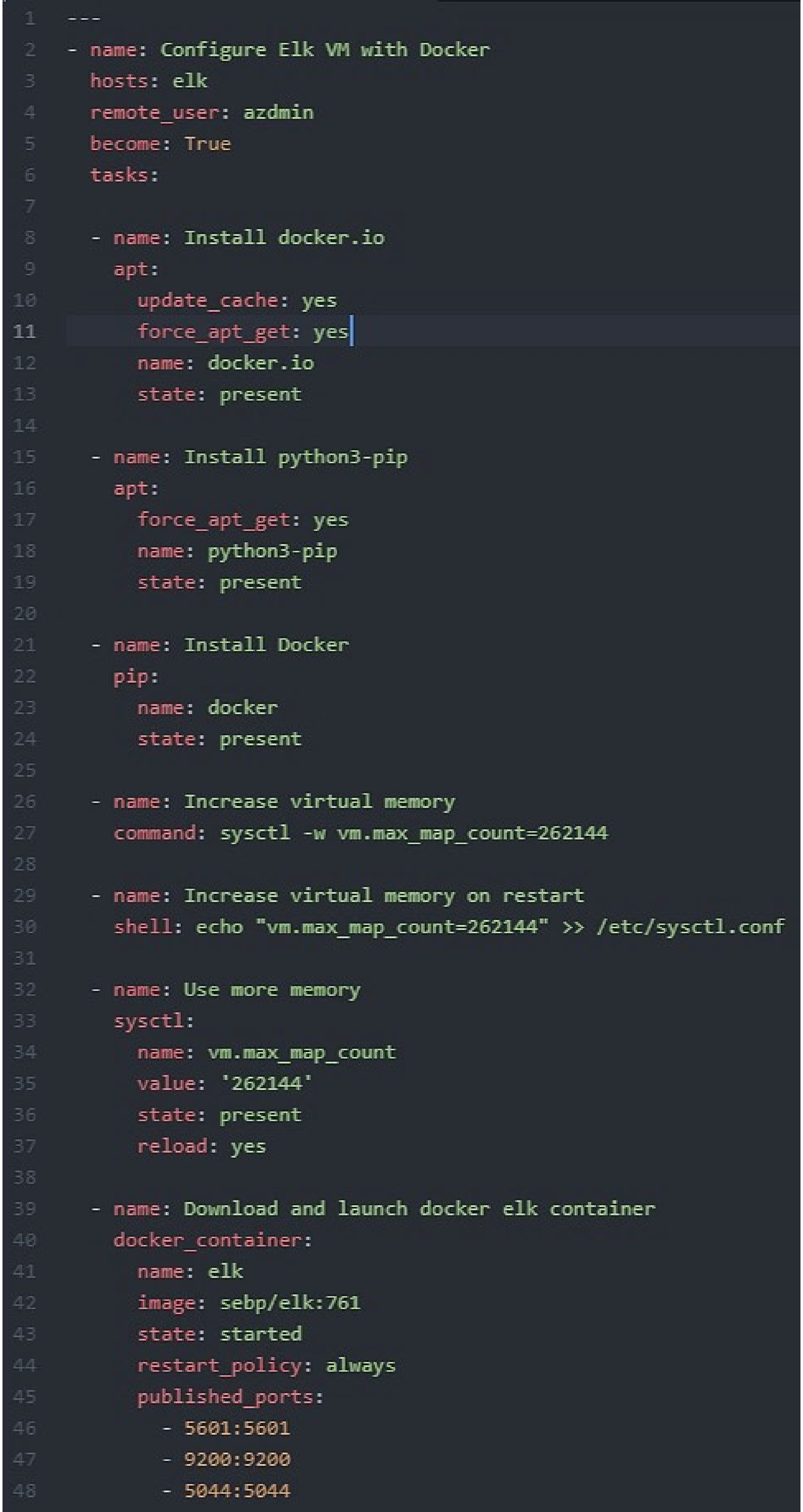
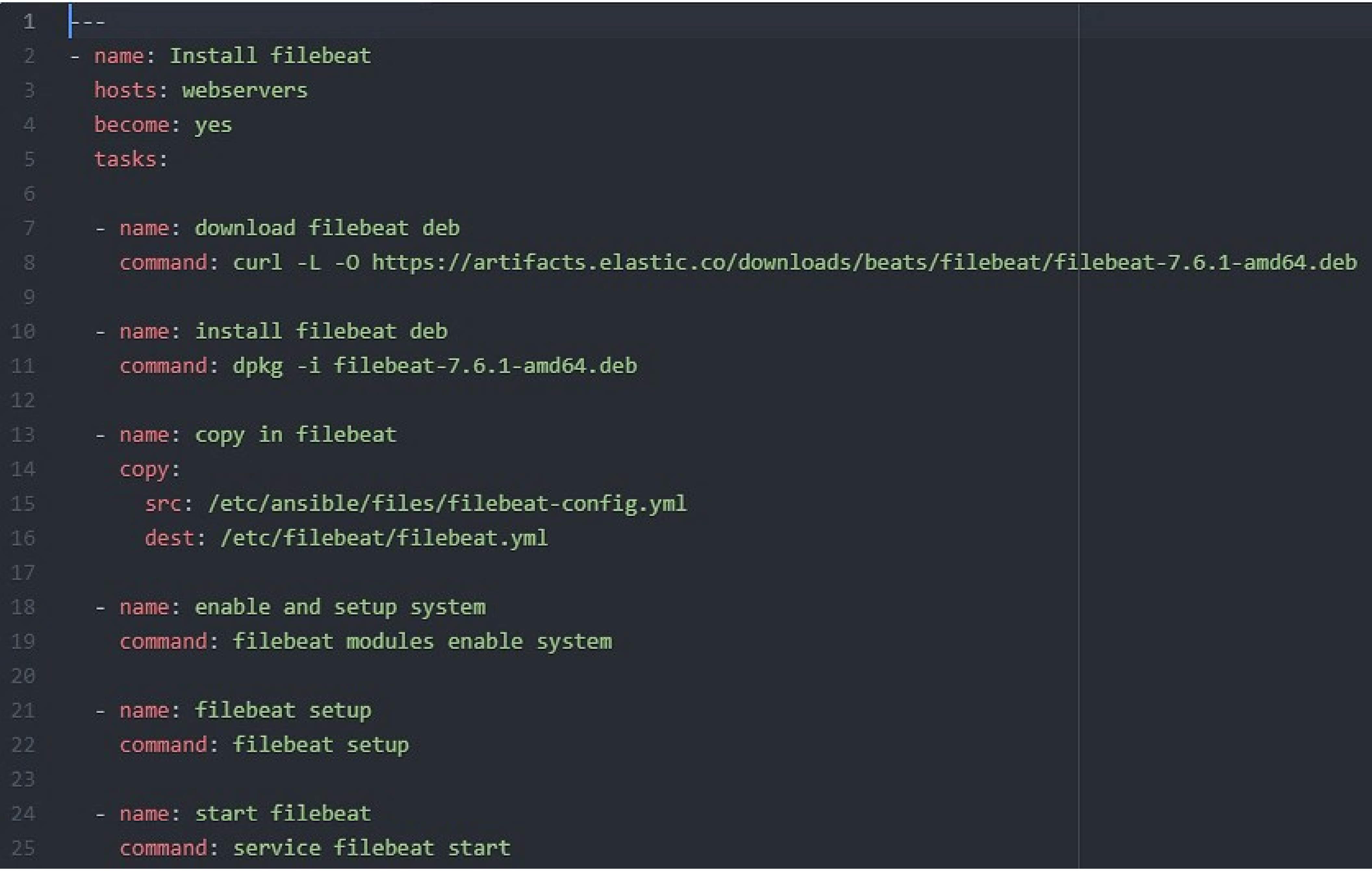
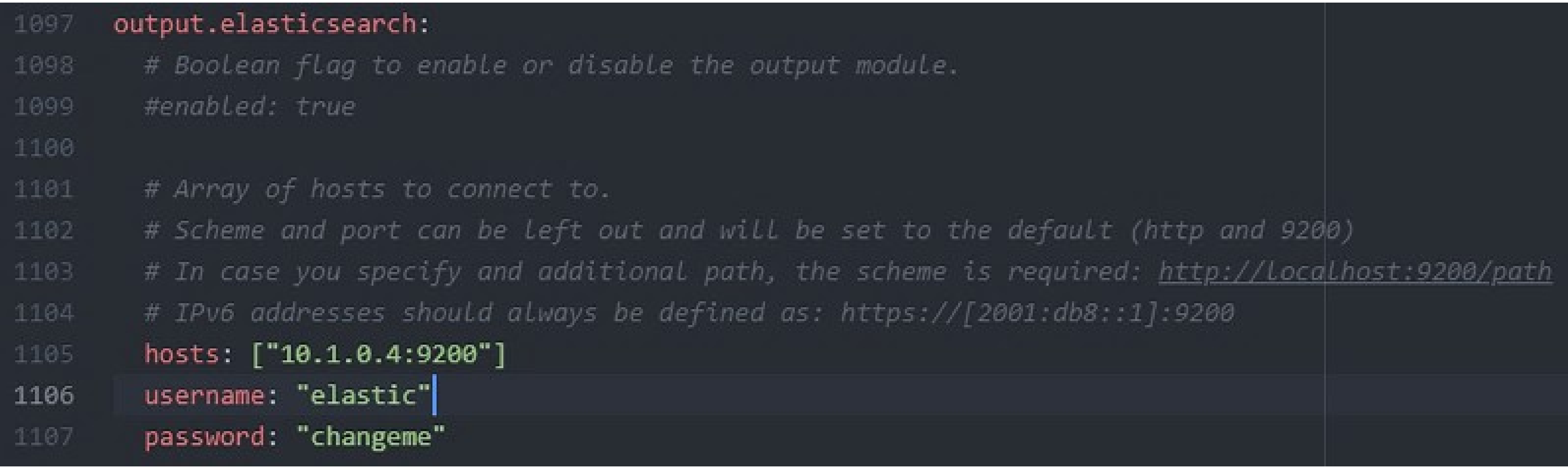


