KÄYTTÖOIKEUKSIEN HALLINTA MICROSOFT WINDOWS-TIEDOSTOPALVELIMILLA

Käyttöoikeuksien hallinnalla (acl, access control lists) tarkoitetaan tässä ohjeessa niitä oikeuksia, joita yksittäisillä käyttäjillä (user) tai käyttäjäryhmillä (user groups) määritetään Windows 200x-tiedostopalvelimella sijaitsevaan kansioon tai tiedostoon.

1 OHJEEN TARKOITUS

Tämä asiakirja on tarkoitettu esimerkinomaiseksi ohjeeksi otettavaksi huomioon tiedostopalvelimien käyttöoikeusasioita suunniteltaessa. Ohjeessa käytetään esimerkkinä Windows 2003-tiedostopalvelinta Active Directory-ympäristössä. Valtaosa ohjeen suosituksista voidaan toteuttaa myös Windows 2000-palvelinympäristössä sekä soveltaen myös muissa käyttöjärjestelmissä.

Jokainen ympäristö on kuitenkin oma erikoistapauksensa ja tämän takia kaiken kattavan ohjeen laatiminen on mahdotonta. Organisaation tietoturvasuunnitelmassa tai palvelinjärjestelmien tietoturvallisuusohjeistuksessa on otettu mahdollisesti kantaa näihin samoihin seikkoihin, joissain tapauksissa näitä suosituksia tiukemmalla tasolla. Tässä ohjeessa ei ole erikseen otettu kantaa vahvaan tunnistamiseen tai kolmansien osapuolien auditointi-tuotteiden käyttöön, joilla Windows-käyttöjärjestelmän puutteita voidaan paikata.

2 YLEISTÄ KÄYTTÖOIKEUKSIEN MYÖNTÄMISESTÄ

Käyttöoikeuksien myöntäminen pitää olla ohjeistettua ja valvottua. Käyttöoikeuksien hallinta tulee olla hallittua siten, että käyttöoikeuksien määrittäminen järjestelmään tapahtuu ennalta valtuutettujen palvelimien pääkäyttäjien toimesta. Muutospyynnöt sekä niiden pohjalta tehdyt käyttöoikeuksien muutokset tulee olla dokumentoituja.

Tyypillisesti käyttöoikeuksia muutetaan uuden käyttäjän tullessa organisaatioon, käyttäjän tarpeiden muuttuessa tai kun käyttäjä jättää organisaation. Työmääräykset käyttöoikeuksien muuttamiseksi pitää tulla kyseisen kansion tai jaetun resurssin omistajalta eli henkilöltä, joka toimii kyseisen tietosisällön hallinnollisena pääkäyttäjänä.

Uusien käyttäjien tapauksessa tämä on tyypillisesti automatisoitu uuden käyttäjän lisäämisprosessiin. Kun käyttäjä jättää organisaation, on erittäin tärkeää huolehtia siitä, että työntekijän tuottamat tiedostot tulevat tehokkaaseen käyttöön hänen seuraajalleen tai muille kollegoille. Tässä yhteydessä pitää huolehtia käyttäjän mahdollisten yksityisten tiedostojen oikeaoppisesta yksityisyyden suojan huomioivasta hävittämisestä. Suositeltavaa olisi pyytää poislähtevää käyttäjää huolehtimaan itse tällaisten yksityisten tiedostojen hävittämisestä.

Kaikille palvelimien pääkäyttäjille ei tulisi olla automaattisesti oikeutta tiedostojen ja kansioiden käyttöoikeuksien myöntämiseen, vaan sitä varten tulisi perustaa oma käyttöoikeusryhmä, jonka käyttö olisi sallittu vain käyttöoikeuksien myöntämises-

tä vastaaville pääkäyttäjille. Tässä ohjeessa käytetään ACL_admin-nimistä käyttäjäryhmää (AccessControlList_Admin) kyseisten oikeuksien antamiseen.

