

Dopo aver fatto l'accesso a Splunk, sono andato nella sezione "Aggiungi dati" e "Carica file dal mio computer" per caricare il file "ssh.log" della consegna:

The screenshot shows the Splunk 'Add Data' wizard. The first screen, titled 'Quali dati vuoi inviare alla piattaforma Splunk?', lists various data sources. The 'Carica' (Upload) option is highlighted with a green box. The second screen, 'Seleziona source', shows the file 'ssh.log' selected, also highlighted with a green box.

Salve, Administrator

Segnalibri Dashboard Cronologia delle ricerche Visualizzati di recente Creato da te Condiviso con te

▼ I miei segnalibri (0) Aggiungi segnalibro

▼ Condiviso con la mia organizzazione (0) Aggiungi segnalibro

Condiviso da me

Condiviso dagli altri amministratori

▼ Consigliato da Splunk (13)

Aggiungi dati
Aggiungi dati da svariate source comuni.

Cerca i tuoi dati
Trasforma i dati in fatti con la ricerca Splunk.

Visualizza i tuoi dati
Crea dashboard che funzionano per i tuoi dati.

Gestisci gli allarmi
Gestire gli allarmi che mo

Aggiungi membri del team
Aggiungi i membri del team alla piattaforma Splunk.

Gestisci autorizzazioni
Controlla chi ha accesso con i ruoli.

Configura dispositivi mobili
Accedi o gestisci i dispositivi mobili con Splunk Secure Gateway.

Quali dati vuoi inviare alla piattaforma Splunk?

Seguire le guide sull'onboarding delle fonti di dati più popolari

Cloud computing
Get your cloud computing data in to the Splunk platform.
10 fonti di dati

Collegamento in rete
Immettere i dati di rete nella piattaforma Splunk.
2 fonti di dati

Sistema operativo
Immettere i dati del sistema operativo nella piattaforma Splunk.
1 fonte di dati

Sicurezza
Immettere i dati di sicurezza nella piattaforma Splunk.
3 fonti di dati

4 fonti di dati in totale

Oppure, inserisci i dati utilizzando uno dei seguenti metodi

Carica
file dal mio computer
File di log locali
File strutturati locali (ad es. CSV)
[Esercitazione per l'aggiunta di dati](#)

Monitora
file e porte su questa istanza della piattaforma Splunk
File - HTTP - WMI - TCP/UDP - Script
Input modulari per le fonti dati esterne

Inoltra
dati da un forwarder di Splunk
File - TCP/UDP - Script

Aggiungi dati

Selezione source Imposta source type Impostazioni di input Verifica Fine

< Indietro Avanti >

Seleziona source

Scegliere un file da caricare nella piattaforma Splunk, cercando nel computer oppure trascinandolo nella casella di destinazione qui di seguito. [Ulteriori inf](#)

File selezionato: **ssh.log**

Seleziona file

Dopo aver visionato i dati, inserito il source type e lasciando le impostazioni di default, sono arrivato alla schermata dov'era possibile inserire dei filtri per ottimizzare la ricerca:



ma Splunk visualizza i dati prima dell'indicizzazione. Se gli eventi appaiono corretti e hanno i
In caso contrario, utilizzare le opzioni di seguito per definire le suddivisioni in eventi e i
source type appropriato per i dati, crearne uno nuovo facendo clic su "Salva come".

Salva come	Formato	Mostra: 20 per pagina	Visualizza: Elenco
	Ora	Evento	
1	10/02/25 16:42:26,000	1331901811.840000 - timestamp = none	CTHc0o3BARDOPjYue 192.168.202.68 53633 192.168.28.254 22 failure INBOUND
2	10/02/25 16:42:26,000	1331901830.210000 -	CBHpSz2Z13rdkbAwvd 192.168.202.68 35820 192.168.23.254 22 failure INBOUND

Salva source type

Nome

Prova

Descrizione

Categoria

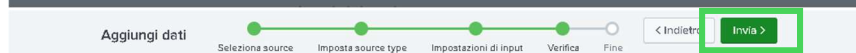
Personalizzata ▼

App

Search & Reporting ▼

Annulla

Salva



Verifica

Tipo di input File caricato
Nome file ssh.log
Source type Prova
Host
Indice Default

Aggiungi dati

Selezione source

Imposta source type

Impostazioni di input

Verifica

Fine

< Indietro

Avanti >

✓

File è stato caricato correttamente.

