DNS

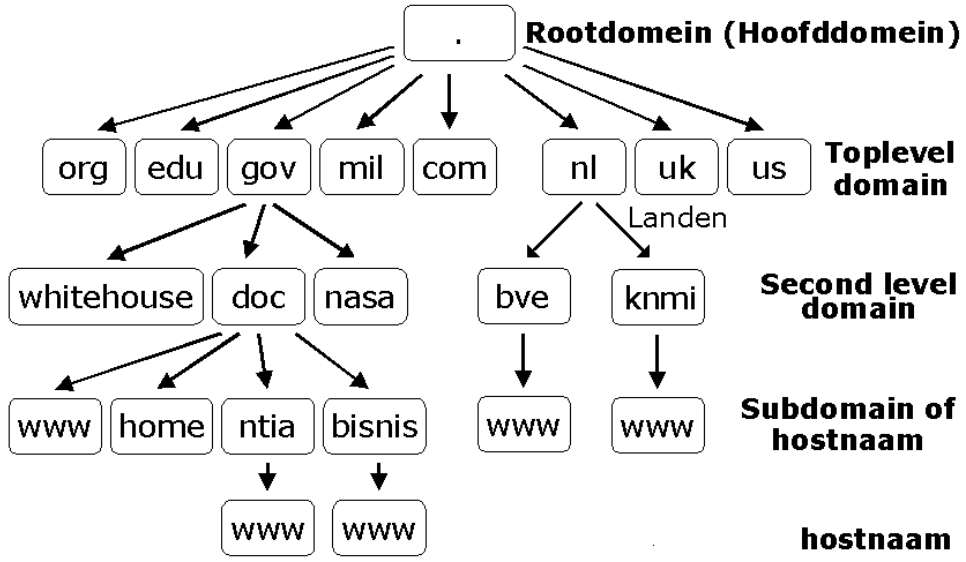
Server OS

DNS = Domain Name System

- Mapping tussen namen en IP-adressen
- IP-adressen moeilijk te onthouden
  - Bij IPv4 valt dit nog mee: 192.168.1.1
  - Bij IPv6 wordt het pas echt moeilijk:
    2001:0DB8:0000:0000:1234:0000:A9FE:133E
- Naamresolutie in Windows-netwerken
  - Oudere Windows-systemen: WINS (Windows Internet Name Service)
  - Vanaf Windows server 2000: DNS
- Evolutie DNS systeem:
  - Vroeger: hosts file (bestaat nog steeds)
    → C:\Windows\System32\Drivers\etc\hosts
  - Nadien op ARPAnet: gecentraliseerde hostfiles
    (door expansie niet meer houdbaar)

DNS = Domain Name System

- Introductie DNS: 1984
- DNS werkt volgens “inverted tree” opbouw
- Root + “.” (voorgesteld door een punt)
- Top-level domains (com, org, be, …)
- Second-level domain (hotmail, ehb, microsoft)
- Subdomains / hostname



erasmus HOGESCHOOL BRUSSEL

DNS = Domain Name System

- Officiële beheerder van het .be domein: http://www.dns.be/
- Registreren via officiële registrar
- Prijzen variëren van 5 tot .. EUR per jaar

Domeinnaam ehb.be

Domein

Naam	ehb
Status	REGISTERED
Registratie	23 juni 1997 CEST
Laatste wijziging	18 december 2008 14:18 CET

Domeinnaamhouder

Naam	Luc Van de Velde
Organisatie	Erasmushogeschool Brussel
Taal	Nederlands
Adres	Nijverheidskaai 170 1070 Brussel BE België
Telefoon	+32.25233737
Fax	+32.25209031
E-mail	hostmaster@ehb.be

