Deploying Fleet Server and Sending Logs Using Elastic Agent

Contents

[1. Introduction 2](#_Toc174604627)

[2. Prerequisites 2](#_Toc174604628)

[3. Steps 2](#_Toc174604629)

[Step 1: Verify Elasticsearch and Kibana Services 2](#_Toc174604630)

[Step 2: Access Kibana Dashboard 2](#_Toc174604631)

[Step 3: Configure Fleet Settings in Elasticsearch 3](#_Toc174604632)

[Open the Elasticsearch configuration file: 3](#_Toc174604633)

[Restart Elasticsearch to apply the changes: 3](#_Toc174604634)

[Step 4: Configure Fleet in Kibana 3](#_Toc174604635)

[Add Fleet Server 3](#_Toc174604636)

[Update the Elasticsearch host setting: 4](#_Toc174604637)

[Step 5: Download and Install Elastic Agent 4](#_Toc174604638)

[Extract the downloaded Elastic Agent package: 4](#_Toc174604639)

[Navigate to the Elastic Agent directory: 4](#_Toc174604640)

[Use the generated service token to enroll the Elastic Agent: 4](#_Toc174604641)

[Step 6: Integrate Logs with Elastic Agent 5](#_Toc174604642)

[Step 7: Verify Logs in Kibana 5](#_Toc174604643)

[Step 8: Monitor Elastic Agent Metrics 5](#_Toc174604644)

[4. Conclusion 5](#_Toc174604645)

# 1. Introduction

Fleet Server is a central component in Elastic's unified agent management system, allowing you to manage Elastic Agents and monitor data from various sources. In this guide, we will deploy a Fleet server, configure it to work with Elasticsearch and Kibana, and use Elastic Agent to send Zeek logs to Elasticsearch.

# 2. Prerequisites

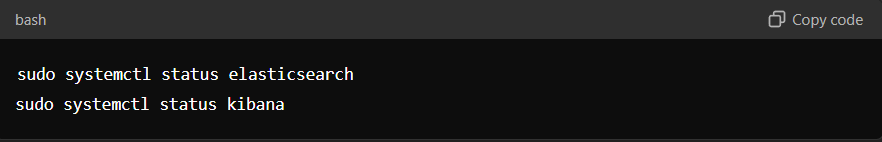
A running instance of the ELK Stack (Elasticsearch, Logstash, Kibana) on Ubuntu.

Sudo or root privileges on the server.

# 3. Steps

## Step 1: Verify Elasticsearch and Kibana Services

Before starting, ensure that both Elasticsearch and Kibana are running.



sudo systemctl status elasticsearch

sudo systemctl status kibana

## Step 2: Access Kibana Dashboard

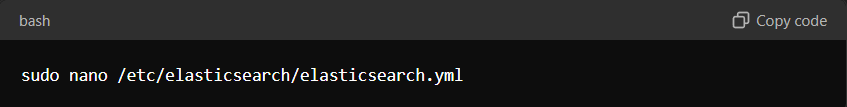
Open your web browser and navigate to the Kibana dashboard. The URL typically follows this format:

http://<your-server-ip>:5601

Log in using the credentials you configured with X-Pack.

## Step 3: Configure Fleet Settings in Elasticsearch

### Open the Elasticsearch configuration file:



sudo nano /etc/elasticsearch/elasticsearch.yml

Ensure that the following settings are added to enable Fleet server functionality:

xpack.security.enabled: true

xpack.security.authc.api\_key.enabled: true

Save the file and exit the editor (Ctrl + X, then Y, then Enter).

### Restart Elasticsearch to apply the changes:



sudo systemctl restart elasticsearch

## Step 4: Configure Fleet in Kibana

Return to the Kibana dashboard and navigate to Management > Fleet.

### Add Fleet Server

In Kibana, go to Fleet > Agents and click Add Fleet Server.

Quick Start: Automatically generate a Fleet Server policy with self-signed certificates (not recommended for production).

Advanced: Use your own Fleet Server policy or TLS certificates. Ensure the --url matches the DNS name used in the --fleet-server-cert.

Follow the in-product instructions to configure and install the Fleet Server.

Include --fleet-server-host and --fleet-server-port options in the elastic-agent install command if using a non-default port.

Upon successful installation, the Fleet Server will be connected and managed through the main Fleet page in Kibana.

### Update the Elasticsearch host setting:

Set the Elasticsearch host IP to your server's IP (e.g., 192.168.68.1).

Set the Fleet Server host to http://<your-server-ip>:8220 (**replace <your-server-ip> with your actual IP address**).

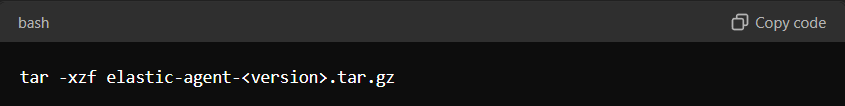
Save and apply these settings.

## Step 5: Download and Install Elastic Agent

Go to the Elastic Agent download page from within the Kibana Fleet UI.

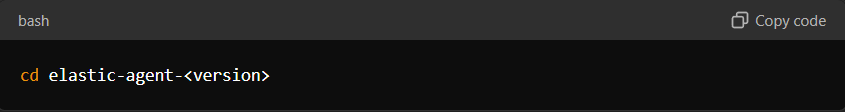
Download the appropriate Elastic Agent for your operating system.

### Extract the downloaded Elastic Agent package:



tar -xzf elastic-agent-<version>.tar.gz

### Navigate to the Elastic Agent directory:



cd elastic-agent-<version>

### Use the generated service token to enroll the Elastic Agent:

sudo ./elastic-agent install --url=http://<your-server-ip>:8220 --enrollment-token=<your-token>

Enter the password when prompted.

Once the Elastic Agent is installed and running, you should see a confirmation message.

## Step 6: Integrate Logs with Elastic Agent

In the Kibana dashboard, go to Integrations and search for the relevant integration (e.g., filebeat, system logs, or any other application logs)

If you haven't already, configure the chosen integration by adding the necessary configuration to your setup.

Specify the path where the logs are stored on your server. For example:

/var/logs/application\_name/

Save and deploy the changes.

## Step 7: Verify Logs in Kibana

Go to the Logs section in Kibana.

Check that logs are being ingested from the Elastic Agent.

You should see logs from integrations, along with relevant data such as host name, timestamps, and log content.

## Step 8: Monitor Elastic Agent Metrics

In Kibana, navigate to Dashboard.

Select the Elastic Agent metrics dashboard to monitor CPU usage, memory usage, and other metrics for the agent.

# 4. Conclusion

By following these steps, you have successfully deployed a Fleet server and configured it to send Zeek logs to Elasticsearch using Elastic Agent. This setup allows for centralized management and monitoring of your data, improving visibility and security.