

LABORATORIO 10 FEBBRAIO 2025 S10-L1

ANALISI LOG CON SPLUNK

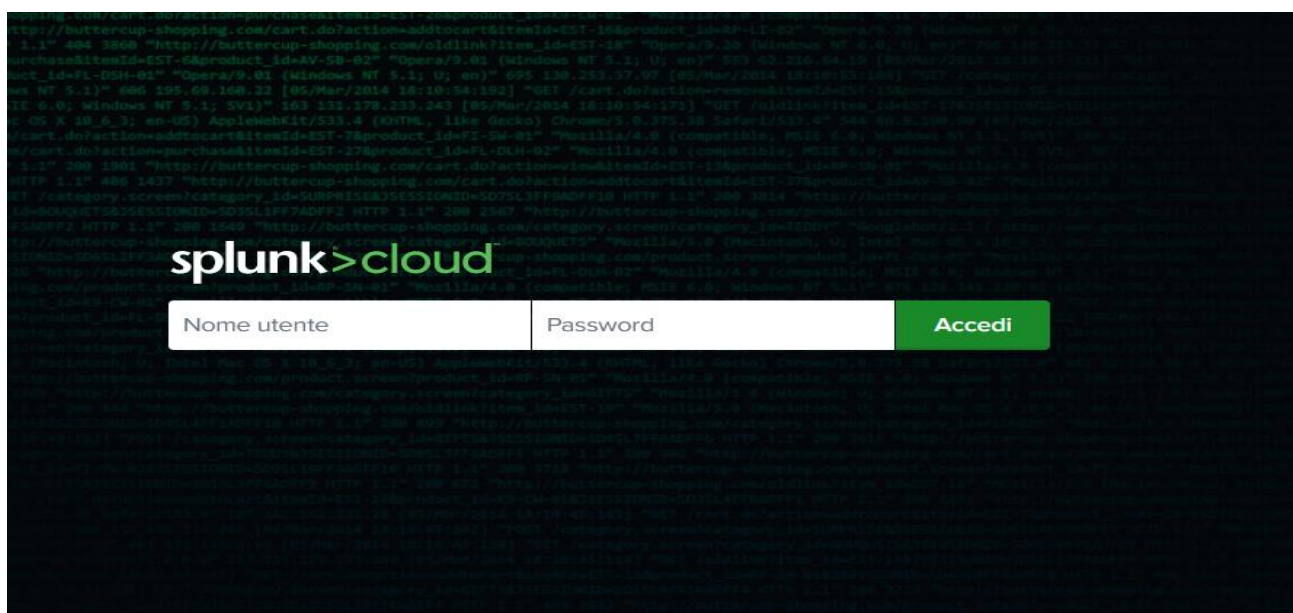
Esercizio di oggi:

