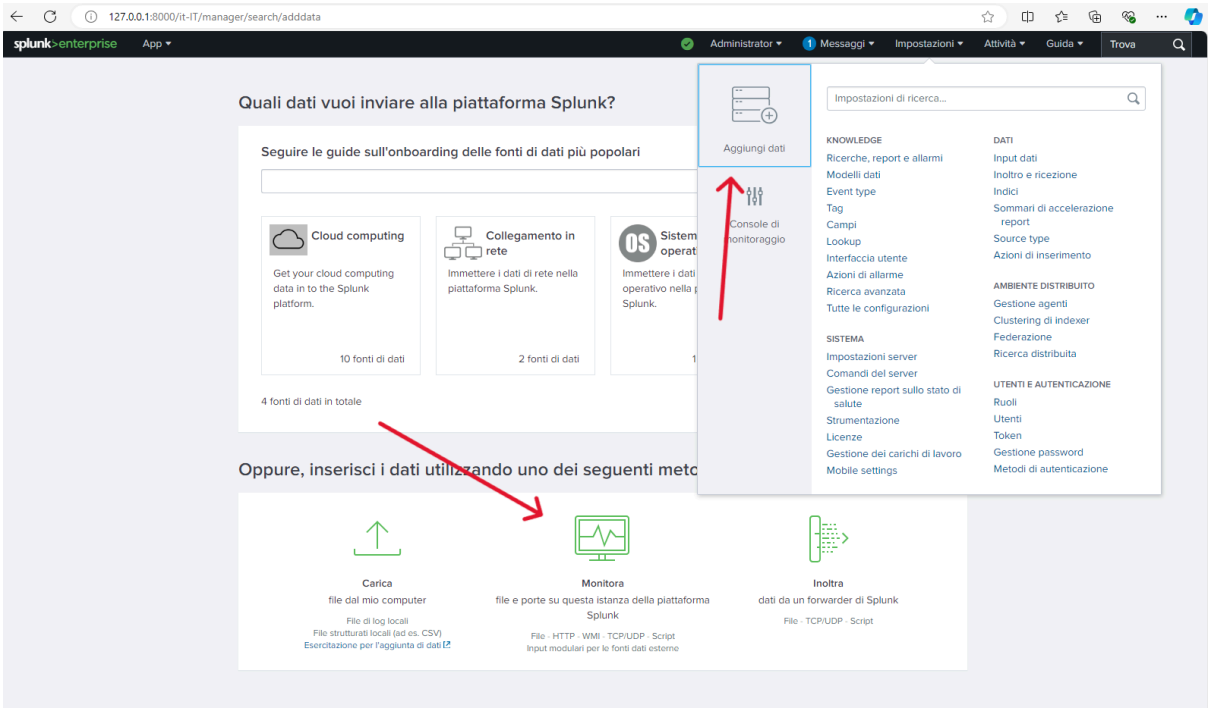
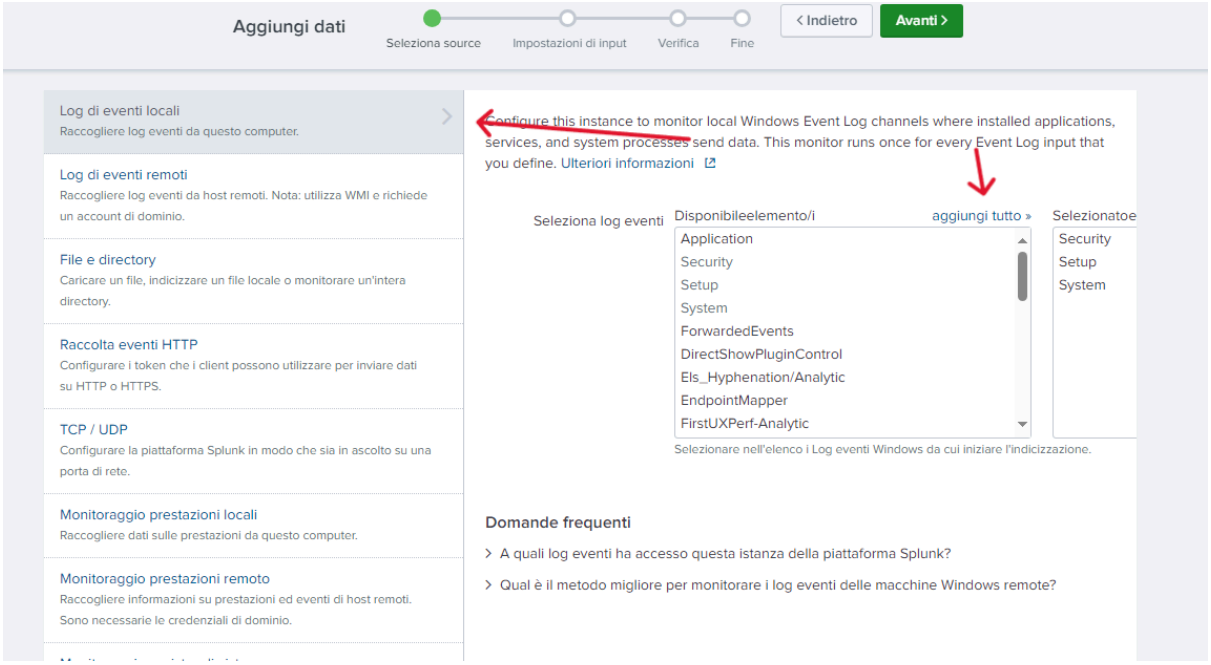
UNIT3 S10/L1 - Modalità Monitora in Splunk

