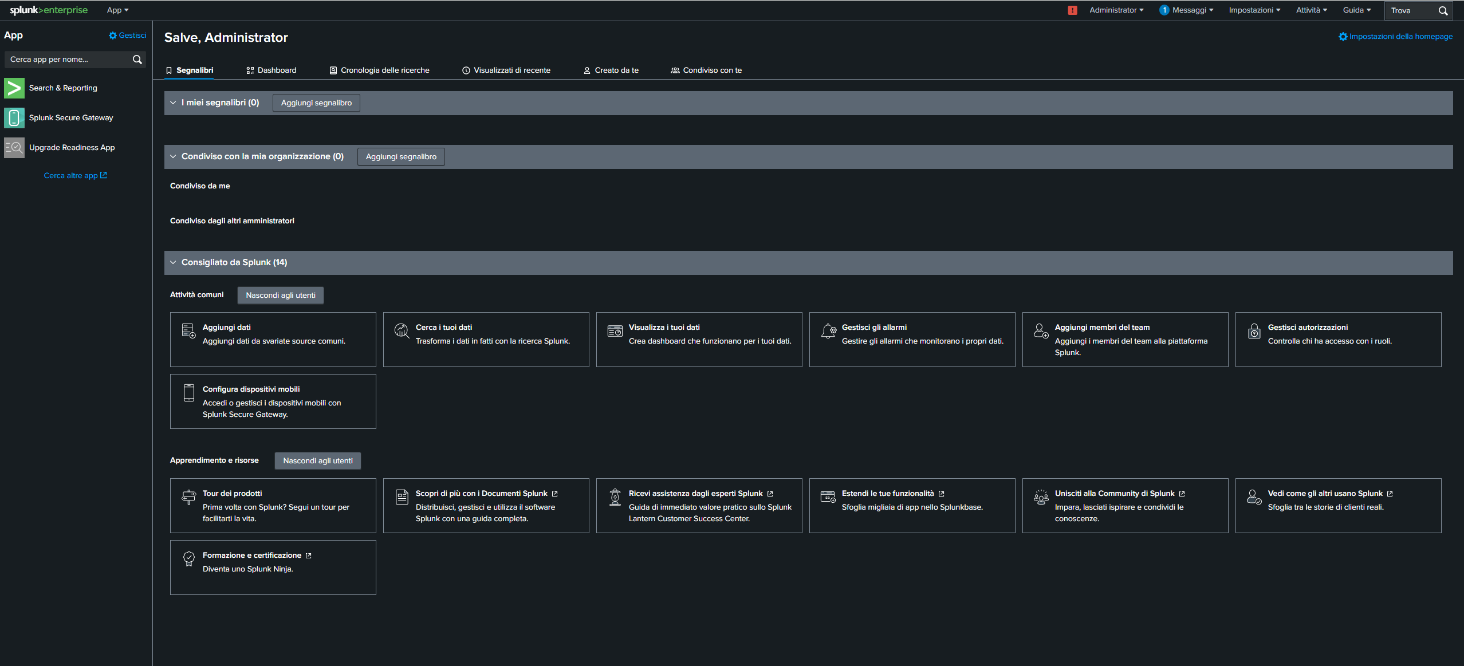
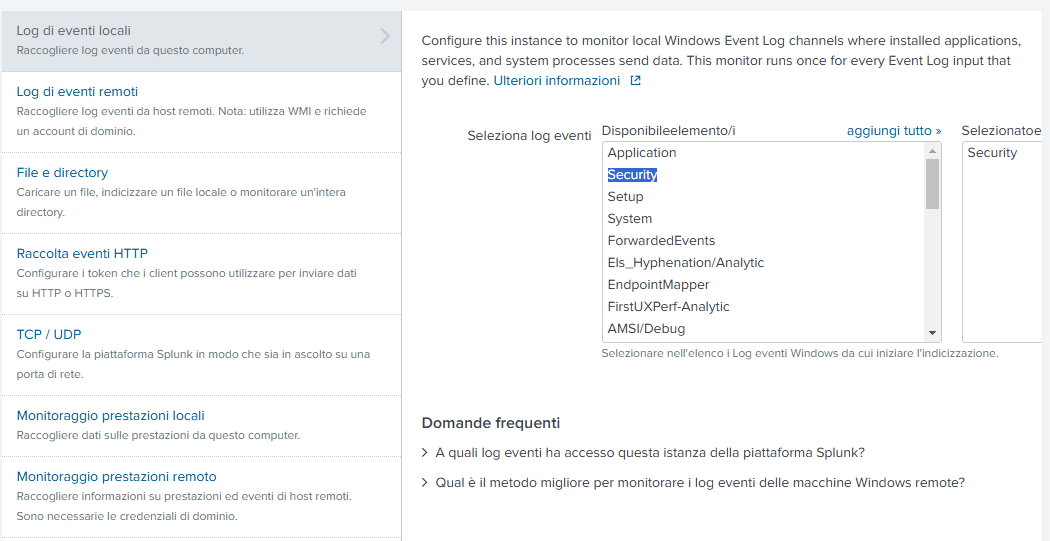
