DNS Lab

av

Pål, Ola, Kristoffer

IKT 208

Tjennesteadministrasjon

Veiledet av

Sigurd Munro Aasev

Fakultet for teknologi og realfag

Universitetet i Agder

Grimstad, September 2020

Contents

List of Figures

Introduksjon

Denne oppgaven skal vi lære om DNS-tjenere og finne ut hvordan de fungerer. Vi skal også se på forskjellige DNS-servere til forskjellige domener som UiA, statoil og google. Vi skal til slutt sette opp vår egen DNS-server.

1 Bruk av dig

For å finne informasjon om uia, uninett og google brukte vi kommandoen "dig ANY"

1.1 Uninett

Figure 1: Uninett

1.2 UiA

Figure 2: UiA

ved bruk av "dig ANY uia.no" fant vi ut at de bruker 2 mailtjenester og 4 DNS servere.

1.3   Google

```
ploopyface@ploopyface:~$ dig ANY google.com

; <<>> DiG 9.11.3-1ubuntu1.12-Ubuntu <<>> ANY google.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2231
;; flags: qr rd ra; QUERY: 1, ANSWER: 18, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;google.com.                    IN      ANY

;; ANSWER SECTION:
google.com.            86400    IN      CAA     0 issue "pki.goog"
google.com.            43       IN      AAAA    2a00:1450:400f:80c::200e
google.com.            300      IN      TXT     "v=spf1 include:_spf.google.com ~all"
google.com.            300      IN      TXT     "globalsign-smime-dv=CDYX+XFHUw2wml6/Gb8+59BsH31KzUr6c1l2BPvqKX8="
google.com.            300      IN      TXT     "docusign=1b0a6754-49b1-4db5-8540-d2c12664b289"
google.com.            300      IN      TXT     "facebook-domain-verification=22rm551cu4k0ab0bxsw536tlds4h95"
google.com.            300      IN      TXT     "docusign=05958488-4752-4ef2-95eb-aa7ba8a3bd0e"
google.com.            600      IN      MX      40 alt3.aspmx.l.google.com.
google.com.            600      IN      MX      20 alt1.aspmx.l.google.com.
google.com.            600      IN      MX      10 aspmx.l.google.com.
google.com.            600      IN      MX      30 alt2.aspmx.l.google.com.
google.com.            600      IN      MX      50 alt4.aspmx.l.google.com.
google.com.            60       IN      SOA     ns1.google.com. dns-admin.google.com. 330686346 900 900 1800 60
google.com.            86400    IN      NS      ns2.google.com.
google.com.            86400    IN      NS      ns3.google.com.
google.com.            86400    IN      NS      ns4.google.com.
google.com.            86400    IN      NS      ns1.google.com.
google.com.            234      IN      A       216.58.207.238

;; Query time: 59 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Thu Sep 10 11:54:35 CEST 2020
;; MSG SIZE  rcvd: 649
```

Figure 3: Google

Informasjonen vi får ut er

- MX - E-mail server
- NS - DNStjener
- A - IPv4
- AAAA - IPv6
- SOA - Autoritet

Mail server prioritering
Mail serverene aksesseres med et designert prioritsnummer. lavest blir prioritert først. for å finne denne informasjonen bruker en kommandoen "dig MX domene"

UiA.no

- 5 mx.uhpost.no
- 10 smto.uia.no

uninett.no

- 0 mx12.electric.net.
- 10 uninett-no.mx1.staysecuregroup.com.
- 20 uninett-no.mx2.staysecuregroup.net.
- 999 mx6.electric.net

google.com

- 10 aspmx.l.google.com
- 20 alt1.aspmx.l.google.com

- 30 alt2.aspmx.l.google.com

- 40 alt3.aspmx.l.google.com

- 50 alt4.aspmx.l.google.com

IPv6

for å finne IPv6 adressene brukte vi kommanden "dig AAAA domenenavn"

UiA.no: 2001:700:1500:7250::242:21, 2001:700:1501:d270::220:160, 2001:700:1501:7250::218:21, 2001:700:1501:7250::218:20
2001:700:1500:7250::242:20
uninett.no: hadde ingen
google.com: 2a00:1450:500f:80c::200e

2   Statoil

ved hjelp av traceroute fant vi ut at statoil.com er i Oslo og statoil.no er i Amsterdam.

