Timo Luukkonen

Verkkolevyn ja sen käyttöoikeuksien toteuttaminen uudelleen

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikka

Insinöörityö

10.11.2014

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Timo Luukkonen Verkkolevyn ja sen käyttöoikeuksien toteuttaminen uudelleen 27 sivua + 1 liitettä 10.11.2014
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikka
Suuntautumisvaihtoehto	Tietoverkot
Ohjaaja(t)	Yliopettaja Janne Salonen Projektipäällikkö Lauri Mäkinen

Insinöörityössä kehitettiin uusi verkkolevyjärjestelmä Lemminkäinen Oyj:n talonrakennustoimialalle. Uusi verkkolevyjärjestelmä kehitettiin korvaamaan vanha, monilta osin rappeutunut vastaavanlainen järjestelmä.

Käyttäjinä verkkolevyllä on tuhansia rakennushankkeissa työskenteleviä Lemminkäisen työntekijöitä, joilla on tarve luoda, jakaa ja muokata rakennusprojekteihin liittyviä dokumentteja.

Suunniteltaessa uutta järjestelmää pyrittiin ottamaan huomioon aikaisemmin käytössä olleen, periaatteessa vastaavanlaisen, rakenteen ongelmat ja luomaan uusi rakenne, jonka avulla näiltä ongelmilta voitaisiin tulevaisuudessa välttyä.

Lopulta päädyttiin luomaan rakenne, jossa oikeuksia verkkolevyllä käytettäviin kansioihin hallinnoidaan Microsoftin Active Directory -järjestelmällä, työnkuviin perustuvilla käyttöoikeusryhmillä. Ryhmien kansiokohtaiset oikeusmäärittelyt suoritetaan NTFS-tiedostojärjestelmän sisäänrakennettuja käyttöoikeusasetuksia muokkaamalla.

Uusi järjestelmä saatiin toteutettua ja siirrettyä tuotantoon aikataulun mukaisesti. Käyttäjille luotiin ohjeistus, joka myös pyrkii vähentämään ongelmia, joita esiintyi vanhan verkkolevyn kanssa (mm. liian pitkät tiedostopolut). Palaute uudesta järjestelmästä oli positiivista niin käyttäjien kuin ylläpidonkin taholta.

Avainsanat	verkkolevy, active directory, NTFS

Author(s) Title Number of Pages Date	Timo Luukkonen Redesigning of a network drive and it's user credentials 27 pages + 1 appendices 10 November 2014
Degree	Bachelor of Engineering
Degree Programme	Information technology
Specialisation option	Data networks
Instructor(s)	Principal Lecturer: Janne Salonen Project Manager: Lauri Mäkinen

The goal of the project documented in this thesis was to design and produce a new network drive for Lemminkäinen Plc's house building branch. The new system was developed to replace the old decadent network drive structure.

The users for this system are the thousands of Lemminkäinen Plc's employees working in the building industry. They have a constant need for creating, sharing and modifying the files associated with the construction projects.

The starting point for designing this new system was to identify the biggest flaws of the old system and create a system that would actively prevent these old problems from being repeated in the future.

We ended up creating a structure where the credentials to the network drives folders were administered using Microsoft's Active Directory system. We created credential groups based on people's job descriptions, the credentials for different folders in the network drive for these groups were assigned using the NTFS file system's built-in credential manager.

The new system was produced and launched to production as scheduled. The users were provided with the instructions that aim to reduce the problems encountered with the old system. The feedback regarding the new system was positive from both the user and from administration side.

Keywords	network drive, active directory, NTFS

Sisällys

Lyhenteet

NTFS	New Technology File System, Microsoftin järjestelmissä käytettävä tiedostojärjestelmä.
AD	Active Directory, toimialueen resurssien hallintaan käytettävä järjestelmä.
OU	Organization Unit, AD:n hierarkkisista osioista käytetty nimitys.
MMC	Microsoft Management Console, Microsoftin palvelinympäristöön suunniteltu hallintapaneeli.
DC	Domain Controller, verkon toimialueen käyttöoikeuksista vastaava palvelin.
LDAP	Lightweight Directory Access Protocol, hakemistopalvelujen käyttöön tarkoitettu verkkoprotokolla.
DNS	Domain Name System, nimipalvelujärjestelmä, joka muuntaa verkkotunnuksia IP-osoitteiksi.

1 Johdanto

Lemminkäisen talonrakennustoimialan, eli Lemminkäinen Talo Oy:n, työntekijöiden käyttämät verkkolevyt olivat päätyneet vuosien mittaan rakenteeltaan vaikeaselkoiseen ja osin jopa korruptoituneeseen tilaan. Tähän oli johtanut useat fuusiot, toimialan uudelleenjärjestelyt ynnä muut liiketoiminnalliset muutokset. Kansioilla ja tiedostoilla ei ollut yhtenevää loogista mallia tai nimeämiskäytäntöjä vaan niitä oli luotu aina tarpeen mukaan useilla toisistaan poikkeavilla käytännöillä.

Tätäkin suuremmaksi ongelmaksi oli muodostunut eri kansioihin ja tiedostoihin liittyvät käyttöoikeudet, jotka olivat myös syntyneet ajan myötä, ilman erityistä suunnittelua ja logiikkaa. Useisiin kansioihin oli määritelty oikeuksia suoraan yksittäisille henkilöille. Kansioiden oikeuksia määritteleville Active Directory -ryhmien nimeämisessä ei ollut yhtenevää käytäntöä ja ryhmien jäsenyyksissä ei ollut selkeää linjausta siitä, kellä käyttäjillä olisi oikeus kuulua mihinkin ryhmään.

Projektin päätavoitteena oli helpottaa niin toimialan kuin tukitoimintojen, eli tässä tapauksessa tietohallinnon työskentelyä verkkolevyn kanssa. Toimialalla kärsittiin mm. verkkolevyn epäjärjestelmällisyydestä, liian pitkistä tiedostopoluista, niistä aiheutuvista tietueiden korruptoitumisista ja muista toimintaongelmista. Myös käyttöoikeuksiin liittyvät ongelmat olivat arkipäiväisiä.

Lemminkäisen tietohallinnossa, jolla on ylläpitovastuu kyseisestä järjestelmästä ja sen oikeuksista, kärsittiin myös samoista ongelmista. Etenkin verkkolevyyn liittyvät käyttöoikeudet olivat päätyneet tilaan, jossa kukaan ei tiennyt tarkalleen, mitkä oikeusryhmät liittyivät mihinkin kansioon, ja kenelle niitä pitäisi myöntää. Dokumentaatiota kyseisen verkkolevyn rakenteesta ja oikeuksista ei ollut.

Lemminkäinen Oyj on Suomessa ja kansainvälisillä markkinoilla toimiva rakennuskonserni, joka toimii infra- ja talonrakentamisessa. Lemminkäinen-konsernin liikevaihto vuonna 2013 oli noin 2,0 miljardia euroa. Konsernin palveluksessa työskentelee noin 6 000 henkilöä. Konsernin pääkonttori sijaitsee Helsingissä.

Toimiala, jonka toimeksiannosta tämä kyseinen projekti tehtiin, on Suomen talonrakentaminen eli Lemminkäinen Talo Oy. Suomen talonrakentaminen on jaettu

kolmeen maantieteelliseen toimialueeseen; Pääkaupunkiseutuun (PKS), Länsi-Suomeen (LS) ja Itä-Suomeen (IS).

Kansio- ja käyttöoikeusrakenteen suunnittelu päätettiin toteuttaa käytännön syistä pääkaupunkiseudun toimialan kanssa. Näin vältyttiin suunnitteluryhmän paisumiselta ja helpotettiin päätöksentekoa.

2 Suunnittelu

Alkuselvityksen varhaisessa vaiheessa kävi ilmi, että vanhan tiedosto- ja oikeusjärjestelmän korjaaminen standardien mukaiseksi ei olisi käytännössä kustannustehokas vaihtoehto. Työ pitäisi aloittaa puhtaalta pöydältä vanhan järjestelmän jäädessä eräänlaiseksi jäädytetyksi arkistoksi.

Uuden kansiorakenteen ja oikeuskäytäntöjen hahmottelu aloitettiin heti alkuun tiiviissä yhteistyössä varsinaisen käyttäjäryhmän kanssa, jotta vältyttäisiin tilanteelta, jossa tietohallinto toimittaisi varsinaisille käyttäjille palvelun, joka ei vastaa käyttötarkoitusta.

Alun perin tämän projektin vastuualueeksi oli tarkoitus jäädä vain varsinaisen käytännön työn toteuttaminen, testaus ja sen jälkeiset korjaukset ja muutostyöt sekä järjestelmän tekninen dokumentaatio. Pian huomattiin kuitenkin, että alkuperäisessä käyttöoikeuksia koskevissa suunnitelmissa ei ollut otettu huomioon kaikkia toimialan vaatimuksia ja oli vaarana, että kyseisillä oikeusmääritteillä vanhaa verkkolevyä vaivanneet ongelmat saattaisivat uusiutua ajan myötä, jos alkuperäistä suunnitelmaa seurattaisiin kokonaisuudessaan.