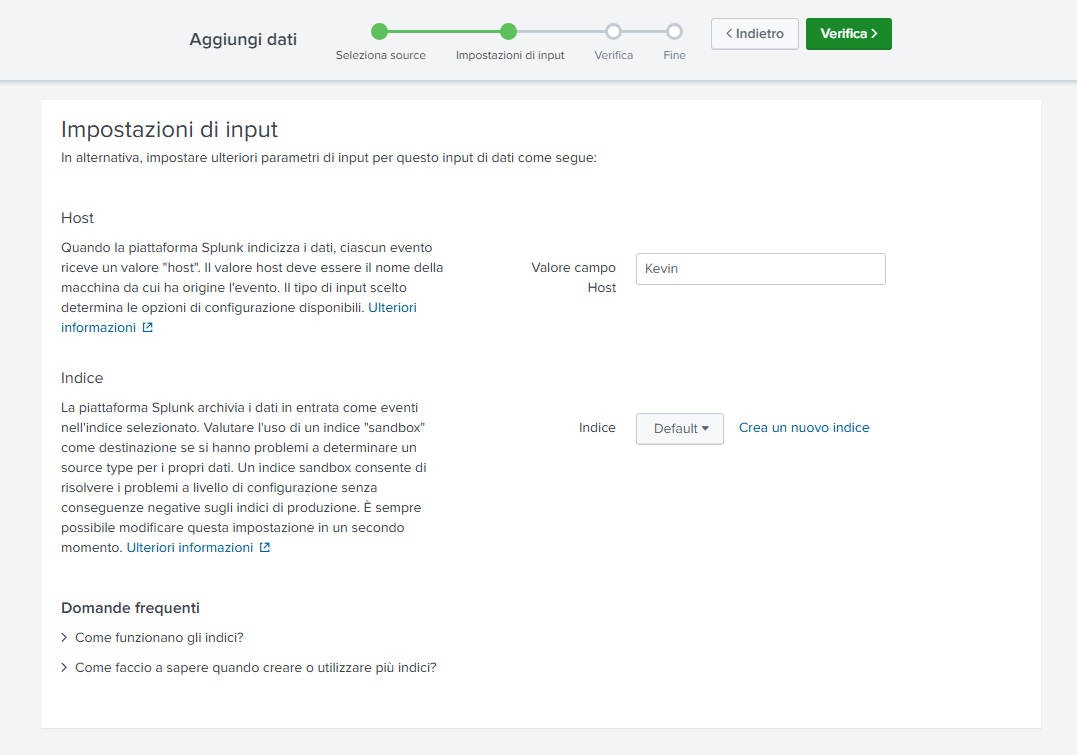
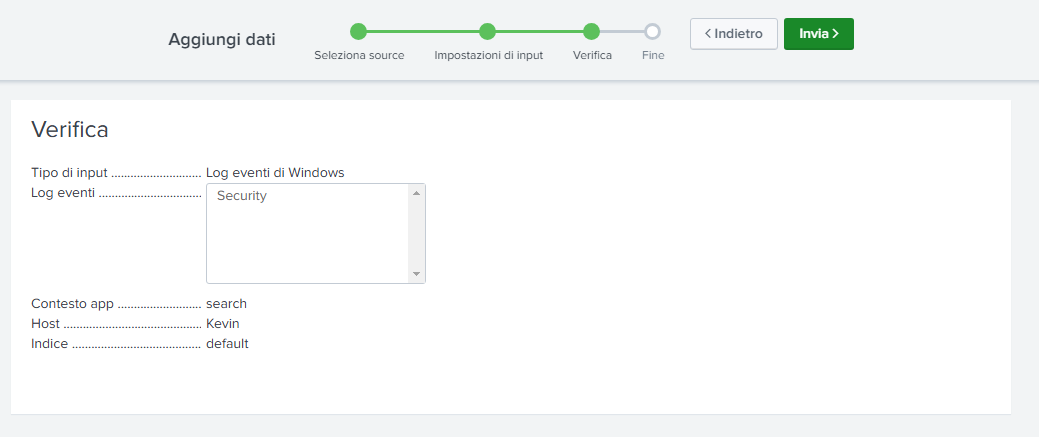
**S10/L1**

