



# S10-L1

S P L U N K

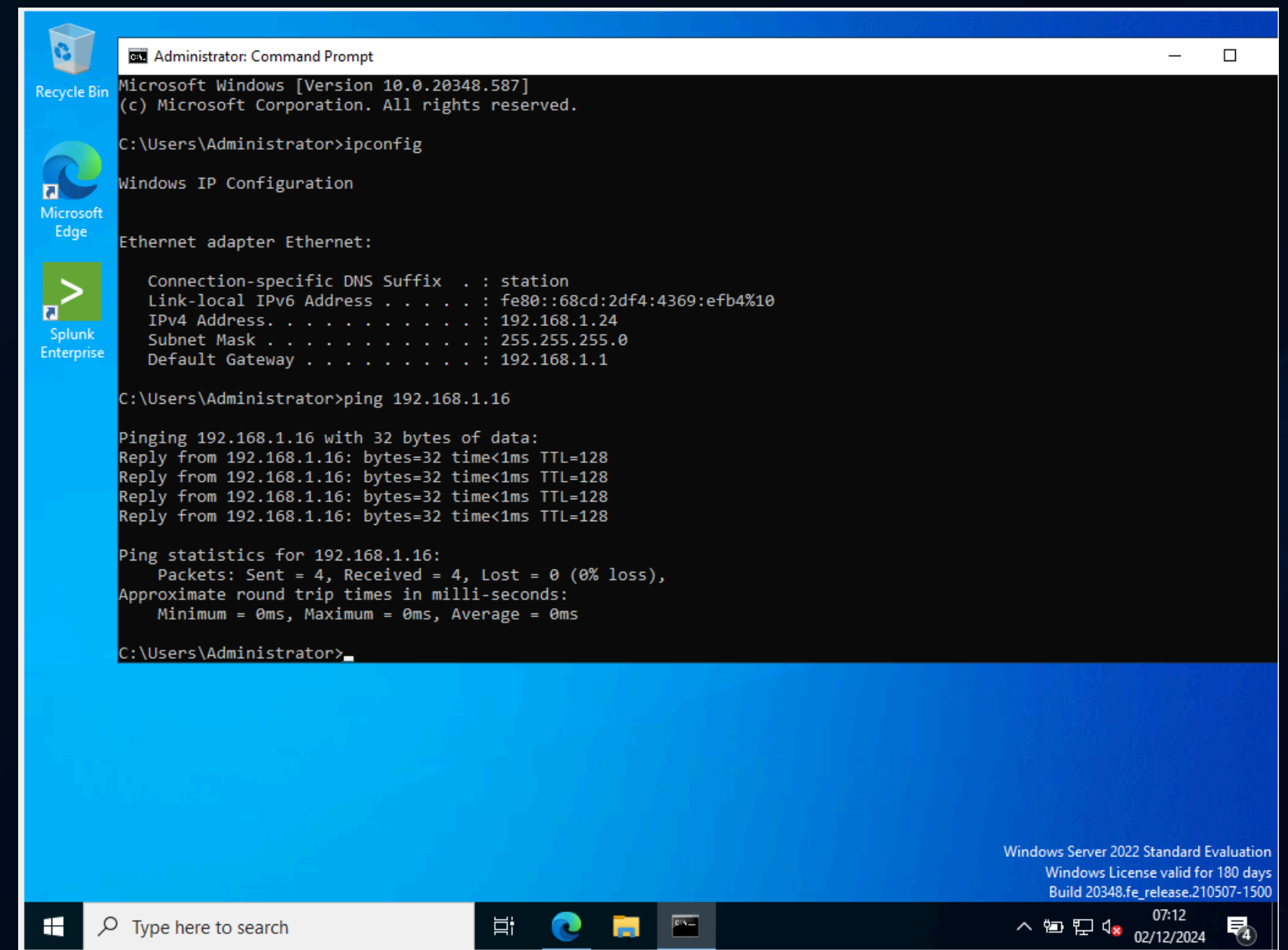


## TRACCIA

dovremo configurare la modalità Monitora in Splunk e realizzare degli screenshot che mostrino l'esecuzione.

# COMUNICAZIONE TRA LE MACCHINE

Per la nostra comunicazione utilizzeremo windows server 2022 e il nostro windows 10. Splunk è un sistema distribuito che raccoglie, analizza e visualizza i dati dei log da più fonti, pertanto la comunicazione tra le macchine virtuali è fondamentale.





