Implementazione di Splunk Enterprise con Universal Forwarder su Windows 10

CONTESTO

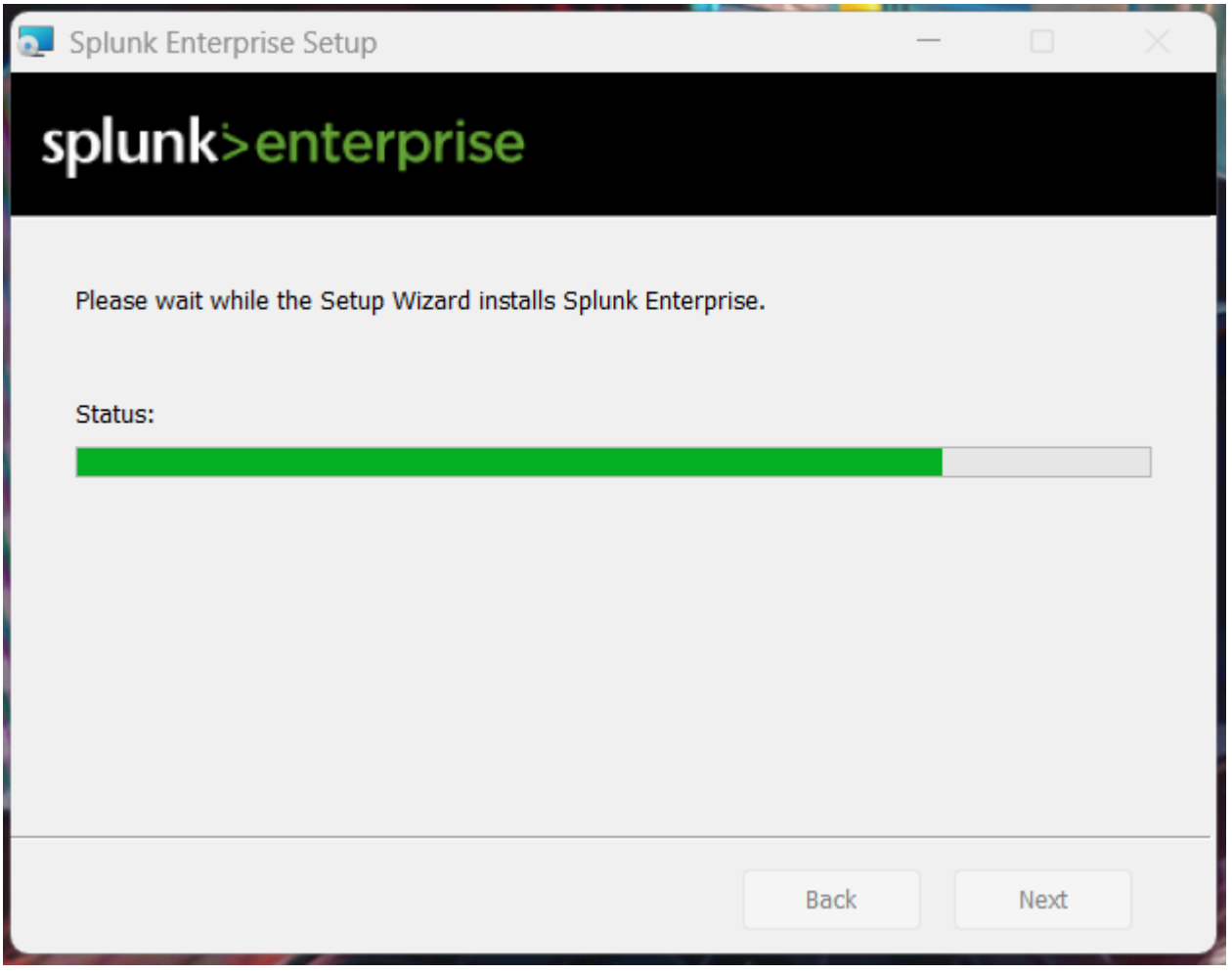
In questo esercizio pratico ho simulato un' ambiente SIEM utilizzando Splunk Enterprise sul mio PC, aggiungendo una macchina virtuale Windows 10 con il Forwarder configurato.

È presente anche una macchina Kali Linux, che in futuro potrei utilizzare per attaccare Windows 10 e analizzare i log raccolti dal Forwarder.