Vi fant ut at statoil ikke bruker ipv6, men vi fant ipv4. Email tjenesten til statoil er hosta av statoil-no.mail.protection.outlook.com og har 3 navntjenester spdns3.cscdns.net, mailwall1.statoil.com og mail-wall2.statoil.com.

ved hjelp av nmap kommandoen så fant vi ut at statoil.no blokkere pingen vår, men statoil.com så får vi lov og finner ut at port 80/tcp http er åpen og 443/tcp stengt https.

Figure 4: dig statoil.no

```
; <<>> DiG 9.11.3-1ubuntu1.13-Ubuntu <<>> ANY statoil.com
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 8414
;; flags: qr rd ra; QUERY: 1, ANSWER: 7, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 65494
;; QUESTION SECTION:
;statoil.com.                    IN      ANY

;; ANSWER SECTION:
statoil.com.            1783    IN      MX      0 statoil-com.mail.protection.outlook.com.
statoil.com.            4246    IN      NS      ns.domainnetwork.se.
statoil.com.            4246    IN      NS      mailwall1.statoil.com.
statoil.com.            4246    IN      NS      mailwall2.statoil.com.
statoil.com.            4246    IN      NS      ns3.domainnetwork.com.
statoil.com.            4246    IN      NS      ns2.domainnetwork.se.
statoil.com.            130     IN      A       143.97.229.220

;; Query time: 1 msec
;; SERVER: 127.0.0.53#53(127.0.0.53)
;; WHEN: Fri Sep 25 14:29:30 CEST 2020
;; MSG SIZE  rcvd: 239
```

Figure 5: dig statoil.com

3   Bind9 filer

Vi fant alle filene som var lastet ned ved hjelp av "find | grep bind9"

