

Configurazione della Data Ingestion in Tempo Reale su Splunk

1. Introduzione e Obiettivi

L'obiettivo di questa sessione di laboratorio è stato il passaggio da un approccio statico (il semplice caricamento di file) a un approccio dinamico e continuo: la **Modalità Monitor**. A differenza dell'upload manuale, la funzione "Monitor" di Splunk permette di sorvegliare file, directory, porte di rete o script in tempo reale.

In questo scenario, il mio compito è configurare un input di dati che osservi attivamente i log di sistema (o un'altra fonte dati presente nella macchina virtuale) e indicizzarli non appena vengono scritti. Questo è il cuore del funzionamento di un SIEM (Security Information and Event Management).

2. Ambiente e Strumenti Utilizzati

Per l'esecuzione dell'esercizio ho utilizzato i seguenti strumenti:

- **Virtualizzazione:** Oracle VirtualBox.
- **Sistema Operativo Guest:** Windows, dove risiede l'istanza Splunk.
- **Software Target:** Splunk Enterprise (versione Web accessibile via browser su porta 8000).
- **Browser:** Edge per l'interazione con la GUI di Splunk.

3. Configurazione

Accesso alla Sezione "Add Data"

Ho iniziato loggandomi nell'interfaccia web di Splunk. Dalla dashboard principale, ho navigato verso le impostazioni per l'aggiunta dei dati.

Ho cliccato sull'icona **Monitora** (Monitor) per iniziare la configurazione di un input locale.

Quale dati vuoi inviare alla piattaforma Splunk?

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

Barra di ricerca

Search


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 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

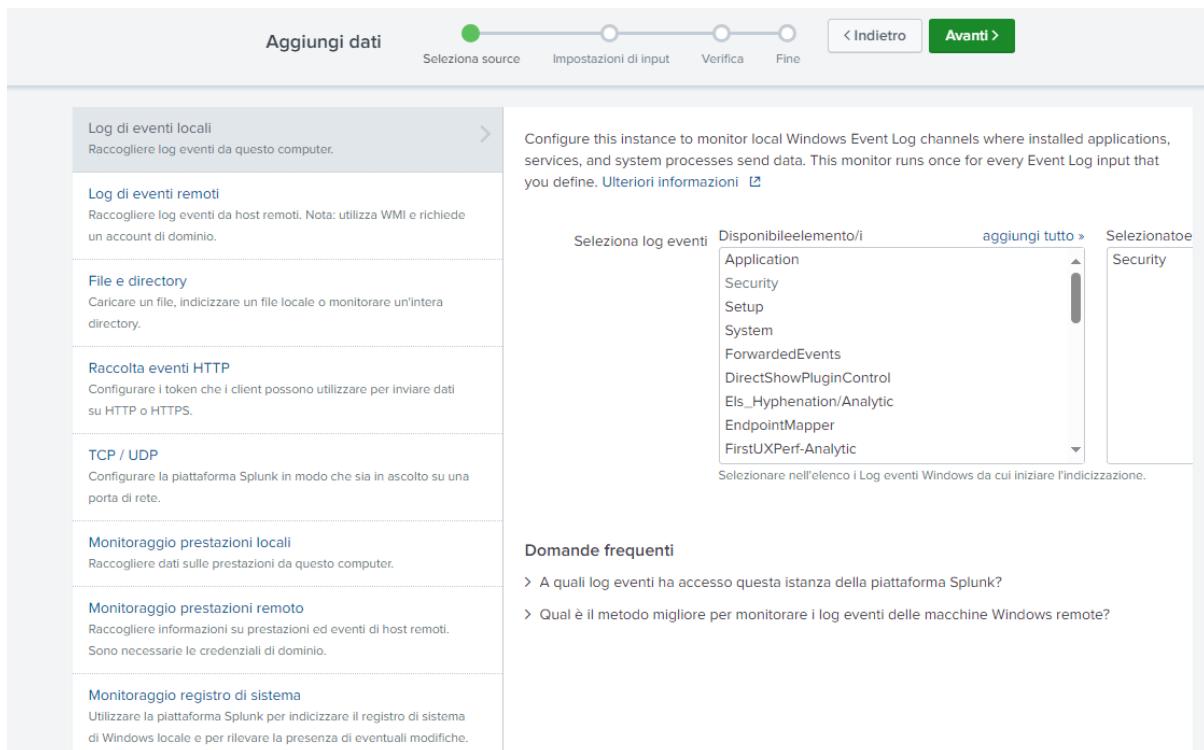
Selezione dei "Local Event Logs" (Log Eventi Locali)