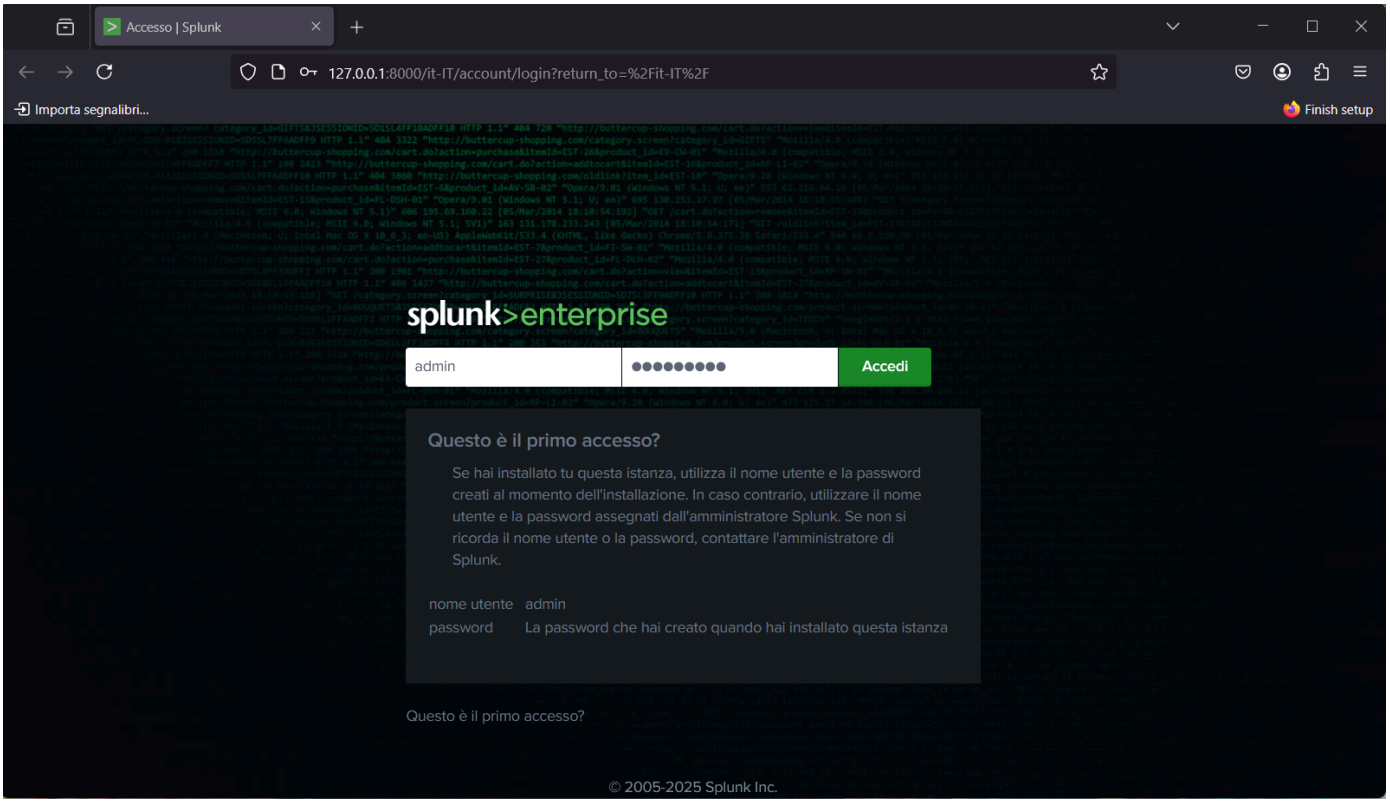
In questa guida, mi limiterò a dimostrare che l'installazione è andata a buon fine e che la configurazione funziona perfettamente.

CREAZIONE

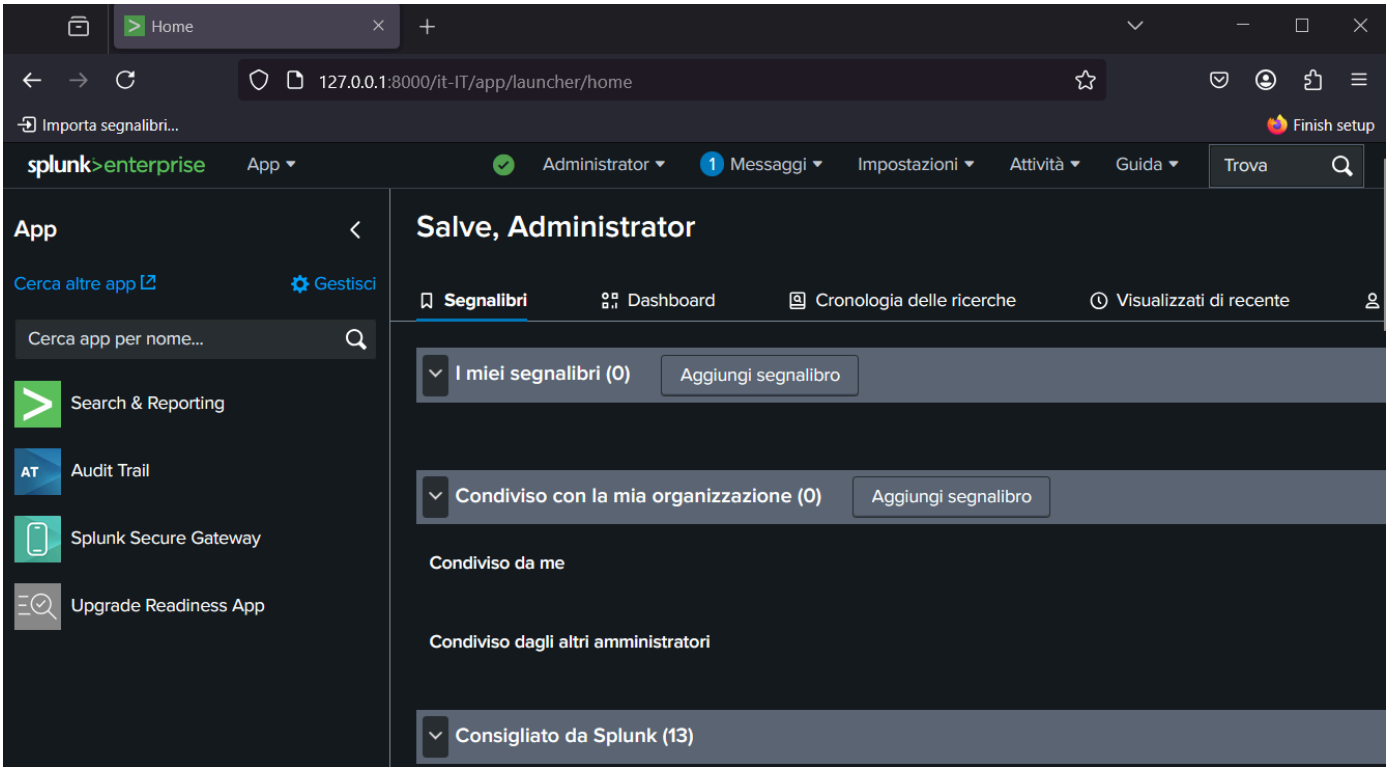
Per iniziare installiamo Splunk enterprise sulla nostra macchina.