./sys/fs/cgroup/devices/system.slice/bind9.service ./sys/fs/cgroup/devices/system.slice/bind9.service/cgroup.procs ./sys/fs/cgroup/devices/system.slice/bind9.service/devices.deny ./sys/fs/cgroup/devices/system.slice/bind9.service/devi ./sys/fs/cgroup/devices/system.slice/bind9.service/devices.allow ./sys/fs/cgroup/devices/system.slice/bind9.service/task ./sys/fs/cgroup/devices/system.slice/bind9.service/notify_on_release ./sys/fs/cgroup/devices/system.slice/bind9.servic ./sys/fs/cgroup/pids/system.slice/bind9.service ./sys/fs/cgroup/pids/system.slice/bind9.service/cgroup.procs ./sys/fs/cgroup/pids/system.slice/bind9.service/pids.current ./sys/fs/cgroup/pids/system.slice/bind9.service/pids.events ./sys/fs/cgroup/pids/system.slice/bind9.service/tasks ./sys/fs/cgroup/pids/system.slice/bind9.service/notify_on_releas ./sys/fs/cgroup/pids/system.slice/bind9.service/pids.max ./sys/fs/cgroup/pids/system.slice/bind9.service/cgroup.clone_ ./sys/fs/cgroup/systemd/system.slice/bind9.service ./sys/fs/cgroup/systemd/system.slice/bind9.service/cgroup.procs ./sys/fs/cgroup/systemd/system.slice/bind9.service/tasks ./sys/fs/cgroup/systemd/system.slice/bind9.service/notify_on ./sys/fs/cgroup/systemd/system.slice/bind9.service/cgroup.clone_children ./sys/fs/cgroup/unified/sys-tem.slice/bind9.service ./sys/fs/cgroup/unified/system.slice/bind9.service/cgroup.events ./sys/fs/cgroup/u-nified/system.slice/bind9.service/io.pressure ./sys/fs/cgroup/unified/system.slice/bind9.service/cgroup.procs ./sys/fs/cgroup/unified/system.slice/bind9.service/cgroup.max.descendants ./sys/fs/cgroup/unified/sys-tem.slice/bind9.service/cpu.stat ./sys/fs/cgroup/unified/system.slice/bind9.service/memory.pressure ./sys/f-s/cgroup/unified/system.slice/bind9.service/cpu.pressure ./sys/fs/cgroup/unified/system.slice/bind9.service/cgroup.type ./sys/fs/cgroup/unified/system.slice/bind9.service/cgroup.stat ./sys/fs/cgroup/unified/system.slice/bind9.service/cgroup ./sys/fs/cgroup/unified/system.slice/bind9.service/cgroup.freeze ./sys/fs/cgroup/unified/system.slice/bind9.service/cgro ./sys/fs/cgroup/unified/system.slice/bind9.service/cgroup.subtree_control ./sys/fs/cgroup/unified/sys-tem.slice/bind9.service/cgroup.max.depth find: '·/run/user/1000/gvfs': Permission denied ./run/sys-temd/units/invocation:bind9.service ./etc/ppp/ip-up.d/bind9 ./etc/ppp/ip-down.d/bind9 ./etc/systemd/system/multi-user.target.wants/bind9.service ./etc/rc2.d/S01bind9 ./etc/ufw/applications.d/bind9 ./etc/rc5.d/S01bind9 ./etc/insserv.conf.d/bind9 ./etc/rc4.d/S01bind9 ./etc/rc3.d/S01bind9 ./etc/rc6.d/K01bind9 ./etc/rc1.d/K01bind9 ./etc/rc0.d/K01bind9 ./etc/default/bind9 ./etc/network/if-down.d/bind9 ./etc/network/if-up.d/bind9 ./etc/init.d/bind9 ./usr/lib/tmpfiles.d/bind9.conf ./usr/lib/x86_64-linux-gnu/libbind9.so.160.0.6 ./usr/lib/x86_64-linux-gnu/samba/bind9 ./usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_11.so ./usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_9.so ./usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9_10.so ./usr/lib/x86_64-linux-gnu/samba/bind9/dlz_bind9.so ./usr/lib/x86_64-linux-gnu/libbind9.so.160 ./usr/share/bind9 ./usr/share/doc/libl 160 ./usr/share/doc/libbind9-160/copyright ./usr/share/doc/libbind9-160/changelog.Debian.gz ./usr/share/-doc/bind9 ./usr/share/doc/bind9/copyright ./usr/share/doc/bind9/README.gz ./usr/share/doc/bind9/changelog.Debi ./usr/share/doc/bind9/NEWS.Debian.gz ./usr/share/doc/bind9/README.Debian.gz ./usr/share/doc/bind9-doc ./usr/share/doc/bind9-doc/copyright ./usr/share/doc/bind9-doc/changelog.Debian.gz ./usr/share/doc/bind9-doc/arm ./usr/share/doc/bind9-doc/arm/man.named.html ./usr/share/doc/bind9-doc/arm/man.pkcs11-tokens.html ./usr/share/doc/bind9-doc/arm/man.named-journalprint.html ./usr/share/doc/bind9-doc/arm/Bv9ARM.ch ./usr/share/doc/bind9-doc/arm/man.dnssec-importkey.html ./usr/share/doc/bind9-doc/arm/man.dnssec-