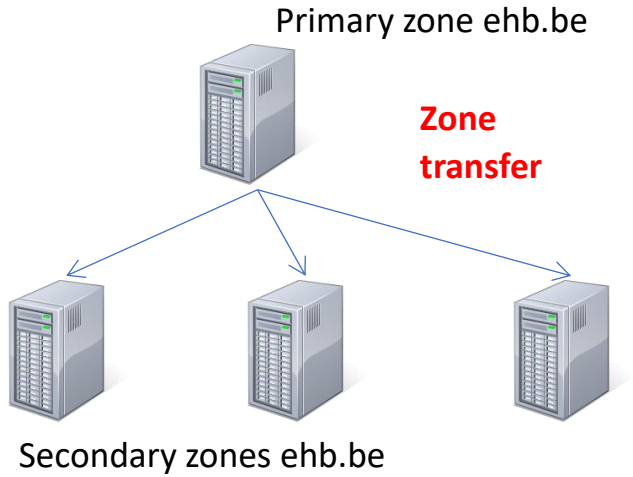
Domeinen vs Zones

- DNS-servers zijn in principe verantwoordelijk voor één of meerdere zones.
- Domein = deel van DNS namespace.
- Zone = informatie over domein (deel van de namespace).
- Wanneer een bedrijf DNS wil implementeren:
  - Minstens 1 DNS server nodig.
  - Op deze DNS server wordt een zone aangemaakt die de informatie (records) zal bevatten van een of meerdere domeinen.

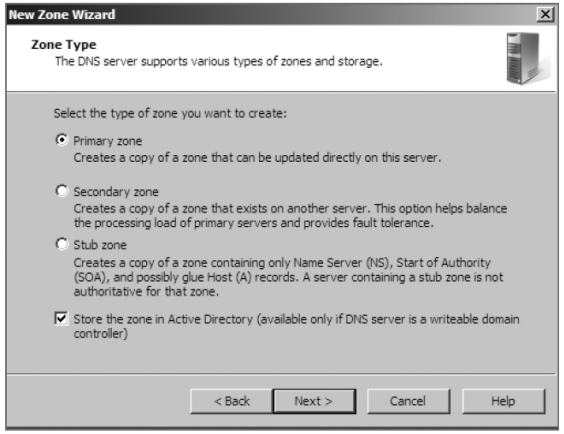
Verschillende Zones

- Forward lookup zone
  - Naam -> IP
- Reverse lookup zone
  - IP -> Naam

Verschillende Zones Types (1)



- Primary Zone
  - RW kopie van de DNS zone
  - Alle updates gebeuren hierop
  - Informatie opgeslagen in .DNS bestanden.
  - Opgelet met fouttolerantie (zolang er geen secondary is), hoge load op 1 server en security (geen secure only updates mogelijk in gewone primary zone die niet AD integrated is).
- Secondary Zone
  - Bevat read-only kopie van de DNS zone.
  - Haalt zijn info bij de primary zone.
  - Voordelen: fouttolerant en load kan verdeeld worden.



erasmus HOGESCHOOL BRUSSEL

Verschillende Zones Types (2)

- Active Directory Integrated Zone
  - Zones worden in Active Directory (NTDS.dit) opgeslagen en via daar gerepliceerd naar andere AD/DNS servers.
  - Geen single point of failure en dus fouttolerant: elke Domain Controller heeft dezelfde data.
  - Secure Dynamic Updates: geëncrypteerde data.
  - Enkel op DC, niet op member server.
  - Elke DC moet niet verplicht DNS-server zijn. Is wel aangeraden.
- Stub Zone
  - Read only kopie van een zone die alleen de bronrecords bevat (SOA, NS en Glue Host (A) records).
  - Deze bronrecords worden gebruikt om de DNS server voor een bepaalde zone terug te vinden: de zogenoemde ‘authoritative Domain Name System (DNS) servers’ voor die zone.

