



# INSTALLING ELASTICSEARCH ON LOCAL VM

## A Step-by-Step Guide



elasticsearch

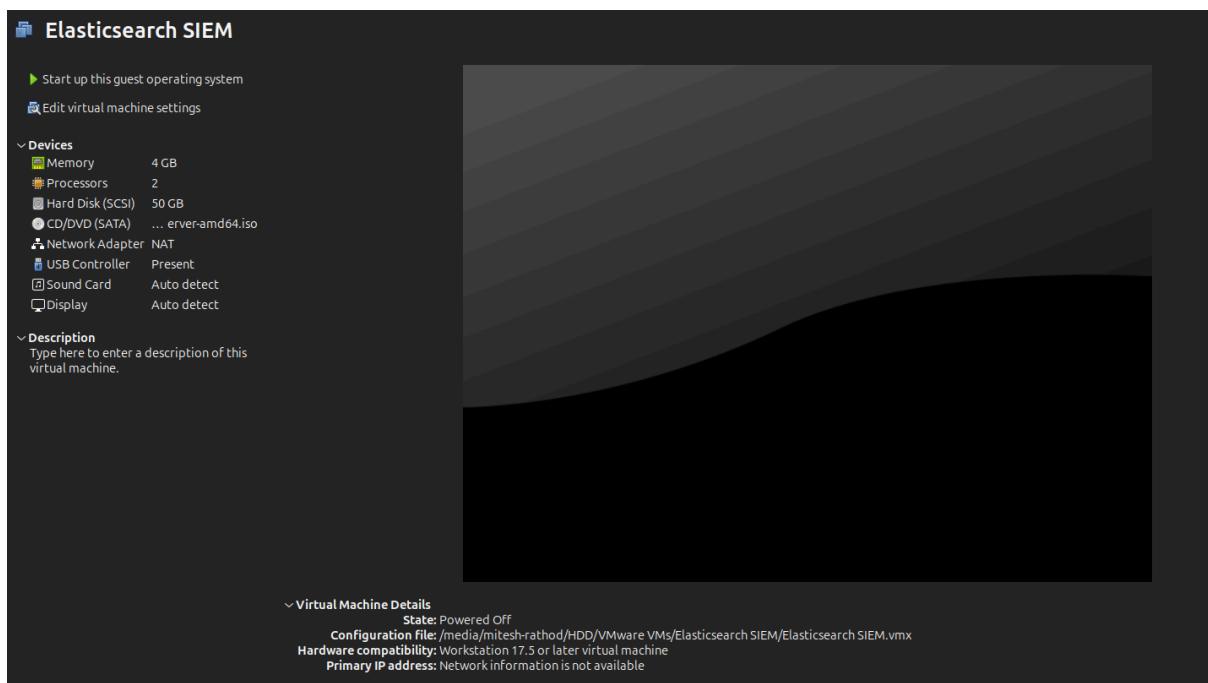
# TABLE OF CONTENTS

1. Setting up Local VM for Elasticsearch ~ [Page no. 3](#)
2. Installing Elasticsearch on Local VM ~ [Page no. 4](#)
3. Filebeat Configuration & Installation ~ [Page no. 11](#)

