Auf den Elch gekommen: Logfile-Analyse mit ELK-Server

Vanessa Rex, 19.03.2016

SerNet

Auf den Elch gekommen: Logfile-Analyse mit ELK-Server

Vanessa Rex, 19.03.2016

SerNet

SerNet GmbH

SerNet

- Ca. 60 Mitarbeiter
- Standorte: Göttingen und Berlin
- Themen: Informationssicherheit und Datenschutz
  - Firewall und VPN für mittlere und große Unternehmen
  - Nutzung von Open Source
- Unterabteilungen: winwerk, Samba und verinice

SerNet GmbH

SerNet

- Ca. 60 Mitarbeiter
- Standorte: Göttingen und Berlin
- Themen: Informationssicherheit und Datenschutz
  - Firewall und VPN für mittlere und große Unternehmen
  - Nutzung von Open Source
- Unterabteilungen: winwerk, Samba und verinice

Übergang

- Wer? Und vorallem WARUM?

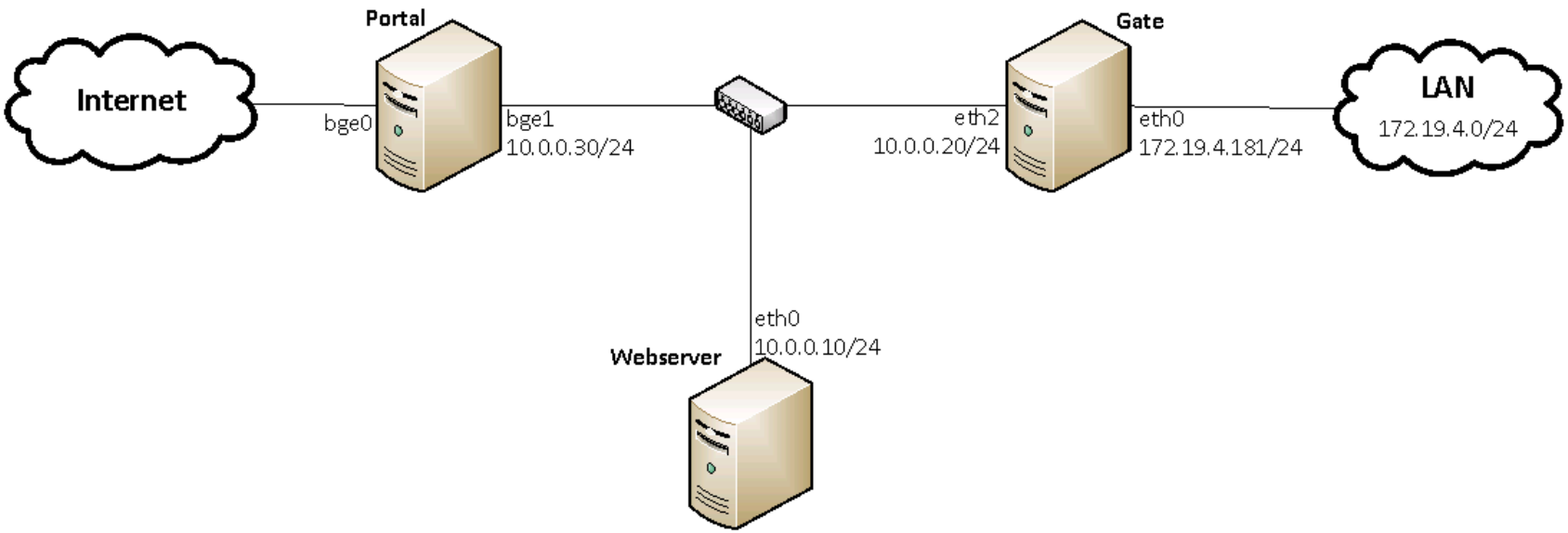
SerNet

Übergang

- Wer? Und vorallem WARUM?