Lopulta päädyttiin suunnittelemaan mm. käyttäjäryhmien oikeusmäärittelyt kokonaan uudelleen. Kyseisten oikeuksien suunnittelu tapahtui käytännössä varsinaisen tekemisen ohella, joten suunnitteluvaiheesta ei ole tarjolla kovinkaan kattavaa dokumentointia.

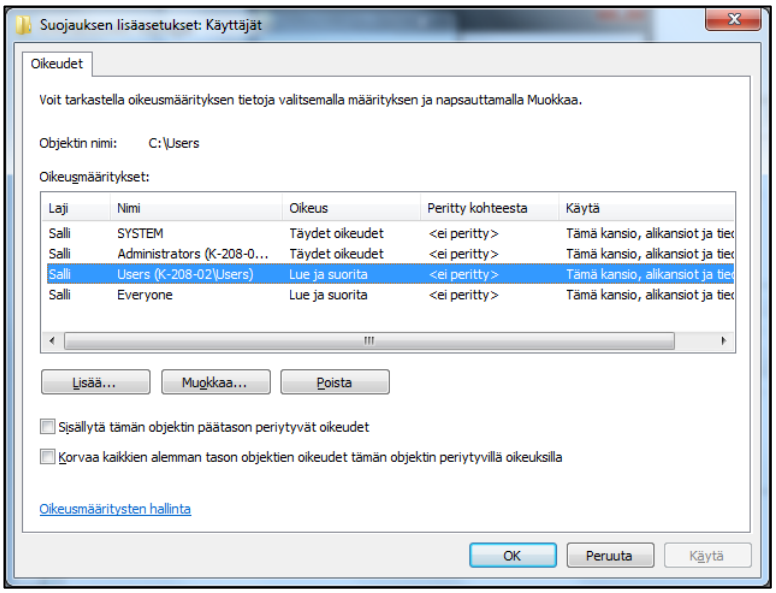
3 Työkalut

Projektissa pääasiallisina työkaluina toimivat Microsoftin Active Directory -käyttäjätietokanta- ja hakemistopalvelu sekä NTFS-tiedostojärjestelmään sisäänrakennettu käyttöoikeuksien hallinta. Seuraavissa osioissa on tarkoitus esitellä lyhyesti kyseisiä työkaluja lyhyesti niiltä osin, jotka olivat olennaisia tämän projektin kannalta.

3.1 NTFS

NTFS (New Technology File System) on Microsoftin kehittämä tiedostojärjestelmä, joka on ollut käytössä kaikissa NT-pohjaisissa käyttöjärjestelmissä vuodesta 1993. Tämän projektin kannalta tärkein NTFS-tiedostojärjestelmän ominaisuus on sen sisäänrakennetut monipuoliset kansioiden ja tiedostojen käyttöoikeudet.

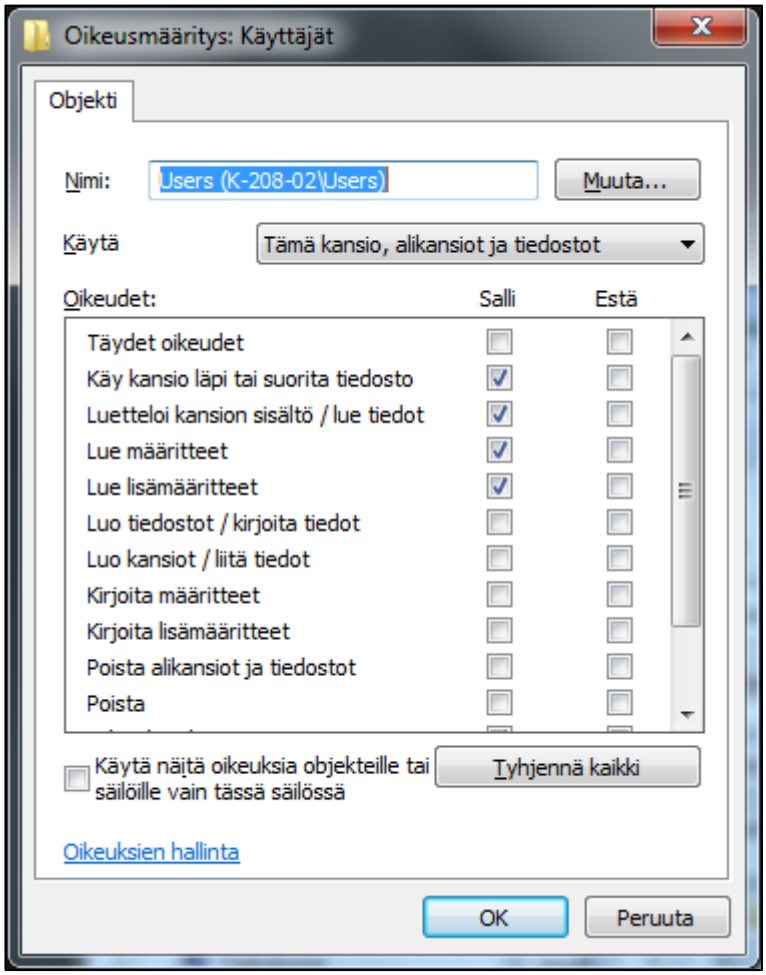
NTFS-tiedostojärjestelmässä jokaiselle tiedostolle tai kansiolle voidaan määritellä yksityiskohtaiset käyttöoikeudet jokaiselle toimialueen käyttäjälle tai ryhmälle. Nämä oikeudet voidaan asettaa kunkin käyttäjän tai ryhmän osalta joko ”Salli”- tai ”Estä”-tilaan, jolla määritellään ko. objekteille näiden oikeus suorittaa kyseistä toimintoa.



Kuva 1. Esimerkkikuva kansion käyttäjien/käyttäjäryhmien hallintatyökalusta.

Kun käyttäjien ja ryhmien hallinnasta siirtyy muokkaamaan kyseisen objektin oikeuksia, aukeaa seuraava ikkuna, josta määritellään yksittäiset oikeusasetukset.

Kyseissä ikkunassa voidaan määritellä tarkasti käyttäjää tai ryhmää koskevat kansiokohtaiset oikeudet. Tässä määritellään myös, mihin objekteihin kyseiset asetukset vaikuttavat ja miten oikeudet periytyvät.



Kuva 2. Esimerkkikuva kansion NTSF-oikeuksien hallintatyökalusta.

3.1.1 Oikeuksien tarkempi kuvaus

Seuraavaksi on luetteloituna ja selitettynä kaikki NTFS-oikeudet, jotka voidaan määritellä kansiolle tai tiedostolle. Olen myös numeroinut oikeudet, jotta pystyn esittämään myöhemmin, miten kyseiset oikeudet on määritelty kunkin kansion kohdalla:

1. Käy kansio läpi tai suorita tiedosto
    - Käy kansio läpi: Määrittelee oikeuden siirtyä muuten rajoitetun kansiorakenteen läpi kansioon, johon oikeus on myönnetty. Tämä oikeus ei automaattisesti anna oikeutta ohjelmien suorittamiseen.
    - Suorita tiedosto: Määrittelee oikeuden ohjelmien suorittamiseen kansiossa.
2. Luetteloi kansion sisältö / lue tiedot
    - Luetteloi kansion sisältö: Määrittelee oikeuden nähdä kansion sisältö, tiedostot ja alikansiot.
    - Lue tiedot: Määrittelee oikeuden nähdä tiedostojen sisältö.
3. Lue määritteet
    - Määrittelee oikeuden tiedoston määritteiden tarkasteluun, esim. ”vain luku, tai piilotettu”.
4. Lue lisämääritteet
    - Määrittelee oikeuden tiedoston määritteiden lisämääritteiden tarkasteluun. Lisämääritteitä määrittelevät erilaiset ohjelmat ja ne vaihtelevat ohjelmien mukaan.
5. Luo tiedostot / kirjoita tiedot
    - Luo tiedostot: Määrittelee oikeuden luoda tiedostoja kansioon.
    - Kirjoita tiedot: Määrittelee oikeuden tehdä muutoksia tiedostoon ja ylikirjoittaa olemassa olevan sisällön päälle.
6. Luo kansiot / liitä tiedot
    - Luo kansiot: Määrittelee oikeuden luoda alikansioita.
    - Liitä tiedot: Määrittelee oikeuden tehdä muutoksia tiedoston jatkeeksi, mutta ei vaikuta oikeuteen muuttaa, poistaa ja ylikirjoittaa olemassa olevaa dataa.

7. Kirjoita määritteet

    - Määrittelee oikeudet muuttaa tiedoston tai kansion määritteitä, esim. ”vain luku” tai ”piilotettu”.

