LABORATORIO 10 FEBBRAIO 2025 S10-L1

ANALISI LOG CON SPLUNK

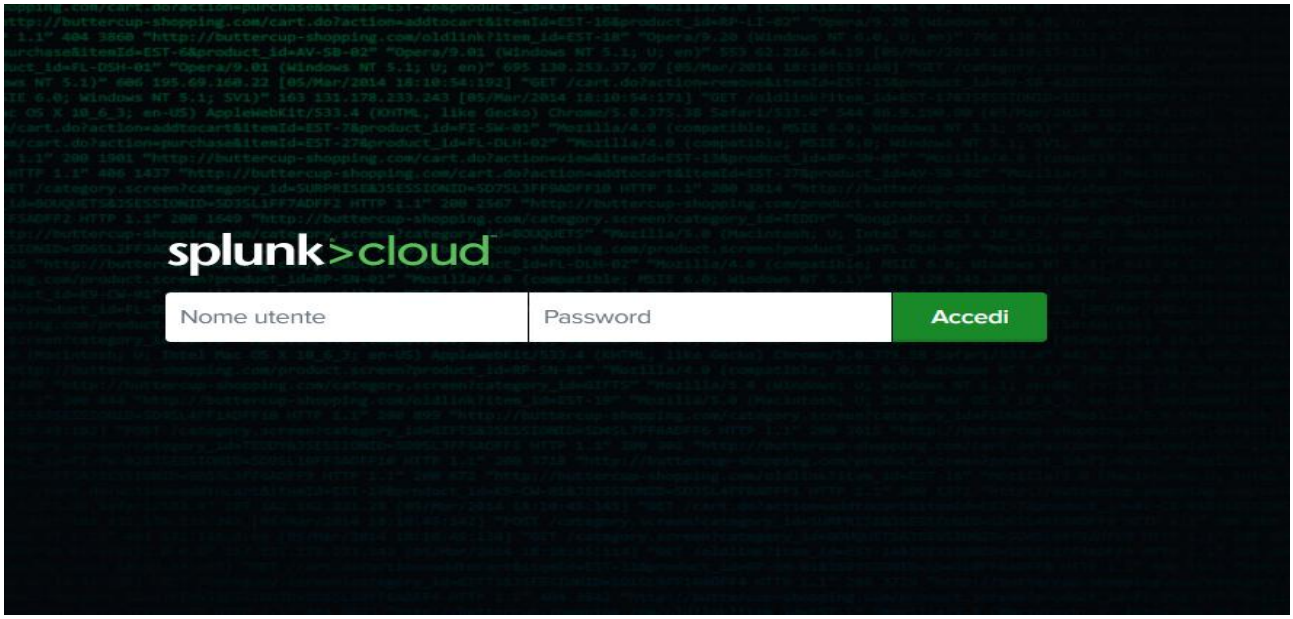
Esercizio di oggi:

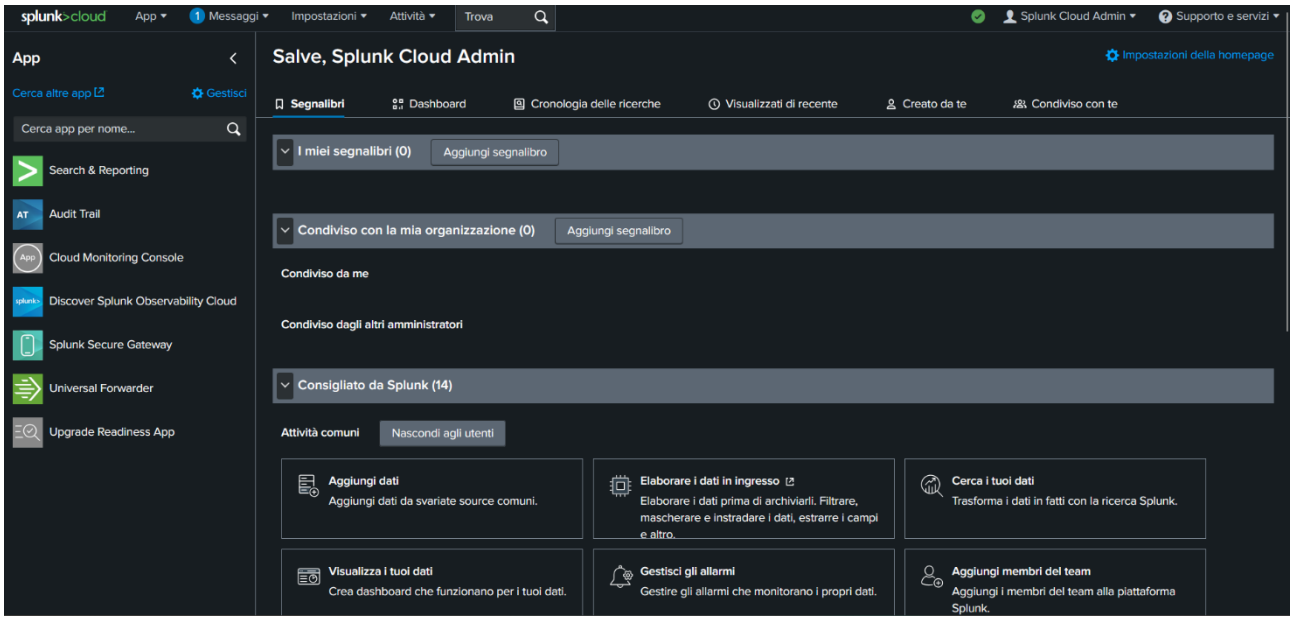
Analizzare il log **ssh.log** fornito e indicare elementi rilevanti, ovvero login falliti, tentativi di attacco ecc.

