von
S & F

Socket Monitoring

29th October

2 Monitoring von Sockets

Wie viele Sockets sind insgesamt geöffnet?

❯ netstat -a | wc -l

843

Wie unterscheiden sich die Einträge von TCP und UDP Sockets?

- TCP
  - baut Verbindung durch Three-Way-Handshake (SYN, SYN-ACK, ACK)
  - im Output steht immer ein Status dabei, zB `LISTEN` oder `ESTABLISHED`
- UDP
  - sendet Datenpakete ohne feste Verbindung aufzubauen
  - kein Status

Was bedeuten die Einträge in der Spalte „State“ bei TCP Sockets?

- LISTEN
  - warten auf Verbindungsanforderung
- ESTABLISHED
  - aktive Verbindung zwischen local und remote
- CLOSE_WAIT
  - remote hat die Verbindung beendet und das muss local noch nachholen
- TIME_WAIT
  - wenn beide beendet haben, wartet man etwas, um sicherzustellen, dass alle Pakete abgebaut werden

Wie viele Server-Ports hat ihr Rechner geöffnet (state=Listening)? Auf diesen Ports (und den UDP Ports) kann ihr Rechner von außen kontaktiert werden.

tcp	0	0	localhost:postgresql	0.0.0.0:*	LISTEN
tcp	0	0	localhost:37877	0.0.0.0:*	LISTEN
tcp	0	0	localhost:ipp	0.0.0.0:*	LISTEN
tcp	0	0	0.0.0.0:ssh	0.0.0.0:*	LISTEN
tcp	0	0	localhost:smtp	0.0.0.0:*	LISTEN
tcp	0	0	localhost:27182	0.0.0.0:*	LISTEN
tcp6	0	0	localhost:smtp	[::]:*	LISTEN
tcp6	0	0	localhost:ipp	[::]:*	LISTEN
tcp6	0	0	localhost:postgresql	[::]:*	LISTEN
tcp6	0	0	[::]:ssh	[::]:*	LISTEN
tcp6	0	0	localhost:52829	[::]:*	LISTEN
tcp6	0	0	localhost:35507	[::]:*	LISTEN

— 12 insgesamt

Wie viele Sockets (ESTABLISHED) werden neu geöffnet, wenn Sie die Messung nach einer Minute erneut durchführen bzw. die Ergebnisse aktualisieren?

Erste Ausgabe (vor einer Minute):

- `yui:32830 mil04s23-in-f14.1:https`
- `yui:43444 93.243.107.34.bc.:https`
- `yui:40212 fra24s07-in-f10.1:https`
- `yui:39586 2a04:4e42:8d::347:https`
- `yui:55734 2606:4700:4400::a:https`

Zweite Ausgabe (nach einer Minute):

- `yui:46828 140.227.186.35.bc:https` (neu)
- `yui:32830 mil04s23-in-f14.1:https`

- `yui:43444 93.243.107.34.bc.:https`
- `yui:39574 fra16s53-in-f10.1:https` (neu)
- `yui:34820 168.207.110.34.bc:https` (neu)
- `yui:39586 2a04:4e42:8d::347:https`
- `yui:55734 2606:4700:4400::a:https`

Sehen Sie zahlreiche Sockets mit IP-Adresse 127.0.0.1? Finden Sie heraus, wofür diese IP Adresse benutzt wird und blenden Sie alle Sockets mit dieser Adresse aus.

aus StackOverflow:
In terms of IP addresses this means that any communications to that address effectively never leave or perhaps never actually enter your network interface card so that you always have a "connection".
This allows you to test client/server software (for example) with both parts running on the same machine.

❯ netstat -at | grep -v '127.0.0.1'

Bestimmen sie anhand der Portnummer und der Portliste für einige interessante/unbekannte Prozesse, mit welchem Protokoll diese kommunizieren.

Die Portnummer 5432 kann man mit einer beliebigen anderen ersetzen.

