X-Pack: Alerting

1. Configuring Metricbeat

```
metricbeat.modules:
    - module: system
        metricsets:
            - cpu # CPU stats
            - core # Per CPU core stats
            - diskio # IO stats
            - filesystem # Per filesystem stats
            - fsstat # File system summary stats
            - load # System load stats
            - memory # Memory stats
            - network # Network stats
            - process # Per process stats
            - socket # Sockets (linux only)
        enabled: true
        period: 10s # can be changed
        processes: ['.*']
        cpu_ticks: false
output.elasticsearch:
    hosts: ["localhost:9200"] # can be changed
    username: "<username>"
    password: "<password>"
```

2. Configuring Elasticsearch

```
xpack.notification.slack:
  account:
    monitoring:
      url: <your-slack-webhook-url>
xpack.notification.email.account:
    gmail_account:
        profile: gmail
        smtp:
            auth: true
            starttls.enable: true
            host: smtp.gmail.com
            port: 587
            user: <username>@<domainname>
            password: <password>
```

3. Getting started with X-Pack: Alerting

- Add your credentials in `configure-alerts.sh` .
- In JSON files of the provided watches, configure the following:
  - **email**: the address to which you want the alerts to be sent
  - **slack**: channel name and username
- Start Elasticsearch.
- Start Metricbeat.
- Execute `bash configure-alerts.sh` .