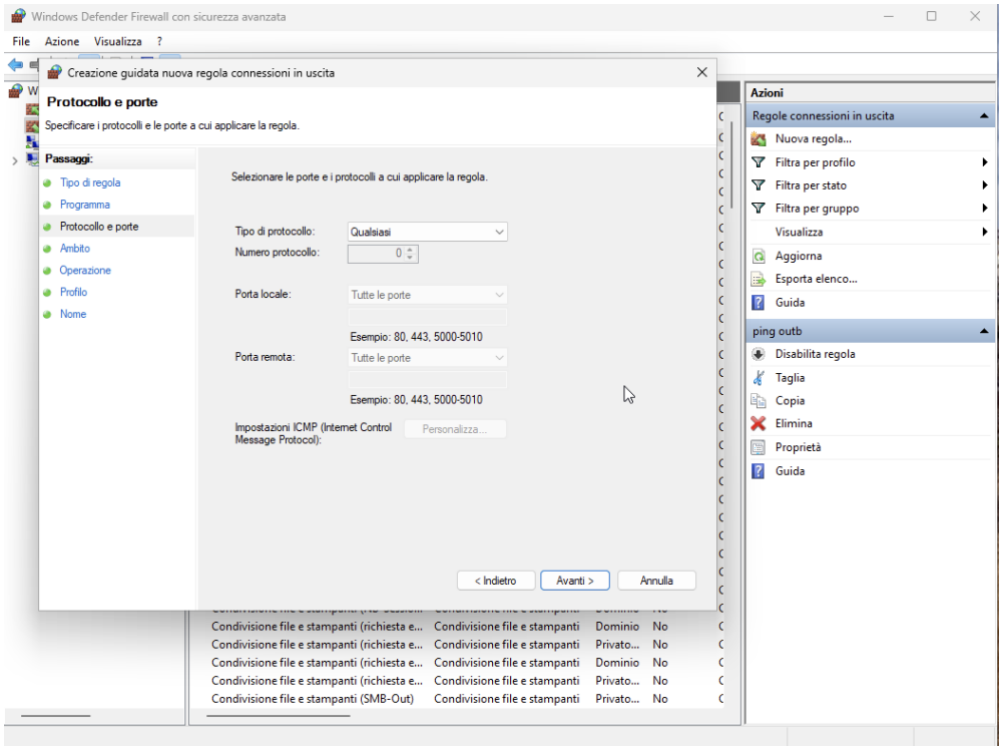
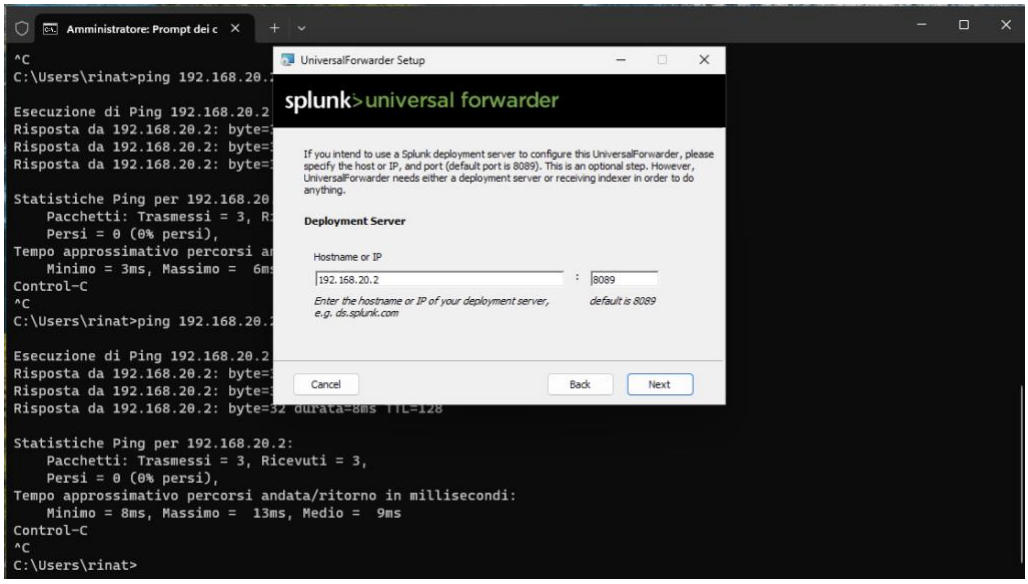
RAPPORRTO

