

Nimipalvelut



Tämän palvelun käyttö sisältyy Funet-jäsenmaksuun.

Kuvaus

Funet-jäsenorganisaation DNS-nimipalvelun eri komponentteja voidaan toteuttaa Funetin nimipalvelimilla. Jäsenorganisaatio välttyy tällöin omien nimipalvelinlaitteiden ja -ohjelmistojen ylläpidolta. Palveluun voidaan joustavasti sisällyttää seuraavia komponentteja:

- resolvointipalvelu ns-cache.funet.fi
- päänimipalvelu ja nimipalvelutietojen hallintakäyttöliittymä
- varanimipalvelu ns-secondary.funet.fi

Tältä sivulta löytyy vastauksia esimerkiksi seuraaviin tilanteisiin:

- Haluan määritellä nimipalvelimet (name servers) työasemaan/päätelaitteeseen – ks. [resolvointipalvelu](#)
- Tarvitsen nimipalvelimet verkkotunnukselleni – ks. [päänimipalvelu](#)
- Haluan varmistaa verkkotunnusteni nimipalvelun toiminnan omien nimipalvelimieni huolto- ja vikatilanteissa – ks. [varanimipalvelu](#)

Resolvointipalvelu ns-cache.funet.fi

Resolvointipalvelun nimipalvelimia voidaan käyttää tavallisten päätelaitteiden, kuten esimerkiksi tietokoneiden nimipalvelinmäärittelyssä palvelinlaitteina (name server). Toinen mahdollinen käyttötapa on nimipalvelukyselyjen keskitetty ohjaaminen jäsenorganisaation omista resolvointipalvelimista ns-cache.funet.fi-palvelimiin (ns. forwarder-käyttö).

Palvelua käyttävän jäsenorganisaation ei tarvitse välttämättä ylläpitää omaa nimipalvelinta. Oman nimipalvelimen käyttö on kuitenkin suositeltavaa teknisistä suorituskykyisistä, mikäli verkon käyttö on laajaa. Huomaa myös, että jos Funet-yhteys katkeaa, resolvointipalvelun puuttuminen voi haitata paikallisverkon toimintaa.

Palvelussa on täysi IPv6- ja IPv4-tuki. DNSSEC-validointi otettiin käyttöön tammikuussa 2012.

Päänimipalveluja nimipalvelutietojen ylläpitokäyttöliittymä

Päänimipalvelun jäsenorganisaation verkkotunnuksen auktoritatiivisina nimipalvelimina voidaan käyttää Funetin nimipalvelimia:

- ns.funet.fi
- ns2.funet.fi
- ns-secondary.funet.fi

Palvelua käyttävien verkkotunnusten nimi- ja IP-osoitetietoja jäsenorganisaatio voi ylläpitää itse www-käyttöliittymällä, jonne jäsenorganisaatiolle luodaan pyynnöstä omat käyttäjätunnukset omien verkkotunnustensa DNS-tietueiden ylläpitämistä varten.

Palvelu tukee täysin sekä IPv6- että IPv4-osoitteita, tavallisia ns. forward-verkkotunnuksia ja käänteisnimipalvelua. Palvelu ei sovellu suoraan Dynamic DNS Update ([RFC 2136](#)) -menetelmällä hallittaville verkkotunnuksille. Palvelu ei toimi DNS-resolverina (vrt. ns-cache.funet.fi-palvelu).

Varanimipalvelu ns-secondary.funet.fi

ns-secondary.funet.fi-palvelua voidaan käyttää jäsenorganisaation verkkotunnusten (esim. organisaatio.fi) varanimipalvelimena. Päänimipalvelimena voi tällöin olla joko Funetin päänimipalvelu tai jäsenorganisaation oma päänimipalvelin. ns-secondary.funet.fi:n käyttöä suositellaan kaikkien Funetin jakamien IP-osoitteiden käänteisnimipalvelussa.

Palvelun tarkoitus on parantaa jäsenorganisaatioiden verkkotunnusten määräävän nimipalvelun saavutettavuutta Internetistä. Palvelua kannattaa käyttää erityisesti silloin, jos jäsenorganisaation omat nimipalvelut sekä niiden Internet-yhteydet eivät ole vikasietoisia.