Trovare tutto ciò che è anomalo.

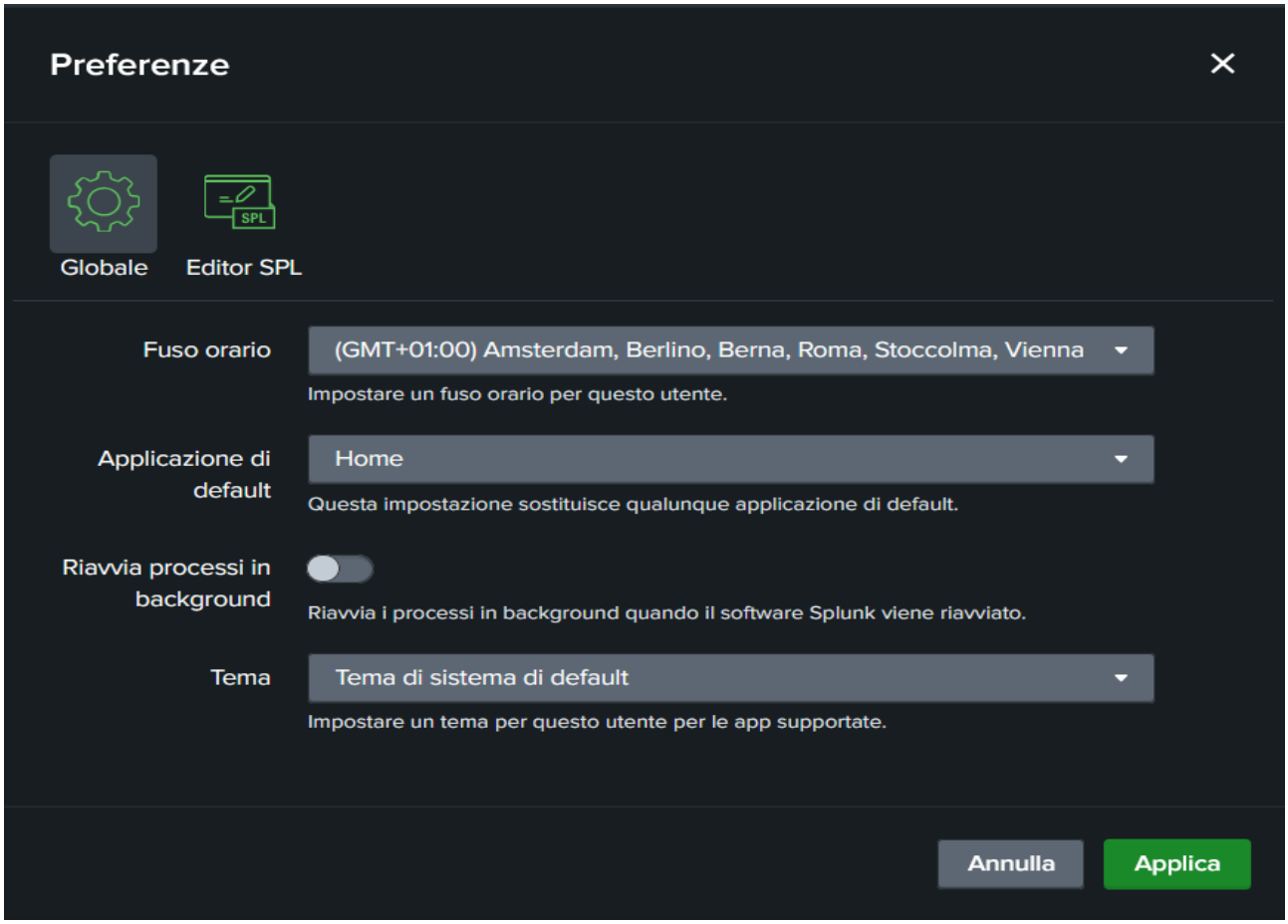
Iniziamo avviando **splunk** ed inseriamo le credenziali ricevute per email al momento della creazione dell'account.

Ci chiederà di cambiare la password.