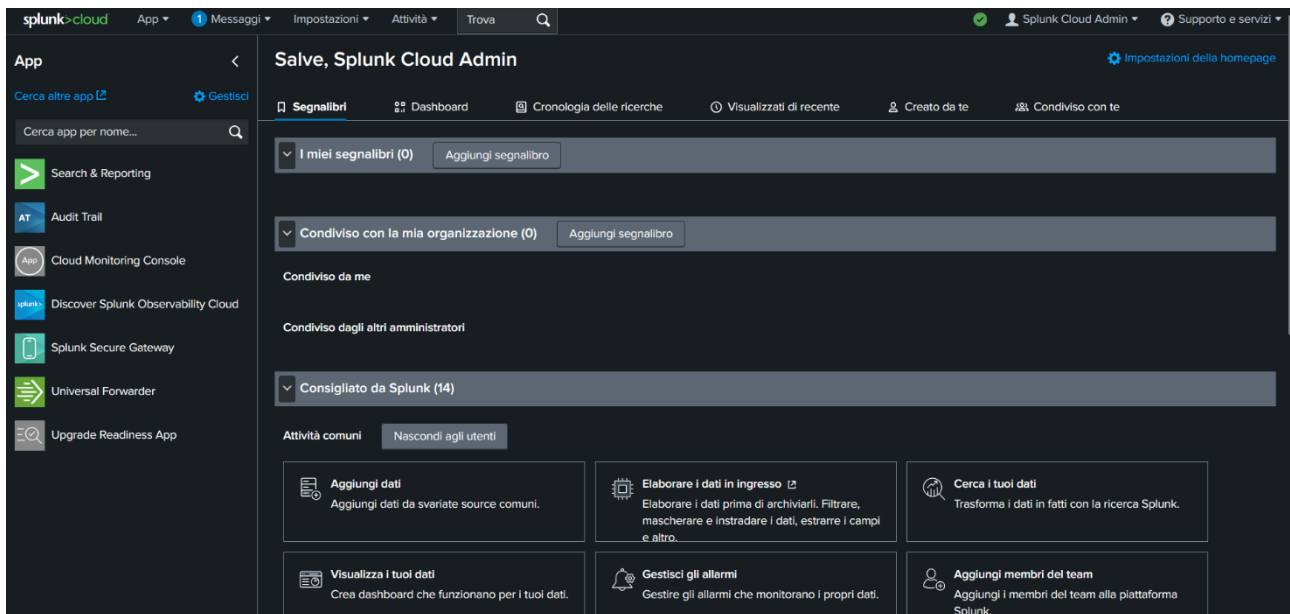
Analizzare il log **ssh.log** fornito e indicare elementi rilevanti, ovvero login falliti, tentativi di attacco ecc.

Trovare tutto ciò che è anomalo.

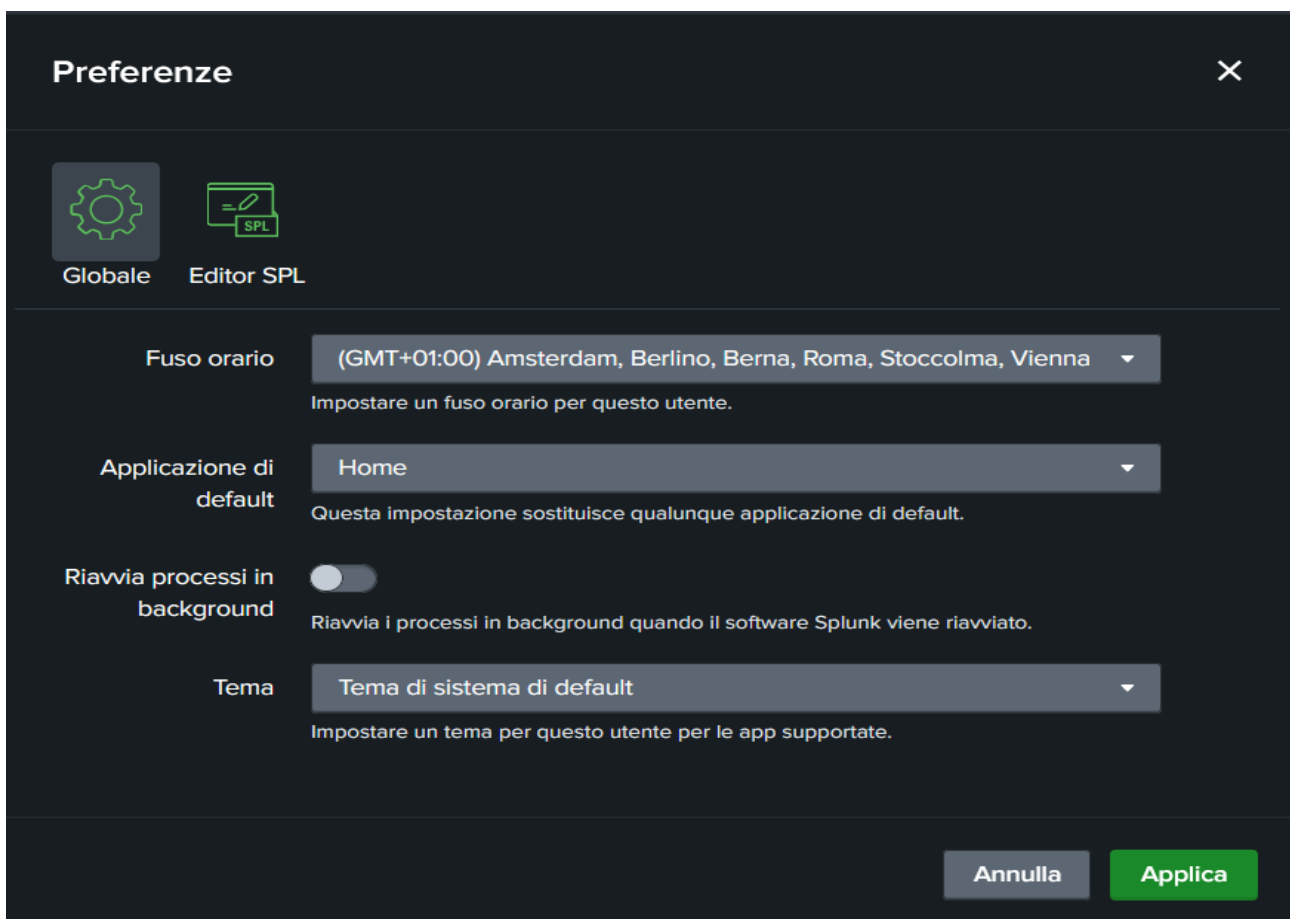
Iniziamo avviando **splunk** ed inseriamo le credenziali ricevute per email al momento della creazione dell'account.

