Elk Stack - Syslogüberwachung

Der ELK Stack ist ein mächtiges Trio aus Open-Source-Projekten: Elasticsearch, Logstash und Kibana. Elasticsearch ist ein skalierbares Such- und Analyse-Engine für komplexe Abfragen in Echtzeit. Logstash sammelt und transformiert Daten, bereitet sie für Elasticsearch auf. Kibana visualisiert diese Daten, bietet interaktive Dashboards für eingehende Erkenntnisse. Zusammen bilden sie den ELK Stack - eine umfassende Lösung für die Echtzeit-Datenanalyse.

Installation

Installation unter Debian Bullseye

Beschreibung:

Installations von Elkstack unter Debian Bullseye.
Dies sind 3 Komponenten

- **Elasticsearch**
- **Kibana**
- **Logstash**
- **Optional Filebeat,**
  (wird benötigt wenn nicht über ssh auf die server zugegriffen werden soll.
  Eigentlich ist filebeat die Standardvariante, aber in restrikten Netzen geht halt nur ssh.)

Installation

Java Installation

Elastisearch und Logstash benötigen Java

```
apt update
apt install default-jdk gnupgp gnupgp2 curl net-tools
```

IPv6 deaktivieren

Dazu

```
nano nano /etc/sysctl.conf
```

Am Ende hinzufügen

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
```

```
net.ipv6.conf.lo.disable_ipv6 = 1
```

Nun anwenden

```
systmctl -p
```

Nun reboot

```
reboot
```

Elasticsearch installation

Elastisearch repo und Keys hinzufügen
Auf dieser Seite schauen ob es eine neue Version gibt.
zur Erstellungszeit des Artikels war es die Version 8

https://www.elastic.co/guide/en/elasticsearch/reference/current/deb.html

```
wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | apt-key add -
echo "deb https://artifacts.elastic.co/packages/8.x/apt stable main" | tee /etc/apt/sources.list.d/elastic-8.x.list
```

Dann Paketdatenbank aktualisieren und Paket installieren

```
apt update
apt install elasticsearch
```

beim Systemstart aktivieren und starten

```
systemctl enable elasticsearch
systemctl start elasticsearch
```

Nun noch Kennwort für die Elastic oberfläche festlegen

```
bash /usr/share/elasticsearch/bin/elasticsearch-reset-password interactive -u elastic


Nun wir ein neues Kennwort ausgeben.
Damit kann isch dann später angemeldet werden.
```

Ausgabe:

```
This tool will reset the password of the [elastic] user to an autogenerated value.
The password will be printed in the console.
```

```
Please confirm that you would like to continue [y/N]y


Password for the [elastic] user successfully reset.
New value: =7-xan*******
```

Installation Kibana

Kibana wird aus dem gleichen Repository installiert.
Also direkt eingeben, installieren.

```
apt install kibana
```

Nun die config bearbeiten, damit Kibana auf dem Interface lauscht.
Standard ist nämlich nur localhost

```
nano /etc/kibana/kibana.yml
```

Dort die Zeile hinzufügen

```
server.host: "0.0.0.0"
```

Beim Systemstart aktivieren und gleich starten

```
systemctl enable kibana
systemctl start kibana
```

Installation Logstash

Logstash wird aus dem gleichen Repository installiert.
Also direkt eingeben, installieren

```
apt install logstash
```

Nun die Konfig erstellen dazu öffnen wir

```
nano /etc/logstash/conf.d/logstash.conf
```

Folgender Inhalt:
Password für den Elastic user anpassen (wurde zuvor in der Console ausgeben) und den path anpassen wenn gewünscht wir lassen diesen path aber so.

in den Path werden alle Logdateioen gesammelt, ausreichend großes Volume oder ein cephfs was erweitert werden kann ;-)

```
input {
  file {
    path => "/var/log/syslog-copies/*"
    start_position => "beginning"
    sincedb_path => "/var/log/syslog-copies/sincedb"
  }
}

output {
  elasticsearch {
  ssl => true
    ssl_certificate_verification => false
    cacert => "/etc/elasticsearch/certs/http_ca.crt"
    hosts => ["localhost:9200"]
    user => "elastic"
    password => "1234567890"
    index => "syslog-%{+YYYY.MM.dd}"
  }
}
```

Nun noch das Verzeichnius unter path anlegen, hier bei uns

```
mkdir -p /var/log/syslog-copies/
```

beim Systemstart aktivieren und starten

```
systemctl enable logstash
systemctl start logstash
```

Ohne Filebeat Syslogs per SSH abholen, wenn Filebeat verwendet dann überspringen und bei Installation Filebeat weitermachen

ein sh Skript anlegen

```
nano /root/getsyslog.sh
```

Inhalt:
Diese Skript kopiert die Syslogs von den Servern in Unterverzeichnisse der mit den Namen der IPs in das Syslogserver Verzeichnis.
Möchte man einen speziellen Benutzer auf dem Zielsystem haben das nur logs lesen kann, dann in dem script den Benutzernamen anpassen, das heißt root durch einen anderen Namen ersetzen z.b elkstack. Die Benutzereinrichtung findest sich weiter unten, als Optional markiert.

```
#!/bin/bash
TARGET_DIR="/var/log/syslog-copies"

SERVERS=("192.168.178.101" "192.168.178.102")

for server in ${SERVERS[@]}
do
  if [ ! -d "$$TARGET_DIR/syslog-$server" ]; then
    mkdir -p $TARGET_DIR/syslog-$server/
  fi

  scp root@$server:/var/log/syslog $TARGET_DIR/syslog-$server/
  #Hier können weitere Log Dateien angefügt werden zum Beispiel ssh logins
  scp root@$server:/var/log/auth.log $TARGET_DIR/syslog-$server/
done
chown -R logstash. $TARGET_DIR/
```

Dann noch das Skript ausführbar machen

```
chmod +x /root/getsyslog.sh
```

Nun per crontab -e das skript hinzufügen damit es jede 5 Minuten läuft

```
*/5 * * * * /root/getsyslog.sh
```

Damit das klappt muss der elkstack Server sich via Schlüsseldatei verbinden können.

Auf dem Elkstackserver ssh key erstellen, wenn nicht schon getan

```
ssh-keygen -t rsa -b 4096
```

Nun per ssh-copy id die den Schlüssel auf die zu überwachenden Server kopieren.

Optional, einen Benutzer nur für log lesen, mit den Namen elkstack und der gruppe logreaders auf dem zu Überwachenden Server einrichten.

```
adduser elkstack
```

Nun eine Gruppe erstellen, z.b logreaders. Dies wird eine Gruppe die nur Logs lesen darf.

```
groupadd logreaders
```

Nun den Benutzer der Gruppe hinzufügen.

```
usermod -aG logreaders elkstack
```

Nun der Gruppe logreaders rechte auf das /var/log Verzeichnis geben