# SETTING UP LOCAL VM FOR ELASTICSEARCH

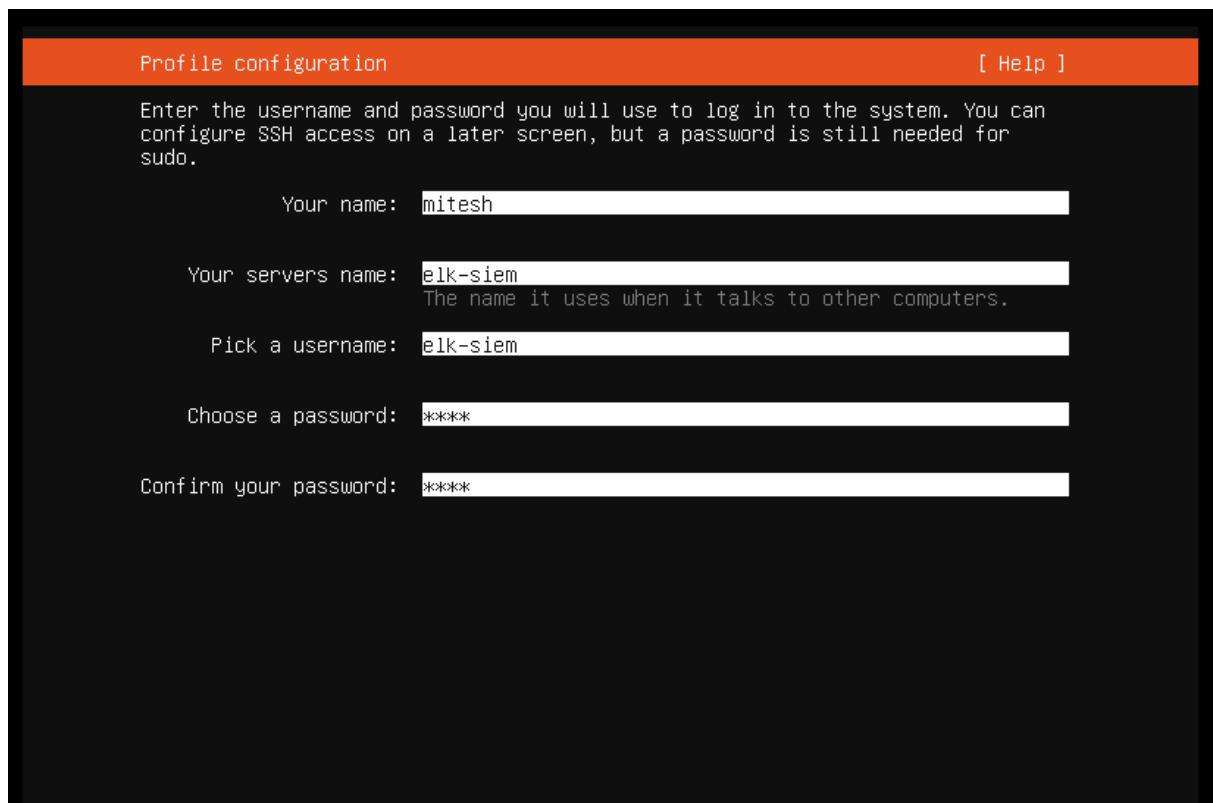
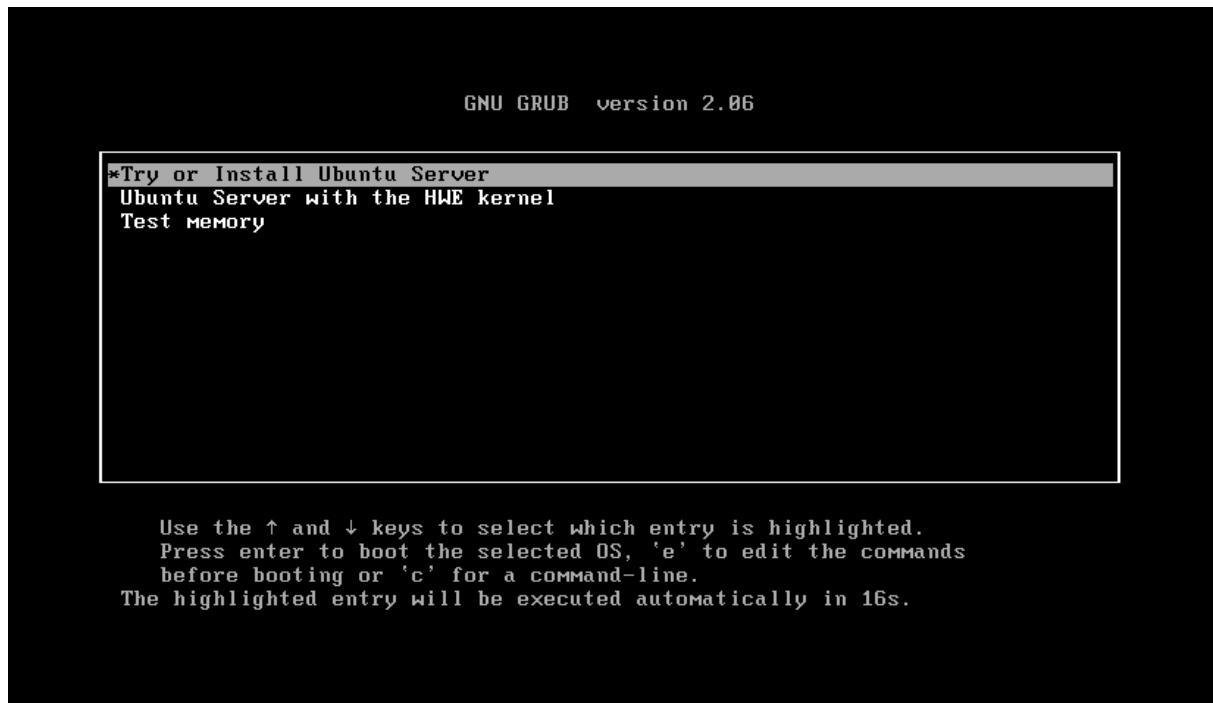
## Requirements:

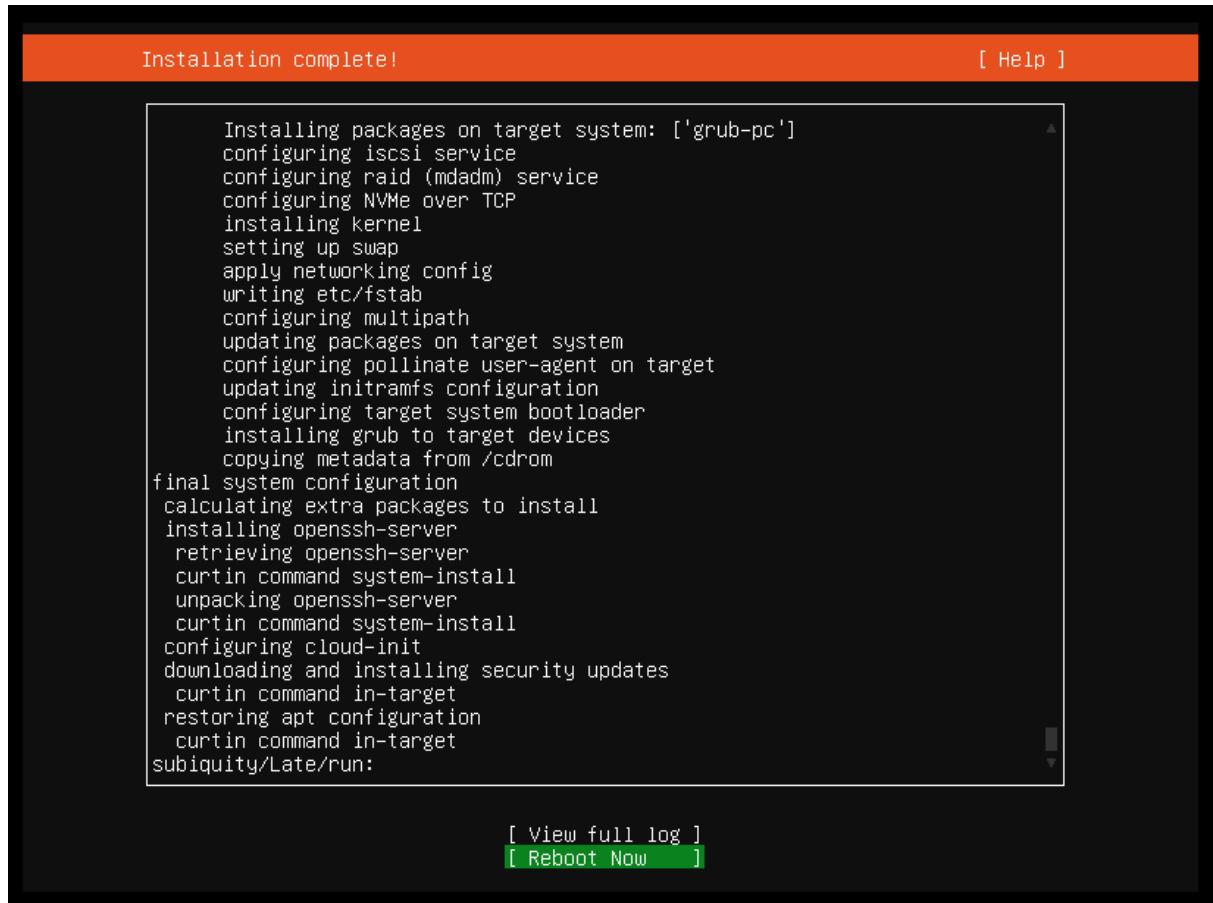
1. Ubuntu Server .iso file: I'm using the 22.04 version.
2. VirtualBox/VMware: I'm using VMware.
3. 50 GB SSD/HDD, 4 GB RAM & 2 CPU



