

Report Tecnico: Configurazione Data Input e Monitoraggio Eventi su Splunk

Studente: Rocco Paolo Caccamo

Oggetto: Monitoraggio Log Locali Windows Mediante Splunk

Data: 09/02/2026

1. Obiettivo dell'Esercizio

L'attività ha lo scopo di configurare la modalità "Monitora" all'interno della piattaforma Splunk Enterprise. L'obiettivo specifico è abilitare l'ingestione dei log di sistema locali (Windows Event Logs) e verificare la corretta indicizzazione dei dati.

2. Metodologia di Configurazione

Sulla base delle evidenze raccolte, la configurazione è stata eseguita seguendo questi step sequenziali:

2.1 Selezione della Sorgente Dati

È stata utilizzata la procedura guidata "Aggiungi dati" di Splunk, selezionando l'opzione "**Log di eventi locali**" per raccogliere i log direttamente dal computer ospite.

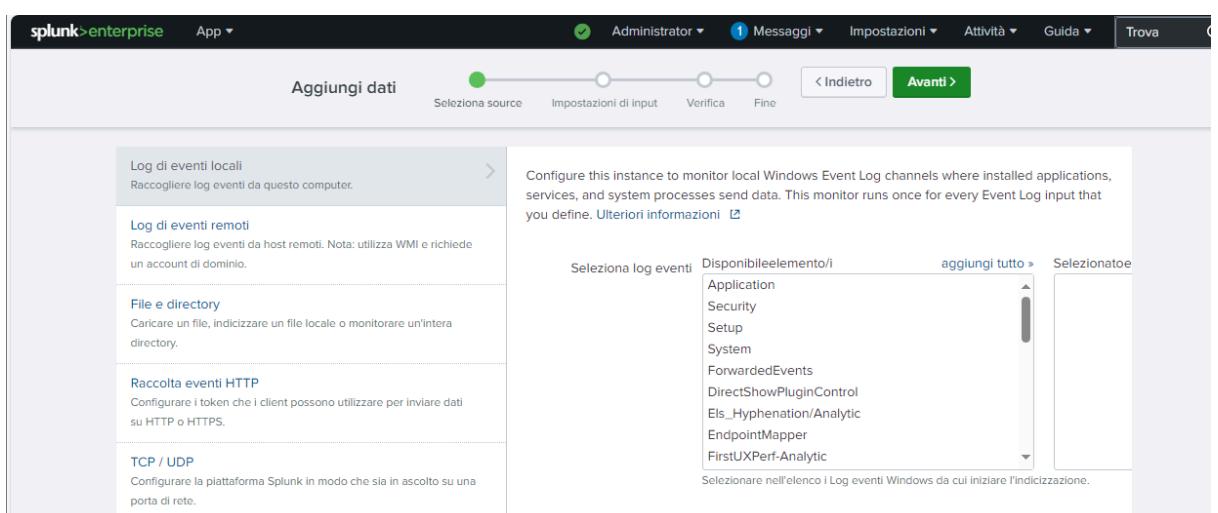


Figura 1: Procedura guidata 'Add Data': selezione della tipologia di sorgente 'Local Event Logs' (Log di eventi locali) per acquisire i dati dall'endpoint Windows.

2.2 Selezione dei Canali

Sono stati selezionati i canali standard di Windows, inclusi **Application**, **Security**, e **System**, per garantire una visibilità completa sugli eventi di sistema.

The screenshot shows a user interface for selecting log events. On the left, a list of available Windows log channels is shown: Application, Security, Setup, System, ForwardedEvents, DirectShowPluginControl, Els_Hyphenation/Analytic, EndpointMapper, and FirstUXPerf-Analytic. An 'aggiungi tutto' button is at the top right of this list. To the right, a vertical scroll bar indicates more items are present. A second column lists selected channels: Application, DirectShow, Els_Hyper, EndpointMa, FirstUXPerf, ForwardedE, HardwareE, IHM_Debug, and Intel-iaLPSS. Below the list is a note: "Selezionare nell'elenco i Log eventi Windows da cui iniziare l'indicizzazione." (Select in the list the Windows event logs from which to start indexing).

Figura 2: Menu di selezione dei log: inclusione dei canali standard di Windows (Application, Security, System) nel perimetro di monitoraggio.

2.3 Configurazione dell'Input

- **Host:** Il nome host è stato rilevato come **DESKTOP-8CAJRT0**.
- **Indice:** È stato creato e configurato un indice personalizzato denominato **prove** per segregare i dati di questo laboratorio.

The screenshot shows the input settings configuration. It includes fields for 'Valore campo Host' containing 'DESKTOP-8CAJRT0', an 'Indice' dropdown set to 'prove', and a link 'Crea un nuovo indice' (Create a new index). The 'Indice' dropdown has a downward arrow indicating it is a dropdown menu.

