laituri.local

Active Directory yleiskuvaus

18.4.2014

© Teppo Rinne

Public

<http://spad.dy.fi/>

<http://fi.linkedin.com/pub/teppo-rinne/75/508/601/>



Contents

[2. Muutoshallinta 3](#_Toc385330806)

[3. Yleistä 3](#_Toc385330807)

[4. Verkkoinfrastruktuuri 4](#_Toc385330808)

[4.1. Tietoturva verkkotasolla 4](#_Toc385330809)

[5. Active Directory 5](#_Toc385330810)

[5.1. AD DS 5](#_Toc385330811)

[5.2. Aikapalvelut 6](#_Toc385330812)

[5.3. OU-hierarkia 6](#_Toc385330813)

[5.4. Luvitusten toteutus 7](#_Toc385330814)

[5.4.1. Tiedostopalvelut 8](#_Toc385330815)

[5.5. Group Policyt 8](#_Toc385330816)

[6. Hallintamenetelmät 8](#_Toc385330817)

[6.1. Liiketoimintaprosessit 8](#_Toc385330818)

[6.2. Käyttöoikeusmuutos: Service desk -malli 9](#_Toc385330819)

[6.3. Käyttöoikeusmuutos: Itsepalvelumalli 9](#_Toc385330820)

[7. Tiedostopalvelut 9](#_Toc385330821)

[7.1. Distributed File System 10](#_Toc385330822)

[7.2. Kotihakemistojen uudelleenohjaus 10](#_Toc385330823)

[7.3. Offline Files 12](#_Toc385330824)

[7.4. Kotihakemistojen tilanrajoitus 13](#_Toc385330825)

[7.5. File screen policyt 14](#_Toc385330826)

[7.6. Shadow Copies 14](#_Toc385330827)

[7.7. Access-Denied Assistance ja Folder Owner email 15](#_Toc385330828)

[7.8. File Classification Infrastructure 16](#_Toc385330829)

[7.9. Dynamic Access Control 16](#_Toc385330830)

[8. Verkkopalvelut 16](#_Toc385330831)

[8.1. DHCP 16](#_Toc385330832)

[8.2. DNS 17](#_Toc385330833)

[8.3. WINS 17](#_Toc385330834)

[9. Etäyhteydet 17](#_Toc385330835)

[9.1. DirectAccess 18](#_Toc385330836)

[9.1.1. NLS 18](#_Toc385330837)

[9.1.1. Vianselvitys 18](#_Toc385330838)

[10. Sertifikaattipalvelut 19](#_Toc385330839)

[10.1. Certificate Authority 19](#_Toc385330840)

[10.2. Certificate Revocation List 20](#_Toc385330841)

[11. Vinkit 20](#_Toc385330842)

# Muutoshallinta

|  |  |  |
| --- | --- | --- |
| Päivä | Tekijä | Muutos |
| 3.4.2014 | Teppo Rinne | Dokumentti luotu. |
| 5.4.2014 | Teppo Rinne | Oikoluku ja Luvitusten toteutus siirretty pääotsikon Active Directory alle |
| 11.4.2014 | Teppo Rinne | Kappaleet Etäyhteydet ja Sertifikaattipalvelut luotu alustavasti. Lisätty kappaleet Shadow Copies ja Offline Files. |
| 18.4.2014 | Teppo Rinne | Kappaleet Access-Denied Assistance ja Folder Owner email lisätty |

# Yleistä

Tässä dokumentissa kuvataan erittäin pienen demoympäristön toteutusfilosofia. Samaa ideologiaa, pienillä muutoksilla, voidaan käyttää pienen yrityksen omassa palvelinympäristössä.

Ympäristöjen toteutuksissa ei ole yleensä ehdottoman oikeaa tai väärää tapaa. Hyvin toimivat menetelmät syntyvät luovalla ajattelulla mahdollisuuksista ja tukea niitä toimivaksi tiedetyillä käytännöillä. On kustannustehokkuuden kannalta tärkeää kehittää ongelmallisia prosesseja ja olla koskematta hyvin toimiviin.

Muutama keskeinen asia on huomioitava:

* Tämä dokumentti ei ota kantaa siihen, missä tapauksissa omaa palvelinkapasiteettia kannattaa hankkia, tai muutenkaan palvelun tuotantotapaan
* Kuvattu ympäristö tarjoaa alustan sen päälle rakennettaville palveluille ja liiketoimintasovelluksille. Tämän vuoksi sen jalanjälki on pyritty minimoimaan
* Kriittisiä palvelimia ei ole kahdennettu: otettava huomioon käytettävyydessä ja varmuuskopioinnin rutiineissa

Suosittelen tekemään tekniset toteutukset englanniksi, vaikka dokumentaatio ja käyttöohjeet olisivatkin yrityksen käyttökielellä. Liiketoiminta saattaa muuttua ennakoimattomasti ja osa ympäristön hallinnasta voidaan joutua antamaan esim. toisessa maassa olevalle liiketoimintayksikölle. Tällöin hyvin tehty ympäristö on ymmärrettävissä jopa ilman ohjeita.

Ympäristön dokumentointi on jaettu seuraaviin dokumentteihin.

|  |  |  |
| --- | --- | --- |
| Dokumentti | Sisältö | Linkki dokumenttiin |
| Looginen verkkokaavio | Liittymät, verkkolaitteet ja niihin kytketyt verkot | <http://spad.dy.fi/laituri/laituri.local_verkkokaavio.pptx> |
| IP-osoitelista | Laitekohtaiset IP-osoitteet aliverkoittain |  |
| AD-dokumentaatio | Peruspalveluiden toteutuksen yleinen kuvaus | <http://spad.dy.fi/laituri/laituri.local-ad-yleiskuvaus.docx> |
| Prosessikuvaukset | Tietohallintoon liittyvät prosessikuvaukset |  |
| Järjestelmäympäristön muut tekniset kuvaukset | Laajempien osakokonaisuuksien tekniset kuvaukset, mm. sovellusvirtualisointi yms. |  |
| Liiketoimintasovellusten tekniset kuvaukset |  |  |

# Verkkoinfrastruktuuri

Verkkoympäristön tärkeimpinä tavoitteina on tarjota luotettavuutta, kapasiteettia, tietoturvaa ja hallittavuutta.