```
setfacl -Rm g:logreaders:rx /var/log
```

(Nur bei Endian Systemen, muss in der SSH Config /etc/ssh/sshd_config der Benutzer nochmals elkstack explizit eingetragen werden.
Sonst ist keine Anmeldung möglich, trotz Schlüssel)

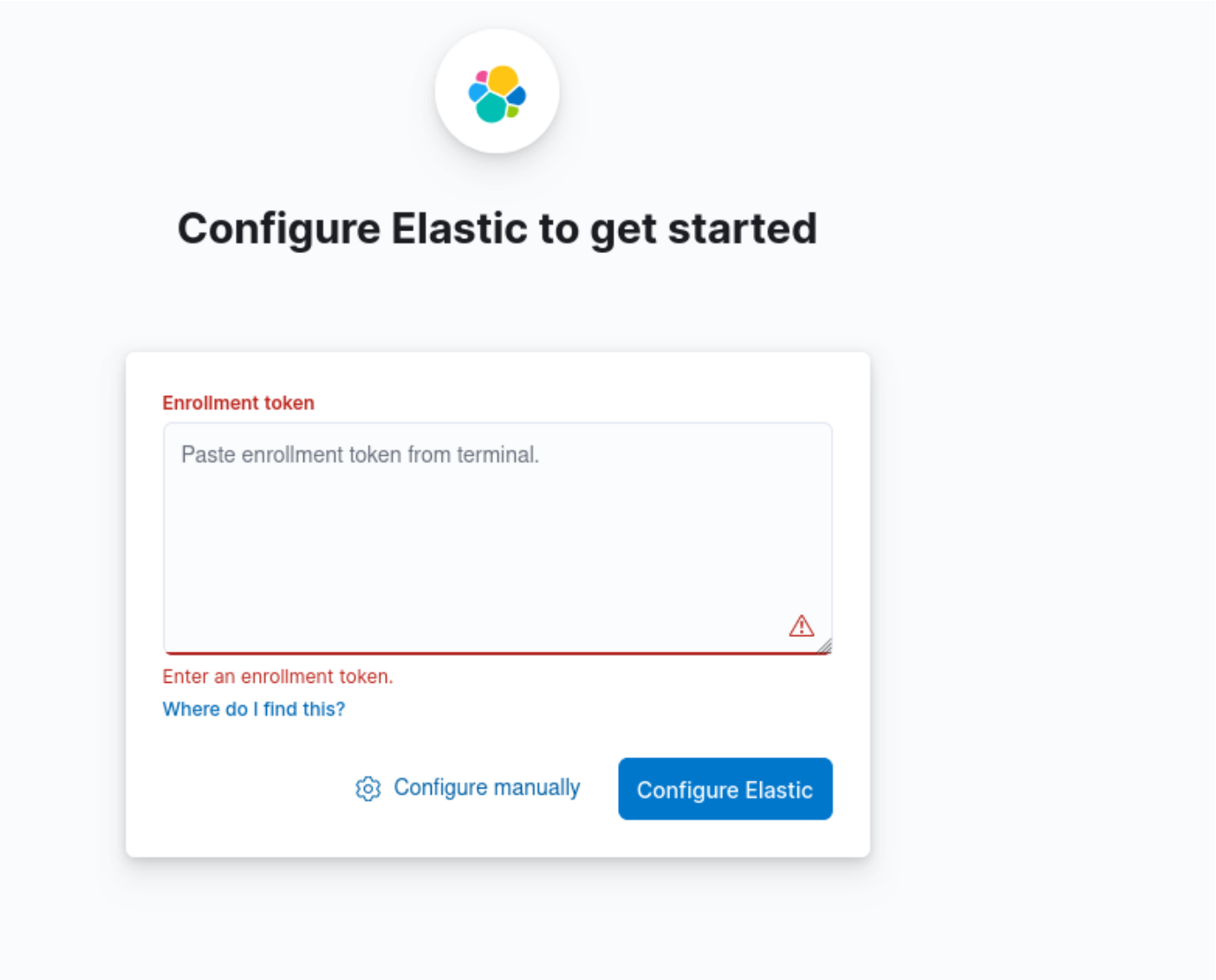
```
...
AllowUsers root support provisioning elkstack
...
```

Installation Filebeat, kann übersprungen werden, wenn SSH benutzt wurde.

ss

Aufrufen der Oberfläche Kibana

Unter http://ip-hostname-elkstack:5601/ kann die Oberfläche aufgerufen werden.
beim ersten Start kommt der Willkommensbildschirm und die Abfrage eines Keys für Elsaticsearch. Denn Kibana greift ja auf elasticsearch zu.



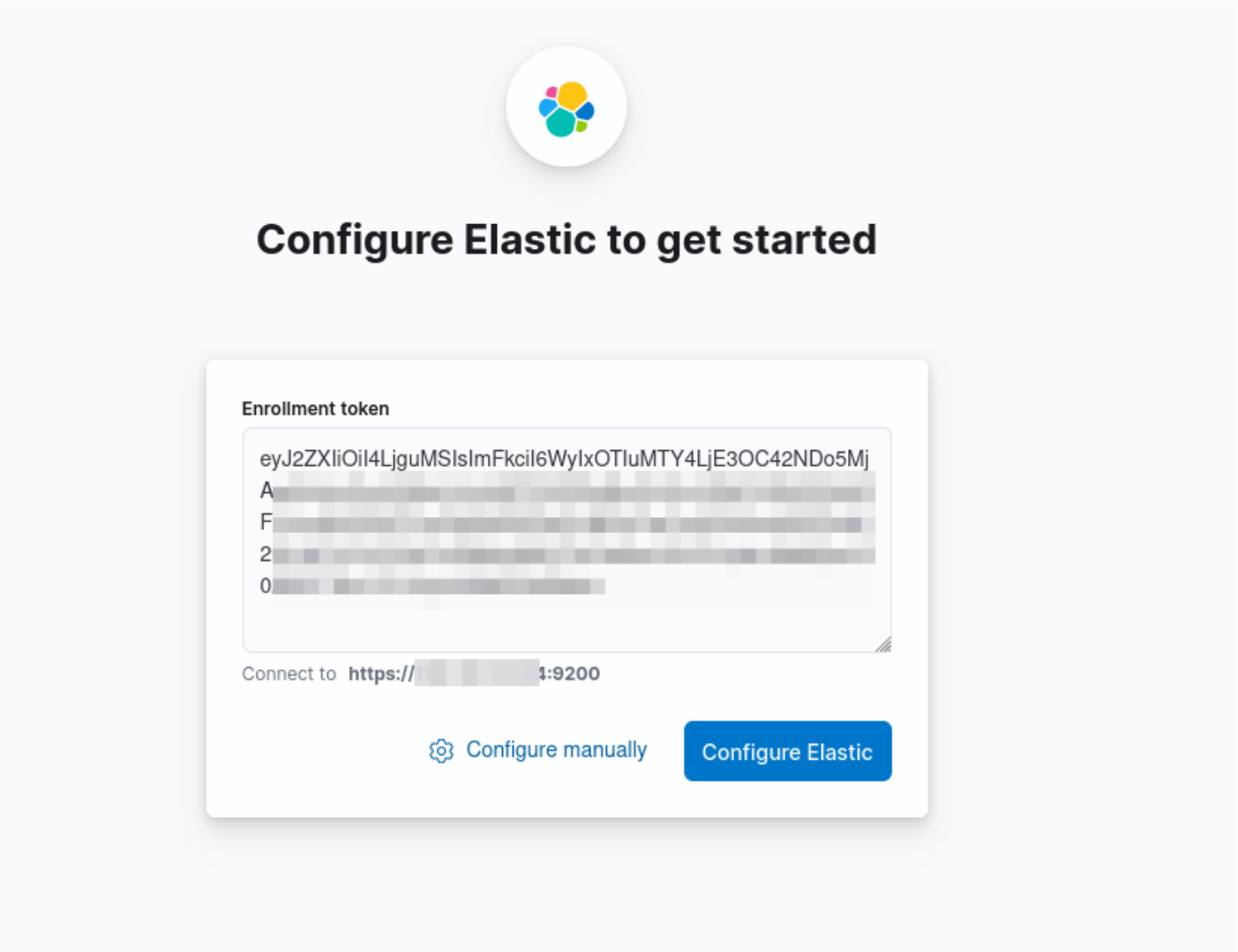
Diesen Key holen wir uns aus dem Terminal mittels:

```
bash /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token --scope kibana
```

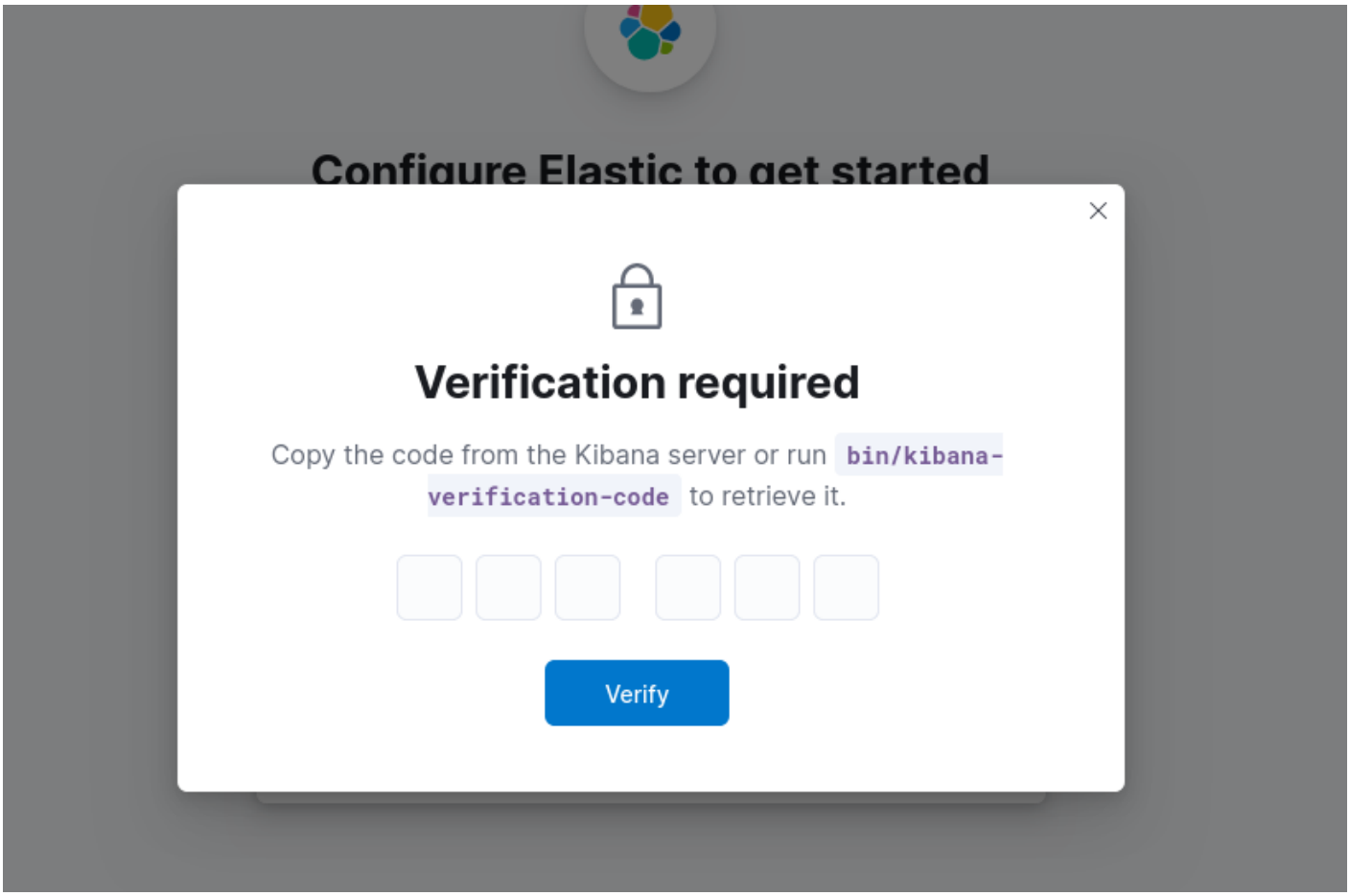
Ausgabe:

```
eyJ2ZXIiOiI4LjguMSIsImFkciI6WyIxOTIuMTY4LjE3**********************************************************************
**********DZiNzZhMDJjZmQxNGI2NmM5ZDdiM2Q1NjYiLCJrZXkiOiJWMmM5bTRnQkNncGZnZ21pdnNsMDpsYll0ZlRCTlRvYTlYS1pUVlNDZ3NRIn0=
root@elkstack:/#
```

Diesen Token kopieren und auf der Weboberfläche einfügen und auf configure Elastic klicken.



Nun muss ein Verifierzungscode eingeben werden.



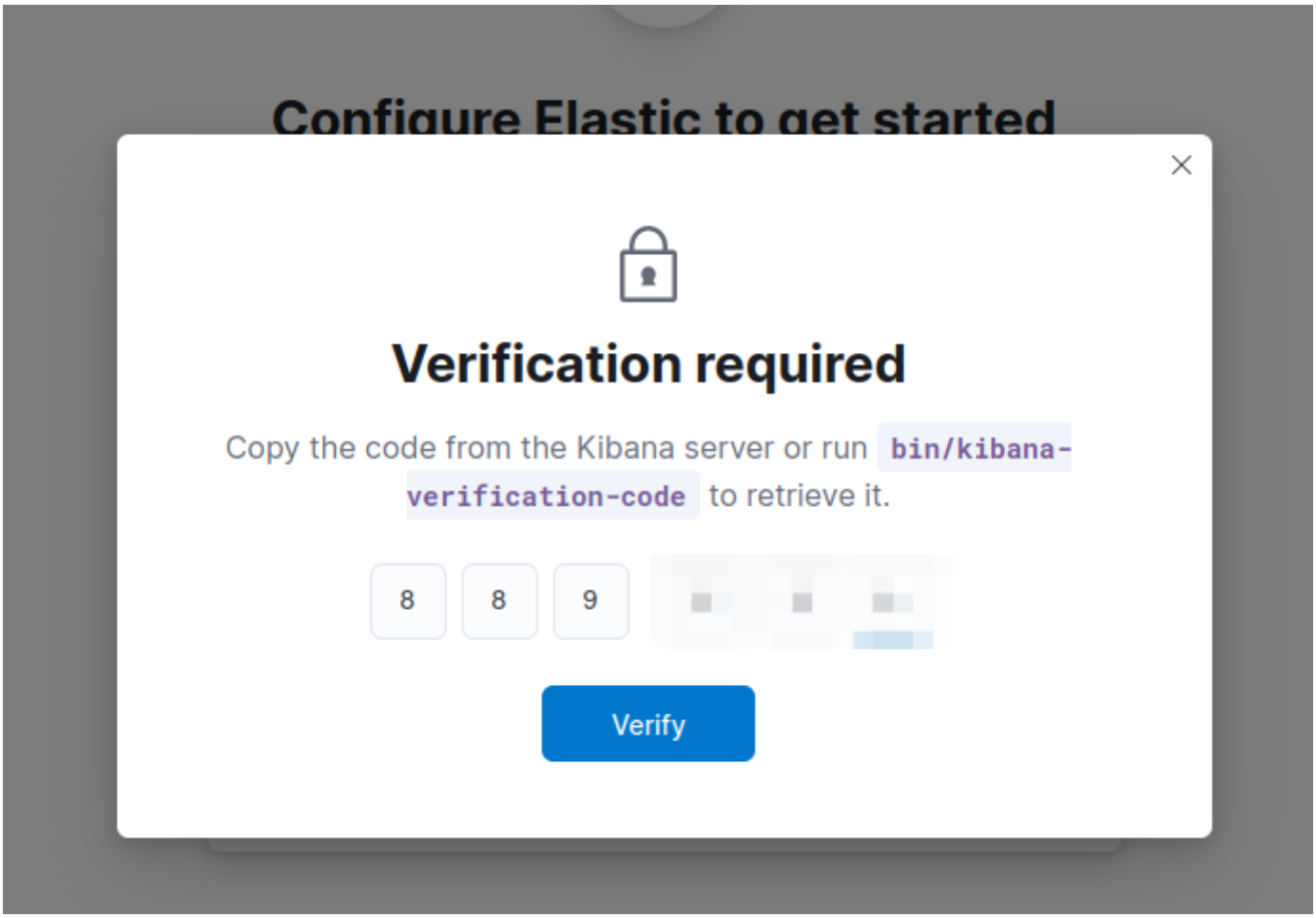
Diesen holen wir uns auch wieder ausm Terminal

```
bash /usr/share/kibana/bin/kibana-verification-code
```

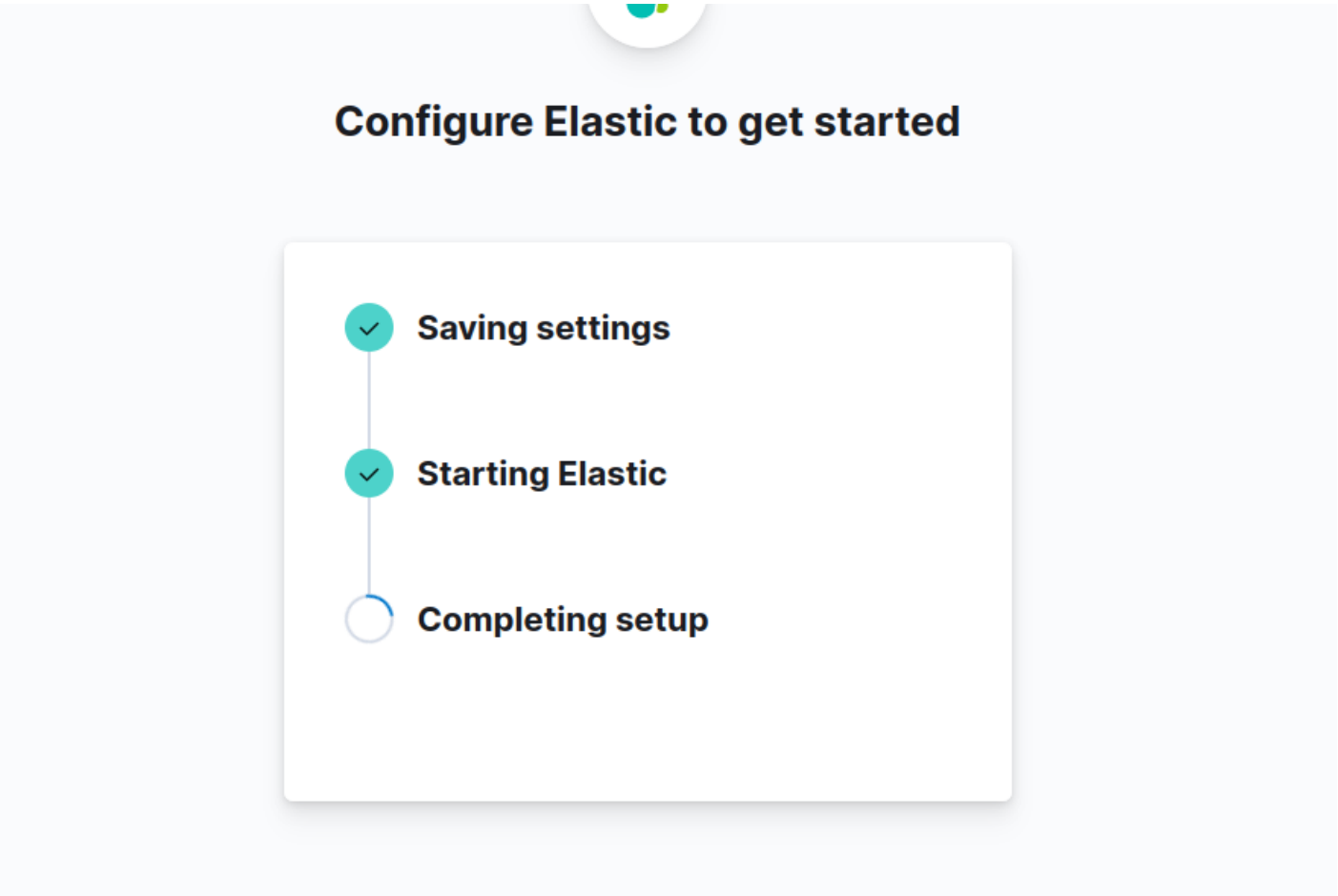
Ausgabe:

