.

CAMPI SELEZIONATI

- host 1
- source 1
- sourcetype 1

CAMPI INTERESSANTI

- ComputerName 3
- # date_hour 4
- # date_mday 3
- # date_minute 39
- # date_month 2
- # date_second 60
- # date_wday 3
- # date_year 2
- # date_zone 1

15/09/25 09/15/2025 12:10:37 PM
12:10:37,000 LogName=Security

_ora

Eventi prima o dopo

Prima di questo orario Dopo questo orario A questo orario

Eventi vicini

+/- 5 giorno/i

Applica

server

source = WinEventLog:Secu

PM

server

mostra tutte le 70 righe

host = splank-server source = WinEventLog:Secu

Figura 9: Filtri temporali sugli eventi.

Formato

Mostra: 20 per pagina

Visualizza: Elenco

Tutti i campi

i

Ora

Evento

▼

15/09/25
12:31:27,000

09/15/2025 12:31:27 PM
LogName=Security
EventCode=4672
EventType=0
ComputerName=splank-server
[Mostra tutte le 31 righe](#)

Azioni evento ▼

Tipo	<input checked="" type="checkbox"/>	Campo	Valore
Selezionato	<input checked="" type="checkbox"/>	host ▼	splank-server
	<input checked="" type="checkbox"/>	source ▼	WinEventLog:Security
	<input checked="" type="checkbox"/>	sourcetype ▼	WinEventLog:Security
Evento	<input type="checkbox"/>	ComputerName ▼	splank-server
	<input type="checkbox"/>	Dominio_account ▼	NT AUTHORITY
	<input type="checkbox"/>	EventCode ▼	4672
	<input type="checkbox"/>	EventType ▼	0
	<input type="checkbox"/>	ID_accesso ▼	0x3E7

Figura 10: Dettaglio evento con codice 4672.