
djbdns

Reto Schuettel <reto@schuettel.ch>

LUGS Treff – 11.11.2004

Agenda

- Was und von wem ist djbdns
 - Bestandteile
 - Beispiel Setup
 - Datenfile
 - Nette Features
 - Weitere Infos
-

Was ist djbdns?

- DNS Cache / DNS Server
 - Verschiedene Client Tools
 - ideal für Shell Scripts etc.
 - Client Library (resolver)

 - Schnell / klein / robust / sicher
-

... und von wem?

- Dan J.(?) Bernstein
 - qmail
 - ucpi-tcp
 - daemontools
- Crypto- / Mathematik-Experte
- Teilweise umstrittene Persönlichkeit ;)

Und wer verwendet es?

- Provider
 - Lycos
 - Hosteurope
 - Strato
 - Einige wenige TLD Server
 - Ein paar .edu Server
 - EIN .ch Server ;)
 - DJBs Studie: 8% aller DNS Server (2002)
-

Bestandteile (1)

- tinydns
 - Zonen publizieren (udp)
- axfrdns
 - Schwester von tinydns (tcp)
- dnscache
 - Cache für Client Anfragen

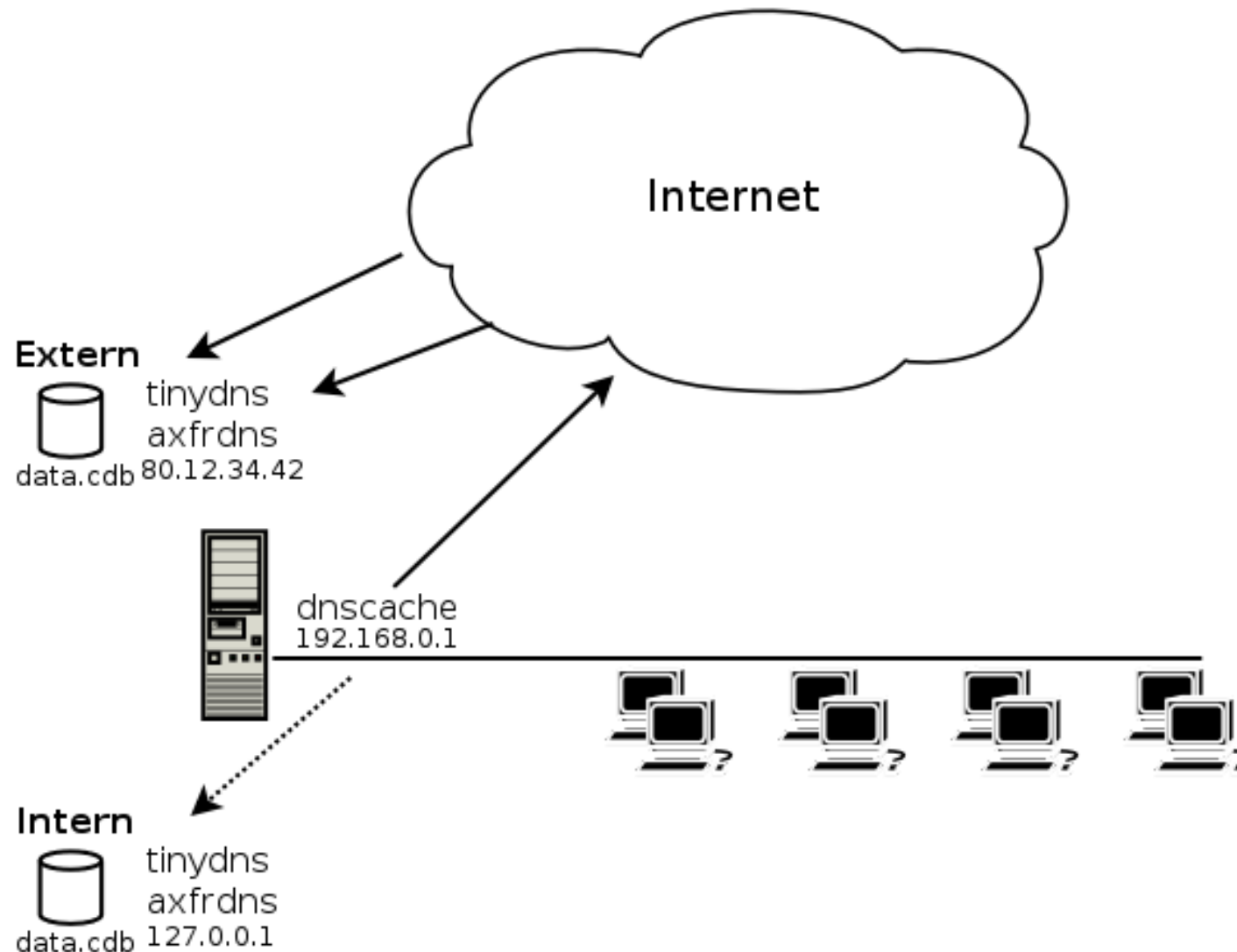
Bestandteile (2)