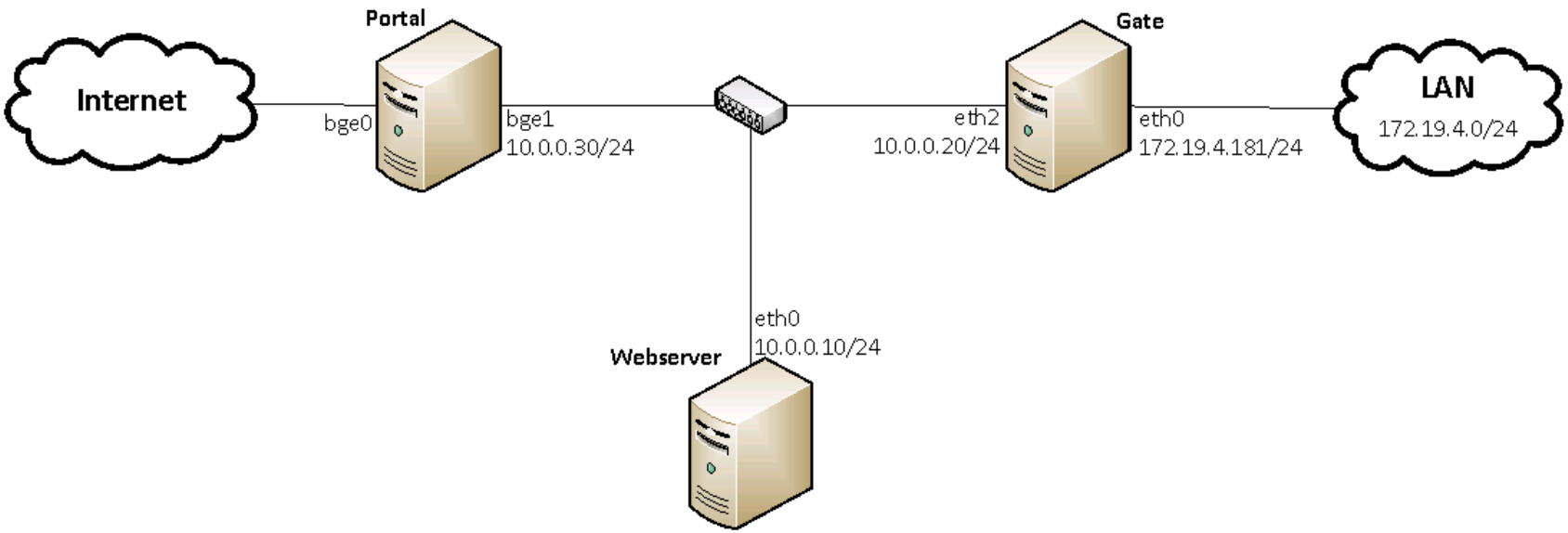
SerNet

Ausgangssituation



SerNet

Ausgangssituation



SerNet

Ausgangssituation

- Firewalls und Webserver schreiben Logfiles
- Analyse sehr aufwendig
- Statistiken kaum möglich
- Zugriff auf die Logfiles nur per Konsole

SerNet

Ausgangssituation

- Firewalls und Webserver schreiben Logfiles
- Analyse sehr aufwendig
- Statistiken kaum möglich
- Zugriff auf die Logfiles nur per Konsole

SerNet

Vereinfachtes Beispiel

SerNet

Vereinfachtes Beispiel

SerNet

Echtes Beispiel

Mar 1 12:07:40 portal1 kernel: 8222926.303576] crt251:Drop.FORWARD.invalid:IN=eth0 OUT=eth1.105
MAC=00:1b:21:9f:b3:50:78:2b:cb:5e:24:00:08:00 SRC=178.111.222.211 DST=193.111.222.49 LEN=70 TOS=0x00 PREC=0x20
TTL=54 ID=62938 PROTO=ICMP TYPE=3 CODE=3 [SRC=193.111.222.49 DST=178.111.222.211 LEN=42 TOS=0x00 PREC=0x00
TTL=240 ID=45607 PROTO=UDP SPT=30271 DPT=21 LEN=22] Mar 1 18:07:27 portal1 kernel: [8244476.210681]
crt274:Drop.FORWARD:IN=eth1.105 OUT=eth0 MAC=00:1b:21:9f:b3:51:9e:6c:1b:56:6f:a5:08:00 SRC=193.111.222.49
DST=80.111.222.50 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=11120 DF PROTO=TCP SPT=48206 DPT=80 WINDOW=29200
RES=0x00 SYN URGP=0 Mar 1 18:07:28 portal1 kernel: [8244477.208956] crt274:Drop.FORWARD:IN=eth1.105 OUT=eth0
MAC=00:1b:21:9f:b3:51:9e:6c:1b:56:6f:00:08:00 SRC=193.111.222.49 DST=80.111.222.50 LEN=60 TOS=0x00 PREC=0x00 TTL=63
ID=11121 DF PROTO=TCP SPT=48206 DPT=80 WINDOW=29200 RES=0x00 SYN URGP=0 Mar 1 18:07:30 portal1 kernel:
[8244479.209918] crt274:Drop.FORWARD:IN=eth1.105 OUT=eth0 MAC=00:1b:21:9f:b3:51:9e:6c:1b:56:6f:00:08:00
SRC=193.111.222.49 DST=80.111.222.50 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=11122 DF PROTO=TCP SPT=48206
DPT=80 WINDOW=29200 RES=0x00 SYN URGP=0 Mar 1 18:07:33 portal1 kernel: [8244482.205273]
crt274:Drop.FORWARD:IN=eth1.105 OUT=eth0 MAC=00:1b:21:9f:b3:51:9e:6c:1b:56:6f:00:08:00 SRC=193.111.222.49
DST=80.111.222.35 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=33148 DF PROTO=TCP SPT=52670 DPT=80 WINDOW=29200
RES=0x00 SYN URGP=0 Mar 1 18:07:35 portal1 kernel: [8244484.206076] crt74:Drop.FORWARD:IN=eth1.105 OUT=eth0
MAC=00:1b:21:9f:b3:51:9e:6c:1b:56:6f:00:08:00 SRC=193.111.222.49 DST=80.111.222.35 LEN=60 TOS=0x00 PREC=0x00 TTL=63
ID=33149 DF PROTO=TCP SPT=52670 DPT=80 WINDOW=29200 RES=0x00 SYN URGP=0