# Installing Elasticsearch on Local VM

1. Start your VM and install Ubuntu Server first.





```
mitesh-rathod@mitesh-rathod:~$ ssh elk-siem@192.168.29.251
The authenticity of host '192.168.29.251 (192.168.29.251)' can't be established.
ED25519 key fingerprint is SHA256:u60Bb4pp4o3FI+Yegn+zk0Tp1XBsH4zWXj3aAQcc07k.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '192.168.29.251' (ED25519) to the list of known hosts.
elk-siem@192.168.29.251's password:
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-153-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

System information as of Wed Aug 27 04:07:09 AM UTC 2025

  System load:          0.75
  Usage of /:           29.2% of 23.45GB
  Memory usage:         9%
  Swap usage:          0%
  Processes:            242
  Users logged in:     0
  IPv4 address for ens3: 192.168.29.251
  IPv6 address for ens3: 2405:201:2009:2087:20c:29ff:fe82:6d3a

Expanded Security Maintenance for Applications is not enabled.

54 updates can be applied immediately.
To see these additional updates run: apt list --upgradable

Enable ESM Apps to receive additional future security updates.
See https://ubuntu.com/esm or run: sudo pro status

New release '24.04.3 LTS' available.
Run 'do-release-upgrade' to upgrade to it.

Last login: Wed Aug 27 04:07:10 2025
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

elk-siem@elk-siem:~$
```

**2. Update & Upgrade your VM using the command:**

```
sudo apt-get update && sudo apt-get upgrade
```

**3. Install Docker Compose using the command:**

```
sudo apt install docker-compose
sudo apt install docker.io
```

4. Create a folder/directory named “elasticsearch” and create a “docker-compose.yml” in it.

```
root@elk-siem:/home/elk-siem# mkdir elasticsearch
root@elk-siem:/home/elk-siem# cd elasticsearch/
root@elk-siem:/home/elk-siem/elasticsearch# touch docker_compose.yml
root@elk-siem:/home/elk-siem/elasticsearch#
```

5. Copy & paste the following code inside the “docker-compose.yml” file, and save it.

**Source Code:**

```
version: "2"
```

```
networks:
```

```
  elastic:
```

```
    driver: bridge
```

```
volumes:
```

```
  elasticsearch:
```

```
    driver: local
```

```
services:
```

```
  elasticsearch:
```

```
    image: docker.elastic.co/elasticsearch/elasticsearch:7.15.0
```

```
    restart: unless-stopped
```

```
    environment:
```

- "discovery.type=single-node"
- "ES\_JAVA\_OPTS=-Xms512m -Xmx512m"
- "xpack.security.enabled=true"
- "xpack.security.authc.api\_key.enabled=true"
- "ELASTIC\_PASSWORD=Elastic@123"

```
    ulimits:
```

```
      memlock:
```

```
        soft: -1
```

```
        hard: -1
```

```
    volumes:
```

- elasticsearch:/usr/share/elasticsearch/data

```
  ports:
```

- 0.0.0.0:9200:9200

```
  networks:
```

- elastic

```
ent-search:  
  image: docker.elastic.co/enterprise-search/enterprise-search:7.15.0  
  restart: unless-stopped  
  depends_on:  
    - "elasticsearch"  
  environment:  
    - "JAVA_OPTS=-Xms512m -Xmx512m"  
    - "ENT_SEARCH_DEFAULT_PASSWORD=Elastic@123" # Added  
missing closing quote here  
  here  
    - "elasticsearch.username=elastic"  
    - "elasticsearch.password=Elastic@123" # Added missing closing quote  
  -  
    - "elasticsearch.host=http://elasticsearch:9200"  
    - "allow_es_settings_modification=true"  
    -  
      "secret_management.encryption_keys=[4a2cd3f81d39bf28738c10db0ca7820  
95ffac07279561809eecc722e0c20eb09]"  
      - "elasticsearch.startup_retry.interval=15"  
  ports:  
    - 0.0.0.0:3002:3002  
  networks:  
    - elastic  
  
kibana:  
  image: docker.elastic.co/kibana/kibana:7.15.0  
  restart: unless-stopped  
  depends_on:  
    - "elasticsearch"  
    - "ent-search"  
  ports:  
    - 0.0.0.0:5601:5601  
  environment:  
    ELASTICSEARCH_HOSTS: http://elasticsearch:9200  
    ENTERPRISESEARCH_HOST: http://ent-search:3002  
    ELASTICSEARCH_USERNAME: elastic  
    ELASTICSEARCH_PASSWORD: Elastic@123  
    XPACK_ENCRYPTEDSAVEDOBJECTS_ENCRYPTIONKEY:  
    "X5rtEXBA3Js1sNMu7VpY4QKIEBpjwzkb231"  
  networks:  
    - elastic
```