Luotettavuuden kannalta kokemusperäisesti merkityksellisintä on laitevalinta, hyvä asennustapa ja oikein tehty konfigurointi. Keskimääräinen vikaantumisväli kuluttajatuotteilla on noin 5 vuotta ja yrityskäyttöön tarkoitetuilla verkkolaitteilla noin 20 vuotta. Hyvään asennustapaan kuuluu laadukkaat asennustarpeet, siistit ja verkkosegmenttien mukaan värikoodatut kaapeloinnit sekä kytkinporttien ja kaapeloinnin dokumentaatio. Jatkuvuuden turvaamiseksi tulee huolehtia myös säännöllisistä firmware-päivityksistä vähintään vuoden välein.

Tietoturva on luotettavuuden jälkeen tärkein huomioitava asia. Verkkolaitteet ovat suojattava ulkopuolisten fyysisen pääsyn estämiseksi ja suojattava vähintään yrityskohtaisella salasanalla. Verkon osuus tietoturvaan oli pitkään lähde/kohde -sääntöihin perustuvaa. Tietoturva avataan kohdassa Tietoturva verkkotasolla.

Tarvittavan kapasiteetin määrittää lähinnä muu ympäristö: palvelininfrastruktuuri ja liiketoimintasovellukset. Tällä hetkellä (2014) 1 Gb -portit riittävät PK-yrityksille erittäin hyvin. Kuormitetuimmissa linkeissä kannattaa harkita trunkkauksen (<https://en.wikipedia.org/wiki/Link_aggregation>) käyttämistä.

Keskitetty hallittavuus ei ole juurikaan merkityksellistä itse hallitussa pienympäristössä. Hallittavuus tulee merkitykselliseksi jos konfiguraatio muuttuu usein, hallittavia laitteita on useita kymmeniä tai vaatimuksena on versiohallinta ja automaattiset varmuuskopioinnit.

## Tietoturva verkkotasolla

Yleisesti käytetyt verkon toteuttamat tietoturva-asiat ovat seuraavat:

* Tilallinen palomuuri
* Verkkojen eristäminen toisistaan (802.1q)
* Pääsynhallinta (802.1x)
* Käyttäytymisen tutkiminen (esim. connection-rate filtering)
* Liikenteen sisällön tutkiminen ja esto (IPS/IDPS)

Tietoturvauhat muuttuvat jatkuvasti. 1990-luvulla virukset liikkuivat lähinnä siirtomedioilla ja sovellustiedostoissa. 2000-luvun alussa oli havaittavissa mato-tyyppiset ongelmat, kun taas kymmenisen vuotta myöhemmin merkittävintä on tiedostoihin (pdf, doc yms) sisällytetyt haittakoodit. Lisänsä tähän tuovat kohdistetut hyökkäykset.

Työskentelytavat ja tietoturvahaasteet ovat siis muuttuneet eikä yritysverkon tietoturvaa voida enää rakentaa pelkän pääsynhallinnan varaan. Jokaista työasemaa tulee pitää yhtä epäluotettavana niiden hetkellisestä verkkosijainnista riippumatta. Perinteistä lähiverkkoa voisi jopa ajatella vain yhtenä julkisena verkkona muiden rinnalla. Saastumisia ei kuitenkaan voida täydellisesti välttää, joten huomio tulee keskittää epänormaalin toiminnan havainnoimiseen.

Suositukseni on käyttää IPS-palomuuria, joiden hinnat ovat nykyisin hyvin kohtuullisia. Laitetta tärkeämpää on oikea konfigurointi: tarpeeton liikenne tulee estää ja tarpeelliseen liikenteeseen tulee kohdistaa sisällön analysointia ja protokollan sääntöjen noudattamisesta. Tunnisteisiin pohjautuva suodatus on aina myöhässä ja helposti kierrettävissä, joten oleellista on tutkia liikennekäyttäytymistä ja käytettävää protokollaa vastaan tehtäviä hyökkäyksiä.

Tässä ympäristössä ei voida käyttää IPS-palomuuria kustannuksien vuoksi.

# Active Directory

Active Directory voi koostua seuraavista rooleista:

* AD Domain Services (AD DS, Active Directoryn keskeisin palvelu)
* AD Certificate Services (AD CS)
* AD Federation Services (AD FS)
* AD Lightweight Directory Services (AD LDS)
* AD Rights Management Services (AD RMS)

AD DS käyttää Domain Controllereja (DC) kirjautumispalvelimina.

Domain on nimetty laituri.local ja netbios-nimellä LAITURI.

Huom: Hyvä tapa nimetä domain on muoto ad.yritys.fi. Perustelut tälle löytyy <http://acbrownit.wordpress.com/2013/04/15/active-directory-domain-naming-in-the-modern-age/>

TODO

## AD DS

AD DS:llä on seuraavat roolit, joista kukin voi olla vain yhdellä palvelimella kerrallaan.

* Schema master
* Domain naming master
* Primary Domain Controller emulatur (PDC)
* RID pool manager
* Infrastructure master

Roolien kohdepalvelimet voi katsoa komennolla netdom /query fsmo

TODO: AD Sitet

## Aikapalvelut

Aikapalvelut toteutetaan yleensä hyvin yksinkertaisella kaavalla:

* Yksi fyysinen DC (PDC) hakee ajan ulkoisesta NTP-lähteestä (time1.mikes.fi tai operaattorilta)
* Muut DC:t hakevat ajan tästä DC:stä automaattisesti
* Sovelluspalvelimet, työasemat ja verkkolaitteet hakevat ajan Logon-DC:ltä

Huomaa, että verkon aikaa ylläpitävän palvelimen suositellaan olevan fyysinen. Lisätietoa esimerkiksi dokumentista Timekeeping in VMware Virtual Machines (<http://www.vmware.com/files/pdf/techpaper/Timekeeping-In-VirtualMachines.pdf>)

Tässä tapauksessa ajan hakeva DC on virtuaalikone, joten aikapalveluissa voi esiintyä epäjatkuvuuksia. NTP-lähteestä ajan hakevalle palvelulle määritetään säätörajaksi +/- 12 tuntia (oletus 48 tuntia), jolloin lähdepalvelun katastrofitilanteet eivät voi heijastua omaan ympäristöön.

