

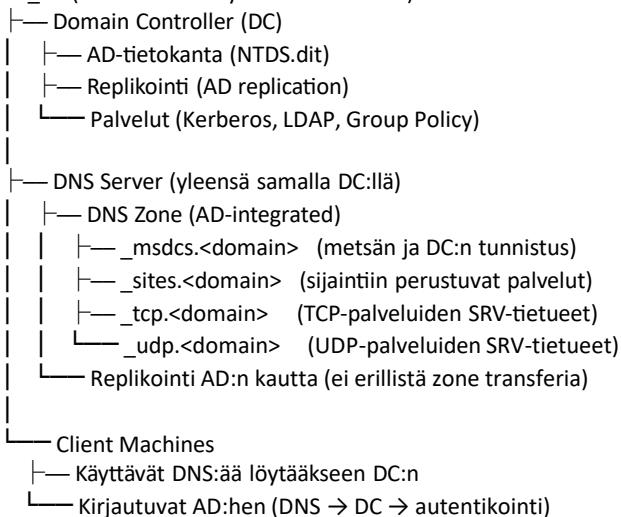
Windows server - AD - DNS

Friday, October 17, 2025 11:00

[Demystifying the AD Integrated DNS: Your Guide for IT Admins](#)



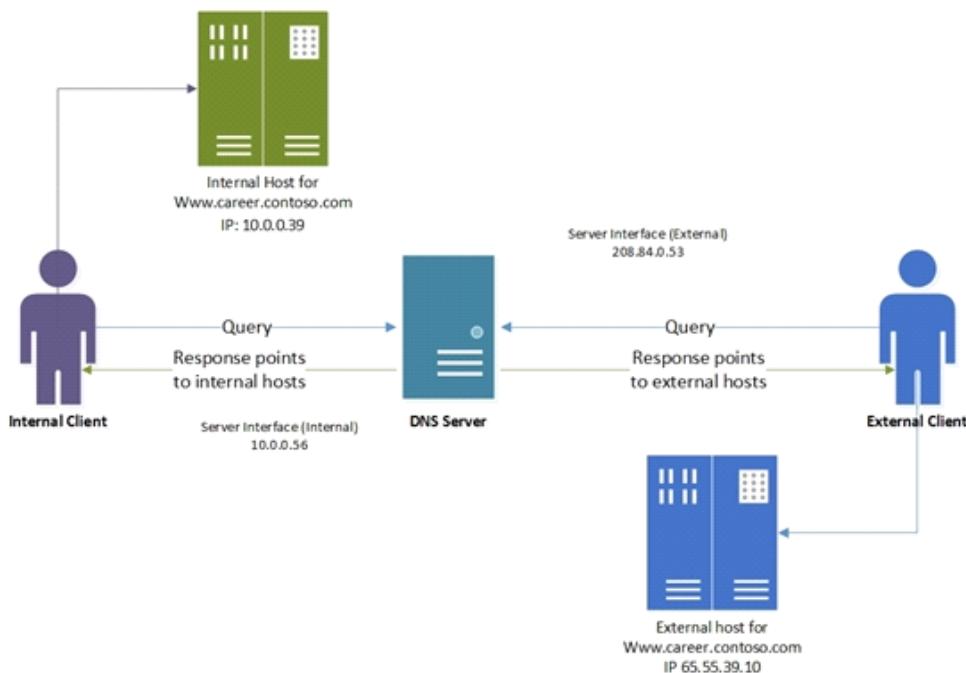
AD_DS (Active Directory Domain Services)



- **DNS server run on domain controller is integrated with Active Directory** → Kun DNS-palvelinrooli ajetaan domain controllerilla, DNS-vyöhykkeet voidaan tallentaa AD DS -tietokantaan. Tätä kutsutaan *AD-integrated DNS zoneksi*.
- **DNS automatically replicates DNS records using AD replication services** → Koska vyöhykkeen tiedot ovat AD:n sisällä, ne replikoituvat automaattisesti samalla mekanismilla kuin itse AD-objektit. Erillistä zone transfer -topologiaa ei tarvita.
- **DNS scales as it is configured on each domain controller deployed and can be configured for load balancing and fail-over** → Jokainen DC, jolla on DNS-rooli, voi toimia kirjoittavana DNS-palvelimena. Tämä mahdollistaa kuormanjakautumisen (load balancing) ja vikasietoisuuden (failover), koska asiakaskoneet voivat käyttää mitä tahansa DC:tä DNS-kyselyihin.

Active Directory -integroitu DNS tarkoittaa, että domain controllerilla ajettava DNS-palvelin tallentaa vyöhyketietonsa AD DS -tietokantaan. Näin DNS-tietueet replikoituvat automaattisesti AD:n replikointipalveluiden avulla ilman erillisiä zone transfer -asetuksia. Jokainen domain controller, jolla on DNS-rooli, voi toimia sekä kyselyiden että päivitysten vastaanottajana, mikä mahdollistaa kuormanjakautumisen ja vikasietoisuuden.

AD ja DNS ovat integroituja yhdessä. AD on riippui DNS:stä (ad on depended on DNS)



how to test to see if my DNS software is Working:

Powershell

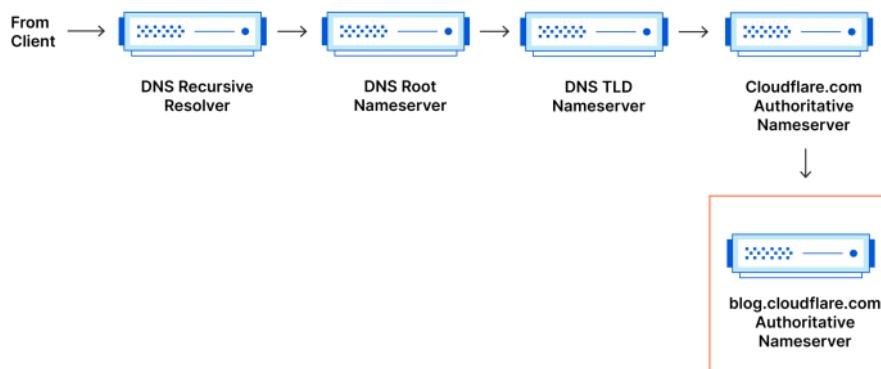
```
$test-netconnection -computername <name> -Port 53
```

Cmd

```
$dns cmd <device> /info
```

Miten DNS record ja konsepti toimii periaatteessa?

CNAME DNS Record Request Sequence



CLIENT (esim. selain pyytää www.google.com)

DNS Recursive Resolver (yleensä operaattorin tai paikallisen verkon DNS)

Root Name Server (.)

TLD Name Server (Top-Level Domain) – esim. .com, .fi, .net

Authoritative Name Server (joka vastaa google.com-alueesta)

Palauttaa IP-osoitteen (esim. 142.250.185.68)

Kun asiakas esimerkiksi kirjoittaa selaimen www.google.com, DNS-resoluutio alkaa. Kysely menee ensin recursive resolverille (esim. reitittimen tai operaattorin DNS-palvelin), joka hakee tietoa välimuistista. Jos tietoa ei ole, resolver kysyy ensin Root-nimipalvelimelta (.), joka ohjaa TLD-nimipalvelimelle (esim. .com). TLD puolestaan ohjaa authoritative nameserverille, joka vastaa varsinaisesta domainista (google.com). Lopulta authoritative server palauttaa IP-osoitteen, ja selain voi ottaa yhteyden palvelimeen.