- walldns
 - Generiert generische PTR/A RR's
- rblDNS
 - Publizieren von RBL's
- dnsq/dnsqr & dnsip/dnsname/etc.
 - dns clients (à la dig/host/nslookup)

Unterschiede djbdns : bind

djbdns 1.05	Bind 9
viele kleine Tools	Monolith
rsync [over ssh]	AXFR/IXFR NOTIFYs
wie man will :)	Zonefiles
AFAIK clean	Security-history: ...
cd \$ROOT; make	haariges reloaden

Typischer SOHO Aufbau



Installation (1)

- Requirements
 - daemontools (alternativ init scripts)
 - ucpi-tcp
 - djbdns
- User einrichten
 - pro daemon ein User (tinydns, axfrdns, ...)
 - fürs logging noch dnslog

Installation (2)

- **Konfiguration dnscache**

```
dnscache-conf dnscache dnslog  
  /etc/dnscache 192.168.0.1
```

```
touch /etc/dnscache/root/ip/192.168.0  
  /etc/dnscache/root/ip/127
```

```
echo 127.0.0.1 >
```

```
  /etc/dnscache/root/servers/example.com
```

```
echo 127.0.0.1 >
```

```
  /etc/dnscache/root/servers/0.168.192.in  
  -addr.arpa
```

Installation (3)

- **Konfiguration tinydns-int**

```
tinydns-conf tinydns dnsmlog /etc/tinydns-  
int/ 127.0.0.1
```

- **Konfiguration tinydns-ext**

```
tinydns-conf tinydns dnsmlog /etc/tinydns-  
ext/ 80.12.34.42
```

Installation (4)

- **Konfiguration axfrdns-int**

```
axfrdns-conf axfrdns dnslog /etc/axfrdns-  
int/ /etc/tinydns-int/ 127.0.0.1
```

- **Konfiguration axfrdns-ext**

```
axfrdns-conf axfrdns dnslog /etc/axfrdns-  
ext/ /etc/tinydns-ext/ 80.12.34.42
```

Aufbau

```
|-- env
|   |-- IP
|   `-- ROOT
|-- log
|   |-- main -> /var/log/djbdns/tinydns-ext
|   |-- run
|-- root
|   |-- Makefile
|   |-- data
|   |-- data.cdb
|   `-- zones
|       `-- schuettel.ch
|-- run
```

Datenfile (SOA/NS/A)

.example.com:1.2.3.4:x ttl:timestamp:lo

- example.com IN NS x.ns.example.com
 - x.ns.example.com IN A 1.2.3.4
 - example.com IN SOA ...
 - Wenn x ein Punkt drin hat gibt's keinen magischen foo.ns. FQDN.
-

Datenfile (NS/A)

&example.com:1.2.3.4:x.ttl.timestamp:lo

- example.com IN NS x.ns.example.com
 - x.ns.example.com IN A 1.2.3.4
 - Delegation
-

Datenfile (A/PTR)

= *foo.bar.com:1.2.3.4:tth.timestamp:lo*

– *foo.bar.com* IN A 1.2.3.4

– 4.3.2.1.in-addr.arpa IN PTR *foo.bar.com*

Datenfile (A)

+ *fqdn:ip:tth.timestamp:lo*

– *foo.bar.com IN A 1.2.3.4*

- Alias

Datenfile (MX/A)

@example.com:1.2.3.4:x.dist.ttl.timestamp:lo

- *example.com* IN MX x.mx.example.com
 - x.mx.example.com IN A 1.2.3.4
 - Wenn x ein Punkt drin hat gibt's keinen magischen foo.mx. FQDN.
-

Makefile

```
data.cdb: data
    tinydns-data
    # rsync auf anderen Server
data: zones/* rsync/*/zones
    cat $^ > $@
```

Testlauf

```
# cd /etc/tinydns-int/
```

```
# ./run # testlauf
```

```
$ dig example.com @127.0.0.1
```

```
example.com 86400 IN A 80.12.34.42
```

```
schuettel.ch 259200 IN NS
```

```
  a.ns.example.com
```

Inbetriebnahme

```
for I in /etc/tinydns* /etc/axfrdns*  
    /etc/dnscache; do  
    ln -s $I /service  
done
```

Oder einfach `/etc/init.d/djbdns start # ;)`

Sonstige nette Features

- Gültigkeit bis/ab Zeitpunkt X

```
+foo.bar:1.2.3.4:0:4000000038af1379
```

```
+foo.bar:1.2.3.7::4000000038af1379
```

- Automatische Generierung von RR's
 - Logfiles (ausführlich, aber kryptisch :))
-

Weitere Infos

- <http://tinydns.org/>
 - <http://cr.yp.to/djbdns.html>
 - <http://www.fefe.de/djbdns/>
-