

# 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

Elasticsearch 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

```
systemctl -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

Elasticsearch 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 ausgegeben.

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 editieren 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 ausgegeben) und den path anpassen wenn gewünscht wir lassen diesen path aber so.

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

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

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 Verzeichnis 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

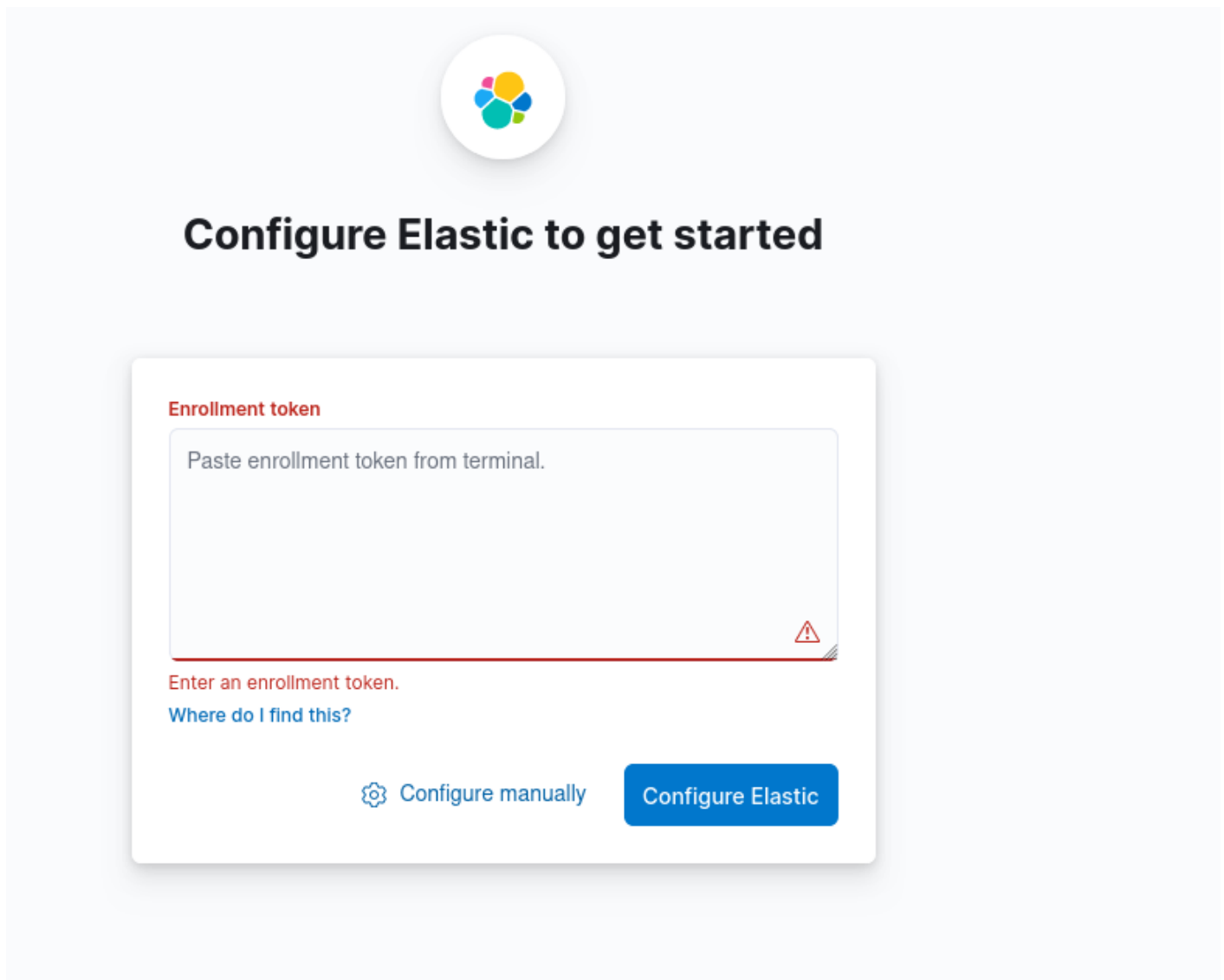
```
*/5 * * * * /root/getsyslog.sh
```

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 Elasticsearch. 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:

```
eyJ2ZXliOiI4LjguMSIsImFkcil6WyIxOTluMTY4LjE3*****  
*****DZiNzZhMDJjZmQxNGI2NmM5ZDdiM2Q1NjYiLCJrZXkiOiJWMmM5bTRnQkNncGZnZ21pdnNsMDpsYll0ZIR  
CTIRvYTIYS1pUVINDZ3NRIn0=  
root@elkstack:/#
```

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



## Configure Elastic to get started

### Enrollment token

eyJ2ZXliOiI4LjguMSIsImFkcil6WylxOTluMTY4LjE3OC42NDo5Mj

A  
F  
2  
0

Connect to <https://> :49200


 [Configure manually](#)

[Configure Elastic](#)

Nun muss ein Verifizierungscode eingegeben werden.



## Configure Elastic to get started

×  
  

### Verification required

Copy the code from the Kibana server or run `bin/kibana-verification-code` to retrieve it.

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

## Configure Elastic to get started

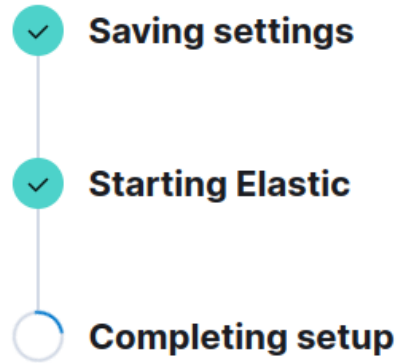


### Verification required

Copy the code from the Kibana server or run `bin/kibana-verification-code` to retrieve it.

Nun abwarten

## Configure Elastic to get started

- 
- ✓ Saving settings
  - ✓ Starting Elastic
  - Completing setup

Nun der Loginscreen

Benutzername : elastic

Kennwort : Das Password aus dem Reset.



# Welcome to Elastic

**Username**

**Password**



**Log in**

Nun sind wir im Login Screen und gehen Explore my Own



# Welcome to Elastic



## Start by adding integrations

Add data to your cluster from any source, then analyze and visualize it in real time. Use our solutions to add search anywhere, observe your ecosystem, and defend against security threats.

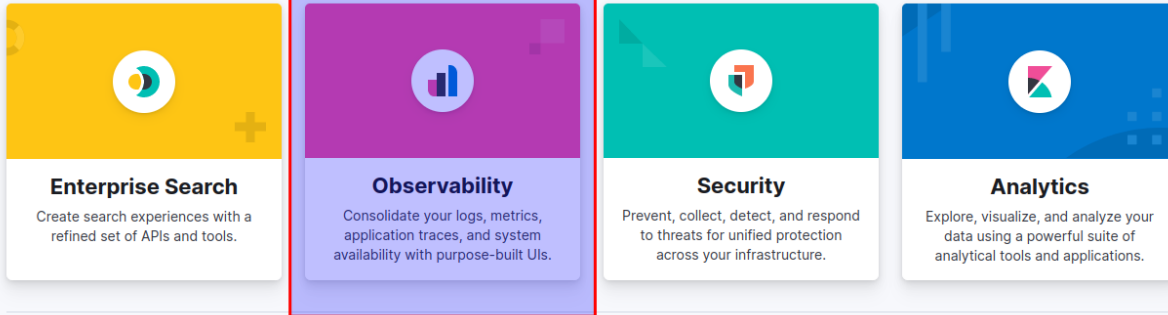
[Add integrations](#)

[Explore on my own](#)

Usage collection (also known as Telemetry) is *enabled*. This allows us to learn what our users are most interested in, so we can improve our products and services. Refer to our [Privacy Statement](#) [↗](#). [Disable usage collection.](#)

und nun auf Observability klicken

## Welcome home



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

---

Version #11

Erstellt: 19 Juni 2023 11:58:40 von Admin

Zuletzt aktualisiert: 11 Juli 2023 09:35:04 von Admin