Ci chiederà di cambiare la password.



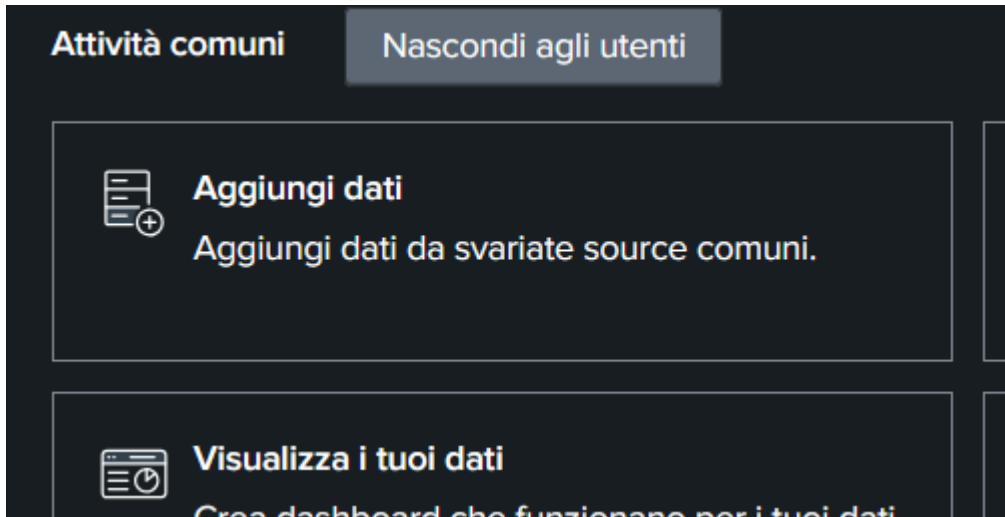


Una volta entrati, procediamo con la modifica delle preferenze configurando il fuso orario corretto.



Applichiamo le modifiche e torniamo alla home page.

A questo punto selezioniamo l'opzione **aggiungi dati** e andiamo a caricare il file **ssh.log** che ci è stato fornito.



Aggiungi dati

Seleziona 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 informazioni](#)

File selezionato: **ssh.log**

Seleziona file

Trascina i file di dati qui

La dimensione di caricamento massima per i file è di 500 MB

✓ File caricato con successo.