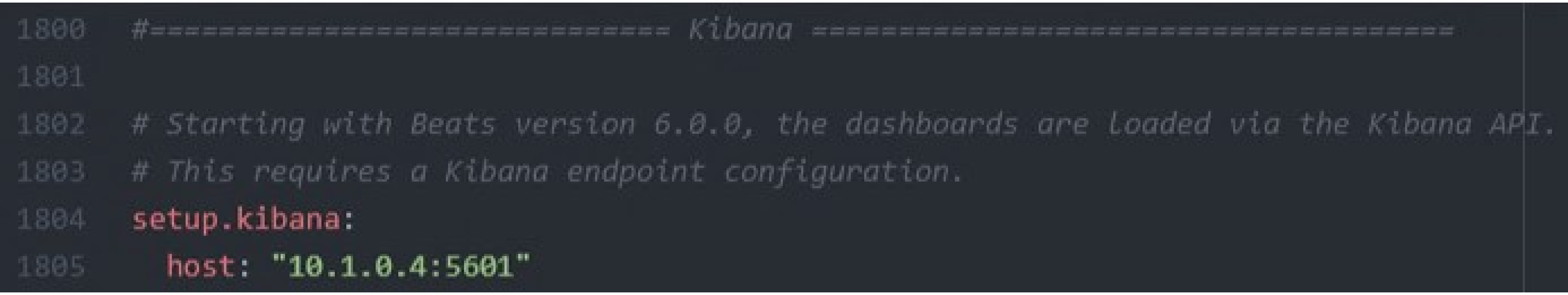
```yaml
---
- name: Configure Elk VM with Docker
  hosts: elk
  remote_user: azdmin
  become: True
  tasks:

  - name: Install docker.io
    apt:
      update_cache: yes
      force_apt_get: yes
      name: docker.io
      state: present

  - name: Install python3-pip
    apt:
      force_apt_get: yes
      name: python3-pip
      state: present

  - name: Install Docker
    pip:
      name: docker
      state: present

  - name: Increase virtual memory
    command: sysctl -w vm.max_map_count=262144

  - name: Increase virtual memory on restart
    shell: echo "vm.max_map_count=262144" >> /etc/sysctl.conf

  - name: Use more memory
    sysctl:
      name: vm.max_map_count
      value: '262144'
      state: present
      reload: yes

  - name: Download and launch docker elk container
    docker_container:
      name: elk
      image: sebp/elk:761
      state: started
      restart_policy: always
      published_ports:
        - 5601:5601
        - 9200:9200
        - 5044:5044
```