Conditional Forwarder vs Stub Zone

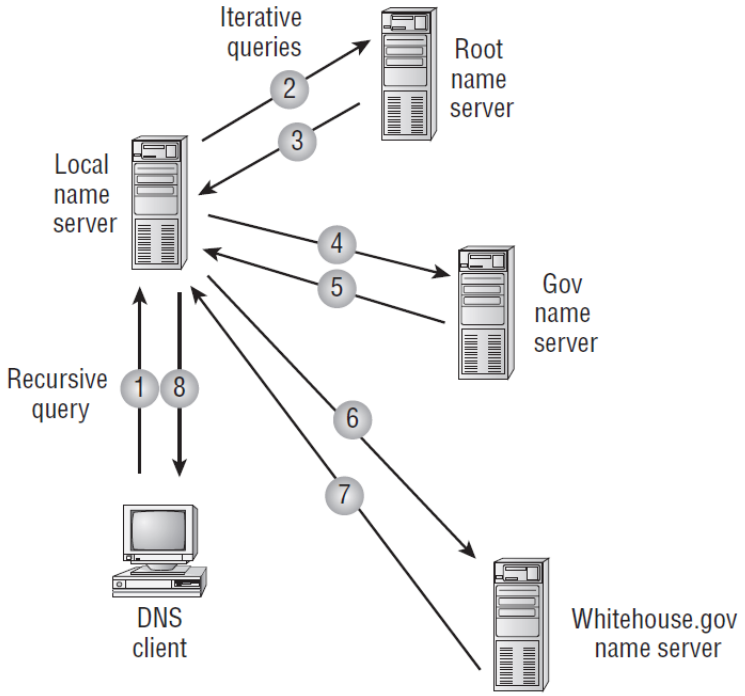
- Stub Zone
  - Actuele zone (replicate from master DNS server).
  - Kan gebruikt worden voor redundantie en load balancing.
- Conditional Forwarder
  - Query’s forwarden voor een specifiek domein.
  - Kan even goed gebruikt worden voor performantie.

Het DNS Proces

- Naamgeving
  - DNS Server: de server die de domain name service aanbiedt.
  - DNS Client: de computer die query's stuurt naar een DNS server.
  - Query: vraag om informatie.
- DNS Query's
  - Forward Lookup Query
    - DNS-Naam → IP
  - Reverse Lookup Query
    - Gebruik maken van PTR records
    - IP → DNS naam
    - In-addr.arpa domein: bv. 1.0.168.192.in-addr.arpa
    - DNS kan alleen fully qualified domain names (FQDN) omzetten naar een ander type gegeven. Daarom wordt het gevraagde IP-adres omgezet naar een FQDN door het om te keren en voor in-addr.arpa te plaatsen

DNS Query's (Iteratief en Recursief)

- De client stuurt een recursieve query naar zijn lokale DNS server en vraagt het IP voor www.whitehouse.gov. Deze is verantwoordelijk voor de aanvraag (geen forward)
- De lokale DNS server checkt zijn lokale zones en vindt niets.
- De root name server zal reply'en met het IP adres van het .gov toplevel domain.
- De lokale DNS server stuurt een iteratieve query voor www.whitehouse.gov naar de .gov DNS server
- De .gov DNS server stuurt het IP voor de DNS server van whitehouse.gov terug.
- De lokale DNS server stuurt een iteratieve query voor www.whitehouse.gov naar de whitehouse.gov DNS server.
- De whitehouse.gov nameserver stuurt het IP-adres voor de website terug naar de lokale name server.
- De lokale name server stuurt op zijn beurt het IP adres terug naar de client (resolver).



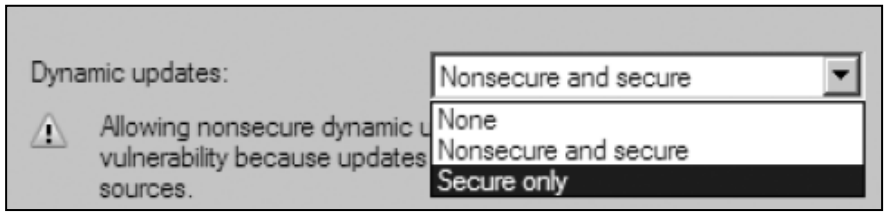
erasmus HOGESCHOOL BRUSSEL

Caching en TTL

- Elke record bevat een TTL veldje.
- TTL = tijd dat deze record lokaal mag gecached worden.
- Kan ook bij negatief antwoord (bv. record niet gevonden).
- TTL kan dezelfde zijn voor heel de zone, maar kan ook individueel per record aangepast worden.

Dynamic DNS

- None (geen DDNS)
- Nonsecure and secure
- Secure only: beste keuze, want enkel AD machines kunnen zichzelf registreren
- Non-dynamic DNS: admin moet alles manueel ingeven: administratieve nachtmerrie.



