DNS

Domain Name System

Functie DNS

- **Een nameserver is een server waaraan je vragen kan stellen zoals**
  - Waar moet ik de mail voor kdg.be naartoe sturen?
  - Wat is het IP adres van www.kdg.be?
- **Als we het IP adres kennen, kunnen we communiceren met HTTP, FTP, TELNET,...**
- **Mensen hebben van nature uit meer aanleg om een naam te onthouden dan een reeks getalletjes.**
  - DNS vertaalt voor ons namen naar nummers

Zonder DNS

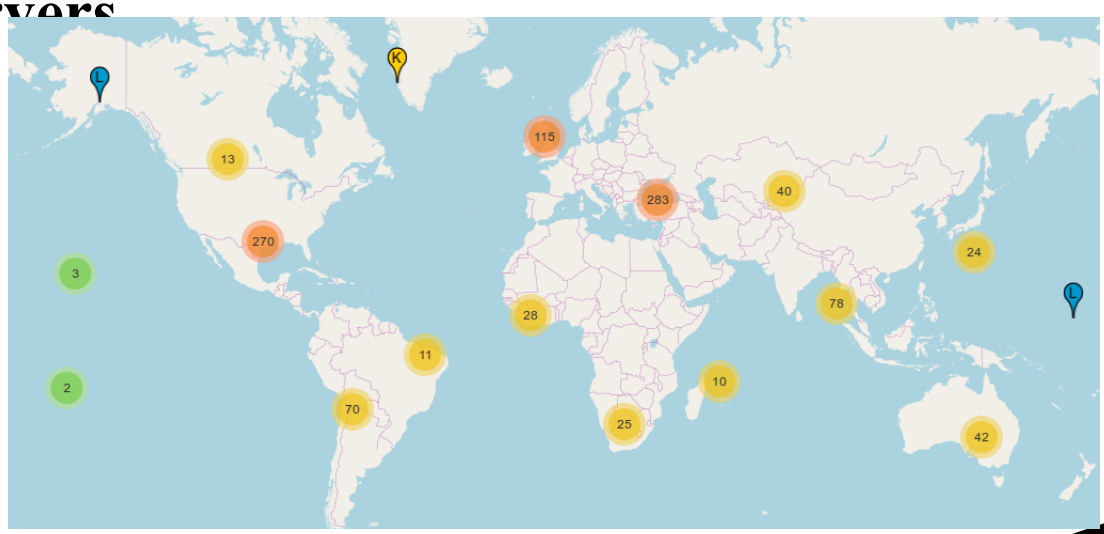
- **Elke host houdt zelf een lijst bij van welke namen welke IP adressen betekenen**
- **In de begindagen van internet werd deze lijst doorgecopieerd tussen alle servers**
- **Windows: hosts.sam en lmhosts.sam (netbios naam)**
  - `Windows 95/98 in c:\windows`
  - `WinNT/2k c:\winnt\system32`
  - `Win2k8 c:\windows\system32\drivers`
  - `bv   172.17.164.1 hebedu01.kdg.be`
- **Unix: /etc/hosts**
  - `bv   172.17.164.1 hebedu01 hebedu01.kdg.be`
- **Cisco**
  - `Router(config)# ip host lab_d 210.93.205.1 204.204.7.2`

Nameservers

- **Een nameserver houdt een lijst bij van namen en ip nummers (deze worden tussen nameservers geupdated). In deze lijst staan:**
  - computers
  - andere nameservers
  - mailservers
- **De meeste ISP's voorzien minstens 2 domain name servers die beiden dezelfde lijsten bijhouden. Deze kan je ingeven als DNS 1 en DNS 2**
- **Een top level nameserver houdt informatie bij over één bepaald domein. Uiteraard zijn er meerdere top level nameservers.**

Hierarchie

- **Root servers .**
  - 13 logische servers
  - [a-m].root-servers.net.
  - 1551 fysieke servers *
- **TLD**
  Top Level Domain Servers
  - .com. .org. .be. ,...
- **Sub level DNS**
  - kdg.be, ...

