

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

Elasticsearch und Logstash benötigen Java

```
apt update  
apt install default-jdk gnupg gnupg2 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

```
systemctl -p
```

Nun reboot

```
reboot
```

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/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 ich 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 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.

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 Elasticsearch. Denn Kibana greift ja auf elasticsearch zu.



Configure Elastic to get started

Enrollment token

Paste enrollment token from terminal.

Enter an enrollment token.
[Where do I find this?](#)

[Configure manually](#) [Configure Elastic](#)

Diesen Key holen wir uns aus dem Terminal mittels:

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

Ausgabe:

```
eyJ2ZXliOiI4LjguMSlsmFkcil6WyIxOTluMTY4LjE3*****  
*****DZiNzZhMDJjZmQxNGI2NmM5ZDdiM2Q1NjYiLCJrZXkiOiJWMM5bTRnQkNncGZnZ21pdnNsMDpsYlI0ZIR  
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 [blurred]
F [blurred]
2 [blurred]
0 [blurred]

Connect to `https://[blurred]:9200`


 [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.



Verify

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.](#)

Nun auf das Burgermenü und dann ganz unten Stack Management anklicken



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

Version #24

Erstellt: 8 Juni 2023 10:13:33 von Admin

Zuletzt aktualisiert: 22 August 2023 08:37:08 von Admin