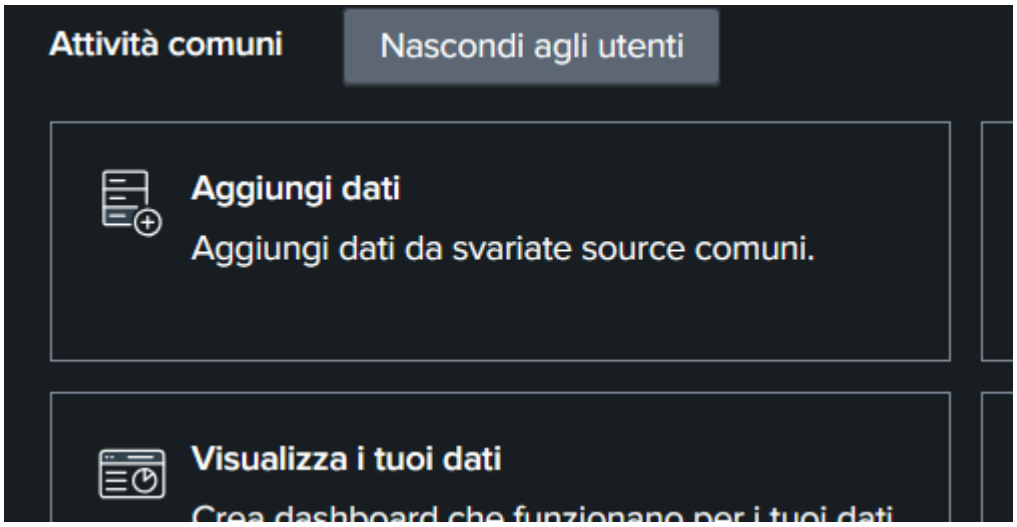


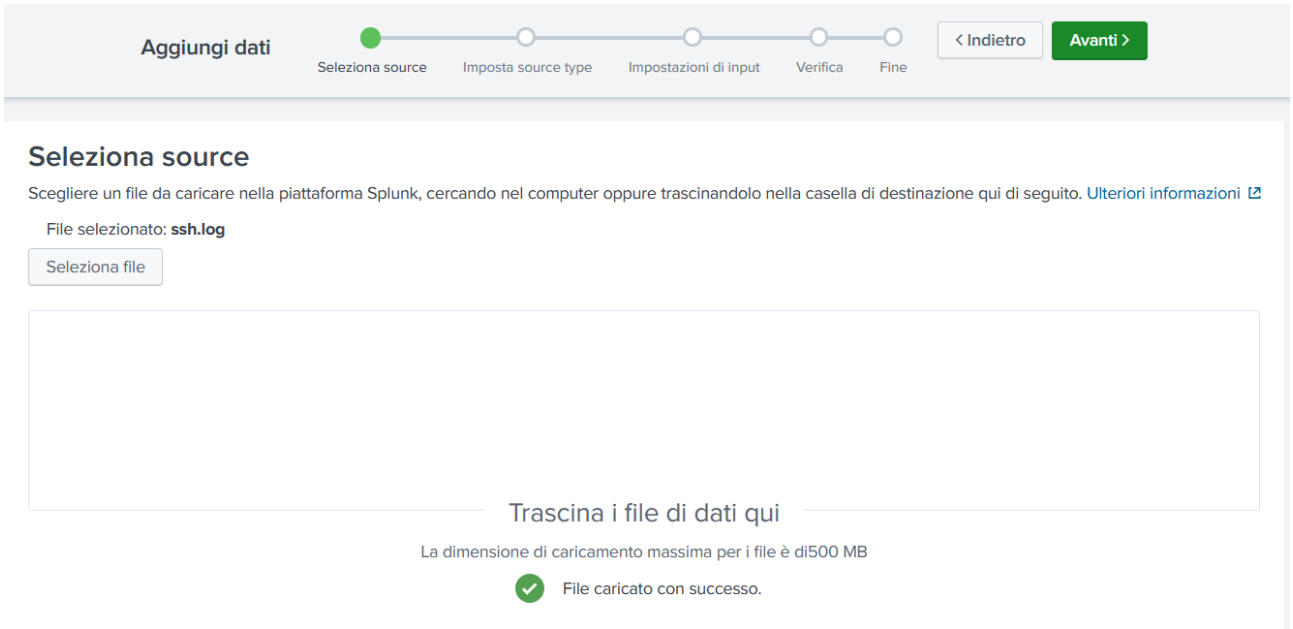
Una volta entrati, procediamo con la modifica delle preferenze configurando il fuso orario corretto.



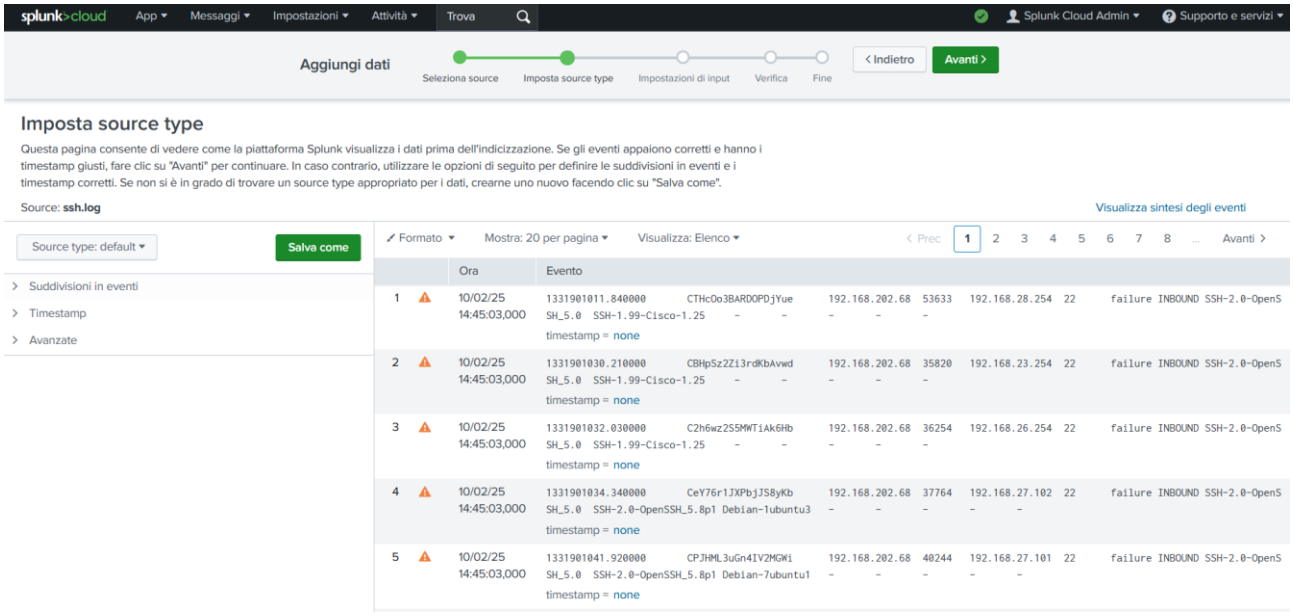
Applichiamo le modifiche e torniamo alla home page.