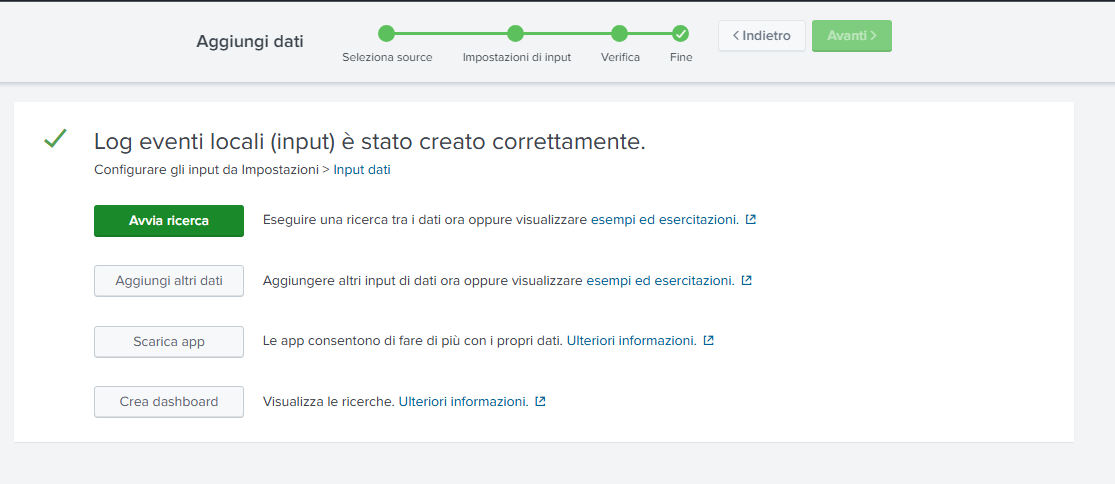
**Splunk**L’obiettivo di oggi consiste nel configurare la modalità “Monitora” su Splunk per osservare i file di log.  
  
