
splunk>

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.

# Cos’è Splunk?

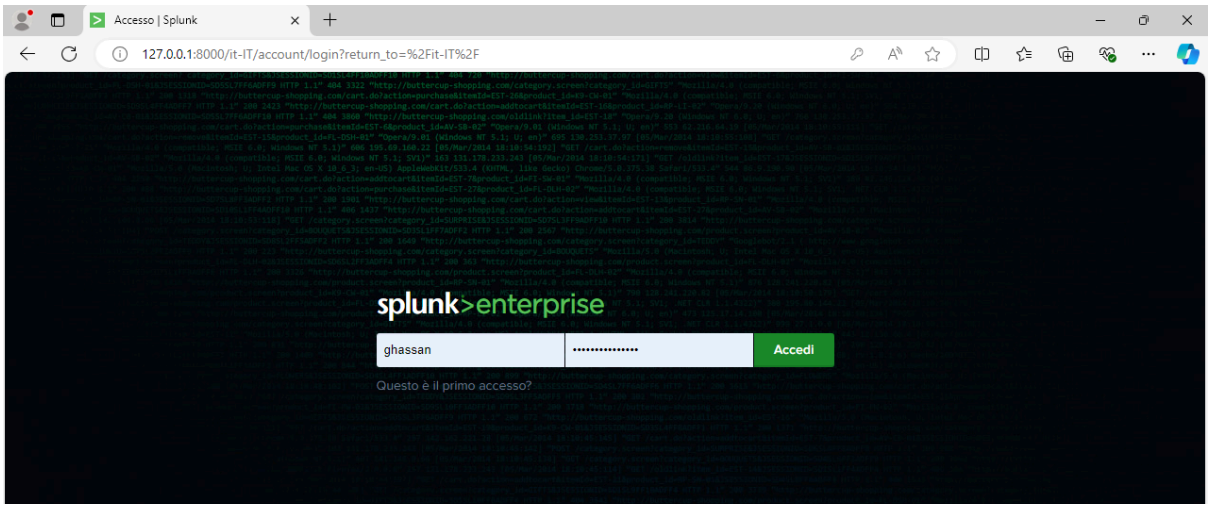
Splunk è una piattaforma software per il monitoraggio, l'analisi e la visualizzazione in tempo reale di dati generati da macchine, come log di sistema, eventi, metriche o dati provenienti da applicazioni. Il suo obiettivo principale è trasformare enormi volumi di dati non strutturati o semi-strutturati in informazioni utili.

Splunk raccoglie i dati da una vasta gamma di fonti, come server, applicazioni, dispositivi di rete e sensori IoT. Una volta acquisiti, li indicizza, rendendoli facilmente ricercabili. Gli utenti possono quindi interrogare i dati con un linguaggio di ricerca (SPL - Search Processing Language) per trovare anomalie, analizzare trend, monitorare sistemi o generare dashboard e report interattivi.

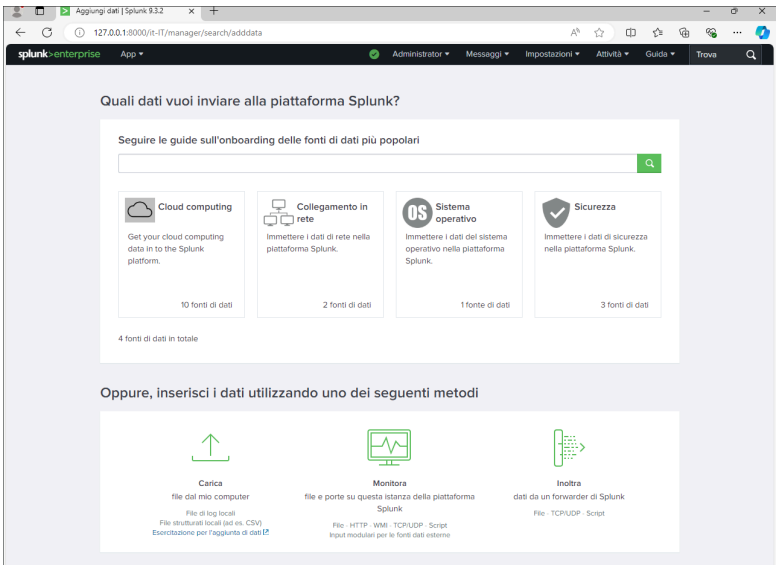
Ad esempio, è utilizzato per rilevare errori, analizzare la sicurezza informatica, ottimizzare le prestazioni o monitorare l'infrastruttura IT. La sua forza sta nella capacità di gestire enormi quantità di dati in tempo reale e di renderli comprensibili attraverso visualizzazioni intuitive.

