S10L1

UNIT 3

Marco Falchi

Consegna

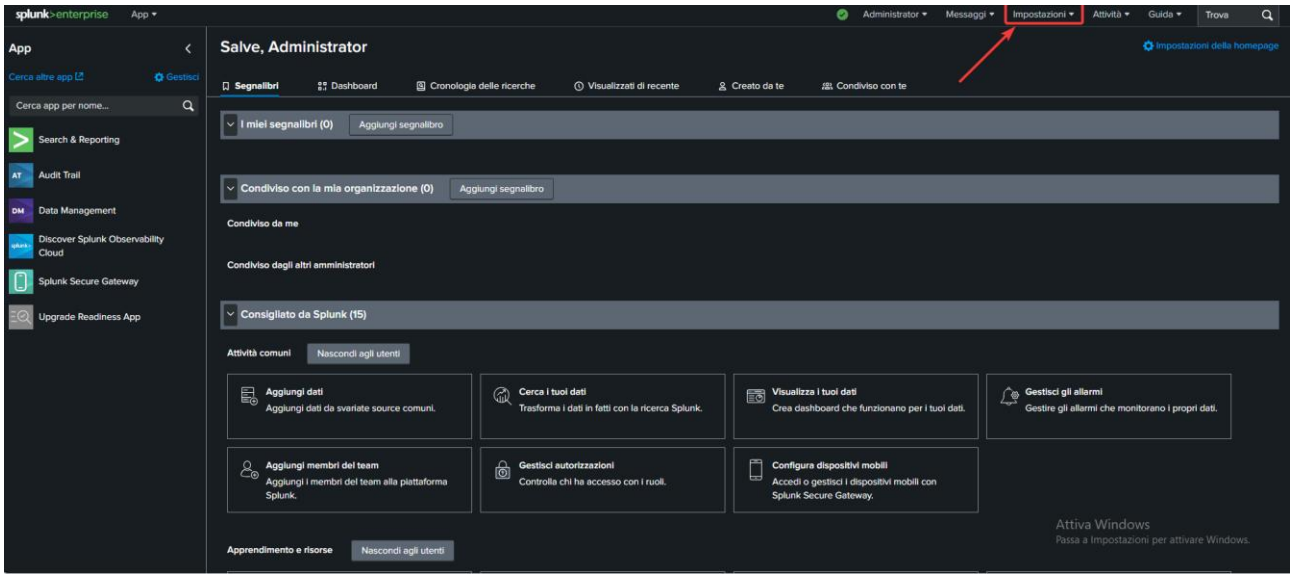
Esercizio di oggi: Configurazione della Modalità Monitora in Splunk

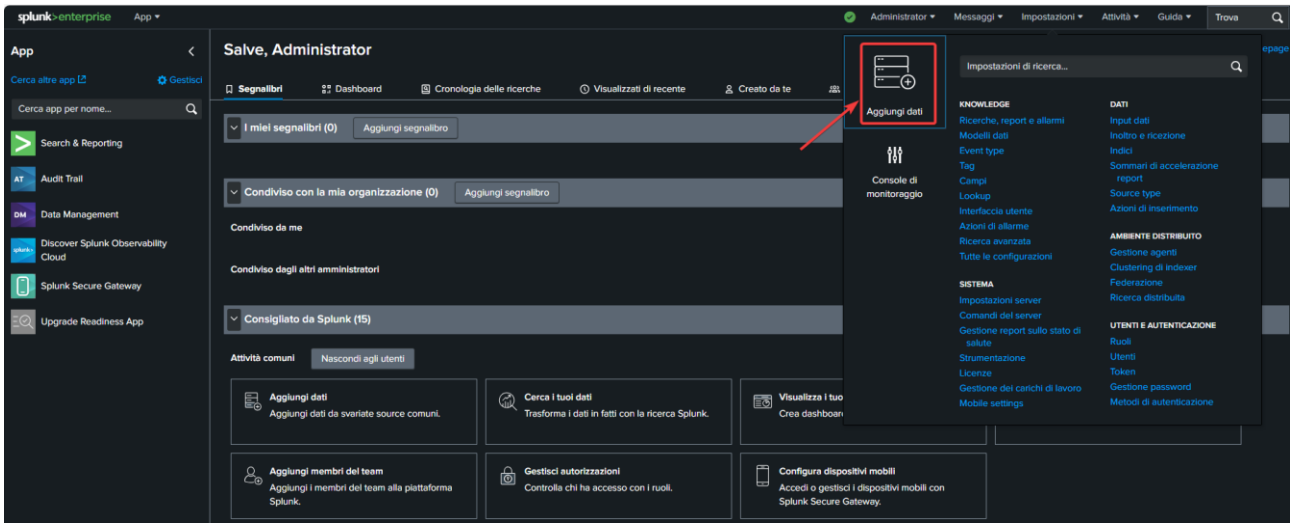
Abbiamo esplorato diverse funzionalità offerte da Splunk. Oggi ci concentreremo sulla modalità "Monitora". Il compito di oggi consiste nel configurare la modalità Monitora in Splunk e realizzare degli screenshot che confermino l'avvenuta configurazione.