Active Directory-ympäristössä tulee rajata pääkäyttäjien käyttöoikeuksia esimerkiksi delegoimalla oikeuksia siten, että käyttäjätileistä (user account) vastaavilla henkilöillä olisi vain kyseiseen toimintaan tarvittavat käyttöoikeudet eikä kaikkia mahdollisia käyttöoikeuksia. Käyttöoikeuksien määrittäminen pitäisi olla dokumentoitu valmiiksi erilaisia käyttötarpeita varten.

a) Yleisimpiä käyttöoikeuksien myöntämiskohteita

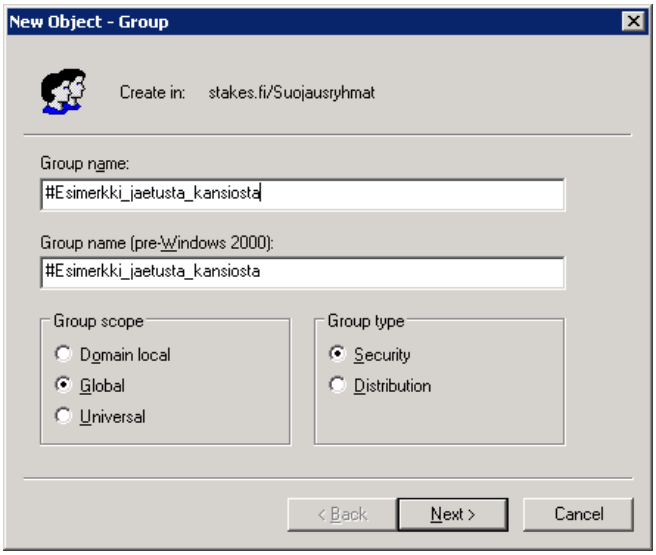
Tyypillisesti käyttöoikeuksia joudutaan myöntämään ja vaihtamaan seuraaviissa tilanteissa:

a) käyttäjän kotihakemisto (home directory)
b) käyttäjän mahdollinen palvelimelle tallennettu käyttäjäprofiili (user profile)
c) käyttäjän jokin muu palvelimella sijaitseva yksityinen kansio
d) useammasta käyttäjästä muodostuvan käyttäjäryhmän käyttämä kansio
e) kansiotaso, jonne kaikille käyttäjille halutaan antaa pääsy

Kohdissa a-c kyseisiin kansioihin ei normaalisti anneta kenellekään muille käyttäjille käyttöoikeutta kuin kansion loppukäyttäjä. Tällöin loppukäyttäjälle annetaan muutos- eli modify-oikeus, jolloin hän periaatteessa voi itse muuttaa käyttöoikeuksia. Mikäli lisäksi järjestelmän pääkäyttäjälle halutaan sallia pääsyoikeus, pitää se myöntää ACL_admin-ryhmälle oletuksena olevien administrators tai domain admins-ryhmien sijaan.

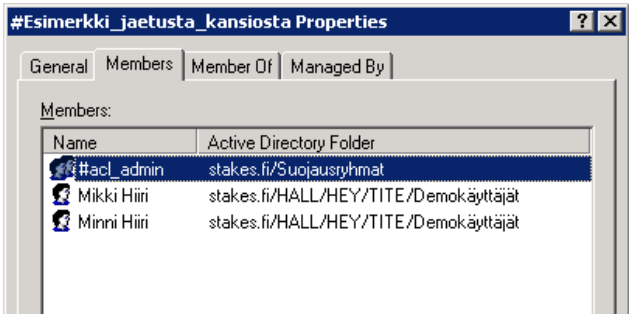
b) Suojausryhmien hyödyntäminen

Kun jaettavaksi halutaan laittaa kansio, johon pitää sallia pääsy useammalle kuin yhdelle henkilölle, pitää tätä varten perustaa oma suojausryhmä (security group). Älä lisää jaettavaan kansioon käyttöoikeuksia yksittäisille käyttäjille, vaan käytä aina suojausryhmiä! Tämä helpottaa oikeuksien muuttamista sekä mikäli käyttäjä jättää organisaation, on hänen käyttöoikeudet helppo hävittää poistamalla käyttäjä niistä suojausryhmistä, joissa hän on jäsenenä.