```
root@elkstack:/# bash /usr/share/kibana/bin/kibana-verification-code
Your verification code is:  889 ***
root@elkstack:/#
```

nun den Code auf der Website eingeben

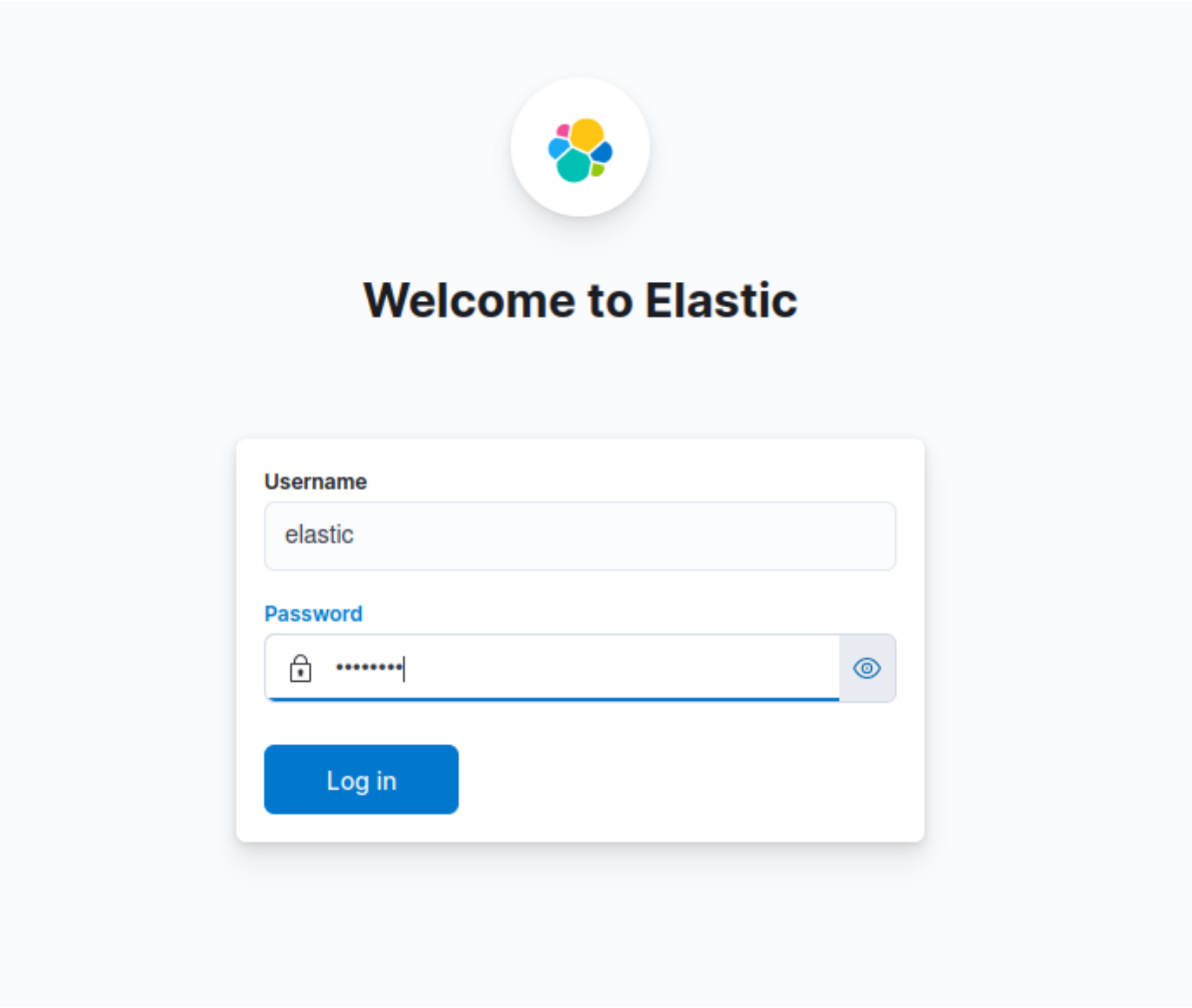


Nun abwarten

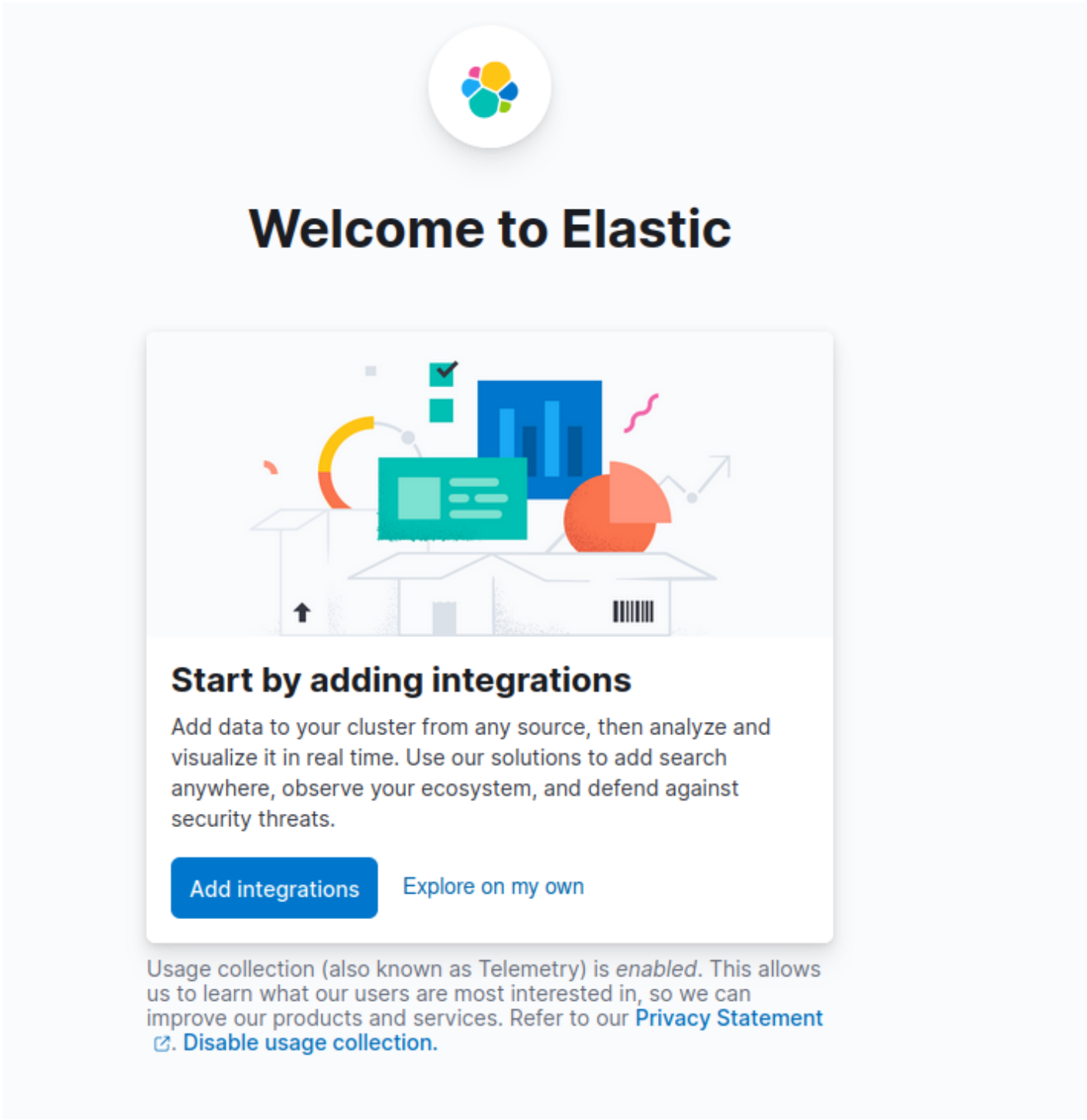


Nun der Loginscreen

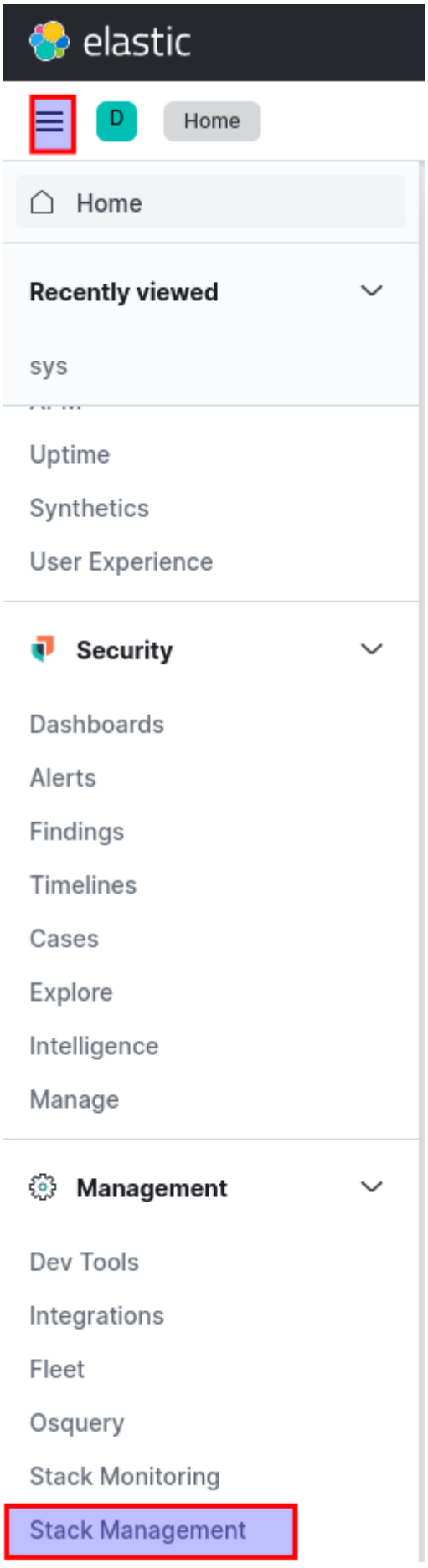
Benutzername : elastic
Kennwort : Das Password aus dem Reset.



Nun sind wir im Login Screen und gehen Explore my Own



Nun auf das Burgermenü und dann ganz untel Stack Managment anklicken


elastic
D
Home
Home
Recently viewed
sys
Uptime
Synthetics
User Experience
Security
Dashboards
Alerts
Findings
Timelines
Cases
Explore
Intelligence
Manage
Management
Dev Tools
Integrations
Fleet
Osquery
Stack Monitoring
Stack Management

IP-Adresse ändern. Sollte sich die IP vom Host ändern muss sie an folgenden stellen angepasst werden

Fehler

Kibana server is not ready yet. Wenn die Weboberfläche aufgerufen wird.

Meistens tritt dieser Fehler bei Fehlkonfiguration von den ips in den Konfigdateien.
Meist nach einem IP-Wechsel.

Dazu schauen wir in die LOG

Installation unter Cent OS 8

Beschreibung:

Installations von Elkstack unter Cent OS 8.
Dies sind 3 Komponenten

- **Elasticsearch**
- **Kibana**
- **Logstash**
- **Optional Filebeat,**
  (wird benötigt wenn nicht über ssh auf die server zugegriffen werden soll.
  Eigentlich ist filebeat die Standardvariante, aber in restrikten Netzen geht halt nur ssh.)

Installation

Java Installation

Elastisearch und Logstash benötigen Java

```
yum update
dnf install java-11-openjdk-devel curl net-tools
```

IPv6 deaktivieren

Dazu

```
nano /etc/sysctl.d/99-sysctl.conf
```

Am Ende hinzufügen

```
net.ipv6.conf.all.disable_ipv6 = 1
net.ipv6.conf.default.disable_ipv6 = 1
net.ipv6.conf.lo.disable_ipv6 = 1
```

Nun anwenden