Una volta caricato il file ci troviamo davanti questa schermata in cui ci chiede di impostare il **source type**.

splunkcloud

App

Messaggi

Impostazioni

Attività

Trova

Aggiungi dati

Selezione source

Imposta source type

Impostazioni di input

Verifica

Fine

< Indietro

Avanti >

Imposta source type

Questa pagina consente di vedere come la piattaforma Splunk visualizza i dati prima dell'indicizzazione. Se gli eventi appaiono corretti e hanno i timestamp giusti, fare clic su "Avanti" per continuare. In caso contrario, utilizzare le opzioni di seguito per definire le suddivisioni in eventi e i timestamp corretti. Se non si è in grado di trovare un source type appropriato per i dati, crearne uno nuovo facendo clic su "Salva come".

Source: **ssh.log**

Visualizza sintesi degli eventi

Source type: default

Salva come

		Formato	Mostra: 20 per pagina	Visualizza: Elenco	< Prec 1 2 3 4 5 6 7 8 ... Avanti >									
		Ora	Evento											
> Suddivisioni in eventi	1	▲	10/02/25 14:45:03,000	1331981011.840000 SH_5.0 SSH-1.99-Cisco-1.25 timestamp = none	CTHc0o3BARDPDjYue - - - - -	192.168.202.68 - - -	53633	192.168.28.254	22	failure INBOUND SSH-2.0-OpenS				
> Timestamp	2	▲	10/02/25 14:45:03,000	1331981030.210000 SH_5.0 SSH-1.99-Cisco-1.25 timestamp = none	CBHpSz2L3rKbKvwd - - -	192.168.202.68 - - -	35820	192.168.23.254	22	failure INBOUND SSH-2.0-OpenS				
> Avanzate	3	▲	10/02/25 14:45:03,000	1331981032.030000 SH_5.0 SSH-1.99-Cisco-1.25 timestamp = none	C2hfWz25SMWTIAK6hb - - -	192.168.202.68 - - -	36254	192.168.26.254	22	failure INBOUND SSH-2.0-OpenS				
	4	▲	10/02/25 14:45:03,000	1331981034.340000 SH_5.0 SSH-2.0-OpenSSH_5.8p1 Debian-tubuntu3 timestamp = none	CeY76r1JXPbJ758yKb - - -	192.168.202.68 - - -	37764	192.168.27.102	22	failure INBOUND SSH-2.0-OpenS				
	5	▲	10/02/25 14:45:03,000	1331981041.920000 SH_5.0 SSH-2.0-OpenSSH_5.8p1 Debian-tubuntu1 timestamp = none	CPJHML3uGn41V2MGW1 - - -	192.168.202.68 - - -	40244	192.168.27.101	22	failure INBOUND SSH-2.0-OpenS				

Lasciando il source type di default e andando avanti ci chiede di salvarlo con un nuovo nome. Lo chiamiamo **source_type_ssh_log**.

Salva source type

Nome

source_type_ssh_log

Descrizione

Categoria

Personalizzata ▼

App

Search & Reporting ▼

Annulla

Salva

Lasciamo le impostazioni di input predefinite, andiamo avanti e osserviamo il riepilogo nella sezione **verifica**.

Aggiungi dati

Seleziona source

Imposta source type

Impostazioni di input

Verifica

Fine

< Indietro

Invia >

Verifica

Tipo di input File caricato
Nome file ssh.log
Source type source_type_ssh_log
Host si-i-0c03c0c1aa88c6552,prd-p-ssa1g.splunkcloud.com
Indice Default

A questo punto possiamo iniziare la ricerca.