Zone Files (zones) bevatten resource records

- SOA (Start of Authority) record
- NS (Name Server) record
- A (Host) record (of AAAA bij IPv6)
- CNAME (Alias) record
- PTR (Pointer) record
- MX (Mail eXchanger) record
- SRV (Service) record

SOA (Start of Authority) record

- Algemene parameters voor de zone
- Authoritative server van de zone (primary zone)

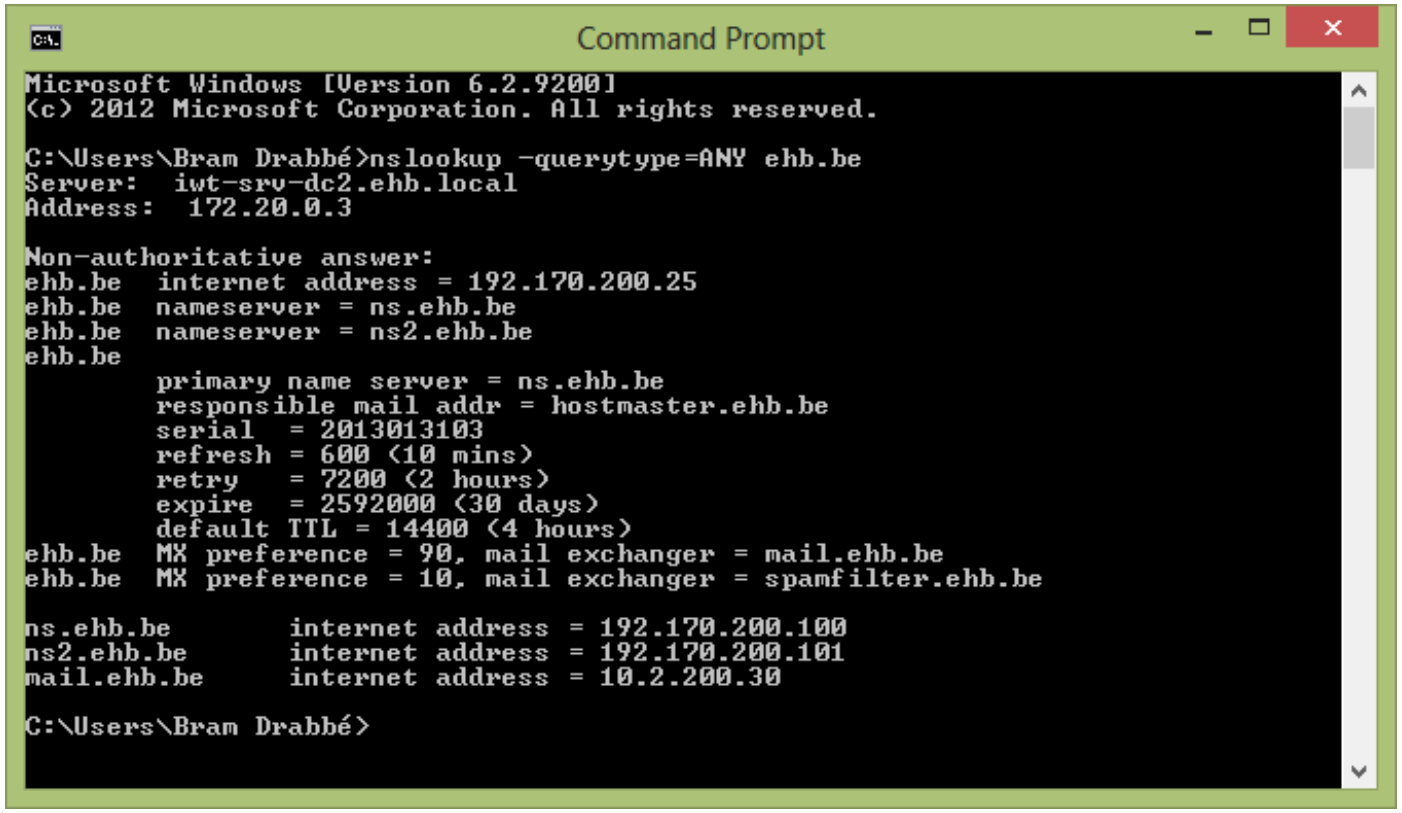
```
@ IN SOA win2k3r2.example.com. hostmaster.example.com. (
                          5            ; serial number
                          900          ; refresh
                          600          ; retry
                          86400        ; expire
                          3600       ) ; default TTL
```

- Serial number: verhoogt bij elke aanpassing.
- Refresh: de tijd dat een secondary server wacht tussen checks of de database file gewijzigd is op de primary server.
- Retry: de tijd dat een secondary server wacht tussen het opnieuw proberen van een gefaalde zone transfer.
- Expire: maximum tijd dat een secondary server heeft om de zone binnen te halen.