Configurare gli input da Impostazioni > [Input dati](#)

Avvia ricerca

Eseguire una ricerca tra i dati ora oppure visualizzare [esempi ed esercitazioni](#).

Estrai campi

Creare estrazioni di campi search-time. [Ulteriori informazioni sui campi](#).

Aggiungi altri dati

Aggiungere altri input di dati ora oppure visualizzare [esempi ed esercitazioni](#).

Scarica app

Le app consentono di fare di più con i propri dati. [Ulteriori informazioni](#).

Crea dashboard

Visualizza le ricerche. [Ulteriori informazioni](#).

✓ 14.286 eventi prima di 10/02/25 16:43:56,000) Nessun campionamento degli eventi ▼

Eventi (14.286) Pattern Statistiche Visualizzazione

Formato timeline ▼ Zoom indietro + Zoom area selezionata X Deseleziona

Formato ▼ Mostra: 50 per pagina ▼ Visualizza: Elenco ▼

< Nascondi campi Tutti i campi

CAMPI SELEZIONATI
a host 1
a source 1
a sourcetype 1

CAMPI INTERESSANTI
a index 1
linecount 1
a punct 19
a splunk_server 1
a timestamp 1

+ Estrai nuovi campi

i	Ora	Evento
>	10/02/25 16:43:43,000	1332016697.010000 CvEd9z3v2QM9aIBfbd 192.168.202.69 378 host = [redacted] source = ssh.log sourcetype = Prova
>	10/02/25 16:43:43,000	1332017793.040000 CrUTZx1hjVklqFFTl1 192.168.202.136 568 - - - host = [redacted] source = ssh.log sourcetype = Prova
>	10/02/25 16:43:43,000	1332017778.370000 CZhg1136uZbVNG8uYl 192.168.202.136 568 - - - host = [redacted] source = ssh.log sourcetype = Prova
>	10/02/25 16:43:43,000	1332017154.520000 C0XOE9Wej5K5IETpj 192.168.202.136 568 - - - host = [redacted] source = ssh.log sourcetype = Prova
>	10/02/25 16:43:43,000	1332017111.420000 CB4eVG4sDCR1pFqRa 192.168.202.136 411 - - - host = [redacted] source = ssh.log sourcetype = Prova
>	10/02/25 16:43:43,000	1332017087.510000 COkT4dasAfZ4hxP9i 192.168.202.136 411 - - - host = [redacted] source = ssh.log sourcetype = Prova

Selezione evento di esempio

Scegliere una source o un source type, selezionare un evento campione e fare clic su Avanti per continuare con il passaggio successivo. L'estrattore di campi userà l'evento per estrarre i campi. [Ulteriori informazioni](#)

[Preferisco scrivere io stesso l'espressione regolare >](#)

Source type

[Prova](#)

Intervallo temporale

Ultima 90 giorni ▼

Eventi

✓ 1.000 evento (12/11/24 00:00:00,000 - 10/02/25 16:44:14,000)

20 per pag

raw ↕

1332016697.210000	CyEd9z3v2QM9aIPfbd	192.168.202.69	37012	192.168.28.253	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_4.5	-	-	-
1332017793.040000	CrUTZx1hjVkJqFFT1i	192.168.202.136	56815	192.168.21.203	22	Failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	
1332017778.370000	CZhG1136uZbVNG8uYL	192.168.202.136	56814	192.168.21.203	22	Failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	
1332017154.520000	C0XOE9wej5K5IETpj	192.168.202.136	56802	192.168.21.203	22	undetermined	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1	
1332017111.420000	CB4eVG4sDCRT1pFaRa	192.168.202.136	41186	192.168.27.203	22	Failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	

Seleziona metodo

Indicare il metodo che si intende utilizzare per estrarre i campi. [Ulteriori informazioni](#)

[Preferisco scrivere io stesso l'espressione regolare >](#)

Source type
Prova

1332816697.210000	CyEd9z3v2QM9aIBfbd	192.168.202.69	37012	192.168.28.253	22	undetermined	INBOUND SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_4.5	-	-	-
-------------------	--------------------	----------------	-------	----------------	----	--------------	-----------------------------	---------------------	---	---	---

(.*?)

Espressione regolare

Splunk Enterprise estrarrà i campi usando un'espressione regolare.

x|y|z

Delimitatori

Splunk Enterprise estrarrà i campi utilizzando un delimitatore (come ad es. virgole, spazi o caratteri). Usare questo metodo per i dati delimitati, come i valori separati da virgola (file CSV).

