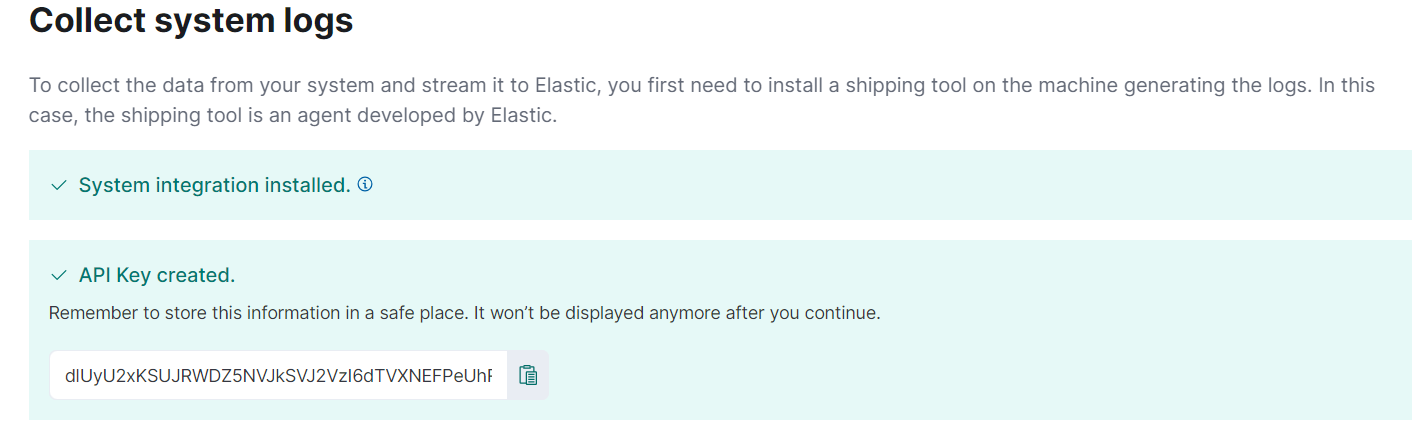
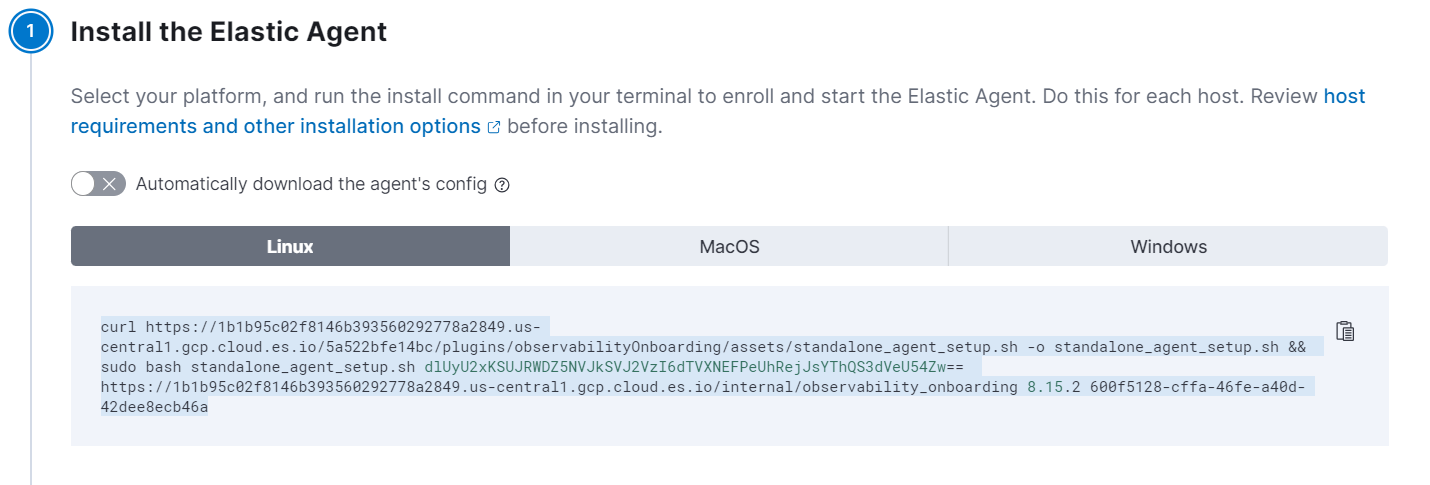
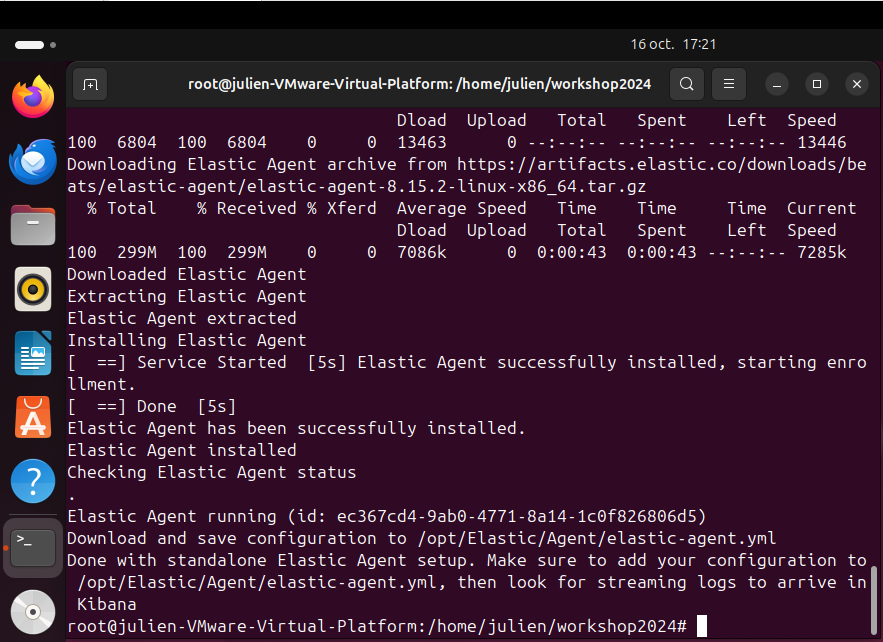
Parser log : ELK deployé dans GCP