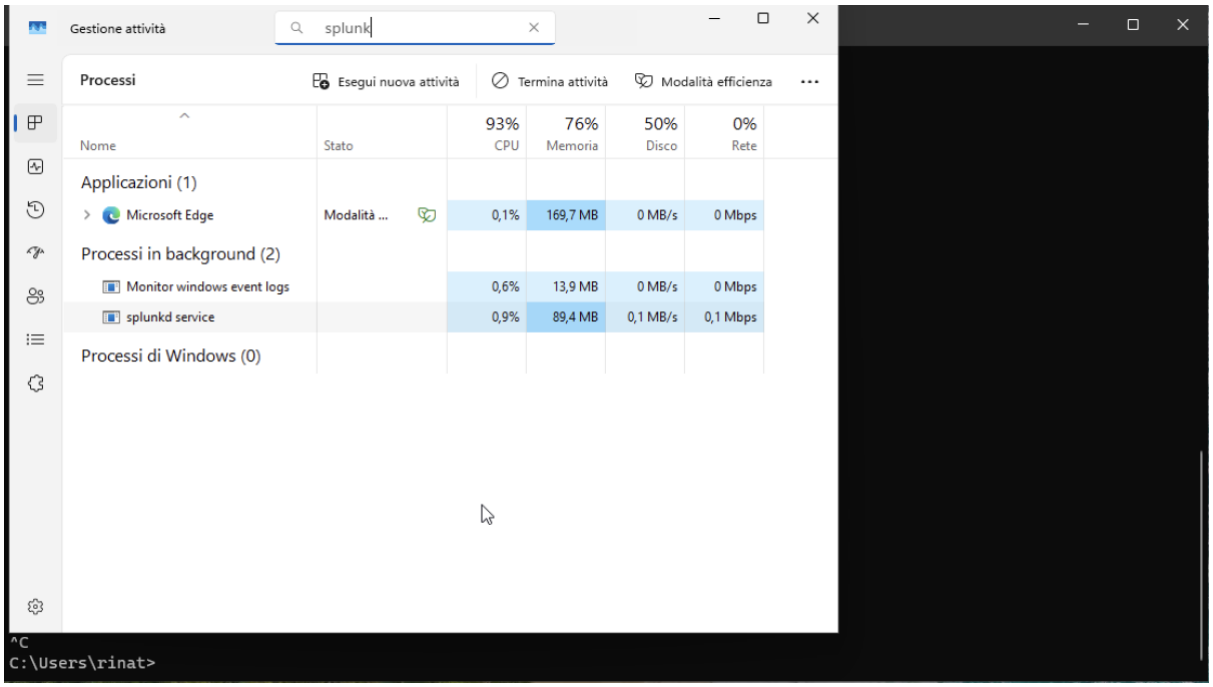
La prima cosa che ho fatto è stata creare policy firewall in entrata e in uscita per entrambe le macchine virtuali:



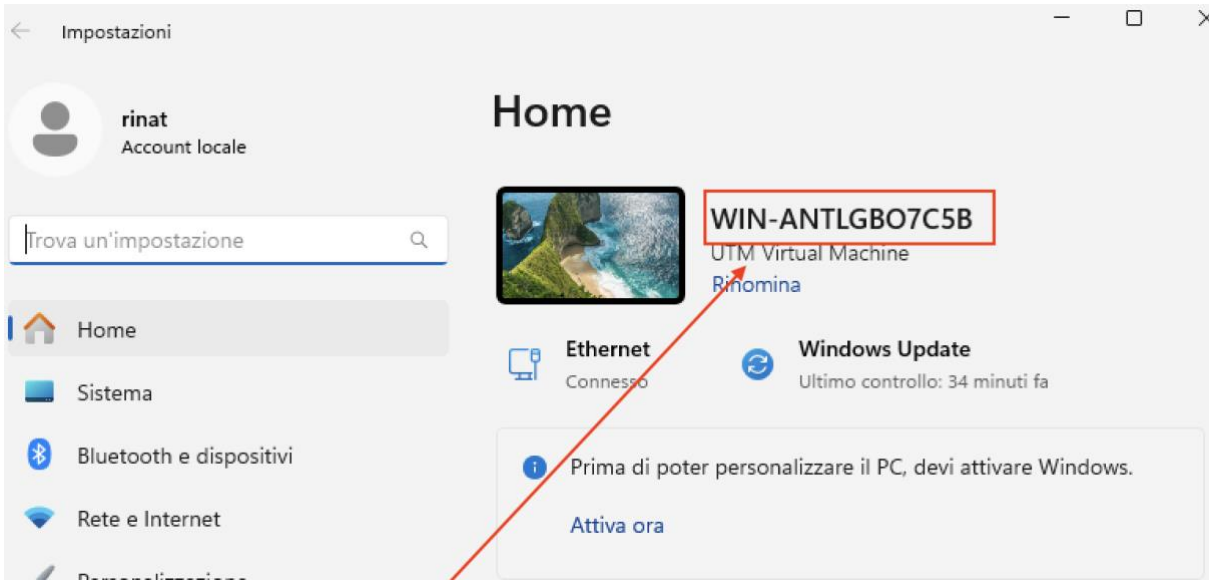
Quindi ho scaricato il software di inoltro Splunk, l'ho configurato e ho anche aggiunto la porta 9997 in localhost:8000:



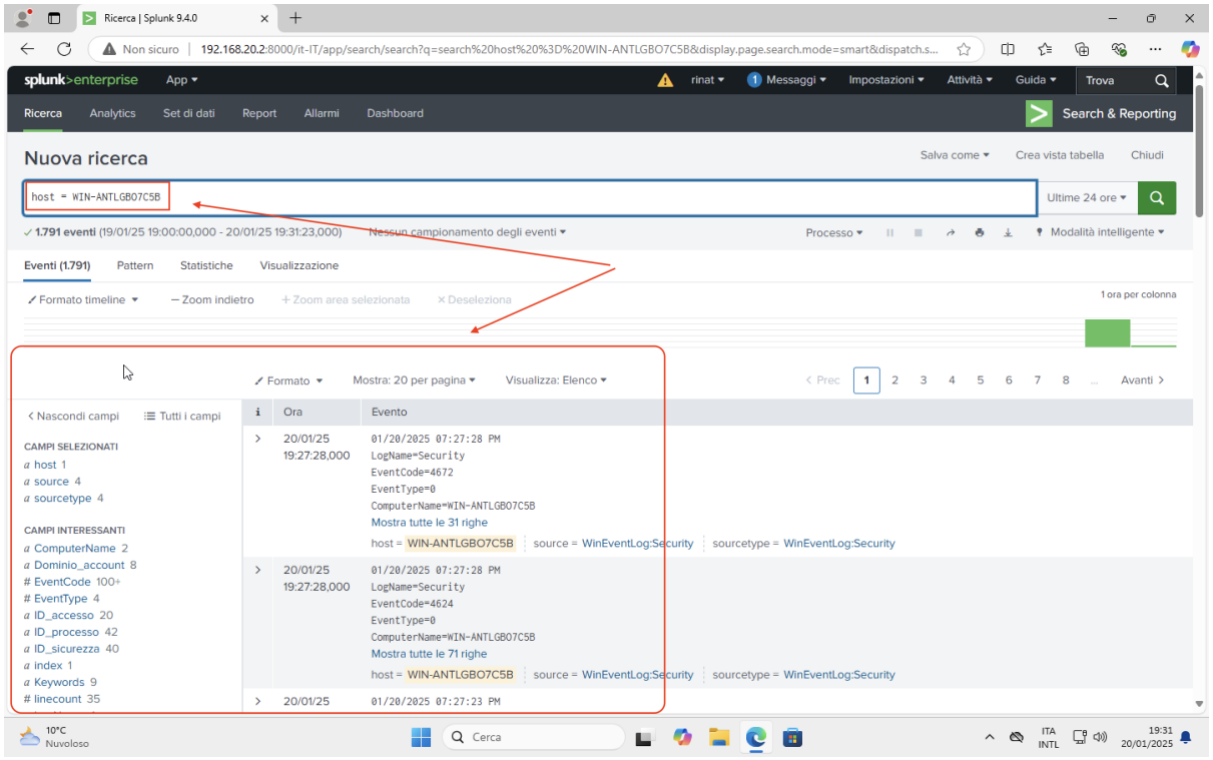
Successivamente ho verificato se la configurazione funziona correttamente:



Poi ho cercato il nome dell'host che verrà monitorato tramite Splunk:



Ho quindi cercato questo host in Splunk e i risultati sono quelli previsti:


Ricerca | Splunk 9.4.0
Non sicuro | 192.168.20.2:8000/it-IT/app/search/search?q=search%20host%20%3D%20WIN-ANTLGBO7C5B&display.page.search.mode=smart&dispatch.s...
splunk>enterprise
App
rinat
Messaggi
Impostazioni
Attività
Guida
Trova
Ricerca
Analytics
Set di dati
Report
Allarmi
Dashboard
Search & Reporting
Nuova ricerca
Salva come
Crea vista tabella
Chiudi
host = WIN-ANTLGBO7C5B
Ultime 24 ore
1.791 eventi (19/01/25 19:00:00,000 - 20/01/25 19:31:23,000)
Nessun campionamento degli eventi
Processo
Modalità intelligente
Eventi (1.791)
Pattern
Statistiche
Visualizzazione
Formato timeline
Zoom indietro
Zoom area selezionata
Deseleziona
1 ora per colonna
Formato
Mostra: 20 per pagina
Visualizza: Elenco
Prec
1 2 3 4 5 6 7 8
Avanti
Nascondi campi
Tutti i campi
CAMPI SELEZIONATI
a host 1
a source 4
a sourcetype 4
CAMPI INTERESSANTI
a ComputerName 2
a Dominio_account 8
EventCode 100+
EventType 4
a ID_accesso 20
a ID_processo 42
a ID_sicurezza 40
a index 1
a Keywords 9
linecount 35
Ora
Evento
20/01/25 19:27:28,000
01/20/2025 07:27:28 PM
LogName=Security
EventCode=4672
EventType=0
ComputerName=WIN-ANTLGBO7C5B
Mostra tutte le 31 righe
host = WIN-ANTLGBO7C5B
source = WinEventLog:Security
sourcetype = WinEventLog:Security
20/01/25 19:27:28,000
01/20/2025 07:27:28 PM
LogName=Security
EventCode=4624
EventType=0
ComputerName=WIN-ANTLGBO7C5B
Mostra tutte le 71 righe
host = WIN-ANTLGBO7C5B
source = WinEventLog:Security
sourcetype = WinEventLog:Security
20/01/25
01/20/2025 07:27:23 PM
10°C
Nuvoloso
Cerca
ITA
INTL
19:31
20/01/2025