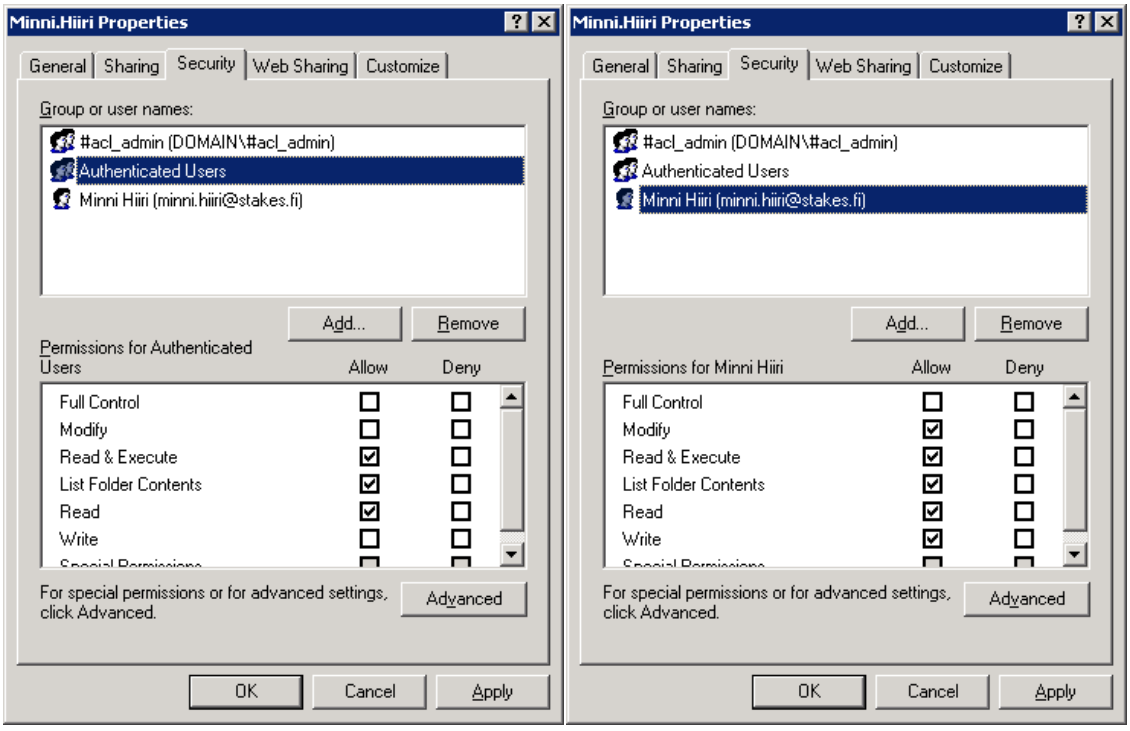
Kuva 1. AD-hakemistoon tehdään suojausryhmä, jonka nimeksi annetaan jaetun resurssin nimi. Ryhmän tyyppi riippuu käytössä olevasta AD/toimialue-ratkaisusta.

Uuden ryhmän nimi voi olla esimerkiksi jaettavan resurssin nimi ja siihen voidaan valita sopiva erikoismerkeistä koostuva alkuliite, jolla tällaiset ryhmät on helppo erottaa toisistaan, esimerkiksi #-merkki ryhmän nimen alkuun.



Kuva 2. Ryhmään lisätään ne yksittäiset käyttäjät tai muut suojausryhmät, joille halutaan sallia käyttöoikeus tehtyyn jaettuun resurssiin.

Kohdassa e) halutaan tehdä jaettu resurssi, jonne kaikille käyttäjille halutaan sallia pääsy. Tällaisessa ratkaisussa yleisin virhe on se, että kaikille käyttäjille sallitaan kaikki oikeudet kaikkiin kansioihin! Mikäli tällaisessa tapauksessa yksittäisen käyttäjän työasemaan pääsee leviämään haittaohjelma, pystyy se levittämään itsensä myös kaikkien muiden käyttäjien kansioihin, mikäli käyttäjällä on niihin kansioihin muutosoikeus.