NS (Name Server) record

```
example.com.    IN    NS    Hostname.example.com
```

- Lijst de nameservers voor een domein op.
- NS record per DNS server van een domein.
- Zorgt ervoor dat geweten is welke DNS servers moeten gecontacteerd worden voor een bepaald domein.



erasmus HOGESCHOOL BRUSSEL

A-record

- DNS naam → IPv4 mapping.
- Optioneel: TTL veld (anders wordt de TTL van het SOA record als default gebruikt)

```
www   IN   A   192.168.0.204
SMTP  IN   A   192.168.3.144
```

AAAA-record

- DNS naam → IPv6 mapping.

CNAME-record

- Alias voor bestaande FQDN

```
www IN CNAME chaos.example.com.
```

PTR-record

- IP naar naam omzetten
- Gebruik van in-addr.arpa zone
- IP adressen: meer specifiek van links naar rechts (10.0.0.1)
- FQDN: meer specifiek van rechts naar links (www.ehb.be)
- PTR records zijn nodig om deze andere opbouw te ondersteunen

```
10.1.168.192.in-addr.arpa. IN PTR www.example.com.
```

MX-record

- Voor het opgeven van de SMTP server die van buitenaf bereikbaar is voor het afleveren van mail.
- Indien meerdere: prioriteit (lager eerst)

```
example.com.    IN  MX  0  mail.example.com.
example.com.    IN  MX  10 backupmail.example.com.
```

SRV-record

- Mappen van service naar IP adres.
- Enorm belangrijk in Active Directory domeinen: Vinden van logon server(s) voor verifiëren username/password.

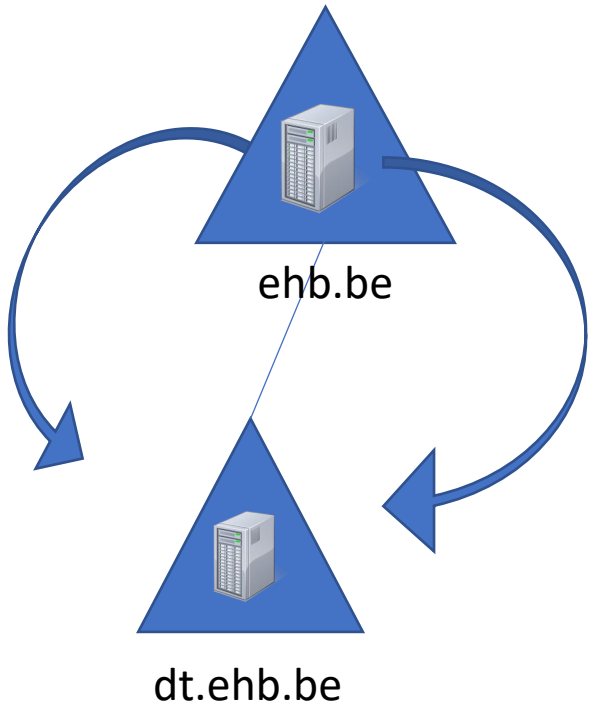
```
ldap.tcp.example.com.   86400 IN SRV   10   100   389   hsv.example.com
ldap.tcp.example.com.   86400 IN SRV   20   100   389   msy.example.com
```