Una volta scaricato si avvierà, apriamo una pagina del browser ed inseriamo nell'URL il nostro indirizzo di loopback con la porta sulla quale funziona la nostra interfaccia Splunk quindi : `127.0.0.1:8000`



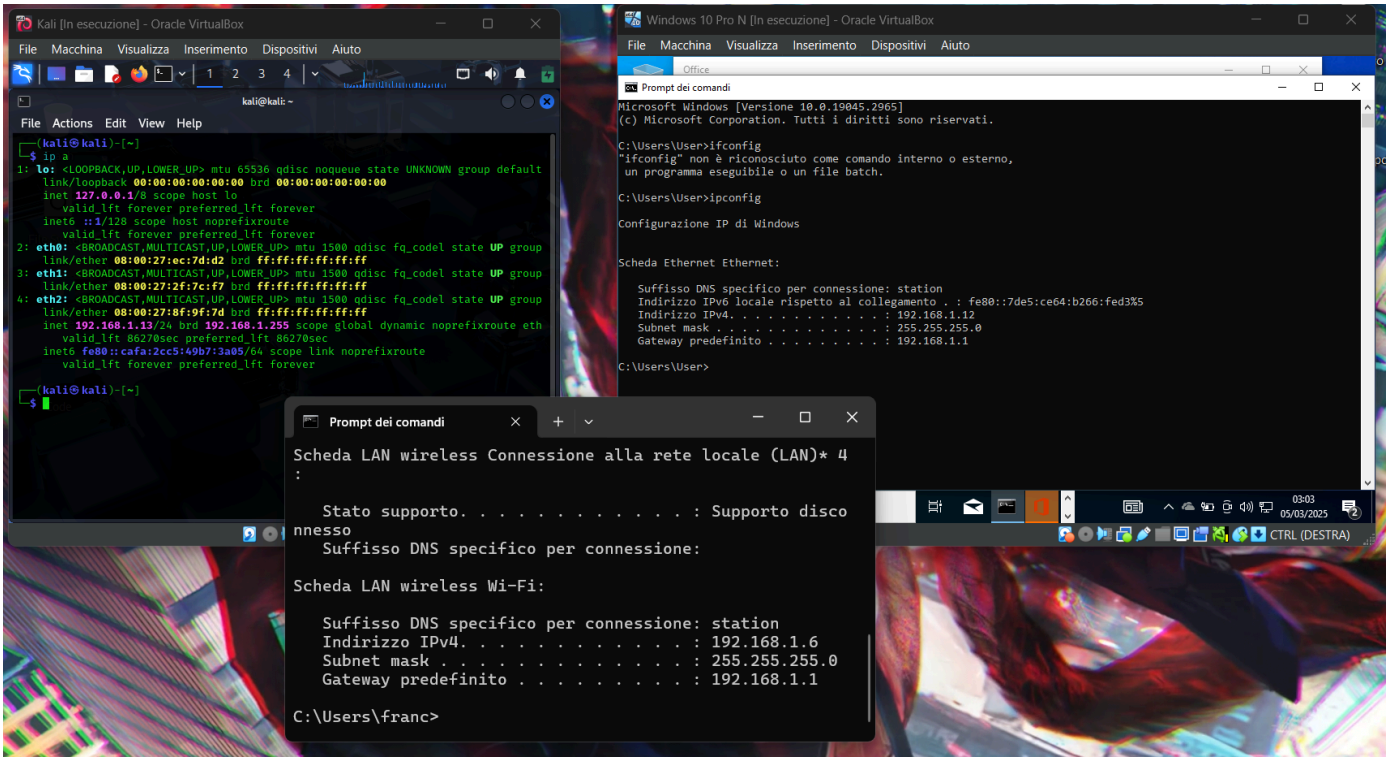
Si presenterà a noi la pagina del login, logghiamoci e diamo un'occhiata.



Fino a qui tutto liscio si presenterà a noi l'interfaccia principale di Splunk, ora andiamo sul sito ufficiale e scarichiamo il forwarder adatto a noi.