Palvelu tukee täysin sekä IPv6- että IPv4-osoitteita, tavallisia ns. forward-verkkotunnuksia ja käänteisnimipalvelua. Zone-päivitykset jäsenorganisaation omista päänimipalvelimista ns-secondary.funet.fi-palveluun on mahdollista varmentaa TSIG-menetelmällä. Palvelu tukee DNS NOTIFY -menetelmää ([RFC 1996](#)) zone-päivitysten nopeuttamiseksi. Palvelu ei toimi DNS-resolverina (vrt. ns-cache.funet.fi-palvelu).

Käyttöönotto

Resolvointipalvelu ns-cache.funet.fi

Palvelu on käytettävissä Funet-asiakasyhteyden kautta ilman erillisiä Funetin toimenpiteitä. Tietoturvasyistä palvelua ei kuitenkaan voi käyttää sellaisista jäsenorganisaation verkoista, jotka on liitetty Internetiin myös muiden kuin Funet-verkon kautta. Ota halutessasi yhteyttä Funet Hostmasteriin: [Yhteystiedot](#).

Palveluosoitteet:

IPv6	IPv4
------	------

2001:708::53:1	193.166.4.24
2001:708::53:2	193.166.4.25

Päänimipalvelu ja nimipalvelutietojen ylläpitokäyttöliittymä

Yhteydenottoa Funet Hostmasterille edellyttäviä asioita ovat:

- päänimipalvelun käyttöönotto verkkotunnukselle (esim. organisaatio.fi)
- verkkotunnuksen poistaminen palvelusta
- ylläpitokäyttöliittymän käyttöoikeuksiin ja -tunnuksiin liittyvät muutokset

Hostmasterin yhteystiedot: [Yhteystiedot](#).

Lisäohjeita löytyy tämän sivun [Ohjeet](#)-kohdasta.

Varanimipalvelu ns-secondary.funet.fi

Varanimipalvelun käyttöönottamiseksi jäsenorganisaatio voi tehdä osan tarvittavista toimenpiteistä itsenäisesti ja osa vaatii yhteydenottoa Funet Hostmasteriin; yhteystiedot: [Yhteystiedot](#).

Lisäohjeita löytyy tämän sivun [Ohjeet](#)-kohdasta.

Hinnoittelu

Nimipalvelut sisältyvät Funet-maksuun.

Ohjeet

Jäsenorganisaatio voi ylläpitää itsenäisesti nimipalvelutietoja eli lisätä, muuttaa ja poistaa verkkotunnuksiinsa kuuluvia Internetissä näkyviä IP-osoitetietoja (esim. nimen www.organisaatio.fi IP-osoite). Hallinta tapahtuu [www-käyttöliittymällä](#), jossa käyttäjätunnuksella on pääsy ainoastaan käyttäjätunnuksensa liitettyjen jäsenorganisaatioiden verkkotunnusten tietoihin. Sisäänkirjautumisessa käytetään salasanaa tunnistautumiseen ja lisärajoituksena tietyllä käyttäjätunnuksella voi kirjautua palveluun ainoastaan jäsenorganisaation valitsemista verkoista.

Nimipalvelutietojen hallinnan [www-käyttöliittymän](http://www.funet.fi/dns-admin) osoite on <https://dns-admin.funet.fi/>. Palveluun pääsy on rajattu pääsilystoin vain palvelua käyttävien jäsenorganisaatioiden IP-osoitteista.

Hallintakäyttöliittymällä tehdyt muutokset tulevat näkyviin Internetin nimipalvelussa Funetin auktoritatiivisten nimipalvelinten (ns.funet.fi, ns2.funet.fi ja ns-secondary.funet.fi) kautta.