AD-ympäristössä (eli intranetissä) toimitaan hieman tiiviimmässä DNS-struktuurissa, mutta periaate – **client kysyy > resolver etsii > authoritative vastaa** – on silti täysin sama.

Miten harjoitella AD:n DNS-toimintoja hiekkalaatikossa

1. Rakenna testiverkko VM Workstationissa

- Luo vähintään kaksi virtuaalikonetta:
 - DC1: Windows Server 2019/2022, jossa AD DS ja DNS rootit
 - CLIENT1: Windows 10/11 -työasema, joka liittyy domainiin
- Käytä sisäistä verkkoa (**host-only tai NAT**), jotta koneet näkevät toisensa mutta eivät ulkomaailmaa

2. Asenna ja konfiguroi AD DS ja DNS

- Asenna Active Directory Domain Services ja DNS Server rootit DC1:lle
- Luo uusi domain (esim. test.local)
- Varmista, että DNS toimii:
 - DC1 toimii nimipalvelimena
 - CLIENT1 käyttää DC1:n IP:tä DNS-palvelimena

3. Harjoittele DNS-tehtäviä

- Luo ja hallinnoi vyöhykkeitä (forward/reverse)
- Lisää A-, CNAME-, MX- ja TXT-tietueita
- Testaa SPF/DKIM/DMARC-tyyppisiä TXT-tietueita
- Harjoittele nslookup, ping, ipconfig /displaydns ja dnscmd-komentoja
- Simuloi domain join ja tarkkaile, miten DNS-tietueet syntyvät

Onko DNS:n hallinta päivittäistä?

Riippuu roolista:

Päivittäistä:

- Jos olet järjestelmääsiantuntija, verkkoadmin tai AD-yläpitäjä, DNS voi olla osa päivittäistä vianmääritystä ja valvontaa
- Esim. ongelmat kirjautumisessa, domain joinissa, Outlookin yhteyksissä → usein DNS-taustalla

Satunnaista:

- Jos olet enemmän loppukäyttäjätuen tai M365-puolen rooleissa, DNS voi olla taustalla mutta ei päivittäinen työ
- Silloin DNS liittyy enemmän tietoturvaan (SPF/DKIM/DMARC) tai verkkoyhteyksien vianmääritykseen

AD + DNS -testausympäristö: Vaiheittainen harjoitussuunnitelma

◊ 1. Perusympäristön tarkistus

Varmista, että nämä ovat kunnossa:

- DC1: Windows Server 2019/2022, rootit: **AD DS + DNS**
- Domain: yritysxc.local
- CLIENT1: Windows 10/11, liittynyt domainiin
- DNS toimii: DC1 on nimipalvelin, CLIENT1 käyttää DC1:n IP:tä DNS:ssä

◊ 2. DNS-vyöhykkeiden hallinta

Harjoittele DNS-palvelimen hallintaa:

- Tarkista että **Forward Lookup Zone** yritysxc.local on olemassa
- Luo **Reverse Lookup Zone** (esim. 192.168.1.x → 1.168.192.in-addr.arpa)
- Lisää manuaalisesti:
 - A-tietueita (esim. intra.yritysxc.local → 192.168.1.10)
 - CNAME-tietueita (alias esim. helpdesk → intra.yritysxc.local)
 - MX-tietue (simuloitu sähköpostipalvelin)
 - TXT-tietueita (esim. SPF: "v=spf1 a mx ~all")

Testaa:

- nslookup intra.yritysxc.local
- ping helpdesk.yritysxc.local
- ipconfig /displaydns

◊ 3. GPO-sääntöjen testaus

Luo ja linkitä GPO:

- Esim. kirjautumisviesti, taustakuva, USB-estot, palomuurisäännöt
- Linkitä OU:hun, jossa CLIENT1 sijaitsee
- Testaa vaikutus kirjautumalla CLIENT1:lle

◊ 4. Käyttäjähallinta ja OU-rakenne

- Luo OU-rakenne: esim. Henkilöstö, IT, Johto
- Luo testikäyttäjiä ja ryhmät
- Delegoi hallintaoikeuksia OU-tasolla (esim. IT saa hallita Henkilöstö-OU:ta)

◊ 5. PowerShell-harjoitukset

- Luo käyttäjiä PowerShellillä
- Hae ryhmän jäsenet
- Luo raportti: kaikki käyttäjät + viimeinen kirjautumisaika
- Muokkaa DNS-tietueita PowerShellillä (Add-DnsServerResourceRecordA jne.)

◊ 6. Simuloi vikatilanteita

- Poista DNS-tietue → testaa domain joinin epäonnistuminen
- Luo ristiriittainen GPO → testaa mikä säädöntö voittaa
- Simuloi nimipalvelinongelma → muuta CLIENT1:n DNS-asetuksia väärin

◊ 7. Valvonta ja auditointi

- Ota käyttöön **auditointipolitiikat** GPO:lla
- Tarkkaile **Security Event Logia** DC1:llä
- Testaa kirjautumisten, GPO-muutosten ja epäonnistuneiden kirjautumisyritysten lokit

◊ 8. Valmistautuminen hybridiin

- Asenna **Azure AD Connect** (ei tarvitse vielä yhdistää)
- Tutki synkronointiasetuksia
- Luo testikäyttäjiä, jotka olisi tarkoitus synkronoida

```
#####
#####
```

❖ Lisäharjoituksia AD + DNS -ympäristöön

⌚ 1. AD Certificate Services (AD CS)

- Asenna ja konfiguroi **sertifikaattipalvelin**
- Luo **sisäinen CA** ja testaa koneiden tai käyttäjien sertifikaattien jakelua
- Simuloi **HTTPS-palvelua** omalla sertifikaatilla

✳️ 2. Conditional Access / Group Membership

- Luo ryhmät ja testaa **ryhmäperusteisia GPO-sääntöjä**
- Simuloi tilannetta, jossa vain tietyt ryhmän jäsenet saavat tietyn asetuksen

📝 3. AD Replikointi

- Lisää toinen DC (DC2) ja testaa **replikointia**
- Simuloi replikointivirheitä (esim. DNS-ongelma tai aikavirhe)

📅 4. Dynamic DNS ja DHCP-integraatio

- Asenna DHCP-palvelin ja konfiguroi se päivittämään DNS-tietueet automaattisesti
- Testaa, miten uudet koneet saavat DNS-tietueet dynaamisesti

⌚ Yksittäinen AD-ominaisuus: **Group Policy Preferences (GPP)**

Jos haluat nyt keskittyä yhteen AD-ominaisuuteen, **Group Policy Preferences** on erinomainen valinta. Se laajentaa GPO:n mahdollisuuksia ja on usein alikäytetty.