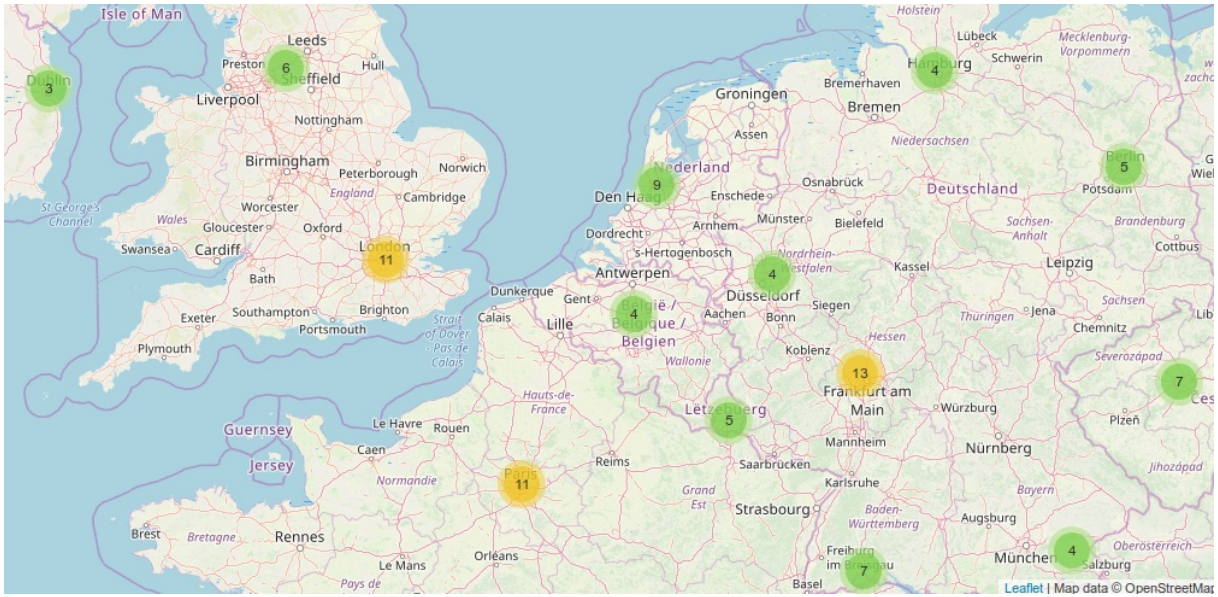


- * sept 2022 www.root-servers.org

Root server

- **Voorbeeld root server cache record**

```
.                       3600000  IN  NS     A.ROOT-SERVERS.NET.
A.ROOT-SERVERS.NET.     3600000  A          198.41.0.4
A.ROOT-SERVERS.NET.     3600000  AAAA       2001:503:BA3E::2:30
```

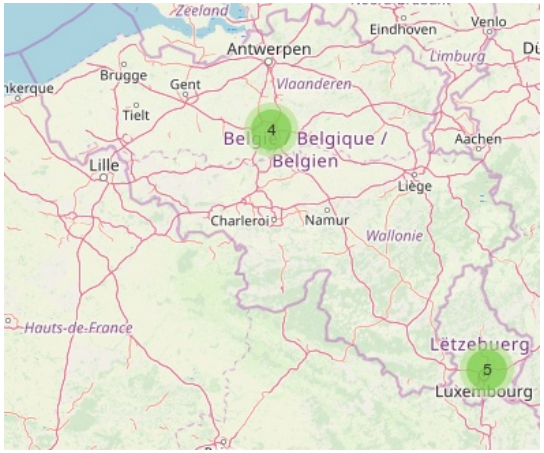


(c) 2019 OpenStreetMap www.root-servers.org

Voorbeeld .be Top Level Domain

- **Uit ftp://ftp.internic.net/domain/root.zone:**

```
be.        172800    IN  NS a.ns.dns.be.
be.        172800    IN  NS b.ns.dns.be.
be.        172800    IN  NS d.ns.dns.be.
be.        172800    IN  NS x.ns.dns.be.
be.        172800    IN  NS london.ns.dns.be.
be.        172800    IN  NS brussels.ns.dns.be.
```