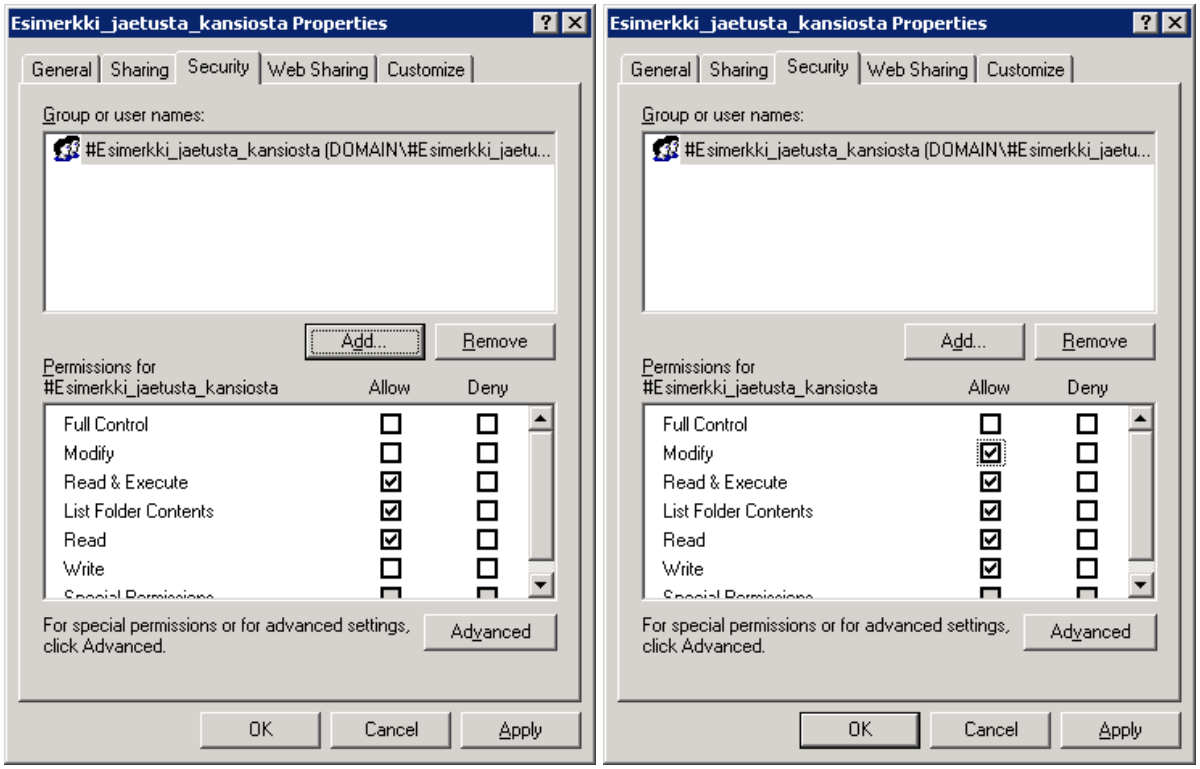


Kuva 3. Ryhmän ”everyone” sijaan kannattaa käyttää authenticated users, tässä tapauksessa sen ryhmän jäsenet eli kaikki toimialueelle kirjautuneet käyttäjät saavat lukuoikeuden Minni Hiiren kansioon. Minni.Hiiri-käyttäjälle annetaan hänen omaan kansioon muutos-oikeudet.Tämän lisäksi #alc_admin-ryhmälle annetaan Full Control eli täydet oikeudet, mikäli kansion omistaja ei osaa/halua itse määrittää mahdollisia muita lisäoikeuksia.

3 TARVITTAVAT KÄYTTÖOIKEUDET

AD-ympäristössä voidaan luoda satoja erilaisia käyttöoikeuksia yhdistelemällä eri käyttöoikeustasoja. Käytännössä toimeen tullaan 99 % tapauksista kolmella eri käyttöoikeustasolla:

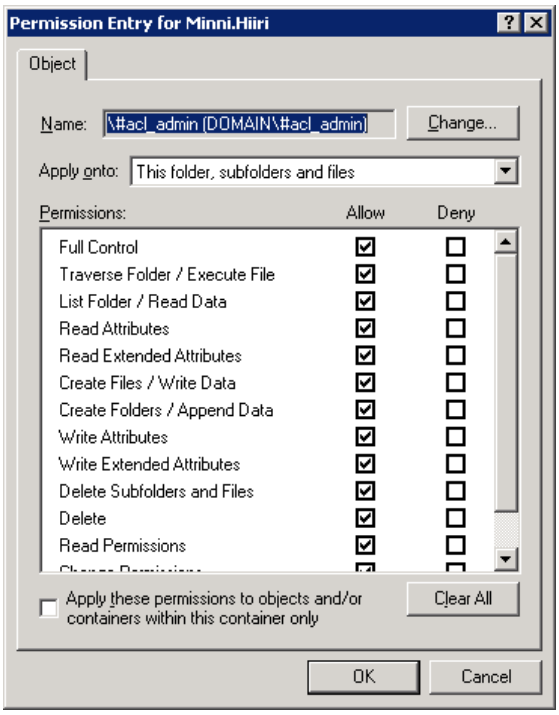
a) lukuoikeus (read)
b) muutosoikeus (modify)
c) täydet oikeudet (full control)



Kuva 4. Vasemmalla #Esimerkki-ryhmälle on määritetty lukuoikeus ja oikeanpuoleisessa kuvassa samalle ryhmälle on annettu muutos- eli modify-oikeus, joka koostuu read & execute-oikeuksien ohella myös write- ja modify-oikeuksista.

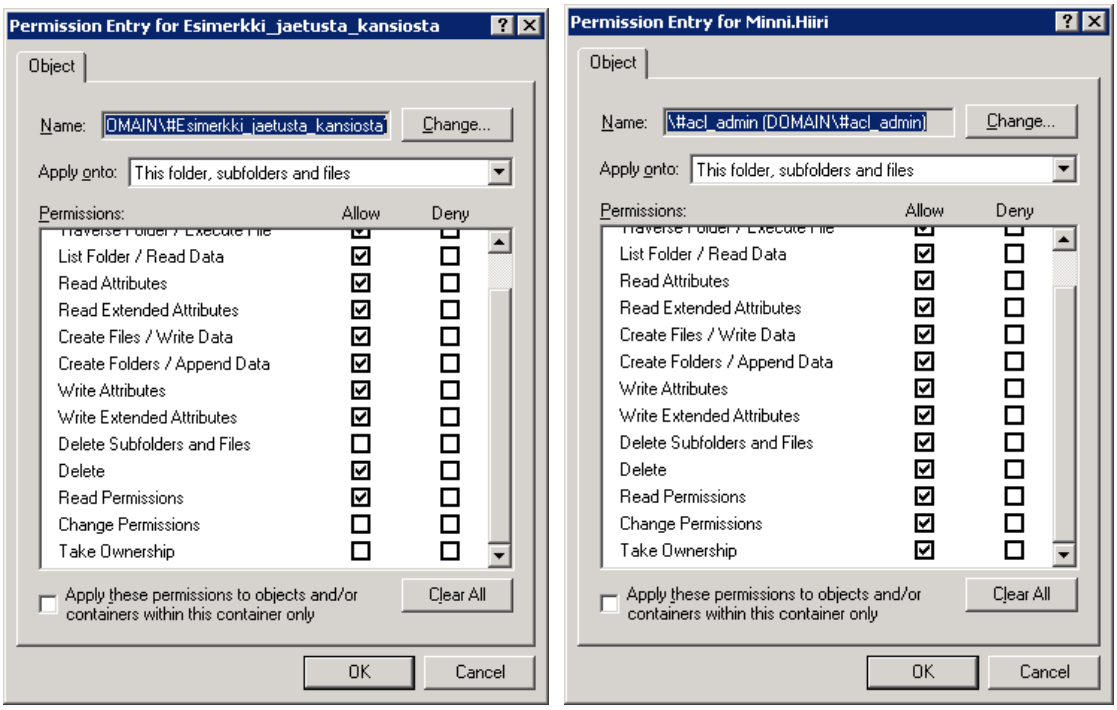
Lukuoikeus (read) tulee antaa käyttäjälle tai ryhmälle, kun kohteen pitää pystyä käynnistämään sovellus tai avaamaan tiedosto ilman, että käyttäjällä on tarvetta tallettaa, poistaa tai uudelleennimetä tiedostoja tai kansioita.

Muutosoikeus (modify) sallii käyttäjän tallettaa, poistaa ja uudelleennimetä tiedostoja tai kansioita. Tämä on normaalisti kaikista laajin käyttöoikeus, joka tulisi sallia tavallisille loppukäyttäjille. Muutosoikeutta ei pidä antaa, ellei sille ole erityinen tarve eli käyttäjän/ryhmän pitää päästä muuttamaan kansion sisältöä.