# USO DI SPLUNK ENTERPRISE

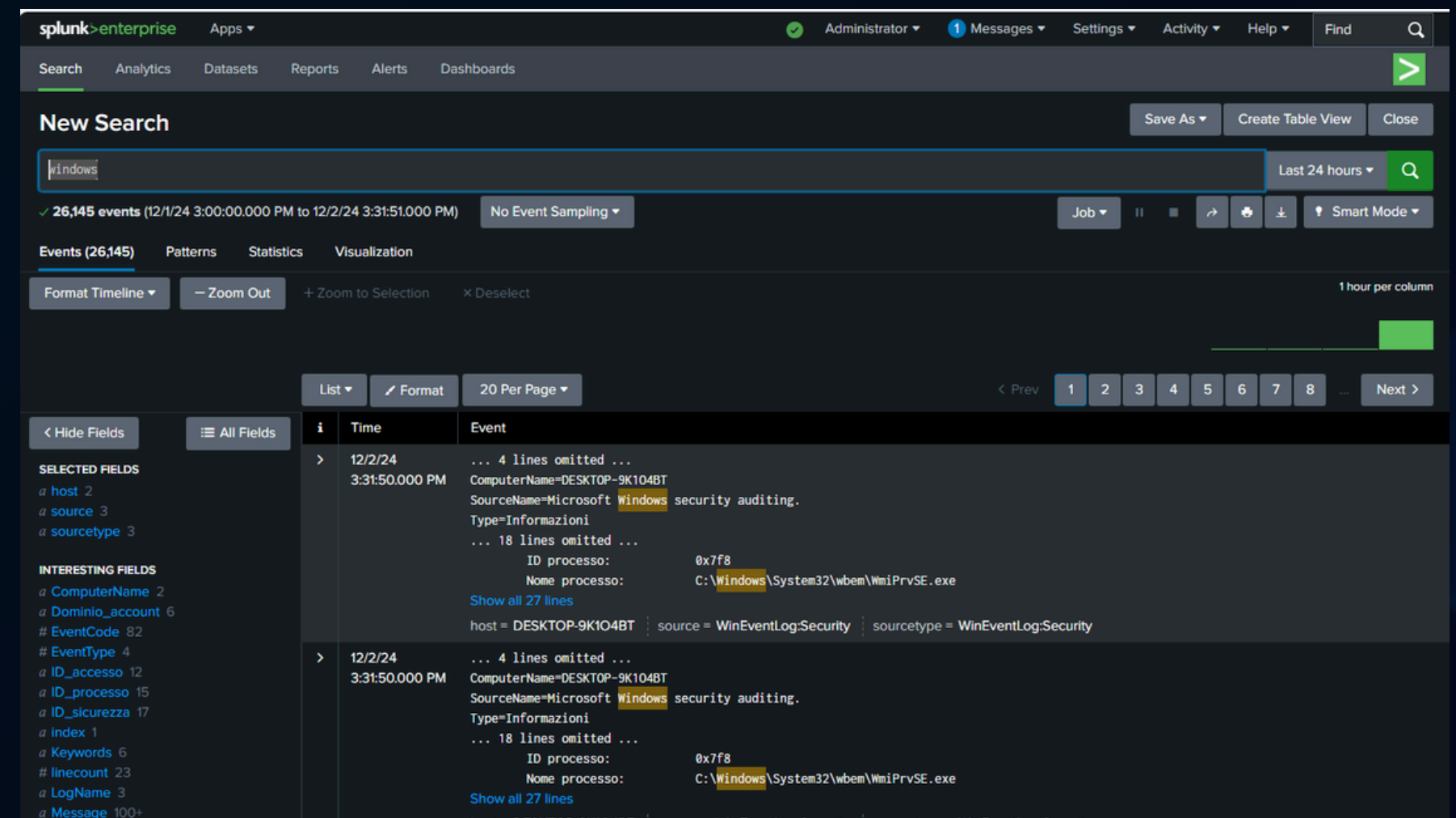
Una volta installato splunk forward sulla nostra macchina windows, procediamo con il monitoraggio.

L'immagine mostra una ricerca eseguita su Splunk utilizzando la parola chiave "Windows". Si tratta di eventi provenienti da un log di sicurezza di un sistema Windows, indicati come Microsoft Windows Security Auditing. L'obiettivo è monitorare eventi di sicurezza e attività correlate al sistema.

Splunk ha restituito 26.145 eventi in un intervallo di tempo che copre le ultime 24 ore.

Avremo poi un host (indicato con Desktop che sarà il nostro dispositivo analizzato).

Il log è stato registrato da WinEventLog:Security, che rappresenta i log di sicurezza del sistema Windows.