Il compito di oggi consiste nel configurare la modalità Monitora in Splunk e realizzare degli screenshot che confermino l'avvenuta configurazione.

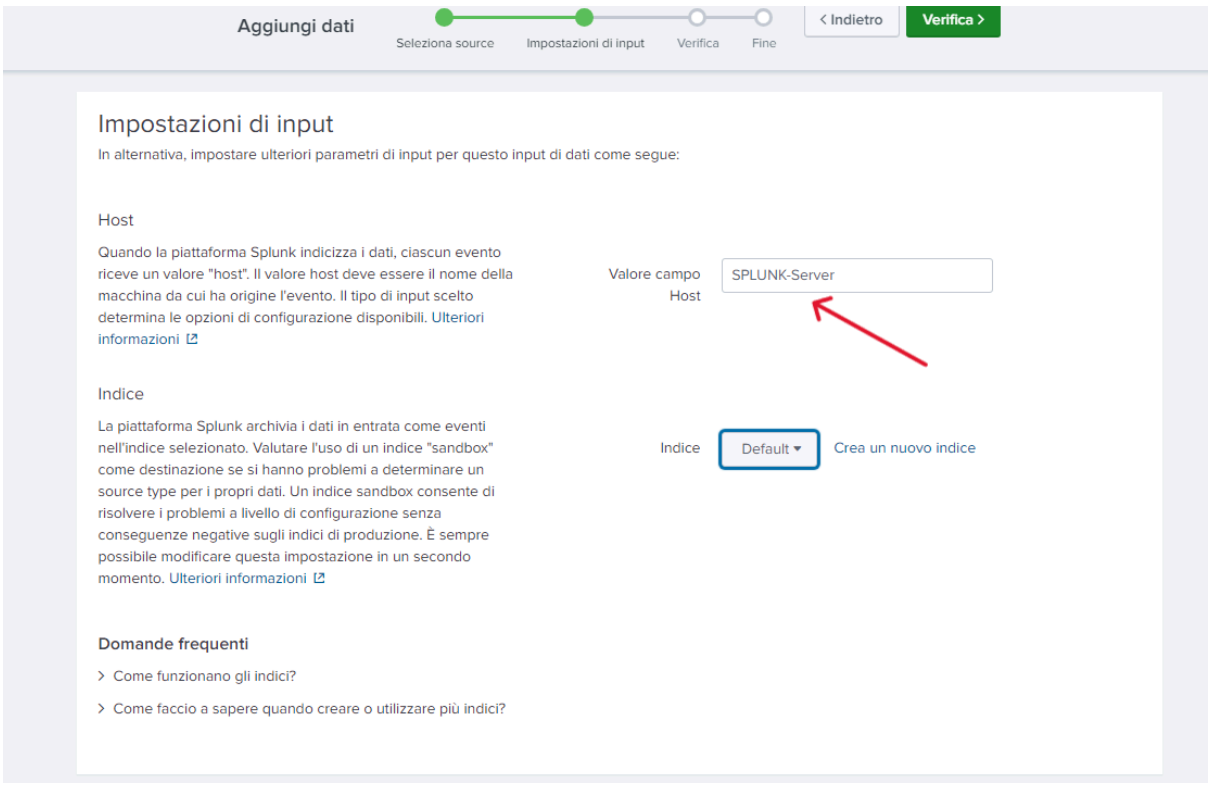
Una volta eseguito l'accesso su splunk