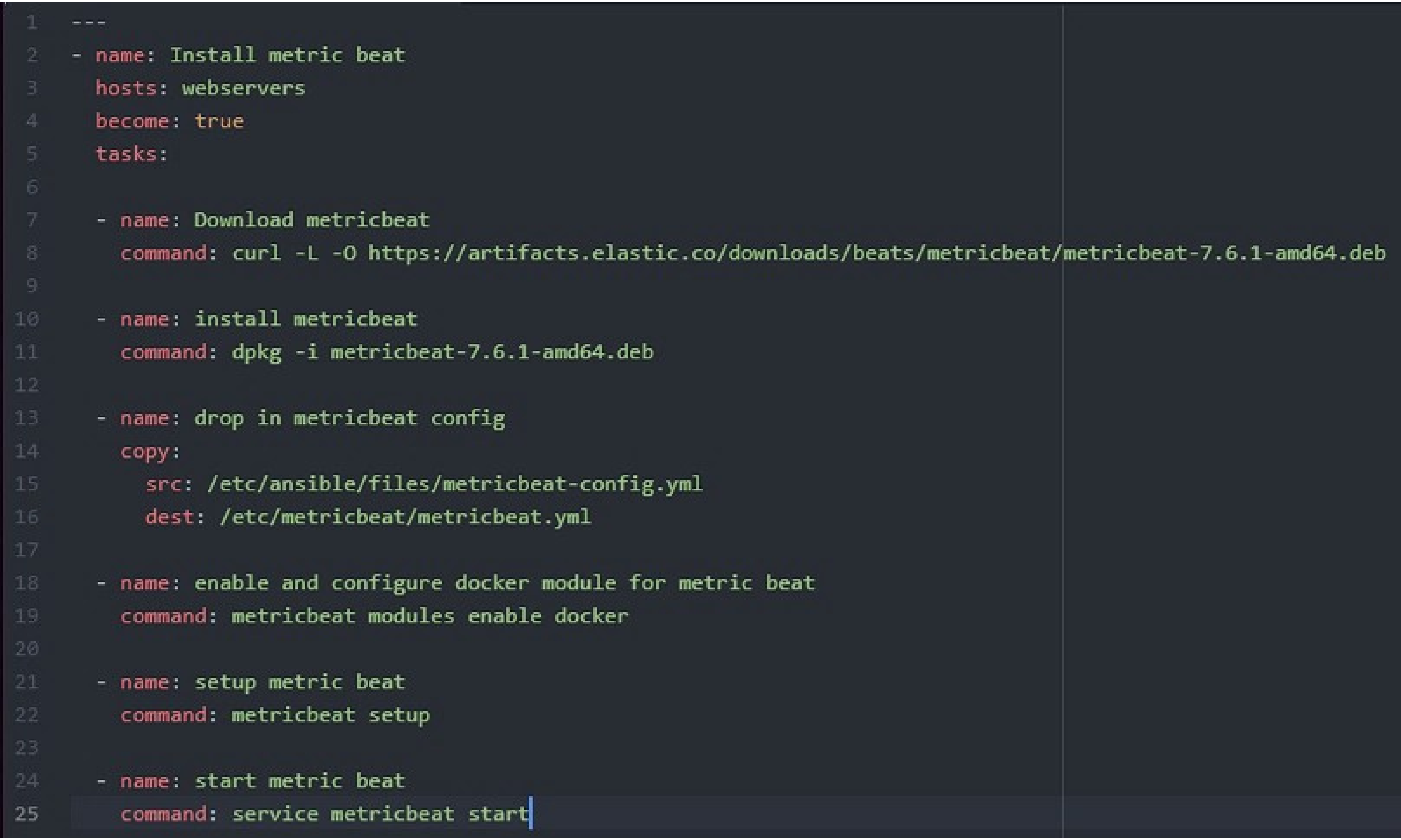
```yaml
---
- name: Install filebeat
  hosts: webservers
  become: yes
  tasks:

  - name: download filebeat deb
    command: curl -L -O https://artifacts.elastic.co/downloads/beats/filebeat/filebeat-7.6.1-amd64.deb

  - name: install filebeat deb
    command: dpkg -i filebeat-7.6.1-amd64.deb

  - name: copy in filebeat
    copy:
      src: /etc/ansible/files/filebeat-config.yml
      dest: /etc/filebeat/filebeat.yml

  - name: enable and setup system
    command: filebeat modules enable system

  - name: filebeat setup
    command: filebeat setup

  - name: start filebeat
    command: service filebeat start
```