# Come configurare Splunk ?

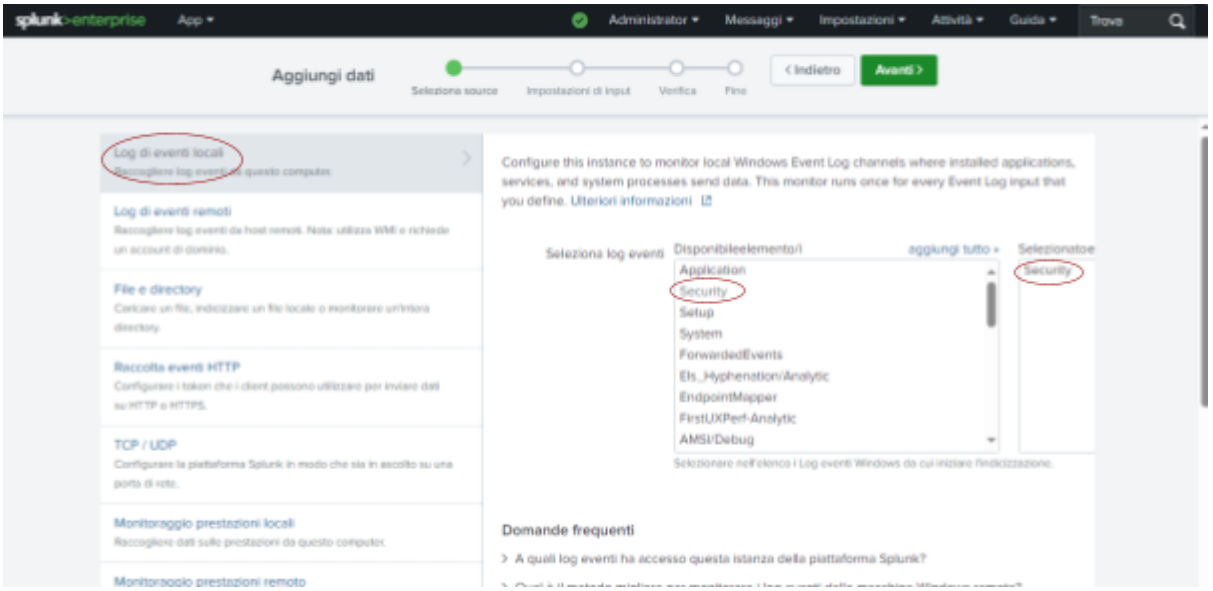
Iniziamo la nostra configurazione accedendo a Splunk



