

18.3.2024

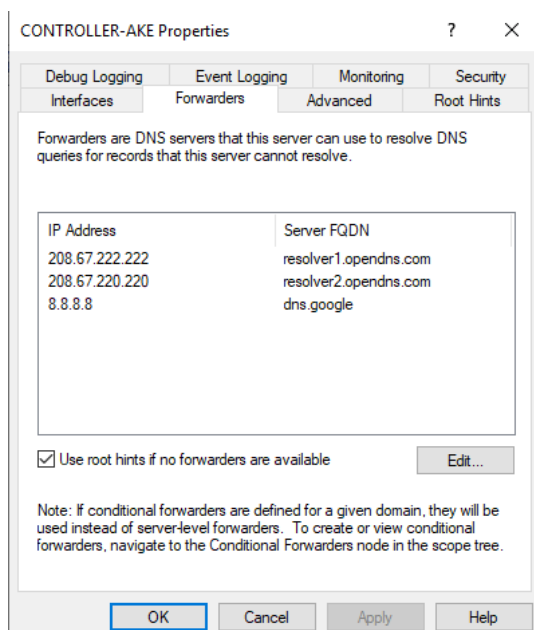
## Johdanto

Tämän viikon tehtävässä tutustutaan DNS nimikyselyn toimintalogiikkaan sekä määritellään omalle toimialueelle DNS vyöhyke. Viikon harjoitteessa kertaan DNS toimintamallin ja tarkastellaan, miten omassa toimialueessa suoritetaan DNS kyselyitä. DNS järjestelmä on itselleni hieman tuttu mutta miten tämä toimii omassa toimialueessa, on täysin uutta minulle. Minun tavoitteeni on saavuttaa syvempi ymmärrys, miten DNS toteutetaan suljetussa toimialueessa.

## DNS Forwarder

Ohjauspalvelin toimii DNS palvelimena toimialueen tietokoneille. Tarkastan mitkä DNS välittäjät on asennettu palvelimelle. Palvelimelle on aikasemmin asennettu DNS palvelu. Tämä tapahtui kun määrittelin ohjauspalvelimelle roolin.

Lisään googlen nimipalvelun ohjauspalvelimen DNS välittäjäksi (Forwarder). Googlen DNS palvelin asuu osoitteessa 8.8.8.8. Forwarderin saa lisättyä ohjauspalvelimen hallintapanelista. Tools→ DNS. Properties valinnasta saan lisättyä Googlen nimipalvelin välittäjäksi.



## DNS cache/välimuisti

Seuraavassa osiossa tarkastellaan DNS välimuisteja ja miten ne tallentuu. DNS palvelimelle tallentuu asiakkaiden (Toimialueen tietokoneet) sekä DNS palvelimen kyselyt. DNS asiakkaalle tallentuu vain sen omat kyselyt. Tarkastan mitä DNS palvelinta tiedostopalvelin käyttää komenolla "nslookup".

18.3.2024

```
CA: Select Administrator: Command Prompt

Microsoft Windows [Version 10.0.17763.1935]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Users\Administrator.AKERLUND>nslookup wikipedia.org
Server: UnKnown
Address: 10.208.0.10

Non-authoritative answer:
Name: wikipedia.org
Addresses: 2a02:ec80:300:ed1a::1
          185.15.59.224

C:\Users\Administrator.AKERLUND>
```

Kuvasta näen, että tiedostopalvelin käyttää ohjauspalvelinta DNS palvelimena. (10.208.0.10). nslookup komento kertoo myös minulle että wikipedia.org löytyy osoitteesta 185.15.59.224. Non-authoritative answer tarkoittaa sitä, että kyselyn tulos ei tule suoraan DNS palvelimelta. Eli minun esimerkissäni ohjauspalvelimella ei ole muistissa missä wikipedia.org sijaitsee vaan se välittää kyselyn DNS välittäjille, jotka olivat kuvattu edellisessä vaiheessa.

Lisääkseni wikipedia.org DNS palvelimen välimuistiin minun pitää käydä selaimella wikipedia.org sivustolla. Seuraavaksi tarkastan miltä DNS palvelimen välimuisti näyttää. Aloitan tarkastamalla tiedostopalvelimen muistin.