keygen.html ./usr/share/doc/bind9-doc/arm/man.dnstap-read.html ./usr/share/doc/bind9-doc/arm/Bv9ARM.ch03.htm
./usr/share/doc/bind9-doc/arm/man.dig.html ./usr/share/doc/bind9-doc/arm/Bv9ARM.ch10.html ./usr/share/doc/bin
doc/arm/man.dnssec-verify.html ./usr/share/doc/bind9-doc/arm/man.nsupdate.html ./usr/share/doc/bind9-
doc/arm/man.isc-hmac-fixup.html ./usr/share/doc/bind9-doc/arm/Bv9ARM.html ./usr/share/doc/bind9-
doc/arm/Bv9ARM.ch04.html ./usr/share/doc/bind9-doc/arm/Bv9ARM.ch11.html ./usr/share/doc/bind9-
doc/arm/man.dnssec-revoke.html ./usr/share/doc/bind9-doc/arm/man.mdig.html ./usr/share/doc/bind9-
doc/arm/man.pkcs11-list.html ./usr/share/doc/bind9-doc/arm/man.named-checkconf.html ./usr/share/doc/bind9-
doc/arm/Bv9ARM.ch09.html ./usr/share/doc/bind9-doc/arm/man.rndc.html ./usr/share/doc/bind9-doc/arm/Bv9ARM
./usr/share/doc/bind9-doc/arm/man.arpaname.html ./usr/share/doc/bind9-doc/arm/man.named-checkzone.html
./usr/share/doc/bind9-doc/arm/man.dnssec-signzone.html ./usr/share/doc/bind9-doc/arm/man.dnssec-
checkds.html ./usr/share/doc/bind9-doc/arm/man.ddns-confgen.html ./usr/share/doc/bind9-doc/arm/man.pkcs11-
destroy.html ./usr/share/doc/bind9-doc/arm/man.dnssec-keyfromlabel.html ./usr/share/doc/bind9-doc/arm/man.dnssec
dsfromkey.html ./usr/share/doc/bind9-doc/arm/man.named-nzd2nzf.html ./usr/share/doc/bind9-doc/arm/man.nsec3ha
./usr/share/doc/bind9-doc/arm/Bv9ARM.ch08.html ./usr/share/doc/bind9-doc/arm/man.rndc.conf.html
./usr/share/doc/bind9-doc/arm/man.named.conf.html ./usr/share/doc/bind9-doc/arm/man.pkcs11-keygen.html
./usr/share/doc/bind9-doc/arm/man.genrandom.html ./usr/share/doc/bind9-doc/arm/Bv9ARM.ch02.html
./usr/share/doc/bind9-doc/arm/Bv9ARM.ch01.html ./usr/share/doc/bind9-doc/arm/man.rndc-confgen.html
./usr/share/doc/bind9-doc/arm/Bv9ARM.ch07.html ./usr/share/doc/bind9-doc/arm/Bv9ARM.ch12.html
./usr/share/doc/bind9-doc/arm/man.host.html ./usr/share/doc/bind9-doc/arm/Bv9ARM.ch06.html ./usr/share/doc/bi
doc/arm/man.named-rrchecker.html ./usr/share/doc/bind9-doc/arm/notes.html ./usr/share/doc/bind9-
doc/arm/man.dnssec-coverage.html ./usr/share/doc/bind9-doc/arm/man.delv.html ./usr/share/doc/bind9-
doc/arm/man.dnssec-settime.html ./usr/share/doc/bind9-doc/arm/man.dnssec-keymgr.html ./usr/share/doc/bind9-
doc/arm/man.nslookup.html ./usr/share/doc/bind9-doc/misc ./usr/share/doc/bind9-doc/misc/rfc-compliance.gz
./usr/share/doc/bind9-doc/misc/master.zoneopt ./usr/share/doc/bind9-doc/misc/tcp-fast-open ./usr/share/doc/bind9-
doc/misc/docbook-grammars.pl ./usr/share/doc/bind9-doc/misc/redirect.zoneopt ./usr/share/doc/bind9-
