

## Relazione Monitora Splunk

Nella seguente immagine e prima di iniziare l'installazione di di **Splunk Universal Forwarder**, verifichiamo che ci sia comunicazione tra la **VM Server** e la **VM Client** con il comando **ipconfig**

```
Windows PowerShell
Copyright (C) Microsoft Corporation. Tutti i diritti riservati.

Prova la nuova PowerShell multiplatforma https://aka.ms/pscore6

PS C:\Users\User> ipconfig

Configurazione IP di Windows

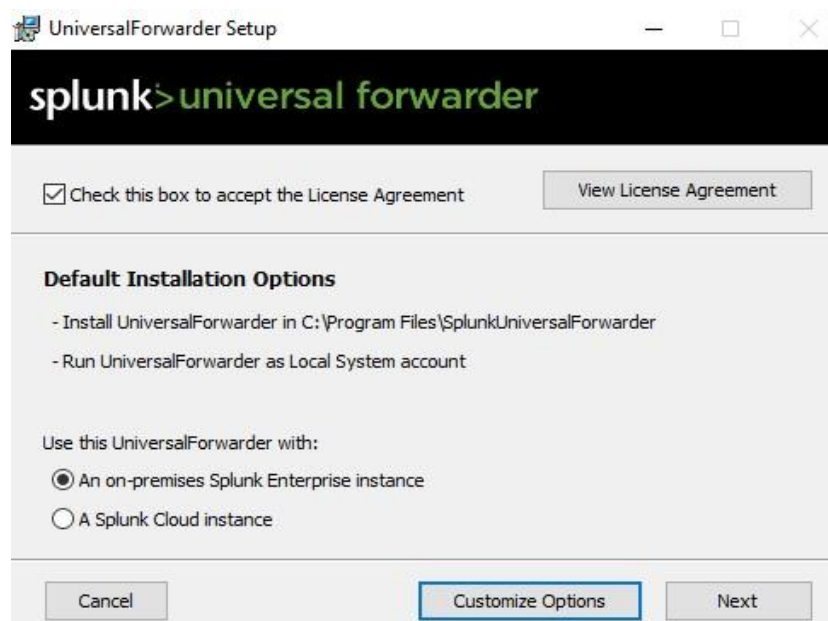
Scheda Ethernet Ethernet:

    Suffisso DNS specifico per connessione: station
    Indirizzo IPv6 locale rispetto al collegamento . : fe80::53cc:ec63:332:e849%5
    Indirizzo IPv4. . . . . : 192.168.1.38
    Subnet mask . . . . . : 255.255.255.0
    Gateway predefinito . . . . . : 192.168.1.1
PS C:\Users\User> ping 192.168.1.37

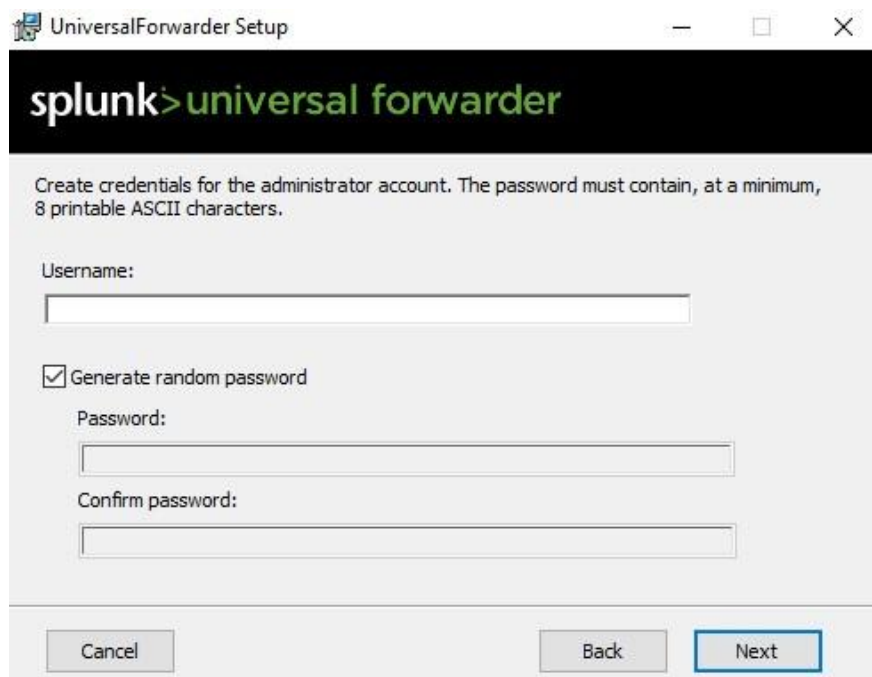
Esecuzione di Ping 192.168.1.37 con 32 byte di dati:
Risposta da 192.168.1.37: byte=32 durata=3ms TTL=128
Risposta da 192.168.1.37: byte=32 durata=1ms TTL=128
Risposta da 192.168.1.37: byte=32 durata=1ms TTL=128
Risposta da 192.168.1.37: byte=32 durata=3ms TTL=128

Statistiche Ping per 192.168.1.37:
    Pacchetti: Trasmessi = 4, Ricevuti = 4,
    Persi = 0 (0% persi),
    Tempo approssimativo percorsi andata/ritorno in millisecondi:
    Minimo = 0ms, Massimo = 3ms, Medio = 1ms
PS C:\Users\User>
```