🔧 Harjoitus: Luo GPP-asetuksia

1. Avaa Group Policy Management Console (GPMC)
2. Luo uusi GPO ja mene kohtaan: Computer Configuration > Preferences > Windows Settings > Registry / Files / Shortcuts
3. Tee jokin näistä:
 - Luo **rekisteriavain** (esim. estä USB)
 - Lisää **tiedosto** koneelle
 - Luo **pikakuvake työpöydälle**
4. Linkitä GPO haluttuun OU:hun
5. Testaa vaikutus CLIENT1-koneella

⌚ GPP:llä voit tehdä asioita, joita tavallinen GPO ei tue — kuten kopioida tiedostoja, luoda kansioita, muokata rekisteriä ilman skriptejä.

<https://activedirectorypro.com/dns-best-practices/>

#####
#####

AD (active directory) windows serveri nettiasetus

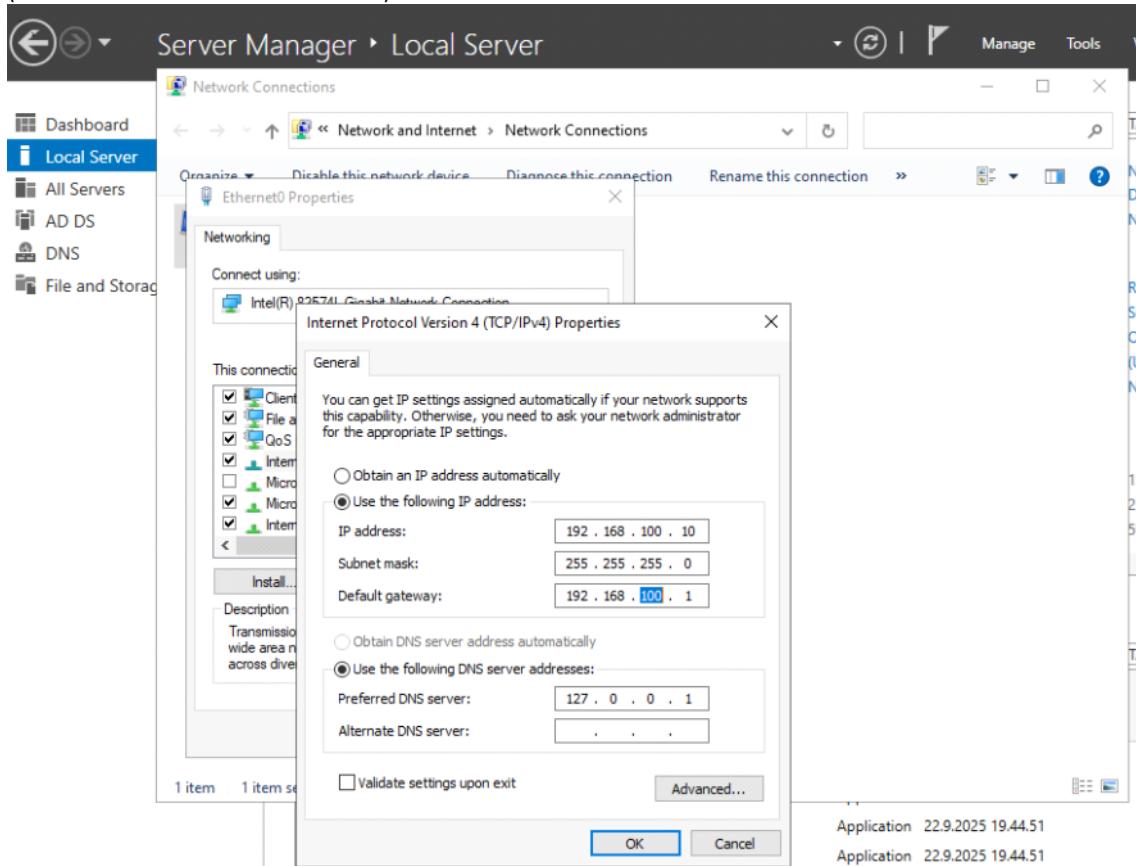
Tämä kappale koskee yleisesti Windows serverin DNS asetusta, että vmworkstation toisen tai useamman VM2 , 3 ja jne 4 työasema (Win 10/11) ottavat yhteyttä ja liittävät yhteyttä serveriin saadakseen yhteyttä ja päästään nettiin.

IPv6:ta ei kannata koskaan poistaa käytöstä Windows Serverissä, varsinkaan *domain controllerilla*, koska Microsoft ei tue sen poistamista ja monet palvelut (esim. Active Directory, DNS, Exchange) käyttävät IPv6:ta taustalla. Jos verkossasi on domain kuten *yritysxc.local*, IPv6:n poistaminen voi aiheuttaa toimintahäiriötä DNS-resolvointiin ja AD:n replikointiin.

Jos verkossasi on domain esimerkiksi *yritysxc.local*, IPv6:n poistaminen voi aiheuttaa:

- toimintahäiriötä DNS-resolvointiin
- ongelmia AD:n replikoinnissa
- tilanteita, joissa käyttäjät eivät saa yhteyttä Windows Serveriin
- Usein sitä ei kosketakaan ja jätä se oletuksena päälle.

(TOISESTA SIVUSTOLTA OTETTU KUVA)



Tässä asetettu osoitteena joka toimii kuin yksittäisen windows serverin IP-osoite, että määritetty kuin kotiosote.

- IP: 192.168.100.10
- IP osoitteiden laskenta usein se on luokitus siksi menee: 255.255.255.0 /24 maski , sekä default gateway: 192.168.100.1 (väh ä kuin osoitteen numero, mutta num. 10 on kuin missä kerroksen numero).

DNS-asetukset domain controllerilla

Nyt koskien Preferred DNS ja Alternate DNS -palvelimia:

- Usein näkee, että Preferred DNS asetetaan julkiseksi osoitteeksi, kuten **8.8.8.8 (Google DNS)**.
 - Tätä ei saa tehdä, koska Google DNS ei tunne sisäistä domainiasi (*yritysxc.local*) eikä pysty ratkaisemaan domain controllerin nimiä.
 - Tämän seurauksena Active Directoryn replikointi ja domainin liittyminen voivat epäonnistua.
- Oikea käytäntö on asettaa Preferred DNS osoittamaan **domain controlleriin itseensä** (esim. sen oma IP-osoite tai loopback-osoite **127.0.0.1**).
 - Näin varmistetaan, että kaikki sisäiset AD- ja DNS-kyselyt ratkaistaan oikein.
 - Jos verkossa on useampi DC, Alternate DNS voidaan asettaa toisen DC:n IP-osoitteeksi.

- Jos halutaan, että DC pystyy ratkaisemaan myös internet-nimet, tämä tehdään **DNS Managerin Forwarders-asetuksilla**, jolloin ulkoiset kyselyt ohjataan esim. 8.8.8.8:aan.
- Älä koskaan käytä julkista DNS:ää (8.8.8.8) Preferred DNS:ssä domain controllerilla.
- Preferred DNS = DC:n oma IP (tai 127.0.0.1).
- Alternate DNS = toinen DC, jos sellainen on.
- Forwarders = julkiset DNS:t internet-nimiä varten.
- Älä käytä 8.8.8.8 Preferred/Alternate DNS:ssä domain controllerilla.