Toimenpiteet, jotka edellyttävät yhteydenpitoa Funet Hostmasteriin

Funet Hostmasterilta edellytetään toimenpiteitä varanimipalvelun käyttöönottamiseksi seuraavissa tapauksissa:

- jäsenorganisaation n.s. ylimmän tason verkkotunnuksen (esim. organisaatio.fi) liittäminen palveluun
- muualta kuin Funetilta jäsenorganisaatiolle delegoidun käänteisnimipalvelun ylimmän tason verkkotunnuksen (esim. 2.1.in-addr.arpa) liittäminen palveluun
- TSIG-avainten käyttö zone-päivitysten ja DNS NOTIFY -viestien varmentamiseksi
- jos verkkotunnuksen zone-päivitykset halutaan jakaa varanimipalveluun jostain muualta kuin verkkotunnuksen muilta nimipalvelimilta (n.s. hidden master:in käyttö)

Yhteydenotto Funet Hostmasteriin: [Yhteystiedot](#).

Varanimipalvelu päivittää verkkotunnuksen tiedot zone transfer (AXFR) -menetelmällä verkkotunnuksen muista nimipalvelimista tai erikseen määriteltäviltä hiddenen master palvelimilta. Näiltä samoilta palvelimilta varanimipalvelu hyväksyy myös DNS NOTIFY -viestit zone-päivitysten nopeuttamiseksi.

Toimenpiteet, jotka jäsenorganisaatio voi suorittaa itsenäisesti

Palvelun käyttöönotto alemman tason verkkotunnukselle: Kun varanimipalvelu on otettu käyttöön jäsenorganisaation ylimmän tason verkkotunnukselle eli zonelle (esim. organisaatio.fi tai 2.1.in-addr.arpa - sovittava Funet Hostmasterin kanssa), voi palvelu ottaa käyttöön myös alemman tason zonelle (esim. osasto.organisaatio.fi tai 3.2.1.in-addr.arpa) lisäämällä ylemmän tason zoneen delegointi-NS-tietueeksi ns-secondary.funet.fi: Kaikki varanimipalvelua käyttävät zonet käydään automaattisesti läpi noin kerran vuorokaudessa ja varanimipalvelu konfiguroituu silloin slave-nimipalvelimeksi kaikille niille zoneille, joiden delegointi-NS-tietueyhmässä on mukana ns-secondary.funet.fi. Huomaa, että nimenomaan delegoivassa ylemmän tason zonessa oleva NS-tietueyhmä ohjaa automaattista käyttöönottoa, eikä ns-secondary.funet.fi:n lisääminen zonen omaan NS-tietueyhmään siis riitä.

Esimerkki 1: ns-secondary.funet.fi-palvelun käyttö zoneille *organisaatio.fi* ja *osasto.organisaatio.fi*.

1. *organisaatio.fi*. on jäsenorganisaation päätason zone. Varanimipalvelun käyttöönotto sille on sovittu Funet Hostmasterin kanssa.
2. *osasto.organisaatio.fi*. on asiakkaan alizone. Koska sille on **parent zonessa** organisaatio.fi. lisätty delegointi-NS-tietueeksi *ns-secondary.funet.fi*, konfiguroituu varanimipalvelu automaattisesti zonen nimipalvelimeksi. Oleelliset kohdat **parent zonesta** organisaatio.fi.:

```

$ORIGIN organisaatio.fi.
@      24h      IN SOA  ns.organisaatio.fi. hostmaster.organisaatio.fi. ( ; ... tietueen loppuosa poistettu
; zonen organisaatio.fi omat NS- ja tarvittavat A/AAAA-tietueet:
@      NS       ns1
      NS       ns2
      NS       ns-secondary.funet.fi.
ns1     A        1.2.3.4
      AAAA     2001:708:abc:d::1:53
ns2     A        1.2.4.4
      AAAA     2001:708:abc:e::2:53
; alizonen osasto.organisaatio.fi delegointi-NS-tietueet:
osasto  NS       ns1
      NS       ns2
      NS       ns-secondary.funet.fi.

