Monitoraggio Splunk

Obiettivo dell’attività

L'attività odierna si è focalizzata sull’esplorazione e configurazione della modalità **"Monitora"** in Splunk, una funzionalità chiave per acquisire e gestire i dati in tempo reale. Il compito assegnato prevedeva due obiettivi principali:

1. **Configurare la modalità "Monitora"** per acquisire specifici flussi di dati.
2. **Documentare l’intero processo** con screenshot che confermassero l’avvenuta configurazione e l’esecuzione corretta.

Introduzione alla modalità "Monitora" di Splunk

Splunk è una piattaforma software avanzata per la gestione e l'analisi dei dati generati da macchine. La sua capacità di raccogliere, indicizzare e visualizzare grandi volumi di dati provenienti da fonti diverse lo rende uno strumento essenziale per il monitoraggio IT, la sicurezza informatica e l'ottimizzazione delle performance aziendali. La modalità **"Monitora"** è una delle funzionalità chiave di Splunk, progettata per acquisire e indicizzare dati in tempo reale da file, directory e flussi dinamici.

L’obiettivo dell’attività è stato configurare correttamente la modalità "Monitora" in Splunk, esplorandone le caratteristiche principali e documentando il processo con screenshot che testimoniano il corretto funzionamento dello strumento.

Cos'è la modalità "Monitora"?

La modalità "Monitora" è progettata per raccogliere dati da file o directory in aggiornamento continuo, flussi di rete, e altre sorgenti dinamiche. Attraverso questa modalità, Splunk consente di:

- **Acquisire dati in tempo reale:** Ogni modifica o aggiornamento nelle fonti configurate viene immediatamente rilevato e processato.
- **Supportare fonti diverse:** La modalità è compatibile con file di log, dati strutturati (ad esempio, file CSV o JSON), e flussi di eventi generati da applicazioni o sistemi.
- **Indicizzare i dati:** I dati raccolti vengono automaticamente indicizzati e resi disponibili per analisi dettagliate.

Questa funzione è essenziale in contesti aziendali e operativi, come il monitoraggio delle performance dei sistemi, l'analisi dei log di sicurezza, e la gestione degli eventi di rete.

Preparazione dell’ambiente

Prima di procedere con la configurazione, sono state eseguite le seguenti operazioni:

- Avvio dell’ambiente Splunk.
- Identificazione delle fonti di dati da monitorare (ad esempio, file di log locali o remoti).
- Verifica dei permessi di accesso ai file di origine.

Svolgimento dell’attività

L’attività si è articolata nelle seguenti fasi principali:

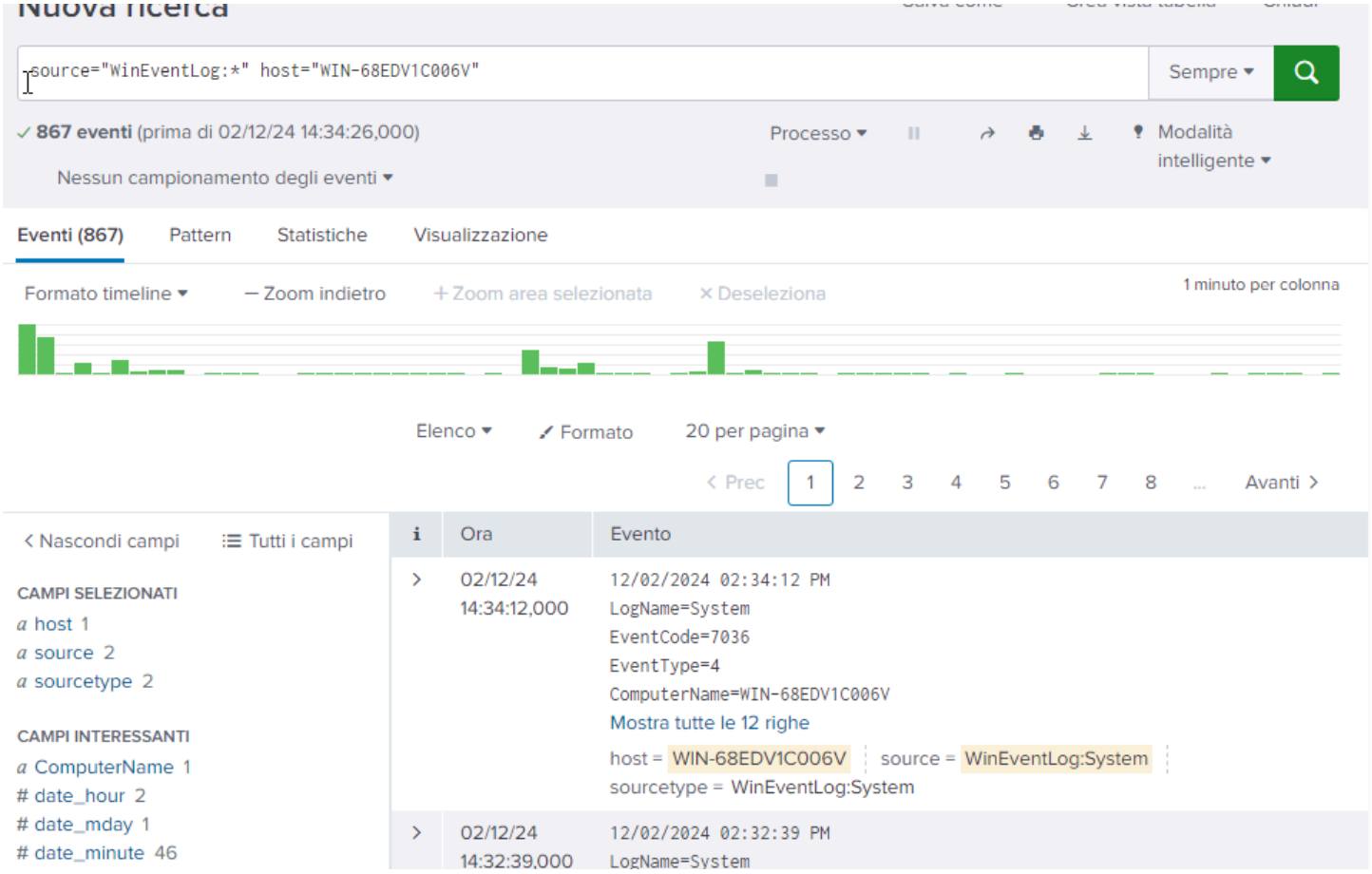
- **Preparazione della configurazione**
  Dopo aver avviato Splunk, si è selezionata l’opzione "Aggiungi dati" all'interno dell'interfaccia. La scelta della modalità "Monitora" è stata motivata dalla necessità di acquisire dati aggiornati in tempo reale da una fonte specifica, come una directory contenente file di log o un flusso continuo di eventi.
- **Selezione della fonte dei dati**
  È stata individuata una fonte dati appropriata per il test, configurandola per l'indicizzazione. In particolare, è stato scelto di monitorare una directory locale contenente file di log generati dinamicamente, simulando un ambiente operativo reale.
- **Configurazione degli indici**
  Durante il processo, è stato configurato un indice dedicato per organizzare i dati raccolti. Questa fase è stata essenziale per garantire una separazione logica dei dati e facilitarne la gestione e l'analisi successiva.
- **Verifica della raccolta dati**
  Dopo aver completato la configurazione, sono state eseguite delle ricerche di test utilizzando il linguaggio SPL (Search Processing Language) di Splunk per verificare che i dati fossero stati correttamente acquisiti e indicizzati. Gli screenshot allegati alla relazione mostrano i dati acquisiti in tempo reale e la loro visualizzazione tramite dashboard.

Risultati ottenuti

La configurazione della modalità "Monitora" è stata completata con successo, consentendo di acquisire dati dinamici e di indicizzarli in maniera efficiente. Gli strumenti analitici di Splunk

hanno permesso di visualizzare i dati raccolti e di interpretare le informazioni attraverso grafici e tabelle. Questo risultato ha evidenziato diversi punti di forza dello strumento:

- **Efficienza operativa:** La raccolta dei dati è avvenuta senza interruzioni, dimostrando l'affidabilità della modalità "Monitora".
- **Facilità di utilizzo:** L'interfaccia utente si è dimostrata intuitiva e ben progettata, rendendo la configurazione accessibile anche a chi si avvicina a Splunk per la prima volta.
- **Versatilità delle visualizzazioni:** Le dashboard generate hanno consentito una chiara rappresentazione dei dati, facilitando l'identificazione di pattern e anomalie.
- Gli screenshot allegati dimostrano il corretto funzionamento del monitoraggio e l'effettiva indicizzazione dei dati nel sistema Splunk.



Conclusioni

L'attività svolta ha consentito di approfondire l'utilizzo della modalità **"Monitora"** di Splunk, mettendo in evidenza l'importanza e le potenzialità della piattaforma nel contesto del monitoraggio in tempo reale. La configurazione è stata completata con successo, garantendo l'acquisizione di dati dinamici da fonti selezionate e la loro visualizzazione tramite strumenti di

analisi e ricerca. Questo processo ha confermato l'efficacia di Splunk nel trasformare dati grezzi in informazioni utili e facilmente consultabili.