NTP-aikalähde määrittiin seuraavilla komennoilla:

* net stop w32time
* w32tm /config /syncfromflags:manual /manualpeerlist:"time-a.nist.gov, time-b.nist.gov, time-c.nist.gov, time-d.nist.gov"
* w32tm /config /reliable:yes
* net start w32time

Aikamuutoksen maksimirajat määritettiin rekisteriin:

* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxPosPhaseCorrection
* HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W32Time\Config\MaxNegPhaseCorrection
* Avainten DWORD-arvoksi asetetaan 43200 (Dec)

Aikasynkronoinnin toiminta tallentuu system logiin sourcella Time-Service.

## OU-hierarkia

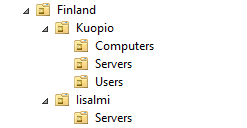
Organization Unit (OU) -hierarkia on toteutettu pääasiassa halutun hallinnan toteuttamiseksi. Näihin kuuluu Group policyjen kohdistus ja hallinnan delegointi.

OU-rakenteen yleissääntöinä ovat:

* Käyttäjät, työasemat ja palvelimet sijoitetaan eri OU:hin
* Enintään 15 tasoa syvä OU-rakenne
* Yksittäinen OU-nimi alle 64 merkkiä
* Koko OU-polku enintään 260 merkkiä

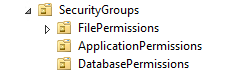
Huom: DC-palvelimia ei koskaan siirretä pois Domain Controllers –OU:sta, ei edes sen alle tehtyihin OU:hin.

Seuraava malli on todettu toimivaksi käyttäjien ja raudan hallinnoinnissa:

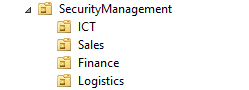


Huom: Työasemat ja käyttäjät voi olla tarpeen jakaa vielä osastokohtaisiin OU:ksi esim. GPO:n kohdistamiseksi. Toinen toimiva, joskin suorituskyvyltään huonompi tapa GPO:n kohdistukseen on käyttää objektien globaaleja ryhmiä suodatukseen.

Seuraava malli on todettu toimivaksi Domain Local -ryhmien hallintaan:



Seuraava malli on todettu toimivaksi Globaalien käyttöoikeusryhmien hallintaan:



## Luvitusten toteutus

Määritettävä: Roolien omistajat.

Microsoftin Best Practises -ohje on toteuttaa luvitukset mallilla: A – G – DL – P. (<https://en.wikipedia.org/wiki/AGDLP>)

* A tarkoittaa Accountia, eli käyttäjää tai resurssia.
* G tarkoittaa Global security group.
* DL tarkoittaa Domain Local security group.
* P tarkoittaa Permission, eli luvituksen kohteena oleva oikeus.

Tämän tarkoituksena on mm. mahdollistaa jäljitettävyys AD:n työkaluilla siihen, mihin käyttäjällä tai resurssilla on pääsy. Lisäksi ryhmät ovat valmiiksi oikein domainien liittyessä toisiinsa luottosuhteilla.

G:n ja DL:n käsite vaihtelee toteuttajien mukaan. De facto -standardiksi on kuitenkin muodostunut seuraava:

* G on käyttäjän liiketoimintaosasto tai -rooli
* DL viittaa palveluun tai palvelimeen ja siellä olevaan oikeuteen tai rooliin

Oikeusryhmät nimetään seuraavalla tavalla:

|  |  |  |
| --- | --- | --- |
| Tyyppi | Nimeämiskäytäntö | Selite |
| Liiketoimintarooli | G-Asiakaspalvelu-Kuluttajaasiakkaat | Kuluttaja-asiakaspalvelun tarvitsemat oikeudet |
| Tiedosto-oikeus | DL-DFS-Tiedostot-Kuluttajat-M | DFS-jaon ”Tiedostot” hakemiston ”Kuluttajat” muokkausoikeus. |
| Tietokantaoikeudet | DL-DB-SERVER-Instance-Permission | Tietokannan määritetyn instanssin oikeus |
| Liiketoimintasovelluksen oikeus | DL-WIKI-User | Esim. Wikipedia-alustan käyttäjä. |

### Tiedostopalvelut

Määritettävä: Datan omistajat.

Esimerkiksi:

Jaettu DFS-hakemisto [\\laituri.local\Public\Dokumentit](file:///\\laituri.local\Public\Dokumentit), jonka käyttöoikeuksia hallitaan vain ylimmällä tasolla, NTFS-oikeuksiin laitetaan ryhmät (SecurityGroups/FilePermissions/)

* DL-DFS-Dokumentit-R: oikeus Read
* DL-DFS-Dokumentit-M: oikeus Modify

Nämistä ryhmistä liitetään jäseniksi globaaleihin ryhmiin (SecurityManagement/Finance/):

* DL-DFS-Dokumentit-M 🡪 G-Talous-Reskontra
* DL-DFS-Dokumentit-R 🡪 G-Talous-Lukuoikeudet

## Group Policyt

TODO

Yleisesti ottaen Group policyiden määrä pyritään minimoimaan. Käytännössä policyt on jaettava pienempiin palasiin siten, että kukin niistä muodostaa loogisen kokonaisuuden. Policyissä vältetään security- ja wmi-filtteröintiä niiden huonon suorituskyvyn takia.

Yksittäiseen policyyn tehdään vain käyttäjä- tai koneasetuksia. Tarpeeton puoli disabloidaan koko policystä suorituskyvyn maksimoimiseksi.

Huom: Default policyjä (Default Domain Controllers ja Deafault Domain Policy) ei koskaan poisteta käytöstä. Lisäksi niihin vältetään tekemästä mitään muutoksia.