Aggiungi dati

Seleziona 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. 🔗](#)

splunkcloud App Messaggi Impostazioni Attività Trova

Ricerca Analytics Set di dati Report Allarmi Dashboard

Nuova ricerca Salva come Crea vista tabella Chiudi

source="ssh_log" host="si-1-0c03c0c1aa88c6552.prd-p-ssa1g.splunkcloud.com" sourcetype="source_type_ssh_log" Sempre

✓ 14.286 eventi (prima di 10/02/25 15:51:25,000) Nessun campionamento degli eventi Processo

Eventi (14.286) Pattern Statistiche Visualizzazione

Formato timeline Zoom indietro + Zoom area selezionata X Deselezione 1 minuto per colonna

Formato Mostra: 20 per pagina Visualizza: Elenco

	Ora	Evento
>	10/02/25 15:51:16,000	1332016697.210000 CyEd9z3v2Qh9a1Bfbd 192.168.202.69 37012 192.168.28.253 22 undetermined INBOUND SSH-2.0-OpenSSH_5.0 SSH-2.0-OpenSSH_4.5 - - - - - host = si-1-0c03c0c1aa88c6552.prd-p-ssa1g.splunkcloud.com source = ssh_log sourcetype = source_type_ssh_log
>	10/02/25 15:51:16,000	1332017793.040000 CrUTZx1hYk1qFFT11 192.168.202.136 56815 192.168.21.203 22 failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7 SS H-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - host = si-1-0c03c0c1aa88c6552.prd-p-ssa1g.splunkcloud.com source = ssh_log sourcetype = source_type_ssh_log
>	10/02/25 15:51:16,000	1332017778.370000 CZHG1136uzbVNG8uY1 192.168.202.136 56814 192.168.21.203 22 failure INBOUND SSH-2.0-OpenSSH_5.3p1 Debian-3ubuntu7 SS H-2.0-OpenSSH_5.8p1 Debian-1ubuntu3 - - - - - host = si-1-0c03c0c1aa88c6552.prd-p-ssa1g.splunkcloud.com source = ssh_log sourcetype = source_type_ssh_log
>	10/02/25 15:51:16,000	1332017154.520000 C0XOE9WejSK5IETpJ 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-1ubuntu3 - - - - - host = si-1-0c03c0c1aa88c6552.prd-p-ssa1g.splunkcloud.com source = ssh_log sourcetype = source_type_ssh_log

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

Sono stati trovati 14286 eventi.

Selezioniamo **Estrai nuovi campi** nel menù in basso a sinistra e proseguiamo con l'analisi degli eventi. Applichiamo il filtro **failure** per ricevere in output tutti i tentativi di accesso non andati a buon fine.

Eventi

✓ 2.000 eventi (prima di 10/02/25 15:53:38,000)

failure Applica Esempio: 10.000 eventi

Ci restituisce **1960** eventi inerenti a login falliti effettuati da diversi indirizzi IP.

✓ 1.960 eventi (prima di 10/02/25 17:49:39,000)

20 per pagina

< Prec

1

2

3

4

5

6

7

8

...

Avanti >

failure

Applica

Esempio: 10.000 eventi

Tutti gli eventi

_raw											
1332017793.040000	CrUTz1hjVklqFFTL1	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	CZHGI136uZbVNGbuY1	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
1332017111.420000	CB4eVG4sDCR1pFqRa	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
1332017087.510000	COkT4dasAFZ4nxP9i	192.168.202.136	41184	192.168.27.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3
1332017090.970000	CW0yQE1tr8Gkj159	192.168.202.136	44979	192.168.23.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3
1332017054.540000	C6JLw32NSXO2e4PF1	192.168.202.136	44977	192.168.23.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3
1332016795.530000	CyVZs24LS0hOop4Fb	192.168.202.136	41175	192.168.27.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3
1332016778.080000	CC9PGvy2Vv9nDQ8	192.168.202.136	51551	192.168.26.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3
1332016737.580000	CEa3kw3syn1nW1GhG3	192.168.202.136	51549	192.168.26.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3
1332016700.300000	Cx0BoskLu4U30ztR7	192.168.202.136	41171	192.168.27.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.3p1	Debian-3ubuntu7	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3
1332016097.140000	CTDov73pPdLFLznHk	192.168.202.69	36782	192.168.26.203	22	failure	INBOUND	SSH-2.0-OpenSSH_5.0	SSH-2.0-OpenSSH_5.8p1	Debian-1ubuntu3	