Voorbeeld indeling

- **Voorbeeld van een domeinnaam is www.kdg.be.**
- **Wanneer we http:// hiervoor zetten, krijgen we een URL. Deze domeinnaam bestaat uit verschillende onderdelen.**
  - Sub Level Domain: kdg
  - Top Level Domain: be
  - Root: .

Eigenaar DNS nakijken met whois

- **Je kan nakijken door wie een domein geregistreerd is door het commando whois domeinnaam te geven, je krijgt dan ook het adres te zien van de administrator van het domein.**
- **bv** `whois kdg.be.`

- In windows installeer je best de sysinternal tools suite hiervoor.

Soorten nameserver configuraties

- **Primary Master Nameserver**
  - Kennis over een geregistreerde zone
- **Secondary Master Nameserver**
  - Copy van een Primary Master
- **Caching Nameserver**
  - Onthoudt eerdere aanvragen
  - Snelheidswinst

Soorten nameserver configuraties

- **Hybride Nameserver**
  - Zowel Primary of Secondary als Caching
  - Nameservers zijn meestal ook Caching
- **Stealth Primary Nameserver**
  - Primary Nameserver enkel voor intern gebruik
  - Nameservers van provider zijn Slaves voor jouw zone
  - Alle queries voor jouw zone vanuit internet gebeuren naar de DNS servers van de provider

DNS testen met NSLOOKUP

```
kdguntu@kdguntu:~$ nslookup kdg.be.
Server:    127.0.0.1
Address:   127.0.0.1#53

Non-authoritative answer:
Name: kdg.be
Address: 109.74.196.225
```

- **Opmerking: NSLOOKUP heeft ook een interactieve modus met meer opties. Deze krijg je als je geen argumenten meegeeft. Om deze te verlaten tik je exit.**

Werking en timing testen met "dig"

```
kdguntu@kdguntu $ dig kdg.be
; <<>> DiG 9.8.1-P1 <<>> kdg.be
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 44761
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
;kdg.be.                        IN    A

;; ANSWER SECTION:
kdg.be.                 3600    IN    A     109.74.196.225

;; AUTHORITY SECTION:
kdg.be.                 67379   IN    NS    ns2.belnet.be.
kdg.be.                 67379   IN    NS    ns2.kdg.be.
kdg.be.                 67379   IN    NS    ns1.kdg.be.
kdg.be.                 67379   IN    NS    ns1.belnet.be.

;; Query time: 31 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Aug 21 21:45:45 2013
;; MSG SIZE  rcvd: 119
```

Caching nameserver met dig

```
kdguntu@kdguntu $ dig kdg.be
; <<>> DiG 9.8.1-P1 <<>> kdg.be
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 3008
;; flags: qr rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 4, ADDITIONAL: 0

;; QUESTION SECTION:
;kdg.be.                        IN    A

;; ANSWER SECTION:
kdg.be.                 3338   IN    A     109.74.196.225

;; AUTHORITY SECTION:
kdg.be.                 67117  IN    NS    ns2.kdg.be.
kdg.be.                 67117  IN    NS    ns2.belnet.be.
kdg.be.                 67117  IN    NS    ns1.kdg.be.
kdg.be.                 67117  IN    NS    ns1.belnet.be.

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Aug 21 21:50:07 2013
;; MSG SIZE  rcvd: 119
```

Opgelet! dig naar onbestaand domein

```
kdguntu@kdguntu:~$ dig kdgbestaatniet.be

; <<>> DiG 9.8.1-P1 <<>> kdgbestaatniet.be
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NXDOMAIN, id: 3507
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 1, ADDITIONAL: 0

;; QUESTION SECTION:
;kdgbestaatniet.be.          IN    A

;; AUTHORITY SECTION:
be.                 600   IN    SOA   a.ns.dns.be. tech.dns.be. 1010376465 3600 1800 2419200 600

;; Query time: 15 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Wed Aug 21 21:53:16 2013
;; MSG SIZE  rcvd: 85
```