- In CMD:
  - typ: Nslookup
  - typ: Set type=srv
  - typ: _ldap._tcp.ehb.local

```
_ldap._tcp.ehb.local    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = ehbdc02.ehb.local
_ldap._tcp.ehb.local    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = iwt-srv-dc.ehb.local
_ldap._tcp.ehb.local    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = iwt-srv-dc2.ehb.local
_ldap._tcp.ehb.local    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = jetdc02.ehb.local
_ldap._tcp.ehb.local    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = jetdc01.ehb.local
_ldap._tcp.ehb.local    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = dandc01.ehb.local
_ldap._tcp.ehb.local    SRV service location:
          priority       = 0
          weight         = 100
          port           = 389
          svr hostname   = ehbdc04.ehb.local
ehbdc02.ehb.local       internet address = 10.2.200.26
iwt-srv-dc.ehb.local    internet address = 172.20.0.2
iwt-srv-dc2.ehb.local   internet address = 172.20.0.3
jetdc02.ehb.local       internet address = 10.4.200.200
jetdc02.ehb.local       internet address = 192.168.1.9
jetdc01.ehb.local       internet address = 10.4.200.99
jetdc01.ehb.local       internet address = 192.168.1.6
dandc01.ehb.local       internet address = 192.168.11.4
ehbdc04.ehb.local       internet address = 192.168.0.214
> _
```

Delegated Zones

- Subdomein laten beheren door een andere server.