**6. Type the following command to up and running our ELK stack:**

```
sudo docker-compose up -d
```

```
54678bb77310: Pull complete
7914e53b543b: Pull complete
Digest: sha256:160b4ebbb9e06cef347012ea8102d05642716855498c5415814aa9b91a5ecbb
Status: Downloaded newer image for docker.elastic.co/kibana/kibana:7.15.0
Creating elasticsearch_elasticsearch_1 ... done
Creating elasticsearch_ent-search_1    ... done
Creating elasticsearch_kibana_1       ... done
root@elk-siem:/home/elk-siem/elasticsearch#
```

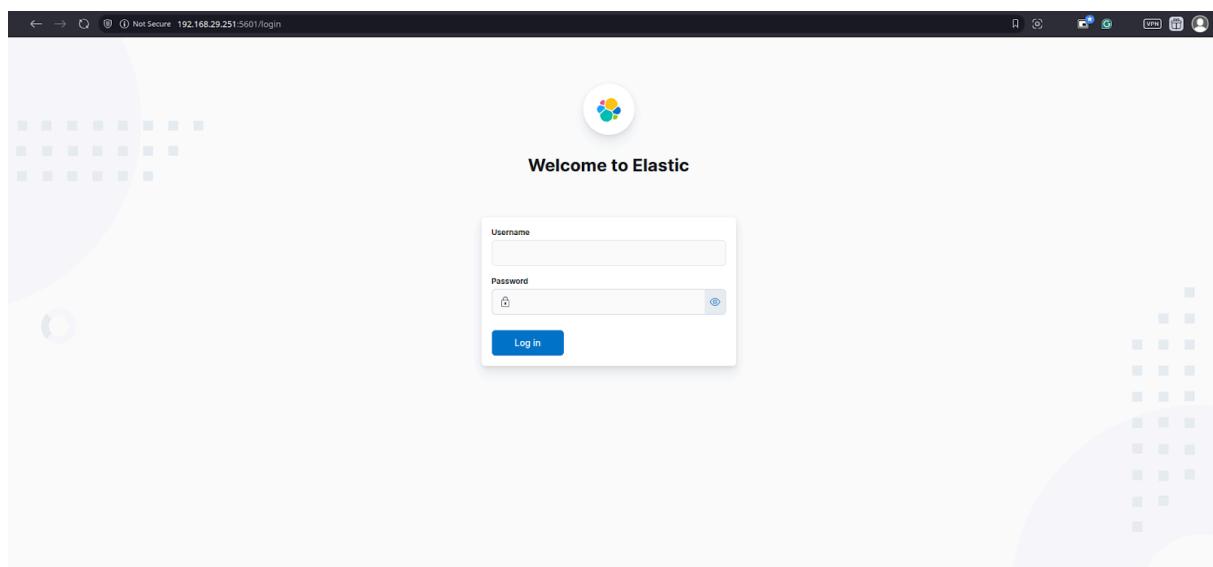
**7. Type the following command to check the status of our container:**

```
sudo docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
a2013155a75d	docker.elastic.co/kibana/kibana:7.15.0	/bin/tini -- /usr/l...	4 minutes ago	Up 4 minutes	0.0.0.0:5601->5601/tcp	elasticsearch_kibana_1
1bc5f74922b3	docker.elastic.co/enterprise-search/enterprise-search:7.15.0	/bin/tini -- /usr/l...	4 minutes ago	Up 4 minutes	0.0.0.0:3002->3002/tcp	elasticsearch_ent-search_1
bbc52fb83420	docker.elastic.co/elasticsearch/elasticsearch:7.15.0	/bin/tini -- /usr/l...	4 minutes ago	Up 4 minutes	0.0.0.0:9200->9200/tcp, 9300/tcp	elasticsearch_elasticsearch_1

**8. Access the Kibana dashboard by typing the following in the browser URL:**

<http://your-ubuntu-vm-ip:5601>



**Username:** elastic

**Password:** Elastic@123

9. Click on “Explore on my own” and you will be redirected to the home page.

The image consists of two vertically stacked screenshots of the Elastic search interface. The top screenshot shows the initial 'Welcome to Elastic' page. It features a central card with the text 'Start by adding your data' and a sub-section about usage data collection. Below this are two buttons: 'Add data' and 'Explore on my own'. The bottom screenshot shows the 'Welcome home' page. It displays four service cards: 'Enterprise Search' (yellow), 'Observability' (pink), 'Security' (teal), and 'Analytics' (blue). Each card has a brief description and a small icon. Below these cards is a section titled 'Get started by adding your data' with a 'Try sample data' button. The overall design is clean and modern, using a light blue and white color scheme.

# FILEBEAT CONFIGURATION & INSTALLATION

## 1. Download the Filebeat Debian package :

