# Configurazione della Modalità Monitora in Splunk

## Introduzione

Nell'ambito dell'esplorazione delle funzionalità di Splunk, l'esercizio odierno si è concentrato sulla configurazione della modalità Monitora per raccogliere e analizzare i log provenienti da una porta specifica (porta 9997). Questo tipo di configurazione è fondamentale per centralizzare i dati provenienti da diverse fonti e monitorare in tempo reale le attività di sistemi distribuiti.

L'obiettivo principale dell'esercizio era configurare correttamente la modalità Monitora su Splunk Enterprise e verificare che i log inviati dal Forwarder fossero ricevuti ed elaborati correttamente. Sono stati inclusi anche screenshot per documentare il processo e confermare l'avvenuta configurazione.

## Preparazione ambiente

Per eseguire l'esercizio, è stato predisposto un ambiente composto da due macchine virtuali collegate in rete interna:

- Splunk Enterprise : Installato su una macchina con indirizzo IP 10.0.0.3. Questa macchina funge da server centrale per la raccolta e l'analisi dei log.
- Splunk Universal Forwarder : Installato su una seconda macchina con indirizzo IP 10.0.0.2. Questa macchina è stata configurata per inoltrare i log verso Splunk Enterprise.

Prima di procedere con la configurazione, è stata verificata la connettività tra le due macchine tramite il comando ping e si è assicurato che la porta 9997 fosse aperta sul server Splunk Enterprise per consentire la ricezione dei dati. La preparazione dell'ambiente ha richiesto anche la verifica delle autorizzazioni necessarie per l'accesso ai log e la corretta installazione di Splunk Enterprise e del Forwarder.

## Raccolta dati dalla porta 9997 ed analisi dei log

Una volta completata la fase di preparazione, è stata avviata la configurazione della modalità Monitora su Splunk Enterprise. Di seguito sono descritte le attività svolte:

### Configurazione del listener sulla porta 9997

Sul server Splunk Enterprise (10.0.0.3), è stata abilitata la modalità Monitora per ricevere i dati inviati dal Forwarder tramite la porta 9997. Questa operazione è stata eseguita accedendo all'interfaccia web di Splunk e configurando il servizio di ascolto nella sezione dedicata alle impostazioni di input.

**Configurazione del Forwarder**

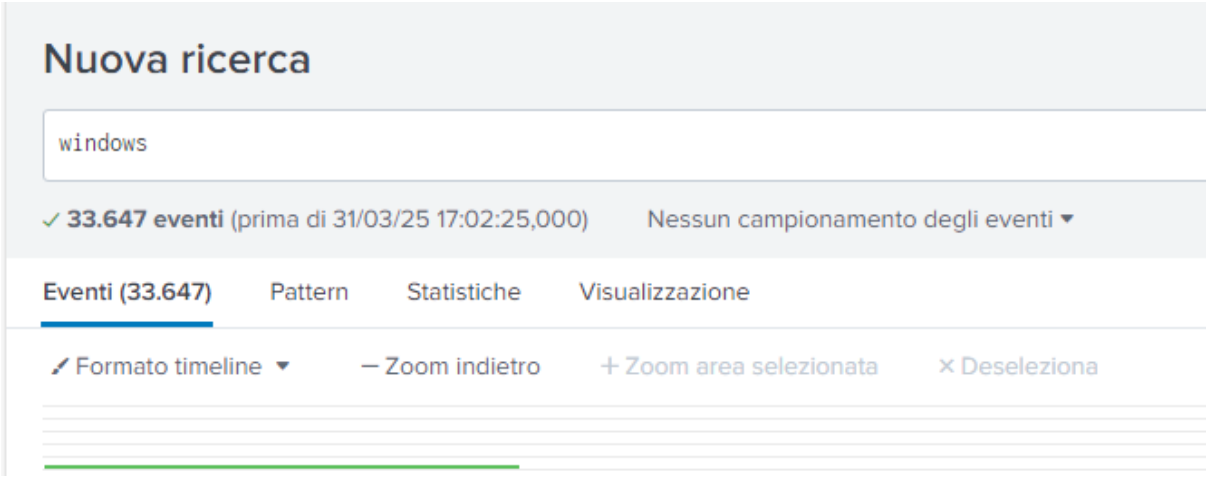
Sulla macchina con Splunk Universal Forwarder (10.0.0.2), è stato impostato l'inoltro dei log verso l'indirizzo IP del server Splunk Enterprise (10.0.0.3) utilizzando la porta 9997. I log selezionati per l'inoltro includevano file di sistema Windows, come quelli relativi a sicurezza, applicazioni e servizi.