8. Kirjoita lisämääritteet

    - Määrittää oikeuden laajennettujen määritteiden muokkaamiseen.

9. Poista alikansiot ja tiedostot

    - Määrittelee oikeuden poistaa alikansioita ja tiedostoja jopa silloin, kun oikeutta ei ole erikseen määritetty alikansiolle tai tiedostolle.

10. Poista

    - Määrittelee oikeuden tiedoston tai kansion poistoon. Jos esim. käyttäjällä ei ole määritetty oikeutta kansion tai tiedoston poistamiseen, on kuitenkin mahdollista poistaa, jos yläkansiossa on määritelty oikeus ”Poista alikansiot ja tiedostot”.

11. Lukuoikeudet

    - Määrittelee oikeuden lukea tiedosto tai kansio.

12. Muutosoikeudet

    - Määrittelee oikeuden kansion tai tiedoston NTFS-oikeuksien muokkaamiseen.

13. Ota omistukseen

    - Määrittelee oikeuden tiedoston tai kansion omistajuuden muuttamiseen omiin nimiin. Tiedoston tai kansion omistaja voi aina muokata objektin oikeuksia riippumatta muista siihen vaikuttavista määritteistä.

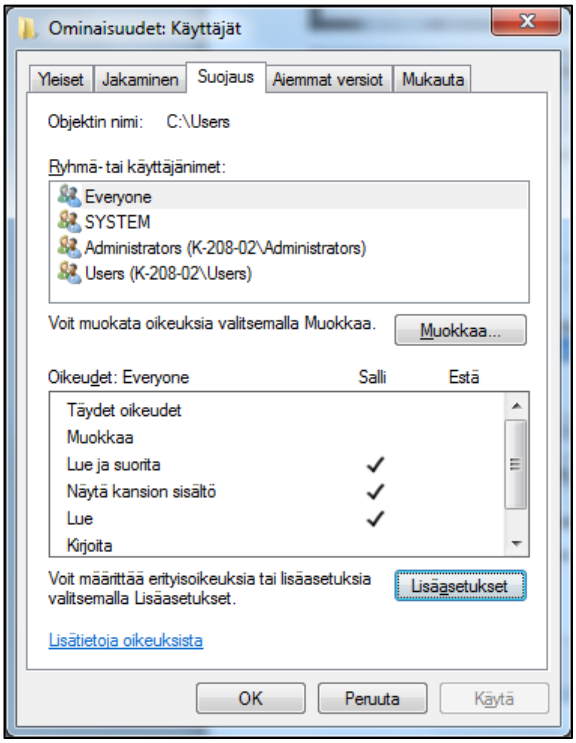
14. Synkronoi

    - Määrittelee oikeuden tiedoston tai synkronointiin, eli automaattiseen kopiointiin toiseen kohteeseen. Käytössä vain tietyissä ohjelmissa [1].

3.1.2 Perusoikeudet

Oikeuksille on myös olemassa valmiiksi määritellyt ”perusoikeudet”, joissa on valmiiksi luotu yleisimpiin käyttökohteisiin soveltuvat paketit yleisimmin tarvittavista käyttöoikeuksista.

Perusoikeudet tarjoavat nopean ja helpon tavan määrittää oikeudet käyttäjille, mutta usein nämä valmiit ratkaisut eivät täytä kaikkia tilannekohtaisia tarpeita. Tällaisissa tapauksissa joudutaan turvautumaan yksityiskohtaisempiin asetusten määrittelyyn.



Kuva 3. Esimerkkikuva kansion perusoikeuksien hallintatyökalusta.

Seuraavassa taulukossa on selvitetty tarkemmin, mitä oikeuksia kukin perusoikeusprofiili sisältää ja miten ne vaikuttavat niin kansioiden kuin tiedostojen oikeuksiin.

Taulukko 1. NTFS-järjestelmän perusoikeuksien vaikutus kansioihin ja tiedostoihin [2].

Perusoikeus	Merkitys kansiossa	Merkitys tiedostossa
Lue	Oikeus lukemiseen ja tiedostojen listaamiseen kansiossa ja alikansioissa	Oikeus tiedoston sisällön lukemiseen
Kirjoita	Oikeus tiedostojen ja alikansioiden lisäämiseen	Oikeus tiedostoon kirjoittamiseen
Lue ja suorita	Oikeus tiedostojen ja alikansioiden listaamiseen, sekä tiedostojen suorittamiseen	Oikeus tiedoston sisällön lukemiseen, sekä tiedoston suorittamiseen
Luetteloi kansion sisältö	Oikeus kansion sisällön näkemiseen ja listaamiseen sekä tiedostojen suorittamiseen	Ei käytössä
Muokkaa	Oikeus lukemiseen ja kirjoittamiseen, oikeus myös poistamiseen	Oikeus tiedostoon kirjoittamiseen ja sen lukemiseen, oikeus myös poistamiseen
Täydet oikeudet	Oikeus lukemiseen, kirjoittamiseen, muuttamiseen ja poistamiseen	Oikeus lukemiseen, kirjoittamiseen, muuttamiseen ja poistamiseen

Perusoikeuksien tarkempi sisältö koostuu etukäteen valituista NTFS-oikeuksista. Taulukossa on esitettynä mitä oikeuksia tietty ”perusoikeus” sisältää.

Taulukko 2. NTFS-järjestelmän perusoikeuksien tarkempi sisältö [2].

Käyttöoikeudet	Täydet oikeudet	Muokkaus	Luku- ja suoritusoikeudet	Luetteloi kansion sisältö	Luku	Kirjoitus
Käy kansio läpi tai suorita tiedosto	X		X	X		
Käy kansio läpi tai suorita tiedosto	X	X	X	X	X	
Lue määritteet	X	X	X	X	X	
Lue lisämääritteet	X	X	X	X	X	
luo tiedostot / kirjoita tiedot	X	X				X
Luo kansiot / liitä tiedot	X	X				X
Kirjoita määritteet	X	X				X
Kirjoita lisämääritteet	X	X				X
Poista alikansiot ja tiedostot	X					
Poista	X	X				
Lukuoikeudet	X	X	X	X	X	X
Muutosoikeudet	X					
Ota omistukseen	X					
Synkronoi	X	X	X	X	X	X

3.1.3 Oikeuksien kohdistus

Kansioiden oikeuksia määriteltäessä tulee myös määritellä, mihin kyseiselle käyttäjälle tai käyttäjäryhmälle myönnetyt oikeudet vaikuttavat ja miten kyseiset oikeudet periytyvät kyseisen kansion alikansioille ja tiedostoille.

Kohdistuksessa on valittavana seitsemän eri vaihtoehtoa, jotka kaikki vaikuttavat erilailla siihen, miten kyseisen oikeusmäärittely periytyy ja mihin tiedostoihin ja/tai kansioihin se vaikuttaa.

Taulukko 3. Oikeuksien kohdistuksen vaikutukset [3].

Kohdistus	Tähän kansioon	kansion alikansioihin	kansion tiedostoihin	Kaikkiin alikansioihin	Tiedostoihin kaikissa alikansioissa
Vain tämä kansio	X				
Tämä kansio, alikansiot, ja tiedostot	X	X	X	X	X
Tämä kansio ja alikansiot	X	X		X	
Tämä kansio ja tiedosto	X		X		X
Vain alikansiot ja tiedostot		X	X	X	X
Vain alikansiot		X		X	
Vain tiedostot			X		X

3.2 Active Directory

Active Directory (AD) on Microsoftin IT-Infrastruktuurin hallintajärjestelmä, käyttäjätietokanta ja hakemistopalvelu. Järjestelmä tarjoaa tavan nimetä, kuvata ja hallita käytössä olevia verkon käyttäjiä, ryhmiä, laitteita, sovelluksia, verkon resursseja jne.

Ensimmäiset testiversiot Active Directorystä esiteltiin vuonna 1996, mutta varsinaiset julkaistut versiot vuonna 1999-2000 Windows 2000 -käyttöjärjestelmän mukana. Sen jälkeen AD on ollut olennainen osa Microsoftin palvelinteknologiaa ja on vakiona kaikissa nykyisissä palvelinkäyttöjärjestelmissä [4].

Microsoftin Active Directoryn ainoa varsinainen kilpailija on Novellin eDirectory-järjestelmä, joka on rakenteeltaan hyvin samankaltainen ja sisältää vastaavia ominaisuuksia. Suurimpina eroina on mm. parempi tuki Unix-järjestelmille.

