Huiswerk Linux: domein-configuratie server

De meeste bedrijfsnetwerken worden tegenwoording beheerd door het *Windows* operating system. Voor Windows administrators kost het bijhouden van een Linux server in zijn netwerk nogal wat extra werk. Hij moet dan namelijk op de Linux machine aparte *gebruikersprofielen* (combinatie van gebruikersnaam en wachtwoord) bijhouden.

De opdracht voor deze week is: controleer of onze testmachines correct vermeld staan in het DNS ter voorbereiding voor communicatie met een Windows *Domain Controller* (DC).

Let op: deze opdracht gaat ervan uit dat je kunt beschikken over een werkende Domain Controller. De minimaal benodigde *role* is: *Active Directory*.

Over DNS

In het Domein Naam Systeem (DNS) worden de namen van alle computers in het netwerk centraal bijgehouden. Een eenvoudig voorbeeld van zo'n systeem kun je vinden in het bestand */etc/hosts*. Vroeger werd deze informatie rondgestuurd per e-mail, zodat alle computers in het domein van elkaars bestaan afwisten. Tegenwoordig wordt deze informatie centraal bijgehouden via de zogenaamde *named* (name daemon) op één van de servers in het netwerk.

De meest gebruikte DNS server in de Linux-wereld heet *BIND* (Berkeley Internet Name Domain), geschreven door studenten van de Berkeley universiteit in Californië (USA). In de Windows-wereld wordt de DNS server ook wel de *Domain Controller* genoemd.

Reverse lookups (FQDN opzoeken via een IP-adres) worden vaak niet ingesteld op DNS systemen, maar ze zijn belangrijk voor zogenaamde *trusted connections* (zie ook: Linux opdracht *Ring of Trust*). Servers die vertrouwelijke informatie verwerken zoals wachtwoorden, willen weten of de client-computer wel in hun netwerk thuishoort. Dit doen ze door het IP-adres te gebruiken om de *fully qualified domain name* (FQDN) van de client-computer te vinden.

FQDN van de server controleren

Om lid te worden van een Windows domein, moeten zowel de server als de clients *volledig geldige domeinnamen* (FQDN) hebben. Bovendien moeten ook de *reverse lookups* weer terugverwijzen naar dezelfde domeinnamen. Het controleren van de domein-gegevens van de Domain Controller doen we in drie stappen. Eerst zoeken we de host-naam van onze server op. Daarna zoeken we het IP-adres op en daarna voeren we een *reverse lookup* uit.

Let op: de volgende acties moeten op de Domain Controller uitgevoerd worden. Ga naar je DC, toets **<Windows>-R** en geef het volgende commando:

```
cmd
```

Je krijgt dan een venster met de Windows command-line.

Opzoeken host-naam

Allereerst moeten we weten wat de host-naam van onze Domain Controller is. Dit doen we met het *hostname* commando:

```
hostname
```

Mijn output ziet er alsvolgt uit:

```
intra
```

Opzoeken FQDN

Nu zoeken we de FQDN van onze Domain Controller op. Dit doen we met het nslookup (name service lookup) commando:

```
nslookup intra
```

Let op: *intra* is de host-naam van mijn DC. Gebruik hier de door jou gevonden host-naam. Mijn output ziet er alsvolgt uit:

```
Name:   intra.linux.local
Address: 192.168.137.50
```

Reverse lookup uitvoeren

Met het gevonden IP-adres kunnen we nu we de *reverse lookup* uitvoeren. Dit doen we ook weer met het *nslookup* programma:

nslookup 192.168.137.50

Let op: het IP-adres *192.168.137.50* is van mijn DC. Gebruik hier het door jou gevonden IP-adres. Mijn output ziet er alsvolgt uit:

```
50.137.168.192.in-addr.arpa name = intra.linux.local.
```

Het hoera-moment

Als alles werkt, kunnen we nu het volgende concluderen:

1. dat het IP-adres van mijn Domain Controller *192.168.137.50* is;
2. dat dit IP-adres ook weer terugverwijst naar de FQDN van mijn DC (*intra.linux.local*) en
3. dat het domein van mijn DC *linux.local* is.

Zorg ervoor dat de *reverse lookup* werkt en onthoud het domein van jouw eigen DC. Anders kunnen we straks niet lid worden van het Windows domein.

Huiswerk opsturen

Aftekenen via email op de Domain Controller kan niet. Dit doen we via de Linux machine in de volgende opdracht.

Problemen oplossen

Als je in bovenstaande test een foutmelding krijgt, dan heeft jouw DC geen *reverse lookup* record. Om een reverse lookup in te stellen moet je allereerst weten wat de *zone*, de *node* en de *FQDN* is. De eerder (bovenstaand) gevonden gevens zien er dan alsvolgt uit:

FQDN: intra.linux.local
Zone: 137.168.192.in-addr.arpa
Node: 50

Zoals je ziet bestaat de combinatie van zone en node uit de **omgekeerde getallen** van het eerder gevonden IP-adres:

```
50.137.168.192.in-addr.arpa
-node-    -zone-------------------------------------------------------------
```

Allereerst moeten we de *zone* aanmaken. Dit doen we met het Windows programma *dnscmd*:

dnscmd localhost /ZoneAdd 137.168.192.in-addr.arpa /primary

Let op: de zone 137.168.192.in-addr.arpa is die van mijn eigen DC. Gebruik het in vorige stap door jou gevonden (omgekeerde!) IP-adres.

Middels het Windows programma *dnscmd* kunnen we nu de *node* aan het DNS toevoegen:

dnscmd localhost /RecordAdd 137.168.192.in-addr.arpa 50 PTR intra.linux.local

Let goed op: de onderstreepte gegevens zijn van mijn eigen DC. Gebruik de in vorige stap door jou gevonden gegevens. Middels de optie *localhost* geven we aan dat de actie op onze DC moet plaatsvinden. Via de actie *RecordAdd* geven we aan dat we een nieuwe DNS-regel (record) willen toevoegen (*zone* 56.168.192.in-addr.arpa, *node* 50). Via het *record-type* PTR (pointer) geven we aan dat we een verwijzing naar *intra.linux.local* willen toevoegen.