doc/misc/format-options.pl ./usr/share/doc/bind9-doc/misc/hint.zoneopt ./usr/share/doc/bind9-doc/misc/sdb.gz
./usr/share/doc/bind9-doc/misc/Makefile.in ./usr/share/doc/bind9-doc/misc/stub.zoneopt ./usr/share/doc/bind9-
doc/misc/ipv6.gz ./usr/share/doc/bind9-doc/misc/dnssec ./usr/share/doc/bind9-doc/misc/delegation-
only.zoneopt ./usr/share/doc/bind9-doc/misc/migration-4to9 ./usr/share/doc/bind9-doc/misc/docbook-
options.pl.gz ./usr/share/doc/bind9-doc/misc/roadmap ./usr/share/doc/bind9-doc/misc/forward.zoneopt
./usr/share/doc/bind9-doc/misc/sort-options.pl ./usr/share/doc/bind9-doc/misc/docbook-zoneopt.pl ./usr/share/doc/b
doc/misc/options.gz ./usr/share/doc/bind9-doc/misc/slave.zoneopt ./usr/share/doc/bind9-doc/misc/static-
stub.zoneopt ./usr/share/doc/bind9-doc/misc/in-view.zoneopt ./usr/share/doc/bind9-doc/misc/migration.gz
./usr/share/doc/bind9utils ./usr/share/doc/bind9utils/copyright ./usr/share/doc/bind9utils/changelog.Debian.gz
./usr/share/doc/bind9-host ./usr/share/doc/bind9-host/copyright ./usr/share/doc/bind9-host/changelog.Debian.gz
./usr/share/man/man1/bind9-config.1.gz ./usr/bin/bind9-config ./lib/systemd/system/bind9.service ./lib/systemd/syste
resolvconf.service ./lib/systemd/system/bind9-pkcs11.service ./var/lib/bind/bind9-default.md5sum ./var/lib/systemd/de
systemd-helper-enabled/bind9.service.dsh-also ./var/lib/systemd/deb-systemd-helper-enabled/bind9-resolvconf.service.ds
also ./var/lib/systemd/deb-systemd-helper-enabled/multi-user.target.wants/bind9.service ./var/lib/systemd/deb-
systemd-helper-enabled/bind9-pkcs11.service.dsh-also ./var/lib/dpkg/info/bind9.postrm ./var/lib/dpkg/info/bind9-
host.list ./var/lib/dpkg/info/bind9.postinst ./var/lib/dpkg/info/bind9utils.md5sums ./var/lib/dpkg/in-
fo/bind9utils.postinst ./var/lib/dpkg/info/bind9utils.list ./var/lib/dpkg/info/libbind9-160:amd64.list ./var/lib/dpkg/info
160:amd64.symbols ./var/lib/dpkg/info/libbind9-160:amd64.shlibs ./var/lib/dpkg/info/bind9.list ./var/lib/dpkg/info/bin
host.md5sums ./var/lib/dpkg/info/libbind9-160:amd64.triggers ./var/lib/dpkg/info/bind9.md5sums ./var/lib/dpkg/info/
160:amd64.md5sums ./var/lib/dpkg/info/bind9.config ./var/lib/dpkg/info/bind9.prerm ./var/lib/dpkg/in-
fo/bind9.conffiles ./var/lib/dpkg/info/bind9utils.prerm ./var/lib/dpkg/info/bind9-doc.list ./var/lib/dpkg/info/bind9-
doc.md5sums ./var/lib/dpkg/info/bind9.templates ./var/cache/apt/archives/bind9-doc_1%3a9.11.3+dfsg-
1ubuntu1.13_all.deb ./var/cache/apt/archives/bind9utils_1%3a9.11.3+dfsg-1ubuntu1.13_amd64.deb ./var/cache/apt/a
1ubuntu1.13_amd64.deb