# Hallintamenetelmät

Käyttäjien hallinta vaikuttaa merkittävästi ylläpitotyön määrään. Hyvin toteutettu käyttäjien hallinta nitoutuu liiketoimintaprosesseihin huomaamattomaksi osaksi. Huonosti toteutettuna siitä voi aiheutua valtava määrä muutostikettejä, pitkä läpimenoaika oikeuksien muutoksiin ja pahimmillaan ei nähdä ilman suurta työtä, minne käyttäjällä on pääsyoikeus.

## Liiketoimintaprosessit

Käyttäjien hallinta on tärkeää nitoa osaksi yrityksen henkilöstöprosesseja. Hyvin mietityt liiketoimintaroolit voidaan tuoda valmiiksi valinnoiksi työsuhteen alkamiseen, muuttumiseen ja päättymiseen liittyviin dokumentteihin. Näin niistä saadaan tieto mahdollisimman varhaisessa vaiheessa ja vältetään tulipalokiireiden syntyminen.

Uudet käyttäjät perustetaan työsuhdetiedoilla täytetyn lomakkeen perusteella. Tässä lomakkeessa on nähtävillä kaikki liiketoimintaroolit, joista henkilön tai osaston esimies valitsee tarvittavat.

## Käyttöoikeusmuutos: Service desk -malli

Yleisin käytössä oleva käyttäjäoikeuksien hallintatapa perustuu Service desksin käyttöön ja muutospyyntöihin. Tässä mallissa:

* Käyttäjä tekee muutostiketin service deskille
* Service desk tekee tarkastuksen, voiko oikeuden myöntää
* Mahdollisesti: muutospyyntö käy hyväksynnässä sovitun prosessin mukaisesti
* Service desk tekee muutoksen, tiedottaa käyttäjää ja tallentaa hyväksynnän perusteen tiketille
* Käyttäjä saa tiketin sulkemisvahvistuksen
* Oikeudet päivittyvät käyttäjän kirjautuessa

Tässä mallissa on perustavaa laatua oleva tehokkuusongelma. Service desk ei yleensä voi tehdä itsenäisesti päätöstä käyttöoikeuksien muuttamisesta. Varsinaisen muutoksen tekemiseen menee noin 1-2 min, kun tiketin kokonaistyöaika voi olla 10-30 min.

## Käyttöoikeusmuutos: Itsepalvelumalli

Kun OU-hierarkia ja Luvitusten toteutus on tehty oikein, voidaan työkalut oikeuksien muuttamiseksi antaa suoraan oikeusmuutoksen hyväksyjälle (Sami Laiho, Techdays 2012, <https://www.youtube.com/watch?v=kuNdLJ-EDmg>). Liiketoimintayksikkö-OU:lle myönnetään sitä hallitsevalle DL-oikeusryhmälle oikeus Modify Members.

Tässä mallissa:

* Käyttäjä pyytää oikeusmuutoksen liiketoiminnasta vastaavalta
* Liiketoiminnasta vastaava hylkää tai hyväksyy muutoksen ja pystyy tekemään muutoksen välittömästi omalta koneeltaan
* Oikeudet päivittyvät käyttäjän kirjautuessa

Käyttöoikeuksien hyväksyjien työasemille asennetaan Remote Server Administration Tools (RSAT) ja luodaan linkki kustomoituun MMC-konsoliin. Tästä konsolista hyväksyjät voivat liittää ja poistaa käyttäjiä oman liiketoimintayksikkönsä rooleista.

Tässäkin toimintamallissa G – DL -oikeusmuutokset tehdään Service deskin tai oman tietohallinnon kautta.

Tämän toteutustavan toiminta on hyvä verrata mm. tietoturvapolitiikkaan ja erilaisten intressiryhmien vaatimuksiin (tilintarkastajat yms.). Etuna on, että esimiehet voivat milloin vaan tarkastaa omiin liiketoimintarooleihinsa liitetyt henkilöt. Haittapuolena on vaikea dokumentoida käyttöoikeuden muutossyy.

# Tiedostopalvelut

Tiedostopalvelut perustuvat Windows Server SMB-protokollaan. Kaikki käyttäjille tarjottavat verkkohakemistot näytetään ja käytetään DFS Namespacen kautta. Toteutuksen filosofiana on ohjata käyttäjää toimimaan valmiiksi yrityksen politiikan mukaisesti.

Toiminnan laajetessa muihin toimipisteisiin tulee harkita Branchcachea tai tiedostopalveluiden DFS-replikoimista tarpeen mukaan.

Offline Files -toiminto on erinomainen silloin, kun sitä käytetään vain käyttäjän omiin tiedostoihin tai tiedostoihin ei ole käyttäjillä kirjoitusoikeuksia. Yhteiset tiedostoihin sitä ei kannata synkronointikonfliktien takia käyttää.

Windows Server käyttää kaksi- tai kolmitasoista käyttöoikeushallintaa tiedostopalveluissa. Käyttäjä tai laite pääsee käsiksi kohteeseen vain, jos kaikki näistä portaista sallivat pääsyn.

**Share**

**NTFS**

**DAC**

\\srv\fol\file.txt

Verkkojakoihin ja NTFS-tiedostojärjestelmään perustuva käyttöoikeushallinta on ollut käytössä suunnilleen samanlaisena NT-käyttöjärjestelmästä saakka (vuodesta 1995, ACL). Tässä mallissa on kaksi vakavaa ongelmaa:

* Käyttöoikeushallinta vaikuttaa vain, kun data on sijoitettuna palvelimen ”levypinnalle”
* Käyttöoikeudet eivät liity mitenkään siihen, mitä tiedosto sisältää

Näiden ongelmien ratkaisemiseksi Microsoft julkaisi Dynamic Access Control -toiminnon. Tässä ideologiassa tiedoston piirteet tallennetaan tiedoston luokitteluksi (File Classfication), jonka perusteella pääsy hallitaan. Tiedoston sijainnilla ei tällöin ole mitään merkitystä. Nämä määrittelyt koskevat kuitenkin vain domainiin liitettyjä koneita ja käyttäjiä. Tiedostojen salaus on tarpeen, jotta menetelmä on tietoturvallinen.