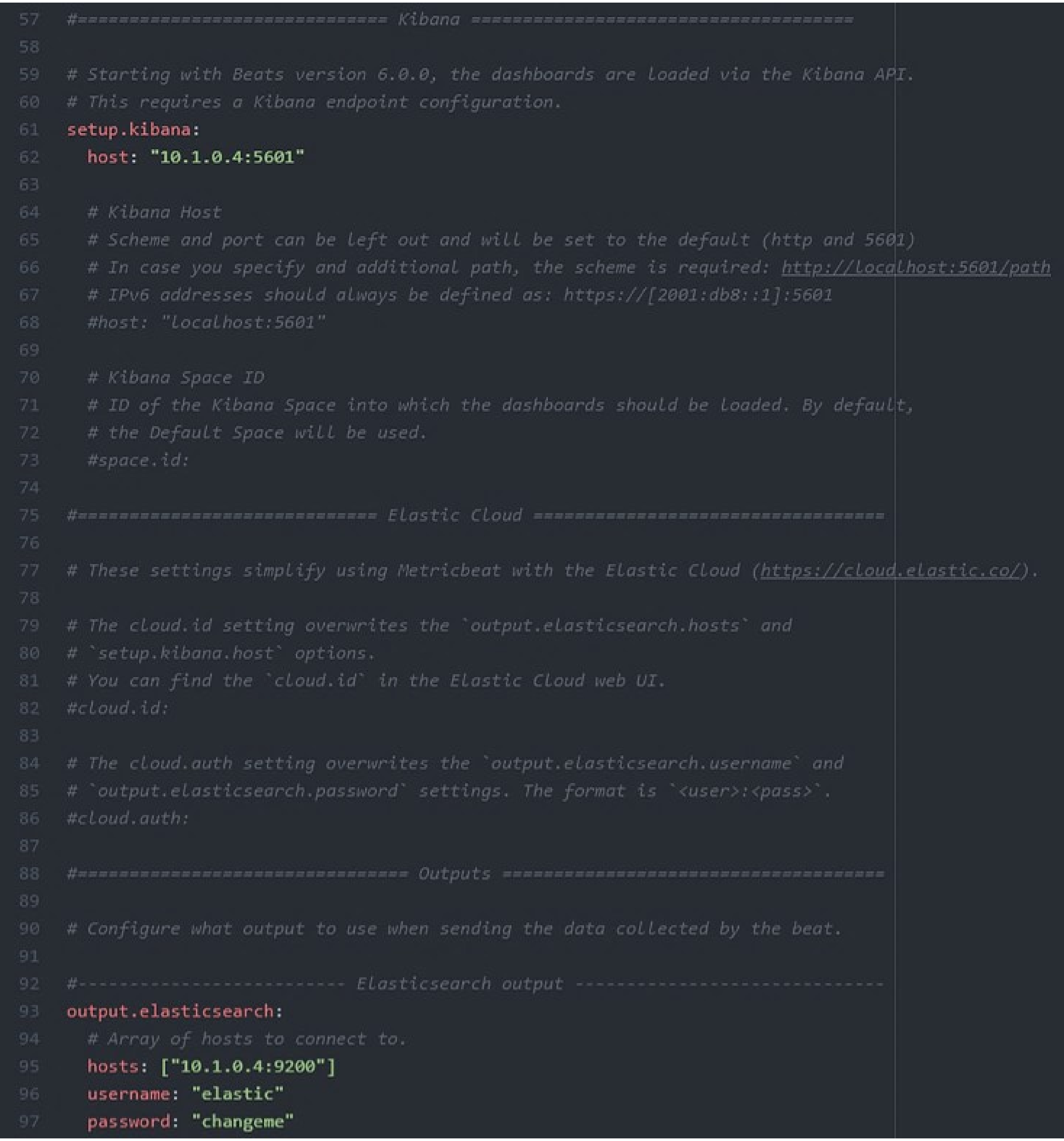
```
output.elasticsearch:
  # Boolean flag to enable or disable the output module.
  #enabled: true

  # Array of hosts to connect to.
  # Scheme and port can be left out and will be set to the default (http and 9200)
  # In case you specify and additional path, the scheme is required: http://localhost:9200/path
  # IPv6 addresses should always be defined as: https://[2001:db8::1]:9200
  hosts: ["10.1.0.4:9200"]
  username: "elastic"
  password: "changeme"
```



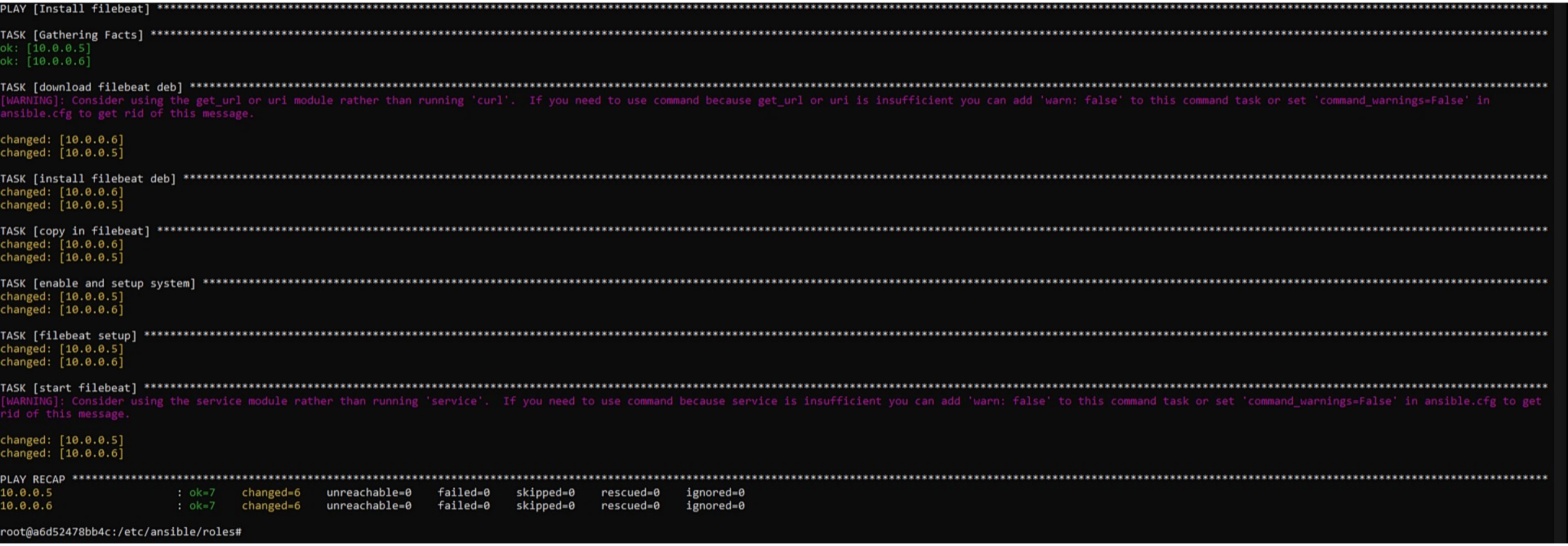
```
#============================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  host: "10.1.0.4:5601"
```