Nella seguente immagine e primo passaggio, dopo aver installato **Splunk Universal Forwarder**, clicco sul pulsante, **Customize Options**, dove, posso selezionare tutte le opzioni e scegliere, cosa analizzare con **Splunk** dalla mia Virtual Machine (**Server**)

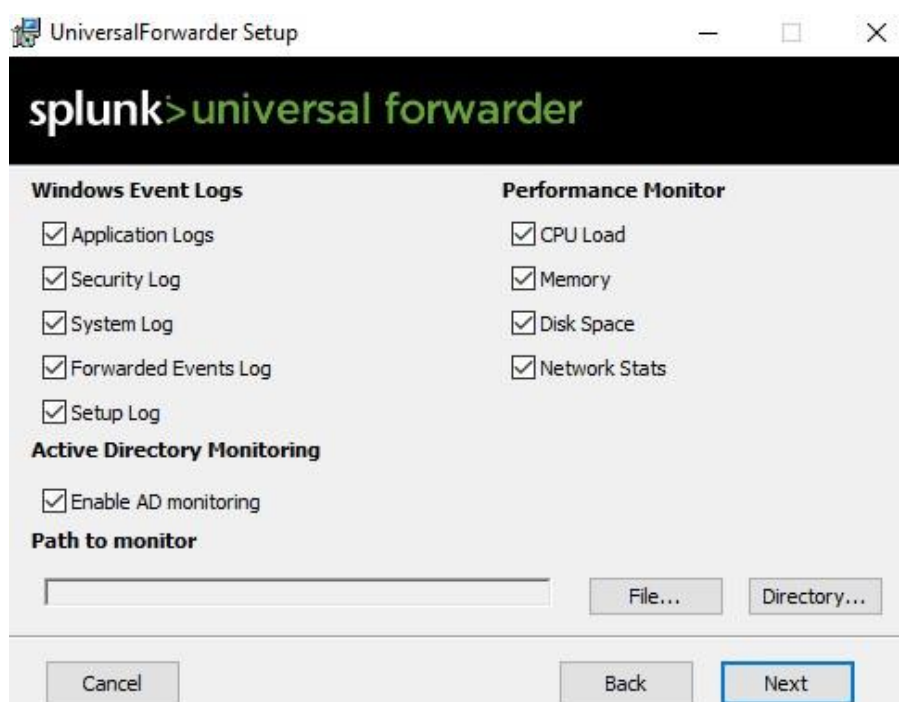


Dopo aver inserito i dati richiesti in **Deployment Server** e **Receiving Indexer**, clicchiamo su next ed abbiamo la pagina in cui scegliamo **Username** e **Password**, come illustrato di seguito:



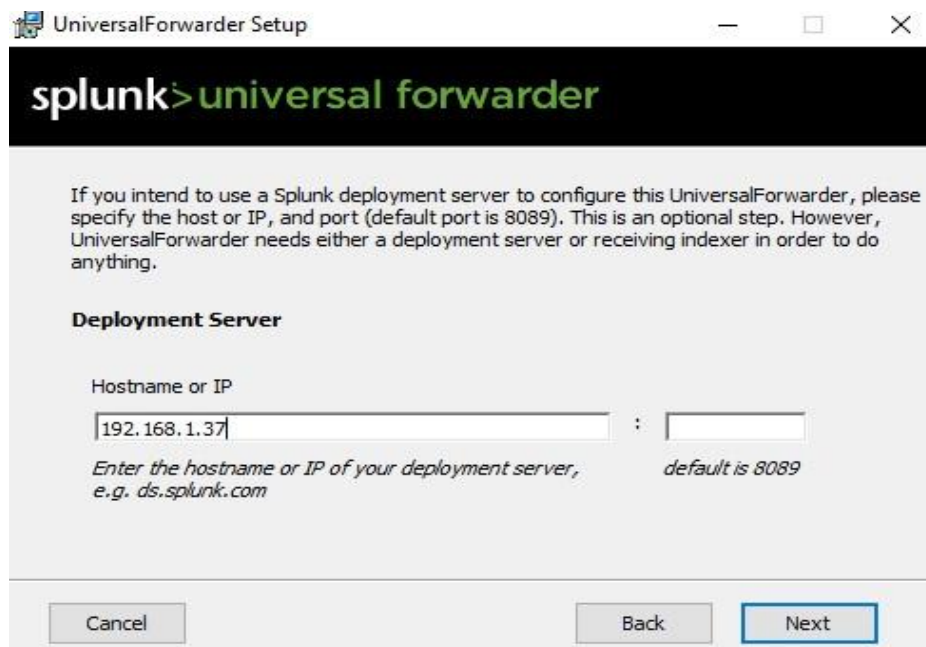
The screenshot shows the 'UniversalForwarder Setup' window. At the top, there's a black header with the 'splunk>universal forwarder' logo. Below the header, a message states: 'Create credentials for the administrator account. The password must contain, at a minimum, 8 printable ASCII characters.' The form includes a 'Username:' label followed by a text input field. Below that is a checked checkbox labeled 'Generate random password'. Underneath, there are 'Password:' and 'Confirm password:' labels, each followed by a text input field. At the bottom, there are three buttons: 'Cancel', 'Back', and 'Next' (which is highlighted with a blue border).

Come descritto in precedenza e come da immagini allegate al seguito, possiamo vedere dall'immagine sottostante le varie opzioni da selezionare e quindi, da analizzare con **Splunk**



The screenshot shows the 'UniversalForwarder Setup' window with the 'Monitoring' options. The window has the same header as the previous one. The main content area is divided into two columns. The left column is titled 'Windows Event Logs' and contains five checked checkboxes: 'Application Logs', 'Security Log', 'System Log', 'Forwarded Events Log', and 'Setup Log'. Below these is a section titled 'Active Directory Monitoring' with one checked checkbox: 'Enable AD monitoring'. At the bottom of this column is a section titled 'Path to monitor' with a text input field and two buttons: 'File...' and 'Directory...'. The right column is titled 'Performance Monitor' and contains four checked checkboxes: 'CPU Load', 'Memory', 'Disk Space', and 'Network Stats'. At the bottom of the window, there are three buttons: 'Cancel', 'Back', and 'Next' (which is highlighted with a blue border).