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

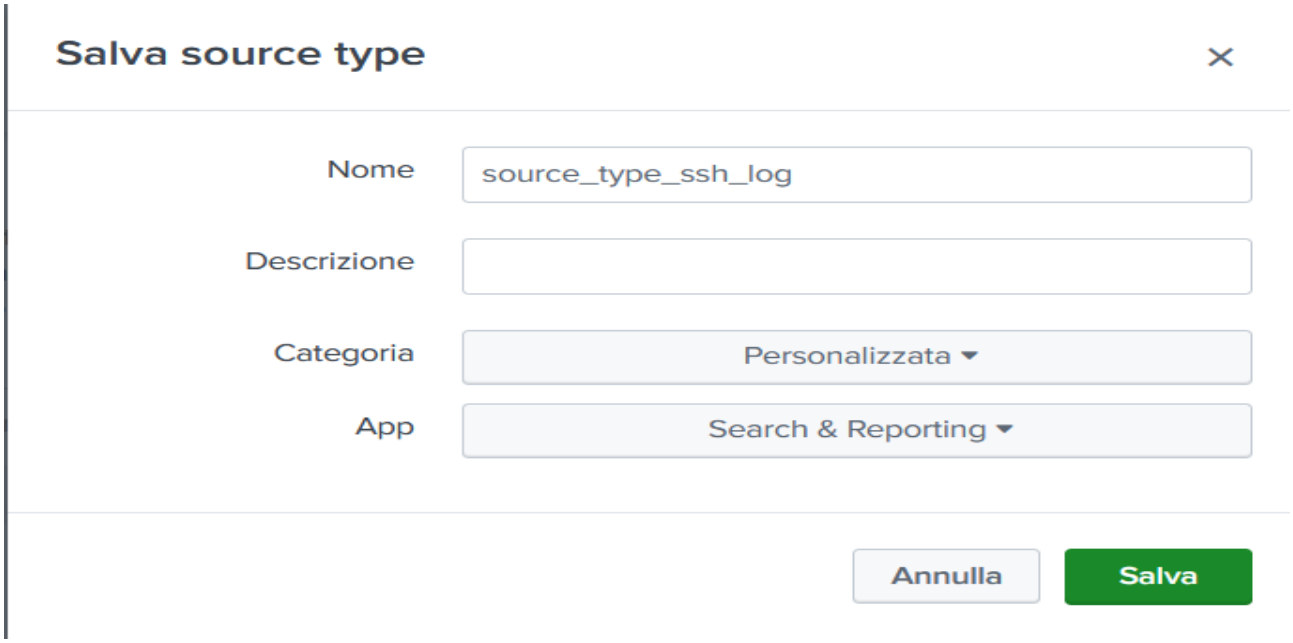




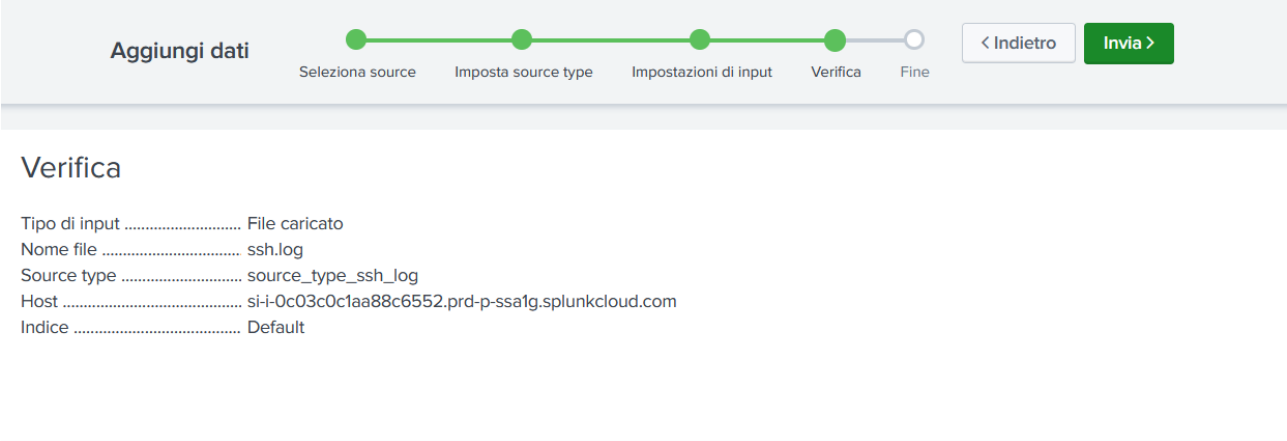
Una volta caricato il file ci troviamo davanti questa schermata in cui ci chiede di impostare il **source type.**