A questo punto per perfezionare ancora di più la ricerca andiamo ad inserire una query specifica per ricevere in output i tentativi falliti verso uno specifico IP del server di destinazione. Dopo aver effettuato un controllo ci accorgiamo che ci sono **4804** tentativi falliti (failure) sul server 192.168.221.101 su porta 22 SSH.

source="ssh.log" host="si-1-i-0c03c0c1aa88c6552.prd-p-sa1g.splunkcloud.com" sourcetype="source_type_ssh_log" failure 192.168.229.101

✓ 4.804 eventi (prima di 10/02/25 18:11:13,000)

Nessun campionamento degli eventi

Processo

Gruppo basato sui criteri

Modalità intelligente

Eventi (4.804)

Formato timeline

Zoom indietro

1 minuto per colonna

Formato Mostra: 20 per pagina Visualizza: Elenco												
< Nascondi campi Tutti i campi												
	i	Ora	Evento									
CAMPI SELEZIONATI	>	10/02/25 15:51:16,000	1332013747.040000	Ckrzg6HPuq1Hpa88	192.168.202.141	8121	192.168.229.101	22	failure	INBOUND	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu
				host = si-1-i-0c03c0c1aa88c6552.prd-p-sa1g.splunkcloud.com	source = ssh.log	sourcetype = source_type_ssh_log						
CAMPI INTERESSANTI	>	10/02/25 15:51:16,000	1332013747.030000	C1MLdW1R1uZmPkaJ3	192.168.202.141	8120	192.168.229.101	22	failure	INBOUND	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu
				host = si-1-i-0c03c0c1aa88c6552.prd-p-sa1g.splunkcloud.com	source = ssh.log	sourcetype = source_type_ssh_log						
	>	10/02/25 15:51:16,000	1332013747.010000	C42KYP3uz5YV1g7J14	192.168.202.141	8119	192.168.229.101	22	failure	INBOUND	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu
				host = si-1-i-0c03c0c1aa88c6552.prd-p-sa1g.splunkcloud.com	source = ssh.log	sourcetype = source_type_ssh_log						
	>	10/02/25 15:51:16,000	1332013747.000000	CKEwn83QmYcY13xV1	192.168.202.141	8118	192.168.229.101	22	failure	INBOUND	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu
				host = si-1-i-0c03c0c1aa88c6552.prd-p-sa1g.splunkcloud.com	source = ssh.log	sourcetype = source_type_ssh_log						
	>	10/02/25 15:51:16,000	1332013746.980000	CY97nF3Ej34wI1V2Vb	192.168.202.141	8117	192.168.229.101	22	failure	INBOUND	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu
				host = si-1-i-0c03c0c1aa88c6552.prd-p-sa1g.splunkcloud.com	source = ssh.log	sourcetype = source_type_ssh_log						
	>	10/02/25 15:51:16,000	1332013746.970000	CwFF13N1t989xwN1	192.168.202.141	8116	192.168.229.101	22	failure	INBOUND	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu