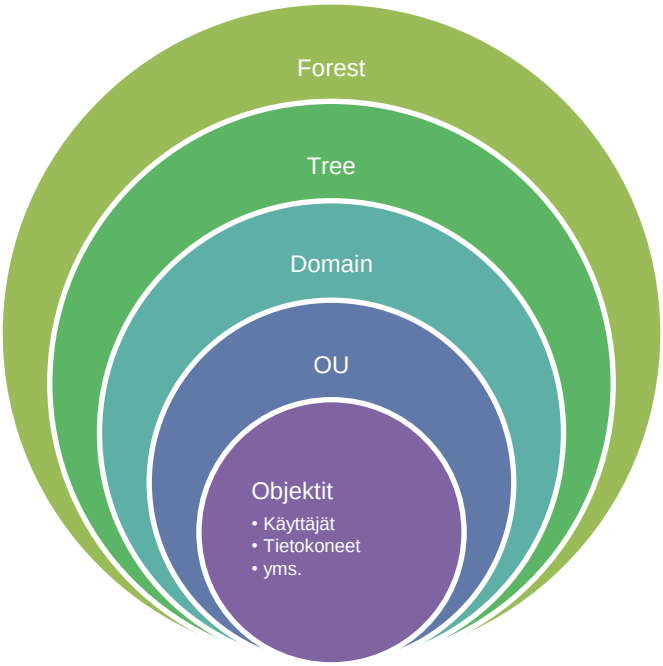
3.2.1 AD:n rakenne

Active Directoryn voisi sanoa toimivan toimialueen eräänlaisena selkärankana ja hallinnoinnin tärkeimpänä työkaluna, joka liittää yhteen käyttäjän, verkon resurssit sekä näiden väliset oikeudet. Sitä voidaan käyttää myös keskitettyyn ohjelmistojen ja asetusten jakeluun.

Active Directory -järjestelmää ajetaan Domain Controller (DC) –palvelimella, joka vastaa toimialueen (domain) käyttöoikeuksien todennuksesta. DC-palvelimelle säilötään tiedot toimialueen resursseista, käyttäjistä ja näiden välisistä käyttöoikeuksista, esim. kun käyttäjä kirjautuu tietokoneelle, joka kuuluu toimialueeseen, Active Directory tarkastaa syötetyn salasanan ja onko käyttäjä määritelty kyseisen tietokoneen peruskäyttäjäksi vai järjestelmänvalvojaksi.

Active Directory käyttää hyväkseen LDAP (Lightweight Directory Access Protocol) -protokollaa , jonka rakenne perustuu X.500-standardiin. Sen perustana on puumainen rakenne, jonka objektit voidaan jakaa rakenteellisesti kahteen ryhmään: säiliöviin ja ei-säiliöviin. Ei-säilövä objekti ei voi sisältää muita objekteja, kun taas säilövä objekti voi sisältää toisia objekteja, esim. ryhmät voivat sisältää käyttäjiä tai toisia ryhmiä [5].

Loogisesti rakenne on kolmitasoinen, joista ylimpänä ovat metsät (Forest), keskimmäisenä puut (Tree) ja alimpana toimialueet (Domain) joilla määritellään mm. käyttäjä- ja konetilit. Tasot ovat yhteydessä toisiinsa luottamussuhteiden avulla, jotka ovat transitiivisia, eli jos A:lla on luottamussuhde B:hen ja B:llä luottamussuhde C:hen, niin tällöin myös A:lla on luottamussuhde C:hen.

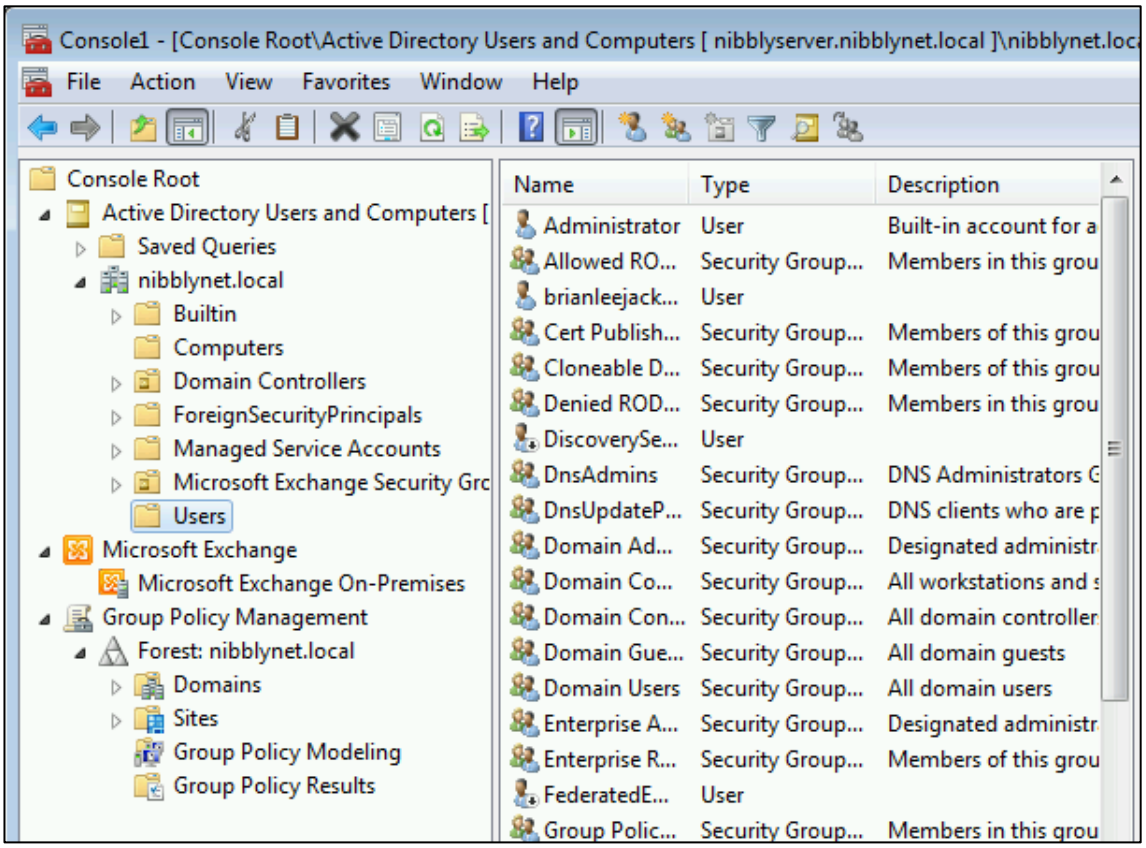


Kuva 4. Active Directoryn looginen rakenne.

Toimialueelle annetaan NetBios-nimi, joka noudattaa DNS (Domain Name System) – menetelmää, joka muuttaa numeropohjaiset IP-osoitteet helpommin muistettaviksi nimiksi. Active Directory vaatii tästä johtuen toiminnassa olevan DNS-palvelun [6].

3.2.2 AD:n käyttö

Tavallisimmin AD:n käyttäminen käyttäjien yms. hallintaan tapahtuu ottamalla yhteys Domain Controller -palvelimeen Microsoft Management Consolen (MMC) sovelluksella. Tämän kautta on mahdollista suorittaa suurin osa hallinnallisista toimenpiteistä, joihin AD on tarkoitettu. MMC-hallintapaneelissa Organisation Unit (OU) -rakenne esitetään kansioina, ja esimerkiksi käyttäjät ja tietokoneet yksittäisinä objekteina.