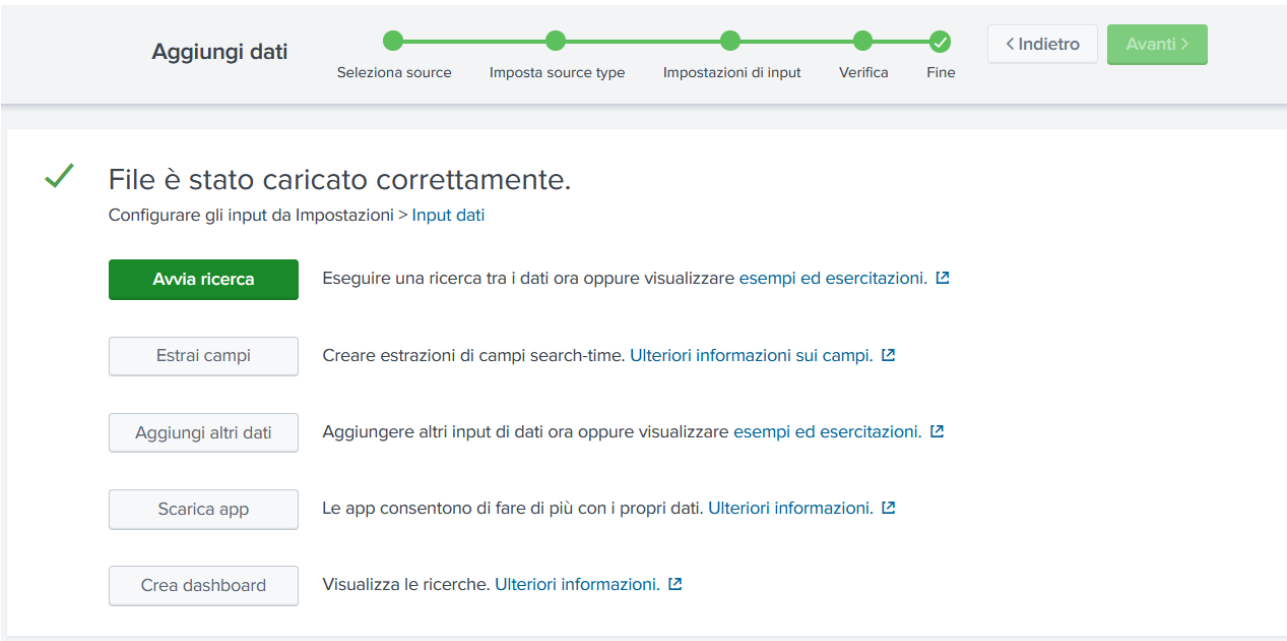
Lasciando il source type di default e andando avanti ci chiede di salvarlo con un nuovo nome. Lo chiamiamo **source_type_ssh_log.**

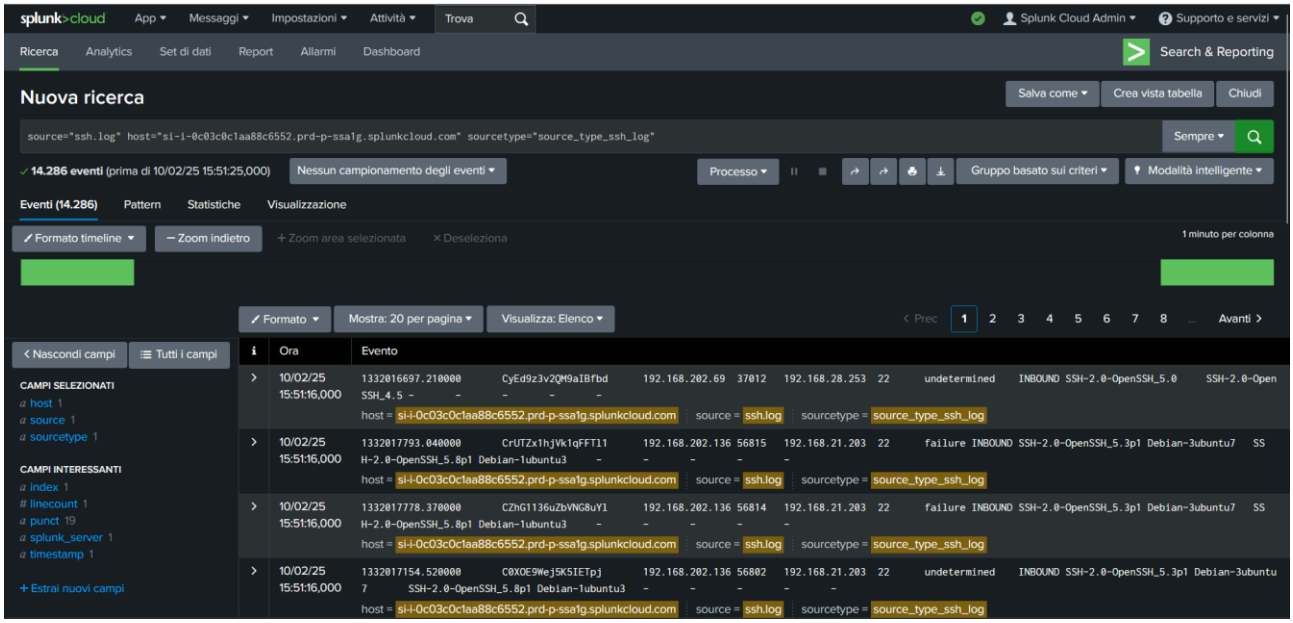


Lasciamo le impostazioni di input predefinite, andiamo avanti e osserviamo il riepilogo nella sezione **verifica.**