Komennolla "Get-DnsClientCache" näen tiedostopalvelimelta että Wikipedia.org löytyy nyt DNS asiakkaan DNS välimuistissa. Tällä tavoin tietokone ei tarvitse ottaa yhteyttä muihin DNS palvelimiin vaan voi suoraan hakea tietuen omasta muistista.

Vierailen campusonline.fi sivustolla tiedostopalvelimella. Eli lisään osoitteen DNS asiakkaan välimuistiin. Tämän jälkeen tarkastan, että DNS kysely jää myös DNS palvelimen välimuistiin. Ohjauspalvelimella pitäisi näkyä asiakkaiden välimuisti. Mutta jostain syystä osoite ei jää ohjauspalvelimen muistiin.

```
PS C:\Users\Administrator> Get-DnsClientCache
```

Entry	RecordName	Record Type	Status	Section	TimeTo Live	Data Length	Data
-----	-----	-----	-----	-----	-----	-----	-----
ieonline.microsoft.com	ieonline.microsoft.com	CNAME	Success	Answer	226	8	any.edge.bing.com
ieonline.microsoft.com	any.edge.bing.com	A	Success	Answer	226	4	204.79.197.200
fileserv-akerlund.ak...	fileserv-akerlund.ak...	A	Success	Answer	619	4	10.208.0.12
fileserv-akerlund.ak...	fileserv-akerlund.ak...	A	Success	Answer	619	4	10.208.0.12
_ldap._tcp.default-fir...	_ldap._tcp.Default-fir...	SRV	Success	Answer	596	16	controller-ake.akerlund.1...
_ldap._tcp.default-fir...	controller-ake.akerlun...	A	Success	Addi...	596	4	10.208.0.10
ocsp.digicert.com	ocsp.digicert.com	CNAME	Success	Answer	2110	8	ocsp.edge.digicert.com
ocsp.digicert.com	ocsp.edge.digicert.com	CNAME	Success	Answer	2110	8	fp2e7a.wpc.2be4.phicdn.net
ocsp.digicert.com	fp2e7a.wpc.2be4.phicdn...	CNAME	Success	Answer	2110	8	fp2e7a.wpc.phicdn.net
ocsp.digicert.com	fp2e7a.wpc.phicdn.net	A	Success	Answer	2110	4	192.229.221.95

18.3.2024

## DNS välimuistin tarkastelu

DNS välimuistia voidaan tarkastella graafisesti ohjauspalvelimelta DNS managerin valikon alla. Valitsemalla "advanced" näkymä saan näkyviin "cached lookups". Valikon alla näen kaikki tallennetut haut. Hakuja voi myös tarkastella powershellissä komennolla "Show-DnsServerCache". Vlaikoista näkyy hakujen tulokset sekä TTL (Elinikä).

Name	Type	Data	Timestamp
campusonline	Host (A)	35.228.66.119	static
any.edge.bing.com	NS	2	00:00:00
any.edge.bing.com	PTR	12	23:40:21
any.edge.bing.com	A	1	00:16:22
www.bing.com	CNAME	5	00:16:13
consent.cookiebot.com	CNAME	5	00:16:21
consent.cookiebot.com	RRSIG	46	00:16:21
ocsip.edge.digicert.com	CNAME	5	00:16:21
ocsip.digicert.com	CNAME	5	00:16:21
fredrikakerlund.com	A	1	00:16:21
go.microsoft.com	CNAME	5	00:16:21
oneocsp.microsoft.com	CNAME	5	00:16:21
uns.microsoft.com	CNAME	5	00:16:21
www.microsoft.com	CNAME	5	00:16:21
campusonline.fi	A	1	00:16:21
localhost	A	1	00:16:21
www.bing.com.edgekey.net	CNAME	5	00:16:21
consent.cookiebot.com	CNAME	5	00:16:21
crl.root-x1.letsencrypt.org	CNAME	5	00:16:21
o.lencr.edgesuite.net	CNAME	5	00:16:21
fp2e7a.wpc.2be4.phicdn.net	CNAME	5	00:16:21
fp2e7a.wpc.phicdn.net	A	1	00:16:21
a.root-servers.net	AAAA	28	00:16:21
a.root-servers.net	AAAA	28	00:16:21

Kahdessa ylläolevassa kuvassa voidaan nähdä DNS välimuistissa olevat osoitteet.

