

# 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**

The screenshot shows the Elastic Agent console interface. The top navigation bar includes the Elastic logo, a search bar, and user profile icons. The left sidebar shows the 'Fleet' section with sub-tabs for 'Agents', 'Agent policies', 'Enrollment tokens', 'Uninstall tokens', 'Data streams', and 'Settings'. The main content area displays the 'Fleet' section with a description and a table of existing policies. A modal window titled 'Create agent policy' is open on the right, showing a form to create a new policy.

**Fleet**  
Centralized management for Elastic Agents.

[Agents](#) [Agent policies](#) [Enrollment tokens](#) [Uninstall tokens](#) [Data streams](#) [Settings](#)

Filter your data using KQL syntax

| Name ↕  | Last updated on ↓ | Unprivi |
|---|-------------------|---------|
| Windows-Policy rev. 4   | Sep 21, 2024      |         |
| Fleet Server Policy rev. 2<br>Fleet Server policy generated by Kibana | Sep 19, 2024      |         |

Rows per page: 20 ▾

### Create agent policy

Agent policies are used to manage settings across a group of agents. You can add integrations to your agent policy to specify what data your agents collect. When you edit an agent policy, you can use Fleet to deploy updates to a specified group of agents.

**Name**

Linux-Policy

☒ Collect system logs and metrics ⓘ

> [Advanced options](#)

# Elastic Agent on Ubuntu

```
root@Linux-johndoe:~# cd /var/log
root@Linux-johndoe:/var/log# ls
alternatives.log  bootstrap.log  dist-upgrade  image_build_date  landscape  syslog  watchdog
appport.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**.

☒ **Collect logs from System instances** [Change defaults ^](#)

☒ **System auth logs (log)**  
Collect System auth logs using log input

**Paths**

/var/log/auth.log\* ×

/var/log/secure\* ×

[⊕ Add row](#)

**Preserve original event**

☐ ×

Preserves a raw copy of the original event, added to the field event.original.

[> Advanced options](#)

# 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 has been successfully installed.  
root@Linux-johndoe:/var/log/elastic-agent-8.15.1-linux-x86_64#
```

## Add agent

Add Elastic Agents to your hosts to collect data and send it to the Elastic Stack.

### 1 What type of host do you want to monitor?

Settings for the monitored host are configured in the [agent policy](#). Choose an agent policy or create a new one.

[Create new agent policy](#)

Linux-Policy

The selected agent policy will collect data for 1 integration:

System

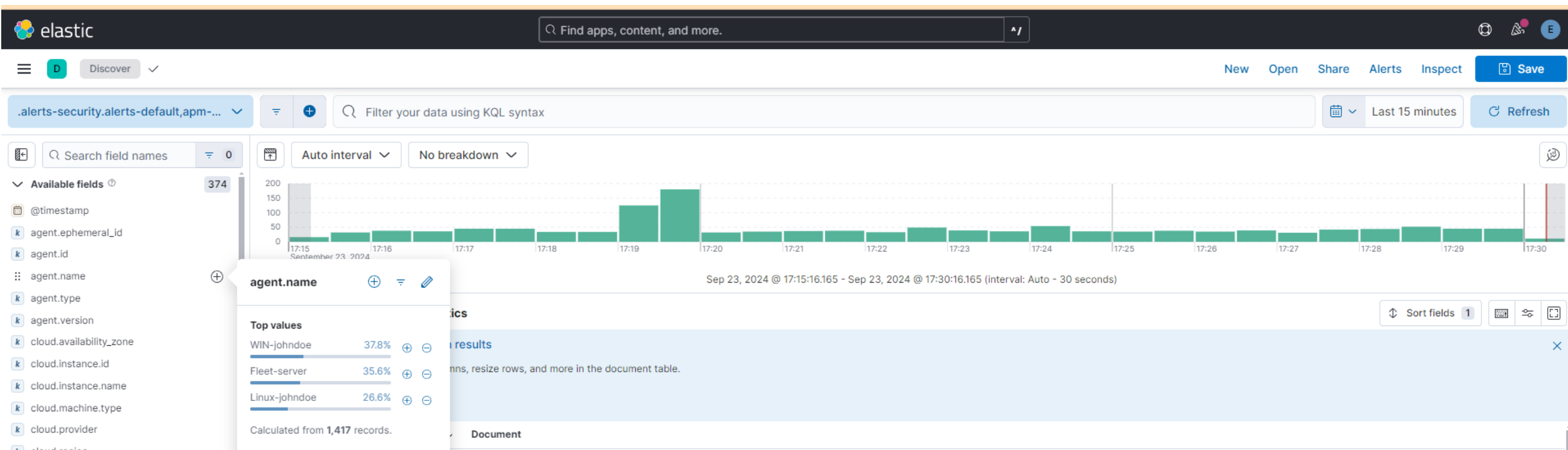
[Authentication settings](#)

### 2 Enroll in Fleet?

- ☒ **Enroll in Fleet (recommended)** – Enroll in Elastic Agent in Fleet to automatically deploy updates and centrally manage the agent.
- ☐ **Run standalone** – Run an Elastic Agent standalone to configure and update the agent manually on the host where the agent is installed.