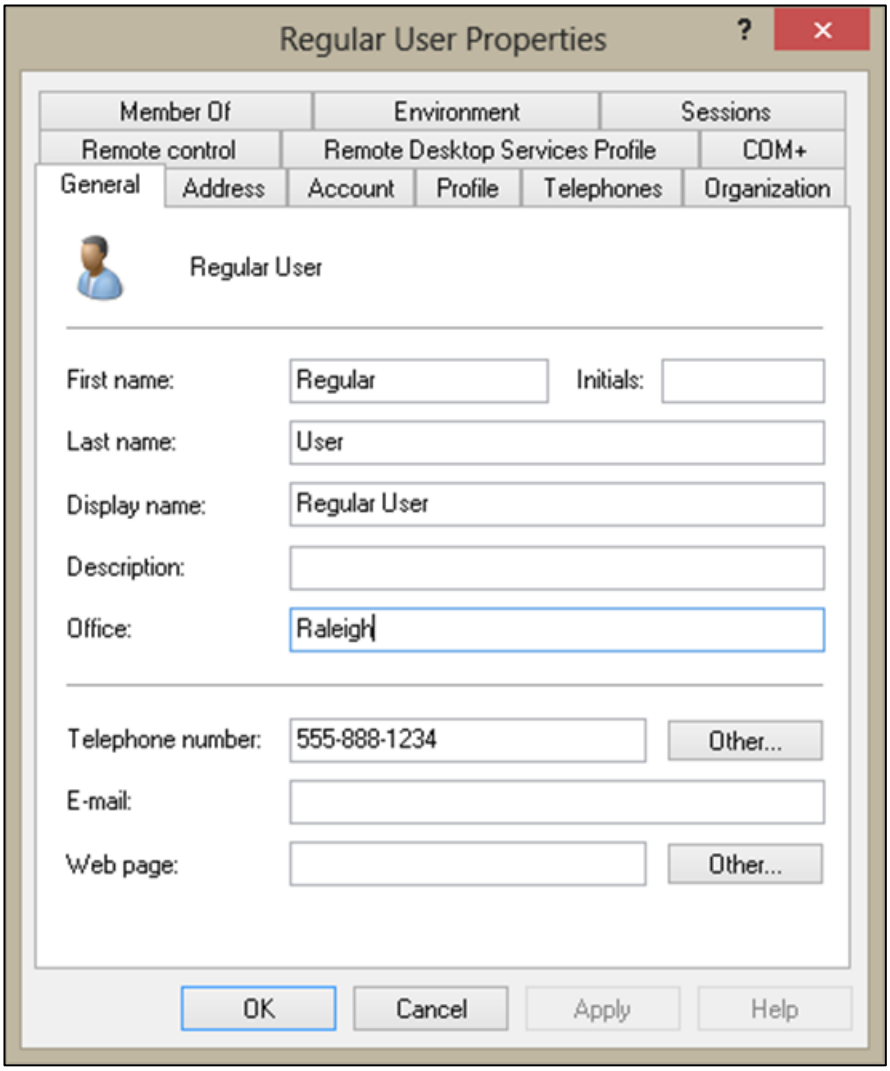


Kuva 5. Esimerkkikuva MMC-hallintapaneelista, jota käytetään Active Directoryn käyttäjien hallintaan [7].

3.2.3 AD-objektit

Active Directoryn hierarkkiseen tietokantaan tallennetaan tietoyksikköjä eli objekteja. Nämä objektit jaotellaan sisällöllisesti karkeasti kolmeen eri kategoriaan: resursseihin eli esimerkiksi työasemiin, palvelimiin ja tulostimiin. Niitä voivat olla palvelut, jotka käsittävät muun muassa tiedostopalvelimet ja sähköpostin, sekä käyttäjät, joihin kuuluvat käyttäjätunnukset ja ryhmät.

Active Directoryn objektit sisältävät oletusarvoisesti uniikkia tietoa: käyttäjä-objekti sisältää tietoa yksittäisestä käyttäjästä, käyttäjäryhmästä, työasemasta tms. Jokaisella objektilla on yksilöllinen DNS-nimi, joka sisältää tyypillisesti yhden tai useamman määritteen, johon tiedot tallennetaan [4].



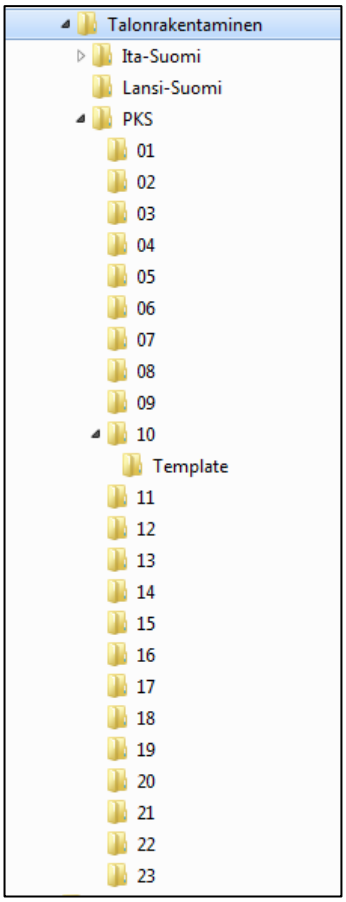
Kuva 6. Esimerkkikuva AD:n käyttäjätunnus-objektista [8].

4 Toteutus

4.1 Kansiorakenne

Uuden verkkolevyn kansiorakenne pyrittiin pitämään mahdollisimman yksinkertaisena ja ylimääräisiä tasoja pyrittiin välttämään. Vanhassa kansiorakenteessa alkoi muodostumaan ongelmaksi liian syvät rakenteet, jotka johtivat liian pitkiin tiedostopolkuihin. Vaikka NTFS-tiedostojärjestelmä pystyy periaatteessa käsittelemään jopa yli 32000 merkin pituisia tiedostopolkuja, rajaa Microsoftin käyttöjärjestelmien ohjelmointirajapinta pituuden alle 260 merkkiin. Tästä saattaa aiheutua tilanteita, joissa on esimerkiksi onnistuttu tallentamaan tiedosto, jonka polku ylittää mainitun 260 merkin pituuden, mutta joka monesti jatkossa estää tiedoston kopioinnin, muokkaamisen ja jopa poistamisen.

Lopulta päädyttiin rakenteeseen, jossa pääkansiona toimii toimialan oma kansio. Tämän jälkeen kansiot jaetaan toimialueiden mukaan. Eri toimialueiden rakenteet ovat keskenään identtisiä, ja esimerkkinä käytämme tässä PKS-toimialueen rakennetta.



Kuva 7. Kansiorakenne, esimerkkinä PKS-toimialueen kansiorakenne. Kansioiden varsinaiset nimet poistettu liiketoiminnallisista syistä.

Eri toimintojen kansioiden numerointi on perua vanhasta verkkolevyjärjestelmästä, johon käyttäjät olivat jo vuosien saatossa tottuneet. Tämä helpottaa myös monesti mm. oikeuksien määrittelyä, kun eri kansioista puhuttaessa voidaan mainita vain numero nimen sijaan. Täten ehkäistään mahdollisia väärinkäsityksiä ja virheitä.

Kansio ”10 Työmaat” oli ainoa kansio, jolle oli tarvetta luoda vielä alikansio, eli Template. Kyseinen Template-kansio toimii kopioitavana pohjana käyttäjille, jotka luovat uusien työmaiden työkansiot. Uutta työmaata perustettaessa käyttäjien on tarkoitus kopioida kyseinen Template-kansio ja nimetä se standardin mukaisesti työmaan tunnistetiedoilla. Näin uusissa työmaakansioissa säilyvät etukäteen määritellyt oikeudet ja rakenne.

4.2 Active Directory-ryhmät

Käyttäjien oikeuksien jakaminen piti suunnitella kokonaan uudelleen. Tähän asti käytössä olleet käytännöt olivat monin paikoin epäselviä, toisistaan poikkeavia ja epäjohdonmukaisia.

Uuden järjestelmän tarkoituksena oli saada aikaan käytäntö, jossa käyttäjän työnkuva määrittelee hänelle oikeudet lukea ja muokata tarvittavia kansioita, ja estää pääsy järjestelmän tiettyihin osiin. Järjestelmän toimiessa suunnitellusti voidaan uudelle työntekijälle myöntää juuri oikeanlaiset oikeudet jo uutta käyttäjää luodessa yksinkertaisesti liittämällä hänet vain käyttäjän työnkuvaa vastaavaan ryhmään.

Käyttäjien työnkuvien ja niihin liittyvien oikeuksien määrittely jäi luonnollisesti toimialan selvitettäväksi. Heidän tehtävänään oli kehittää mahdollisimman pieni määrä käyttäjäryhmiä, johon kaikki erilaiset toimenkuvan omaavat käyttäjät saataisiin lokeroitua. Tehtävä oli luonnollisesti haastava johtuen rakennusalan moninaisista työnkuvista.

Haasteita tarjosi myös kansioiden oikeuksien määrittely. Jokaiselle kansiolle piti olla vähintään kolme erilaista käyttäjäprofiilia: luku-, kirjoitusversio ja täysin estetty versio.

4.2.1 Active Directory -ryhmien rakenne

Tärkeänä kriteerinä ryhmien rakennetta luodessa oli, että käyttäjät ja kansiot eivät olisi suoraan yhteydessä toisiinsa. Näin kansio- tai käyttäjärakenteiden muutoksissa ja uudelleenjärjestelyissä niillä olisi mahdollisimman pieni vaikutus toisiinsa.

Lopulta päädyttiin rakenteeseen, jossa luotiin ryhmät (Security Group) eri toimenkuvan omaaville henkilöille. Näihin ryhmiin siis asetettiin jäseniksi suoraan AD:n käyttäjäprofiileita. Tämän lisäksi jokaiselle kansiolle luotiin kaksi erillistä ryhmää: luku- ja kirjoitusoikeudet sallivat ryhmät. Näihin, tilanteen mukaan oikeisiin, ryhmiin oli tarkoitus liittää jäseniksi eri toimenkuvien käyttöoikeusryhmät.

