DNS 101

Laborationsinstruktioner

2024-01-24

Innehåll

1 DNS **1**
- Innan ni börjar . . . 1
- Uppgift 1 . . . 1
  - Auktoritativ namnserver - Primary . 1
- Uppgift 2 . . . 2
  - Auktoritativ namnserver - Secondary 2

2 DNSSEC **3**
- Uppgift 3 . . . 3
  - Signera er domän . . . 3
  - Bonus: Felsök er domän trasiga domän . . . 3

3 DNS cheat sheet **4**
- KNOT . . . 4
  - Exempel på SOA . . . 4
  - Exempel på Konfiguration-statements (Primär/Master) . . . 4
  - Exempel på Konfiguration (Sekundär/Slav) 5
  - TSIG . . . 6
  - Exempel på Konfiguration (DNSSEC) 6
- Tips och trix . . . 6
  - Tänk på att . . . 6
  - Felsökning . . . 7

Kapitel 1: DNS

Innan ni börjar

Ni har åtkomst till era servrar via den SSH-nyckel ni fått. Användaren är 'ubuntu' på alla maskiner och ni har root-access via *sudo*. Ändringar i filer gör ni via valfri tillgänglig texteditor (som vim eller nano). Nyttiga sökvägar, kommandon och exempel finner ni under Sektion 3.
Terminologi. I en grupp namnservrar som är auktoritativa för samma zon är det i de flesta fall en av dem som har den gällande zonfilen, i vilken man gör ändringar. De andra kopierar endast över zondata från denna namnserver. Den styrande namnservern kallas *Primär* eller *Master* och de andra *Sekundär* eller *Slave*. Båda termer kan förekoma i dokumentation och konfiguration, beroende på vilken programvara som används eller när dokumentationen skrevs. De har dock i praktiken samma tekniska betydelse.

Uppgift 1

Auktoritativ namnserver - Primary

1. Konfigurera er namnserver att vara primär namnserver för er tilldelade domän
   - Logga in på er *DNS Primary*
   - Skapa en zonfil för er domän med all nödvändig information (för enkelhetens skull, sätt NS till ns1.<domän>)
   - Lägg till domänen som masterzon i konfigurationen för KNOT
   - Starta om KNOT
   - Kontrollera med DIG att namnservern svarar korrekt
2. Lägg till en pekare för en websida under er domän (med och utan www)
   - Lägg till pekare för webservern (IPv4)
   - Ladda om KNOT
   - Kontrollera med DIG att namnservern svarar korrekt
   - Testa att surfa till <*domän*>
3. Ändra webpekaren för www.<domännamn> till ett CNAME
   - Byt ut A-pekaren mot en CNAME-pekare
   - Ladda om KNOT
   - Kontrollera med DIG att namnservern svarar korrekt
   - Testa att surfa till er websida (med och utan www)
4. Lägg till en mailpekare för er domän
   - Lägg till en MX-pekare i zonen
   - Lägg till en A-pekare för MX-pekarens namn
   - Ladda om KNOT
   - Kontrollera med DIG att namnservern svarar korrekt

Uppgift 2

Auktoritativ namnserver - Secondary

1. Lägg till en sekundär namnserver (slavserver) för er domän
   - *På primära namnservern:* Tillåt zonöverföring till *sekundära namnservern* i konfigurationen för KNOT
   - *På primära namnservern:* Lägg till NS och glue för sekundära namnservern i zonfilen
   - *På sekundära namnservern:* Lägg till domänen som slavzon i konfigurationen för KNOT
   - Ladda om KNOT på både primära och sekundära namnservern
   - Kontrollera med DIG att båda namnservrar svarar korrekt
2. Säkra upp zonöverföringen med TSIG
   - *På primära namnservern:* Generera en TSIG-nyckel
   - *På primära namnservern:* Lägg till nyckeln i konfigurationen för KNOT
   - *På primära namnservern:* Ändra så att zonöverföring bara tillåts med TSIG
   - *På slavservern:* Lägg till nyckeln i konfigurationen för KNOT
   - Ladda om KNOT på både primära och sekundära namnervern
   - Verifiera att det fungerar
     - *På primära namnservern:* lägg till en valfri TXT-pekare i zonen
     - *På primära namnservern:* Ladda om KNOT
     - Kontrollera med DIG att båda namnservrar uppdaterats och svarar korrekt

Kapitel 2: DNSSEC

Uppgift 3

Signera er domän

1. Skapa en policy för DNSSEC signering
2. Skapa en ny template för zonen med lämpliga parametrar
3. Kontrollera med DIG att zonen blivit signerad
4. Generera ett DS-record att skicka upp till föräldrazonen
5. Skicka DS-record till kursinstruktör
6. Vänta på ett OK från kursinstruktör att DS ligger i föräldrazonen
7. Kontrollera med DIG *mot en extern resolver* att zonen validerar
8. Undersök zonen med DNSVIZ

Bonus: Felsök er domän trasiga domän

1. Be kursinstruktören ha sönder ert DS
2. Undersök med DIG *mot en extern resolver* vad ni får för svar
3. Verifiera med DIG och flaggan +cd för att påvisa att just DNSSEC är problemet
4. Undersök zonen med DNSVIZ
5. Be kursinstruktören ha laga ert DS
6. Kontrollera med DIG *mot en extern resolver* att zonen fungerar igen
7. Undersök zonen med DNSVIZ