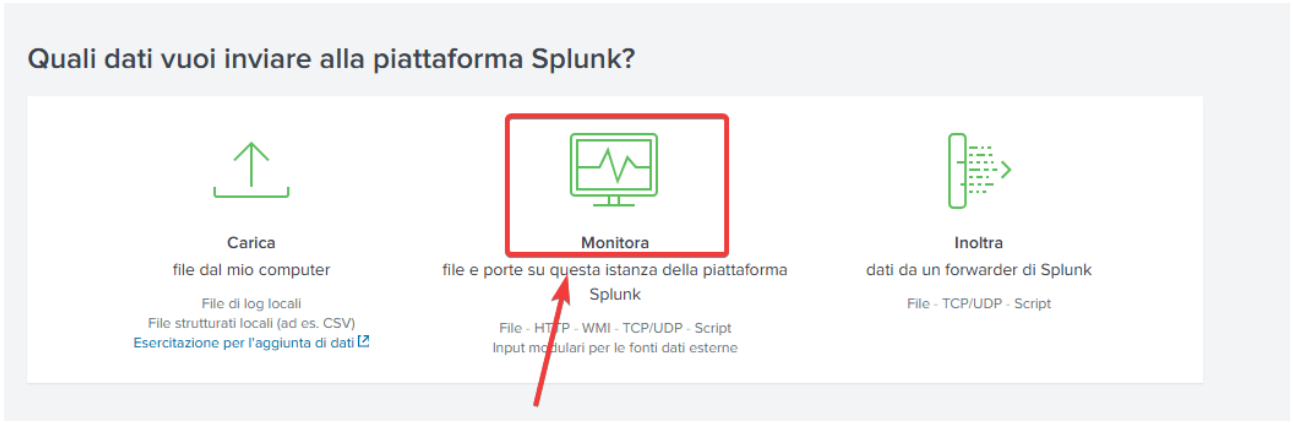
In breve: Lo studente dovrà configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.