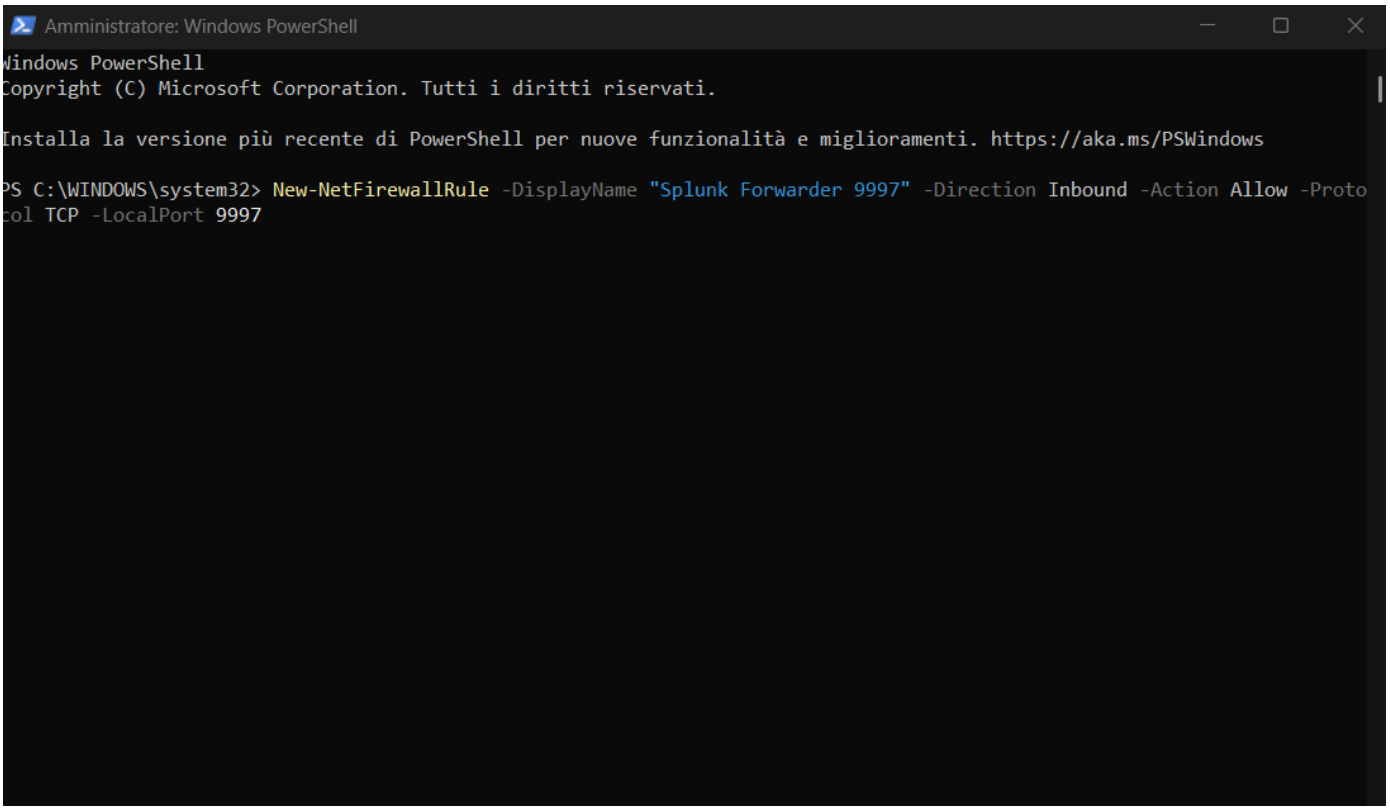
64-bit	Windows 10, 11 Windows Server 2019, 2022, 2025	.msi	180.04 MB	Download Now	Copy wget link	More

Nel mentre che scarica assicuriamoci che sia il mio Pc host (dove appunto ho installato Splunk) che le 2 VM Kali e Windows 10 siano nella stessa rete in modo che non ci siano problemi di comunicazione.