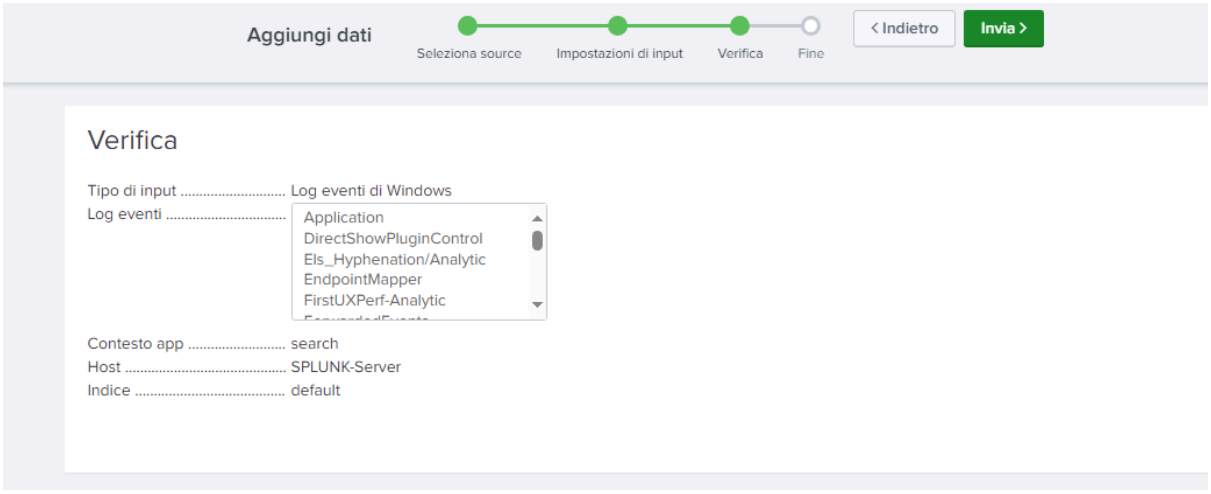
si clicca dal menù a tendina "impostazioni" → "aggiungi dati" → "monitora"



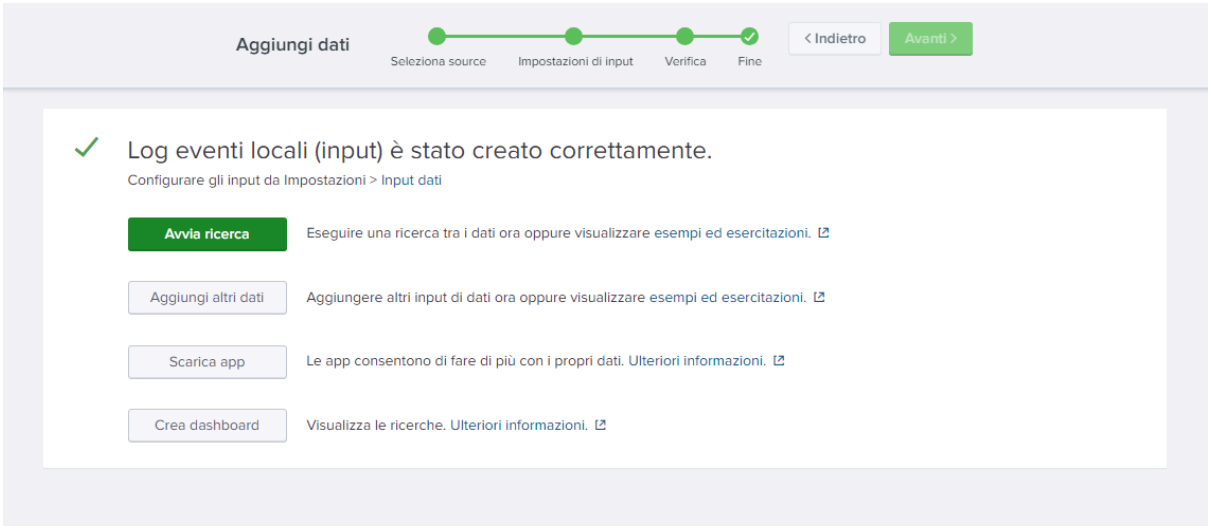
si sceglie quali log inserire (in questo caso solo event log locali) selezionando tutti gli eventi.