Tiedostopalveluiden suunnittelussa ja toteutuksessa oleellista on miettiä, mitkä toiminnat ovat tarpeen ja kustannustehokkaita yrityksen toiminnan kannalta. Suunnittelu on tasapainottelua tietoturvan, käytettävyyden ja kustannusten välillä.

## Distributed File System

Distributed File System muodostuu kahdesta osasta: Namespace ja Replication.

DFS Namespacea voisi kuvata kokoelmaksi linkkejä, jotka osoittavat automaattisesti lähimpään palvelimeen käyttäjän sijainnin mukaan. Käyttäjälle kaikki toimii kuitenkin näkymättömästi. DFS Namespace mahdollistaa tiedostojen vapaan sijoituspaikan rikkomatta käyttäjien tekemiä tai dokumenteissa olleita linkkejä.

DFS Replication toteuttaa usean tiedostosijainnin sisällön synkronoimisesta keskenään. Replikointi käyttää siirrossa pakkausalgoritmiä ja pystyy replikoimaan muutoksia blokkitasolla. AD DS Sysvol-kansio replikoituu automaattisesti DC-palvelimien välillä DFS Replikoinnin avulla.

Käytössä on Domain-based DFS Namespace. Jokainen DC toimii DFS namespace-palveluna. Replikointi ei ole käytössä, koska AD saitteja on vain yksi.

Esimerkki ilman DFS Namespacea: Wordiin tehty linkki J:\ICT\tiedosto.txt osoittaa oikeasti \\file1.laituri.local\Documents\ICT\tiedosto.txt. Jos Documents tarvitsee koskaan siirtää toiselle palvelimelle, nämä linkit osoittavat väärään paikkaan.

Esimerkki DFS namespacella: Wordiin tehty linkki J:\ICT\tiedosto.txt osoittaa oikeasti \\laituri.local\Public\Documents\ICT\tiedosto.txt. Tätä tiedostoa pyydettäessä DFS uudelleenohjaa pyynnön kohteeseen \\file1.laituri.local\Documents\ICT\tiedosto.txt. Jos Documents-hakemisto siirretään palvelimelle \\file2.laituri.local, DFS huolehtii uudelleenohjauksesta ja tiedostojen linkit säilyvät toimivina.

On tietysti mahdollista pakottaa linkit osoittamaan mapattuun verkkolevyyn, mutta esim. Office-tuotteet muuttavat linkin automaattisesti UNC-poluksi.

Namespacet on luotu seuraavilla asetuksilla:

* Namespace name: \\laituri.local\Private
* Namespace type: Domain (Windows Server 2008 mode)
* Namespace server: DC1.laituri.local
* Root shared folder: A shared folder will be created if one does not exist.
* Local path of namespace shared folder: C:\DFSRoots\Private
* Permissions for namespace shared folder: Everyone read only

## Kotihakemistojen uudelleenohjaus

Käyttäjän kotihakemistot uudelleenohjataan DFS-jakoon [\\laituri.local\Private\UserHome](file:///\\laituri.local\Private\UserHome).

Folder Redirection Documents-hakemistolle tarjoaa seuraavat edut:

* Käyttäjien data on tarjolla niin työasemilla kuin kannettavilla, paikallisesti ja ilman verkkoyhteyttä
* Data siirtyy näkymättömästi konetta vaihdettaessa
* Data voidaan varmuuskopioida (yhdestä) paikasta

Seuraavat haittapuolet kannattaa huomioida:

* Käyttäjän tiedostojen käyttö saattaa hidastua hitaiden verkkoyhteyksien päässä merkittävästi. Tätä voi parantaa parametroimalla GPO Group policy Offline Files Slow-Link Threshold tiukaksi.

Uudelleenohjauksen määrittely on ohjeessa [http://blogs.technet.com/b/askds/archive/...](http://blogs.technet.com/b/askds/archive/2008/06/30/automatic-creation-of-user-folders-for-home-roaming-profile-and-redirected-folders.aspx). Roaming Profiles ei tule käyttöön: en suosittele sen käyttöä suorituskykyongelmien takia.

Hyvä ohje konfigurointiin on myös <http://technet.microsoft.com/en-us/library/ff633429(v=ws.10).aspx>.

Kohdehakemiston NTFS-oikeudet tulee näyttää seuraavalta:



Kohdehakemiston jaon Caching-optioksi tulee valita ”Only the files and programs that users specify will be available offline”, jotta tiedostot ovat automaattisesti käytettävissä ilman verkkoyhteyksiä.

Folder Redirection -policyn asetukset User configuration/Policies/Windows settings/Folder Redirection on asetettu seuraavasti:

Huom: NTFS-käyttöoikeudet tulee testata huolellisesti, jotta käyttäjien yksityisyyden suoja toteutuu.