SerNet

Echtes Beispiel

Mar 1 12:07:40 portal1 kernel: 8222926.303576] crt251:Drop.FORWARD.invalid:IN=eth0 OUT=eth1.105
MAC=00:1b:21:9f:b3:50:78:2b:cb:5e:24:00:08:00 SRC=178.111.222.211 DST=193.111.222.49 LEN=70 TOS=0x00 PREC=0x20
TTL=54 ID=62938 PROTO=ICMP TYPE=3 CODE=3 [SRC=193.111.222.49 DST=178.111.222.211 LEN=42 TOS=0x00 PREC=0x00
TTL=240 ID=45607 PROTO=UDP SPT=30271 DPT=21 LEN=22] Mar 1 18:07:27 portal1 kernel: [8244476.210681]
crt274:Drop.FORWARD:IN=eth1.105 OUT=eth0 MAC=00:1b:21:9f:b3:51:9e:6c:1b:56:6f:a5:08:00 SRC=193.111.222.49
DST=80.111.222.50 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=11120 DF PROTO=TCP SPT=48206 DPT=80 WINDOW=29200
RES=0x00 SYN URGP=0 Mar 1 18:07:28 portal1 kernel: [8244477.208956] crt274:Drop.FORWARD:IN=eth1.105 OUT=eth0
MAC=00:1b:21:9f:b3:51:9e:6c:1b:56:6f:00:08:00 SRC=193.111.222.49 DST=80.111.222.50 LEN=60 TOS=0x00 PREC=0x00 TTL=63
ID=11121 DF PROTO=TCP SPT=48206 DPT=80 WINDOW=29200 RES=0x00 SYN URGP=0 Mar 1 18:07:30 portal1 kernel:
[8244479.209918] crt274:Drop.FORWARD:IN=eth1.105 OUT=eth0 MAC=00:1b:21:9f:b3:51:9e:6c:1b:56:6f:00:08:00
SRC=193.111.222.49 DST=80.111.222.50 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=11122 DF PROTO=TCP SPT=48206
DPT=80 WINDOW=29200 RES=0x00 SYN URGP=0 Mar 1 18:07:33 portal1 kernel: [8244482.205273]
crt274:Drop.FORWARD:IN=eth1.105 OUT=eth0 MAC=00:1b:21:9f:b3:51:9e:6c:1b:56:6f:00:08:00 SRC=193.111.222.49
DST=80.111.222.35 LEN=60 TOS=0x00 PREC=0x00 TTL=63 ID=33148 DF PROTO=TCP SPT=52670 DPT=80 WINDOW=29200
RES=0x00 SYN URGP=0 Mar 1 18:07:35 portal1 kernel: [8244484.206076] crt74:Drop.FORWARD:IN=eth1.105 OUT=eth0
MAC=00:1b:21:9f:b3:51:9e:6c:1b:56:6f:00:08:00 SRC=193.111.222.49 DST=80.111.222.35 LEN=60 TOS=0x00 PREC=0x00 TTL=63
ID=33149 DF PROTO=TCP SPT=52670 DPT=80 WINDOW=29200 RES=0x00 SYN URGP=0

SerNet

Ziel

- Ziel: vereinfachte Fehleranalyse
- Analyse-Server in einer DMZ
- Logfiles zentral sammeln
- Filter-Möglichkeiten bieten
- Visualisierung via interner Webseite

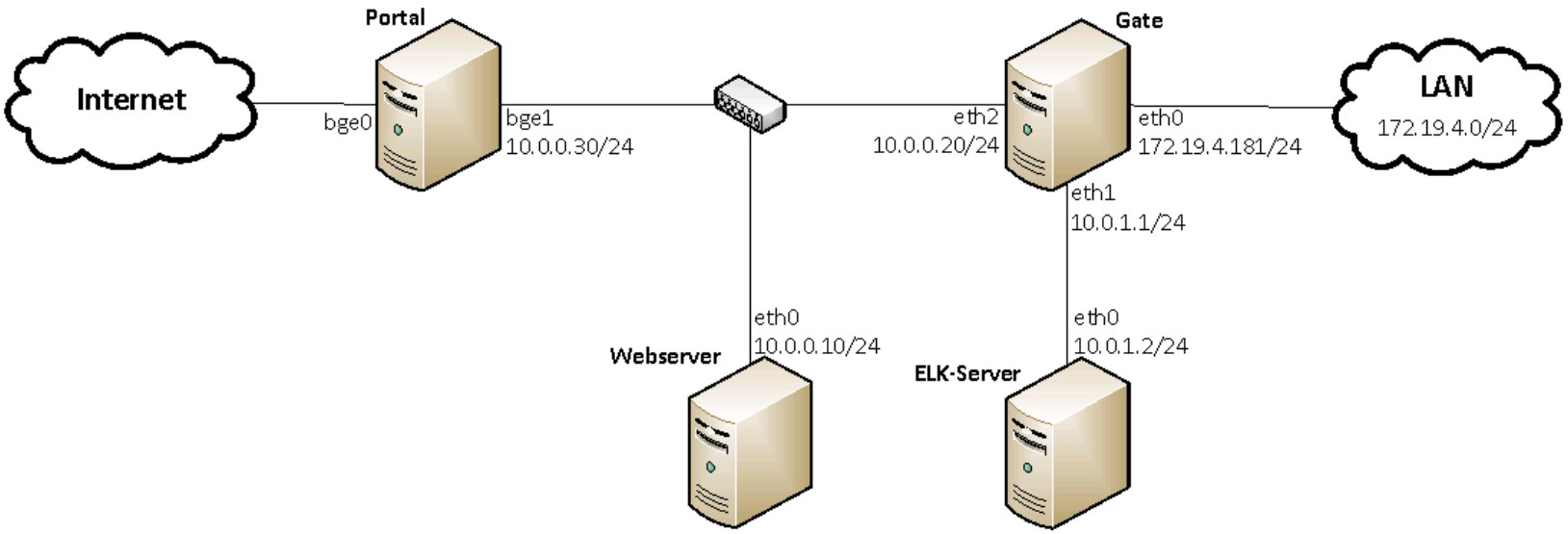
SerNet

Ziel

- Ziel: vereinfachte Fehleranalyse
- Analyse-Server in einer DMZ
- Logfiles zentral sammeln
- Filter-Möglichkeiten bieten
- Visualisierung via interner Webseite

