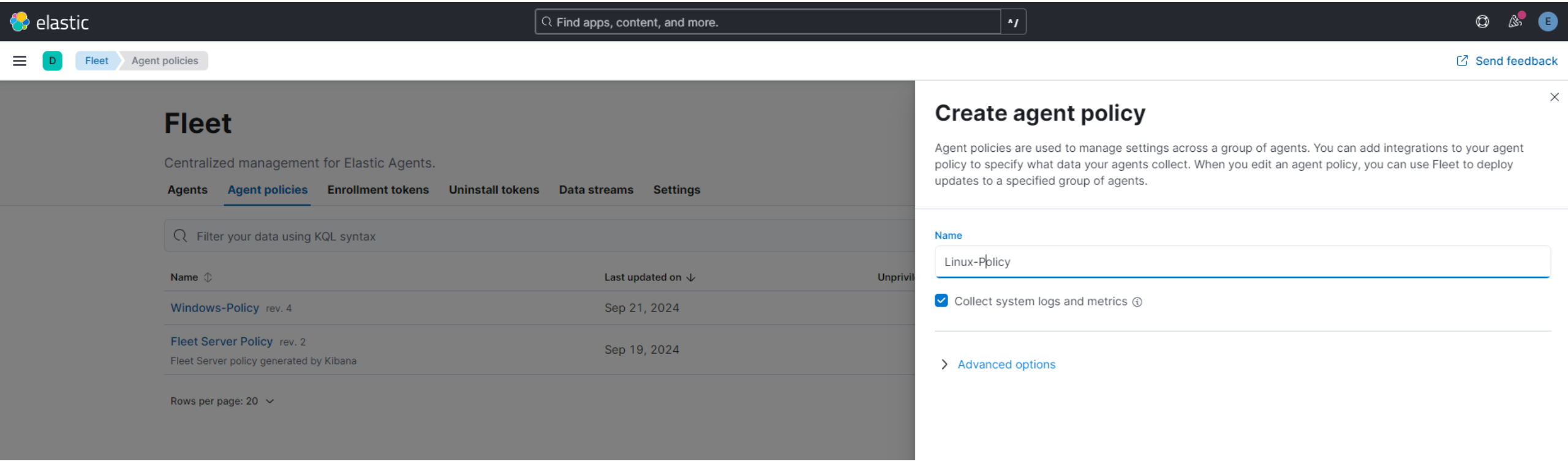
Day 13 - Elastic Agent on Ubuntu

Obiettivo

- **Installare Elastic Agent sull'Ubuntu Server e riscontrare i logs su Elasticsearch**

Elastic Agent on Ubuntu

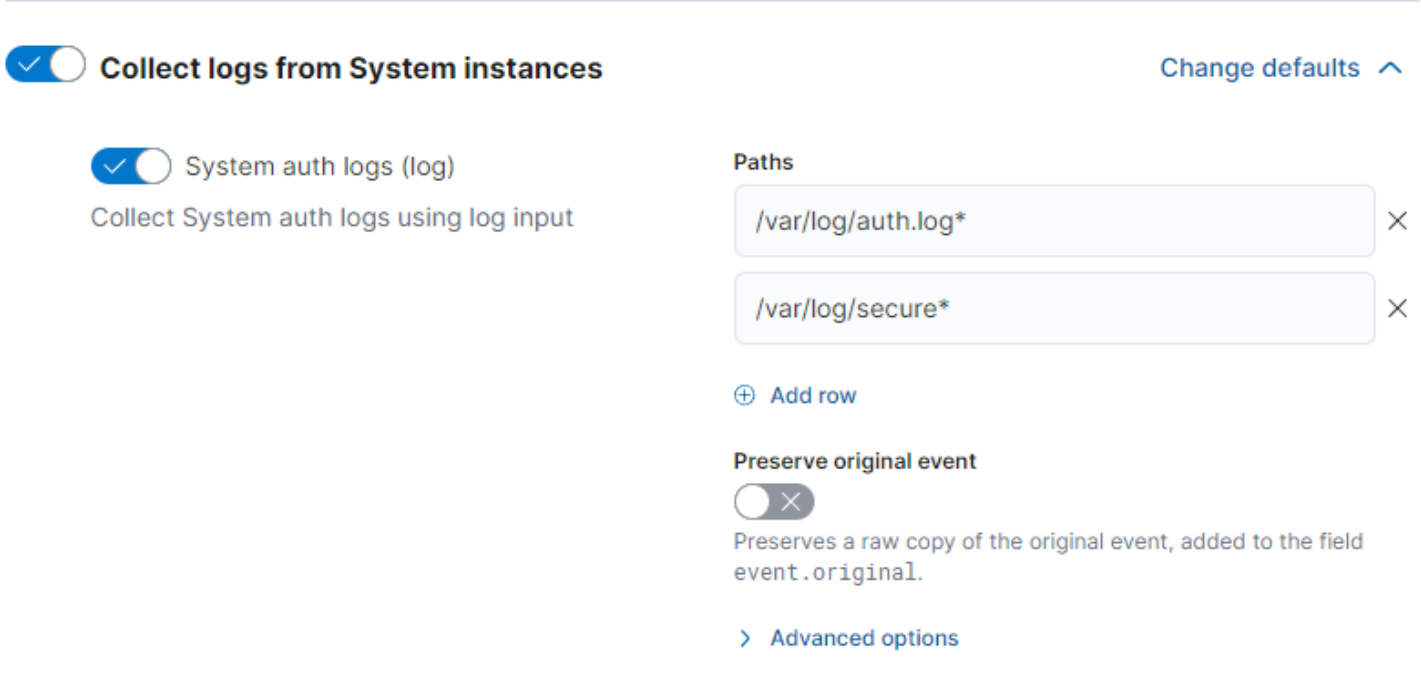
Creiamo una nuova policy nella sezione ‘Fleet’ di **Elasticsearch**