**Verifica della ricezione dei dati**

Dopo aver completato la configurazione, è stata verificata la ricezione dei dati su Splunk Enterprise. Nell'interfaccia web di Splunk, è stato possibile visualizzare i log ricevuti e analizzarne il contenuto. Sono stati inclusi screenshot per documentare:

1. La schermata di configurazione della modalità Monitora .
2. La lista degli eventi ricevuti tramite la porta 9997.
3. Un esempio di analisi dei log, con dettagli sui campi estratti e sulle informazioni contenute nei log.

I log analizzati includevano informazioni relative a eventi di sistema, accessi utente e attività di servizi. Grazie alla modalità Monitora , è stato possibile centralizzare e monitorare in tempo reale queste informazioni, semplificando il processo di analisi.



| i | Ora | Evento |
|---|---|---|
| > | 31/03/25 16:03:56,000 | 03/31/2025 04:03:56 PM<br>... 2 lines omitted ...<br>EventType=0<br>ComputerName=DESKTOP-8CAJRTO<br>SourceName=Microsoft Windows security auditing.<br>Type=Informazioni<br>Mostra tutte le 31 righe<br>host = DESKTOP-8CAJRTO \| source = WinEventLog:Security \| sourcetype = WinEventLog:Security |
| > | 31/03/25 16:03:56,000 | ... 4 lines omitted ...<br>ComputerName=DESKTOP-8CAJRTO<br>SourceName=Microsoft Windows security auditing.<br>Type=Informazioni<br>... 31 lines omitted ...<br>ID processo: 0x294<br>Nome processo: C:\Windows\System32\services.exe<br>Mostra tutte le 70 righe<br>host = DESKTOP-8CAJRTO \| source = WinEventLog:Security \| sourcetype = WinEventLog:Security |
| > | 31/03/25 16:03:56,000 | 03/31/2025 04:03:56 PM<br>... 2 lines omitted ...<br>EventType=0<br>ComputerName=DESKTOP-8CAJRTO<br>SourceName=Microsoft Windows security auditing.<br>Type=Informazioni<br>Mostra tutte le 31 righe<br>host = DESKTOP-8CAJRTO \| source = WinEventLog:Security \| sourcetype = WinEventLog:Security |
| > | 31/03/25 16:03:56,000 | ... 4 lines omitted ...<br>ComputerName=DESKTOP-8CAJRTO<br>SourceName=Microsoft Windows security auditing.<br>Type=Informazioni<br>... 31 lines omitted ...<br>ID processo: 0x294<br>Nome processo: C:\Windows\System32\services.exe<br>Mostra tutte le 70 righe |

> 31/03/25 16:03:56,000

```
03/31/2025 04:03:56 PM
LogName=Security
EventCode=4672
EventType=0
ComputerName=DESKTOP-8CAJRTO
SourceName=Microsoft Windows security auditing.
Type=Informazioni
RecordNumber=3717
Keywords=Controllo riuscito
TaskCategory=Special Logon
OpCode=Informazioni
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
```

Comprimi

host = DESKTOP-8CAJRTO | source = WinEventLog:Security | sourcetype = WinEventLog:Security

**Conclusione**

L'esercizio di oggi ha permesso di acquisire familiarità con la configurazione della modalità Monitora in Splunk, dimostrando come sia possibile centralizzare e analizzare i log provenienti da diverse fonti. La configurazione della porta 9997 e l'utilizzo del Forwarder hanno reso possibile la raccolta efficiente dei dati, garantendo una visione completa delle attività di sistema.

La documentazione dell'esercizio tramite screenshot ha confermato l'avvenuta configurazione e la corretta ricezione dei log. Questa esperienza ha evidenziato l'importanza di Splunk come strumento per il monitoraggio e l'analisi dei dati in ambienti distribuiti, fornendo una solida base per ulteriori approfondimenti sulle funzionalità avanzate della piattaforma.