

# Configurazione della Modalità Monitora in Splunk

Configuriamo le due macchine in maniera tale che possano comunicare

```
Microsoft Windows [Versione 10.0.10240]
(c) 2015 Microsoft Corporation. Tutti i diritti sono riservati.

C:\Users\user>ping 192.168.1.31

Esecuzione di Ping 192.168.1.31 con 32 byte di dati:
Risposta da 192.168.1.31: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.31: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.31: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.31: byte=32 durata<1ms TTL=128

Statistiche Ping per 192.168.1.31:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\Users\user>
```

```
Microsoft Windows [Versione 10.0.20348.587]
(c) Microsoft Corporation. Tutti i diritti sono riservati.

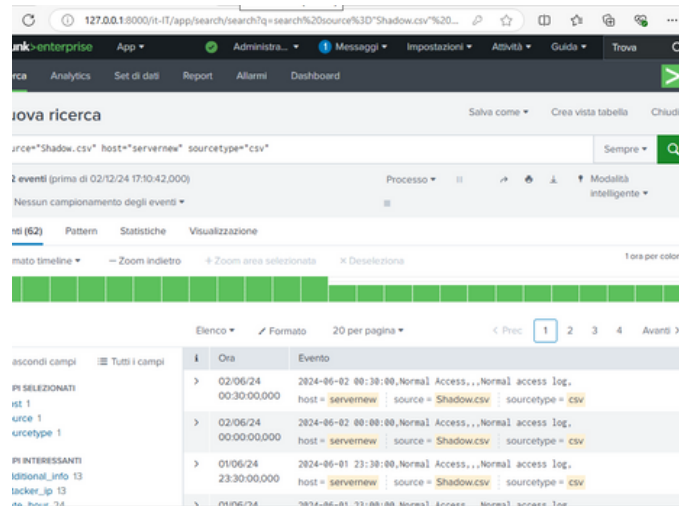
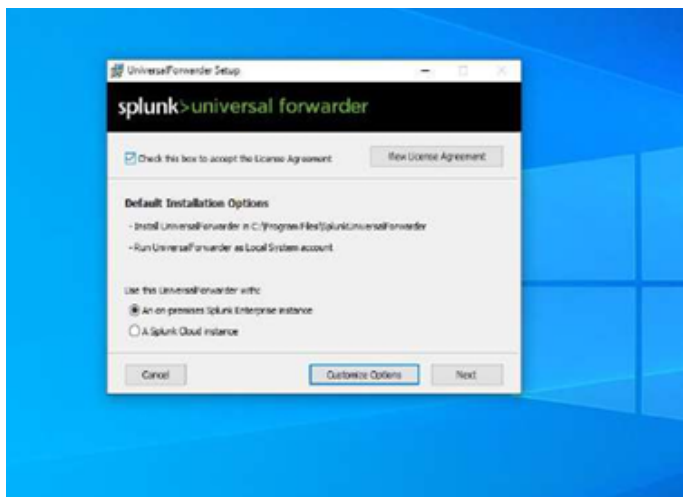
C:\Users\vboxuser>ping 192.168.1.30

Esecuzione di Ping 192.168.1.30 con 32 byte di dati:
Risposta da 192.168.1.30: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.30: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.30: byte=32 durata<1ms TTL=128
Risposta da 192.168.1.30: byte=32 durata<1ms TTL=128

Statistiche Ping per 192.168.1.30:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
        Minimo = 0ms, Massimo = 0ms, Medio = 0ms

C:\Users\vboxuser>
```

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



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

The screenshot shows the Splunk search interface. At the top, the search bar contains the query 'windows'. Below the search bar, it indicates '15.263 eventi (01/12/24 15:00:00,000 - 02/12/24 15:17:44,000)'. The interface includes a timeline visualization and a list of events. The first event is highlighted, showing details like 'LogName=Application' and 'Message=Windows Installer: installazione del prodotto completata.' The interface also includes a sidebar with 'CAMPI SELEZIONATI' and 'CAMPI INTERESSANTI'.

i	Ora	Evento
>	02/12/24 15:16:47,000	12/02/2024 03:16:47 PM LogName=Application ... 10 lines omitted ... TaskCategory=None OpCode=Informazioni Message=Windows Installer: installazione del prodotto completata. Nome prodotto: UniversalForwarder. Versione prodotto: 9.3.2.0. Lingua prodotto: 1033. Produttore: Splunk, Inc.. Installazione riuscita o stato di errore: 0.



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.