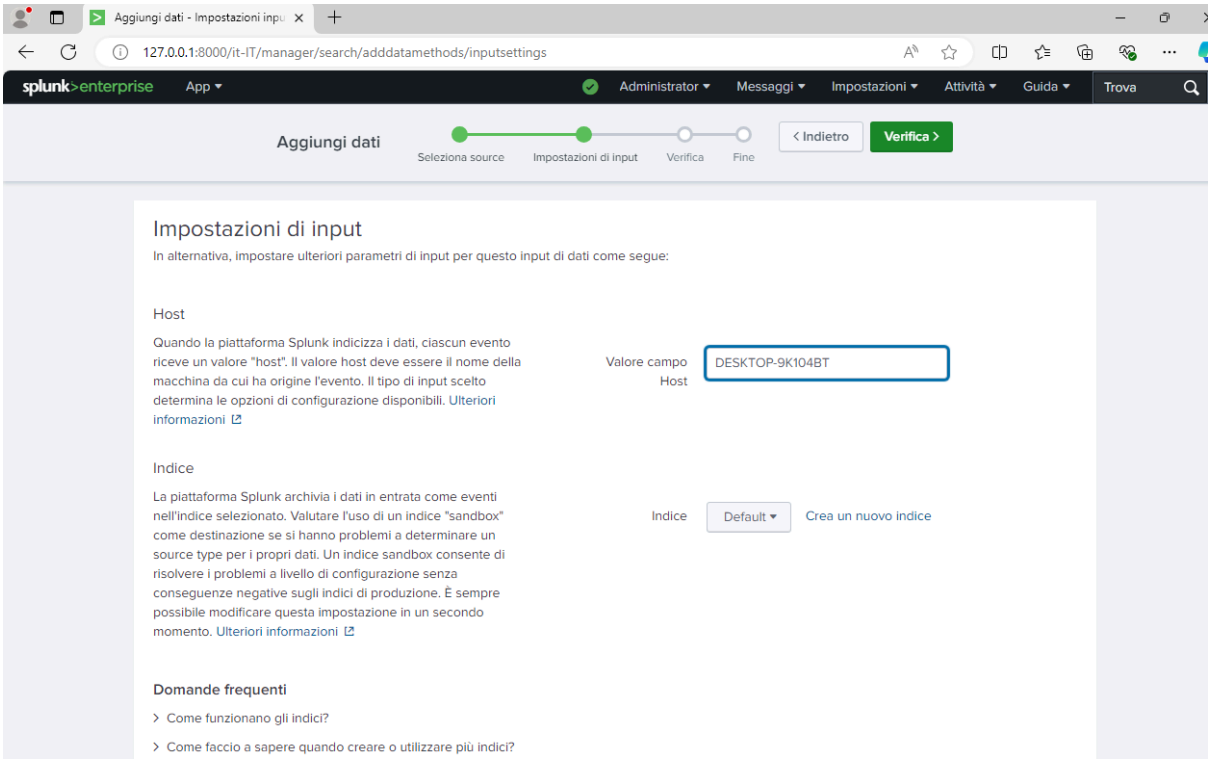

Dopo aver effettuato il login ci dirigiamo verso la sezione “aggiungi Dati” e successivamente clicchiamo su monitora (lo vedrete come uno schermo che effettua una diagnosi.



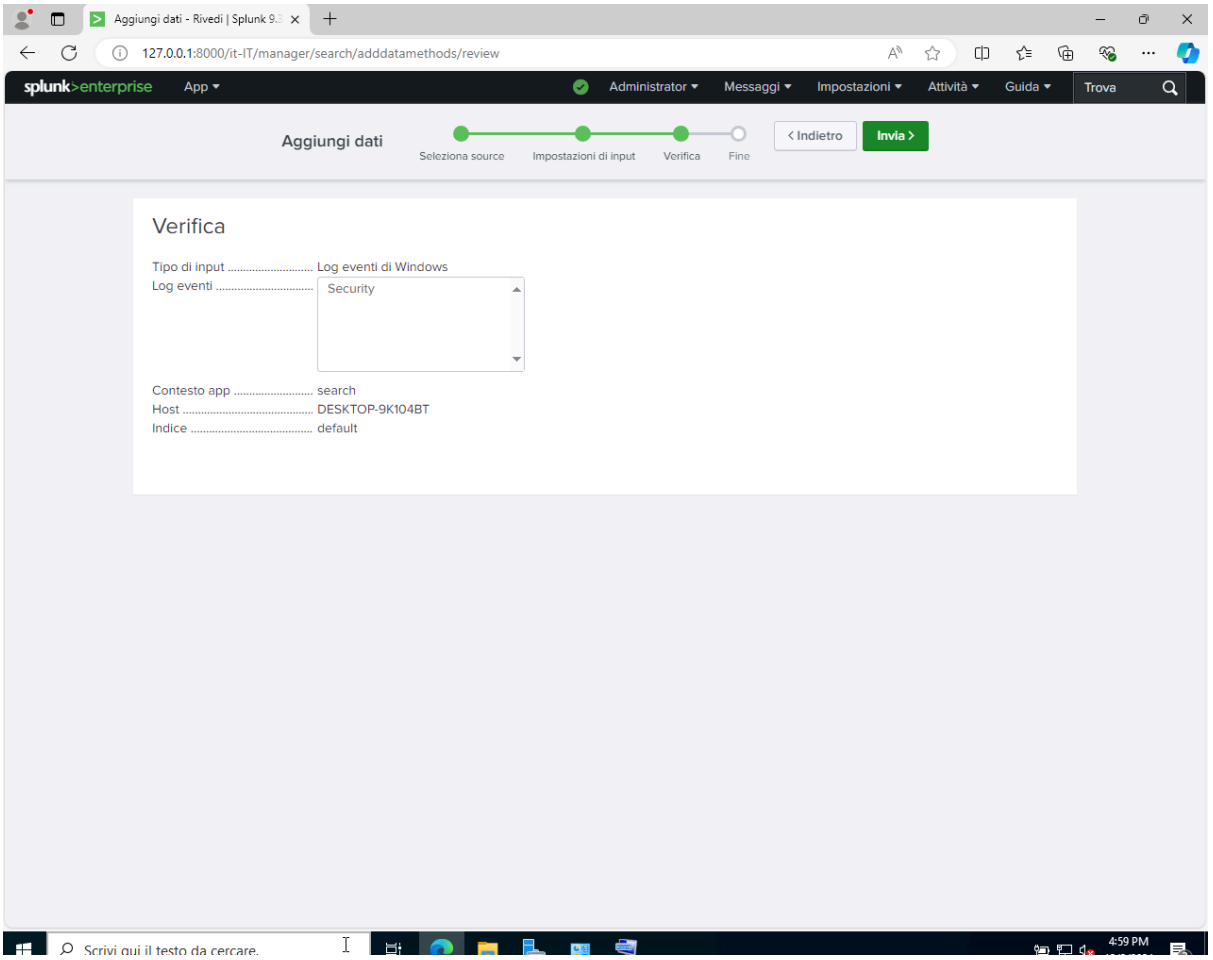
Selezioniamo la prima opzione che troviamo ovvero “ log di eventi locali” e nel menu’ selezioniamo security .