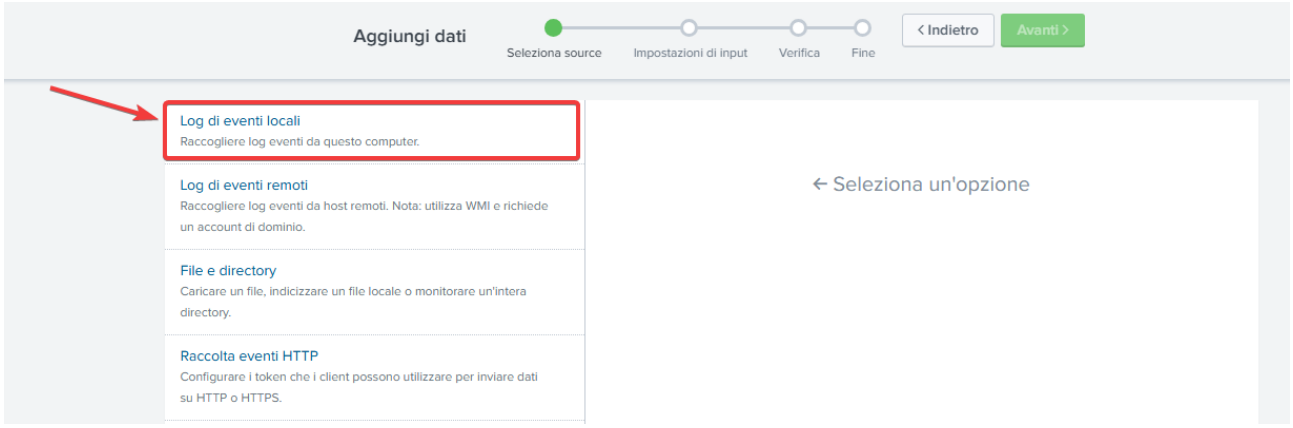
Esecuzione

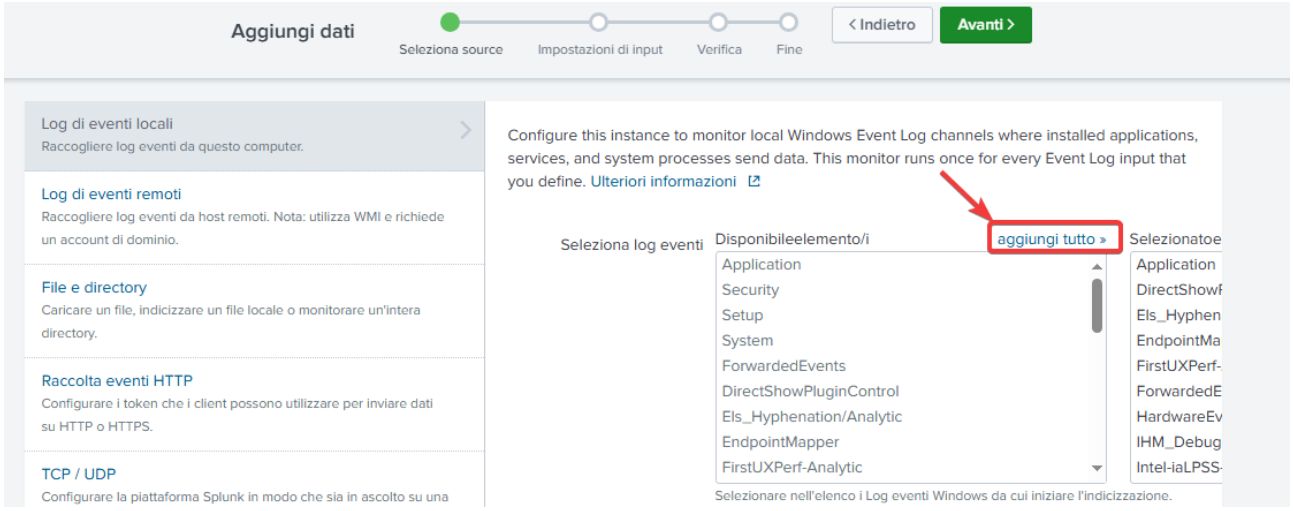
Seguo i passaggi nel seguente ordine come da screen per monitorare i log in tempo reale:

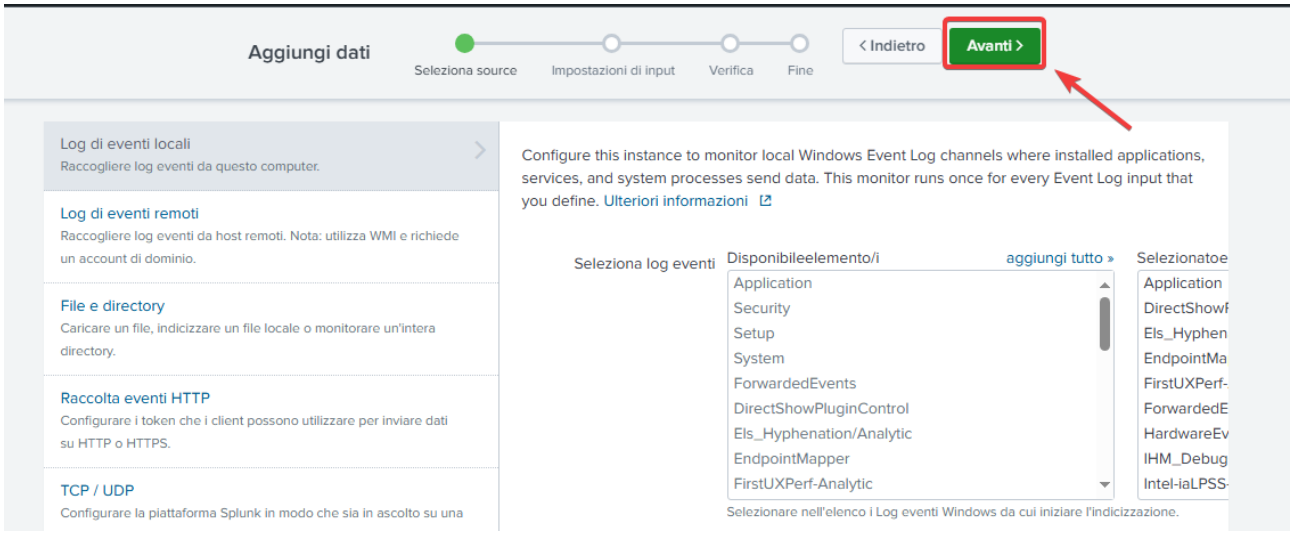



splunk>enterprise
App
Administrator
Messaggi
Impostazioni
Attività
Guida
Trova
App
Cerca altre app
Gestisci
Cerca app per nome...
Search & Reporting
Audit Trail
Data Management
Discover Splunk Observability Cloud
Splunk Secure Gateway
Upgrade Readiness App
Salve, Administrator
Segnalibri
Dashboard
Cronologia delle ricerche
Visualizzati di recente
Creato da te
I miei segnalibri (0)
Aggiungi segnalibro
Condiviso con la mia organizzazione (0)
Aggiungi segnalibro
Condiviso da me
Condiviso dagli altri amministratori
Consigliato da Splunk (15)
Attività comuni
Nascondi agli utenti
Aggiungi dati
Aggiungi dati da svariate source comuni.
Cerca i tuoi dati
Trasforma i dati in fatti con la ricerca Splunk.
Aggiungi membri del team
Aggiungi i membri del team alla piattaforma Splunk.
Gestisci autorizzazioni
Controlla chi ha accesso con i ruoli.
Configura dispositivi mobili
Accedi o gestisci i dispositivi mobili con Splunk Secure Gateway.
Aggiungi dati
Console di monitoraggio
Impostazioni di ricerca...
KNOWLEDGE
Ricerche, report e allarmi
Modelli dati
Event type
Tag
Campi
Lookup
Interfaccia utente
Azioni di allarme
Ricerca avanzata
Tutte le configurazioni
SISTEMA
Impostazioni server
Comandi del server
Gestione report sullo stato di salute
Strumentazione
Licenze
Gestione dei carichi di lavoro
Mobile settings
DATI
Input dati
Inoltro e ricezione
Indici
Sommari di accelerazione report
Source type
Azioni di inserimento
AMBIENTE DISTRIBUITO
Gestione agenti
Clustering di indexer
Federazione
Ricerca distribuita
UTENTI E AUTENTICAZIONE
Ruoli
Utenti
Token
Gestione password
Metodi di autenticazione