_raw											
1332013747.040000	CXrzg6HPuhq1HpA88	192.168.202.141	8121	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013747.030000	C1MLdW1R1uZmPkmJJ3	192.168.202.141	8120	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013747.010000	C4ZKYP3uz5YV1g7J14	192.168.202.141	8119	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013747.000000	CKEm03QmMycY13xV1	192.168.202.141	8118	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.980000	CY97nF3Ej34wI1V2Vb	192.168.202.141	8117	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.970000	CWFF1t3NLts09ozMNj	192.168.202.141	8116	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.950000	C1Et7e273mR8F0UNCc	192.168.202.141	8115	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.940000	ChvKjd105aiQnXQ07	192.168.202.141	8114	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.930000	C3GryL1cafrQADF5Z2	192.168.202.141	8113	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.910000	CPpHoJKZbt1yw7K6	192.168.202.141	8112	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.900000	CuqQY94DM11HE5o755	192.168.202.141	8111	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.890000	C0k0VK2j01UR10X1Fh	192.168.202.141	8110	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.880000	Cur0IAZGQjgN1VVPF	192.168.202.141	8109	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.860000	COYXIC2Q6C9Z1H9d1	192.168.202.141	8108	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.850000	CDJ5Bd1r7nkwYubzre	192.168.202.141	8107	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.810000	CnWd01ix1f2j1jY19	192.168.202.141	8106	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.800000	CLKkFF1HINKt6Xmd2	192.168.202.141	8105	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.790000	Cd6Q1RvTn5eeEntH6a	192.168.202.141	8104	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.760000	C31ny13K8dGfjtx4Q1	192.168.202.141	8103	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
1332013746.740000	C31yxG3u3vGctVv0c	192.168.202.141	8102	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-

Dopo aver selezionato un campione a caso tra tutti questi trovati procediamo con la selezione del metodo.

1332013747.040000	CXrzg6HPuhq1HpA88	192.168.202.141	8121	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
-------------------	-------------------	-----------------	------	-----------------	----	---------	---------	---	-----------------------	-----------------	---

Passiamo alla creazione di campi specifici riguardo alla query.

Selezioneremo IP 192.168.202.141 come **client**; IP 192.168.229.101 22 come **server** e **porta_server** e failure come **esito**.

1332013747.040000	CXrzg6HPuhq1HpA88	192.168.202.141	8121	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1	-
Mostra espressione regolare >											
Anteprima											
Se di seguito appaiono dei risultati non corretti, fare clic su un evento aggiuntivo per aggiungerlo al set degli eventi di esempio. Evidenziarne i valori per migliorare l'estrazione											
Eventi client server porta_server esito											
✓ 2.000 eventi (prima di 10/02/25 18:28:48,000)											
<div> <div>filtra</div> <div>Applica</div> <div>Esempio: 10.000 eventi</div> <div>Tutti gli eventi</div> <div>Tutti gli eventi</div> <div>Corrispondenze</div> <div>Senza corrispondenze</div> </div>											
_raw											
✓	1332013747.040000	CXrzg6HPuhq1HpA88	192.168.202.141	8121	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1
✓	1332013747.030000	C1MLdW1R1uZmPkmJJ3	192.168.202.141	8120	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1
✓	1332013747.010000	C4ZKYP3uz5YV1g7J14	192.168.202.141	8119	192.168.229.101	22	failure	INBOUND	-	SSH-2.0-OpenSSH_5.8p1	Debian-7ubuntu1

Convalidiamo le estrazioni dei campi, avanziamo e salviamo l'estrazione.

The screenshot shows the 'Salva' (Save) step in a Splunk extraction configuration wizard. The progress bar at the top indicates the current step is 'Salva', with previous steps being 'Seleziona campione', 'Seleziona metodo', 'Seleziona campi', and 'Convalida'. The 'Indietro' (Back) button is visible, and the 'Fine' (Finish) button is highlighted in green.

Salva
Assegnare un nome all'estrazione e impostare le autorizzazioni.

Nome estrazioni: **EXTRACT-** client,server,porta_server,esito

Proprietario: sc_admin

App: search

Autorizzazioni: ☒ Proprietario ☐ App ☐ Tutte le app

Source type: source_type_ssh_log

Evento di esempio:

1332013747.040000	CXrzg6HPuhqiHpA88	192.168.202.141	8121	192.168.229.101
22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	- - -

Campi: client,server,porta_server,esito

Espressione regolare: `^(?:[^\t\n]"*)\t(2)(?P<client>[^\t]+)\td+\t(?P<server>[^\t]+)\t(?P<porta_server>\d+)\t(?P<esito>\w+)`

A questo punto abbiamo terminato l'analisi con splunk. Possiamo constatare si sia trattato di un attacco **bruteforce** non andato a buon fine.