curl https://1b1b95c02f8146b393560292778a2849.us-central1.gcp.cloud.es.io/5a522bfe14bc/plugins/observabilityOnboarding/assets/standalone\_agent\_setup.sh -o standalone\_agent\_setup.sh && sudo bash standalone\_agent\_setup.sh dlUyU2xKSUJRWDZ5NVJkSVJ2VzI6dTVXNEFPeUhRejJsYThQS3dVeU54Zw== https://1b1b95c02f8146b393560292778a2849.us-central1.gcp.cloud.es.io/internal/observability\_onboarding 8.15.2 600f5128-cffa-46fe-a40d-42dee8ecb46a



ELK configuration

outputs:

default:

type: elasticsearch

hosts:

- 'https://ef328ac6de974c749fd677d8c0366e52.us-central1.gcp.cloud.es.io:443'

api\_key: 'vU2SlJIBQX6y5RdIRvW2:u5W4AOyHQz2la8PKwUyNxg'

inputs:

- id: system-logs-138c9f4f-5368-4294-98a5-512cfedf51ae

type: logfile

data\_stream:

namespace: default

streams:

- id: logfile-system.auth-138c9f4f-5368-4294-98a5-512cfedf51ae

data\_stream:

dataset: system.auth

type: logs

paths:

- /var/log/auth.log\*

- /var/log/secure\*

exclude\_files:

- .gz$

multiline:

pattern: ^s

match: after

tags:

- system-auth

processors:

- add\_locale: null

- id: logfile-system.syslog-138c9f4f-5368-4294-98a5-512cfedf51ae

data\_stream:

dataset: system.syslog

type: logs

paths:

- /var/log/messages\*

- /var/log/syslog\*

- /var/log/system\*

exclude\_files:

- .gz$

multiline:

pattern: ^s

match: after

processors:

- add\_locale: null