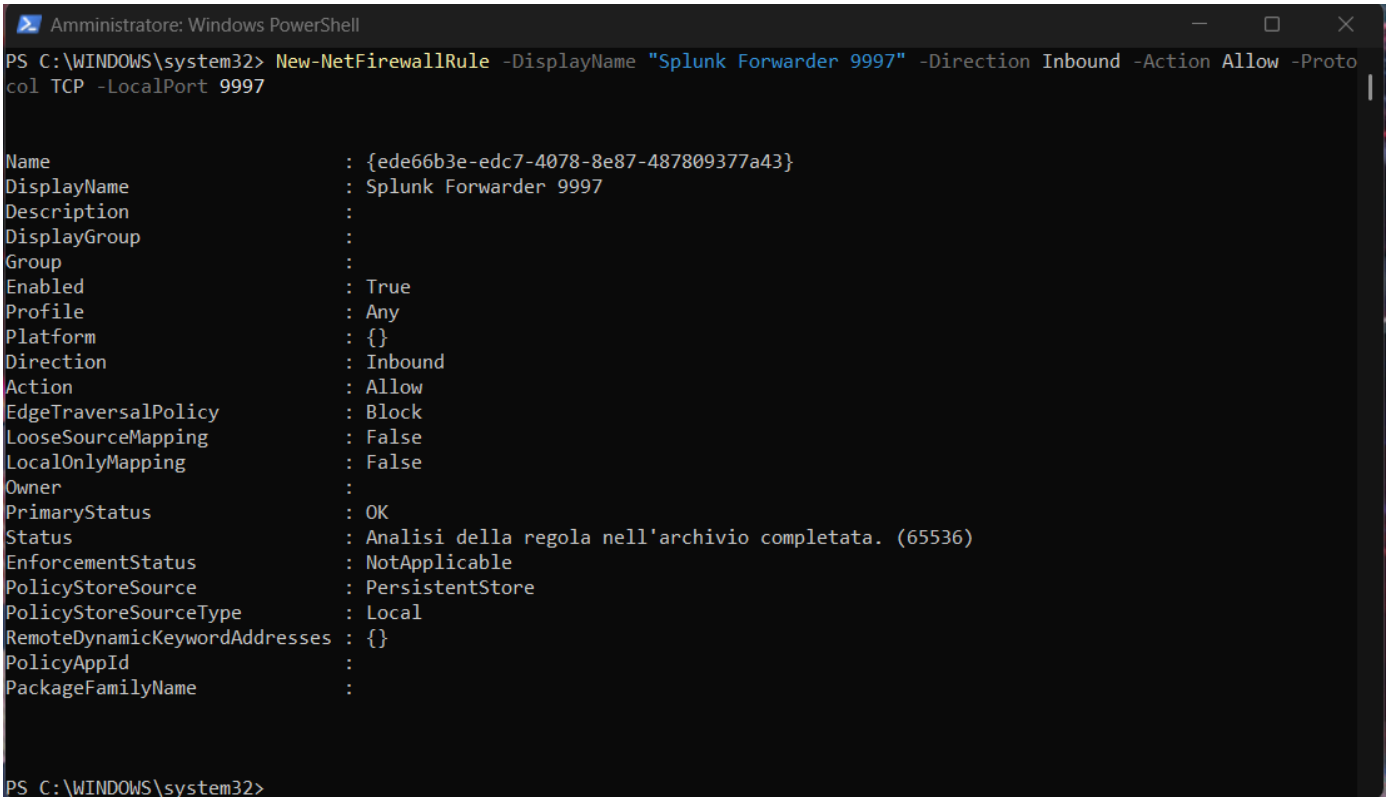


Le macchine sono perfettamente allineate, ho verificato anche con un Ping per sicurezza e tutto ha funzionato a meraviglia. (Windows di solito non risponde al Ping di default per ovviare a ciò potete andare a modificare le regole di entrata e uscita su Windows firewall).

Per evitare un altro errore di connettività dobbiamo autorizzare il forwarder ad effettuare una connessione TCP per mandarci i log su Splunk, quindi procediamo immediatamente a creare la nostra regola firewall sulla macchina che ospita Splunk, apriamo PowerShell come admin e digitiamo questo comando :

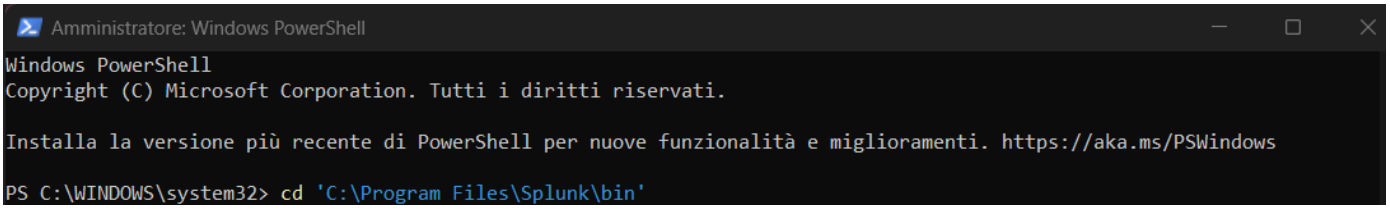


Ho scelto la porta 9997 semplicemente per una questione di comodità dato che è la porta di default che suggerisce Splunk, se tutto andrà a buon fine dovresti ricevere questo output :

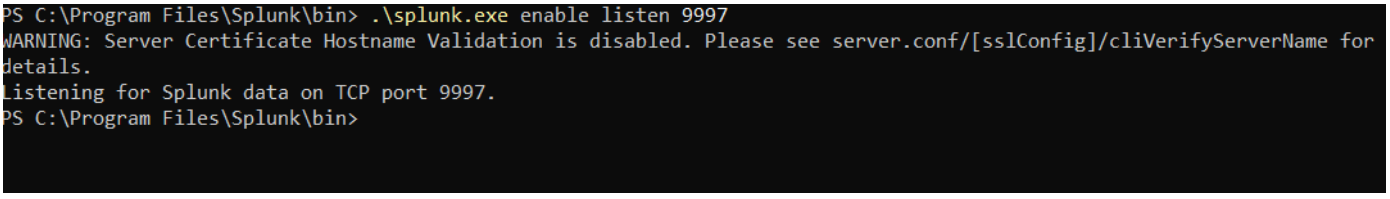


Adesso per essere certi al 100% che la nostra regola sia stata creata correttamente andiamo sul nostro Windows firewall e dovremo vederla in cima.

Ed eccola! La regola è stata configurata correttamente, adesso dobbiamo eseguire un altro step da PowerShell semplicemente dobbiamo abilitare il listener di Splunk perciò andiamo nel percorso corretto che ora mostrero' :