Una volta all'interno del menu di configurazione, invece di selezionare file specifici, ho diretto la mia attenzione alla colonna di sinistra. Qui ho individuato e selezionato la voce Log di eventi locali.

Questa opzione è fondamentale in ambienti Windows perché permette a Splunk di interfacciarsi direttamente con il registro degli eventi di sistema (Event Viewer) senza dover puntare a file .evtx statici.

Azione:

1. Nel menu a sinistra, ho cliccato su **Log di eventi locali**.
2. Nella lista che è apparsa al centro (Available Logs), ho selezionato le tipologie di eventi che desideravo monitorare. Per questo esercizio, ho spuntato:
 - a. **Security** (per i tentativi di accesso e audit)
3. Ho verificato che la raccolta fosse impostata per iniziare immediatamente.



Configurazione delle Impostazioni di Input (Input Settings)

Dopo aver selezionato la sorgente sono arrivato alla schermata di configurazione dei metadati. Questo passaggio è cruciale per etichettare correttamente i dati prima che entrino nel database di Splunk.

Come si vede nello screenshot sottostante, ho configurato i seguenti parametri:

- Host:** Il sistema ha precompilato il campo con il valore DESKTOP-8CAJRT0. Ho confermato questa impostazione, poiché permette di identificare univocamente che i log provengono da questa specifica macchina virtuale.
- Indice:** Ho mantenuto l'impostazione su Default. In Splunk, l'indice di default corrisponde all'indice **main**. Sebbene in produzione si tenda a creare indici separati (es. windows_logs), per questo laboratorio l'indice principale è la destinazione corretta.

Aggiungi dati

Scegliere la sorgente Impostazioni di input Verifica Fine

Indietro Verifica >

Impostazioni di input

In alternativa, impostare obiettivi personalizzati di input per questo input di dati come segue:

Host:
Quando le particelle sono indicate da un solo nome, questo serve come un nome "base". Il campo host deve essere il nome della macchina su cui ha iniziato l'input di input così determinate le opzioni di configurazione disponibili. Vedere informazioni?

Nome host: DESKTOP-BCAURTO

Indice:
Le particelle Splunk archiviano molti eventi come eventi nell'indice selezionato. Vedere l'elenco di un indice "scartato" come destinazione se si hanno problemi a determinare un'ottima legge per i propri dati. Un indice scartato consente di risolvere i problemi a livello di configurazione senza conseguenze negative sugli indici di produzione. È sempre possibile modificare questa impostazione in un secondo momento. (Ultima modifica: 18

Indice: Desktop * Crea un nuovo indice

Domande frequenti:

- > Come funzionano gli indici?
- > Come faccio a sapere quando creare o utilizzare più indici?

Una volta verificate queste impostazioni, ho cliccato su **Verifica** e successivamente ho confermato l'operazione per avviare immediatamente l'ingestione.

Verifica e Analisi dei Log in Tempo Reale

Per confermare il successo dell'operazione, ho cliccato su **Avvia ricerca**. L'obiettivo era verificare non solo la presenza dei dati, ma la qualità del "parsing" (ovvero come Splunk legge e separa i campi).

