

Tips & Tricks

❏ Configuration de Logstash pour recevoir Filebeat en HTTPS

Dans le fichier de configuration **Logstash** (`/etc/logstash/conf.d/http-input.conf`), utilisez le plugin **http** pour recevoir les logs :

```
input {
  http {
    port => 443
    ssl => true
    ssl_certificate => "/etc/logstash/certs/logstash.crt" # Certificat SSL
    ssl_key => "/etc/logstash/certs/logstash.key" # Clé privée SSL
    codec => "json" # Filebeat envoie les données en JSON
  }
}

filter {
  # Ajoutez ici des traitements si nécessaire
}

output {
  elasticsearch {
    hosts => ["https://localhost:9200"]
    index => "filebeat-http-%{+YYYY.MM.dd}"
    user => "elastic" # Si votre cluster Elasticsearch est sécurisé
    password => "changeme"
    ssl_certificate_verification => true
  }
}
```

❏ Configurer Filebeat pour envoyer les logs via HTTPS

Dans le fichier `filebeat.yml`, configurez l'output **HTTP** au lieu de l'output Logstash classique :

output.http:

enabled: true

url: "https://logstash-monserveur"

ssl.verification_mode: full # Vérifie le certificat SSL

headers:

Content-Type: "application/json"

Revision #2

Created 5 January 2025 08:56:29 by NoNo

Updated 24 February 2025 11:26:54 by NoNo