Opzoeken ip adres met nslookup

- Met "nslookup www.kdg.be" vraag je aan een nameserver welke ip een bepaalde computer heeft.
- Je krijgt dan als antwoord van een dns server het ip nummer.
- Met het commando "ping www.kdg.be", vraag je eerst aan de DNS server de IP van www.kdg.be en stuur je daarna een ICMP echo bericht naar het IP adres. Je krijgt dus ook het IP adres te zien.
- Bij een nslookup wordt de computer zelf niet gecontacteerd.

Snelheid: Interne/externe DNS

- **Wanneer je een DNS server installeert binnen je bedrijf kan je communiceren met de naam in plaats van met een nummer.**
- **Om sneller internetverkeer te hebben op je bedrijf valt het te overwegen om ook een DNS server te voorzien voor extern verkeer. Wanneer deze server de meest gebruikte domain names zelf vertaalt naar ip adressen, zullen de clients sneller bediend zijn.**

/etc/resolv.conf

- **Configuratiebestand in Linux dat aangeeft waar een computer moet zoeken naar NAAM -IP vertalingen**

```
search kdg.be                 # eerst zoeken in lokaal domein
nameserver 8.8.8.8
nameserver 8.8.4.4
options edns0                 # ondersteunt ook de nieuwe DNS
                              # extensies (zoals .vlaanderen)
```

/etc/systemd/resolved.conf

- **Default settings voor systemd DNS servers en domains**
- **bv DNS=192.168.56.100**
- root@mail:/home/jancelis# systemd-resolve --status
- Global
- DNS Servers: 192.168.56.100
- DNSSEC NTA: 10.in-addr.arpa
- 16.172.in-addr.arpa
- 168.192.in-addr.arpa
- ...

/etc/nsswitch.conf

- **Zoekvolgorde**
  - files: /etc/hosts
  - mdns4_minimal: (zoekt enkel .local domeinen)
  - dns: via nameserver
  - myhostname: enkel /etc/hostname

DNS server caching

- **Een caching nameserver houdt bij welk IP adres bij een naam hoort, zodat er geen 2de keer aan een "hogerliggende" DNS server een DNS query moet gebeuren.**
- **Hoe lang deze aangevraagde gegevens geldig zijn, hangt af van de Time To Live TTL die gedefinieerd is bij de zone**
  - De TTL van www.kdg.be is 1 uur (3600).
    Dat betekent dat een caching nameserver de naam *www.kdg.be* 1 uur lang gekoppeld houdt aan het IP adres `109.74.196.225`
    Daarna moet opnieuw het mogelijk nieuwe adres aangevraagd worden

Snelheid op de client

- **Je kan de snelheid verhogen door in het hosts bestand van je clients de namen en ip-nummers van veel gebruikte servers zelf in te geven. Er bestaan ook enkele freeware programma's die dit voor jou doen (zogenaamde internet-versnellers).**

BIND configuratie /etc/bind/named.conf

```
zone "kdg.be" {
        type master;
        file "/etc/bind/kdg.be";
};
```

```
zone "1.168.192.in-addr.arpa" {
        type master;
        file "/etc/bind/1.168.192.in-addr.arpa";
};
```

Resource records

- **Bevatten de informatie die wordt doorgegeven naar andere nameservers**
- **Bevatten buiten IP nummer en naam extra informatie zoals:**
  - Time_to_Live: Geeft in seconden aan hoe snel informatie kan veranderen en dus wanneer informatie moet geupdated worden: bv 86400 (elke dag)
    - Mag ook met tijdsafkortingen als volgt:
      - 1h één uur
      - 2d twee dagen
      - 3w drie weken
  - Class: altijd IN bij Internetverkeer