Kapitel 3: DNS cheat sheet

KNOT

Nedan tillhandahålls några tips och exempel relevanta för laborationen. Full dokumentation av KNOT 3.3 går att finna här: https://www.knot-dns.cz/docs/3.3/html/

Filer och sökvägar

/etc/knot/knot.conf.local	Konfigurationsfil för knot
/var/lib/knot/	Katalog för zonfiler med tillhörande metadata

Notera. Tecken för att kommentera text skiljer sig mellan konfigurationsfiler och zonfiler

- konfigurationsfil: // kommenterar all följande text på raden. Det går också att använda /* */ för att konmmentera hela block.
- zonfil: ; för att kommentera bort rad

Exempel på SOA

```
minimal.examples.nu. 3600 IN SOA ns1.minimal.examples.nu. hostmaster.examples.nu. (
                        1606898653 ; serial
                        4400       ; refresh (4 hours)
                        3600       ; retry (1 hour)
                        604800     ; expire (1 week)
                        600        ; minimum (1 hour)
                        )
```

Notera. Kan även skrivas som en rad

```
minimal.examples.nu. 3600 IN SOA ns1.group1.examples.nu. hostmaster.examples.nu. 1606898653 4400 3600 604800 3600
```

Exempel på Konfiguration-statements (Primär/Master)

KEY

```
key:
  - id: tsig-key
    algorithm: hmac-sha256
    secret: 4Tc0K1QkcMCs7cOW2LuSWnxQY0qysdvsZlSb4yTN9pA=
```

ACL utan TSIG

```
acl:
    - id: ip-axfr
      address: 34.244.23.7
      action: [transfer, notify]
```

ACL med TSIG

```
acl:
    - id: tsig-axfr
```

```
      key: tsig-key
      action: [transfer, notify]
```

ACL (regel: deny all)

```
    - id: deny_all
      address: 0.0.0.0/0
      deny: on
```

Notera. Man kan kombinera flera ACL och de appliceras i ordning. 'deny all' bör därför stå sist.

Zone

```
zone:
    - domain: minimal.examples.nu
      template: default
      acl: [ip-axfer, deny_all]
```

Notera. Ersätt ip-axfer med tsig-axfer för att tvinga TSIG

ACL utan TSIG

```
acl:
    - id: ip-axfr
      address: 3.254.134.160
      action: [transfer, notify]
```

ACL med TSIG

```
acl:
    - id: tsig-axfr
      key: tsig-key
      action: [transfer, notify]
```

Exempel på Konfiguration (Sekundär/Slav)

Remote (primär/master) utan TSIG

```
remote:
  - id: ns1
    address: 3.254.134.160@53
```

Remote (primär/master) med TSIG

```
remote:
  - id: ns1
    address: 3.254.134.160@53
    key: tsig-key
```

Zone

```
zone:
  - domain: minimal.examples.nu
    master: ns1
```

TSIG

Använd *keymgr* för att generera en tsig.

```
keymgr -t <namn-på-tsig>
```

Output är formaterat för KNOT och går bra att klistra in direkt i konfigurationen. Vill man ha nyckeln i en fil för att kunna testa AXFR med *dig -k <nyckelfil> <domän> axfr* behöver den ha det format BIND använder:

```
key "tsig-key" {
    algorithm hmac-sha256;
    secret "4Tc0K1QkcMCs7cOW2LuSWnxQY0qysdvsZlSb4yTN9pA=";
};
```

Exempel på Konfiguration (DNSSEC)

Policy

```
policy:
    - id: ecdsa
      algorithm: ECDSAP256SHA256
      ksk-lifetime: 0
```

Template

```
template:
    - id: signed
      storage: "/var/lib/knot"
      file: "%s.zone"
      zonefile-sync: -1
      serial-policy: unixtime
      journal-content: changes
      zonefile-load: difference-no-serial
      semantic-checks: true
      dnssec-signing: on
```

Zone

```
zone:
    - domain: minimal.examples.nu
      template: signed
      acl: tsig-axfr
```

Notera. För att inte zonfilen inte ska fyllas med DNSSEC-records, som genereras automatiskt, så låter vi allt sånt hamna i journalfilen (därav *zonefile-sync: -1*, *journal-content: changes* och *zonefile-load: difference-no-serial*)

Tips och trix

Tänk på att

- Uppdatera zonens serienummer vid varje ändring
- Kontrollera zon och konfiguration med *knotc check-zone* / *knotc check-conf*
- Felorsaken kan ofta hittas i /var/log/syslog

Felsökning

Lokala verktyg

knotc check-conf	Kontrollerar konfiguration i knot.conf
knotc check-zone <zonnamn>	Kontrollerar att KNOT kan läsa och ladda zonen (ingen output = syntax ok)
service knot status	Visar status för KNOT (i.e. om KNOT är igång eller inte)
knotc reload	Laddar om KNOT efter ändringar i zoner och/eller configuration

Externa verktyg

https://zonemaster.se	kontrollerar uppsättningen av en zon. OBS. Cachar resultatet från ett test i ca 10 minuter.
https://zonemaster.net	Alternativ instans av zonemaster.se.
https://dnsviz.net	Visar delegeringsträd grafiskt. Speciellt bra vid felsökning av DNSSEC. Man måste aktivt be verktyget göra om ett test, annars visas resultat från det senaste testet