

Esercizio di Pratica S10L1 – Monitora Splunk

Sergio Falcone

INTRODUZIONE

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

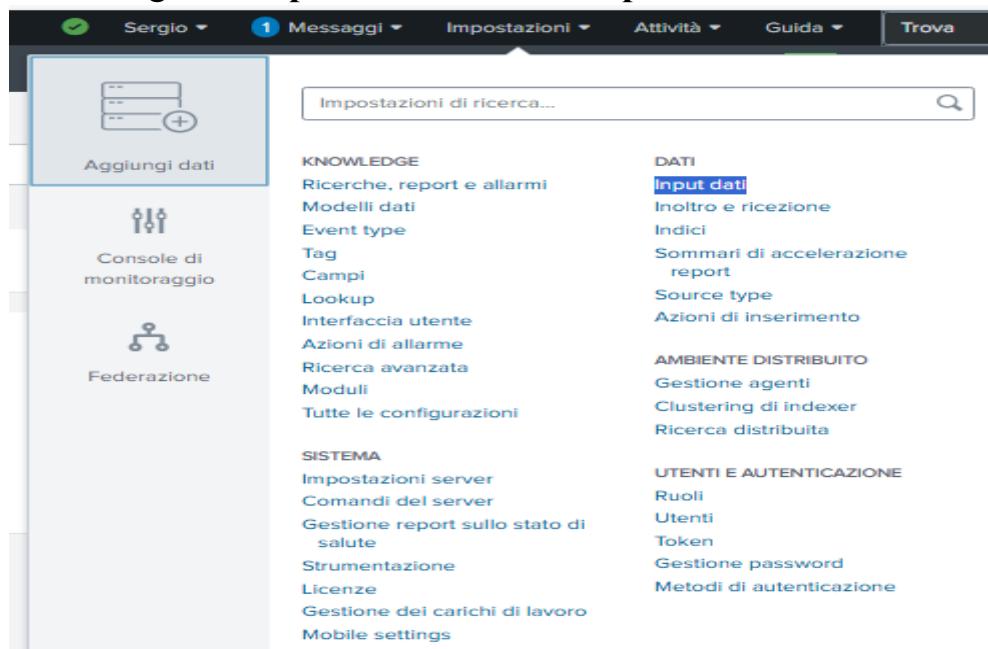
In breve: Lo studente dovrà configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.

PREFAZIONE

Questo Report documenta attraverso gli ScreenShots la configurazione della modalità Monitora del file Shadow il quale contenuto è stato estratto e inserito nella directory C:\\SplunkShdw

ESECUZIONE E SCREENSHOTS

1. Azione eseguita: Impostazioni ->Dati, Input dati



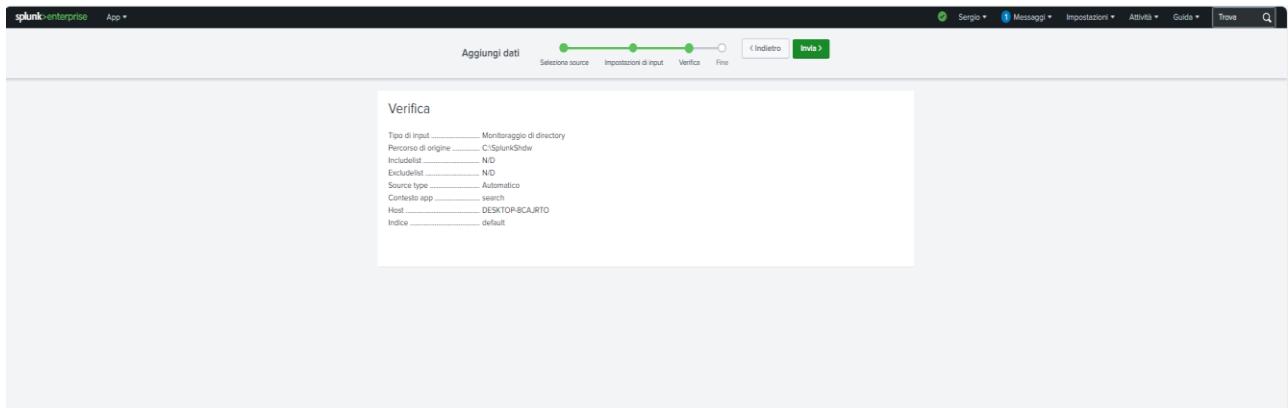
2. Azione eseguita: File e directory -> Aggiungi nuovo/a

Type	Input	Azioni
Raccolta di log eventi locali Raccolgere log eventi da questo computer.	-	Modifica
Raccolta di log eventi remoti Raccolgere log eventi da host remoti. Nota: utilizza WMI e richiede un account di dominio.	1	+ Aggiungi nuovo/a
File e directory Individizzare un file locale o monitorare un'intera directory.	20	+ Aggiungi nuovo/a
Monitoraggio prestazioni locali Raccolgere dati sulle prestazioni del computer locale.	0	+ Aggiungi nuovo/a
Monitoraggio prestazioni remoto Raccolgere informazioni su prestazioni ed eventi di host remoti. Sono necessarie le credenziali di dominio.	0	+ Aggiungi nuovo/a
Raccolta eventi HTTP Ricevere dati su HTTP o HTTPS.	0	+ Aggiungi nuovo/a

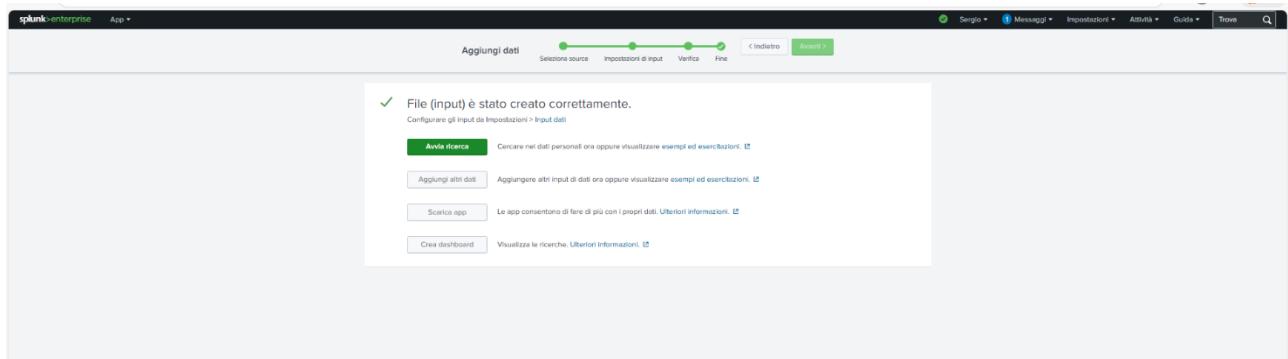
3. Azione eseguita: Sfoglia -> C: -> SplunkShdw -> Avanti

4. Azione eseguita: Impostazioni di input -> Avanti

5. Azione eseguita: Verifica -> Avanti



6. Azione eseguita: Avvia ricerca



7. Esito: Nuova ricerca