DNS välimuistin tyhjentäminen on yksinkertainen toimenpide joka voidaan suorittaa ohjauspalvelimelta. DNS asiakkaan välimuistin tyhjennys tapahtuu komennolla "ipconfig /flushdns". DNS palvelimen välimuisti tyhjennetään powershell komennolla "Clear-DnsServerCache". Suoritan molemmat komennot ja totean että välimuisti on tyhjä pois lukien juurinimi kyselyt. Huomiona että asiakkaan välimuisti pitää tyhjentää paikallisesti siltä koneelta.

## Tietuiden lisäys DNS palvelimelle

Lisään 2 CNAME aliaista jotka viittaavaat tiedostopalvelimeeni. Nämä kaksi aliaista ovat "intra" ja "web". Nämä kaksi aliaista siis viittaavat samaan palvelimeen. Näitä aliaksia käytetään myöhemmässä kun luodaan weppipalvelin.

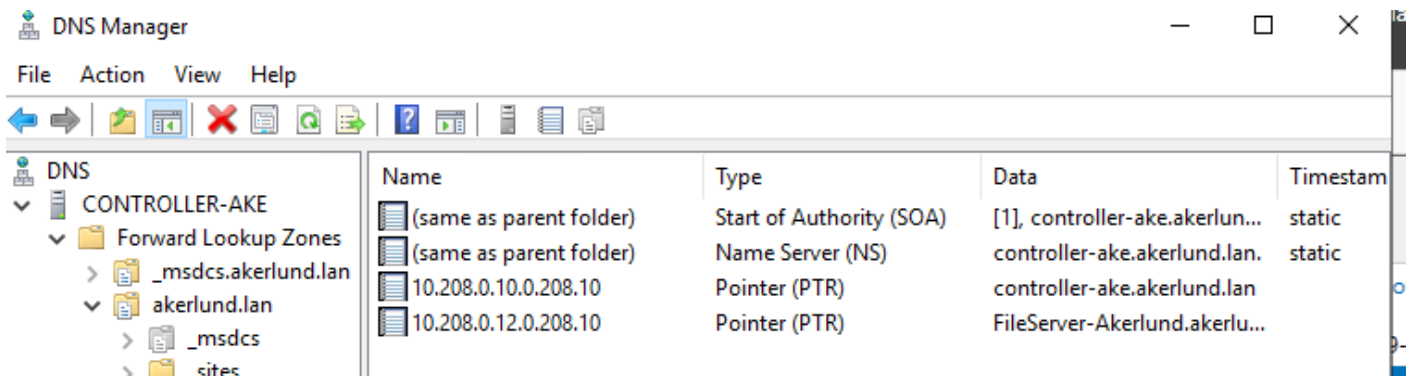
Name	Type	Data	Timestamp
_msdcs	Start of Authority (SOA)	[46], controller-ake.akerlu...	static
_sites	Name Server (NS)	controller-ake.akerlund.lan.	static
_tcp	Host (A)	10.208.0.10	18.3.2024
_udp	Host (A)	10.208.0.10	18.3.2024
DomainDnsZones	Host (A)	10.208.0.12	18.3.2024
ForestDnsZones	Host (A)	10.208.0.12	18.3.2024
(same as parent folder)	Host (A)	10.208.0.12	18.3.2024
controller-ake	Host (A)	10.208.0.10	static
FileServer-Akerlund	Host (A)	10.208.0.12	18.3.2024
intra	Alias (CNAME)	FileServer-Akerlund.akerlu...	
web	Alias (CNAME)	FileServer-Akerlund.akerlu...	