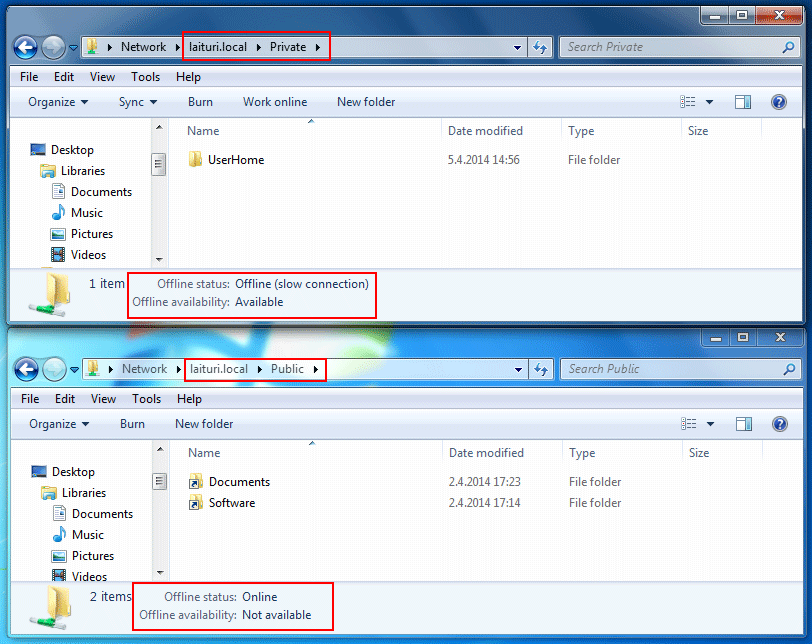
## Offline Files

Offline Files slow-link threshold määritetään Computer Configuration/Policies/Administrative Templates/Network/Offline Files: Configure slow-link mode. Slow-link moden aikana kohteen tiedostoja käytetään paikalliselta levyltä. Background Sync huolehtii säännöllisesti muuttuneiden tiedostojen kopioinnista verkkoon.



Tunnistuksessa kannattaa aluksi käyttää verkon latenssia. 10-20 ms on hyvä alkuarvo. Jos GPO-määrittelyä ei tehdä, oletus Windows 7:ssä on 80 ms ja Windows 8:ssa 35 ms.

Työaseman tilan näkee menemällä UNC-verkkopolkuun. Tätä ei tietääkseni näe millään komentoriviltä.



Huom: Tässä määrittelyssä on bugi joka on kerrottu artikkelissa <http://support.microsoft.com/kb/2801075>. Tämä vaikeuttaa konfigurointia, jos yhteiset ja yksityiset verkkohakemistot ovat saman DFS Namespacen alla.

## Kotihakemistojen tilanrajoitus

Käyttäjien kotihakemiston koko halutaan rajata. Raja määritetään tiedostopalvelimella File Server Resource Managerilla luomalla seuraavan kaltainen Quota. Muokkaa ensin templatesta yrityksen käyttöön sopiva. 5 GB on hyvä lähtökohta.



Huom: Huomaa valita “Auto apply template and create quotas on existing and new subfolders”, jotta quota vaikuttaa vain alihakemistoihin. Create quota on path aiheuttaa rajan olevan kaikille kotihakemistoille yhteensä.

## File screen policyt

Käyttäjien kotihakemistoon halutaan estää audio- ja videotiedostojen tallennus.

Sääntö määritetään tiedostopalvelimella File Server Resource Managerilla luomalla File Screen -sääntö.



Huom: Sääntö estää vain uusien tiedostojen tallennuksen, se ei koske jo hakemistossa olevia tiedostoja. Säännön voi myös kiertää helposti muuttamalla tiedostopäätettä ennen siirtoa. Tällä kuitenkin vain ohjataan käyttäjää tallentamaan isot tiedostot paikallisesti työasemalle.

## Shadow Copies

Shadow Copies on toiminnallisuus, joka mahdollistaa käyttäjille tiedostojen vanhojen versioiden ja palauttamisen ilman ylläpitäjien tukea. Palautus tai vanhojen versioiden katsominen tapahtuu tiedoston tai kansion Properties-ikkunan Previous Versions -välilehdeltä. Toiminnallisuudelle varataan määritetty tilavaraus, joka määrää taaksepäin säilytettävän datan määrän. Maksimiraja on kuitenkin 64 kopiota taaksepäin.

Toiminta kannattaa suunnitella tiedostojakojen ja DFS:n kanssa yhtä aikaa. Konfiguraatio tehdään levykohtaisesti.



Suosituksena on sijoittaa Shadow Copyt eri levylle kuin lähdelevy. Lähdelevyllä tulisi lisäksi olla vähintään 16 kB varausyksikkökoko. Shadow copy ei myöskään koskaan korvaa varmuuskopiointia.

Tärkeintä toiminnossa on kouluttaa ja sisällyttää tiedostojen palautus käyttöohjeisiin.

## Access-Denied Assistance ja Folder Owner email

Folder Owner Email on Windows 8 –työaseman vaativa ominaisuus, joka mahdollistaa käyttäjälle pääsyn estyessä tiedostoon/hakemistoon pyynnön jättämisestä pääsyn saamiseksi. Pyyntö lähetetään käyttäjän kertoman syyn kanssa tiedoston/hakemiston omistajalle tai määritettyyn sähköpostiosoitteeseen. Ominaisuus mahdollistaa automaattisen dokumentaation pyynnöistä ja pääsyn luvituksista.

Hakemistojen omistajien sähköpostiosoitteet määritetään FSRM:n Classification Management/Classification Properties/Set Folder Management Properties. Property Folder Owner Email listaa kaikki omistajat. Microsoft suosittelee käyttämään jakelulistoja, joten hakemisto kannattaa kytkeä aina sen oikeudet määrittämään Security Grouppiin.



HUOM: Missä määritetään yksiselitteisesti hakemiston/datan omistaja?

Pitäisikö olla ryhmä DL-DFS-Documents-ICT-Owner, jota käytettäisiin distribution listana? Pitäisikö jakelulistan osoite nimetä [dfs.ict@laituri.local](mailto:dfs.ict@laituri.local)?

Access-Denied Assistance määritetään käyttöön FRSM:n palvelimen päällä hiiren oikean napin valikosta Configure Options ja välilehti Access-Denied Assistance.



Posti halutaan lähettää Folder Ownerille ja luoda siitä Event log entry auditoinnin mahdollistamiseksi. Lisäksi postin saajalle annetaan suora linkki käyttäjien liiketoimintaroolien hallintaan.

## File Classification Infrastructure

File Classification Infrastructure (FCI) toteuttaa tiedostojen luokittelun haluttujen kriteerien mukaisesti. Luokittelua voidaan käyttää myöhemmin esim. DAC:n toteuttamiseksi.

Yleisesti käytössä olevia luokittelukriteereitä ovat:

* Julkisuus

## Dynamic Access Control

Dynamic Access Control (DAC)mahdollistaa pääsynhallinnan yksittäisiin tiedostoihin asti tiedoston FCI:llä määriteltyjen ominaisuuksien perusteella.