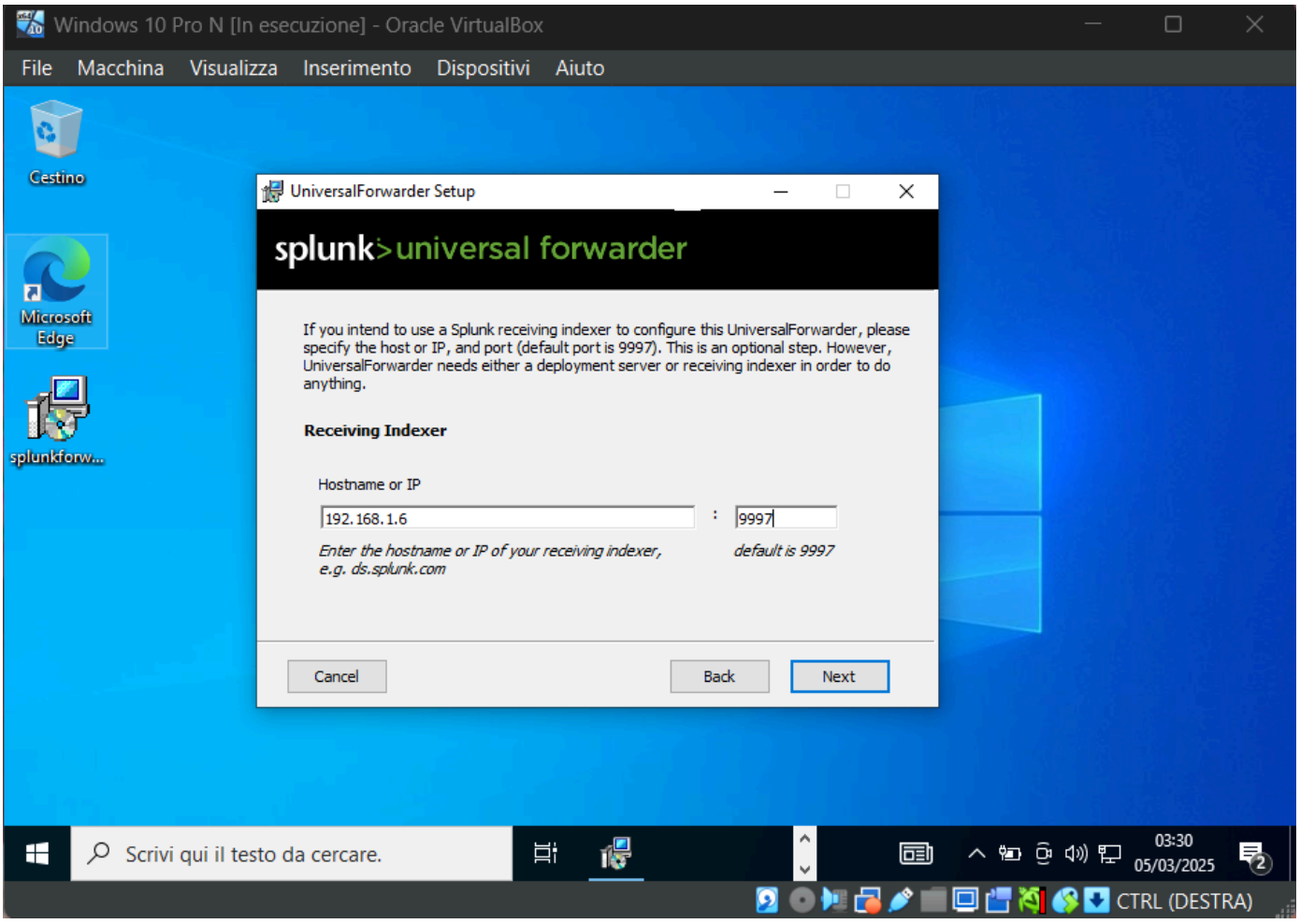


Una volta dentro diamo il comando per attivare il listener :



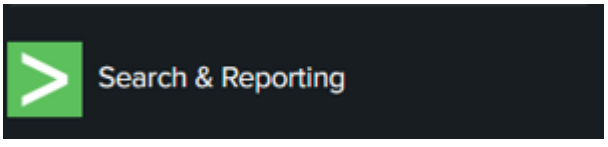
Ed eccoci qua ! L'output è corretto, Splunk si è messo ufficialmente in ascolto sulla porta 9997!

Ora non ci resta che scaricare il nostro forwarder sulla nostra VM di Windows 10 che vogliamo monitorare.