18.3.2024

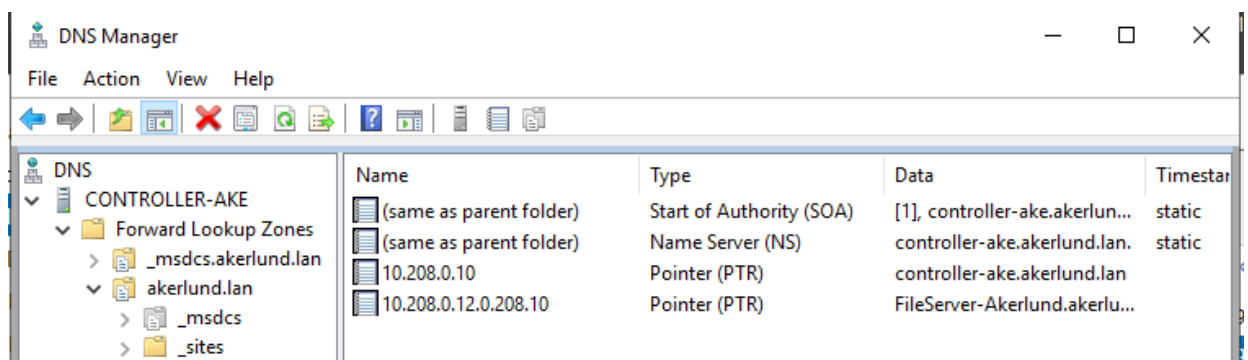
Nämä 2 tietuita ovat siis Forward Look Up zone, mikä etsii siis nimellä IP osoitteen. Seuraavaksi tehdään Reverse Lookup Zone, eli etsitään mimi IP osoitteen perusteella.

Tietue lisätään DNS managerista. Configuration wizardia seuraamalla pystyn lisäämään toimialueeni verkko-osan joka mahdollistaa käänteisen nimikyselyn. Seuraavaksi lisään PTR tietuen joka mahdollistaa käänteisen haun ohjauspalvelimelle sekä tiedostopalvelimelle.

Lisään kaksi PTR osoitetta osoittamaan Tiedostopalvelintani sekä Ohjauspalvelinta.



Nimi kuitenkin on väärä. Jostain syystä FQDN tulee nimeksi. Tein jotain :D joka korjasi virheen ohjauspalvelimen kohdalla mutta en tiedä mitä. Enkä saa korjattua virhettä tiedostopalvelimen kohdalle.



Jatkan kuitenkin. Tähän ongelmaan haluaisin mielelläni vastauksen arvioinnissa.

Seuraavaksi testaan kyselyn tulokset tiedostopalvelimelta. Suoritan nimikyselytestaukset käänteisesti sekä nimen avulla. Alla kuvakaappaukset testeistä.

```
C:\Users\Administrator.AKERLUND>nslookup intra.akerlund.lan
Server: controller-ake.akerlund.lan
Address: 10.208.0.10

Name: FileServer-Akerlund.akerlund.lan
Address: 10.208.0.12
Aliases: intra.akerlund.lan
```

```
C:\Users\Administrator.AKERLUND>nslookup web.akerlund.lan
Server: controller-ake.akerlund.lan
Address: 10.208.0.10

Name: FileServer-Akerlund.akerlund.lan
Address: 10.208.0.12
Aliases: web.akerlund.lan
```

```
C:\Users\Administrator.AKERLUND>nslookup 10.208.0.10
Server: controller-ake.akerlund.lan
Address: 10.208.0.10

Name: controller-ake.akerlund.lan
Address: 10.208.0.10
```

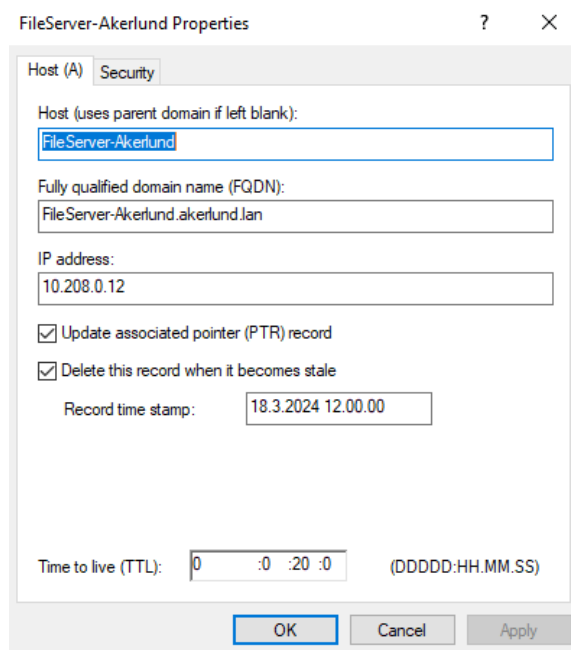
18.3.2024

```
C:\Users\Administrator.AKERLUND>nslookup 10.208.0.12
Server: controller-ake.akerlund.lan
Address: 10.208.0.10

0.208.10.in-addr.arpa
primary name server = controller-ake.akerlund.lan
responsible mail addr = hostmaster.akerlund.lan
serial = 28
refresh = 900 (15 mins)
retry = 600 (10 mins)
expire = 86400 (1 day)
default TTL = 3600 (1 hour)
*** No internal type for both IPv4 and IPv6 Addresses (A+AAAA) records available for 10.208.0.12
```