4   forklaring av bind

BIND (Berkley Internet Name Domain) er en referanse implementering av DNS protokollene og gir tilgang på en rekke komponenter tilknyttet DNS. BIND er en DNS server som er vidt utbredt i internett og brukes i flesteparten (ca 80% i følge isc.org 01.2013) av DNS tjenerene rundt om i verden. Så hvordan virker BIND? Siden bind er en DNS server/navnetjener har den til hensikt og oppgave å oversette navn til adresser i internett og omvendt, samt route mail til riktig plass. Ved å ha flere navneservere rundt om i verden som har ansvar for sine adresser og navnelister vil man til enhver tid kunne slå opp og få

informasjonen man trenger ved å sende request til disse når man vil besøke nettsider. Grunnen til at det er lagt opp på denne måten er at det ville vært lite hensiktsmessig å ha denne listen på alle pcer rundt om i verden, samt veldig ressurskrevende å oppdatere alle lister på alle maskiner rundt om. Derfor er dette ansvaret fordelt ut ansvarlige rundt om i verden som hoster sine globale navneservere som til enhver tid er oppdaterte.
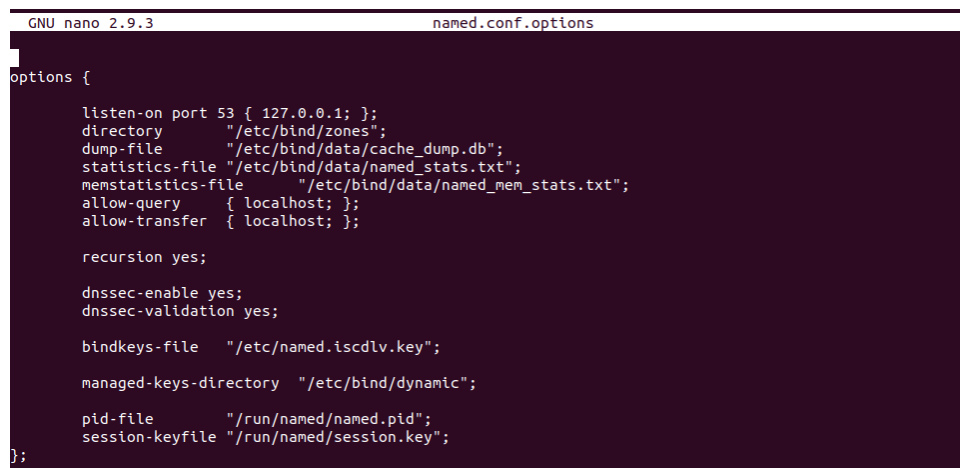
5 Bind oppsett

Figure 6: Local

Figure 7: Options

```
  GNU nano 2.9.3                              db.1.nettlab.grm

$TTL    604800
$ORIGIN 1.nettlab.grm.
@               3600     IN      SOA     ns1.1.nettlab.grm. dathost.1.nettlab.grm. (
                              3         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL

                3600     IN      NS      ns1.
                3600     IN      NS      ns2.

                3600     IN      MX      10      mail1.
                3600     IN      MX      20      mail2.

ns1.            3600     IN      A       127.1.0.11
ns2.            3600     IN      A       127.1.0.42
mail1.          3600     IN      A       127.1.0.12
mail2.          3600     IN      A       127.1.0.43


klient1         3600     IN      A       127.1.0.10
klient2         3600     IN      A       127.1.0.2
klient3         3600     IN      A       127.1.0.3
klient4         3600     IN      A       127.1.0.4
klient5         3600     IN      A       127.1.0.5
klient6         3600     IN      A       127.1.0.6
klient7         3600     IN      A       127.1.0.7
```

Figure 8: zonefile

vi fikk dessverre ikke Bind til å fungere. vi vet ikkje hvorfor vi ikke får ut informasjonen ved hjelp av
"dig @localhost ANY 1.nettlab.grm". Vi prøvde mye frem og tilbake, med forskjellige tips fra forskjellige
personer, men etter 3 timer med feilsøking ga vi opp.