E successivamente selezionato ogni campo che mi interessava, dandogli un nome:

Seleziona campi

Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare un valore come obbligatorio, il che significa che deve esistere in un evento per fare in modo che l'evento sia valido. Per evidenziare il testo che fa già parte di un'estrazione esistente, disabilitare prima le estrazioni esistenti. [Ulteriori informazioni](#)

1332816697.210000	CyEd9z3v2QM9aIBfbd	192.168.202.69	37012	192.168.28.253	22	undetermined	INBOUND SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_4.5
-------------------	--------------------	----------------	-------	----------------	----	--------------	-----------------------------	---------------------

Estrai Richiedi

Nome campo: **IPClient**

Valore di esempio: **192.168.202.69**

Add Extraction

Seleziona campi

Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare un valore come obbligatorio, il che significa che deve esistere in un evento per fare in modo che l'evento sia valido. Per evidenziare il testo che fa già parte di un'estrazione esistente, disabilitare prima le estrazioni esistenti. [Ulteriori informazioni](#)

1332816697.210000	CyEd9z3v2QM9aIBfbd	192.168.202.69	37012	192.168.28.253	22	undetermined	INBOUND SSH-2.0-OpenSSH_5.0
-------------------	--------------------	----------------	-------	----------------	----	--------------	-----------------------------

[Mostra espressione regolare >](#)

Estrai Richiedi

Nome campo: **PortaClient**

Valore di esempio: **37012**

Add Extraction

Anteprima

Se di seguito appaiono dei risultati non corretti, fare clic su [Mostra espressione regolare >](#)

Eventi: ☒ IPClient

✓ 1.000 evento (12/11/24 00:00:00,000 - 10/02/25 16:45:37,000)

Seleziona campi

Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare un valore come obbligatorio, il che significa che deve esistere in un evento per essere considerato valido. Per evidenziare il testo che fa già parte di un'estrazione esistente, disabilitare prima le estrazioni esistenti. [Ulteriori informazioni](#)

1332016697.210000 CyEd9z3v2QM9aIBfbd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0 SSH-2.0-OpenSSH_5.0

[Mostra espressione regolare >](#)

Anteprima

Se di seguito appaiono dei risultati non corretti, fare clic su un evento aggiuntivo per aggiungerlo. Evidenziare i valori per migliorare l'estrazione.

Eventi ☒ IPClient ☒ PortaClient

Nome campo: IPDestinazione

Valore di esempio: 192.168.28.253

[Add Extraction](#)

✓ 1.000 evento (12/11/24 00:00:00,000 - 10/02/25 16:45:57,000)

Seleziona campi

Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare un valore come obbligatorio, il che significa che deve esistere in un evento per essere considerato valido. Per evidenziare il testo che fa già parte di un'estrazione esistente, disabilitare prima le estrazioni esistenti. [Ulteriori informazioni](#)

1332016697.210000 CyEd9z3v2QM9aIBfbd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0

[Mostra espressione regolare >](#)

Anteprima

Se di seguito appaiono dei risultati non corretti, fare clic su un evento aggiuntivo per aggiungerlo. Evidenziare i valori per migliorare l'estrazione.

Eventi ☒ IPClient ☒ PortaClient ☒ IPDestinazione

Nome campo: PortaDestinazione

Valore di esempio: 22

[Add Extraction](#)

✓ 1.000 evento (12/11/24 00:00:00,000 - 10/02/25 16:46:20,000)

Seleziona campi

Evidenziare uno o più valori nell'evento di esempio per creare i campi. È possibile indicare un valore come obbligatorio, il che significa che deve esistere in un evento per essere considerato valido. Per evidenziare il testo che fa già parte di un'estrazione esistente, disabilitare prima le estrazioni esistenti. [Ulteriori informazioni](#)

1332016697.210000 CyEd9z3v2QM9aIBfbd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0

[Mostra espressione regolare >](#)

Anteprima

Se di seguito appaiono dei risultati non corretti, fare clic su un evento aggiuntivo per aggiungerlo. Evidenziare i valori per migliorare l'estrazione.