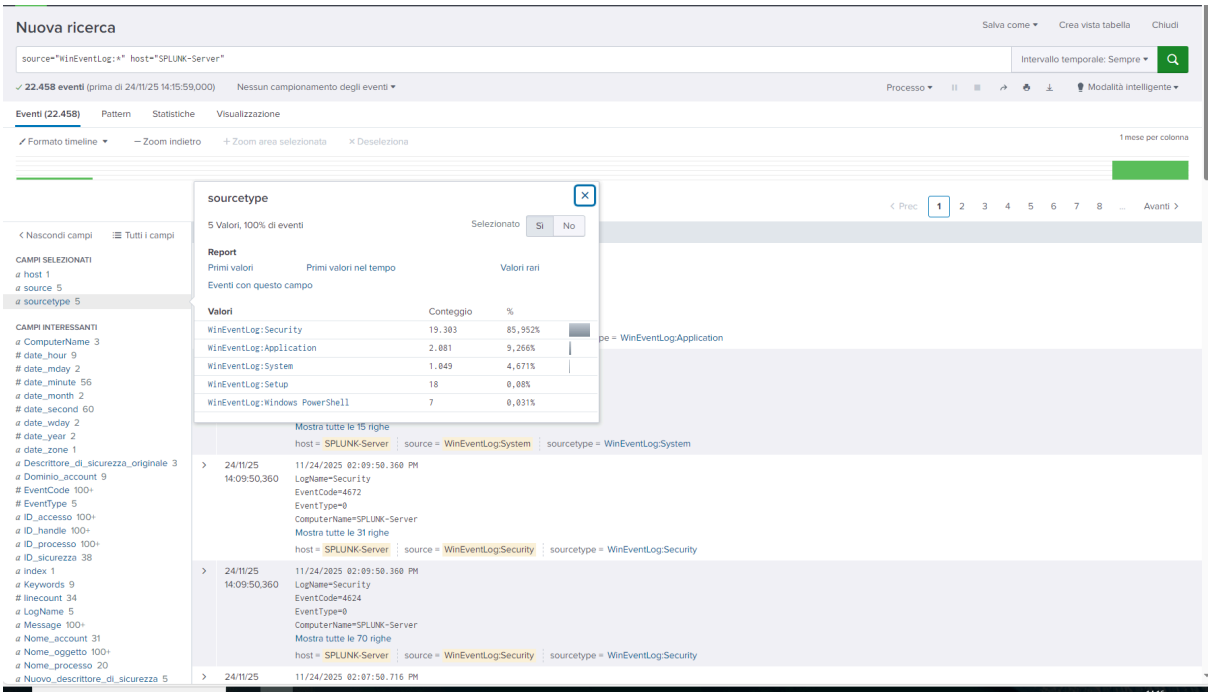
si deve definire nel “valore campo host” il nome del pc (in questo caso SPLUNK-Server)



finestra di verifica prima dell’avvio della ricerca



cliccare sul tasto verde per far partire la ricerca



abbiamo come output l'intera lista di log con la possibilità di filtrare in base al campo che preferiamo