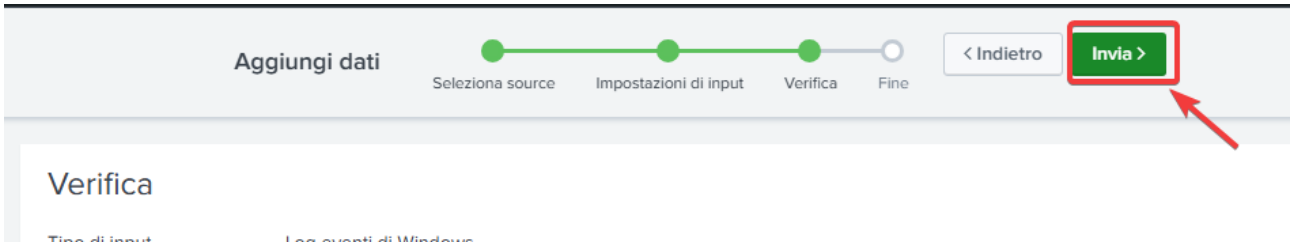

Quali dati vuoi inviare alla piattaforma Splunk?
Carica
file dal mio computer
File di log locali
File strutturati locali (ad es. CSV)
Esercitazione per l'aggiunta di dati
Monitora
file e porte su questa istanza della piattaforma Splunk
File - HTTP - WMI - TCP/UDP - Script
Input modulari per le fonti dati esterne
Inoltra
dati da un forwarder di Splunk
File - TCP/UDP - Script

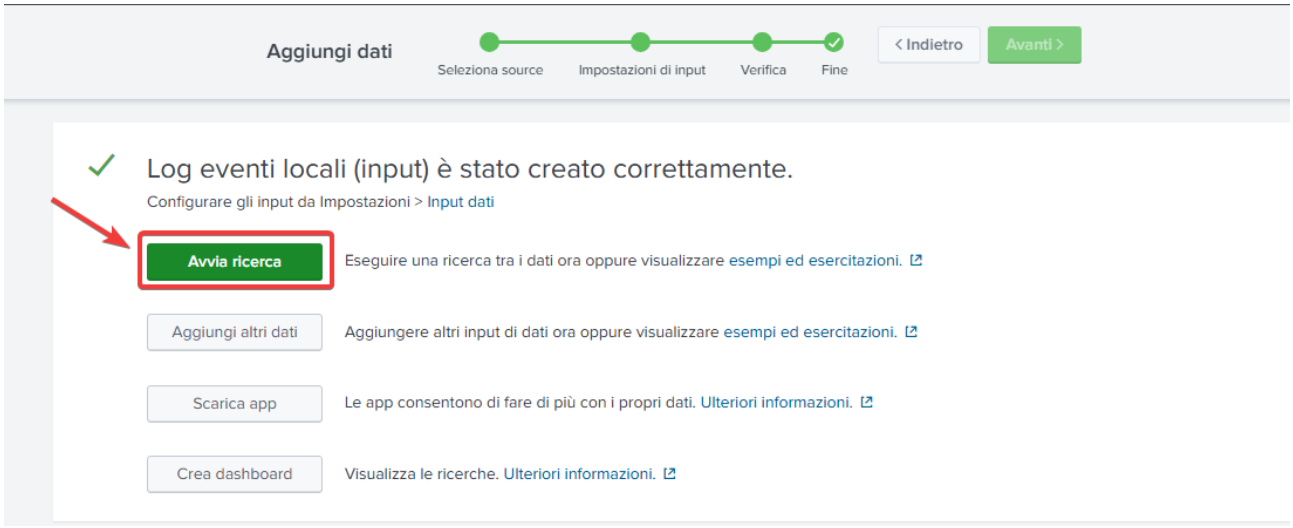

Aggiungi dati
Seleziona source
Impostazioni di input
Verifica
Fine
< Indietro
Avanti >
Log di eventi locali
Raccogliere log eventi da questo computer.
Log di eventi remoti
Raccogliere log eventi da host remoti. Nota: utilizza WMI e richiede un account di dominio.
File e directory
Caricare un file, indicizzare un file locale o monitorare un'intera directory.
Raccolta eventi HTTP
Configurare i token che i client possono utilizzare per inviare dati su HTTP o HTTPS.
← Seleziona un'opzione