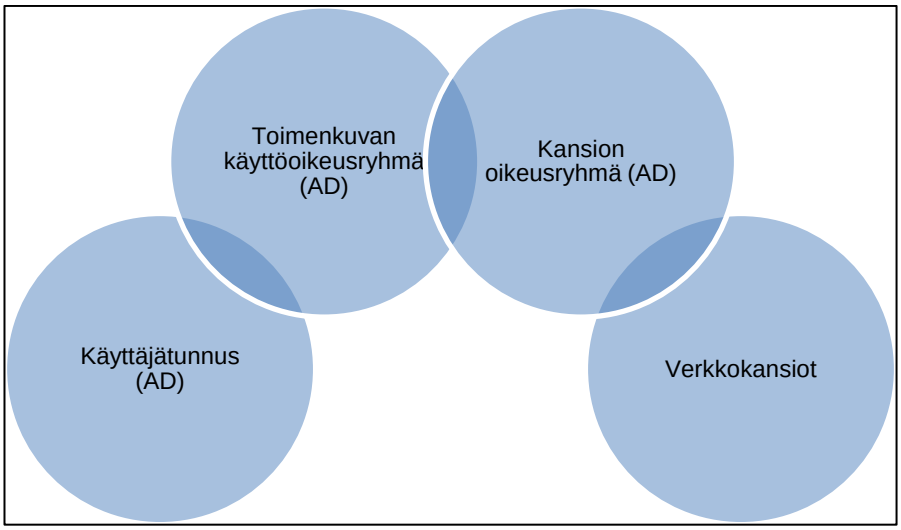
4.2.2 Eri toimenkuvien käyttäjäryhmät

Jokaisella Lemminkäinen Talo Oy:n käyttäjällä on pääsy ”Talonrakennus” -pääkansioon, mutta sen jälkeiset oikeudet määrittelee hänen toimenkuvansa mukainen käyttöoikeusryhmä.

Käyttäjäryhmissä päädyttiin 12 erilliseen ryhmään kunkin toimialueen (PKS, IS, LS) kohdalla, sekä 2:n ryhmään, joilla oli globaaleja oikeuksia eri toimialueiden kesken. Kaksi globaalia ryhmää kuuluivat koko talonrakennustoimialan johdolle, kun taas loput 12 olivat toimialuekohtaisia. Myös käyttäjäryhmät päätettiin numeroida, jotta vältyttäisiin mahdollisilta sekaannuksilta, joita pelkän nimen käyttö voisi aiheuttaa. Käyttäjät ovat siis jäseninä näissä ryhmissä.

4.2.3 Kansioiden oikeusryhmät

Kansioiden oikeusryhmissä oli siis tarkoitus jokaista kansiota varten luoda kaksi erillistä ryhmää: toinen jonka jäsenyys sallisi kirjoitus- ja muokkausoikeudet kyseiseen kansioon, ja toinen, joka sallisi vain lukuoikeudet kyseiseen kansioon.Jjos käyttäjäryhmällä ei ole jäsenyyttä kummassakaan näistä ryhmistä, on kyseisen käyttäjäryhmän jäseniltä pääsy estetty kyseiseen kansioon. Näiden ryhmien jäseninä ovat vain siis aikaisemmin mainitut käyttäjäryhmät.



Kuva 8. Kuvio käyttäjätunnusten, AD-ryhmien ja verkkokansioiden suhteesta.

4.2.4 Ryhmien nimeäminen

Ryhmien nimeämisessä pyrittiin käyttämään loogista rakennetta, joka on käytössä myös muissa samankaltaisissa AD-objekteissa, ja sisältäisi tarvittavan informaation mutta tästä huolimatta pysyisi mahdollisimman kompaktina.

Käyttäjäryhmän nimet muodostuvat osista, jotka on erotettu toisistaan alaviivoilla. Nimen ensimmäinen osa on ”AD”, joka kertoo että kyseessä on Active Directory -objekti. Seuraava osa ”FI” kertoo että kyseessä on Suomen OU:n kuuluva objekti. Tämän jälkeen on lyhenne kyseessä olevasta toimialasta, eli tässä tapauksessa ”Talo”. Tämän jälkeen tulee toimialue, eli joko PKS, IS tai LS. Viimeisenä osana on käyttäjäryhmän numero ja nimi. Lopputuloksena on seuraavan esimerkin kaltainen nimi; ”AD_FI_Talo_PKS_10_Laatu”.

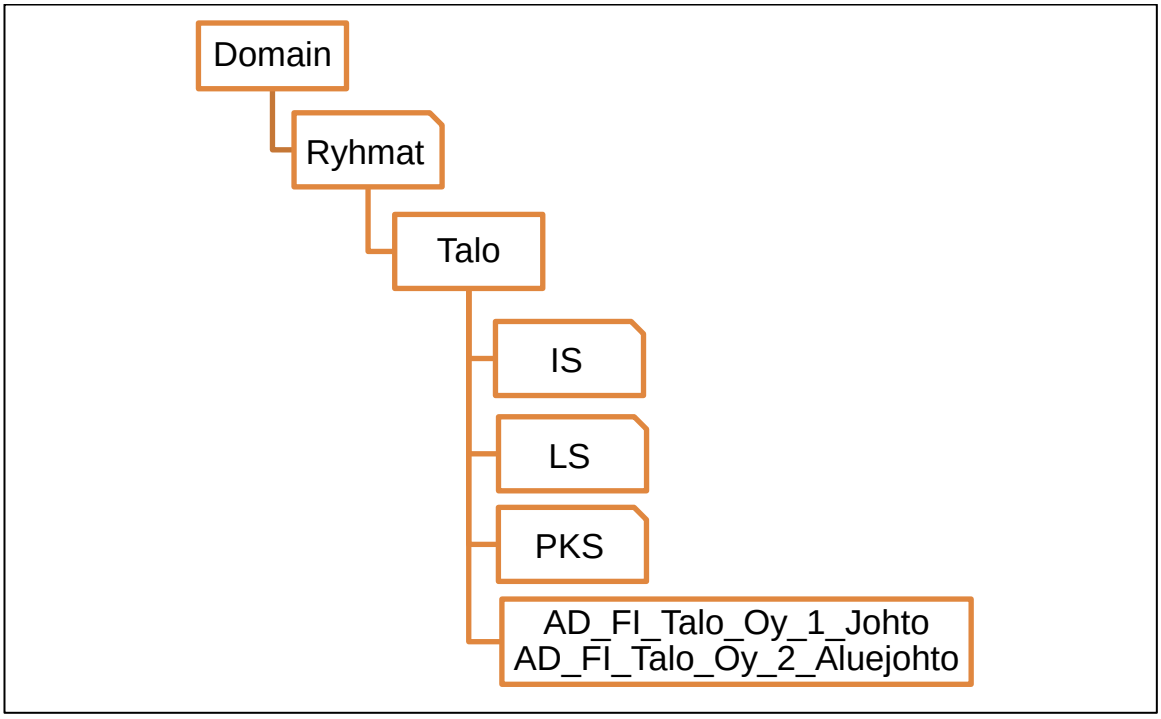
Näiden lisäksi oli vielä kaksi käyttäjäryhmää, jotka oli tarkoitettu toimialan koko maan johdon käyttöön. Nämä käyttäjäryhmät nimettiin muuten samaan tapaan kuin muutkin käyttäjäryhmät lukuun ottamatta toimialuetta, joka korvattiin lyhenteellä ”Oy” koska se kuvaa koko toimialan kattavaa oikeutta.

Kansioryhmien nimiksi muodostui seuraavanlainen: ensimmäinen osa ”FS” on lyhenne sanoista ”File Share”, joka kertoo että kyseessä on tiedostojakoon liittyvä ryhmä. Tämän jälkeen tulee osio, joka kertoo kyseessä olevan toimialan, eli tässä tapauksessa se on ”Talo”. Seuraavaksi toimialue, eli jälleen joko PKS, IS tai LS. Tämän jälkeen tulee kansion nimi ja lopuksi se, onko kyseessä ryhmä, joka antaa oikeuden kirjoittamiseen ”RWD”, vai ainoastaan lukemiseen ”LFC”. Näin syntyy seuraavan esimerkin muotoinen nimi; ”FS_Talo_PKS_asuntomyynti_RWD”.

4.2.5 Ryhmien luonti

Kokonaisuudessaan uusia AD-objekteja tuli luoda 60 kpl / toimialue ja näiden lisäksi kaksi ”globaalia” johdon käyttäjäryhmää. Aluksi tutkitiin mahdollisuutta luoda ryhmät ja niiden väliset jäsenyydet Powershell-scriptiä hyväksikäyttäen, mutta tultiin siihen tulokseen, että ryhmien määrä jäi vielä niin pieneksi, että scriptien luomisesta olisi lopulta ollut enemmän työtä kuin ryhmien manuaalisesti luomisesta.

Alkuperäisessä Active Directoryn OU-rakenteessa on oikeusryhmille oma OU nimeltä ”Ryhmat” suoraan domainin juuressa. Aikaisemmin käytössä olleiden verkkokansioiden oikeusryhmät olivat suoraan tämän ”Ryhmat” OU:n alla. Uutta järjestelmää varten luotiin toimialalle uusi ”Talo”-kansio, jonka alla on jokaiselle toimialueelle oma kansionsa. Nämä kansiot sisältävät tarvittavat AD-objektit. Toimialan johdon kaksi käyttäjäryhmää ovat suoraan ”Talo” OU:n alla.