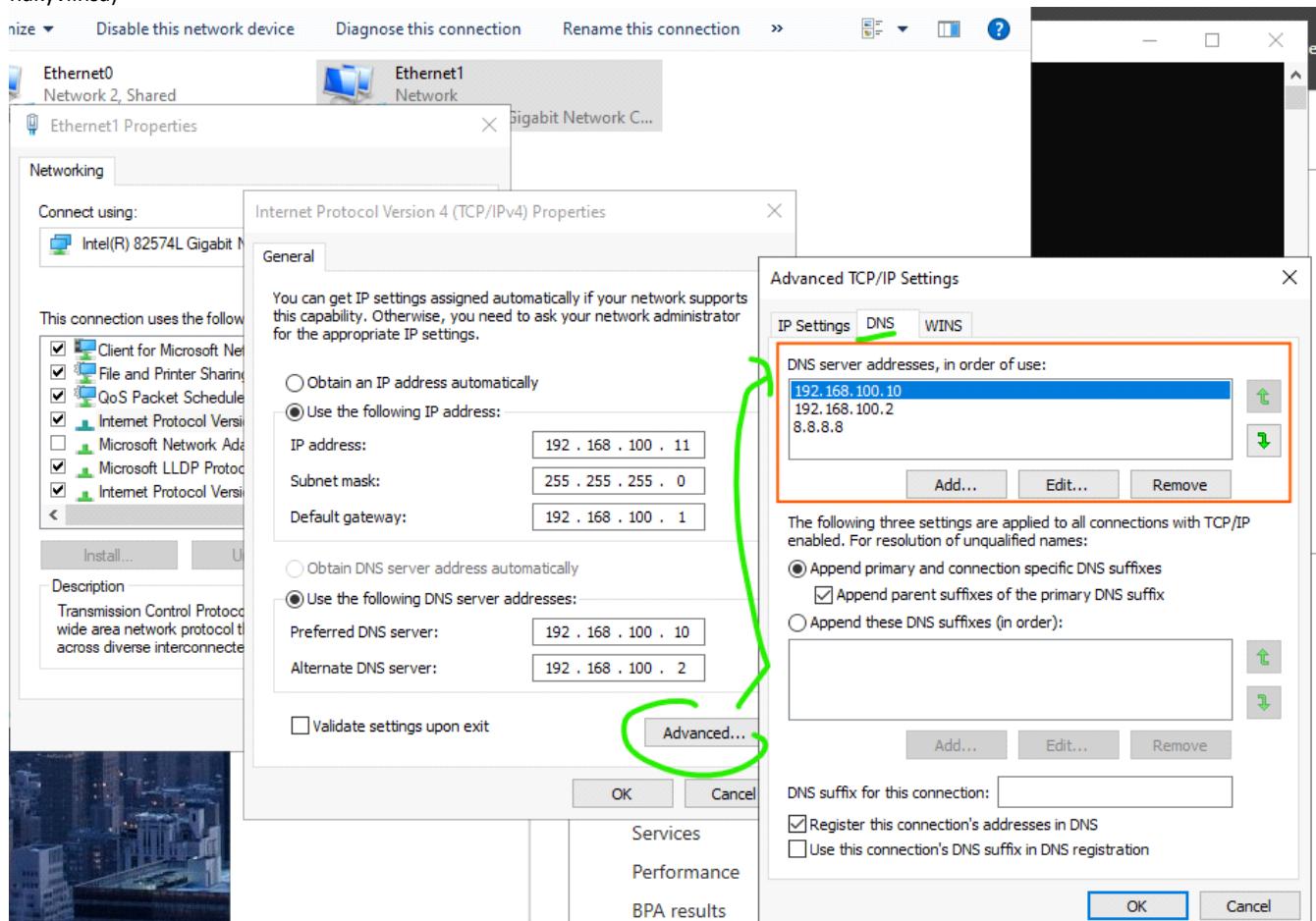
Preferred DNS domain controllerilla

- Jos domain controllerin (DC) IP-osoite on **192.168.100.10**, sen voi ja **pitää** asettaa Preferred DNS:ksi.
- Tämä ei aiheuta hitautta, vaan päinvastoin varmistaa, että AD:n sisäiset DNS-kyselyt (esim. *yritysxc.local*) ratkaistaan oikein.
- Hitaus syntyy yleensä silloin, jos Preferred DNS osoittaa **vääärään paikkaan** (esim. julkiseen DNS:ään), jolloin AD-nimet eivät ratkeaa ja kone yrittää turhaan kysellä ulkoja.

Alternate DNS ja Google DNS

- **Alternate DNS**: kannattaa asettaa toisen domain controllerin IP-osoitteeksi, jos sellainen on.
- Jos sinulla on vain yksi DC, Alternate DNS:n voi jättää tyhjäksi.
- **Google DNS (8.8.8.8)** ei ole hyvä vaihtoehto Alternate DNS:ksi domain controllerilla, koska se ei tunne sisäistä domainiasi.
 - Jos DC joutuu kysymään Alternate DNS:itä, se ei saa vastausta AD:nimistä → ongelmia replikoinnissa ja kirjautumisessa.
 - Oikea tapa käyttää Google DNS:ää on **DNS Managerin Forwarders-asetuksissa**, jolloin ulkoiset kyselyt ohjataan sinne, mutta sisäiset kyselyt ratkaistaan aina AD:n DNS:llä.
- Jos on lisää DNS IP-osoiteita niin voi erikseen asettaa

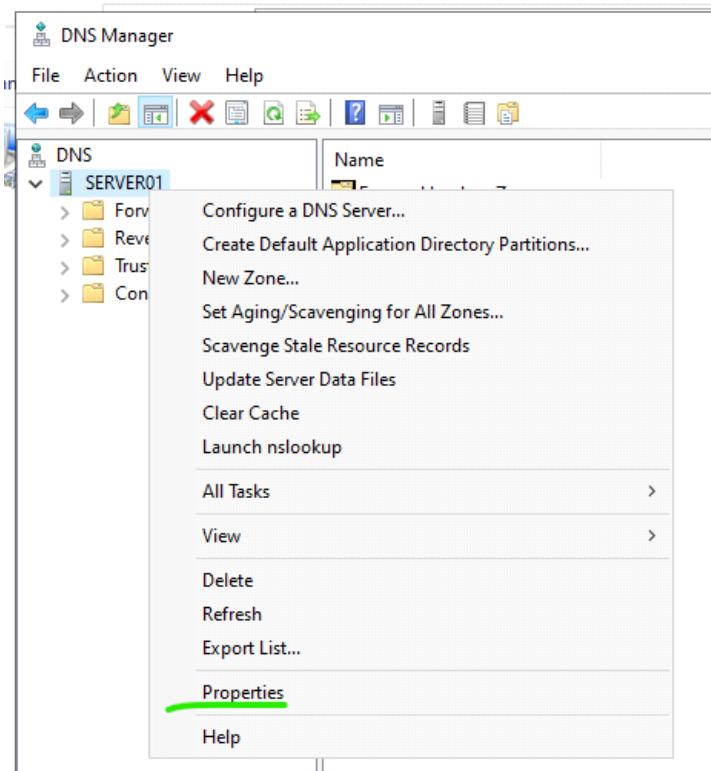
Yleensä kaksi on ok, mutta jos on useampi DNS IP-osoite niin lisääällä (ADD ja lisää kyseisen DNS IP-osoitteen niin se tulee tähän alle näkyviinsä)