Nella seguente immagine dopo aver selezionato le opzioni come visto in precedenza, dobbiamo settare l'IP del nostro Server, come illustrato di seguito, ma senza inserire la porta:



UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk deployment server to configure this UniversalForwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

**Deployment Server**

Hostname or IP

192.168.1.37 :

*Enter the hostname or IP of your deployment server, e.g. ds.splunk.com* *default is 8089*

Cancel Back Next

Nella seguente immagine dopo aver inserito l'IP in **Deployment Server** dobbiamo settare l'IP in **Receiving Indexer** del nostro Server, inserendo questa volta anche la porta, come illustrato di seguito:



UniversalForwarder Setup

splunk>universal forwarder

If you intend to use a Splunk receiving indexer to configure this UniversalForwarder, please specify the host or IP, and port (default port is 9997). This is an optional step. However, UniversalForwarder needs either a deployment server or receiving indexer in order to do anything.

**Receiving Indexer**

Hostname or IP

192.168.1.37 : 9997

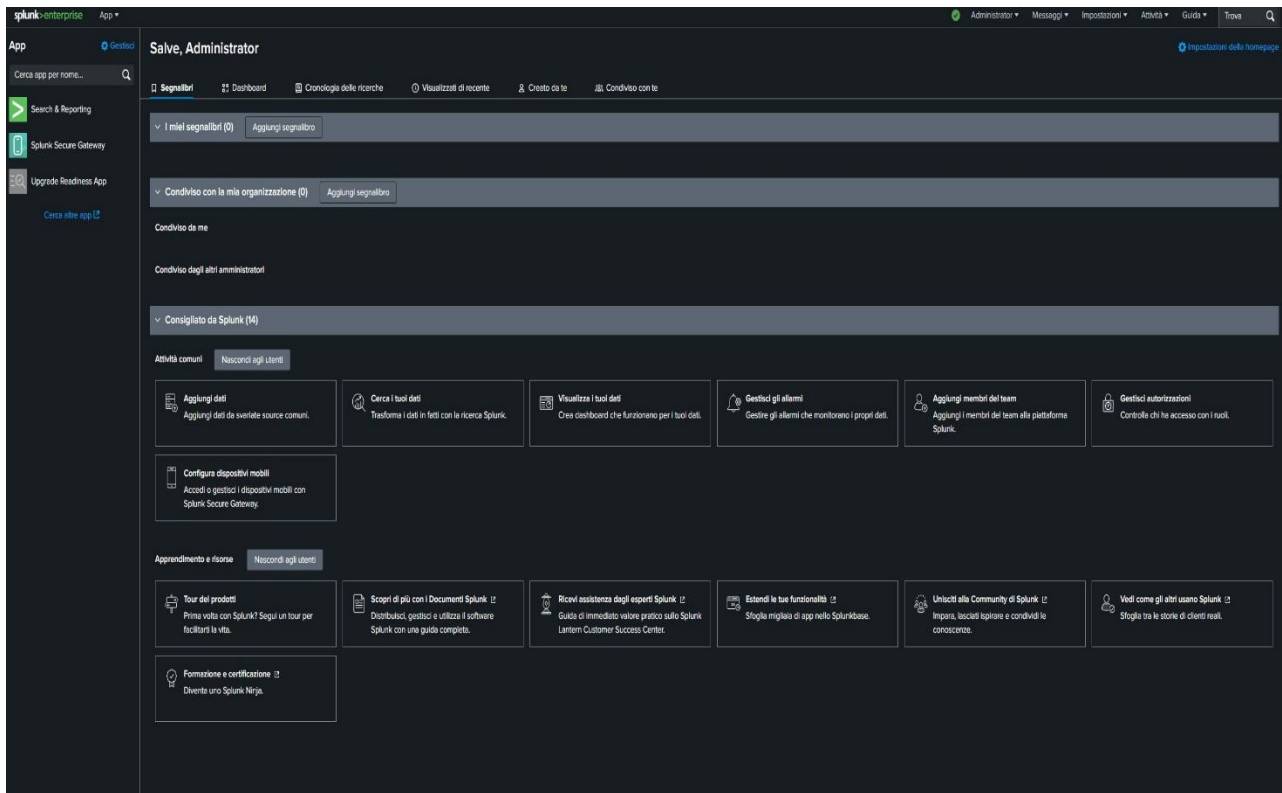
*Enter the hostname or IP of your receiving indexer, e.g. ds.splunk.com* *default is 9997*