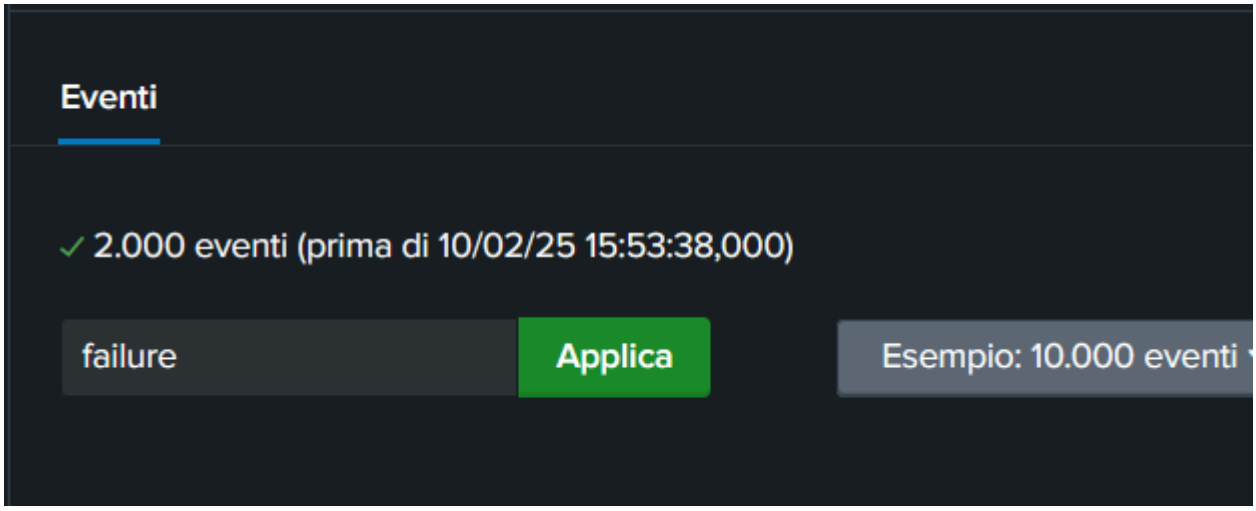
A questo punto possiamo iniziare la ricerca.



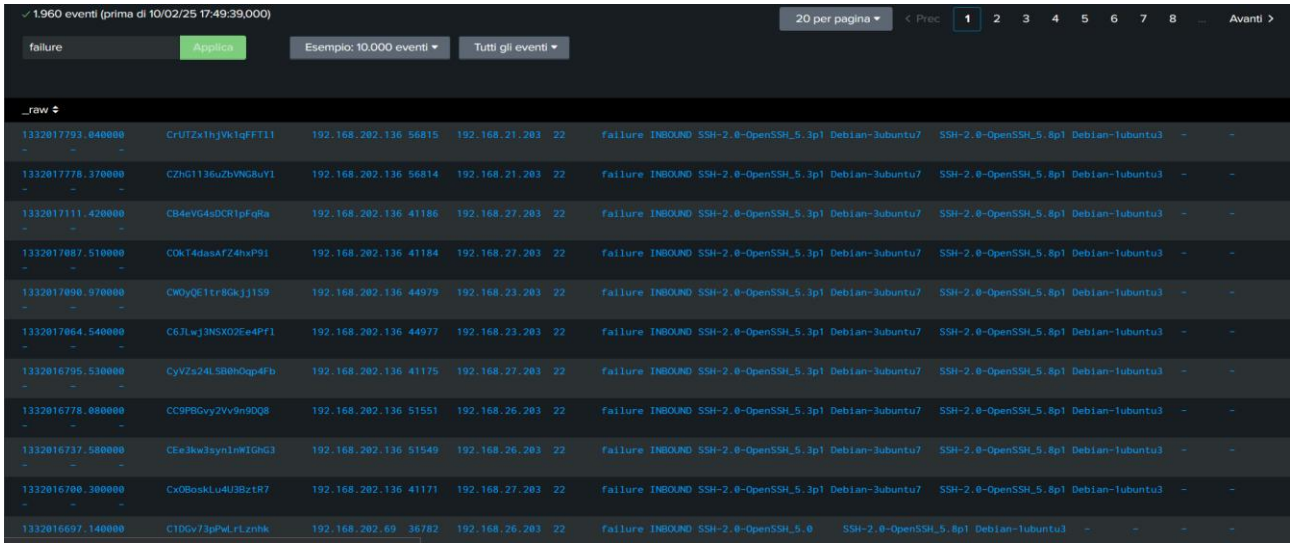


Sono stati trovati 14286 eventi.