Resource records (2)

- Type: Soort informatie
  - SOA:(Start Of Authority) gegevens over deze zone
  - A: (Address) IP adres voor een host
  - AAAA: (Address) IP v6 adres voor een host
  - MX: (Mail Exchange) Mailontvanger voor een domein
  - NS: (Name Servers) Andere nameservers die de DNS kent
  - DS: (Delegation Signer) DNSSEC sleutel info voor sub zone
  - CNAME: (Canonical Name) alias voor een domein, wegwijzer naar een met A gedefinieerd domein
  - PTR: alias voor IP adres (voor reverse DNS)
  - SRV: wijst naar een Domain Controller in de zone
  - TXT: optionele tekst
  - HINFO: optionele info over hardware/OS
- Value: Waarde voor bovenstaande types

Resource records bij linux BIND

```
$TTL    604800 ; hoelang cachen van deze info (default)
@ IN SOA kdg.be. root.kdg.be.( ; whois post
                    ; naar root@kdg.be                2022091801
        ; serial YYYYMMDD+revision
           604800       ; refresh
           86400        ; retry 1 Hour
           2419200      ; expire 1 Month
           604800     ); minimum 1 Week
   @          IN   NS  ns1.kdg.be.
   ns1        IN   A       192.168.1.101
   ns2        IN   A       192.168.1.102
   server   IN A   192.168.1.200
```

Forward Lookup Zone nameservers

- **Nameserver(s) definiëren**
  - met NS (minstens spatie of tab of @ ervoor)
    - NS ns1.kdg.be.
    - NS ns2.kdg.be.
  - én als A record
    - ns1 IN A 192.168.1.1
    - ns2 IN A 192.168.1.2

Forward Lookup Zone

- **Mailserver(s) definiëren**
  - met MX (minstens spatie of tab of @ ervoor)
  - en een waardefactor (kleiner krijgt voorrang)
    - MX 10 mail1.kdg.be.
    - MX 20 mail2.kdg.be.
  - én als A record
    - mail1 IN A 192.168.1.3
    - mail2 IN A 192.168.1.4

Reverse name resolution

- Vertalen van IP adressen naar namen
- Servers op internet gebruiken deze omgekeerde functie om na te kijken of je niet aan het knoeien bent
- Omdat je moeilijk aan elke DNS server op internet kan vragen of deze een bepaald adres kent, bestaat er het speciaal voor reverse name resolution ontworpen domein in-addr.arpa
- De subdomeinen van in-addr.arpa geven het ip adres weer.

- Zoeken wie ip 193.168.1.3 heeft, gebeurt door te zoeken in het ~~domein~~ 1.168.193.in-addr.arpa

Reverse Lookup Zone

- **IP naar naam vertalen**

```
$TTL    604800
@ IN SOA kdg.be. root.kdg.be. (
      2022091801  ; versienummer
      604800    ; refresh
      86400     ; retry 2 Hours
      2419200   ; expire 1 Week
      604800 )    ; minimum 1 Day
          IN NS ns1.
          IN NS ns2.
    101   IN PTR ns1.kdg.be
102       IN PTR ns2.kdg.be
200       IN PTR server.kdg.be
```

Bind hints

- $TTL 0 is niet cachen
- Op het einde van een domeinnaam komt een punt
- Versienummer verhogen als je een aanpassing doet
- Elke A record in een domein heeft een PTR record in reverse