Cancel Back Next

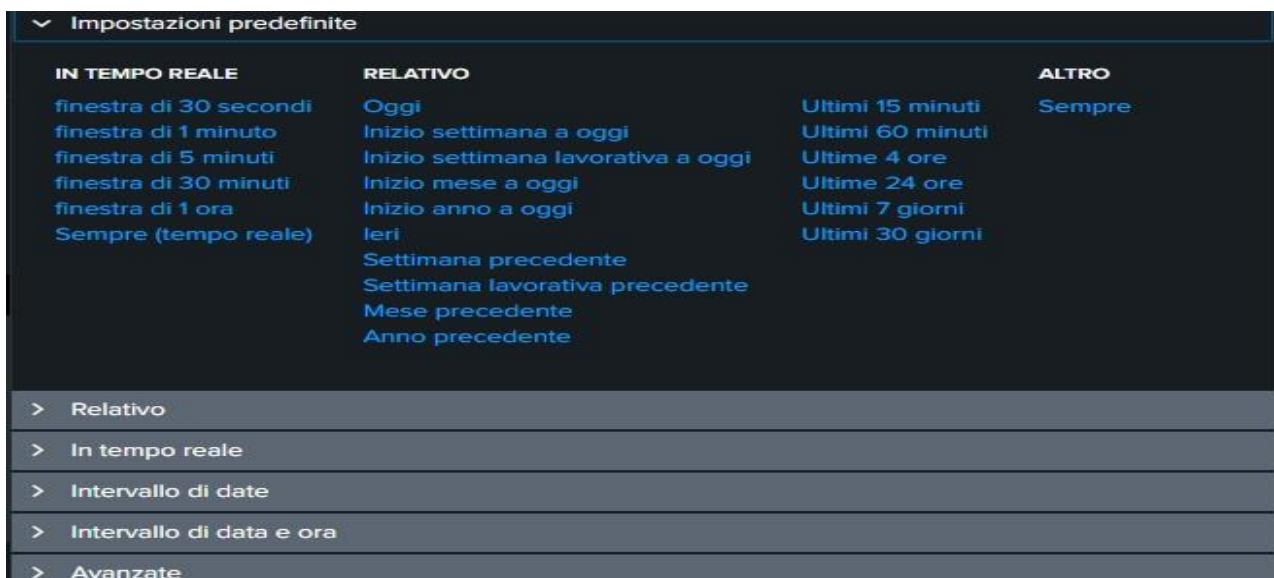
Prima di procedere con l'analisi del nostro **Client**, dobbiamo configurare la porta di ascolto, per far sì che si possa procedere con **Splunk**; come da seguente immagine, dobbiamo andare nella colonna **DATI**, cliccare sulla voce **Inoltro e ricezione**, dove dobbiamo inserire la porta di ascolto, andando in alto a destra su **Nuova porta di ricezione**, ed inserire la porta scelta:



Dopo aver inserito la porta come sopra descritto ed illustrato nelle immagini, torniamo sulla Home di **Splunk**, cliccando su **splunk>enterprise** e clicchiamo sulla scheda **Cerca i tuoi dati**, dove ci troviamo sulla pagina di analisi, in cui abbiamo la stringa per le ricerche specifiche (in questo caso il **Client – VM Windows**), come illustrato nella seguenti immagini:



Prima di procedere con la ricerca e l'analisi del nostro Client, andando sulla scheda a destra, **Impostazioni predefinite**, scegliamo l'opzione **Ultimi 60 minuti**, di tutte le operazioni svolte sul nostro **Client**:



Come descritto in precedenza, di seguito, nella stringa di ricerca, nel nostro caso, scriviamo windows, e cliccando sulla lente di ricerca a destra, avremo i risultati della **VM Windows Client**:

windows

✓ 124 eventi (14/10/24 13:40:00,000 - 14/10/24 14:40:35,000) Nessun campionamento degli eventi

Eventi (124) Pattern Statistiche Visualizzazione

Formato timeline Zoom indietro + Zoom area selezionata x Deseleziona

< Nascondi campi Tutti i campi

CAMPI SELEZIONATI

# EventType 4

a host 1

a source 3

a sourcetype 3

CAMPI INTERESSANTI

a ComputerName 1

a Dominio\_account 3

# EventCode 15

a ID\_accesso 2

a ID\_sicurezza 4

a index 1

a Keywords 6

# linecount 9

a LogName 3

a Message 32

a Nome\_account 3

Elenco Formato 20 per pagina

i	Ora	Evento
>	14/10/24 14:14:45,000	10/14/2024 02:14:45 PM ... 2 lines omitted ... EventType=0 ComputerName=DESKTOP-8CAJRTO SourceName=Microsoft Windows security auditing. Type=Informazioni <a href="#">Mostra tutte le 31 righe</a> EventType = 0   host = DESKTOP-8CAJRTO   source = WinEventLog:Security   sourcetype = WinEventLog:Security
>	14/10/24 14:14:45,000	... 4 lines omitted ... ComputerName=DESKTOP-8CAJRTO SourceName=Microsoft Windows security auditing. Type=Informazioni ... 31 lines omitted ... ID processo: 0x2d8 Nome processo: C:\Windows\System32\services.exe <a href="#">Mostra tutte le 70 righe</a> EventType = 0   host = DESKTOP-8CAJRTO   source = WinEventLog:Security   sourcetype = WinEventLog:Security

A sinistra della pagina di analisi di **Splunk**, cliccando su **host**, vedo il risultato degli eventi, in questo caso **169 eventi**, il **100%** degli eventi del **Client**:

host

1 Valore, 100% di eventi

Selezionato Sì No

Report

Primi valori Primi valori nel tempo Valori rari

Eventi con questo campo

Valori	Conteggio	%
DESKTOP-8CAJRTO	169	100%



Sempre sulla parte sinistra della pagina di analisi di Splunk, cliccando su **source**, posso vedere tre diversi tipi di log di Windows e le fonti da dove provengono, in questo caso:

- **WinEventLog: Security: 92 eventi (54%)**
- **WinEventLog: System: 54 eventi (31,95%)**
- **WinEventLog: Application: 23 eventi (13,61%)**



The screenshot shows the 'source' panel in Splunk. At the top, it says '3 Valori, 100% di eventi'. Below this, there are three tabs: 'Primi valori', 'Primi valori nel tempo', and 'Valori rari'. The 'Primi valori' tab is selected. Below the tabs, there is a table with three columns: 'Valori', 'Conteggio', and '%'. The table lists three event types: 'WinEventLog:Security' with a count of 92 and a percentage of 54,438%, 'WinEventLog:System' with a count of 54 and a percentage of 31,953%, and 'WinEventLog:Application' with a count of 23 and a percentage of 13,609%. To the right of the table, there are three vertical bars representing the relative counts of each event type.

Valori	Conteggio	%
WinEventLog:Security	92	54,438%
WinEventLog:System	54	31,953%
WinEventLog:Application	23	13,609%