DNS Server manager

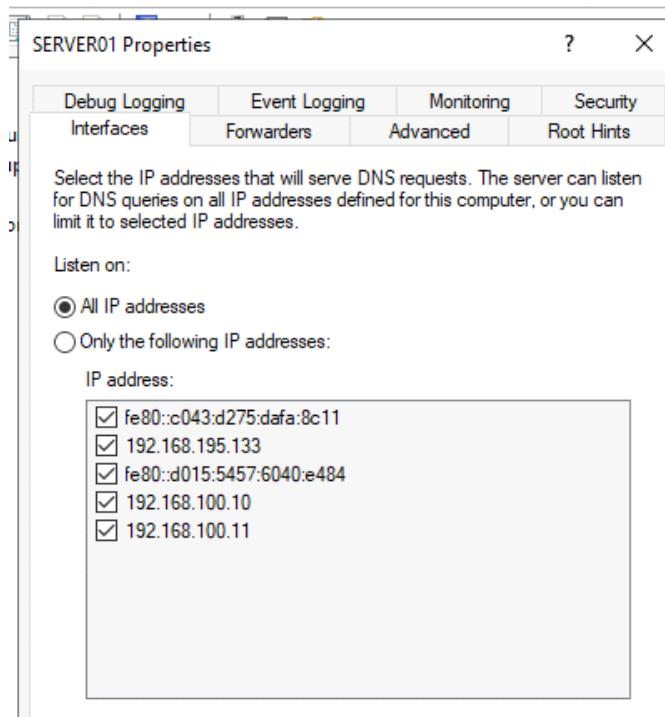
Tämä on serveri manageri ja tästä saa >>> server manager >> Tools >> DNS

Aava seuraavaksi "Ominaisuudet"



Tämä on sama lista kuin se verkkoasetuksen IPV4, jos ei käytä IPV6:sta se voi asettaa pois ja tässä tärkeänä on pitää se Windows serverin siis Active Directory IP-osoite päällä kokoajan kun sitä käytetään ja muut voi esim. Sulkea. Tämä vaikuttaa myös nettin jakamiseen.

- Koska VM1 kun asennettu toisen verkkokorttin, josta ensimmäinen menee NAT hakee nettistä päivitystä ja toisessa verkkokorttissa käyttääneen VM2, 3 ja jne Host only yhteyttä, josta ideana kuin toimii fyysinen yhteys saadakseen yhteyttä VM1 windows serveristä yhteyttä.



DNS Managerin "Forwarders"-kohtaan voidaan asettaa Google julkinen DNS ja kannattaa asettaa (esim. 8.8.8.8 tai 1.1.1.1), **mutta vain forwarderiksi**, ei Preferred DNS:ksi.

- Google julkinen DNS 8.8.8.8
- Cloudflare julkinen DNS 1.1.1.1

Mikä on DNS Forwarder ja mielin se vaikuttaa?

- **Forwarder** on DNS-palvelimen asetus, joka kertoo mielin ulkoihin DNS-kyselyihin ohjataan, jos oma DNS ei osaa vastata.
- Esimerkiksi jos käyttäjä haluaa päästää osoitteeseen www.microsoft.com, mutta domain controllerin DNS ei tunne sitä, se

forwardaa kyselyn eteenpäin esim. Google DNS:lle (8.8.8.8).

- Tämä ei vaikuta sisäisiin kyselyihin kuten vm2.yritysxc.local, jotka ratkaistaan AD:n omalla DNS:llä.

💻 Voiko VM2 päästää nettiin, jos DC:llä on forwarder?

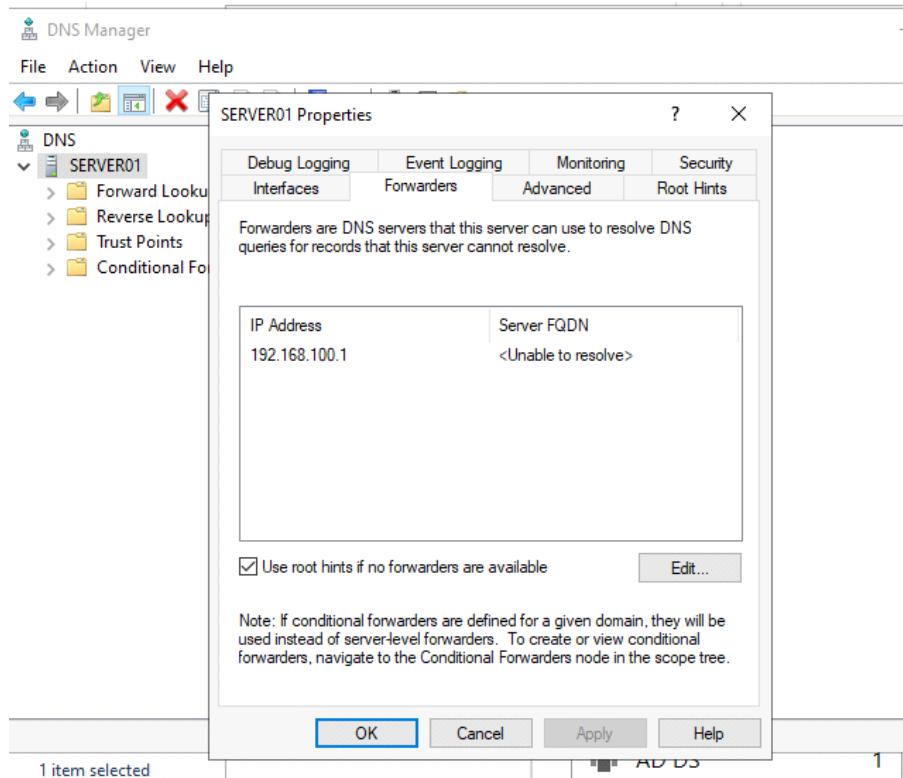
Kyllä voi, jos nämä ehdot täytyvät:

- VM2:n DNS-asetuksissa on domain controllerin IP (esim. 192.168.100.10) Preferred DNS:ksi.
- Domain controllerilla on asetettu **Forwarder** esim. 8.8.8.8.
- Verkkoyhteys (reitti) ulos internetiin on sallittu (esim. NAT tai reititin).

Tällöin VM2 kysyy DC:ltä DNS-nimeä → DC ei tiedä www.microsoft.com → DC kysyy Google DNS:ltä → palauttaa IP VM2:lle → VM2 pääsee nettiin.

Samaan tähän voi konfiguroida VLAN:ia, ja kertauksen VLAN on verkkoporttien määritys. Jos vmworkstation asennettaisiin lisää VLAN niin jouduttaisin lisätä useita verkkokortteja.