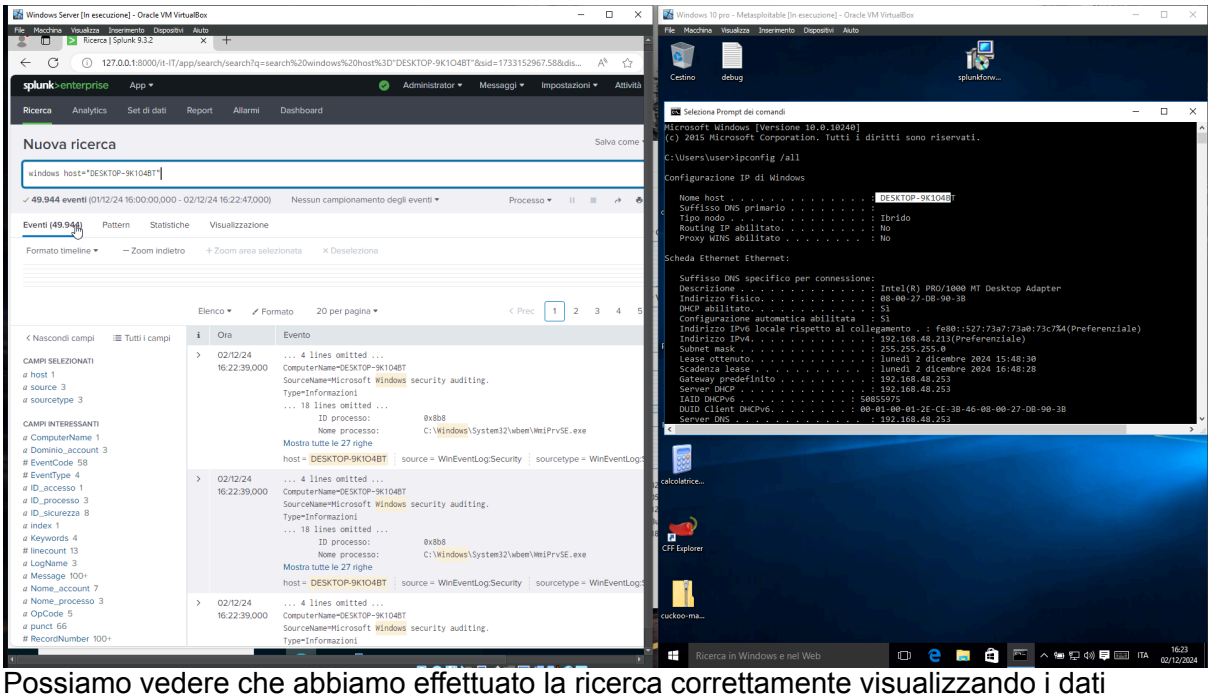

Continuiamo selezionando avanti e immettiamo il nome del nostro host ovvero DESKTOP-9K104BT e facciamo Verifica



Successivamente verifichiamo che i campi che abbiamo inserito siano corretti una volta corretti avviamo la ricerca




Avviamo la ricerca




Possiamo vedere che abbiamo effettuato la ricerca correttamente visualizzando i dati richiesti