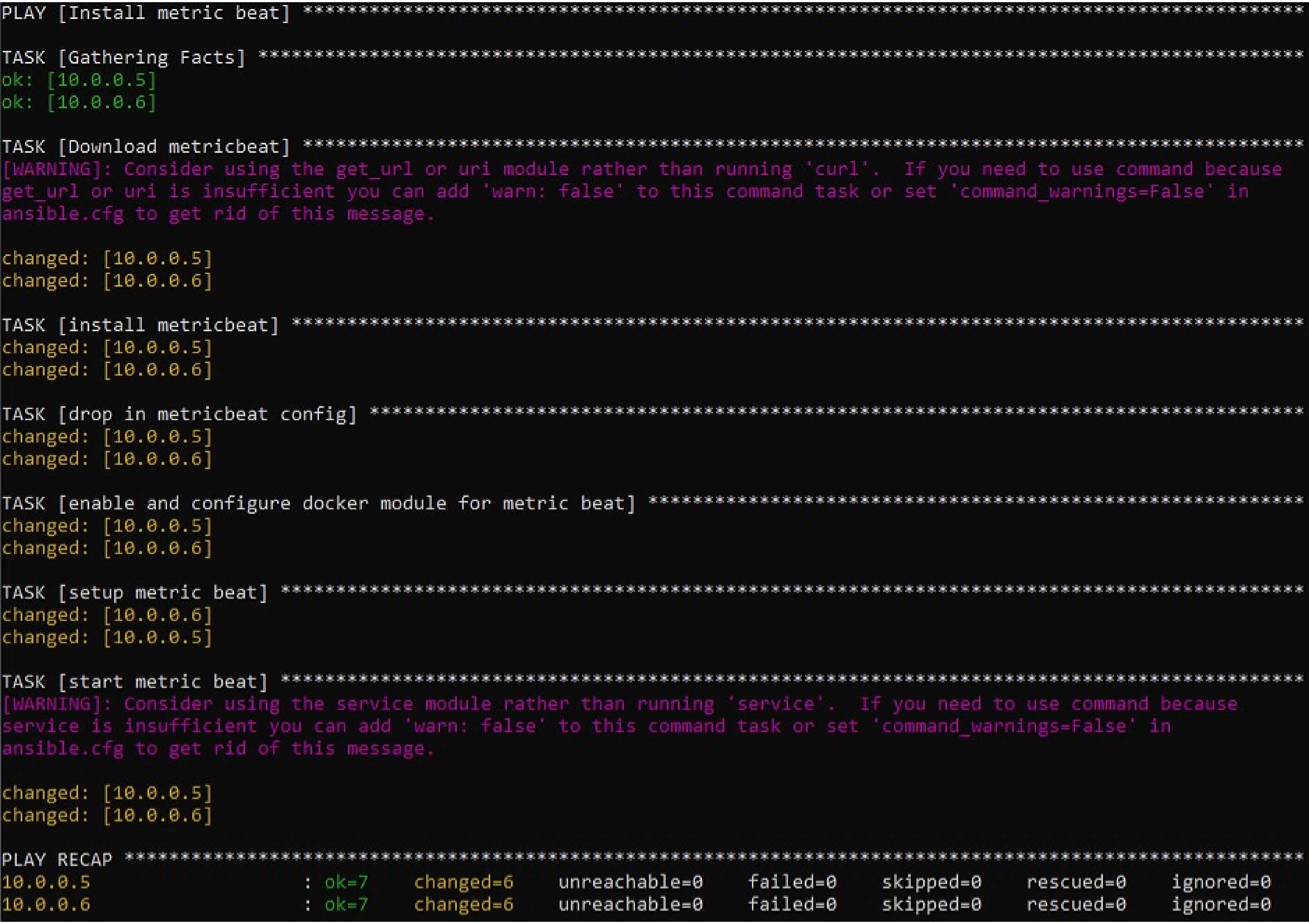
```yaml
---
- name: Install metric beat
  hosts: webservers
  become: true
  tasks:

  - name: Download metricbeat
    command: curl -L -O https://artifacts.elastic.co/downloads/beats/metricbeat/metricbeat-7.6.1-amd64.deb

  - name: install metricbeat
    command: dpkg -i metricbeat-7.6.1-amd64.deb

  - name: drop in metricbeat config
    copy:
      src: /etc/ansible/files/metricbeat-config.yml
      dest: /etc/metricbeat/metricbeat.yml

  - name: enable and configure docker module for metric beat
    command: metricbeat modules enable docker

  - name: setup metric beat
    command: metricbeat setup

  - name: start metric beat
    command: service metricbeat start
```