Per prima cosa, andremo a selezionare l’opzione “Aggiungi dati”:

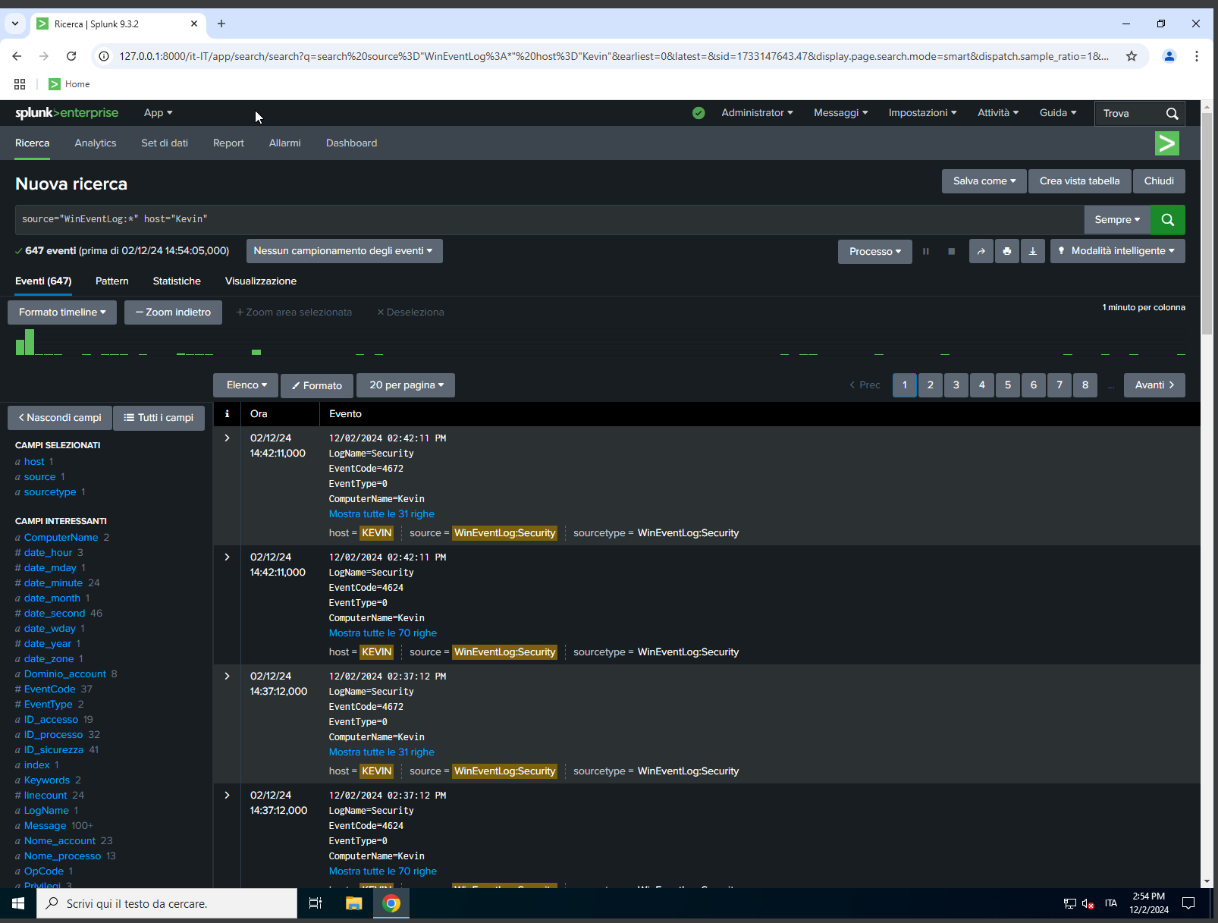


Una volta fatto questo, selezioneremo la modalità “Monitora”  
  
Proseguiamo selezionando il “Log di eventi locali”, selezionando nello specifico la sezione “Security”, Clicchiamo Avanti per continuare

  
  
Controlliamo se l’host coincide con la ricerca necessaria e clicchiamo su “Verifica”  
  


Controlliamo per l’ultima volta tutte le opzioni selezionate e clicchiamo su “Invia”  
  


Se gli step sono stati effettuati correttamente, i file di log saranno pronti ad essere controllati. Andiamo nello specifico cliccando su “Avvia Ricerca”:  
  


Ecco tutti i file riguardanti la macchina host che abbiamo messo in ascolto:  
  
  
  
Per concludere, possiamo controllare nello specifico i dati riguardanti un log specifico:  
  