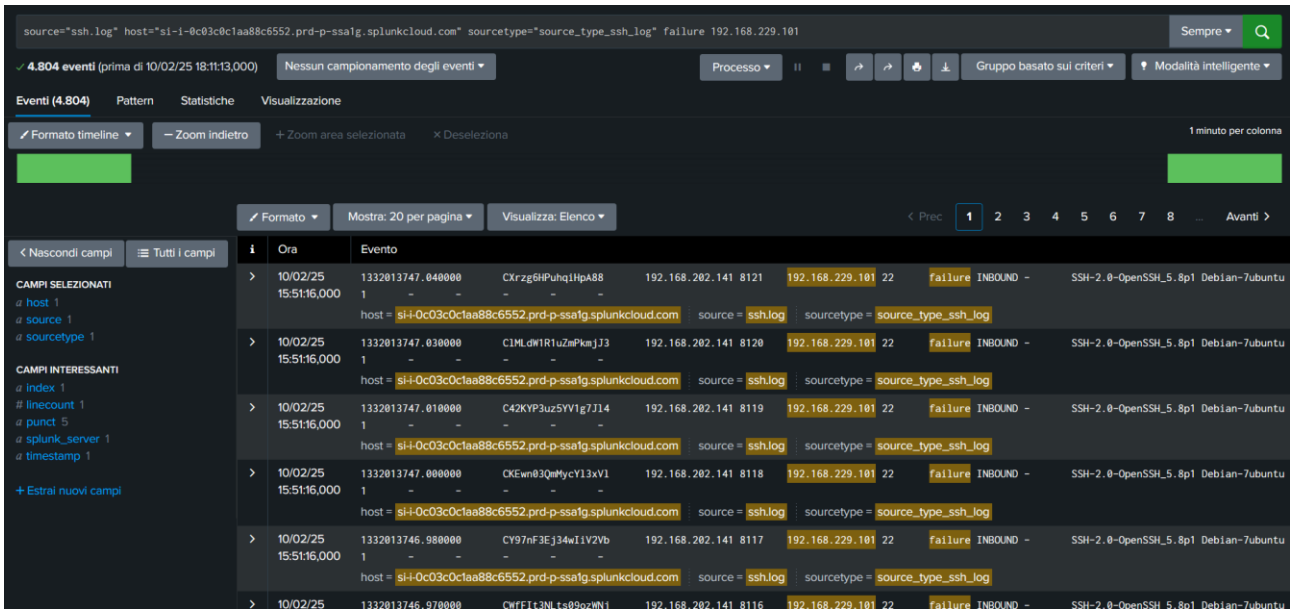
Selezioniamo **Estrai nuovi campi** nel menù in basso a sinistra e proseguiamo con l'analisi degli eventi. Applichiamo il filtro **failure** per ricevere in output tutti i tentativi di accesso non andati a buon fine.

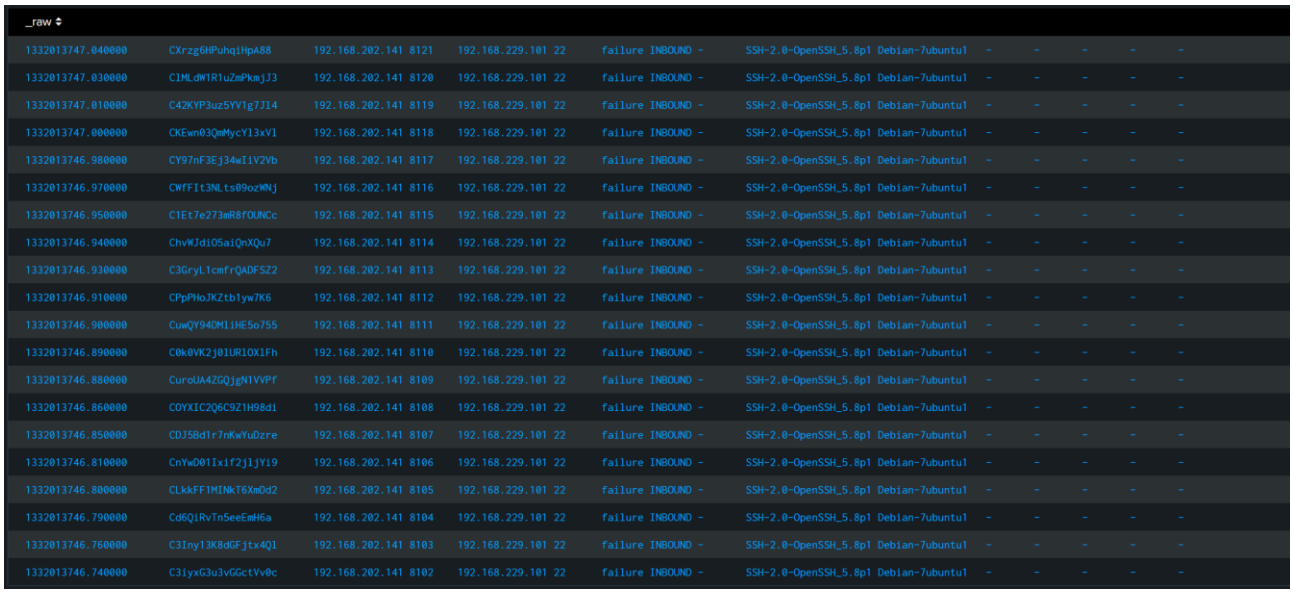


Ci restituisce **1960** eventi inerenti a login falliti effettuati da diversi indirizzi IP.