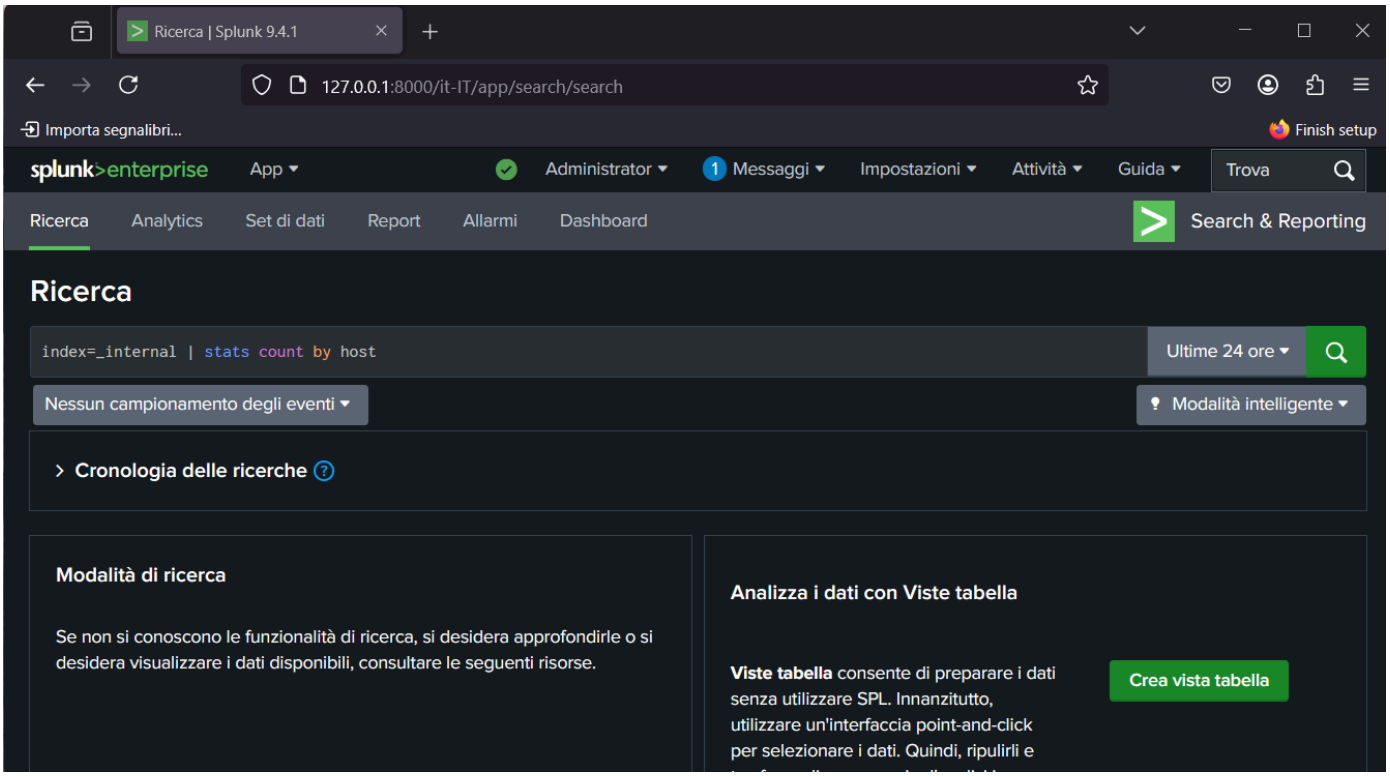
Nell'istallazione vi chiederà di configurare il DS lasciate in bianco non ci serve in questa casistica, mentre nell'immagine qui sopra ci sta chiedendo di configurare il reciver cioè dove vogliamo inoltrare tutte le informazioni che cattureremo, se vi ricordate in precedenza abbiamo attivato il listener sulla porta `9997` e Splunk è ospitato sulla nostra macchina host, quindi mettiamo l'indirizzo Ip e la porta con coerenza altrimenti non funzionerà!!!

Una volta configurato il nostro forwarder, Splunk sarà pronto a catturare tutti i Log, quindi torniamo sulla sua interfaccia e clicchiamo su questa sezione:

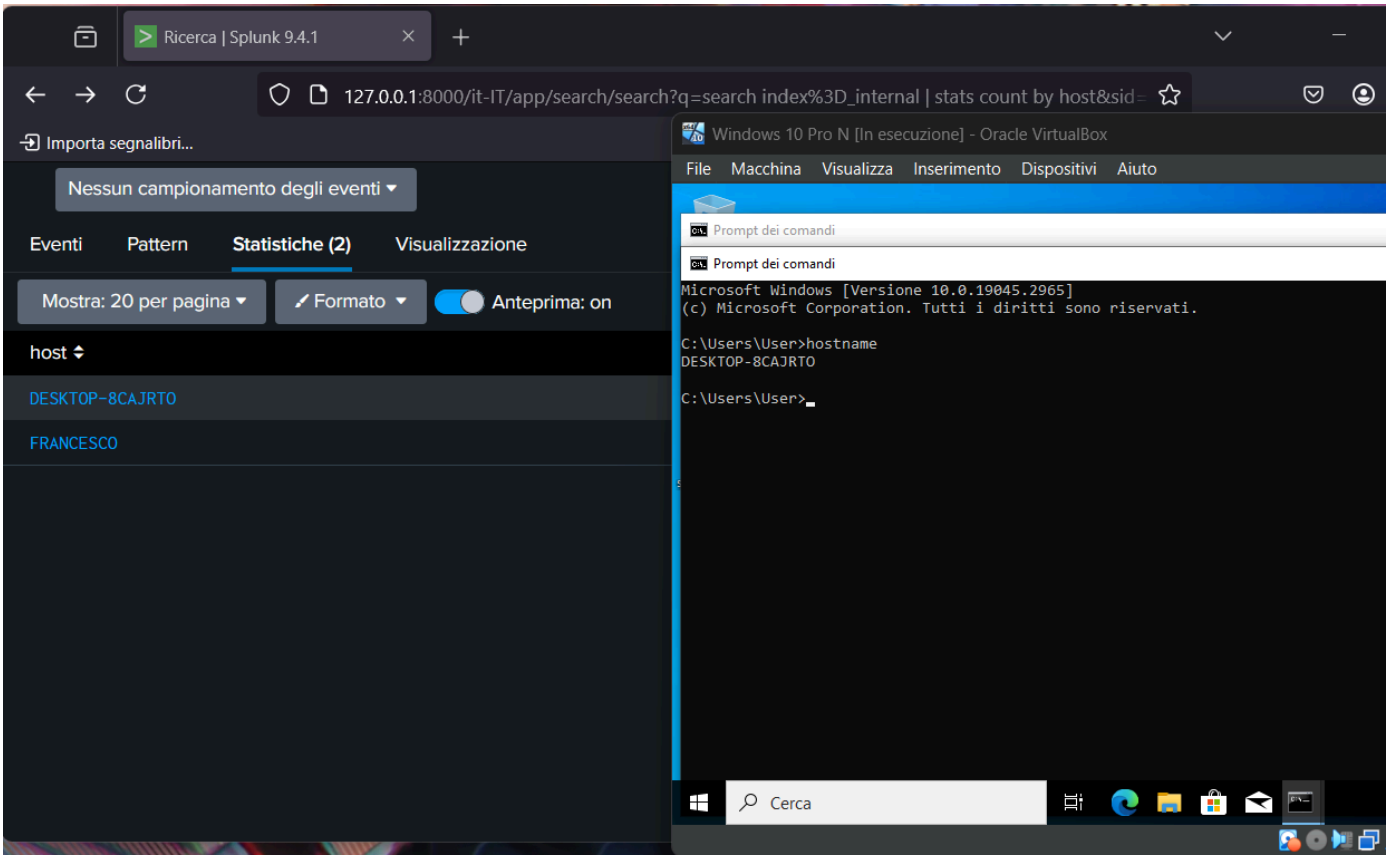


Una volta dentro dovremo inserigli questa query :
`index=_internal | stats count by host`

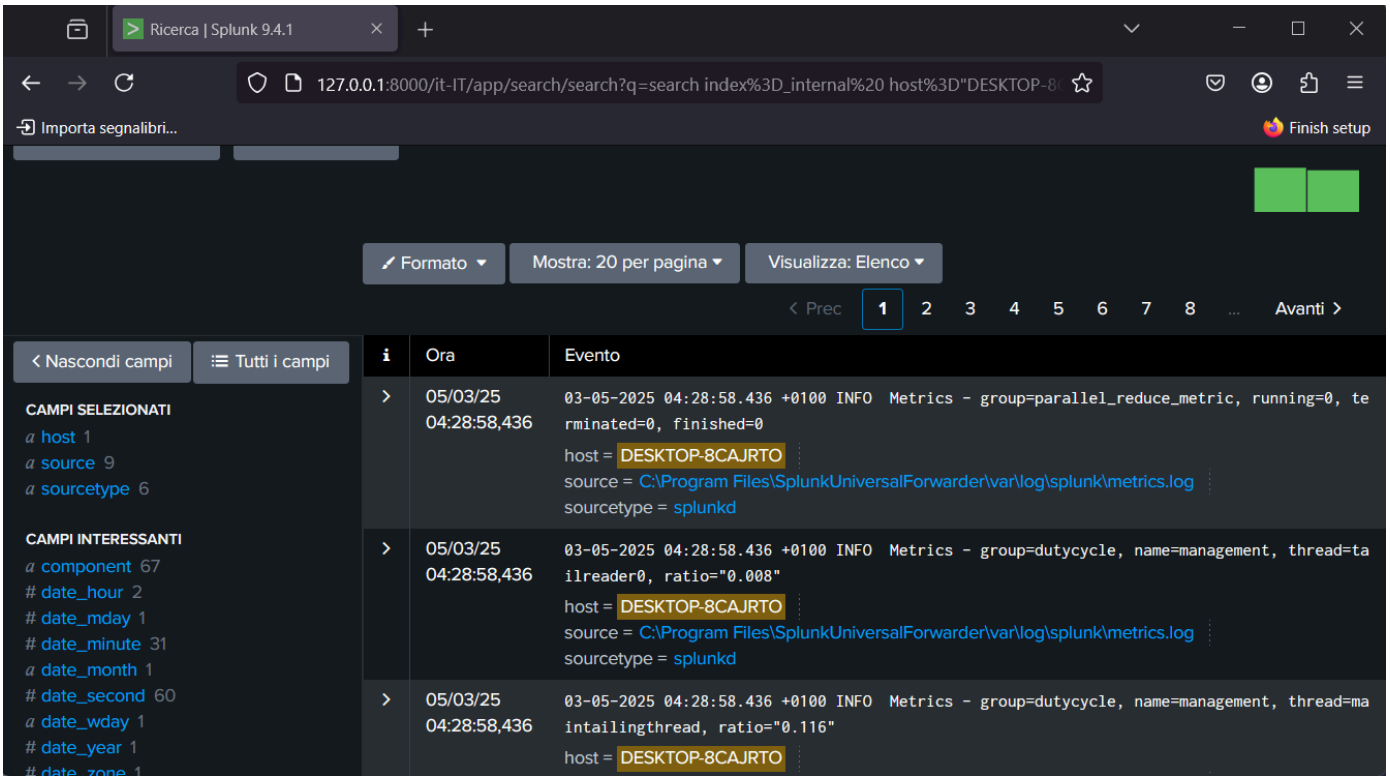
In breve gli stiamo dicendo che questa query di ricerca conta il numero di eventi nell'indice _internal di Splunk e li suddivide per host. In pratica, permette di vedere quanti log sono generati da ciascun dispositivo, aiutando a monitorare l'attività e a individuare eventuali anomalie o problemi nei sistemi.



Diamo l'invio e noteremo immediatamente gli host che sta monitorando.



Troviamo un certo DESKTOP-8CAJRTO verifichiamo se è il nostro Windows 10, e come vediamo sopra è proprio lui, tutta la configurazione ha funzionato a meraviglia, vi lascio uno screen dei log giusto per darvi prova della cosa.



Nel prossimo progetto proverò a settare tutte le varie regole per la raccolta dei log, e faremo qualche test di verifica attaccando la VM Windows 10 con la Kali.