- VLAN (Virtual LAN) ei ole pelkkä ohjelmallinen asetus, vaan se liittyy suoraan **verkkolaitteistoon** – erityisesti **verkkokortteihin, kytkimiin ja reitittimiin** kuten Cisco-laitteisiin.
- Windows Server ei hallinnoi VLANejä suoraan DNS Managerissa, vaan VLAN-konfigurointi tehdään **verkkosovittimen asetuksissa tai NIC Teaming -toiminnoilla**.



Sivullinen harjoitus

Tässä lisätään forwarderin alle pari julkista DNS IP-osoitetta - Google ja Cloudflare. **Cloudflare (1.1.1.1)** ja **Google DNS (8.8.8.8 & 8.8.4.4)** Forwarders-asetukseen DNS Managerissa. Se on itse asiassa **suositeltu tapa** varmistaa, että Windows Serveri pystyy ratkaisemaan ulkoisia DNS-nimiä (esim. www.microsoft.com), vaikka sinulla ei olisi omaa nettisivustoa käytössä.

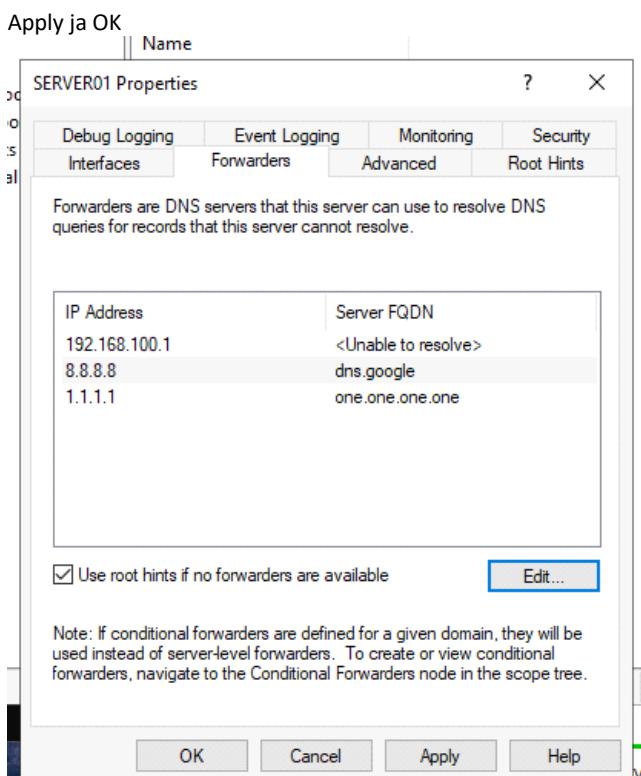
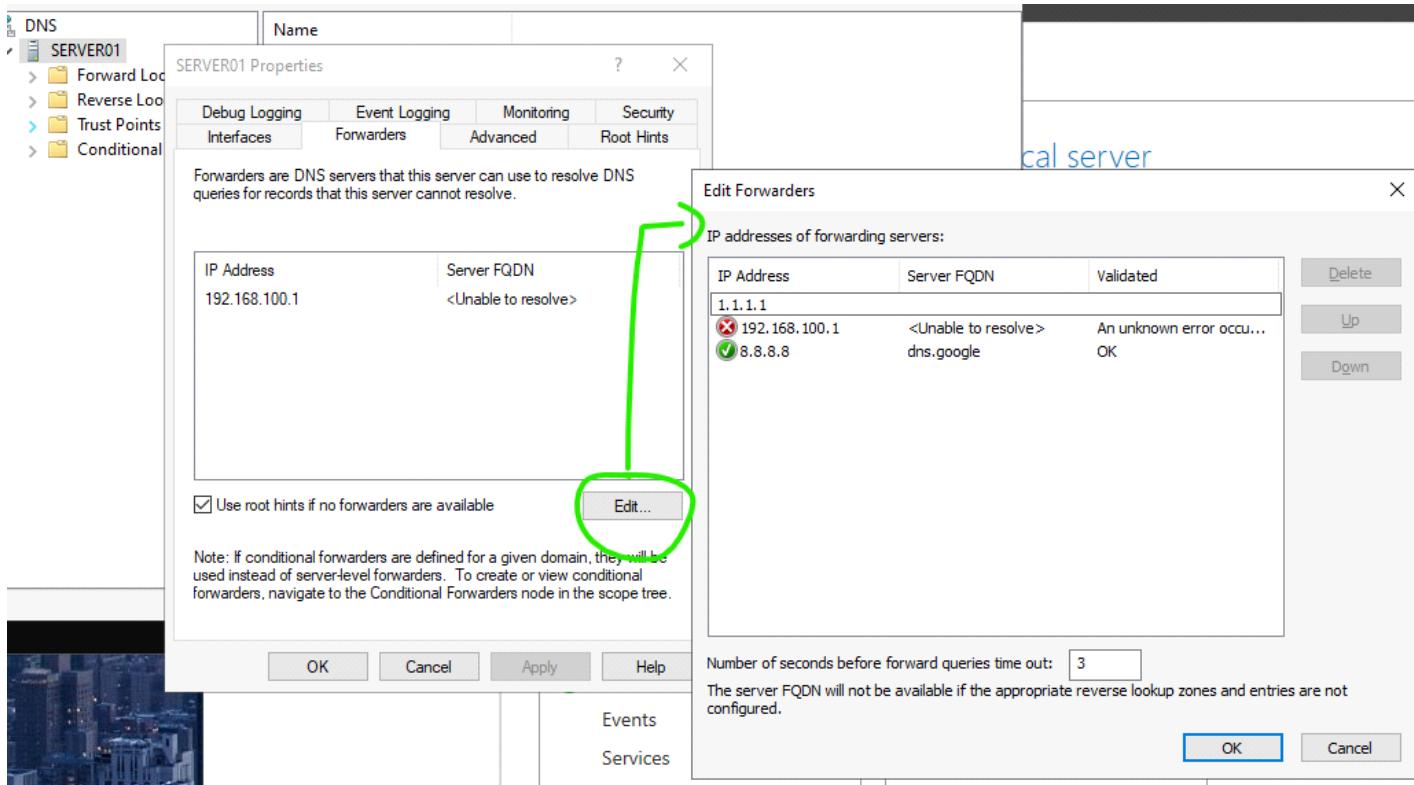
🔄 Miksi forwarderit kannattaa määrittää?

- Forwarderit ohjaavat DNS-kyselyt eteenpäin, jos Windows Serverin DNS ei osaa ratkaista nimeä itse.
- Tämä koskee **ulkopuolisia nimiä**, ei sisäisiä (esim. vm2.yritysxc.local).
- Jos sinulla ei ole omaa nettisivustoa, mutta haluat että palvelin ja verkon koneet pääsevät internetiin, forwarderit ovat tarpeen.

💻 Entä asiakas/käyttäjäkone (esim. VM2)?

- VM2:n DNS-asetuksissa tulee olla **domain controllerin IP** (esim. 192.168.100.10).
- VM2 kysyy DNS-nimiä DC:ltä → DC ratkaisee sisäiset nimet itse → ulkoiset nimet se forwardaa Cloudflarelle tai Googelle.
- Näin VM2 pääsee nettiin, vaikka se ei itse käytä julkisia DNS:iä suoraan.