Kuva 9. Active Directoryn OU-rakenteesta. IS, LS ja PKS ovat eri toimialueiden OU-objekteja, jotka sisältävät tarvittavat oikeusryhmät. ”AD_FI_Talo_Oy_1_Johto” ja ”AD_FI_Talo_Oy_2_Aluejohto” ovat käyttäjäryhmiä.

4.2.6 Käyttäjien liittäminen ryhmiin

Projektin viimeinen osio oli käyttäjien liittäminen oikeisiin käyttäjäryhmiin. Tämä tapahtui yksinkertaisesti niin, että toimiala toimitti listat, joissa oli merkitty, mihin ryhmään kukakin käyttäjä kuului. Tämän jälkeen yksinkertaisesti lisättiin kyseiset käyttäjät ryhmien jäseniksi. Tulevaisuudessa esim. uusien työntekijöiden tullessa taloon tai toimenkuvan muutoksissa näiden ryhmien hallinnoinnista vastaa käyttöoikeuksiin erikoistunut tiimi.

4.3 NTFS-oikeuksien määrittely

Oikeuksien määrittely käyttäjäryhmille kunkin kansion osalta osoittautui työlääksi vaiheeksi. Johtuen tarkoista vaatimuksista kansioiden ja tiedostojen käyttöoikeuksien suhteen emme voineet käyttää kansioiden perusoikeusprofiileja. Käytännössä tämä merkitsi sitä, että kaikkiin 23:n kansioon piti käydä manuaalisesti asettamassa jokainen 14:stä oikeudesta, 2:lle (luku ja kirjoitus oikeudet sallivalle) ryhmälle joko ”Salli”- tai ”Estä”-tilaan.

4.3.1 Suunnittelu

Alkuperäisessä projektisuunnitelmassa kansioille oli määritelty jo tarkkaan, mitkä oikeudet kullekin ryhmälle tulee myöntää. Aluksi seurattiin tätä suunnitelmaa, mutta pian ensimmäisten testien aikana huomattiin, että kyseisessä suunnitelmassa oli useita virheitä, eikä se monilta osin vastannut asiakkaan, eli toimialan toivomuksia. Tämä tarkoitti sitä, että nähtiin tarpeelliseksi suunnitella oikeudet kokonaan uudelleen.

Lähtökohtana oikeuksissa oli yleisten tietoturvasuositusten mukaisesti se, että vain tarpeelliset asiat sallitaan, ja kaikki muu on estetty. Käyttäjille ei ole tarvetta antaa oikeuksia muuhun kuin välttämättömiin toimintoihin, jotta kyseiset verkkolevyt pysyisivät toimintakykyisinä ja organisoituina mahdollisimman pienellä ylläpitovaivalla.

4.3.2 Lopulliset käyttäjäryhmien oikeudet

Toimialueen pääkansioon ei ole millään käyttäjäryhmällä muita kuin lukuoikeudet. Näin käyttäjät eivät pääse edes vahingossa muokkaamaan kansiorakennetta. Sama koskee myös kansiota, jossa sijaitsee vanhan verkkolevyn sisältö. Näiden lisäksi poikkeuksen oikeuksissa muodostaa ”10 Työmaat” -kansio, jonka alikansiona löytyvä, työmaakansioiden pohjana käytettävä ”Template”-kansio, ja siihen liittyvät oikeudet vaativat erikoisempia asetuksia verrattuna muihin rakenteen kansioihin.

Taulukossa on esitetty kaikki kansiorakenteeseen kuuluvat kansiot ja ryhmät, joille on myönnetty oikeudet niihin, miten oikeudet on kohdistettu, ja lopulta numeroin, mitkä oikeudet on kytketty ”Salli” -tilaan kyseisen ryhmän kohdalla. Eri numeroita vastaavat oikeudet löytyvät kohdasta 3.1.1

”SYSTEM” ja ”Domain Admins” ovat luonnollisesti ylläpidollisia käyttäjäryhmiä joilla on tästä syystä täydet oikeudet kyseisten kansiorakenteiden kaikkiin osioihin. Ryhmien nimessä esiintyvä ”...” korvaa kansion nimen kansioiden 1-9 sekä 11-23, kansioon kymmenen määritellyt oikeudet esitellään seuraavassa taulukossa.

Taulukko 4. Kansiorakenteen käyttöoikeudet.

Talonrakentaminen/PKS

Ryhmä	Kohdistus	Oikeudet
SYSTEM	Tämä kansio, alikansiot ja tiedostot	Täydet oikeudet
Domain Admins	Tämä kansio, alikansiot ja tiedostot	Täydet oikeudet
Deleg-it	Tämä kansio, alikansiot ja tiedostot	Täydet oikeudet
FS_talo_pks_LFC	Vain tämä kansio	2, 3

Talonrakentaminen/PKS/1-9 & 11-23

Ryhmä	Kohdistus	Oikeudet
SYSTEM	Tämä kansio, alikansiot ja tiedostot	Täydet oikeudet
Domain Admins	Tämä kansio, alikansiot ja tiedostot	Täydet oikeudet
FS_talo_pks_..._RWD	Tämä kansio ja alikansiot	2, 3, 5-7, 10, 12
FS_talo_pks_..._RWD	Vain tiedostot	3-9, 11, 12
FS_talo_pks_..._LFC	Tämä kansio, alikansiot ja tiedostot	2-5, 12

Talonrakentaminen/PKS/10 Työmaat

Ryhmä	Kohdistus	Oikeudet
SYSTEM	Tämä kansio, alikansiot ja tiedostot	Täydet oikeudet
Domain Admins	Tämä kansio, alikansiot ja tiedostot	Täydet oikeudet
FS_talo_pks_tyomaat_RWD	Vain tämä kansio	2, 3, 6, 7, 12
FS_talo_pks_tyomaat_RWD	Vain alikansiot ja tiedostot	2-9, 11, 12
FS_talo_pks_tyomaat_LFC	Tämä kansio, alikansiot ja tiedostot	2-5, 12

Talonrakentaminen/PKS/10 Työmaat/Template

Ryhmä	Kohdistus	Oikeudet
SYSTEM	Tämä kansio, alikansiot ja tiedostot	Täydet oikeudet
Domain Admins	Tämä kansio, alikansiot ja tiedostot	Täydet oikeudet
FS_talo_pks_tyomaat_LFC	Tämä kansio ja alikansiot	3, 4, 5, 12
FS_talo_pks_tyomaat_RWD	Tämä kansio ja alikansiot	3, 4, 5, 12

4.4 Testaus ja korjaukset

Uuden kansiorakenteen ja siihen liittyvien käyttöoikeuksien testaus suoritettiin kahden henkilön voimin täysin manuaalisesti. Käytännössä työ eteni niin, että yksi henkilö toimi testihenkilönä, ja toinen vastasi AD:n hallinnasta sekä ongelmien ylöskirjaamisesta ja niiden korjaamisesta ”lennossa”. Testausympäristönä toimi tietohallinnon oma testauspalvelin, jolle palvelintiimi oli luonut tuotanto-olosuhteita vastaavan verkkolevy-ympäristön.

Testaus tapahtui niin, että luotiin uusi Active Directory –käyttäjätunnus, jolle myönnettiin oikeudet aivan kuten toimialan henkilölle olisi tehty. Tämän jälkeen siirrettiin käyttäjätunnus aina vuorotellen eri toimenkuvien ryhmien jäseneksi, tarkastettiin, mihin kansioihin hänellä pitäisi olla minkälaiset oikeudet (luku/kirjoitus) ja testattiin, pystyykö käyttäjä suorittamaan tarvittavat toimet tai onko käyttäjältä estetty tiettyjen toimintojen suorittaminen niin kuin kuuluisi.

Testaukseen aikana ei ilmennyt vakavia ongelmia. Joitain satunnaisia oikeuksiin liittyviä epämääräisyyksiä havaittiin, mutta nämä johtuivat poikkeuksetta kansioiden NTFS-oikeuksien määrittelyssä tapahtuneista virheistä. Nämä oli kuitenkin helppo paikallistaa ja korjata. Muita ongelmia ei testauksen aikana järjestelmästä löydetty. Tämä varmasti johtuu suurelta osin siitä, että työtä tehdessä ja suunnitellessa toteutettiin jatkuvasti pienimuotoista testausta, jotta voitiin olla varmoja, että valitut käytännöt ja menetelmät olivat toimivia.

4.5 Järjestelmän siirtäminen tuotantoon

Testauksen jälkeen oli enää jäljellä järjestelmän julkaisu tuotantoon. Käytännössä tästä työstä vastasi palvelintiimi, joka kopioi testiympäristöön luodun kansiorakenteen, säilyttäen kansiolle määritellyt oikeudet, tuotantoympäristöön. Tämän lisäksi vanha tuotantoympäristö linkitettiin osaksi uutta rakennetta ja ”jäädytettiin” niin, että kyseiseen osioon ei pystynyt tekemään enää muutoksia.