```
systmctl -p
```

Nun reboot

```
reboot
```

Firewall anpassen

```
firewall-cmd --add-port=5601/tcp --permanent
firewall-cmd --add-port=9200/tcp --permanent
firewall-cmd --add-port=5044/tcp --permanent
firewall-cmd --reload
```

Elasticsearch installation

Elastisearch repo und Keys hinzufügen
Auf dieser Seite schauen ob es eine neue Version gibt.
zur Erstellungszeit des Artikels war es die Version 8

https://www.elastic.co/guide/en/elasticsearch/reference/current/rpm.html

```
rpm --import https://artifacts.elastic.co/GPG-KEY-elasticsearch
```

Nun eine Repo File erstellen

```
nano /etc/yum.repos.d/elasticsearch.repo
```

Inhalt

```
[elasticsearch]
name=Elasticsearch repository for 8.x packages
baseurl=https://artifacts.elastic.co/packages/8.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=0
autorefresh=1
type=rpm-md
```

Dann Repo aktivieren und Paket installieren

```
dnf install --enablerepo=elasticsearch elasticsearch
```

beim Systemstart aktivieren und starten

```
systemctl enable elasticsearch
systemctl start elasticsearch
```

Nun noch Kennwort für die Elastic oberfläche festlegen

```
bash /usr/share/elasticsearch/bin/elasticsearch-reset-password interactive -u elastic


Nun wird ein neues Kennwort ausgeben.
Damit kann isch dann später angemeldet werden.
```

Ausgabe:

```
This tool will reset the password of the [elastic] user to an autogenerated value.
The password will be printed in the console.
Please confirm that you would like to continue [y/N]y



Password for the [elastic] user successfully reset.
New value: =7-xan*******
```

Elastic search Proxy konfigurieren (optional, halt wenn ein proxy benötigt wird)

Dazu editireren wir die Java Datei zu Elasticsearch

```
nano /etc/elasticsearch/jvm.options
```

Nun folgene Zeilen hinzufügen und den Proxy anpassen

```
-Dhttp.proxyHost=proxyserver
-Dhttp.proxyPort=8080
-Dhttps.proxyHost=proxyserver
-Dhttps.proxyPort=8080
```

Nun den Dienst neustarten

```
service elasticsearch restart
```

Installation Kibana

https://www.elastic.co/guide/en/kibana/current/rpm.html

Also direkt eingeben, installieren.
Repo Datei erstellen

```
nano /etc/yum.repos.d/kibana.repo
```

Inhalt

```
[kibana-8.x]
name=Kibana repository for 8.x packages
baseurl=https://artifacts.elastic.co/packages/8.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Nun das Paket installieren

```
dnf install kibana
```

Nun die config bearbeiten, damit Kibana auf dem Interface lauscht.
Standard ist nämlich nur localhost

```
nano /etc/kibana/kibana.yml
```

Dort die Zeile hinzufügen

```
server.host: "0.0.0.0"
```

Beim Systemstart aktivieren und gleich starten

```
systemctl enable kibana
systemctl start kibana
```

Kibana Proxy konfigurieren (Optional nur wenn proxy benötigt wird)

Wenn ein proxy benötigt wird.
Die umgebungsvariablen im Service setzen

Dazu die Service File öffnen

```
nano /usr/lib/systemd/system/kibana.service
```

Dort im Bereich [Service] folgenden zeilen hinzufügen und den proxy natürlich anpassen

```
Environment=HTTP_PROXY=http://proxyserver:8080
Environment=HTTPS_PROXY=http://proxyserver:8080
```

Danach systemctl reloaden und Kibana neustarten

```
systemctl daemon-reload
service kibana restart
```

Installation Logstash

Repo Datei erstellen

```
nano /etc/yum.repos.d/logstash.repo
```

Inhalt

```
[logstash-8.x]
name=Elastic repository for 8.x packages
baseurl=https://artifacts.elastic.co/packages/8.x/yum
gpgcheck=1
gpgkey=https://artifacts.elastic.co/GPG-KEY-elasticsearch
enabled=1
autorefresh=1
type=rpm-md
```

Nun das Paket installieren

```
dnf install logstash
```

Nun die Konfig erstellen dazu öffnen wir

```
nano /etc/logstash/conf.d/logstash.conf
```

Folgender Inhalt:
Password für den Elastic user anpassen (wurde zuvor in der Console ausgeben) und den path anpassen wenn gewünscht wir lassen diesen path aber so.
in den Path werden alle Logdateioen gesammelt, ausreichend großes Volume oder ein cephfs was erweitert werden kann ;-)

```
input {
  file {
    path => "/var/log/syslog-copies/*"
    start_position => "beginning"
    sincedb_path => "/var/log/syslog-copies/sincedb
  }
}

output {
  elasticsearch {
  ssl => true
    ssl_certificate_verification => false
    cacert => "/etc/elasticsearch/certs/http_ca.crt"
    hosts => ["localhost:9200"]
    user => "elastic"
    password => "1234567890"
    index => "syslog-%{+YYYY.MM.dd}"
  }
}
```

Nun noch das Verzeichnius unter path anlegen, hier bei uns

```
mkdir -p /var/log/syslog-copies/
```

beim Systemstart aktivieren und starten

```
systemctl enable logstash
systemctl start logstash
```

Ohne Filebeat Syslogs per SSH abholen, wenn Filebeat verwendet dann überspringen und bei Installation Filebeat weitermachen

ein sh Skript anlegen

```
nano /root/getsyslog.sh
```

Inhalt:
Diese Skript kopiert die Syslogs von den Servern in Unterverzeichnisse der mit den Namen der IPs in das Syslogserver Verzeichnis.

```
#!/bin/bash
TARGET_DIR="/var/log/syslog-copies"

SERVERS=("192.168.178.101" "192.168.178.102")

for server in ${SERVERS[@]}
do
  scp root@$server:/var/log/syslog $TARGET_DIR/syslog-$server
  #Hier können weitere Log Dateien angefügt werden zum Beispiel ssh logins
  scp root@$server:/var/log/auth.log $TARGET_DIR/syslog-$server
done
chown -R logstash. $TARGET_DIR
```

Dann noch das Skript ausführbar machen

```
chmod +x /root/getsyslog.sh
```

Damit das klappt muss der elkstack Server sich via Schlüsseldatei verbinden können.

Auf dem Elkstackserver ssh key erstellen, wenn nicht schon getan

```
ssh-keygen -t ecdsa
```

Nun per ssh-copy id die den Schlüssel auf die zu überwachenden Server kopieren.
Nun per crontab -e das skript hinzufügen damit es jede 5 Minuten läuft

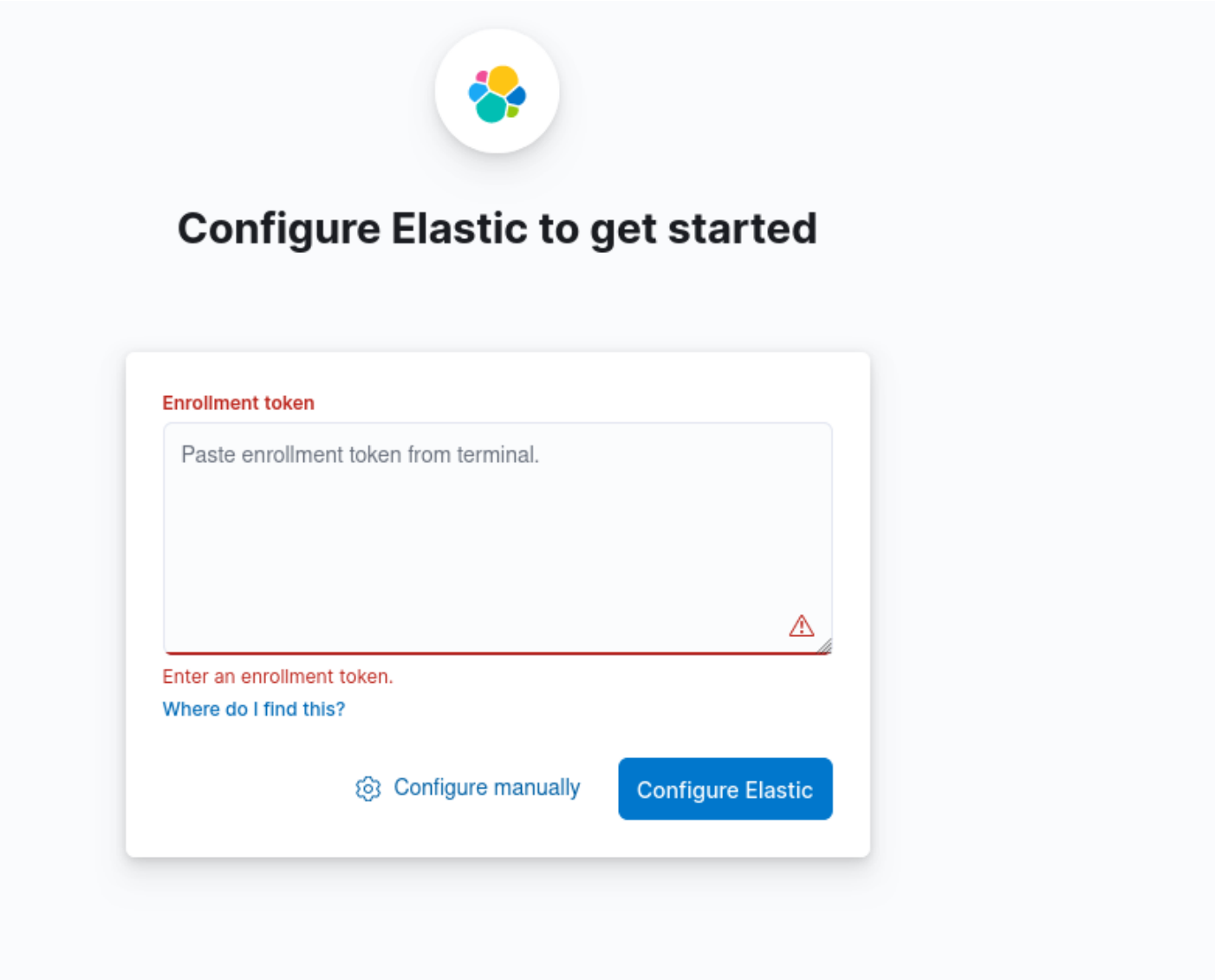
```
*/5 * * * * /root/getsyslog.sh
```

Installation Filebeat, kann übersprungen werden, wenn SSH benutzt wurde.

ss

Aufrufen der Oberfläche Kibana

Unter http://ip-hostname-elkstack:5601/ kann die Oberfläche aufgerufen werden.
beim ersten Start kommt der Willkommensbildschirm und die Abfrage eines Keys für Elsaticsearch.
Denn Kibana greift ja auf elasticsearch zu.