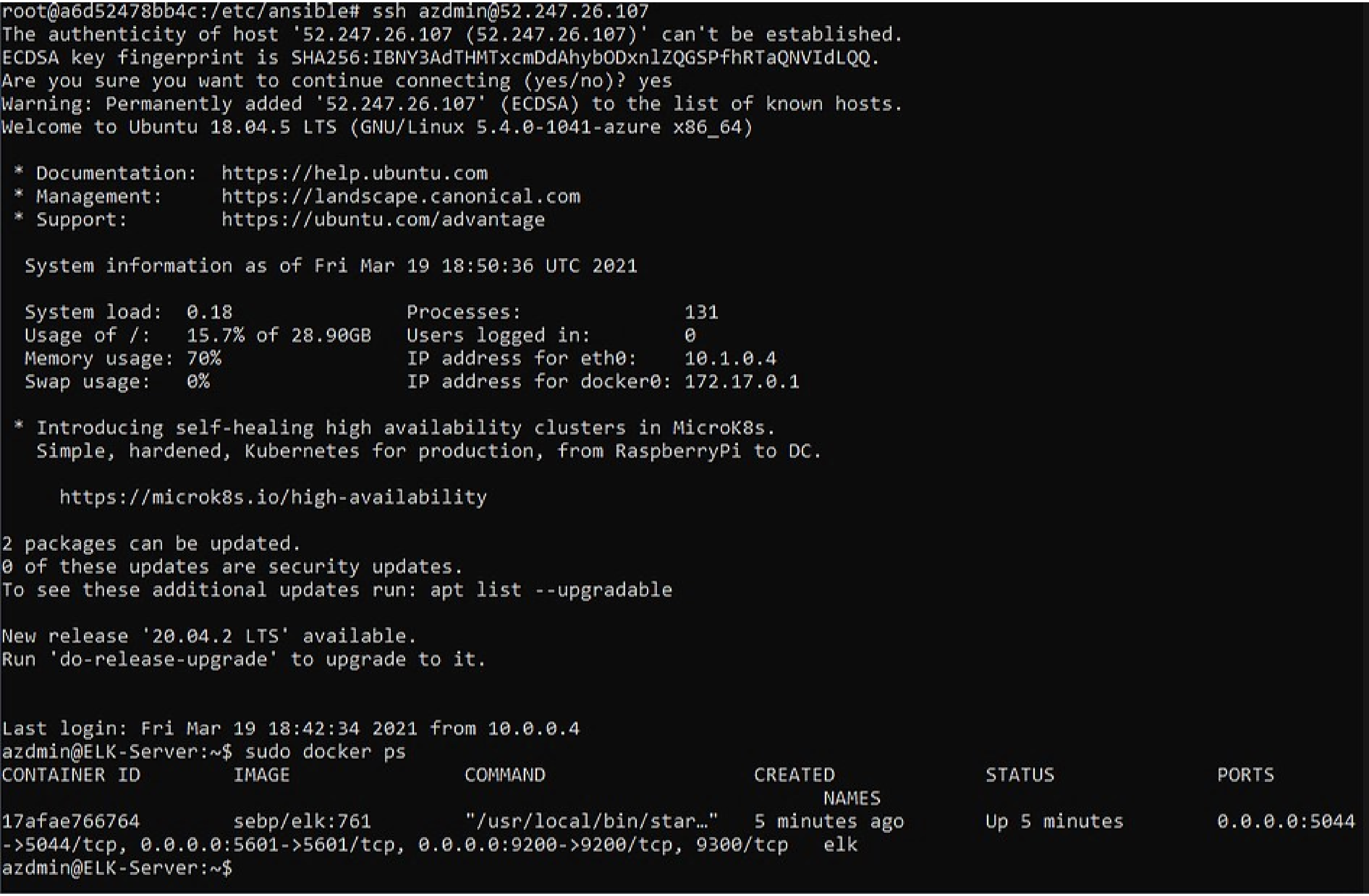
```yaml
#============================== Kibana =====================================

# Starting with Beats version 6.0.0, the dashboards are loaded via the Kibana API.
# This requires a Kibana endpoint configuration.
setup.kibana:
  host: "10.1.0.4:5601"

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

  # Kibana Space ID
  # ID of the Kibana Space into which the dashboards should be loaded. By default,
  # the Default Space will be used.
  #space.id:

#============================= Elastic Cloud ==================================

# These settings simplify using Metricbeat with the Elastic Cloud (https://cloud.elastic.co/).

# The cloud.id setting overwrites the `output.elasticsearch.hosts` and
# `setup.kibana.host` options.
# You can find the `cloud.id` in the Elastic Cloud web UI.
#cloud.id:

# The cloud.auth setting overwrites the `output.elasticsearch.username` and
# `output.elasticsearch.password` settings. The format is `<user>:<pass>`.
#cloud.auth:

#================================ Outputs =====================================

# Configure what output to use when sending the data collected by the beat.

#-------------------------- Elasticsearch output ------------------------------
output.elasticsearch:
  # Array of hosts to connect to.
  hosts: ["10.1.0.4:9200"]
  username: "elastic"
  password: "changeme"
```