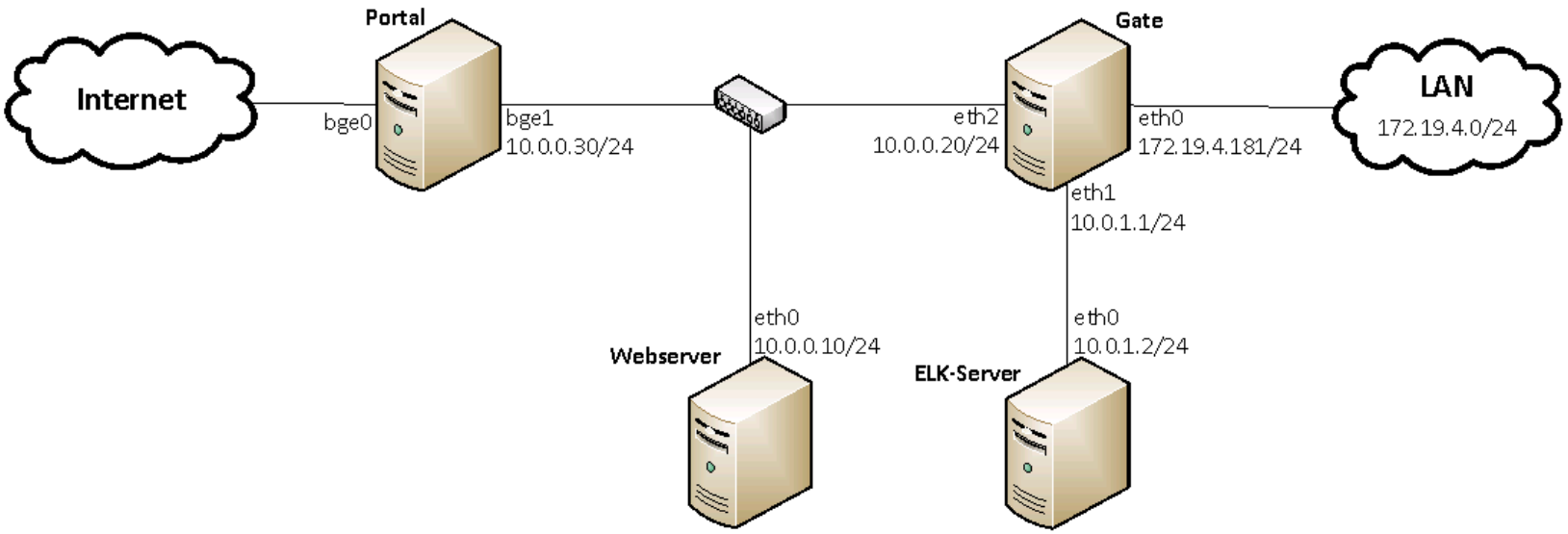
SerNet

Ziel


Internet
Portal
bge0
bge1
10.0.0.30/24
Gate
eth2
10.0.0.20/24
eth0
172.19.4.181/24
LAN
172.19.4.0/24
eth1
10.0.1.1/24
eth0
10.0.0.10/24
Webserver
eth0
10.0.1.2/24
ELK-Server

SerNet

Ziel


Internet
Portal
bge0
bge1
10.0.0.30/24
Gate
eth2
10.0.0.20/24
eth0
172.19.4.181/24
LAN
172.19.4.0/24
eth1
10.0.1.1/24
eth0
10.0.0.10/24
Webserver
eth0
10.0.1.2/24
ELK-Server

SerNet

Übergang

- Wie? Und vorallem WOMIT?

SerNet

Übergang

- Wie? Und vorallem WOMIT?

SerNet

Software-Auswahl

- Verwendung von Open-Source-Produkten
- Betriebssystem: Debian Jessie
- ELK-Setup
  - Elasticsearch - Logstash - Kibana

SerNet

Software-Auswahl

- Elasticsearch: Speichert Daten und ermöglicht schnelle Suche

- Logstash: Sammelt die Logdaten und bietet Filter an

- Kibana: Erstellt Grafen und liefert diese über eine Weboberfläche aus

SerNet

Software-Auswahl

- Elasticsearch: Speichert Daten und ermöglicht schnelle Suche

- Logstash: Sammelt die Logdaten und bietet Filter an

- Kibana: Erstellt Grafen und liefert diese über eine Weboberfläche aus

SerNet

Die Hardware

- Speicherplatz mindestens 1 TB
- mit RAID 1
- oder eine Virtuelle Maschiene
- Kosten ca. 3000 €

SerNet

Die Hardware

- Speicherplatz mindestens 1 TB
- mit RAID 1
- oder eine Virtuelle Maschiene
- Kosten ca. 3000 €

SerNet

Warum Open Source statt proprietärer Lösung?

- **ELK-Server**
- Such-, Analyse- und Visualisierungsfunktionen
- Quellcode offen zugänglich
- eigene Hardware nötig
- Daten bleiben im internen Netz

SerNet

Warum Open Source statt proprietärer Lösung?

- **ELK-Server**
- Such-, Analyse- und Visualisierungsfunktionen
- Quellcode offen zugänglich
- eigene Hardware nötig
- Daten bleiben im internen Netz

- **Splunk**
- Such-, Analyse- und Visualisierungsfunktionen
- Quellcode liegt nicht offen
- Cloud-Nutzung möglich
- Ort der Lagerung unbekannt

SerNet

Warum Open Source statt proprietärer Lösung?