Riittää syöttää 8.8.8 ja 1.1.1.1 ja enter, niin se ponnahtaa alas jotenkin jännästi ja OK



Seuraavaksi voi testata sen hyppyä (hop count), että kuinka kauan siinä menee ja käyttääneen powershell terminaalia. Tämä komento kertoo että kauan siinä DNS serverissä menekään esim. Google DNS julkisen IP-osoitteensa kanssa. Näiden millisekunnista luvut kertovat **viiveen (latenssin)** eli kuinka kauan kestää, että paketti kulkee koneeltasi kyseiseen IP-osoitteesseen ja takaisin.

- Esim. Tässä meni 14 hyppyä ja n. 4ms

```

PS C:\Users\Administrator> tracert -d 8.8.8.8

Tracing route to 8.8.8.8 over a maximum of 30 hops

 1 <1 ms    <1 ms    <1 ms  192.168.195.2
 2 *          *          * Request timed out.
 3 *          *          * Request timed out.
 4 *          *          * Request timed out.
 5 *          *          * Request timed out.
 6 *          *          * Request timed out.
 7 *          *          * Request timed out.
 8 *          *          * Request timed out.
 9 *          *          * Request timed out.
10 *          *          * Request timed out.
11 *          *          * Request timed out.
12 *          *          * Request timed out.
13 *          *          * Request timed out.
14 5 ms      4 ms      4 ms  8.8.8.8

Trace complete.
PS C:\Users\Administrator>

```

Testataan esim. Toinen cloudflare DNS osoite

- Ei paljoo nopeuttanut n. 6ms

```

PS C:\Users\Administrator> tracert -d 1.1.1.1

Tracing route to 1.1.1.1 over a maximum of 30 hops

 1 <1 ms    <1 ms    <1 ms  192.168.195.2
 2 *          *          * Request timed out.
 3 *          *          * Request timed out.
 4 *          *          * Request timed out.
 5 *          *          * Request timed out.
 6 *          *          * Request timed out.
 7 *          *          * Request timed out.
 8 *          *          * Request timed out.
 9 *          *          * Request timed out.
10 *          *          * Request timed out.
11 *          *          * Request timed out.
12 8 ms      6 ms      6 ms  1.1.1.1

```

Nopeuden järjestys onko väliä?

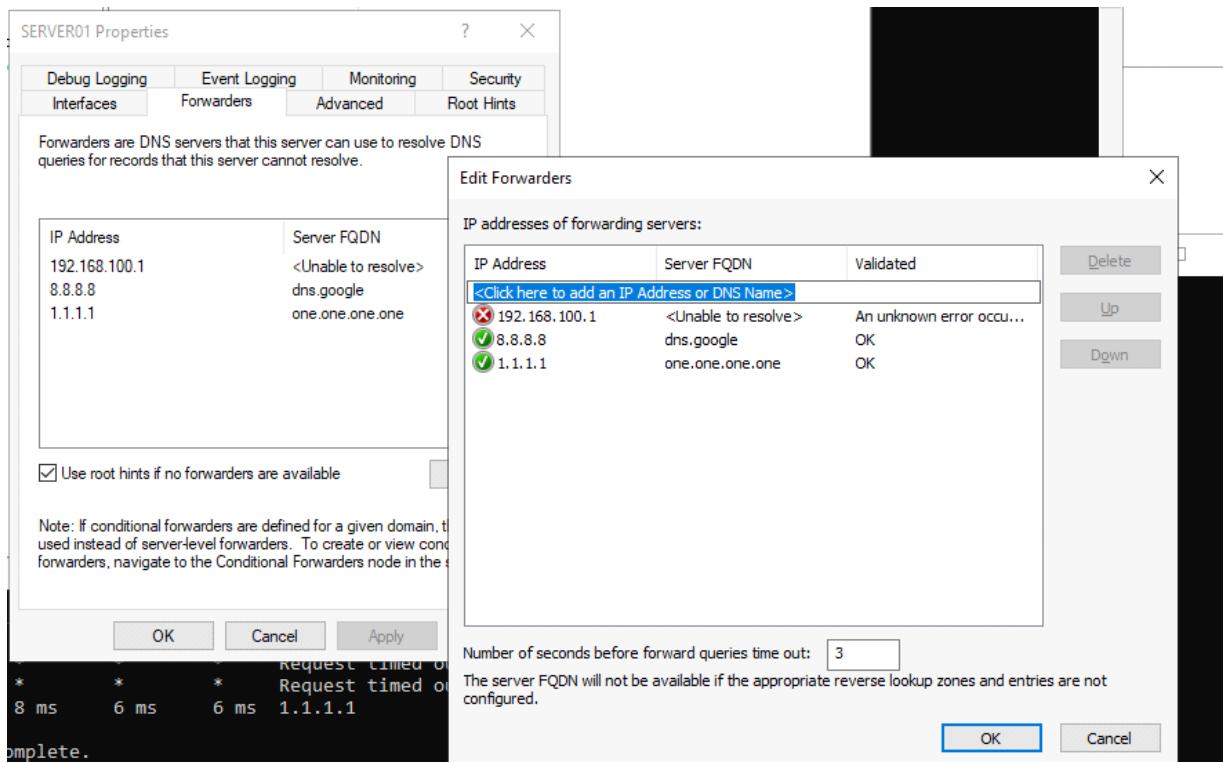
Forwarders-järjestyksen merkitys

- Windows Serverin DNS Managerissa forwarderit ovat **listassa järjestyksessä**.
- Käytännössä palvelin **kokeilee ensimmäistä forwarderia** (tässä 192.168.100.10).
- Jos se ei vastaa, se siirtyy seuraavaan (8.8.8.8), ja jos sekäkin ei vastaa, sitten seuraavaan (1.1.1.1).
- Eli järjestyksellä on väliä: ensimmäinen on aina ensisijainen, muut ovat varalla.