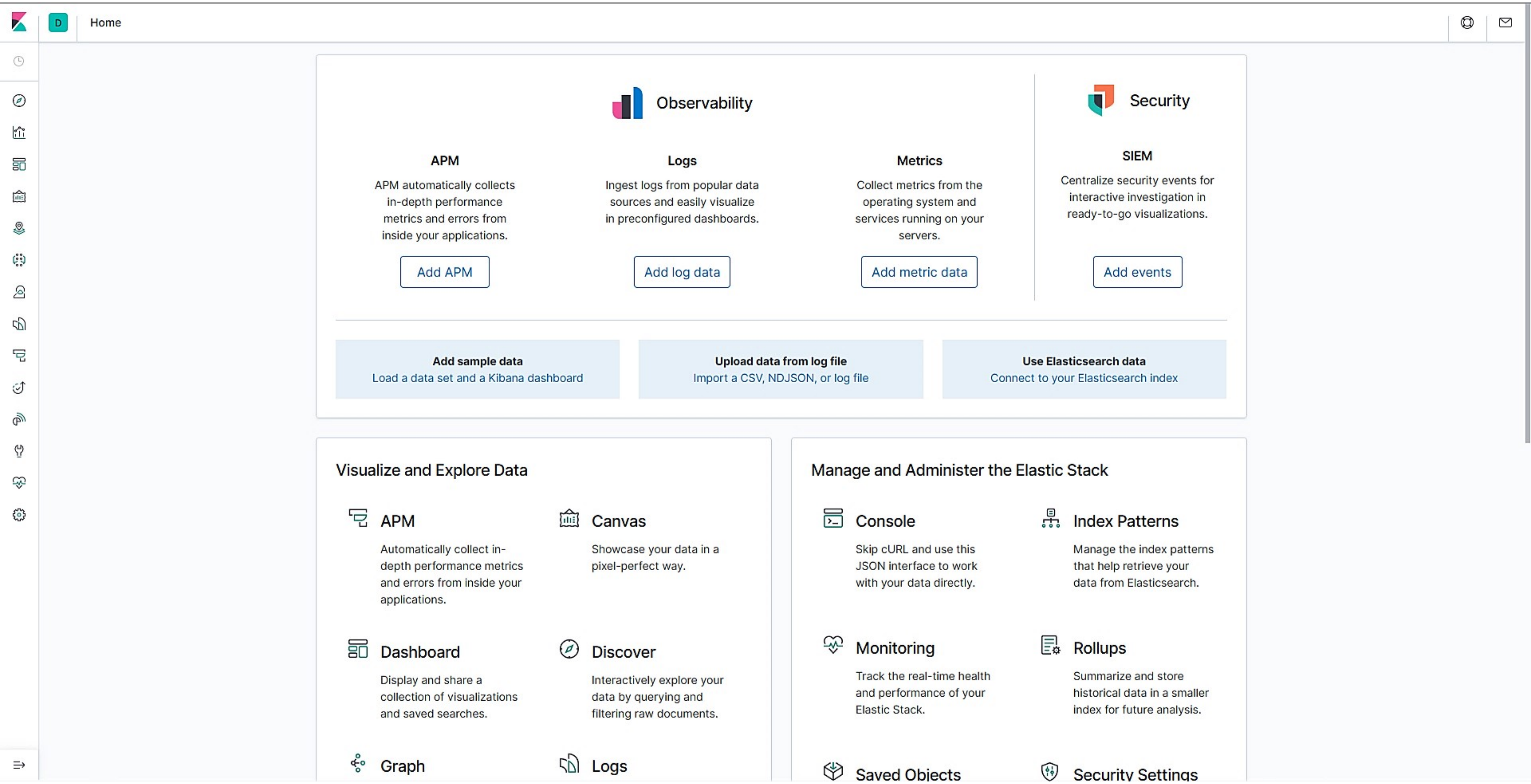
```
PLAY [Install filebeat] *********************************************************************************************************************************************************************************************************************

TASK [Gathering Facts] **********************************************************************************************************************************************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [download filebeat deb] ****************************************************************************************************************************************************************************************************************
[WARNING]: Consider using the get_url or uri module rather than running 'curl'.  If you need to use command because get_url or uri is insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in
ansible.cfg to get rid of this message.

changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [install filebeat deb] *****************************************************************************************************************************************************************************************************************
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [copy in filebeat] *********************************************************************************************************************************************************************************************************************
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [enable and setup system] **************************************************************************************************************************************************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [filebeat setup] ***********************************************************************************************************************************************************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [start filebeat] ***********************************************************************************************************************************************************************************************************************
[WARNING]: Consider using the service module rather than running 'service'.  If you need to use command because service is insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in ansible.cfg to get
rid of this message.

changed: [10.0.0.5]
changed: [10.0.0.6]

PLAY RECAP **********************************************************************************************************************************************************************************************************************************
10.0.0.5                   : ok=7    changed=6    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.6                   : ok=7    changed=6    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0

root@a6d52478bb4c:/etc/ansible/roles#
```



```
PLAY [Install metric beat] *****************************************************************************************

TASK [Gathering Facts] *********************************************************************************************
ok: [10.0.0.5]
ok: [10.0.0.6]

TASK [Download metricbeat] *****************************************************************************************
[WARNING]: Consider using the get_url or uri module rather than running 'curl'.  If you need to use command because
get_url or uri is insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in
ansible.cfg to get rid of this message.

changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [install metricbeat] ******************************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [drop in metricbeat config] ***********************************************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [enable and configure docker module for metric beat] **********************************************************
changed: [10.0.0.5]
changed: [10.0.0.6]

TASK [setup metric beat] *******************************************************************************************
changed: [10.0.0.6]
changed: [10.0.0.5]

TASK [start metric beat] *******************************************************************************************
[WARNING]: Consider using the service module rather than running 'service'.  If you need to use command because
service is insufficient you can add 'warn: false' to this command task or set 'command_warnings=False' in
ansible.cfg to get rid of this message.

changed: [10.0.0.5]
changed: [10.0.0.6]

PLAY RECAP *********************************************************************************************************
10.0.0.5                   : ok=7    changed=6    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
10.0.0.6                   : ok=7    changed=6    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```



```
root@a6d52478bb4c:/etc/ansible# ssh azdmin@52.247.26.107
The authenticity of host '52.247.26.107 (52.247.26.107)' can't be established.
ECDSA key fingerprint is SHA256:IBNY3AdTHMTxcmDdAhybODxnlZQGSPfhRTaQNVIdLQQ.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '52.247.26.107' (ECDSA) to the list of known hosts.
Welcome to Ubuntu 18.04.5 LTS (GNU/Linux 5.4.0-1041-azure x86_64)

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

  System information as of Fri Mar 19 18:50:36 UTC 2021

  System load:  0.18               Processes:              131
  Usage of /:   15.7% of 28.90GB   Users logged in:        0
  Memory usage: 70%                IP address for eth0:    10.1.0.4
  Swap usage:   0%                 IP address for docker0: 172.17.0.1

 * Introducing self-healing high availability clusters in MicroK8s.
   Simple, hardened, Kubernetes for production, from RaspberryPi to DC.

     https://microk8s.io/high-availability

2 packages can be updated.
0 of these updates are security updates.
To see these additional updates run: apt list --upgradable

New release '20.04.2 LTS' available.
Run 'do-release-upgrade' to upgrade to it.