- **ELK-Server**
- Such-, Analyse- und Visualisierungsfunktionen
- Quellcode offen zugänglich
- eigene Hardware nötig
- Daten bleiben im internen Netz

- **Splunk**
- Such-, Analyse- und Visualisierungsfunktionen
- Quellcode liegt nicht offen
- Cloud-Nutzung möglich
- Ort der Lagerung unbekannt

SerNet

Die Kosten

> *'Once we get ELK going it will be cheaper. The time to learn and get ELK figured out is an investment.'*

https://riskfocus.com/splunk-vs-elk-part-1-cost/

SerNet

Übergang

- Auf den ELCH fertig - Los!

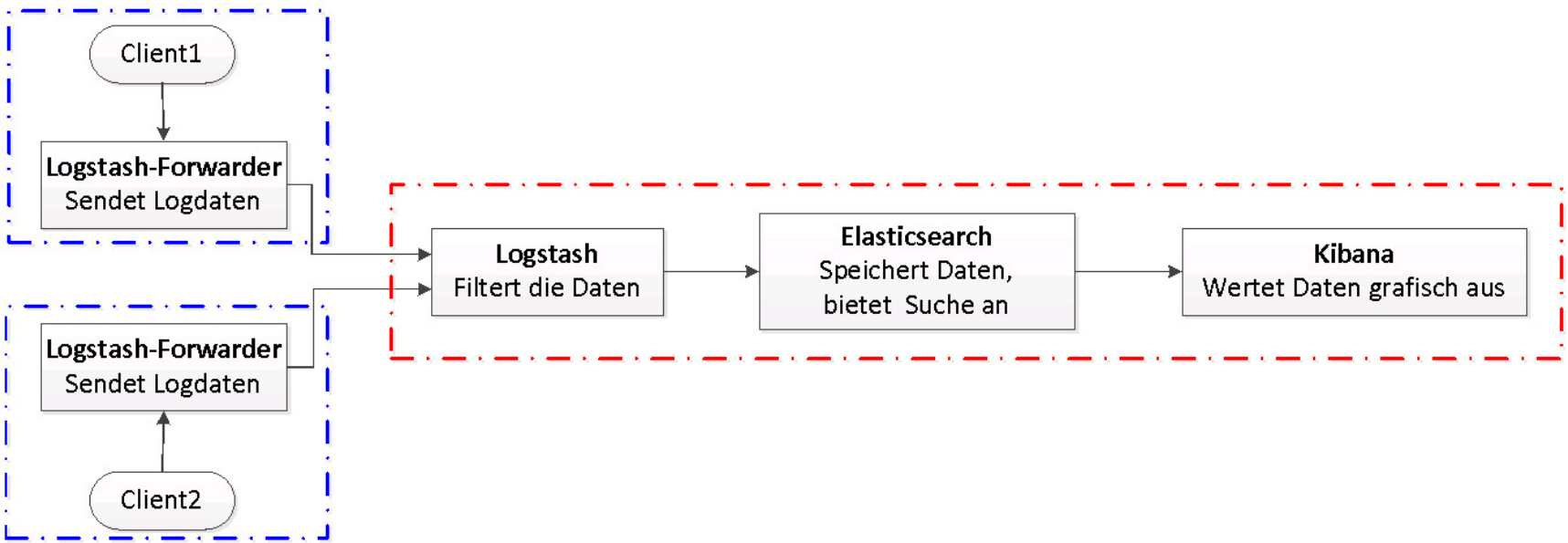
SerNet

Übergang

- Auf den ELCH fertig - Los!