Aggiungi dati
Seleziona source
Impostazioni di input
Verifica
Fine
< Indietro
Avanti >
Log di eventi locali
Raccogliere log eventi da questo computer.
Log di eventi remoti
Raccogliere log eventi da host remoti. Nota: utilizza WMI e richiede un account di dominio.
File e directory
Caricare un file, indicizzare un file locale o monitorare un'intera directory.
Raccolta eventi HTTP
Configurare i token che i client possono utilizzare per inviare dati su HTTP o HTTPS.
TCP / UDP
Configurare la piattaforma Splunk in modo che sia in ascolto su una
Configure this instance to monitor local Windows Event Log channels where installed applications, services, and system processes send data. This monitor runs once for every Event Log input that you define. Ulteriori informazioni
Seleziona log eventi
Disponibileelemento/i
aggiungi tutto »
Selezionatoe
Application
Security
Setup
System
ForwardedEvents
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
Selezionare nell'elenco i Log eventi Windows da cui iniziare l'indicizzazione.

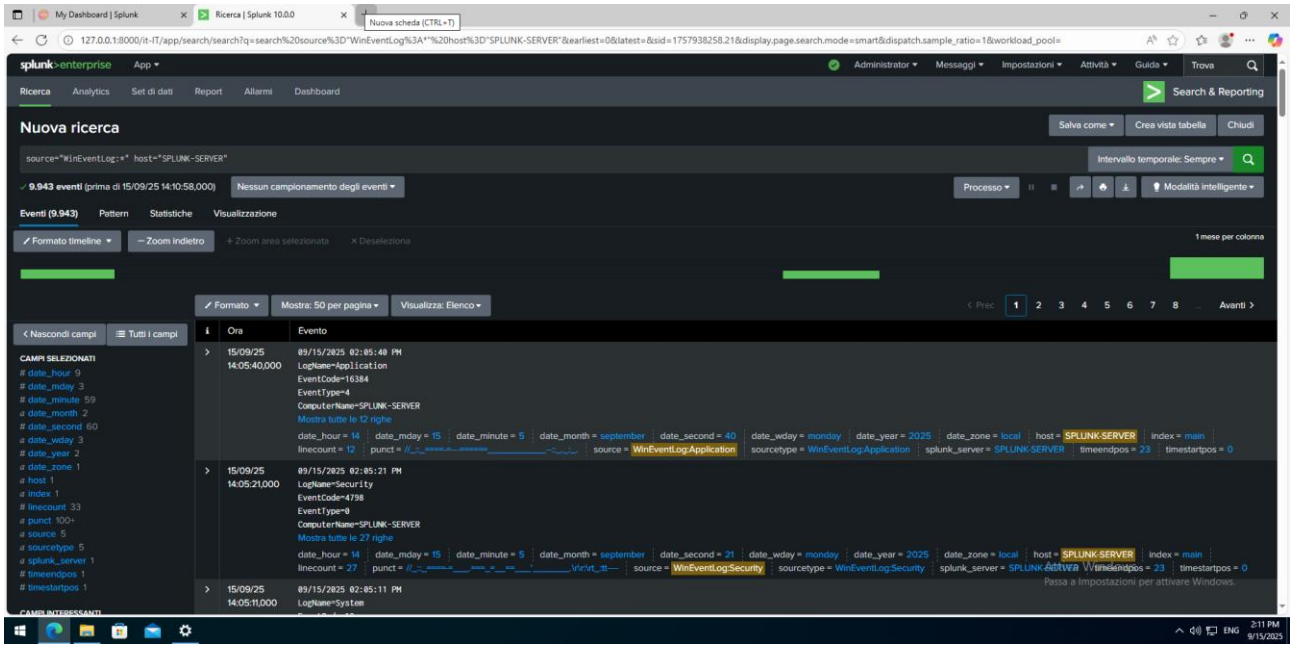

Aggiungi dati
Seleziona source
Impostazioni di input
Verifica
Fine
< Indietro
Avanti >
Log di eventi locali
Raccogliere log eventi da questo computer.
Log di eventi remoti
Raccogliere log eventi da host remoti. Nota: utilizza WMI e richiede un account di dominio.