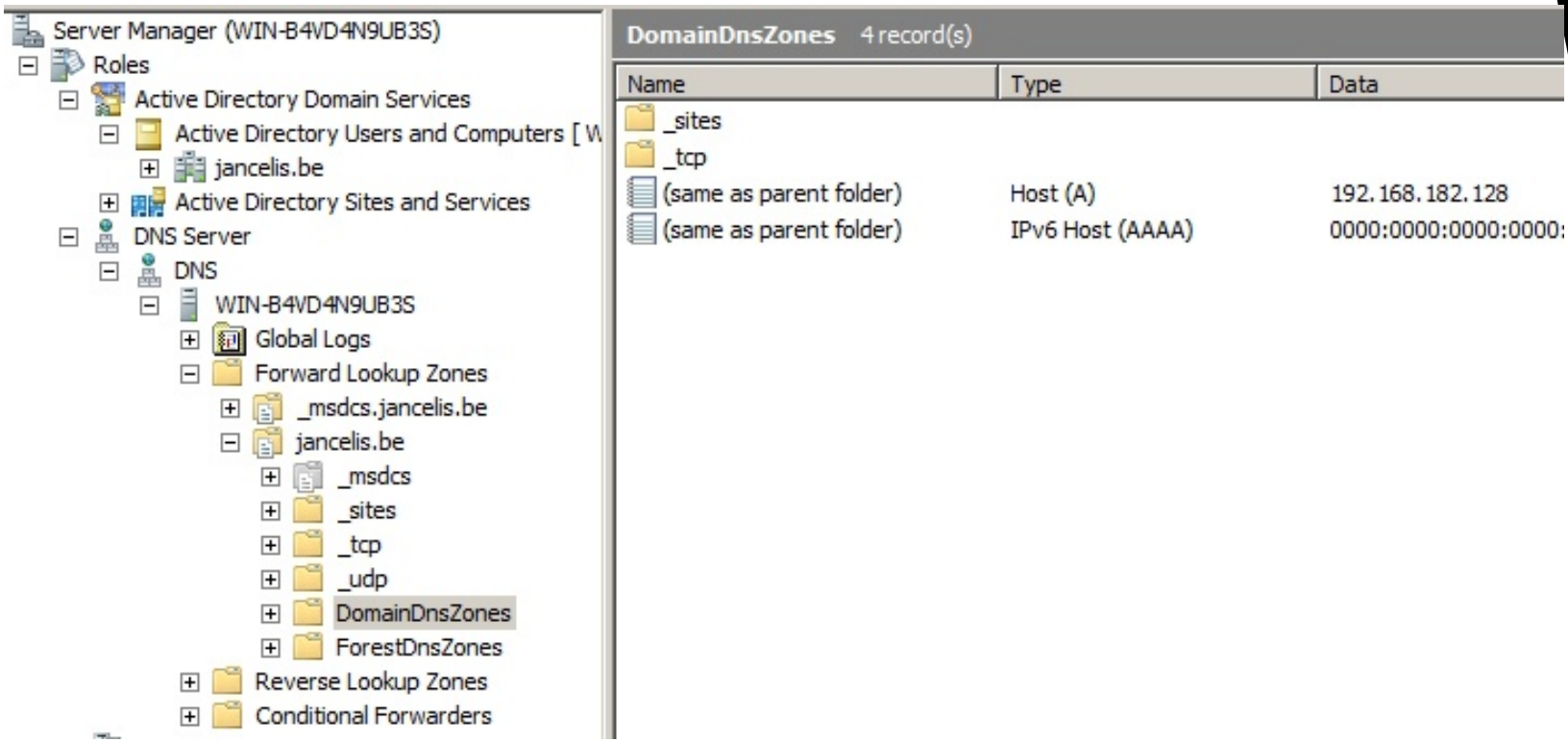
Nakijken configuratie bind9

- **named-checkconf /etc/bind/named.conf**
  - Geen melding is OK
- **named-checkzone kdg.be /etc/bind/kdg.be**

  zone kdg.be/IN: loaded serial 2020101801
- **OK**
- **named-checkzone 1.168.192.in-addr.arpa /etc/bind/1.168.192.in-addr.arpa**
- **zone 1.168.192.in-addr.arpa/IN: loaded serial 2020101801**
- **OK**