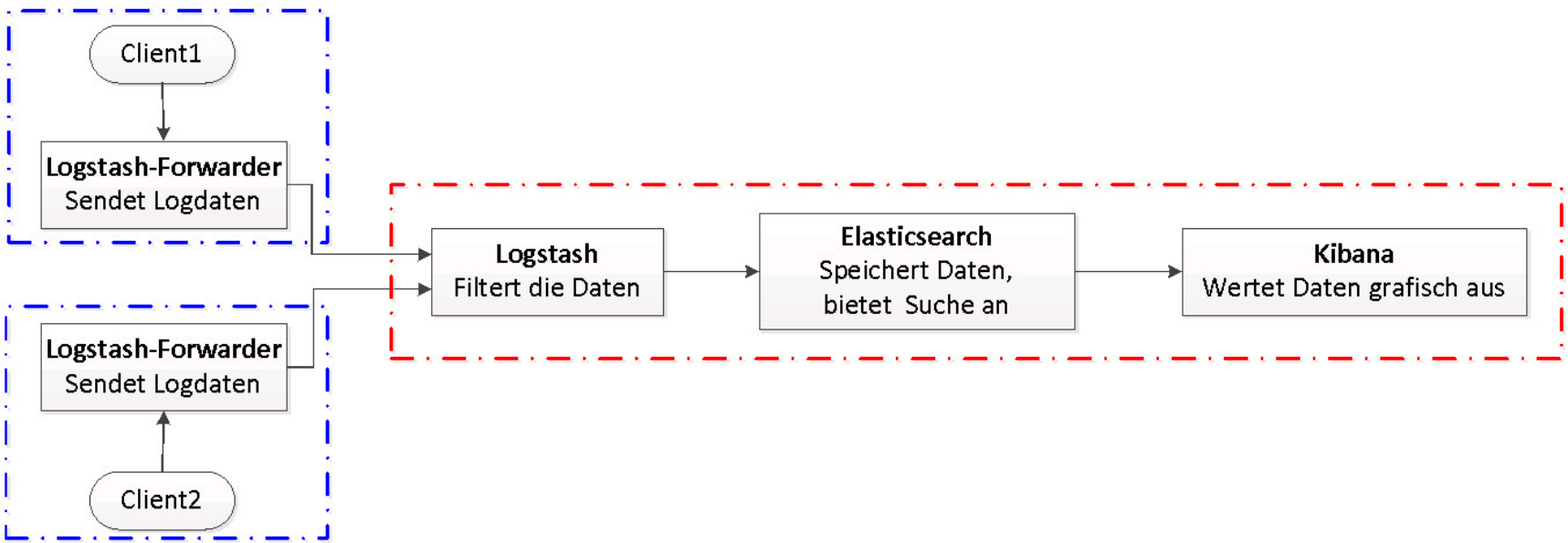
SerNet

So sieht ein 'Elch' für einen Admin aus



SerNet

So sieht ein 'Elch' für einen Admin aus



SerNet

Einrichtung des Logstash-Forwarders

- Installation auf allen verwendeten Rechnern
- Repository runterladen und installieren
- Die Konfigurationsdatei `Logstash-Forwarder.conf` anpassen

SerNet

Einrichtung des Logstash-Forwarders

- Installation auf allen verwendeten Rechnern
- Repository runterladen und installieren
- Die Konfigurationsdatei `Logstash-Forwarder.conf` anpassen

```
# Konfiguration der /etc/logstash-forwarder.conf
    "servers": [ "10.0.1.2:5000" ],
    "timeout": 15,
    "ssl ca": "/etc/pki/tls/certs/logstash-forwarder.crt"

# ...

# Syslog-Datei senden
    {
      "paths": [
        "/var/log/syslog",
       ],
      "fields": { "type": "syslog" }
```

SerNet

Einrichtung des Logstash-Forwarders

- Installation auf allen verwendeten Rechnern
- Repository runterladen und installieren
- Die Konfigurationsdatei `Logstash-Forwarder.conf` anpassen

```
# Konfiguration der /etc/logstash-forwarder.conf
    "servers": [ "10.0.1.2:5000" ],
    "timeout": 15,
    "ssl ca": "/etc/pki/tls/certs/logstash-forwarder.crt"

# ...

# Syslog-Datei senden
    {
      "paths": [
        "/var/log/syslog",
       ],
      "fields": { "type": "syslog" }
```

SerNet

Einrichtung von Logstash

- Filter einrichten
  - Eingabe + Filter + Ausgabe
  - Kriterien: z.B. IP, Port, Host
- Pattern anlegen
- Zertifikat erstellen

SerNet

Einrichtung von Logstash

- Filter einrichten
  - Eingabe + Filter + Ausgabe
  - Kriterien: z.B. IP, Port, Host
- Pattern anlegen
- Zertifikat erstellen

SerNet

Filtern bitte!

- Syslog ausgeben mit Standard-Filter

```
filter {
if [type] == "syslog" {
        grok {
                match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp}
                %{SYSLOGHOST:syslog_hostname}  %{GREEDYDATA:syslog_message}" }
    }
```

SerNet

Filtern bitte!

- Syslog ausgeben mit Standard-Filter

```
filter {
if [type] == "syslog" {
        grok {
                match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp}
                %{SYSLOGHOST:syslog_hostname}  %{GREEDYDATA:syslog_message}" }
    }
```

- Iptables Logs aus dem Syslog filtern mit Hilfe von Pattern

```
# Pattern anlegen
vi /opt/logstash/patterns/iptables.src
IPTABLES_SRC SRC=%{IP:src_ip}

# Pattern einbinden
 vi 03-iptables.conf
if [type] == "iptables" {
        grok {
                break_on_match => true
                patterns_dir => "/opt/logstash/patterns/iptables.src"
                match => [ "message", "%{IPTABLES_SRC:SRC_IP_IPTABLES}"]
        }
}
```

SerNet

Filtern bitte!

- Syslog ausgeben mit Standard-Filter

```
filter {
if [type] == "syslog" {
        grok {
                match => { "message" => "%{SYSLOGTIMESTAMP:syslog_timestamp}
                %{SYSLOGHOST:syslog_hostname}  %{GREEDYDATA:syslog_message}" }
    }
```

- Iptables Logs aus dem Syslog filtern mit Hilfe von Pattern

```
# Pattern anlegen
vi /opt/logstash/patterns/iptables.src
IPTABLES_SRC SRC=%{IP:src_ip}

# Pattern einbinden
 vi 03-iptables.conf
if [type] == "iptables" {
        grok {
                break_on_match => true
                patterns_dir => "/opt/logstash/patterns/iptables.src"
                match => [ "message", "%{IPTABLES_SRC:SRC_IP_IPTABLES}"]
        }
}
```