File e directory
Caricare un file, indicizzare un file locale o monitorare un'intera directory.
Raccolta eventi HTTP
Configurare i token che i client possono utilizzare per inviare dati su HTTP o HTTPS.
TCP / UDP
Configurare la piattaforma Splunk in modo che sia in ascolto su una
Configure this instance to monitor local Windows Event Log channels where installed applications, services, and system processes send data. This monitor runs once for every Event Log input that you define. Ulteriori informazioni
Seleziona log eventi
Disponibileelemento/i
aggiungi tutto »
Selezionatoe
Application
Security
Setup
System
ForwardedEvents
DirectShowPluginControl
Els_Hyphenation/Analytic
EndpointMapper
FirstUXPerf-Analytic
Selezionare nell'elenco i Log eventi Windows da cui iniziare l'indicizzazione.


Aggiungi dati
Seleziona source
Impostazioni di input
Verifica
Fine
< Indietro
Verifica >
Impostazioni di input
In alternativa, impostare ulteriori parametri di input per questo input di dati come segue:

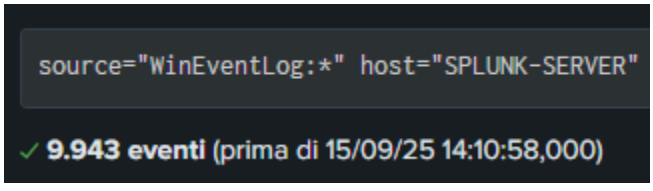

Aggiungi dati
Seleziona source
Impostazioni di input
Verifica
Fine
< Indietro
Invia >
Verifica



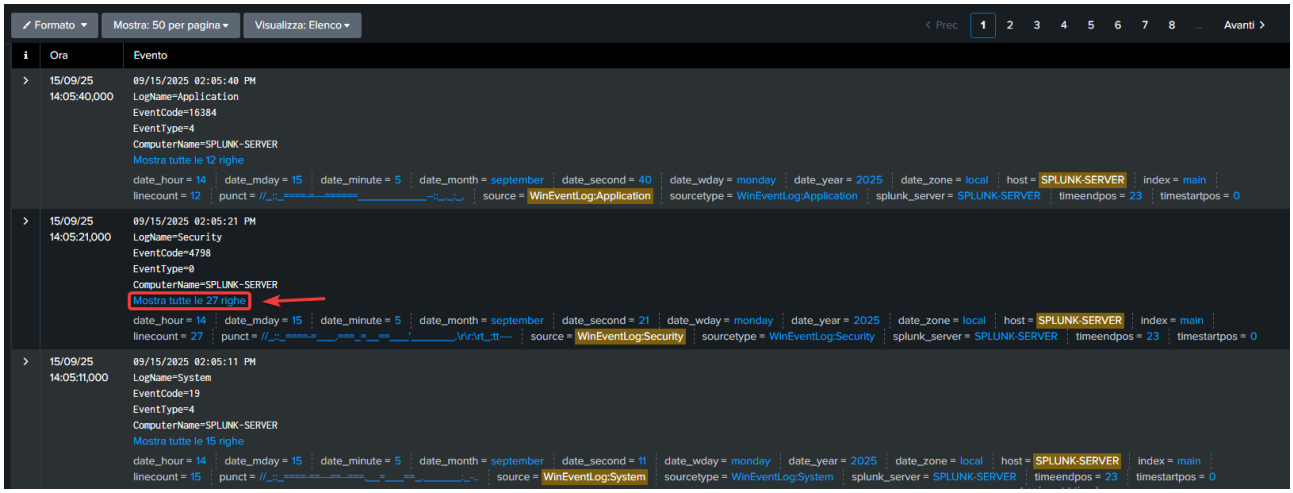
Otteniamo così la schermata di risultato come richiesto da consegna

