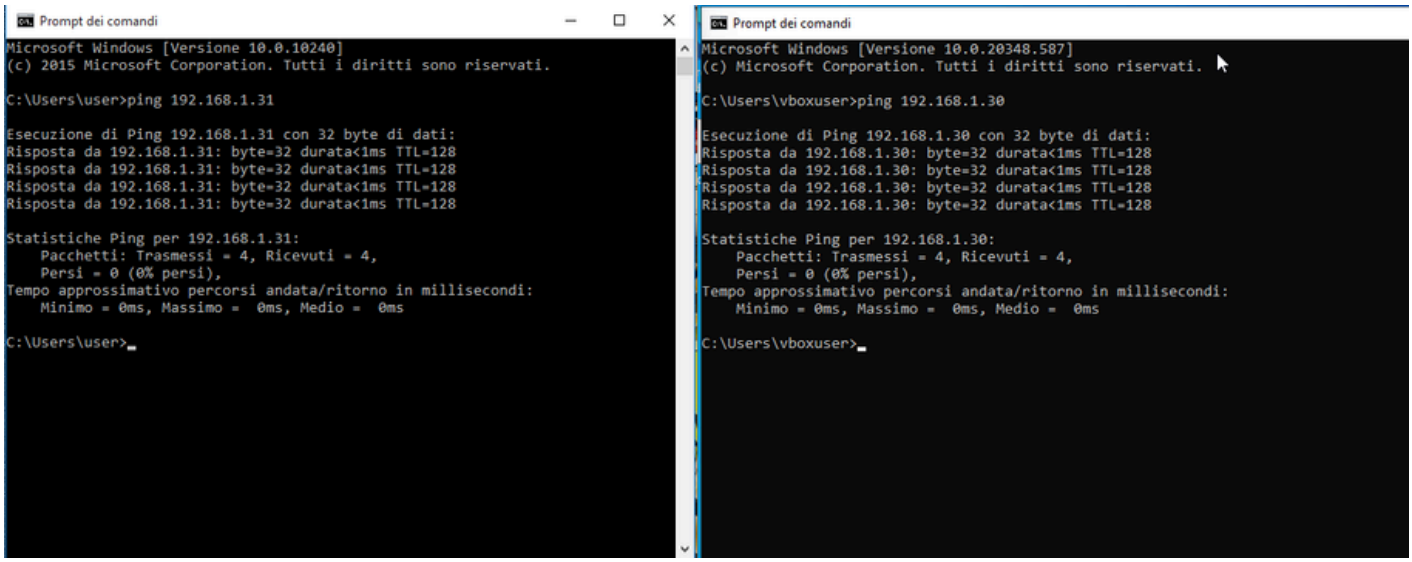
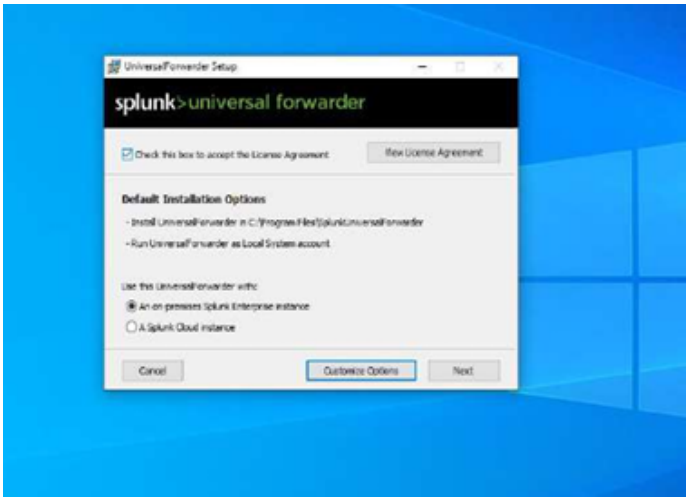
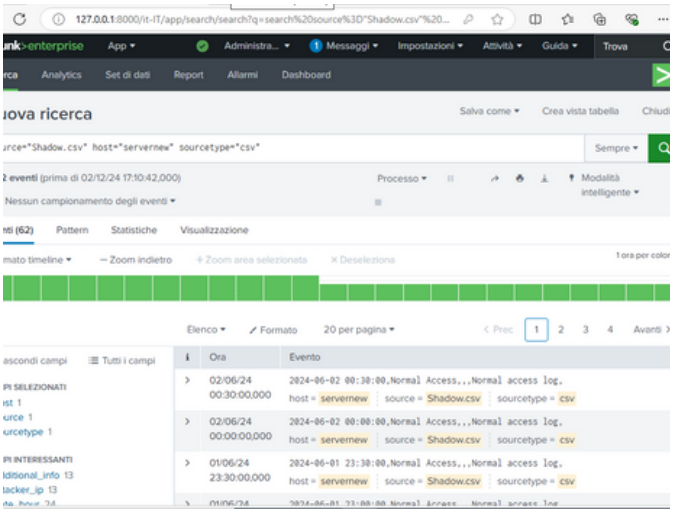
# Configurazione della Modalità Monitora in Splunk