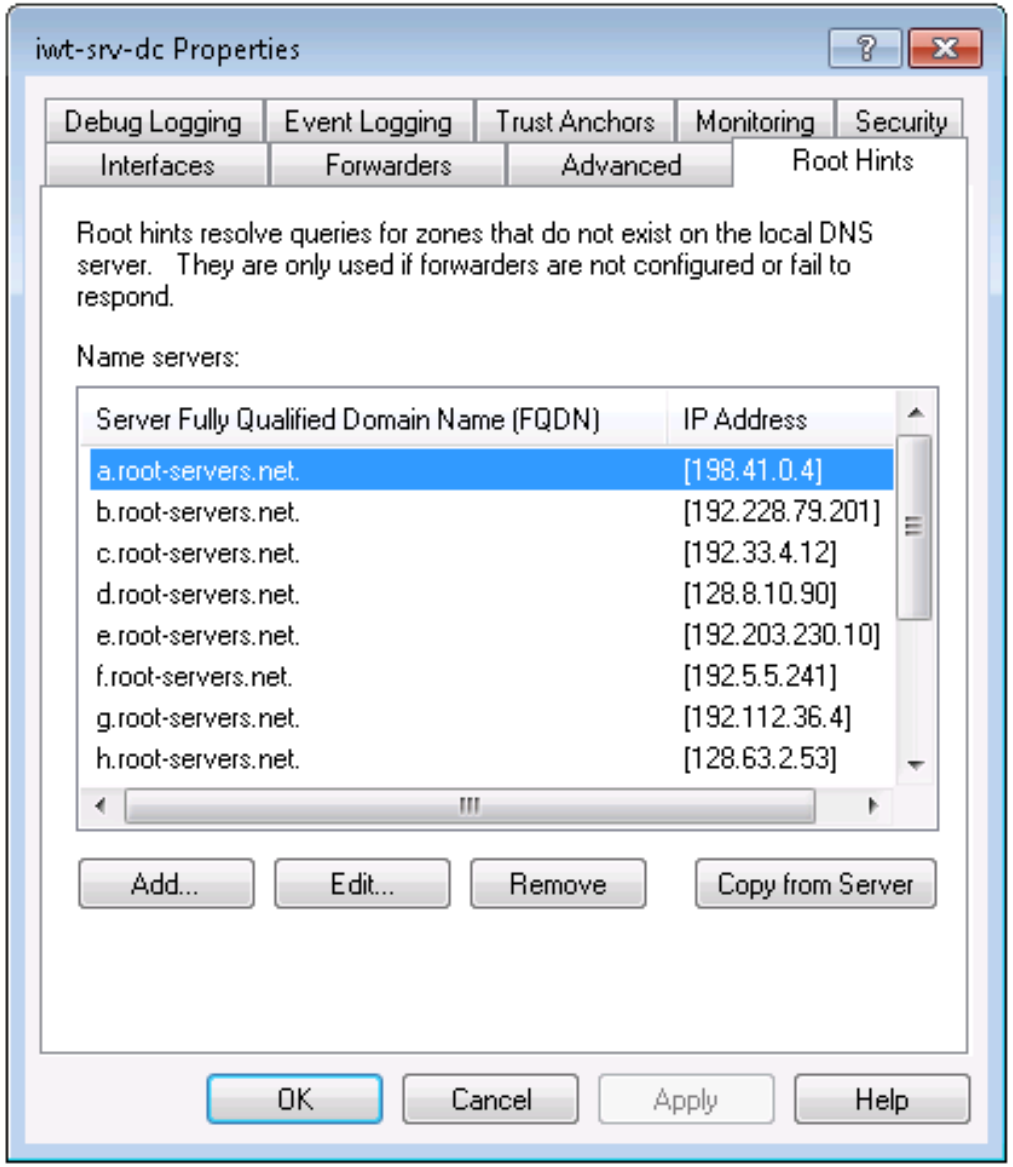
Forwards en root hints

- Indien een query wordt ontvangen die de DNS server niet zelf kan resolven zal hij deze doorsturen via forwarder of root hint.
- Een Windows DNS server zal eerst forwarders aanspreken en dan pas root hints.

Authoritative DNS Server

- Een DNS server zal een query voor zijn eigen domein nooit doorsturen maar steeds zelf beantwoorden!

DNS

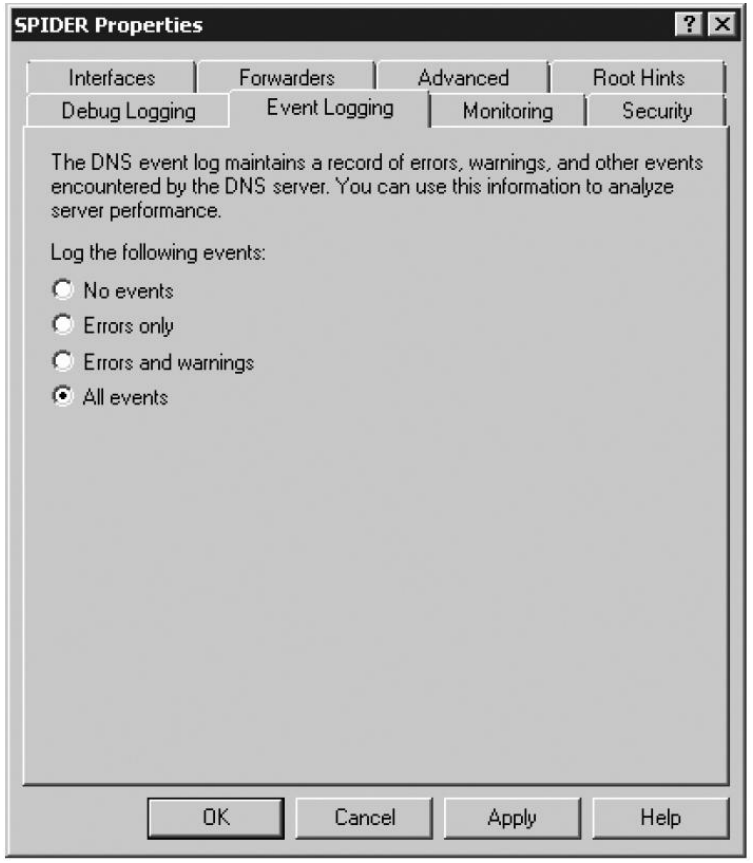


Configuratie

- Installeren via “add roles” in server manager.
- Caching-only server = geen eigen zones. Kijk wel de root hints na.
- Load balancing door round robin, standaard ingeschakeld.

Monitoring

- Event logging tabblad van de DNS server.
- Monitoring tabblad van de DNS server.
- Debug logging tabblad van de DNS server.



Check commando’s

- Nslookup (zie ook terug)
  - Set all (opties bekijken)
  - Set d2 (debug mode)
  - Set domain=domain name (welke domeinnaam achteraan bijvoegen bij query's met 1 woord)
  - Set timeout=timeout
  - Set type=record type
  - Ls –t domeinnaam (full listing, eigenlijk een zone transfer)
  - server [ip van dns server]
- DNSlint
- Ipconfig (/displaydns /flushdns /registerdns)