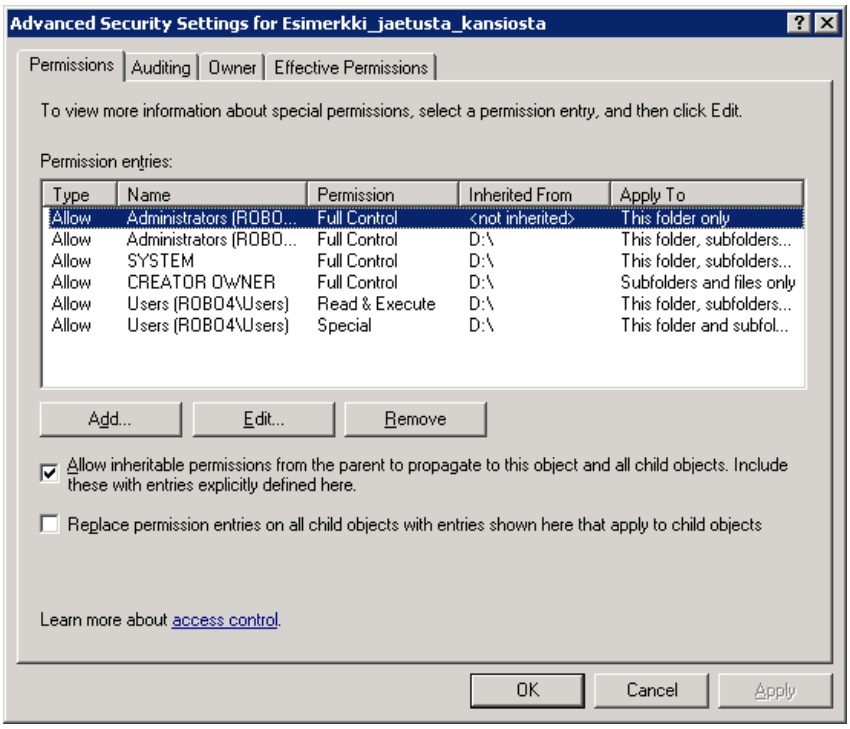


Kuva 5.#ACL_admin-ryhmälle annetaan kansioon täydet oikeudet (Full Control).

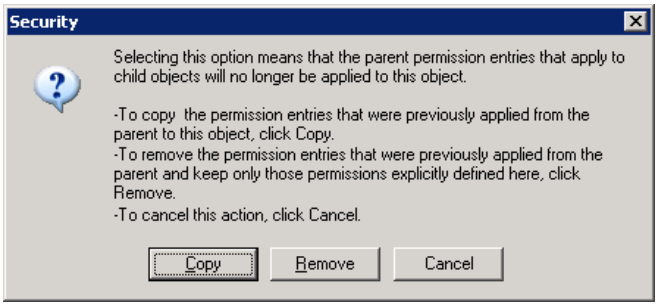
Täydet oikeudet tulee sallia vain järjestelmänvalvoja-tasoisille käyttäjille. Muille käyttäjille tätä oikeutta ei tule antaa, koska se sallii oikeuden myös muuttaa käyttöoikeuksia (Change Permissions) sekä ryöstää omistajuus (Take Ownership).



Kuva 6. Vasemmalla Modify-oikeus tarkemmalle tasolla ja oikealla Full Control-oikeuden tarkemmat käyttöoikeudet, huomaa kolme eroa näissä oikeuksissa.