Elastic Agent on Ubuntu

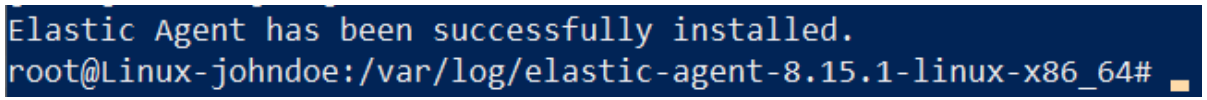
```
root@Linux-johndoe:/var/log# ls
alternatives.log  bootstrap.log          dist-upgrade  image_build_date  landscape  syslog              watchdog
apport.log        btmp                   dmesg         installer         lastlog    sysstat             wtmp
apt               cloud-init.log         dpkg.log      journal           private    ufw.log
auth.log          cloud-init-output.log  faillog       kern.log          README     unattended-upgrades
root@Linux-johndoe:/var/log#
```

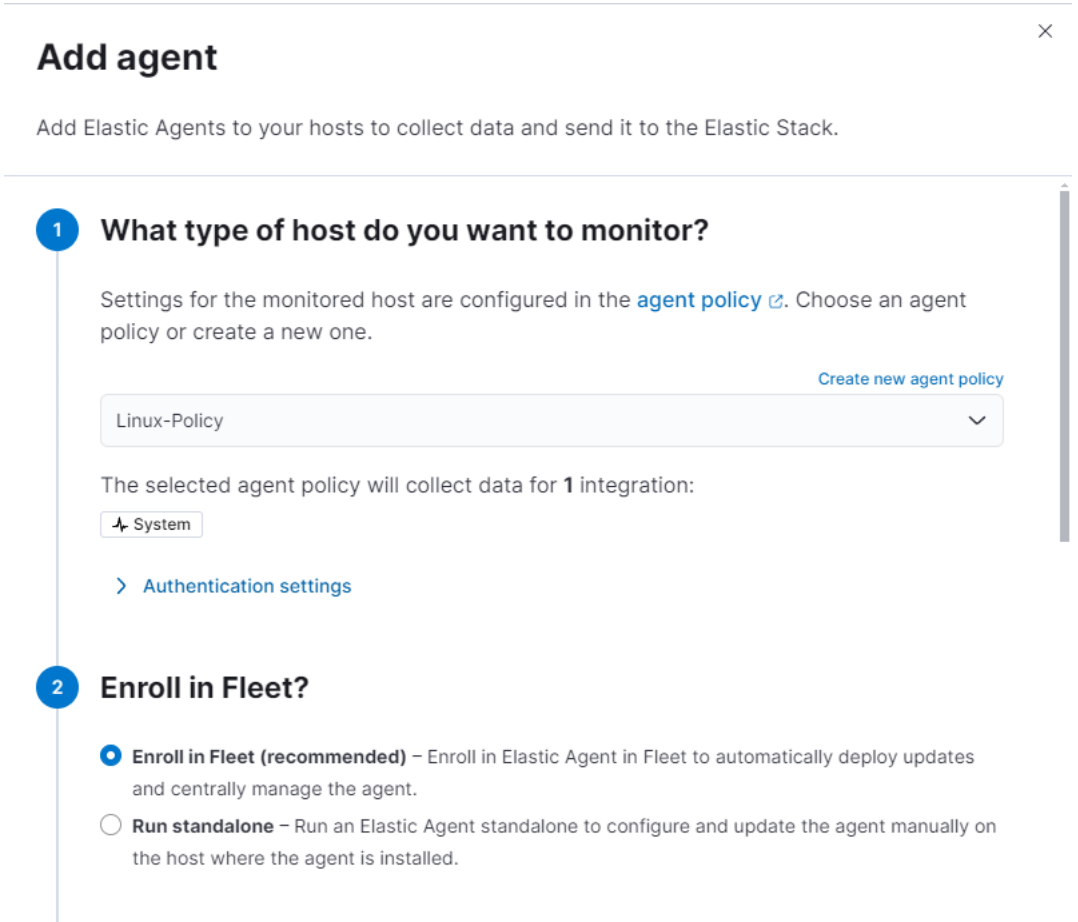
Entriamo nella policy, clicchiamo su System-3 per visualizzare quali log sono configurati per essere inviati dal server **Ubuntu** a **Elasticsearch.**