Figura 4: Input Settings: configurazione dell'Host (DESKTOP-8CAJRT0) e assegnazione dei dati all'indice personalizzato 'prove' per la segregazione dei log dell'esercizio.

3. Analisi dei Risultati (Findings)

La ricerca di convalida è stata effettuata utilizzando la query SPL (Search Processing Language): `index="prove"`.

L'output conferma che l'ingestione è attiva. Sono stati rilevati **6 eventi** nel periodo di campionamento.

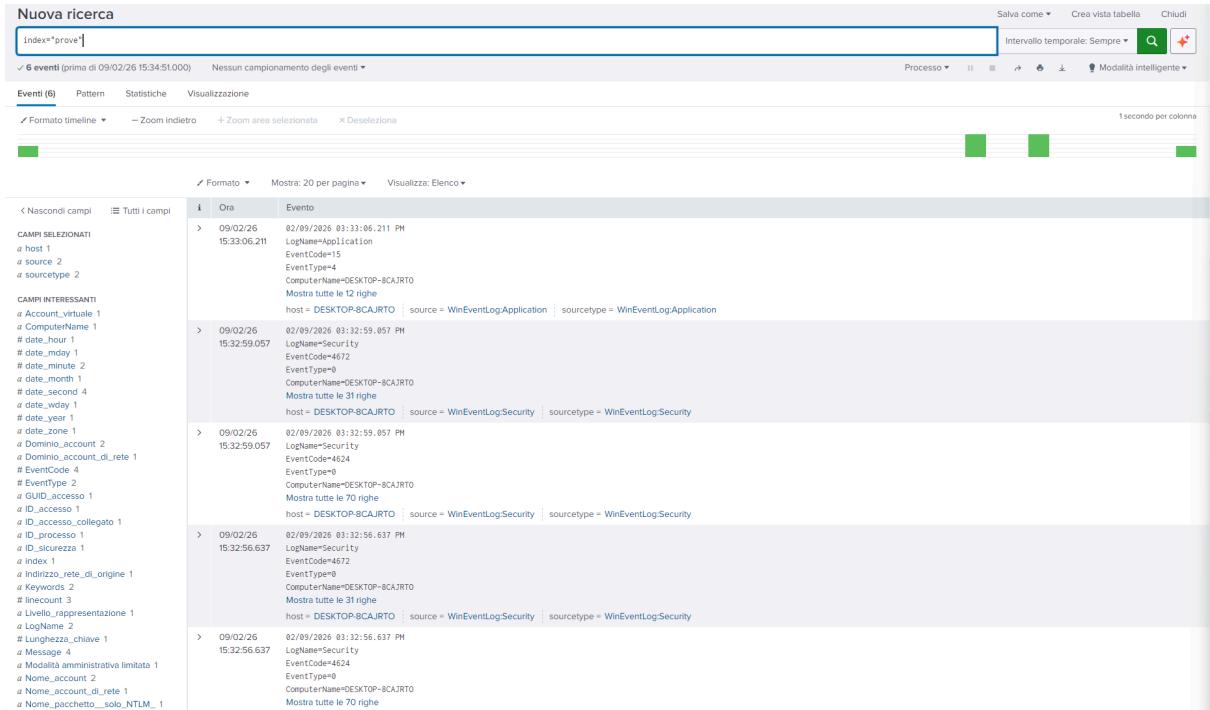


Figura 5: Convalida dell'ingestione: esecuzione della query `index='prove'`. La timeline conferma la ricezione di eventi critici, tra cui il Logon Success (EventCode 4624) e l'assegnazione di privilegi speciali (EventCode 4672).

Dettaglio Eventi Rilevati

Dall'analisi della Figura 5 emergono i seguenti dati tecnici:

1. **EventCode 4624 (Logon Success):**
 - **Source:** `WinEventLog:Security`
 - **Significato:** Indica che un account ha effettuato l'accesso con successo.
2. **EventCode 4672 (Special Privileges Assigned):**
 - **Source:** `WinEventLog:Security`
 - **Significato:** Questo evento, generato contestualmente al logon (stesso timestamp), indica che all'account sono stati assegnati privilegi amministrativi.
3. **EventCode 15 (Application Log):**
 - **Source:** `WinEventLog:Application`
 - **Significato:** Evento generico di livello applicativo.

4. Conclusion

L'esercitazione è stata completata con successo. La piattaforma Splunk sta correttamente monitorando l'endpoint DESKTOP-8CAJRT0 e i dati vengono scritti nell'indice prove. La presenza degli EventCode 4624 e 4672 conferma che il sistema di auditing di sicurezza è attivo.