# USO DI SPLUNK ENTERPRISE

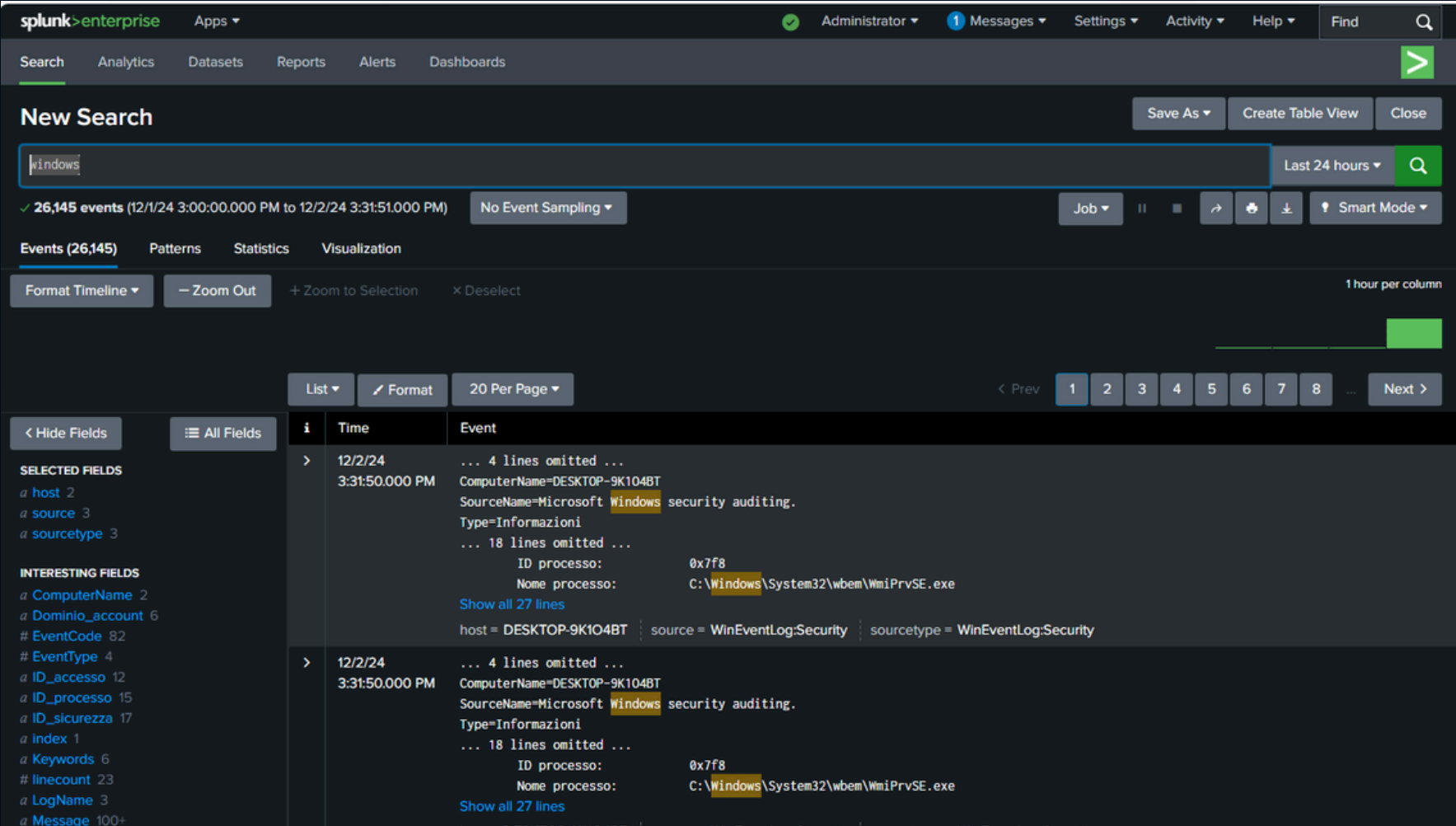
Una volta installato splunk forward sulla nostra macchina windows, procediamo con il monitoraggio.

L'immagine mostra una ricerca eseguita su Splunk utilizzando la parola chiave "Windows". Si tratta di eventi provenienti da un log di sicurezza di un sistema Windows, indicati come Microsoft Windows Security Auditing. L'obiettivo è monitorare eventi di sicurezza e attività correlate al sistema.

Splunk ha restituito 26.145 eventi in un intervallo di tempo che copre le ultime 24 ore.

Avremo poi un host (indicato con Desktop che sarà il nostro dispositivo analizzato).

Il log è stato registrato da WinEventLog:Security, che rappresenta i log di sicurezza del sistema Windows.



The screenshot displays the Splunk Enterprise web interface. At the top, the 'splunk>enterprise' logo is visible alongside user and system information. The main navigation bar includes 'Search', 'Analytics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is active, showing a 'New Search' page. The search query 'Windows' is entered in the search bar, and the results show 26,145 events from 12/1/24 3:00:00 PM to 12/2/24 3:31:51 PM. The interface includes a search bar, navigation tabs, and a list of events with details like Time, Event, and SourceName.

Time	Event
12/2/24 3:31:50.000 PM	... 4 lines omitted ... ComputerName=DESKTOP-9K104BT SourceName=Microsoft Windows security auditing. Type=Informazioni ... 18 lines omitted ... ID processo: 0x7f8 Nome processo: C:\Windows\System32\wbem\WmiPrvSE.exe Show all 27 lines host = DESKTOP-9K104BT   source = WinEventLog:Security   sourcetype = WinEventLog:Security
12/2/24 3:31:50.000 PM	... 4 lines omitted ... ComputerName=DESKTOP-9K104BT SourceName=Microsoft Windows security auditing. Type=Informazioni ... 18 lines omitted ... ID processo: 0x7f8 Nome processo: C:\Windows\System32\wbem\WmiPrvSE.exe Show all 27 lines host = DESKTOP-9K104BT   source = WinEventLog:Security   sourcetype = WinEventLog:Security