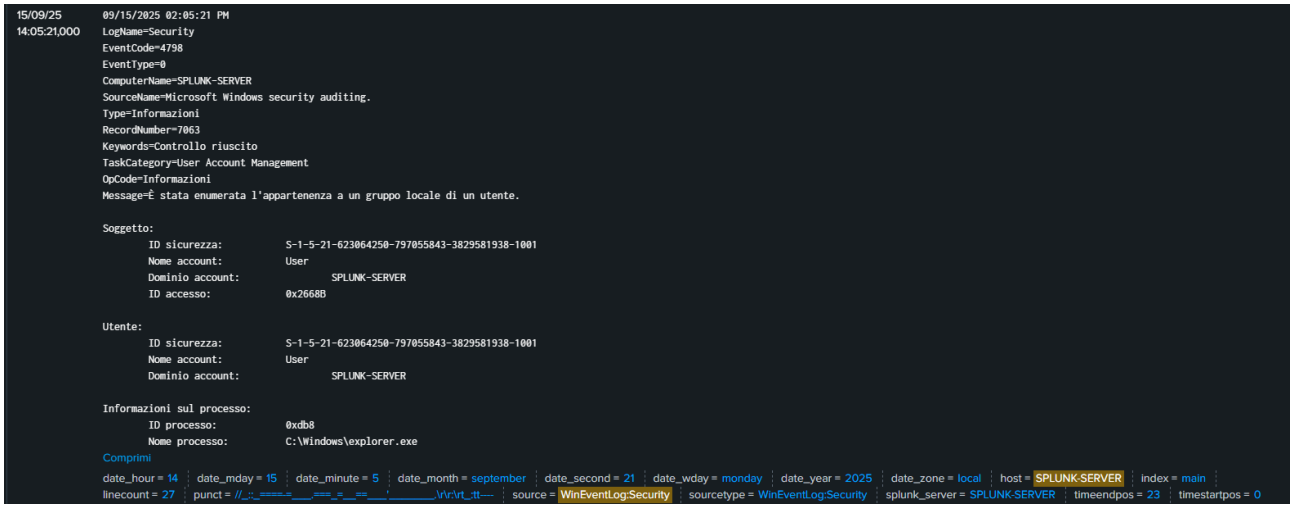


La presenza degli eventi log mostra il corretto funzionamento del procedimento con Splunk della sezione Monitora. Sono presenti 9.9943 eventi



Possiamo anche monitorare il singolo evento log cliccando sul “Mostra tutte le righe (numero righe)





Il log si tratta di un evento di sicurezza di Windows monitorato da **Splunk**.

Informazioni generali sull'evento

- **Data e ora:** 15/09/25 alle 02:05:21 PM.
- **Nome del log:** Security (Sicurezza).
- **ID evento:** 4798.
- **Computer:** SPLUNK-SERVER.
- **Origine:** Microsoft Windows security auditing.
- **Parola chiave:** Controllo riuscito (Success Audit).

- **Messaggio:** È stato enumerata l'appartenenza a un gruppo locale di un utente.

Il log indica che una richiesta di enumerare (cioè elencare) l'appartenenza ai gruppi di un utente è stata completata con successo.

Questo è un evento di routine che può verificarsi per diversi motivi, ad esempio quando un amministratore controlla i permessi di un utente o quando un'applicazione ha bisogno di verificare le sue autorizzazioni.

Dettagli su Utente e Processo

Soggetto (Utente che ha effettuato l'azione)

- **ID sicurezza:** S-1-5-21-623064259-757653843-3829581938-1001.
- **Nome utente:** User.
- **Dominio account:** SPLUNK-SERVER.

Questo è l'utente che ha avviato l'azione. L'ID di sicurezza è un identificatore univoco, mentre il nome utente e il dominio forniscono un'identificazione più leggibile.

Processo (Programma che ha generato l'azione)

- **ID processo:** 0xd80.
- **Nome processo:** C:\Windows\explorer.exe.

Questa è un'informazione fondamentale. Il processo che ha eseguito l'azione di enumerazione è explorer.exe, ovvero il **processo di gestione della shell di Windows**. Questo rafforza l'idea che l'azione sia probabilmente una richiesta legittima, come un'interfaccia utente che visualizza le proprietà di un utente.

In sintesi, il log dice che un utente chiamato "User", tramite il processo explorer.exe, ha verificato con successo quali gruppi locali sono associati a un altro utente.