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.





_raw													
1332013747.040000	CXrzg6HPuhqiHpA88	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	C42KYP3uz5YV1g7Jl4	192.168.202.141 8119	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013747.000000	CKEwn03QmMycYl3xVl	192.168.202.141 8118	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.980000	CY97nF3Ej34wIiV2Vb	192.168.202.141 8117	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.970000	CWfFIt3NLts09ozWNj	192.168.202.141 8116	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.950000	C1Et7e273mR8fOUNCc	192.168.202.141 8115	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.940000	ChvWJdiO5aiQnXQu7	192.168.202.141 8114	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.930000	C3GryL1cmfrQADFSZ2	192.168.202.141 8113	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.910000	CPpPHoJKZtb1yw7K6	192.168.202.141 8112	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.900000	CuwQY94DM1iHE5o755	192.168.202.141 8111	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.890000	C0k0VK2j01UR1OX1Fh	192.168.202.141 8110	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.880000	CuroUA4ZGQjgN1VVPf	192.168.202.141 8109	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.860000	COYXIC2Q6C9Z1H98d1	192.168.202.141 8108	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.850000	CDJ5Bd1r7nKwYuDzre	192.168.202.141 8107	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.810000	CnYwD01Ix1f2jljY19	192.168.202.141 8106	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.800000	CLkkFF1MINkT6XmDd2	192.168.202.141 8105	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.790000	Cd6QiRvTn5eeEmH6a	192.168.202.141 8104	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.760000	C3Iny13K8dGFjtx4Ql	192.168.202.141 8103	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		
1332013746.740000	C3iyxG3u3vGGctVv0c	192.168.202.141 8102	192.168.229.101 22	failure	INBOUND -	SSH-2.0-OpenSSH_5.8p1 Debian-7ubuntu1	-	-	-	-	-		

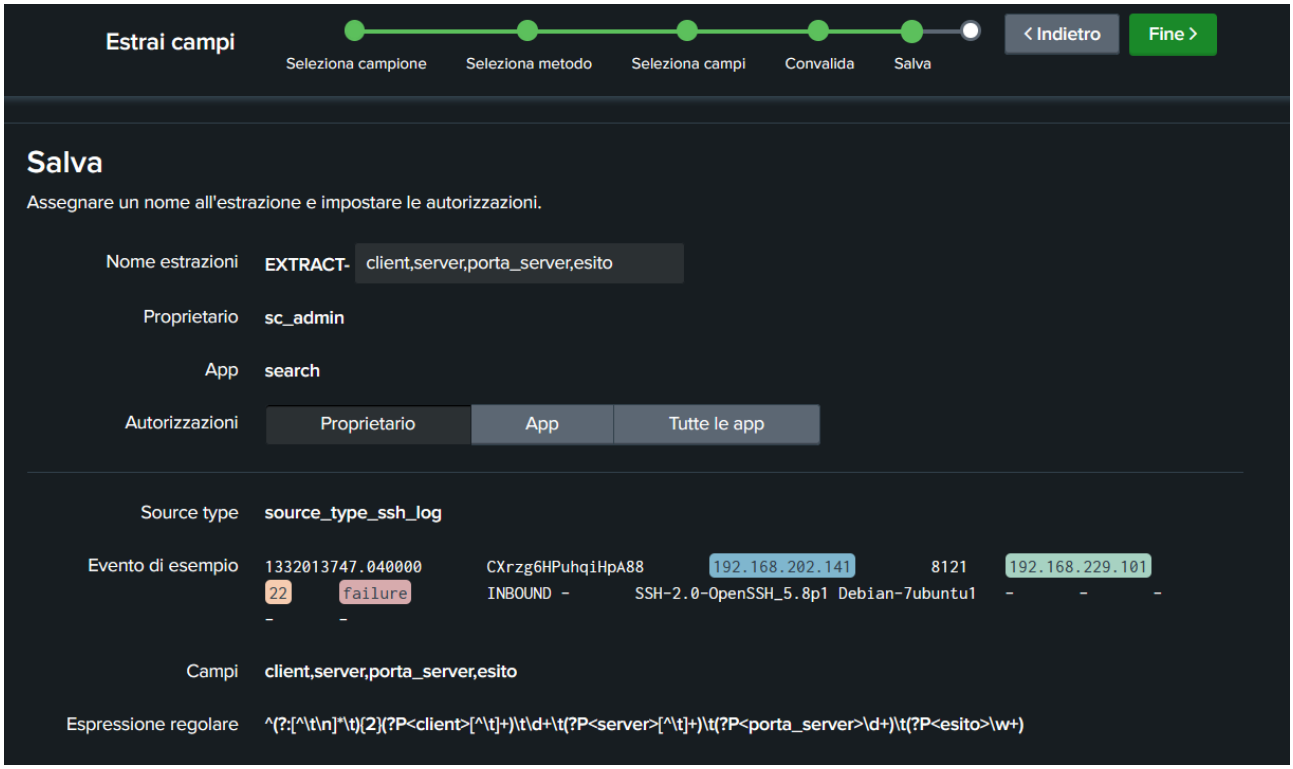
Dopo aver selezionato un campione a caso tra tutti questi trovati procediamo con la selezione del metodo.

1332013747.040000	CXrzg6HPuhqiHpA88	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 rigurado 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.**

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



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