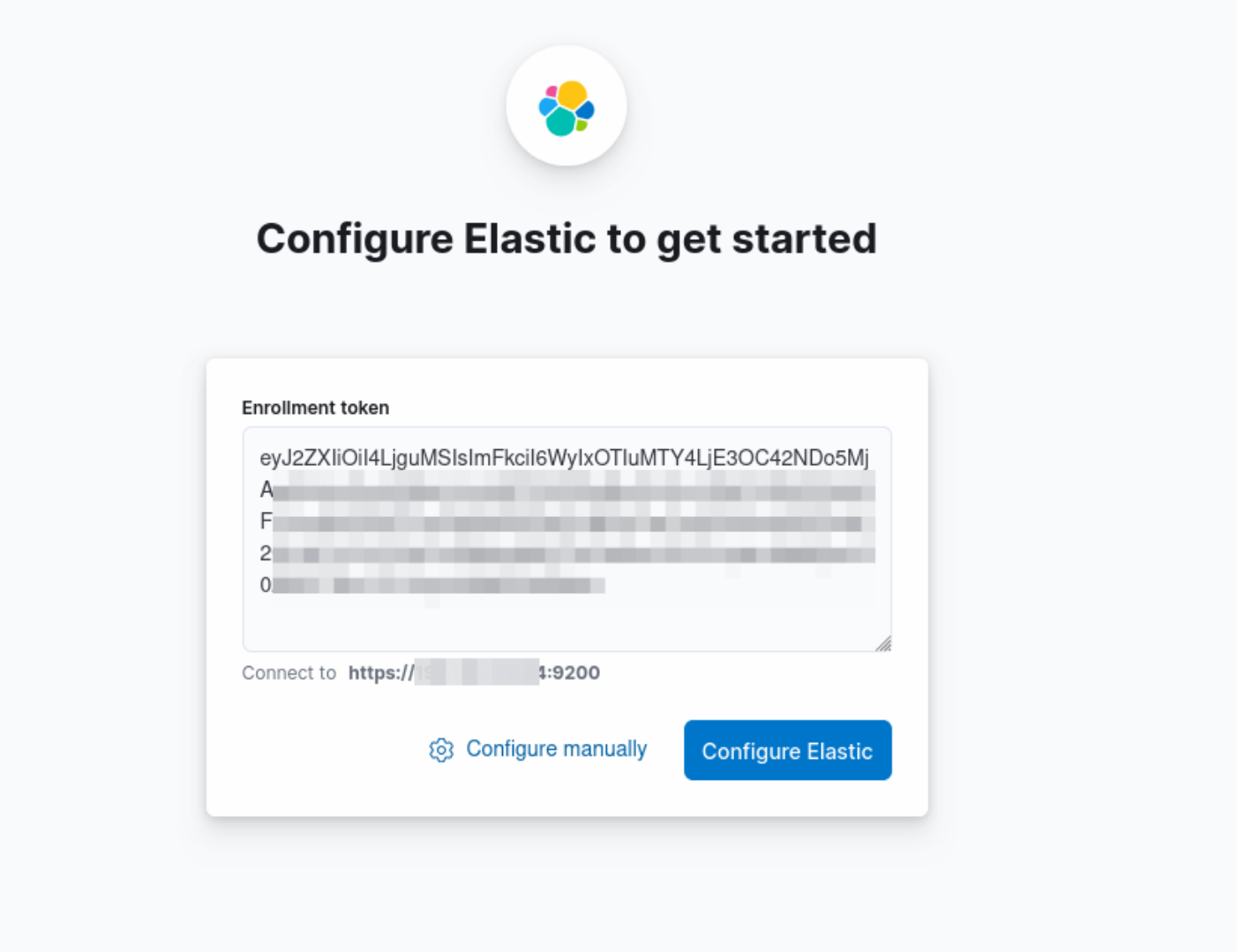
Diesen Key holen wir uns aus dem Terminal mittels:

```
bash /usr/share/elasticsearch/bin/elasticsearch-create-enrollment-token --scope kibana
```

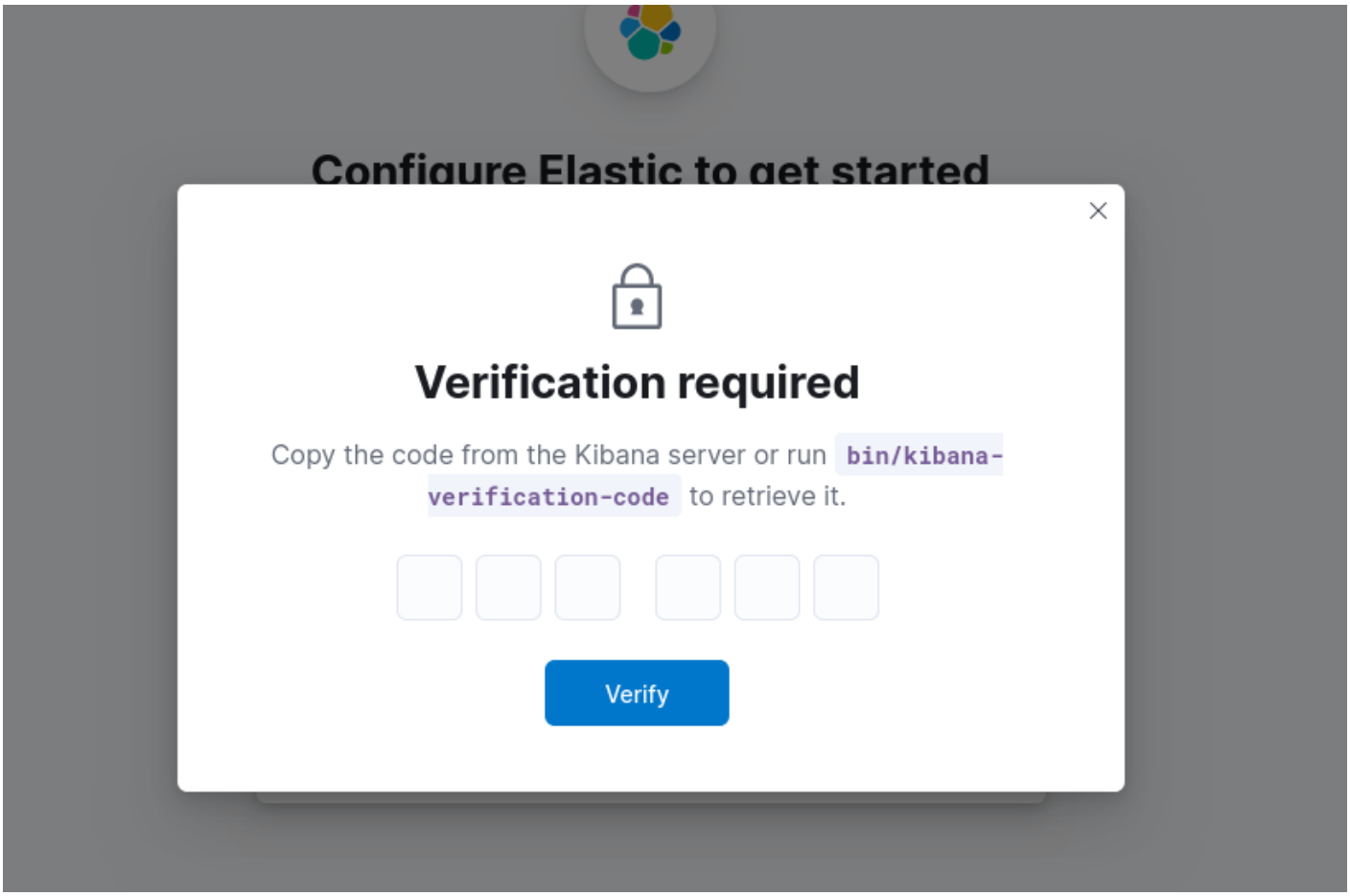
Ausgabe:

```
eyJ2ZXIiOiI4LjguMSIsImFkciI6WyIxOTIuMTY4LjE3**********************************************************************DZiNzZhMDJjZmQxNGI2NmM5ZDdiM2Q1NjYiLCJrZXkiOiJWMmM5bTRnQkNncGZnZ21pdnNsMDpsYll0ZlRCTlRvYTlYS1pUVlNDZ3NRIn0=
root@elkstack:/#
```

Diesen Token kopieren und auf der Weboberfläche einfügen und auf configure Elastic klicken.



Nun muss ein Verifierzungscode eingeben werden.