L'esito è stato positivo. Splunk ha iniziato a mostrare eventi in tempo reale. Ho analizzato nel dettaglio un evento specifico catturato durante la sessione, come mostrato nelle immagini seguenti.

i	Ora	Evento	
▼	11/02/26 16:43:11.913	02/11/2026 04:43:11.913 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-8CAJRT0 Mostra tutte le 31 righe	
Azioni evento ▾			
Tipologia ▾			
	<input checked="" type="checkbox"/> Campo	Valore	Azioni
Selezionato			▼
	<input checked="" type="checkbox"/> host ▾	DESKTOP-8CAJRT0	▼
	<input checked="" type="checkbox"/> source ▾	WinEventLog:Security	▼
	<input checked="" type="checkbox"/> sourcetype ▾	WinEventLog:Security	▼
Evento			▼
	<input type="checkbox"/> ComputerName ▾	DESKTOP-8CAJRT0	▼
	<input type="checkbox"/> Dominio_account ▾	NT AUTHORITY	▼
	<input type="checkbox"/> EventCode ▾	4672	▼
	<input type="checkbox"/> EventType ▾	0	▼
	<input type="checkbox"/> ID_accesso ▾	0x3E7	▼
	<input type="checkbox"/> ID_sicurezza ▾	S-1-5-18	▼
	<input type="checkbox"/> Keywords ▾	Controllo riuscito	▼
	<input type="checkbox"/> LogName ▾	Security	▼
	<input type="checkbox"/> 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 SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege	▼
	<input type="checkbox"/> Nome_account ▾	SYSTEM	▼
	<input type="checkbox"/> OpCode ▾	Informazioni	▼
	<input type="checkbox"/> Privilegi ▾	SeAssignPrimaryTokenPrivilege	▼
	<input type="checkbox"/> RecordNumber ▾	3472	▼
	<input type="checkbox"/> SourceName ▾	Microsoft Windows security auditing.	▼

Dallo screenshot si evince che Splunk ha indicizzato correttamente un evento critico di sicurezza:

- **Timestamp:** 02/11/2026 04:43:11 PM (Orario della VM).
 - **SourceType:** WinEventLog:Security. Questo conferma che stiamo leggendo il registro di Sicurezza di Windows.
 - **Event Code 4672:** Ho espanso i dettagli dell'evento e notato il codice 4672. Questo codice corrisponde a "**Special privileges assigned to new logon**".
 - **Account:** L'utente coinvolto è SYSTEM (NT AUTHORITY), il che indica un'operazione interna di alto livello del sistema operativo.

		viege SeLocalUserPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege
<input type="checkbox"/>	Nome_account ▾	SYSTEM
<input type="checkbox"/>	OpCode ▾	Informazioni
<input type="checkbox"/>	Privilegi ▾	SeAssignPrimaryTokenPrivilege
<input type="checkbox"/>	RecordNumber ▾	3472
<input type="checkbox"/>	SourceName ▾	Microsoft Windows security auditing.
<input type="checkbox"/>	TaskCategory ▾	Special Logon
<input type="checkbox"/>	Type ▾	Informazioni
Ora +	_time ▾	2026-02-11T16:43:11.913-01:00
Default	<input type="checkbox"/> index ▾	main
	<input type="checkbox"/> linecount ▾	31
	<input type="checkbox"/> punct ▾	//___.==_.==_.==_.tt\rt\rt---\rt_tt\rt
	<input type="checkbox"/> splunk_server ▾	DESKTOP-8CAJRTO

ho potuto verificare i metadati tecnici aggiuntivi:

- **index = main:** Conferma che la configurazione della Fase 3 è stata applicata correttamente.
- **Campi Estratti:** Sulla colonna di sinistra (la "Field Sidebar"), Splunk ha estratto automaticamente campi utili come ComputerName, EventCode, Privileges e OpCode. Questo dimostra che la modalità "Monitora" non si limita a copiare il testo, ma lo struttura rendendolo pronto per le query di analisi.

5. Conclusiones

L'esercizio si è concluso con successo.

1. Ho configurato un input di tipo "**Log di eventi locali**" per monitorare Security.
2. Ho verificato che i dati fluiscono nell'indice main con l'host corretto (DESKTOP-8CAJRTO).
3. Ho dimostrato la capacità di Splunk di interpretare eventi complessi (come l'EventCode 4672) in tempo reale, fornendo visibilità immediata sulle operazioni privilegiate del sistema operativo.

Questa configurazione rappresenta la base per qualsiasi attività di monitoraggio SIEM in ambiente Windows.