Viimeisessä kuvankaappauksessa näen, että käänteisessä nimikyselyssä on virhe. Virhe johtuu aikaisemmin mainitussa nimessä. Käänteinen haku ei onnistu koska nimi PTR tietuilla ei ole 10.208.0.12 vaan se on 10.208.0.12.0.208.10 enkö saa sitä muutettua.

Palaan ongelmaan ja Youtuben avulla löydän keinon miten lisään tiedostopalvelimeni PTR tietuen. Tämä tapahtuu valitsemalla tiedostopalvelimen Forward Lookup Zones ja valitsen täpän "update associated PTR record". Tällä vaihtoehdolla PTR tietue lisätään käänteiseen hakukenttään.



FileServer-Akerlund Properties

Host (A) Security

Host (uses parent domain if left blank):  
FileServer-Akerlund

Fully qualified domain name (FQDN):  
FileServer-Akerlund.akerlund.lan

IP address:  
10.208.0.12

☒ Update associated pointer (PTR) record

☒ Delete this record when it becomes stale

Record time stamp: 18.3.2024 12.00.00

Time to live (TTL): 0 :0 :20 :0 (DDDD:HH.MM.SS)

OK Cancel Apply

Kokeilen uudestaan käänteistä nimenhakua tiedostopalvelimelta.

```
C:\Users\Administrator.AKERLUND>nslookup 10.208.0.12
Server: Controller-Ake.akerlund.lan
Address: 10.208.0.10

Name:    FileServer-Akerlund.akerlund.lan
Address: 10.208.0.12

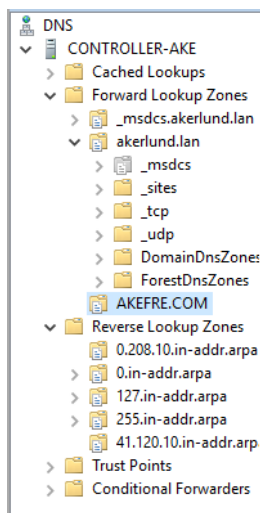
C:\Users\Administrator.AKERLUND>
```

Ja nyt se toimii. En tiedä mikä meni vikaan kun kokeilin ensimmäistä kertaa.

18.3.2024

Testeille kokeiltiin, että nimikysely toimii toimialueeni sisällä. Käänteinen nimikysely toimi myös. Testauksessa lukee Server:Controller-ake.akerlund.lan joka osoittaa, että DNS kysely suoritetaan omassa Domain-Controllerissa ja kaikki tapahtuu sisäisessä verkossa.

### Mielivaltaisten tietuiden lisääminen ohjauspalvelimelle



Seuraavassa vaiheessa lisäilen mielivaltaisesti tietuita ohjauspalvelimelle ja kokeilen niiden toimivuutta. Aloitan lisäämällä käänteisen nimikysely vyöhykkeeseen verkkoavaruuden 10.120.41.0/24. Tämä verkkoavaruus on yksityinen ja minun ei pitäisi löytää mitään tuloksia, jos teen nimikyselyitä kyseiseen verkkoavaruuteen.

Seuraavaksi lisään Forward Lookup vyöhykkeen, jonka nimeän AKEFRE.COM. Lopputulos vieressä olevassa kuvankaappauksessa.

Lisään vyöhykkeeseen kolme A-tietuetta. Ne osoittaa osoitteeseen 10.120.41.10-30 ja nimenä on HOST-1/2/3.AKEFRE.COM. Samalla kuin luon A-tietuet, valitsen vaihtoehdon luodakseni käänteisen pointer tietuen käänteis nimikysely vyöhykkeeseen.