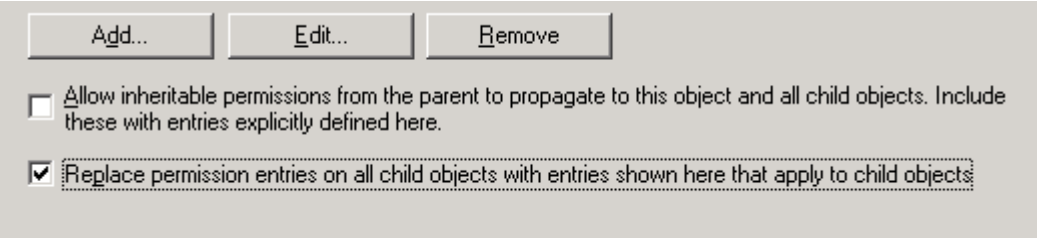
Kuva 7. Jaetusta resurssista pitää poistaa ensimmäisenä kansion periytymiseen liittyvä ominaisuus eli ottaa rasti pois kohdasta "Allow inheritable permissions from the parent to propagate to this object and all child objects. Include these with entries explicitly efined here. " Mikäli rastia ei poisteta, jaettu kansio perii oletuksena ylemmältä tasolta käyttöoikeudet, jolloin niiden muuttuminen muuttaa myös tämän kansion käyttöoikeuksia.



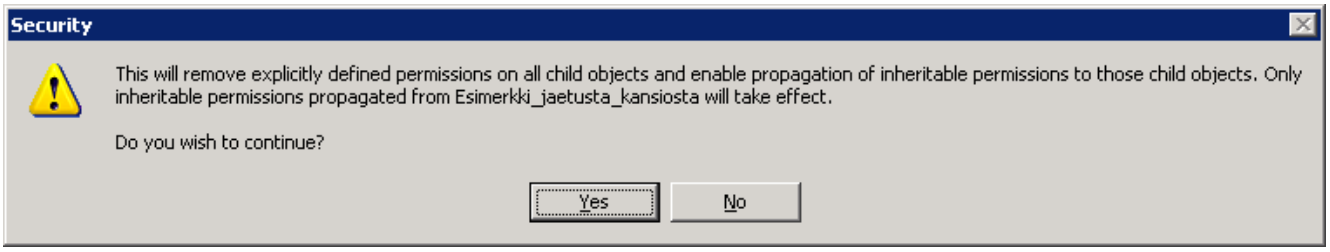
Kuva 8. Kun perintä poistetaan, voit jättää oletuksena olevat käyttöoikeudet voimaan valinnalla Copy tai poistaa kaikki oikeudet valinnalla Remove.

Oletuksena käyttöoikeudet tulevat voimaan valittuun kansiotasoon ja kaikkiin sen alaisiin kansioihin ja tiedostoihin, mikäli niiden perintäoikeuksia ei ole muutettu oletuksista.

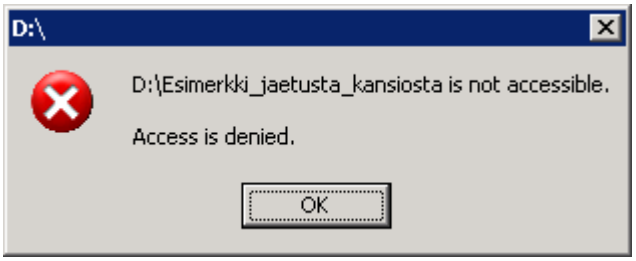
Mikäli on olemassa epäilys siitä, että alikansioiden käyttöoikeudet ovat muuttuneet, voit pakottaa voimaan valittuna olevan kansion käyttöoikeudet Advanced-painikkeen takaa löytyvällä rasti ruutuun kohdalla:



Kuva 9. Voit pakottaa voimaan oletuskansion käyttöoikeudet alempiin kansiotasoihin ja tiedostoihin laittamalla rastin kohtaan "Replace permissions on all child objects with entries shown here that apply to child objects".