```

Päänimipalvelun ja palomuurin konfigurointi

Päänimipalvelimen tai mahdollisesti käytettävän erillisen n.s. hidden master -palvelimen, jolta ns-secondary.funet.fi-varanimipalvelu päivittää zone-tiedot:

1. palomuurin tulee hyväksyä **sekä TCP- että UDP-liikenne** porttiin 53 (domain) ja
2. nimipalveluohjelmiston (tms.) tulee hyväksyä zone transfer pyynnöt

kaikista ns-secondary.funet.fi-palvelun käyttämistä osoitteista, jotka on lueteltu taulukossa alla:

Palvelin	Tehtävä	IPv6-osoite	IPv4-osoite
ns-secondary.funet.fi	julkinen nimipalvelu	2001:708:10:55::53	128.214.248.132
otso.funet.fi	zone-kopiointien lähdeosoite 1. palvelimella	2001:708:10:55::53:1	128.214.248.137
karhu.funet.fi	zone-kopiointien lähdeosoite 2. palvelimella	2001:708:10:55::53:2	128.214.248.138

Pääsilystoissa voi käyttää ylläolevan taulukon yksittäisten osoitteiden sijasta turvallisesti myös osoitealueita 2001:708:10:55::/64 ja 128.214.248.128/28; niitä käyttävät on ainoastaan ns-secondary.funet.fi-varanimipalvelun järjestelmät.

DNS NOTIFY -viestit tulee lähettää aina **molemmille** palvelimille otso.funet.fi ja karhu.funet.fi.

Esimerkki 2: Linux-palvelimen pakettisuodatussäännöt

Pakettisuodatussääntöjen lukumäärän kohtuullistamiseksi hyväksytään yhteydenotot yllämainituista osoitealueista yksittäisten palvelinosoitteiden sijasta. (Huomaa, että parhaat käytännöt sääntöjen toteuttamiseksi vaihtelevat tapauskohtaisesti ja saattavat poiketa tässä esitetystä):

IPv6:

```

ip6tables -I INPUT -j ACCEPT -p tcp -s 2001:708:10:55::/64 --dport 53
ip6tables -I INPUT -j ACCEPT -p udp -s 2001:708:10:55::/64 --dport 53

```

IPv4:

```

iptables -I INPUT -j ACCEPT -p tcp -s 128.214.248.0/24 --dport 53
iptables -I INPUT -j ACCEPT -p udp -s 128.214.248.0/24 --dport 53

```

Esimerkki 3: Zone transfer -pääsilystan ja DNS NOTIFY -asetusten konfigurointi BIND-nimipalvelinohjelmiston named.conf-asetustiedostossa:

```

acl "funet-ns-secondary" {
    128.214.248.0/24;
    2001:708:10:55::/64;
};
options {
    // ... muita asetuksia...
    allow-transfer {
        // ... oma verkonvalvonta tms.
        funet-ns-secondary;
    };
    also-notify {
        2001:708:10:55::53:1; // otso.funet.fi
        128.214.248.137;      // otso.funet.fi
        2001:708:10:55::53:2; // karhu.funet.fi
        128.214.248.138;      // karhu.funet.fi
    };
    // ... muita asetuksia...
};

```

Huomaa, että jos ns-secondary.funet.fi-palvelua halutaan käyttää vain osalle zoneista ja nimenomaan halutaan estää mahdollisuuskin zonen sisällön kopiointi ns-secondary.funet.fi-palveluun, täytyy allow-transfer- ja also-notify- asetukset poistaa options-asetuslohkosta ja panna ne niiden zonejen zone-asetuslohkoihin, joita ns-secondary:n halutaan palvelevan.

Esimerkki 4: Zone transfer -pääsilystan ja DNS NOTIFY -asetusten konfigurointi NSD-nimipalvelinohjelmiston nsd.conf-asetustiedostossa, tehtävä jokaiselle zonelle erikseen:

```
zone:
  name: organisaatio.fi
  # ... muita asetuksia...
  provide-xfr: 2001:708:10:55::/64;
  provide-xfr: 128.214.248.0/24;
  notify:      2001:708:10:55::53;      # ns-secondary.funet.fi
  notify:      128.214.248.132;         # ns-secondary.funet.fi
  notify:      2001:708:10:55::53:1;    # otso.funet.fi
  notify:      128.214.248.137;         # otso.funet.fi
  notify:      2001:708:10:55::53:2;    # karhu.funet.fi
  notify:      128.214.248.138;         # karhu.funet.fi
```

Huomaa, että jos NSD:n konfiguraatiotiedostoa ylläpidetään käsityönä, kannattaa harkita `include`-toiminnon käyttöä.