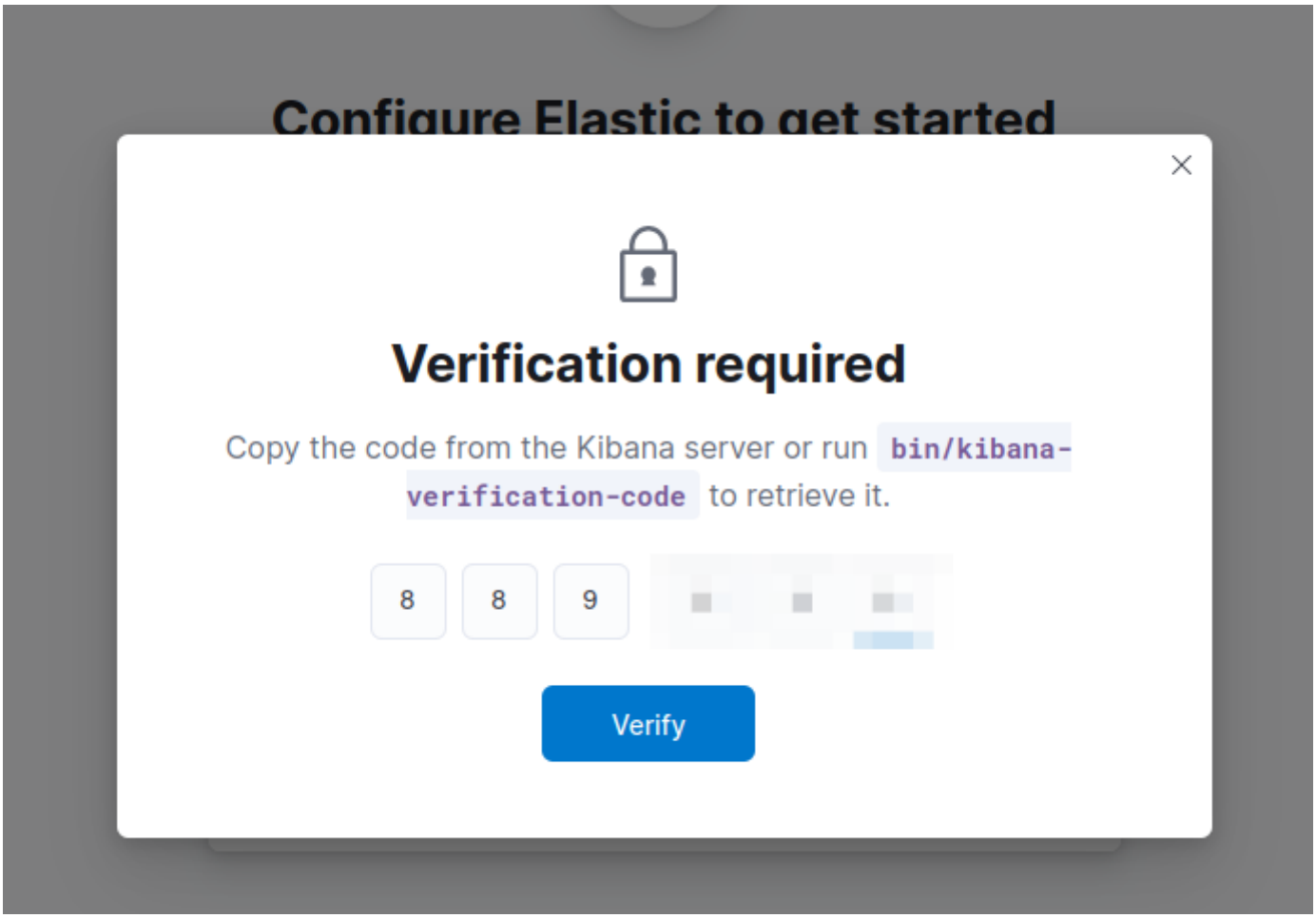
Diesen holen wir uns auch wieder ausm Terminal

```
bash /usr/share/kibana/bin/kibana-verification-code
```

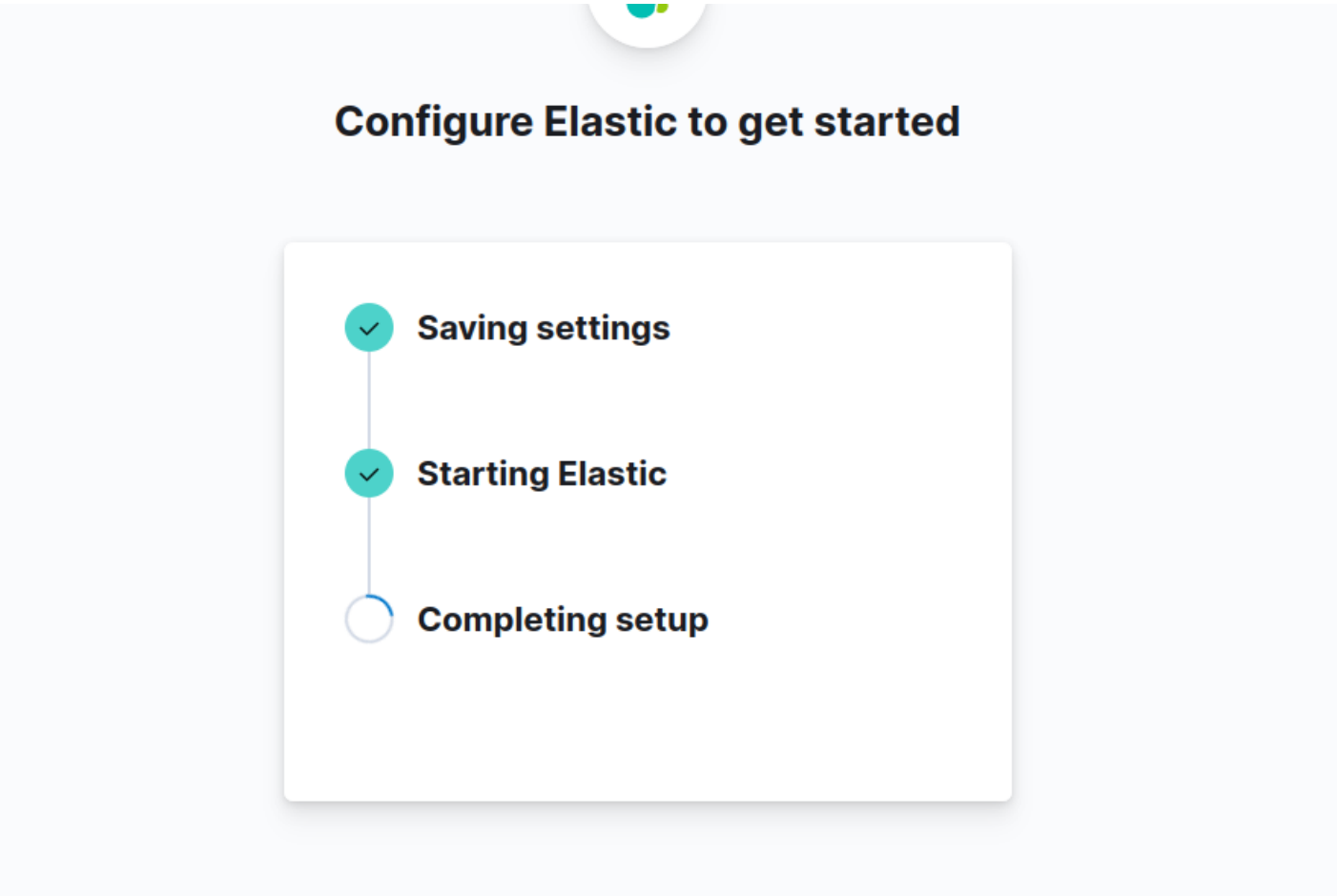
Ausgabe:

```
root@elkstack:/# bash /usr/share/kibana/bin/kibana-verification-code
Your verification code is:  889 ***
root@elkstack:/#
```