Elastic Agent on Ubuntu

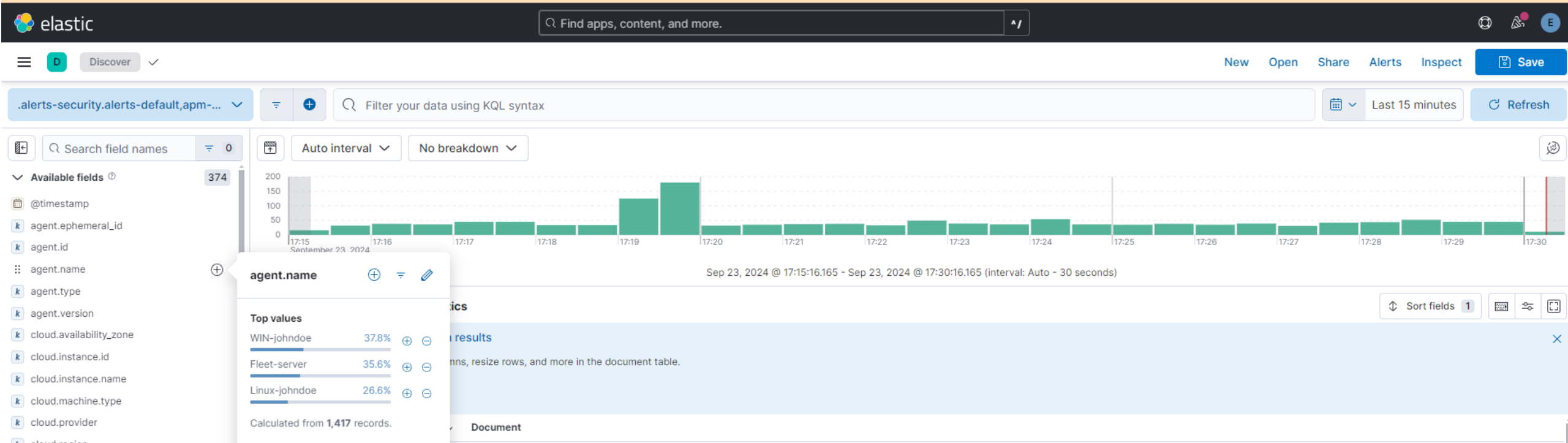
Procediamo ora con l'installazione dell'Agent su Ubuntu. Nella sezione *Fleet*, clicchiamo su *Add Agent*, selezioniamo la policy appena configurata di Linux e copiamo i comandi per installare l'Agent via SSH sul nostro PC. Per evitare problemi legati ai certificati, è possibile aggiungere l'opzione --insecure ai comandi di installazione, che bypassa la verifica dei certificati SSL, utile quando si utilizzano certificati non firmati da un'autorità riconosciuta.