SerNet

Elasticsearch

- Installation
- Beschränkung auf Localhost

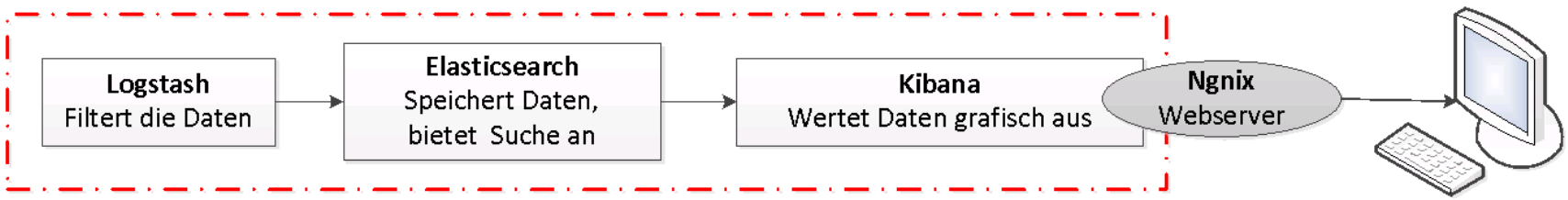
SerNet

Elasticsearch

- Installation
- Beschränkung auf Localhost

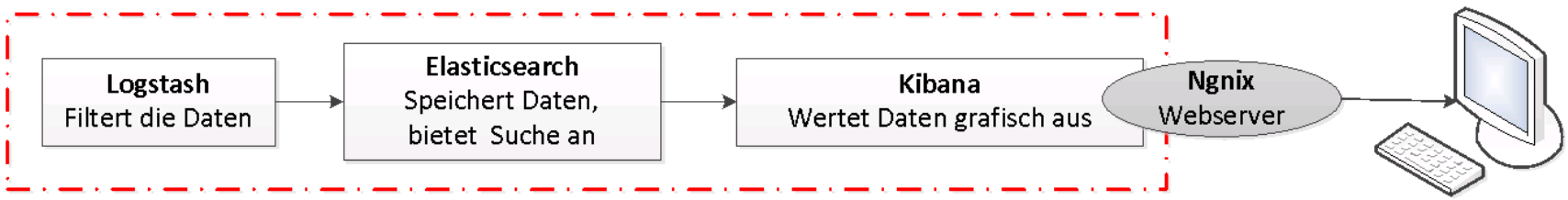
SerNet

Ein 'Elch' aus Nutzersicht



SerNet

Ein 'Elch' aus Nutzersicht



SerNet

Kibana und der Webserver

- Beschränkung auf localhost
- Webserver nginx installieren
  - Passwort geschützten Bereich anlegen
- Webseite einrichten