# 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.

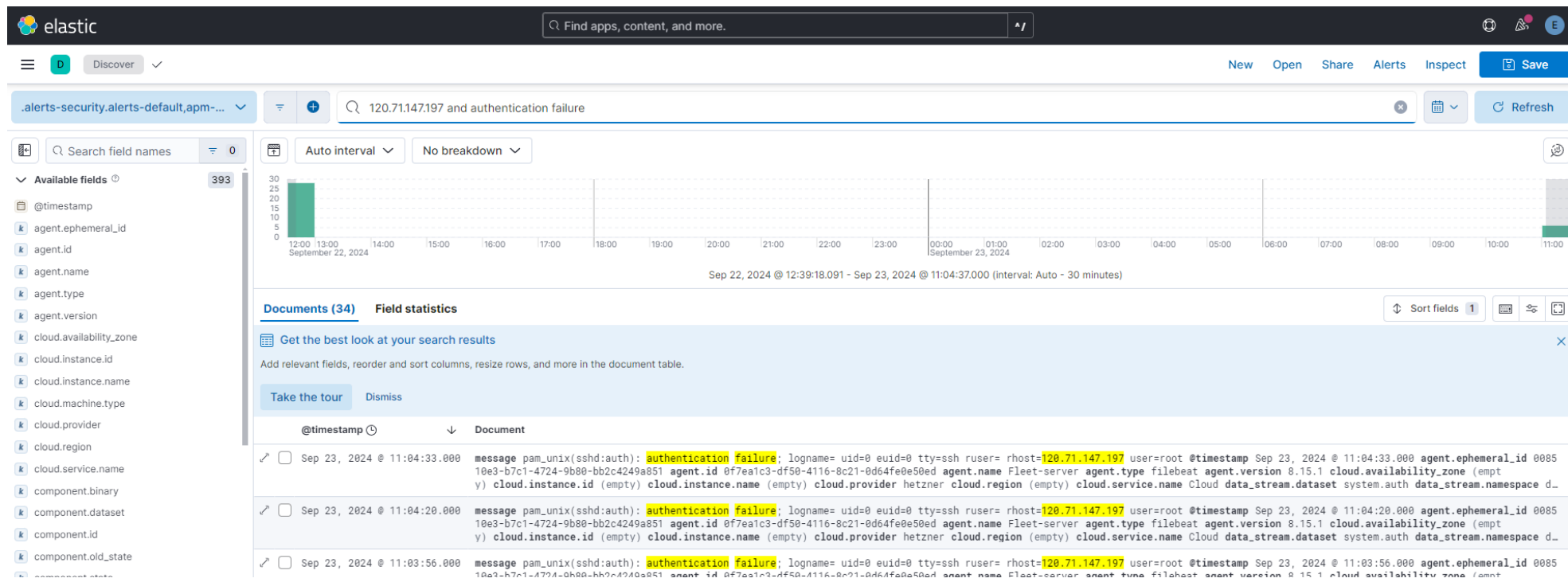


# Elastic Agent on Ubuntu

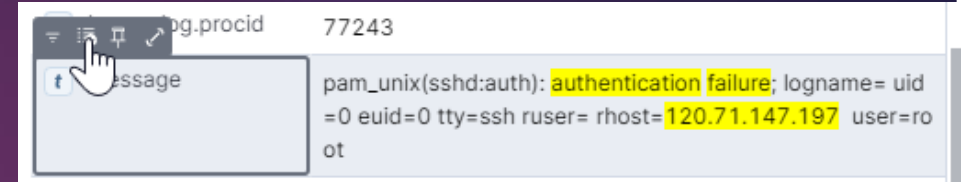
```
var/log# grep -i failed auth.log | grep -i root | cut -d ' ' -f 9
```

```
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**.

A screenshot of the Elastic Discover interface. The top bar shows the 'elastic' logo and a search bar. The main area displays search results for the query '120.71.147.197 and authentication failure'. The results are shown in a table with columns for '@timestamp' and 'message'. The 'message' column is expanded, showing log entries for 'authentication failure'. The interface includes a sidebar with field lists, a top navigation bar with buttons like 'Discover', 'New', 'Open', 'Share', 'Alerts', 'Inspect', and 'Save', and a bottom section for 'Documents (34)' and 'Field statistics'.