DAC:n keskeiset osat ovat:

* Datan luokittelu (Classify)
* Pääsyn kontrollointi (Access control)
* Auditointi (Audit)
* Suojaaminen (Encrypt)

Ensimmäisenä käyttöönotossa on tunnistettava olemassa oleva data ja suunniteltava tuleva luokittelu.

TODO

# Verkkopalvelut

## DHCP

DHCP tarjoaa halutuille verkkoille automaattisen IP-osoitteiden ja verkon asetusten (Reitittimet, DNS-palvelimet yms) määrittämisen.

DHCP-palvelu tarjotaan palvelimelta, joka ei sijaitse samassa aliverkossa asiakkaiden kanssa. DHCP-kyselyt eivät oletuksena poistu omasta aliverkostaan. Asiakas-aliverkon reitittimeen on määritetty IP relay (IP helper), jolle on määritetty DHCP-palvelun oikea IP. Reititin ottaa tällöin vastaan asiakaslaitteen lähettämät pyynnöt, välittää ne DHCP-palvelimelle ja palauttaa vastaukset.

TODO: Windows server 2012 failover cluster

TODO: IPv6

Verkkoihin tehtävät muutokset pitää suunnitella huolella. Verkko-osoitteet, reitittimet, DHCP, DNS, AD-sitet ja DFS ovat yhdessä toimiva kokonaisuus.

## DNS

DNS tarjoaa nimenselvityspalvelut verkon laitteille. Käytössä on Active Directory integrated zonet.

DNS-palveluun on luotu Reverse lookup zonet jokaiselle aliverkolle. Reverse lookup mahdollistaa DNS-nimen haun IP-osoitteen perusteella (esim. nslookup 172.20.1.38)



DNS Scavenging huolehtii käytöstä poistuneiden DNS-tietueiden automaattisesta poistosta. Palvelu tulee olla päällä vain yhdellä DNS-palvelimella kerrallaan. Toiminta on kuvattu hyvin Technetin blogissa [http://blogs.technet.com/b/networking/archive/...](http://blogs.technet.com/b/networking/archive/2008/03/19/don-t-be-afraid-of-dns-scavenging-just-be-patient.aspx).

DNS-tietueet poistavalla palvelimella valitaan DNS-palvelun Properties /Advanced/Enable automatic scavenging of stale records. Scavenging perioid 7 days on hyvä lähtökohta.

DNS-palvelulle valitaan Set Aging/Scavenging for All Zones… ja aktivoidaan Scavenge stale resource records. No-refresh ja Refresh intevallit pidetään 7 päivässä. Asetukset hyväksyvässä vahvistusikkunassa valitaan vielä Apply these settings to the existing Active Directory –integrated zones.

## WINS

TODO

# Etäyhteydet

Ympäristössä käytetään vain Directaccess (DA) -etäyhteyksiä. DA on automaattisesti yhdistyvä tunneli, joka käyttää IPHTTPS-protokollaa.

DA aiheuttaa seuraavia vaatimuksia:

* Vain IPv6- tai Fully Qualified Domain Name (FQDN) -liikenne ohjautuu DA-tunneliin
* IPv4-osoitteiden käyttö osoitteena ei ole tuettu tunnelin läpi
* Windows 7 -koneilla tulee olla konesertifikaatti PKI:stä
* Sovellusjakelu ja muu paljon liikennettä aiheuttava hallinta kannattaa estää työaseman ollessa ulkomaan matkapuhelinverkoissa.

DA tuo seuraavat edut:

* Yhteys yritysverkkoon ilman käyttäjän toimia (yhdistyy alle 10 sekunnissa)
* Aito käyttäjän kirjautuminen domainiin
* Työasemien hallinta on varmempaa
* Työasemien luotettava varmuuskopiointi mahdollista ilman julkisia palveluita

## DirectAccess

DirectAccess (DA) on asennettu DMZ:lla sijaitsevalle palvelimelle End-to-Edge -tyyppisesti.

Suositukseni on käyttää yhden verkkokortin konfiguraatiota siten, että tunnelin salaus puretaan DA-palvelimella. Tämä mahdollistaa verkkojen välissä olevalla palomuurilla IPS-suodatuksen. DMZ:n osoiteavaruus voi olla julkinen tai sisäinen, molemmat toimivat. Kahden verkkokortin konfiguraatiolla, jossa toinen liitäntä on julkisessa ja toinen työasema- tai palvelinverkossa, liikenteen suodatuksen toteutus on vaikeampaa.

Huom: DA-palvelu toimii nykyisin dynaamisen IP:n takana. En kuitenkaan suosittele tätä kuin demoympäristöihin.

Windows 7 -laitteet vaativat muutaman ylimääräisen vaiheen:

* Valitse wizardin Step 2:ssa ”Enable Windows 7 client computers to connect…”
* Valitse Root- tai Intermediate certificate, jolla koneiden sertifikaatit on luotu
* Enrollaa CA:sta DA-palvelimelle computer certificate

### NLS

Network Location Server (NLS) on DirectAccesiin oleellisesti liittyvä HTTPS-palvelu, jolla koneet tunnistavat sijainnikseen lähi- tai julkisen verkon. Palvelu on erittäin tärkeä. NLS asennetaan oletuksena DA-palvelimen IIS-palveluun. NLS voi kuitenkin sijaita millä tahansa korkean käytettävyyden HTTPS-palvelimella, eikä sen toimintaan vaikuta palvelimen index-sivu. Suosittelen käyttämään NLS-palvelimena esimerkiksi palomuurin hallintasivustoa. Palomuuri on yleensä joko kahdennettu tai sen käyttökatkossa liikenne ei muutenkaan toimisi.

Ole varovainen tehdessäsi muutoksia NLS-palvelun sijaintiin. Virheellinen NLS-nimi estää asiakaskoneen toiminnan lähiverkossa kunnes se saa korjaavnt Group policyt domainista DA-yhteyden kautta.