nun den Code auf der Website eingeben

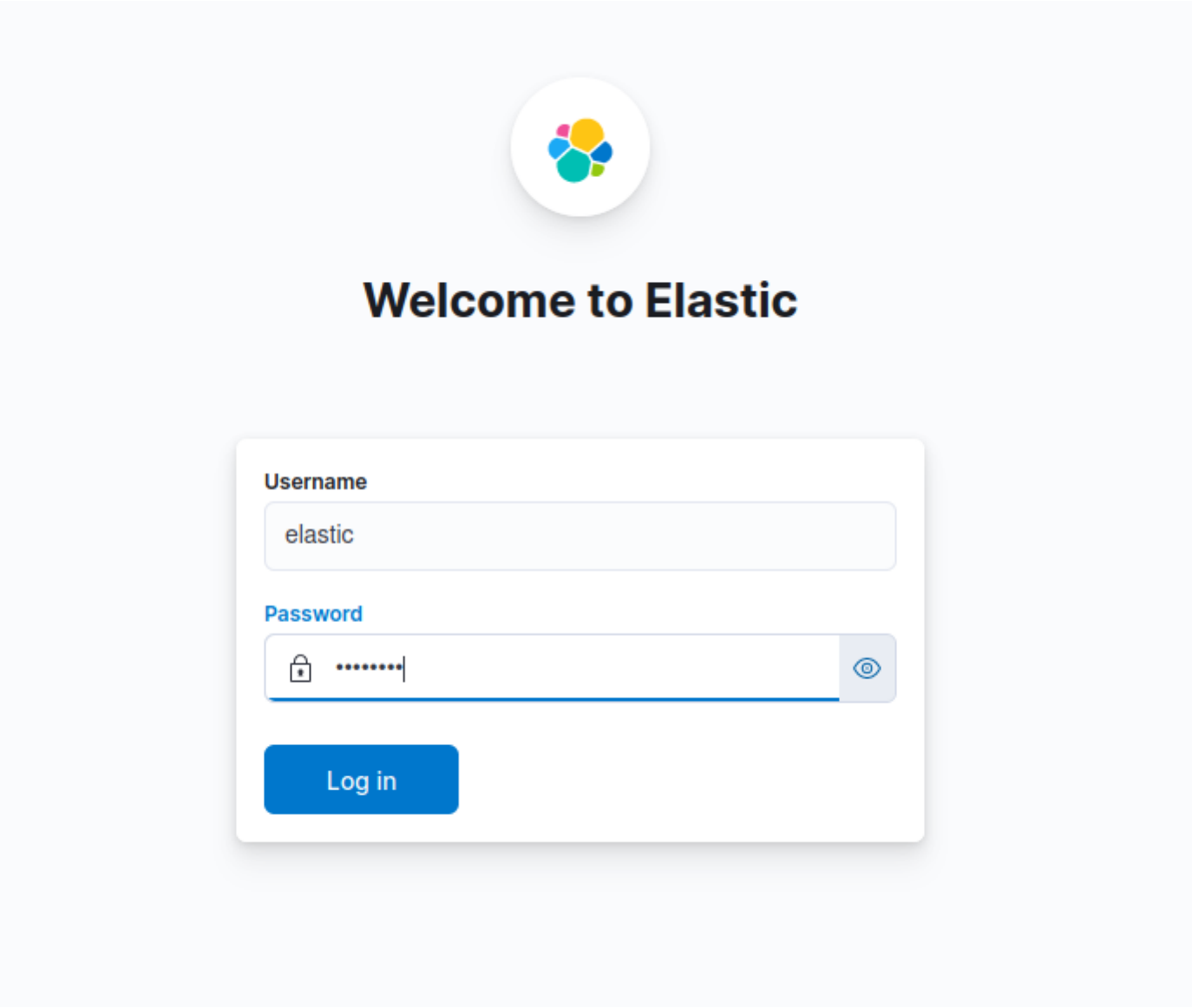


Nun abwarten

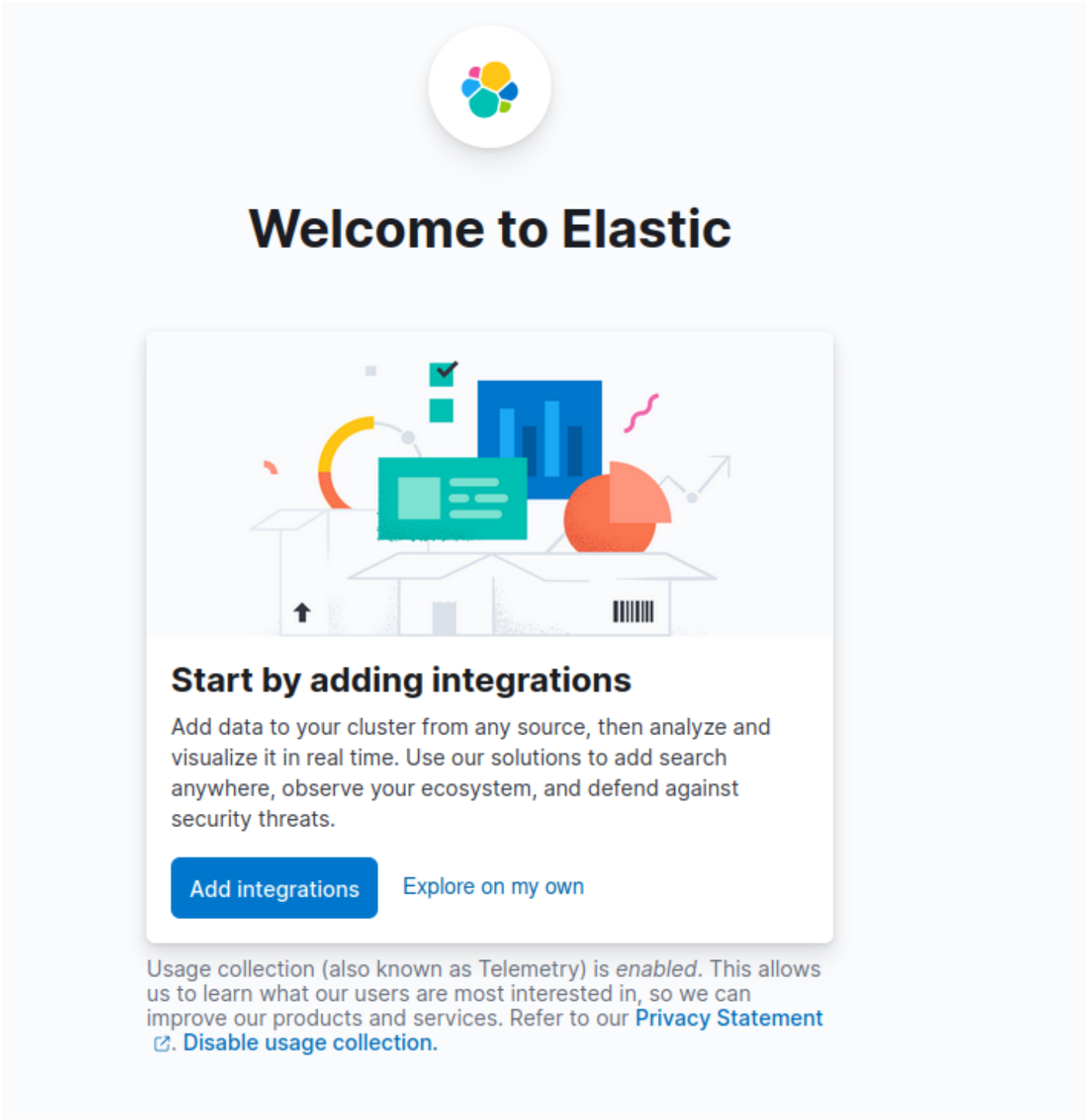


Nun der Loginscreen

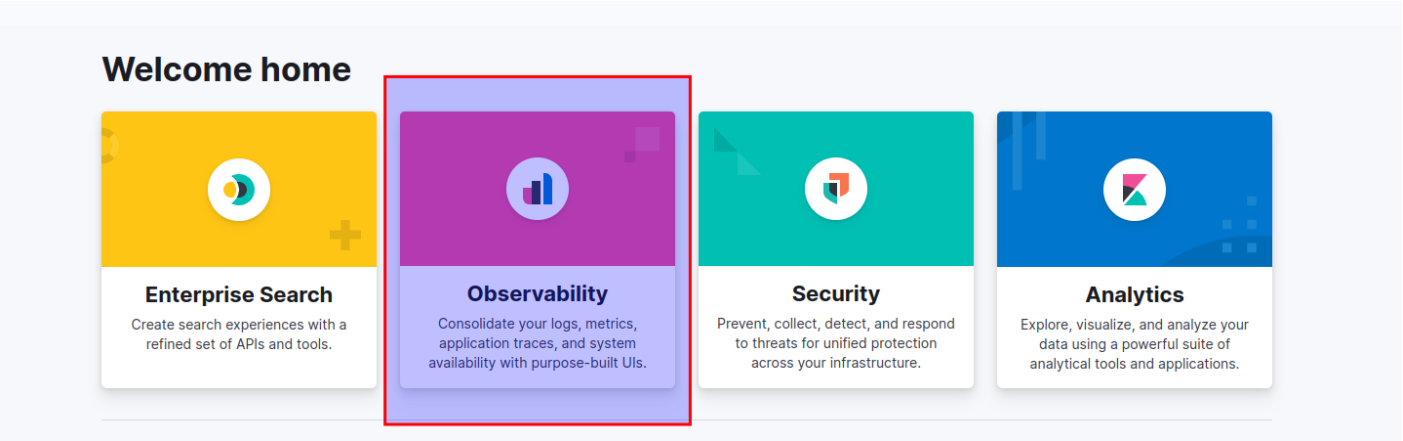
Benutzername : elastic
Kennwort : Das Password aus dem Reset.



Nun sind wir im Login Screen und gehen Explore my Own



und nun auf Observability klicken



IP-Adresse ändern. Sollte sich die IP vom Host ändern muss sie an folgenden stellen angepasst werden

Fehler

Kibana server is not ready yet. Wenn die Weboberfläche aufgerufen wird.

Meistens tritt dieser Fehler bei Fehlkonfiguration von den ips in den Konfigdateien.
Meist nach einem IP-Wechsel.

Dazu schauen wir in die LOG

Verwalten von Elastic

Logs löschen

Beschreibung:

Es gibt Situationen da möchte man logs löschen.
Entweder von einem Zeitraum oder ganz bestimmte, oder einfach alles.
genau wie Logs nach einem angegben Zeitraum löschen.

Die Varianten

- Alle Logs löschen:

  ```
  curl -X DELETE "localhost:9200/_all"
  Ausgabe:
  curl: (52) Empty reply from server
  ```

- Mit Wildcard. Es wird immer der Indexname genommen, der in logtash angegben wurde.

  ```
  curl -X DELETE "localhost:9200/syslog-*"
  ```

- Oder explizit mit Datum :

  ```
  curl -X DELETE "localhost:9200/syslogs-2023_06_19"
  ```

Logs nach einem Datum löschen:

Es können policies angelgt werden nach dem die Logs gelöscht werden soll.
Dies geht über das Terminal mit einem curl Befehl.
In unerem Beispiel heißt die Policy 30days,

Min age und max age bekommen den Wert 30 Tage

Der Befehl

```
curl -X PUT "localhost:9200/_ilm/policy/30days" -H 'Content-Type: application/json' -d'
{
  "policy": {
    "phases": {
      "hot": {
```

```
      "min_age": "0ms",
      "actions": {
        "rollover": {
          "max_age": "30d"
        }
      }
    },
    "delete": {
      "min_age": "30d",
      "actions": {
        "delete": {}
      }
    }
  }
}
'
```

Nun haben wir eine Policy erstellt.
Diese müssen wir noch auf unseren Index ausrollen.
Der index wurde in der logtash festgelegt.