Nopeus vs. järjestys

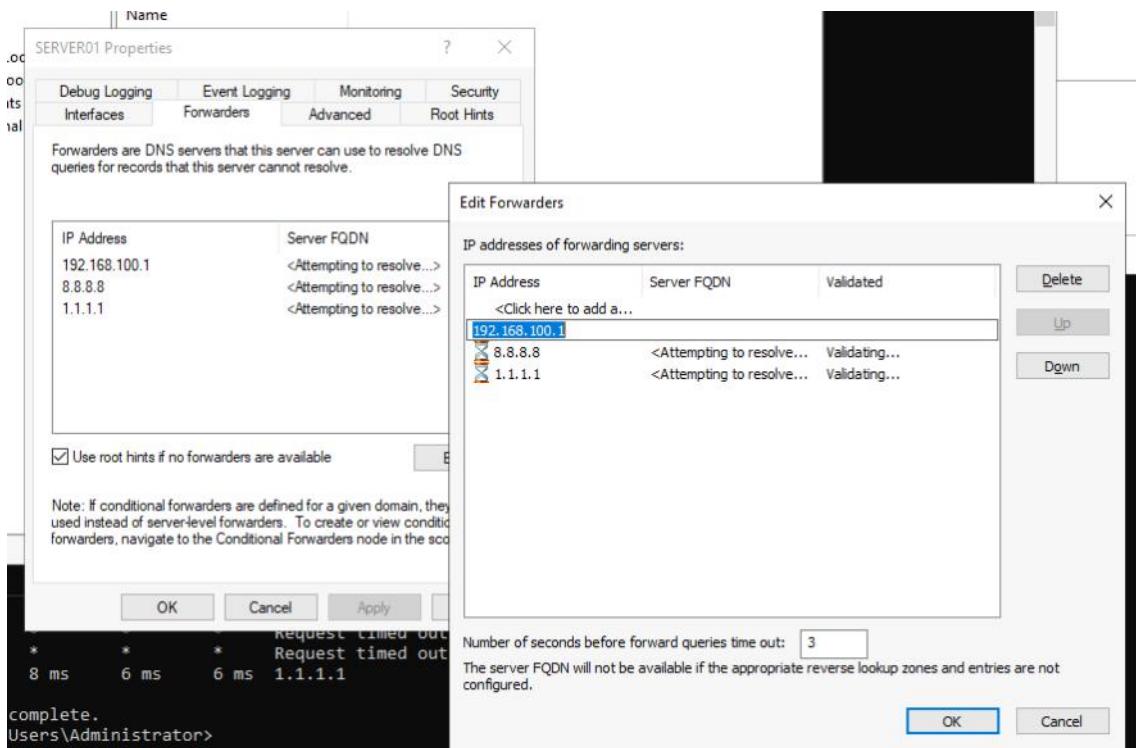
- DNS-palvelin **ei tee nopeustestiä** forwardereiden välillä, vaan käyttää listan ensimmäistä.
- Jos ensimmäinen forwarder toimii, se ei koskaan siirry seuraaviin, vaikka ne olisivat teoriassa nopeampia.
- Nopeus (ms) näkyy tracertissa, mutta DNS-resolvointi on yleensä niin nopeaa (<10 ms), ettei erolla ole käytännön merkitystä.

- Älä laita DC:n omaa IP:tä forwarderiksi. DC ratkaisee sisäiset nimet itse, forwardereita käytetään vain ulkoisiin nimiin.
- Järjestää forwarderit esim. näin:
 - 1.1.1.1 (Cloudflare)
 - 8.8.8.8 (Google)

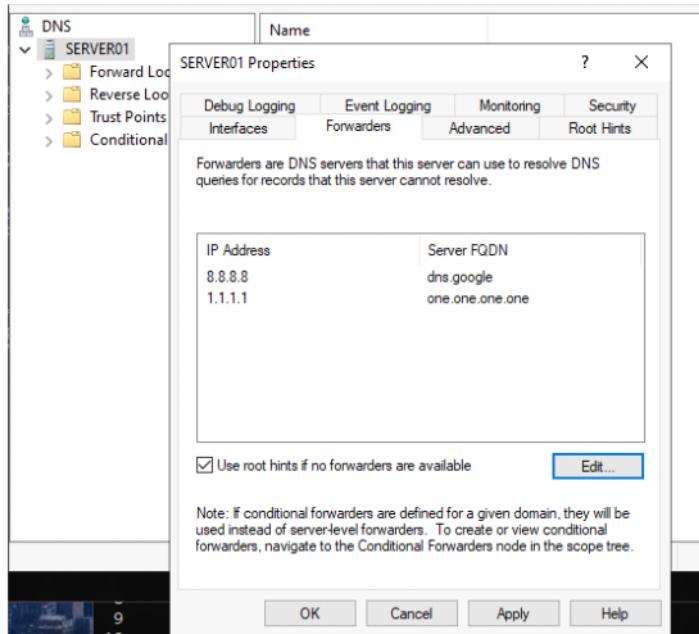


Miksi 192.168.100.1 kannattaa poistaa forwardereista?

- 192.168.100.1 näyttää olevan sisäverkon reitin tai gateway, ei varsinainen DNS-palvelin.
- Jos se ei ole konfiguroitu DNS-palvelimeksi, se ei osaa vastata DNS-kyselyihin kunnolla → aiheuttaa viiveitä tai virheitä.
- Kuvassa näkyy, että sen kohdalla lukee "Attempting to resolve..." ja "Validating...", mikä viittaa siihen, ettei se vastaa odotetusti.



Apply ja OK



Mitä olet oppinut DNS-asetuksista

- **DNS Forwarders:** Ne ohjaavat ulkoiset nimikyselyt (esim. www.microsoft.com) eteenpäin julkisille DNS-palvelimille kuten Google (8.8.8.8) ja Cloudflare (1.1.1.1).
- **Preferred DNS vs. Forwarders:** Preferred DNS on se, mitä asiakaskoneet käyttävät – Forwarders ovat palvelimen sisäisiä asetuksia ulkoisia nimiä varten.
- **Julkisia DNS-osoitteita ei pidä käyttää Preferred DNS:ssä domain controllerilla**, koska ne eivät tunne sisäistä domainiasi.
- **Tracert ja viiveet (ms):** Opit tulkitsemaan vastaikoa ja ymmärtämään, että nopeus ei aina tarkoita paremmuutta, vaan vakaus ja oikea reititys ovat tärkeämpää.
- **VLAN-konsepti:** VLANit eivät liity DNS:ään suoraan, mutta ne vaikuttavat verkon segmentointiin ja siihen, miten DNS-palvelin tavoitetaan eri verkkoalueilta.

Mitä voit tehdä seuraavaksi (jatkotoimenpiteet)

1. **Tarkista asiakaskoneiden DNS-asetukset**
 - Varmista, että ne käyttävät domain controllerin IP:tä (esim. 192.168.100.10) Preferred DNS:ksi.
 - Älä anna niiden käyttää julkisia DNS:ä suoraan.
2. **Optimoi DNS Managerin asetukset**
 - Poista sisäverkon IP:t forwardereista, jos ne eivät ole oikeita DNS-palvelimia.
 - Järjestä forwarderit: esim. 1.1.1.1 ensin, 8.8.8.8 toisena.
3. **Testaa DNS-resolvointi käytännössä**
 - Käytä nslookup-komentoa testataksesi, miten nimet ratkeavat.
 - Voit kokeilla sekä sisäisiä nimiä (vm2.yritysxc.local) että ulkoisia (www.microsoft.com).
4. **Dokumentoi verkon DNS-rakenne**
 - Tee selkeä kaavio: missä DNS-palvelin sijaitsee, mitä forwardereita käytetään, miten asiakaskoneet on konfiguroitu.
 - Tämä auttaa vianhallinnassa ja verkon laajennuksessa.
5. **Varmista palomuurin ja reitityksen toimivuus**
 - DNS käyttää porttia UDP 53 – varmista, ettei se ole estetty VLANien tai reittimen välillä.

Mitä tämä opettaa verkonhallinnasta

- DNS ei ole vain "nimi-IP" -muunnin – se on **kriittinen osa verkon toimintaa**, erityisesti Active Directory -ympäristössä.
- Oikea DNS-konfiguraatio takaa:
 - Nopean ja luotettavan nimiresolvoinnin
 - Toimivan domainin ja kirjautumisen
 - Vakaan yhteyden internettiin ja sisäverkkoon