❯ netstat -anp | grep "5432"

tcp	0	0 127.0.0.1:5432	0.0.0.0:*	LISTEN	-
tcp6	0	0 ::1:5432	:::*	LISTEN	-

3 Details über die Kommunikationspartner ihres PCs

Finden Sie über Wireshark heraus, wie das Programm „IPnetInfo“ die Informationen erhält. Welcher Server wird kontaktiert? Welches Protokoll wird verwendet?

❯ netstat -anp

tcp	0	0 192.168.178.26:38006	185.199.111.153:443	ESTABLISHED	22440/floorp

❯ whois 185.199.111.153

inetnum: 185.199.108.0 - 185.199.111.255

netname: US-GITHUB-20170413

country: US

In welchem Netz befindet sich der Web-Server, der in der ersten WireShark-Aufgabe aufgerufenen Webseite?

Google

Welche Informationen finden Sie über die HTWG?

```
inetnum:          141.37.0.0 - 141.37.255.255
netname:          FH-KN
country:          DE
admin-c:          HKTW1-RIPE
tech-c:           HKTW1-RIPE
org:              ORG-HKTW1-RIPE
status:           LEGACY
remarks:          ************************************************
remarks:          * DEFAULT ABUSE CONTACT: abuse@htwg-konstanz.de  *
remarks:          ************************************************
mnt-by:           BELWUE-MNT
mnt-by:           RIPE-NCC-LEGACY-MNT
created:          2002-04-25T09:54:38Z
last-modified:  2016-04-14T08:23:18Z
source:           RIPE
sponsoring-org: ORG-BA9-RIPE

organisation:   ORG-HKTW1-RIPE
org-name:         Hochschule Konstanz Technik, Wirtschaft und Gestaltung
country:          DE
org-type:         OTHER
address:          Brauneggerstr. 55
address:          78462 Konstanz, Germany
e-mail:           netzwerk@htwg-konstanz.de
admin-c:          HKTW1-RIPE
tech-c:           HKTW1-RIPE
abuse-c:          HKTW1-RIPE
mnt-ref:          BELWUE-MNT
```

```
mnt-by:           BELWUE-MNT
created:          2015-06-17T14:46:25Z
last-modified:  2022-12-01T17:31:18Z
source:           RIPE

role:             Hochschule Konstanz Technik, Wirtschaft und Gestaltung
address:          Brauneggerstr. 55
address:          78462 Konstanz, Germany
e-mail:           netzwerk@htwg-konstanz.de
admin-c:          MS3208-RIPE
tech-c:           MS3208-RIPE
nic-hdl:          HKTW1-RIPE
abuse-mailbox:  abuse@htwg-konstanz.de
mnt-by:           BELWUE-MNT
created:          2015-06-17T14:46:25Z
last-modified:  2015-06-18T11:34:36Z
source:           RIPE

% Information related to '141.37.0.0/16AS553'

route:            141.37.0.0/16
descr:            FH-KONSTANZ
origin:           AS553
mnt-by:           BELWUE-MNT
created:          1970-01-01T00:00:00Z
last-modified:  2001-09-22T09:32:38Z
source:           RIPE
```

4 Sockets beim Laden einer Webseite

Bestimmen Sie die Anzahl Sockets, die geöffnet werden, wenn Sie www.spiegel.de herunterladen.

❯ netstat -anp | grep ESTABLISHED | wc -l

vor dem Öffnen der Seite: 8

danach: 19

Was ist die maximale Anzahl von Sockets pro Remote-IP-Adresse?

❯ netstat -anp | grep 128.65.210.184 | wc -l

Welche Remote-Ports werden verwendet?

443

Wie viele verschiedene Firmen können Sie die Remote-Hosts zuordnen (am Besten über Contact Name in IPNetInfo)?

Link11 GmbH Hostmaster für spiegel.de

Laden Sie eine andere populäre Webseite und vergleichen Sie die Liste der kontaktierten Firmen.

Cloudflare für letterboxd.com