NLS-palvelun sertifikaatin luontiin palomuurille on ohje <http://spad.dy.fi/laituri/m0n0wall-cert-req.php>

Huom: Vaikuttaisi sille, että NLS HTTPS-palvelimen on vastattava HTTP ”200 OK” jotta client hyväksyy sen. Toteutustapa on käytännössä toimivaksi todettu, mutta m0n0wall ei tunnu toimivan samalla tavalla.

### Vianselvitys

DirectAccess-vianselvitys on kuvattu Microsoftin dokumentissa <http://technet.microsoft.com/en-us/library/ee844114(v=WS.10).aspx>.

DA:n toimiminen vaatii seuraavat asiat:

* Asiakaskoneen tulee olla käsitellut “DirectAccess Client Settings” –policy
* Asiakaskoneella tulee olla verkkoyhteys, josta se ei löydä NLS-palvelinta
* Verkkoyhteys DA-palvelimen porttiin 443 syntyy
* Infrastruktuuri- ja Intranet-tunnelit syntyvät
* Optio: NAP ja SmartCard menevät läpi

# Sertifikaattipalvelut

Sertifikaattipalvelut, eli PKI, on rakennettu Active Directory Certificate Services (AD CS) -roolilla ja yhdellä Enterprise Certificate Authority (CA) -palvelimella.

Public Key Infrastructure (PKI) on käsite, joka sisältää sertifikaattien hallintaan käytetyt palvelut ja politiikat. AD CS on rooli Windows Server -tuotteessa, joka myöntää ja hallinnoi julkisen avaimen salausjärjestelmään perustuvia sertifikaatteja. Palvelu mahdollistaa palveluiden, laitteiden ja käyttäjien luotettavan tunnistamisen käyttäen apuna molempien osapuolten yhteisesti hyväksymää tahoa (CA).

Sertifikaattipalveluita tarvitaan esimerkiksi seuraavissa palveluissa:

* Directaccess Windows 7-koneilla
* Langattoman tai kaapeliverkon 802.1x autentikointi
* Käyttäjän autentikointi esim. IIS-palvelimelle

Sertifikaatteja voi ostaa myös julkisesti luotetuilta yrityksiltä (Thawte, VeriSign, Entrust yms). Sisäinen sertifikaattipalvelu tulee kannattavaksi, kun sertifikaattien määrä ylittää noin 10 tai sertifikaattien myöntäminen pitää automatisoida. Yleensä käytössä on molempia, julkisia ja sisäisiä sertifikaatteja.

Huom: Julkisesti luotetut yritykset eivät enää suostu myöntämään samaan sertifikaattiin lisänimeä (Subject Alternative Name, SAN) .local-päätteellä.

CA-tyyppejä on valittavana kaksi: Enterprise CA ja Stand-alone CA. Enterprise mahdollistaa sertifikaattien automaattisen myöntämisprosessin domainin koneille ja käyttäjille. Stand-alone vaatii käsityötä sertifikaattipyyntöjen hyväksyntään ja jakeluun, mutta se on hyvä valinta esimerkiksi sertifikaattien myöntämiseen yrityksen yhteistyökumppaneille.

Sertifikaattipalvelu kannattaa tuotantoympäristössä ehdottomasti asentaa (vähintään) 2-tasoisena. Root CA:lla luodaan sertifikaatti Intermediate CA:lle, jonka jälkeen Root CA sammutetaan. Intermediate CA tekee tällöin kaikki käytännön työt. Jos Intermediate CA -palvelin haavoittuu ja kaikki sen myöntämät sertifikaatit tulee perua, tämä voidaan tehdä root CA:n avulla.

Huom: AD CS -roolin asennuksen jälkeen palvelimen domainia ei voi vaihtaa eikä DC-roolia voi lisätä tai poistaa ennen AD CS -roolin poistamista. Myöskään sertifikaattipalvelun nimeä ei voi vaihtaa asennuksen jälkeen.

## Certificate Authority

CA:n Authority Information Access (AIA) julkaisee Root CA:n itse allekirjoittaman sertifikaatin AD:hen, josta se levittyy palvelimien ja työasemien sertifikaattien Trusted Root Certificates -haaraan. Kaikki domainin koneet luottavat näin automaattisesti PKI:n sertifikaatteihin.

CA julkaisee myös listan Certificate Revocation List Distribution Point (CDP) -sijainnissa, joka sisältää tiedot sertifikaattipalvelun perumista varmenteista. Oletuksena tämäkin tallennetaan AD:hen.

AIA ja CDP ovat hallittavissa CA-palvelimen Extensions-välilehdellä. AD:hen tallennetut objektit voi katsoa esim. ADSI edit -ohjelmalla.

## Certificate Revocation List

Otetaan esimerkki: Meillä on työasema julkisessa verkossa, joka ottaa yhteyttä yrityksen julkiseen DirectAccess- tai RemoteApp -palvelimeen. Palvelin tunnistautuu sertifikaatilla, jonka on myöntänyt yrityksen CA. Mistä työasema voi tietää, onko palvelin oikeasti se miksi itseään väittää? Työasemalla ei ole tässä vaiheessa pääsyä kysyä AD:sta LDAP:lla CRL-listaa. Ratkaisu tähän on julkaista CRL julkiseen verkkoon web-palvelimella, jolloin työasema voi varmistaa palvelimen sertifikaatin kelpoisuuden ”3. osapuolelta”.

TODO

# Vinkit

nltest /sc\_query:laituri.local näyttää mihin secure channell on syntynyt (lue: logon server. Ympäristömuuttuja LOGONSERVER=… ei tätä oikeasti kerro)

dfsutil /pktinfo näyttää, miltä DC:ltä SYSVOL haetaan ja miltä koneelta DFS-jako tulee.

<https://www.youtube.com/watch?v=amLLhAXmSaY> GPO Best Practices and Slow Logon issues, Techdays Finland 2012, Joonas Karjalainen

<https://www.youtube.com/watch?v=kuNdLJ-EDmg> PK-yritysten hallinta ilmaiseksi, Techdays Finland 2012, Sami Laiho

Xperf-työkalu Widowsin käynnistysprosessin tutkimiseen.