```
curl -L -O
```

```
https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.15.0-amd64.deb
```

## 2. Installing Filebeat :

```
sudo dpkg -i filebeat-7.15.0-amd64.deb
```

## 3. Configuring Filebeat :

```
sudo nano /etc/filebeat/filebeat.yml (This is the Filebeat configuration file that needs to be edited.)
```

## 4. Setting Output to Elasticsearch:

```
output.elasticsearch:
```

```
# Array of hosts to connect to.  
hosts: ["http://x.x.x.x:9200"] #this is your Elasticsearch IP address  
# Protocol - either `http` (default) or `https`.  
protocol: "http"  
# Authentication credentials - either API key or username/password.  
#api_key: "id:api_key"  
username: "<elastic username>"  
password: "<elastic password>"
```

```
GNU nano 6.2                                     /etc/filebeat/filebeat.yml  
# ----- Elasticsearch Output -----  
output.elasticsearch:  
  # Array of hosts to connect to.  
  hosts: ["192.168.29.251:9200"]  
  
  # Protocol - either `http` (default) or `https`.  
  protocol: "http"  
  
  # Authentication credentials - either API key or username/password.  
  #api_key: "id:api_key"  
  username: "elastic"  
  password: "Elastic@123"
```

## 5. Setting Up Kibana:

setup.kibana:

```
host: "http://x.x.x.x:5601" # this is your Kibana IP address
```

```
GNU nano 6.2                                     /etc/filebeat/filebeat.yml

# ====== Kibana ======
# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.

setup.kibana:

  # Kibana Host
  # Scheme and port can be left out and will be set to the default (http and 5601)
  # In case you specify an additional path, the scheme is required: http://localhost:5601/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:5601
  host: "192.168.29.251:5601"
```

## 6. Enabling Filebeat Module:

```
cd /etc/filebeat/modules.d/
```

```
sudo filebeat modules enable system
```

## 7. Starting Filebeat Service:

```
sudo service filebeat start
```

## 8. Verify that Filebeat is working properly or not:

```
Go to browser http://your-elk-vm-ip:5601 -> Management -> Stack Management -> Data -> Index Management
```

The screenshot shows the Elastic Stack Management interface. At the top, there's a header bar with a left arrow, a right arrow, a refresh icon, a shield icon indicating 'Not Secure', and the URL '192.168.29.251:5601/app/home'. Below the header is the Elastic logo and the word 'elastic'.

The main navigation menu on the left includes:

- Home (selected)
- Logs
- Metrics
- APM
- Uptime
- User Experience

Under the 'Security' section:

- Overview
- Alerts
- Hosts
- Network
- Timelines
- Cases
- Endpoints

Under the 'Management' section:

- Dev Tools
- Integrations
- Fleet
- Osquery
- Stack Monitoring
- Stack Management (highlighted in a grey box)

The central content area features a large 'Welcome' banner with a yellow background, a white circular icon with a teal 'o' inside, and the word 'Enterprise'. Below it, a call-to-action button says '+ Add your data'.

On the right side, there's a 'Get started by' section with a message: 'To start working with data from an app or your own data, add a sample'.

The screenshot shows the Elasticsearch Index Management interface. The left sidebar has sections for Management, Ingest, Data, and Alerts and Insights. Under Data, the Index Management section is selected. The main area is titled "Index Management" and contains tabs for Indices, Data Streams, Index Templates, and Component Templates. The Indices tab is active. A search bar at the top right says "Search Elastic". Below the tabs, there's a message: "Update your Elasticsearch indices individually or in bulk. [Learn more.](#)". There are checkboxes for "Include rollup indices" and "Include hidden indices". A "Lifecycle status" dropdown is set to "yellow". A "Lifecycle phase" dropdown is set to "green". A "Reload indices" button is visible. A table lists the index details:

Name	Health	Status	Primaries	Replicas	Docs count	Storage size	Data stream
filebeat-715.0-2025.08.28-000001	yellow	open	1	1	2350	512.9kb	

At the bottom, it says "Rows per page: 10" and has navigation arrows.

We can see Filebeat is working fine as expected.