Elastic Agent on Ubuntu

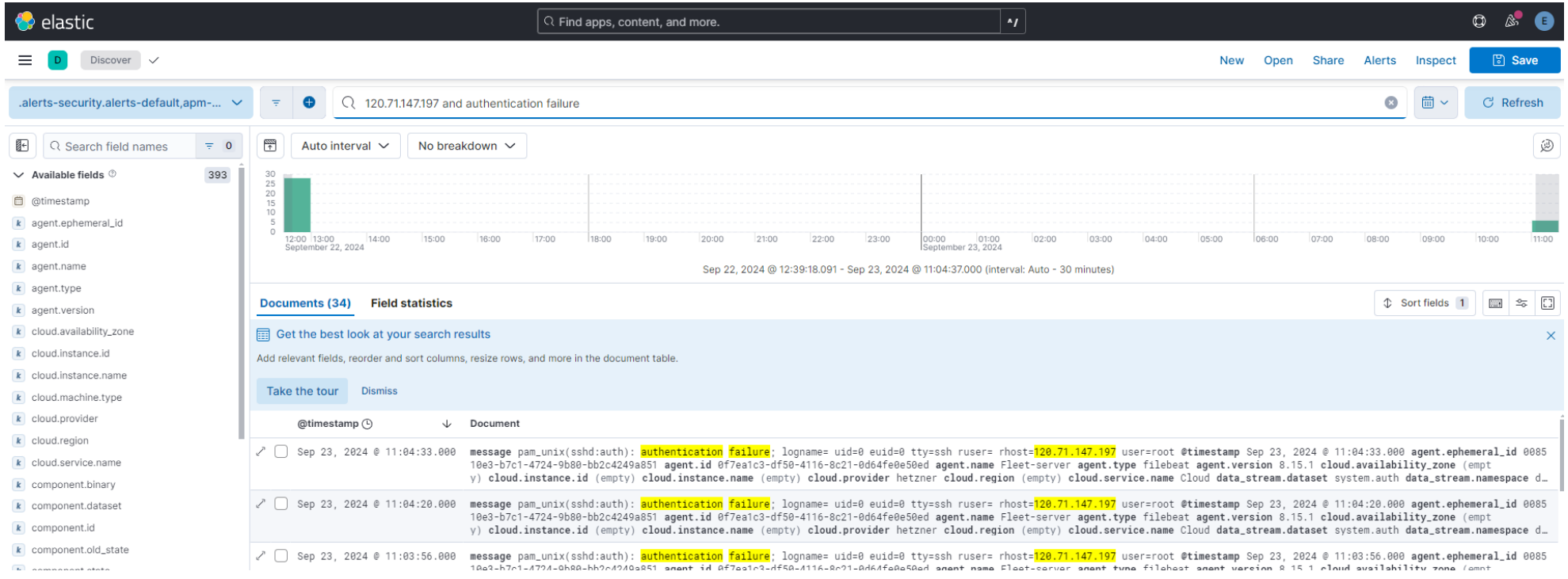
Testiamo il funzionamento nella sezione **Discover** e osserviamo che è possibile filtrare i log ricevuti, selezionando i dati relativi all'agent appena installato attraverso il campo corrispondente.



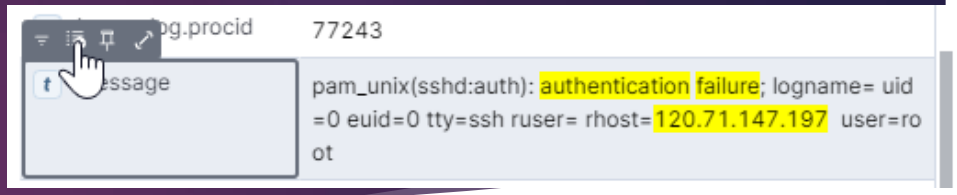
Elastic Agent on Ubuntu

```
var/log# grep -i failed auth.log | grep -i root | cut -d ' ' -f 9
120.71.147.197
120.71.147.197
120.71.147.197
```

Come ulteriore verifica possiamo prendere i risultati dei tentativi di autenticazione del Day-12 e riscontrarli nei log.



Elastic Agent on Ubuntu



Espandendo una delle entries possiamo selezionare uno dei campi che ci interessa, in questo caso 'message' , ed inserirlo nella tabella dei risultati di del **Discover**.