Configuriamo le due macchine in maniera tale che possano comunicare

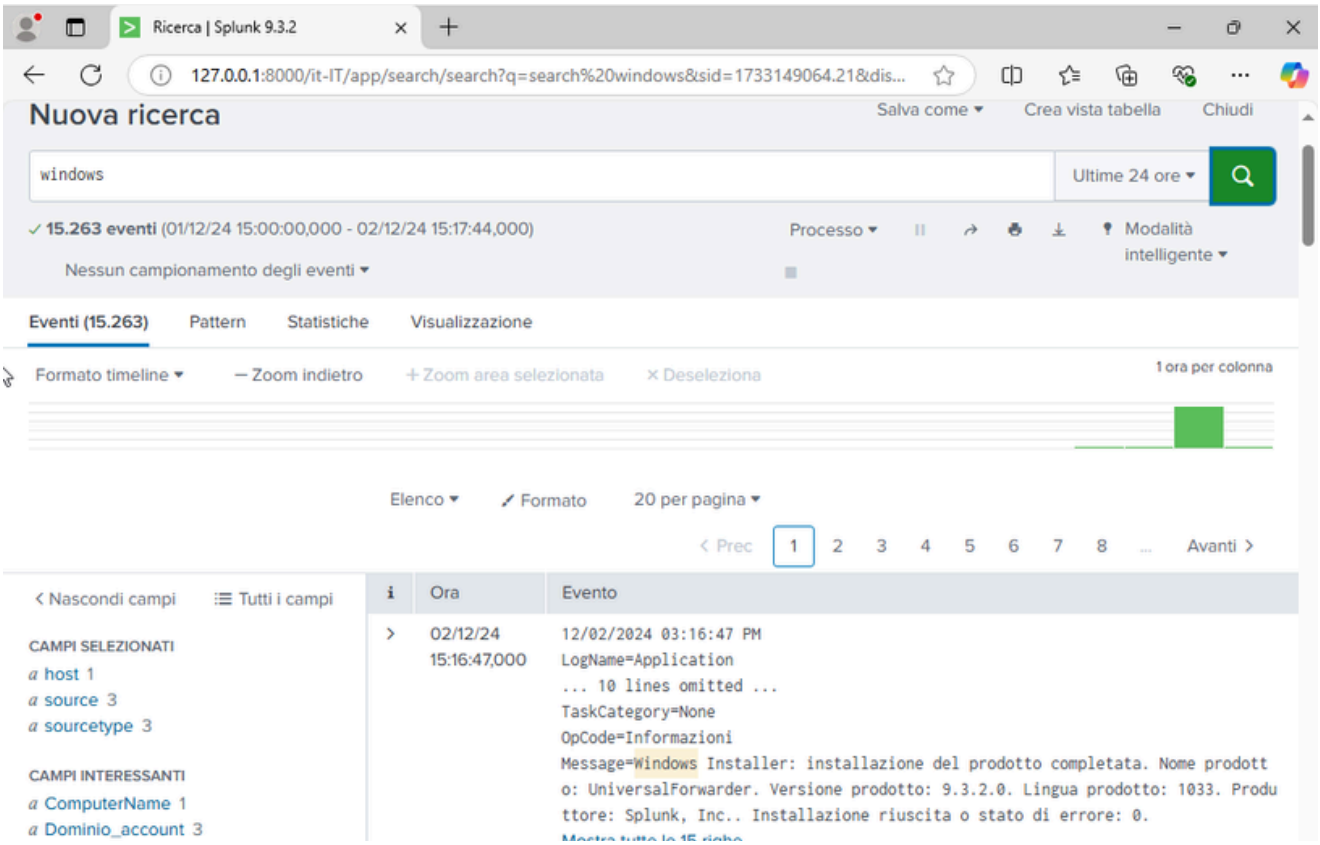



Scarichiamo Splunk forwarder per la macchina di windows 10 e splunk enterprice per la macchina server.



Colleghiamo i due Splunk in modo che possano comunicare. Subito dopo, faremo una prova per verificare se i log vengono letti correttamente.




Splunk è una piattaforma software avanzata progettata per raccogliere, analizzare e visualizzare i dati generati da macchine in tempo reale. È ampiamente utilizzato per la gestione dei log e il monitoraggio delle infrastrutture IT, offrendo alle aziende strumenti per prendere decisioni basate su informazioni concrete. La sua capacità di raccogliere dati da diverse fonti, come server, applicazioni, dispositivi di rete e sistemi operativi, lo rende estremamente versatile. Splunk indicizza i dati per consentire ricerche rapide e flessibili, fornendo al contempo strumenti di analisi avanzati e dashboard interattivi per la rappresentazione visiva. È particolarmente utile per il monitoraggio della sicurezza, la gestione centralizzata dei log, l'ottimizzazione dei processi aziendali e il controllo delle prestazioni IT. Sebbene presenti vantaggi significativi, come scalabilità, personalizzazione e un'interfaccia intuitiva, il software può risultare costoso e richiede competenze tecniche per configurazioni avanzate. Nonostante ciò, Splunk rappresenta una soluzione essenziale per le aziende che desiderano ottimizzare il monitoraggio dei dati e migliorare la sicurezza e le prestazioni delle loro infrastrutture.