Last login: Fri Mar 19 18:42:34 2021 from 10.0.0.4
azdmin@ELK-Server:~$ sudo docker ps
CONTAINER ID        IMAGE               COMMAND                  CREATED             STATUS              PORTS
                                                                       NAMES
17afae766764        sebp/elk:761        "/usr/local/bin/star…"   5 minutes ago       Up 5 minutes        0.0.0.0:5044
->5044/tcp, 0.0.0.0:5601->5601/tcp, 0.0.0.0:9200->9200/tcp, 9300/tcp   elk
azdmin@ELK-Server:~$
```



Observability

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Logs

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Metrics

Collect metrics from the operating system and services running on your servers.

Security

SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

Visualize and Explore Data

APM

Automatically collect in-depth performance metrics and errors from inside your applications.

Canvas

Showcase your data in a pixel-perfect way.

Dashboard

Display and share a collection of visualizations and saved searches.

Discover

Interactively explore your data by querying and filtering raw documents.

Graph

Logs

Manage and Administer the Elastic Stack

Console

Skip cURL and use this JSON interface to work with your data directly.

Index Patterns

Manage the index patterns that help retrieve your data from Elasticsearch.

Monitoring

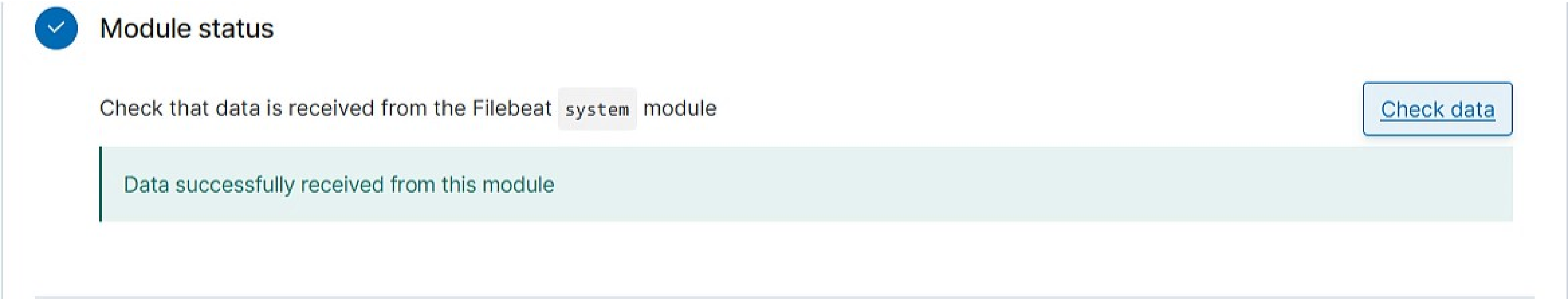
Track the real-time health and performance of your Elastic Stack.

Rollups

Summarize and store historical data in a smaller index for future analysis.

Saved Objects

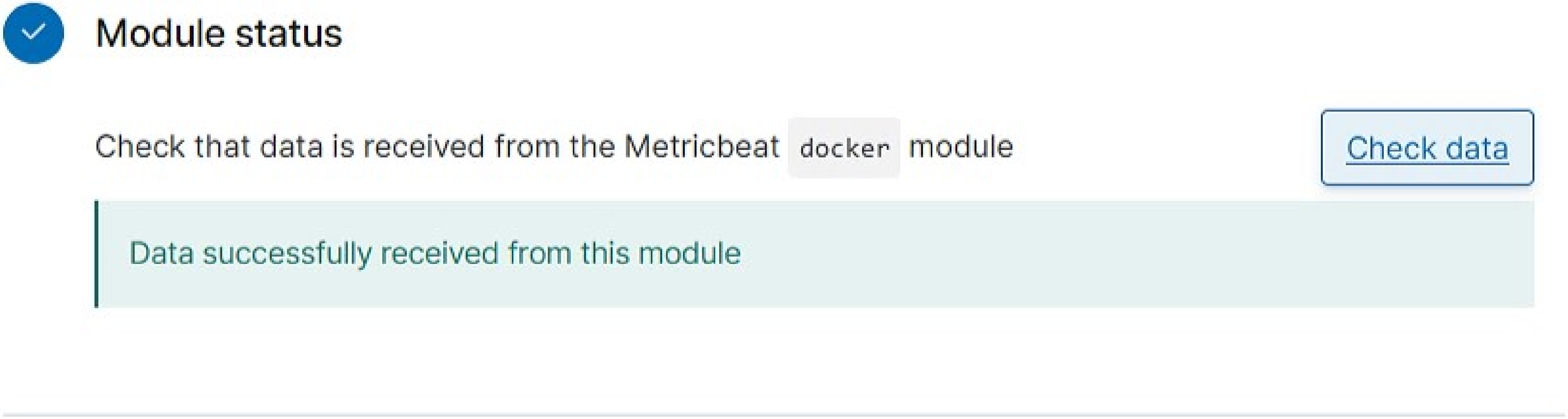
Security Settings



Module status

Check that data is received from the Filebeat `system` module

Data successfully received from this module



Module status

Check that data is received from the Metricbeat `docker` module

Data successfully received from this module