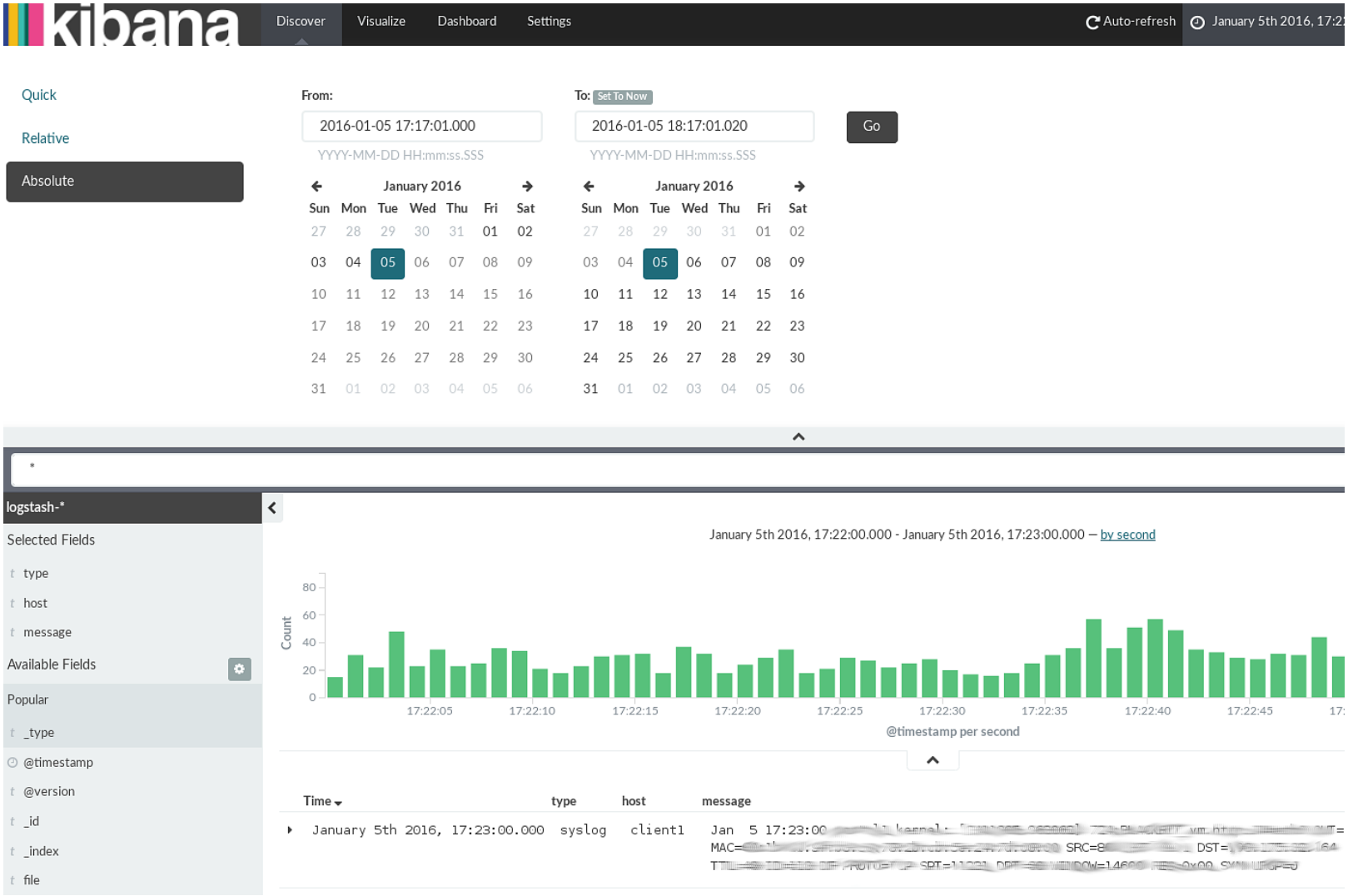
SerNet

Kibana und der Webserver

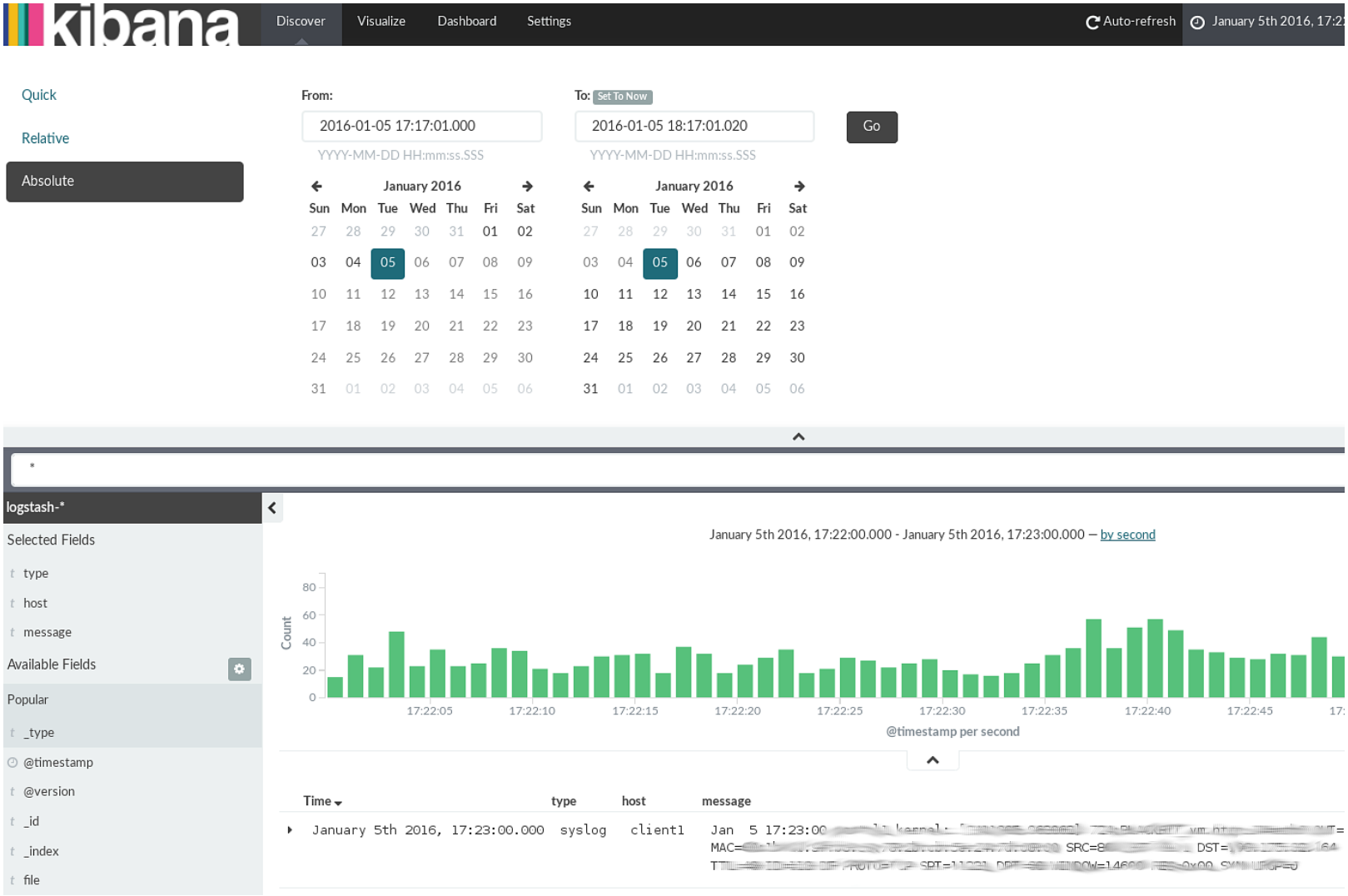
- Beschränkung auf localhost
- Webserver nginx installieren
  - Passwort geschützten Bereich anlegen
- Webseite einrichten

SerNet

Die Weboberfläche



Die Weboberfläche



Übergang

- Und nun?

Übergang

- Und nun?

Fazit und Ausblick

- Filtert Logfiles
  - wenige Filter vorhanden
- Kein Allrounder
  - Grafanna

SerNet

Fazit und Ausblick

- Filtert Logfiles
  - wenige Filter vorhanden
- Kein Allrounder
  - Grafanna

SerNet

Quellen

Alle verwendeten Bilder und Logos sind zur Wiederverwendung frei gegeben.
Alle Fotos und Netzpläne, etc. sind von mir selbst erstellt worden.

SerNet

Quellen

Alle verwendeten Bilder und Logos sind zur Wiederverwendung frei gegeben.
Alle Fotos und Netzpläne, etc. sind von mir selbst erstellt worden.

SerNet

Kontakt

Vanessa Rex, vr@sernet.de

SerNet GmbH
Bahnhofsallee 1b
37081 Göttingen
tel +49 551 370000-0
fax +49 551 370000-9
http://www.sernet.de

Torstraße 6
10119 Berlin
+49 30 5 779 779 0
+49 30 5 779 779 9

SerNet