Eventi ☒ IPClient ☒ PortaClient ☒ IPDestinazione ☒ PortaDestinazione

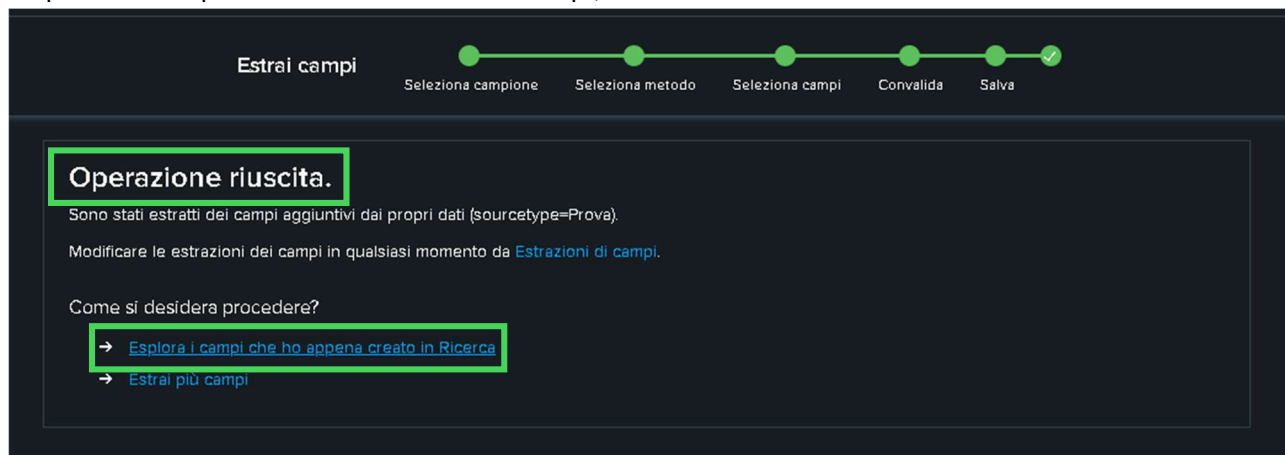
Nome campo: Status

Valore di esempio: undetermined

[Add Extraction](#)

✓ 1.000 evento (12/11/24 00:00:00,000 - 10/02/25 16:46:42,000)

Dopo aver completato l'inserimento dei campi, ho visualizzato la nuova schermata di ricerca:



Nottando che erano presenti altri campi più ordinati e interessanti

The screenshot shows the Splunk search results interface. On the left, there is a sidebar with 'CAMPI SELEZIONATI' (Selected fields) and 'CAMPI INTERESSANTI' (Interesting fields). The 'CAMPI INTERESSANTI' section is highlighted with a green box and lists the following fields: index 1, IPClient 49, IPDestinazione 58, linecount 1, PortaClient 100+, PortaDestinazione 1, punct 19, splunk_server 1, Status 3, and timestamp 1. Below this list is a button '+ Estrai nuovi campi' (Extract new fields). The main search results table shows columns for 'Ora' (Time) and 'Evento' (Event). The table contains several rows of data, including timestamps like '10/02/25 16:43:43,000' and event IDs like '1332016697.210000'. The 'host' field is also visible in the event details.

Andando a selezionare "IPClient" era comparsa una schermata che indicava la percentuale di eventi legata a quel campo.

Nella schermata quindi era presente che l'IP 192.168.202.141 era presente negli eventi il 33% per 4.760 volte e andando a cliccarlo, si aggiungeva nella query di ricerca, riducendo al minimo la ricerca

IPClient

49 Valori, 100% di eventi

Selezionato ☒ Sì ☐ No

Report

Primi valori Primi valori nel tempo Valori rari

Eventi con questo campo

Primi 10 valori	Conteggio	%
192.168.202.141	4.760	33,319%
192.168.202.110	1.972	13,884%
192.168.202.140	1.788	12,516%
192.168.204.45	1.678	11,746%
192.168.202.79	548	3,836%
192.168.202.138	474	3,318%
192.168.202.109	440	3,08%
192.168.202.108	378	2,646%
192.168.202.68	352	2,464%
192.168.203.45	332	2,324%

Ho visualizzato poi l'IP destinazione notando che l'IP 192.168.229.101 era presente al 100% in tutti gli eventi riguardanti il precedente indirizzo IP client

IPDestinazione

1 Valore, 100% di eventi

Selezionato ☒ Sì ☐ No

Report

Primi valori Primi valori nel tempo Valori rari

Eventi con questo campo

Valori	Conteggio	%
192.168.229.101	4.760	100%

Dato che gli eventi erano tutti sulla porta 22, ho supposto che si trattasse di un attacco brute force dalla macchina 192.168.202.141 verso la macchina 192.168.229.101 usando il servizio SSH.