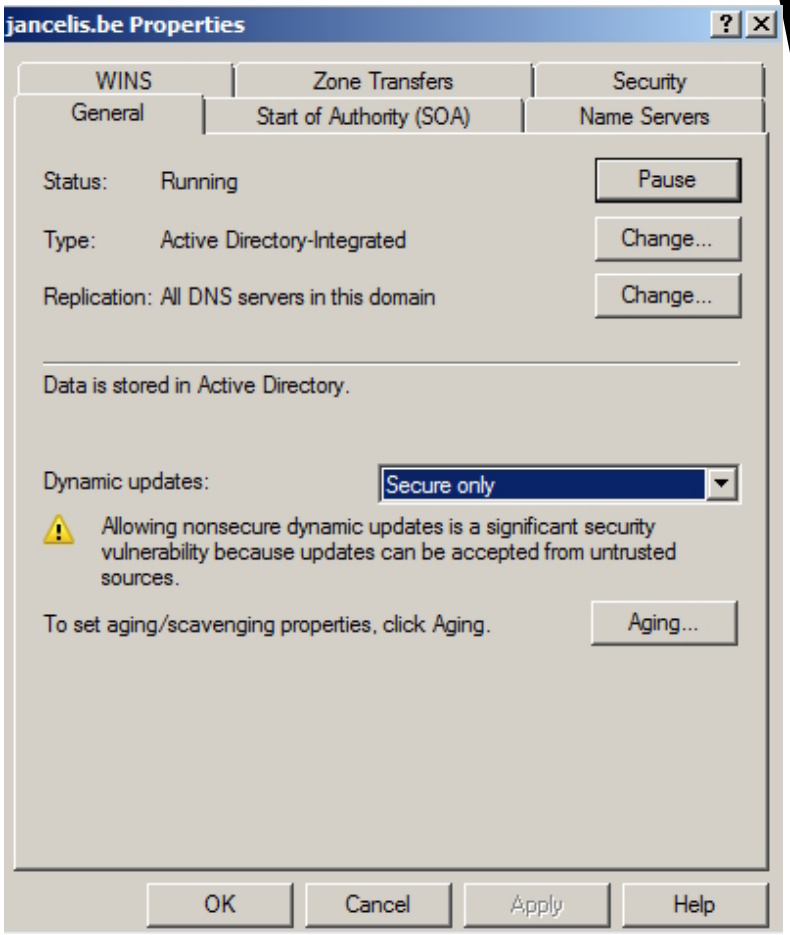
DNS Windows 2k8

- **Moet geïnstalleerd zijn als je AD wil gebruiken**



DNS Dynamisch Windows Server

- DNS werkt samen met DHCP om namen aan IP adressen te koppelen
- Bij Dynamic DNS geeft de DHCP server updates aan de DNS server
- Instellen door bij DNS domein te selecteren, rechtermuistoets en properties



DNSSEC

- **Ontstaan: De oude DNS werking liet toe dat er aan cache poisoning kon gedaan worden door valse berichten te sturen tussen de authoritatieve en de caching DNS servers**
- **DNSSEC beveiligt met een public key / private key paar de resource records (RR)**
- **DS: Delegation Signer Record**
  - Deze bevat informatie over de sleutels van je domein
  - Bv de Top Level DNS servers hebben DS records voor hun second level domains

Toepassing van DNSSEC

- **Oktober 2010**
  - .be TLD werkt met DNSSEC
- **Sept 2020**
  - 1508 TLD's in totaal, 1383 zijn signed *
    - alfaromeo. cisco. christmas. school. vlaanderen.
    - ...

* http://stats.research.icann.org/dns/tld_report/

Referenties

- **There are not 13 root servers**
  - http://blog.icann.org/2007/11/there-are-not-13-root-servers/
- **Root servers**
  - http://www.root-servers.org
- **Voorbeeld van de root zone**
  - ftp://ftp.internic.net/domain/root.zone
- **DNSSEC Operational practices, version 2**
  - http://tools.ietf.org/html/rfc6781
- **Domain Name System**
  - http://tools.ietf.org/html/rfc1034
- **TLD DNS SEC report**
  - http://stats.research.icann.org/dns/tld_report/