Käyttäjille luotiin tiukka ohjeistus uuden kansiorakenteen käyttöön, jotta tulevaisuudessa vältyttäisiin rakenteen pirstoutumiselta. Ohjeistus sisälsi seuraavat pääkohdat:

- Nyt käytössä oleva Y-asema siirretään kansioon ”23 Alueen vanha Y-asema”.
  - Kyseiseen kansioon ei voi tulevaisuudessa tallentaa uusia tiedostoja.
  - Kyseisestä kansiosta voidaan lukea ja kopioida tiedostoja.
- Maksimipituus tiedostonimelle ja tiedostopolulle saa olla enimmillään 240 merkkiä. Tästä syystä pyritään välttämään lauseiden käyttöä tiedostojen/kansioiden nimeämisissä.
- Kansion maksimimerkkimäärä nimessä on 20 merkkiä.
- Tiedoston maksimimerkkimäärä nimessä on 30 merkkiä.
- Allekkaisten kansiorakenteiden määrä saa olla enintään 6 kpl.
- Sallitut merkit kansioissa tai tiedostoissa ovat kirjaimet a-ö, numerot 0-9, välilyönnit, alaviivat sekä väliviivat.

Tästä ohjeistuksesta luotiin Powerpoint-esitys, joka sisälsi ohjeiden lisäksi myös käytännön esimerkkejä sekä kokonaisvaltaisemman selostuksen uuden järjestelmän käyttöönotosta.

5 Yhteenveto

Insinöörityön tavoitteena oli toteuttaa uusi verkkolevyjärjestelmä yrityksen toimialan käyttöön. Uuden järjestelmän tarkoitus oli korjata vanhaan järjestelmään vuosien myötä syntyneet ongelmat ottaen huomioon suunnittelussa niin käyttäjien kuin ylläpidon tarpeet. Tärkeänä kriteerinä uuden järjestelmän suunnittelussa oli myös pyrkiä välttämään samanlaisten ongelmien uusiutuminen, joita lopulta syntyi vanhaan järjestelmään.

Uuden järjestelmän vastaanotto oli positiivinen niin käyttäjien kuin ylläpidonkin taholta. Uuden järjestelmän käyttöoikeusrakenne on selkeä, jonka myötä aika säästyy molemmilla tahoilla.

Aikaisemmin esimerkiksi uusi käyttäjä piti lisätä useaan käyttöoikeusryhmään sitä mukaan, kun tarpeita ilmeni. Nyt uuden järjestelmän ansiosta lisäämällä käyttäjän vain yhteen ryhmään saa hän käyttöönsä kaikki tarvittavat resurssit verkkolevyltä. Myös esimerkiksi Active Directoryn OU-rakenteiden tai verkkolevyn palvelinten muutokset ja siirtelyt tulevaisuudessa pystytään toteuttamaan paljon joustavammin, kun suorat kytkökset käyttäjien ja tiedostopalvelinten resurssien väliltä on korvattu uudella käyttäjäryhmiin perustuvalla järjestelmällä.

Uusi kansiorakenne on myös saanut kiitosta tehokkaasta toiminnasta. Aikaisemmin ongelmia esiintyi muun muassa vanhojen dokumenttien paikallistamisessa, ja myös liian pitkistä tiedostopoluista johtuvat ongelmat esimerkiksi varmistuksessa. Uusien ratkaisujen myötä näistä ongelmista on päästy eroon ja tiukkojen oikeusmäärittelyiden sekä käyttäjien ohjeistuksen myötä kyseisiä ongelmia ei esiinny jatkossa.

Kokonaisuudessaan projekti oli kuitenkin onnistunut, asetetut tavoitteet saavutettiin ja kokonaisuus valmistui aikataulussa. Uudesta järjestelmästä saatiin aikaan myös kattava dokumentaatio, jonka avulla pystytään tulevaisuudessa välttymään monilta vanhaa järjestelmää vaivanneelta ongelmalta.

Lähteet

1 File and folder advanced permissions. NTFS.com; 2014. Saatavilla: http://www.ntfs.com/ntfs-permissions-file-advanced.htm.

2 File and folder permissions. Microsoft Technet; 2014. Saatavilla: http://technet.microsoft.com/en-us/library/bb727008.aspx.

3 Determine where to apply permissions. Microsoft Technet; 2014. Saatavilla: http://technet.microsoft.com/en-us/library/cc771309.aspx.

4 Verkon nimi- ja hakemistopalvelut. Talvivaara, Jarmo; 2014. Saatavilla: http://www2.amk.fi/mater/tietotekniikka/nimipalvelut/8_activedirectory.html.

5 Technical Overview of directory services using the X.500 protocol, Weider, C. Reynolds, J. Heker, S.; 1992. Saatavilla: http://www.ietf.org/rfc/rfc1309.txt?number=1309.

6 Active Directory. Technoxx; 2014. Saatavilla: http://www.technoxx.com/active-directory.htm.

7 Configure MMC Snap-ins on Fresh Windows 7 Install. Jackson, Brian; 2014. Saatavilla: http://theitbros.com/configure-mmc-snap-ins-on-fresh-windows-7-install/.

8 Use the PowerShell AD Provider to Modify User Attributes. Wilson, Ed; 2013. Saatavilla: http://blogs.technet.com/b/heyscriptingguy/archive/2013/03/21/use-the-powershell-ad-provider-to-modify-user-attributes.aspx.

Taulukko käyttäjäryhmien oikeuksista kansioihin

Käyttäjäryhmä	1	2	2.1	3	4	5	6	7	8	9	10	11	12
Kansio													
1	L	ei	L,M,P	L	L	L	ei	ei	ei	L,M,P	ei	L	ei
2	L	ei	L,M,P	L,M,P	L,M,P	L,M,P	ei	ei	ei	ei	ei	L,M,P	ei
3	L	ei	L,M,P	L,M,P	L,M,P	ei	ei	ei	ei	ei	ei	ei	ei
4	ei	ei	L,M,P	ei	ei	ei	ei	ei	ei	ei	ei	L,M,P	ei
5	L	ei	L,M,P	L,M,P	L,M,P	L,M,P	ei	ei	ei	ei	L,M,P	L	L
6	L	ei	L,M,P	L,M,P	L	L,M,P	ei	L	L	L	L,M,P	L	L
7	L	ei	L,M,P	L,M,P	L,M,P	L,M,P	L	L	L	L	L,M,P	L	L
8	L	ei	L,M,P	L,M,P	L,M,P	L,M,P	ei	L	L	L	L,M,P	L,M,P	L
9	L,M,P	ei	L,M,P	L,M,P	L,M,P	L,M,P	ei	ei	L	ei	L,M,P	L,M,P	L
10	L	ei	L,M,P	L,M,P	L	L,M,P	L,M,P	L,M,P	L	ei	L,M,P	L	L
11	L	ei	L,M,P	L,M,P	L	L,M,P	ei	L	L,M,P	ei	L,M,P	L	L
12	L	ei	L,M,P	L	L	L	L	L,M,P	L	L	L,M,P	L	L
13	L	ei	L,M,P	L	L	L	L	L	L	L	L,M,P	L	L
14	L	ei	L,M,P	L,M,P	L	L,M,P	L,M,P	L, M, P	L, M, P	ei	L, M, P	L,M,P	L,M,P
15	L	ei	L,M,P	L,M,P	L, M, P	L, M, P	L	L	L	L	L, M, P	L,M,P	L
16	L,M,P	ei	L,M,P	L,M,P	L	L	L	L	L	L	L,M,P	L	L
17	L,M,P	ei	L,M,P	L,M,P	L, M, P	L, M, P	ei	ei	ei	ei	L, M, P	L,M,P	ei
18	L,M,P	ei	L,M,P	L,M,P	L, M, P	L, M, P	L, M, P	L, M, P	L, M, P	L, M, P	L, M, P	L,M,P	L, M, P
19	L,M,P	ei	L,M,P	L	ei	ei	ei	ei	ei	ei	ei	L,M,P	ei
20	L,M,P	ei	L,M,P	L,M,P	L,M,P	L,M,P	L	L	L	L	L, M, P	L	L
21	L	ei	L,M,P	L	L	L	L	L	L	L	L, M, P	L	L, M, P
22	L	ei	L,M,P	L,M,P	L	L,M,P	L,M,P	L,M,P	L,M,P	L,M,P	L,M,P	L	L, M, P
23	L	ei	L,M,P	L	L	L	L	L	L	L	L	L	L

Käyttöoikeuksien selitykset: Lukuoikeus = L, muokkaus = M ja poisto = P, ei= ei mitään oikeuksia.