Seuraavaksi tarkistan saako tiedostopalvelimeni vastauksen nimikyselyihin juuri äsken luomiini tietuihini. Nämä sivustot eivät siis ole olemassa mutta nslookup saa vastauksen ohjainpalvelimeltani, minne juuri luotiin mielivaltaiset tietuet.

```
C:\Users\Administrator.AKERLUND>nslookup host-1.akefre.com
Server: Controller-Ake.akerlund.lan
Address: 10.208.0.10

Name: host-1.akefre.com
Address: 10.120.41.10

C:\Users\Administrator.AKERLUND>nslookup host-2.akefre.com
Server: Controller-Ake.akerlund.lan
Address: 10.208.0.10

Name: host-2.akefre.com
Address: 10.120.41.20

C:\Users\Administrator.AKERLUND>nslookup host-3.akefre.com
Server: Controller-Ake.akerlund.lan
Address: 10.208.0.10

Name: host-3.akefre.com
Address: 10.120.41.30
```

Vieressä olevassa kuvankaappauksessa voidaan todeta että nimikyselyyn saan vastauksen että kyseinen palvelin on olemassa tässä IP osoitteessa.

Seuraavassa kokeilen käänteistä nimenhakua luomilleni DNS tietuilleni.

Nimikysely saa vastauksen.

```
C:\Users\Administrator.AKERLUND>nslookup 10.120.41.10
Server: Controller-Ake.akerlund.lan
Address: 10.208.0.10

Name: HOST-1.akefre.com
Address: 10.120.41.10

C:\Users\Administrator.AKERLUND>nslookup 10.120.41.20
Server: Controller-Ake.akerlund.lan
Address: 10.208.0.10

Name: HOST-2.akefre.com
Address: 10.120.41.20

C:\Users\Administrator.AKERLUND>nslookup 10.120.41.30
Server: Controller-Ake.akerlund.lan
Address: 10.208.0.10

Name: HOST-3.akefre.com
Address: 10.120.41.30
```

### Yhteenveto

Tehtävässä tutustuttiin miten DNS toimii toimialueellani. Tehtävässä lisättiin DNS tietuita suoraan ohjauspalvelimelleni, josta tietokoneet saivat suoraan vastauksen nimikyselyyni. Viimeisenä lisättiin "Vääriä" tietuita ohjauspalvelimeeni, jotka viittaavat olemattomiin osoitteisiin.

18.3.2024

## DNSSEC

DNSSEC on laajennus, joka varmistaa DNS nimipalvelun eheyden. Allekirjoittamalla DNS vyöhykkeen SHA/RSA256 avaimella voidaan varmentaa DNS kyselyiden tuloksien luotettavuuden. DNSSEC on protokolla, joka perustuu julkisen avaimen salausperiaatteella. DNSSEC laajennus luo avainparin, jolla voidaan varmentaa liikenteen. DNSSEC avulla voidaan välttyä haitallisilta verkkohyökkäyksiltä kuten välimieshyökkäys. DNSSEC estää DNS-tietuiden haitallisen manipuloinnin.

Vastauksia tehtävänannon olevissa kysymyksiin:

DNSSEC loi uusia tietuita. Nämä tietuet ovat: RRSIG (Resource Record Signature), DNSKEY (DNS Key), NSEC (Next Secure), ja DS (Delegation Signer).

DNSSEC loi uusia tietuita A-tietuiden kylkeen. Nämä ovat RRSIG-tietueita, jotka sisältävät digitaalisia allekirjoituksia kyseisille A-tietueille. Nämä allekirjoitukset varmistavat tietueiden aitouden ja eheyden.

"Types Present" -kentän arvo tarkoittaa niitä tietueiden tyyppejä, jotka ovat olemassa kyseisellä toimialueella.

RRSIG-tietueet allekirjoittavat muita DNS-tietueita, kuten A-tietueita, varmistaen niiden aitouden. DNSKEY-tietueet puolestaan sisältävät julkisia avaimia, joita käytetään RRSIG-tietueiden allekirjoittamiseen ja varmentamiseen. Selkeä yhteys näiden kahden tietueen välillä on se, että DNSKEY-tietueiden avulla RRSIG-tietueiden digitaaliset allekirjoitukset voidaan varmistaa ja validoida.