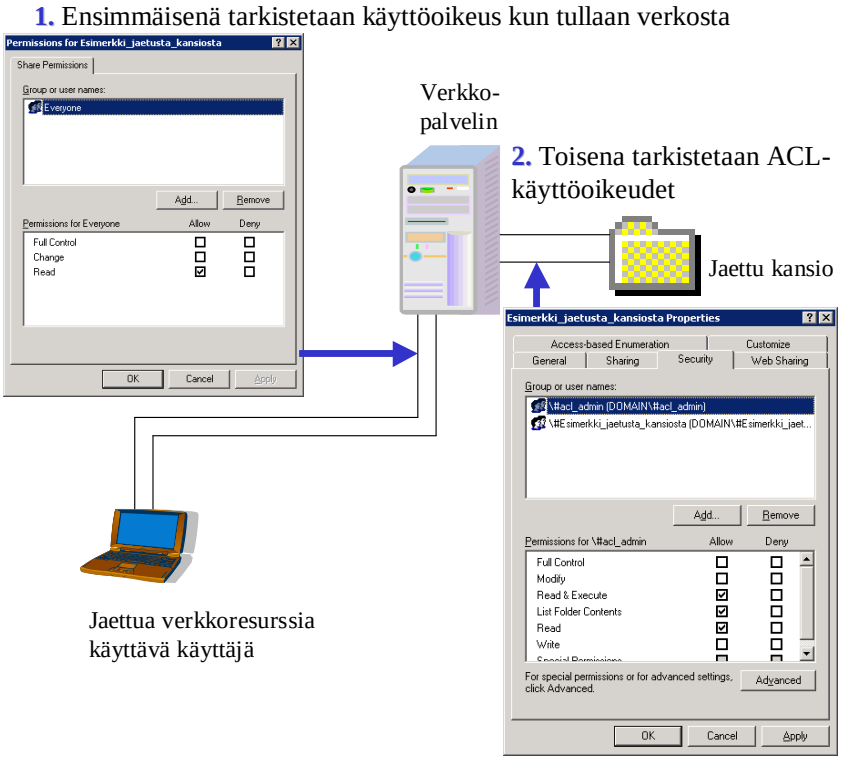
Kuva 10. Pakotus korvaa kaikki alikansioissa olevat olemassa olevat oikeudet, joten tämän takia tässä kohtaa tulee olla huolellinen.



Kuva 11. Riittämättömät käyttöoikeudet heijastuvat erilaisina virheilmoituksina.

4 KÄYTTÖOIKEUKSIEN MYÖNTÄMINEN JA NIIDEN TARKISTAMINEN

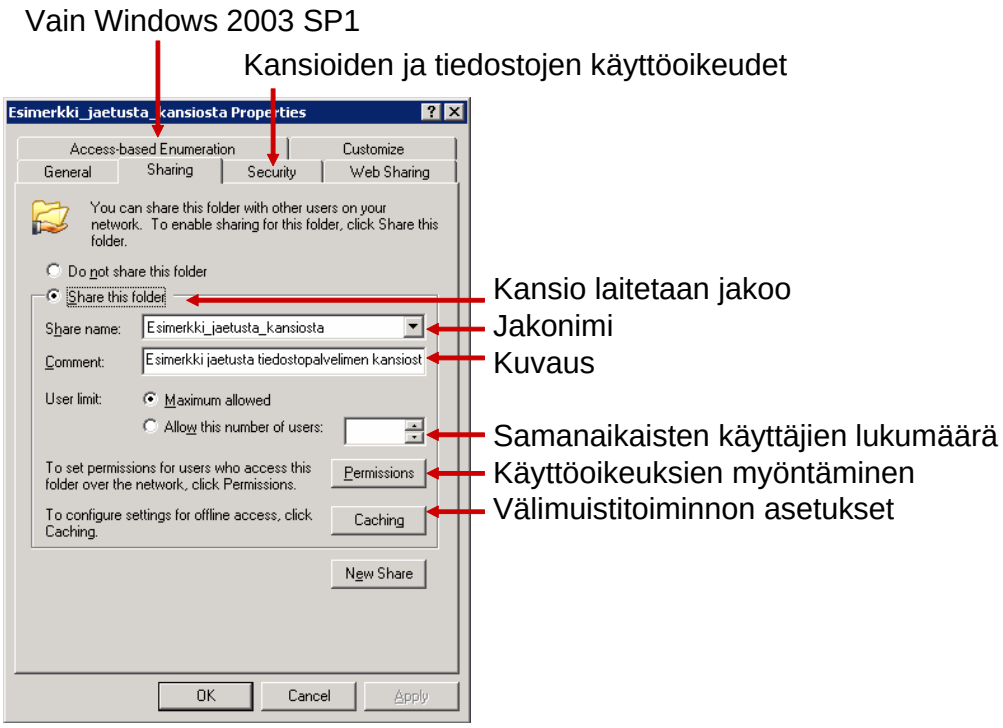
Kun käyttäjä siirtyy käyttämään verkossa olevaa resurssia, käyttöoikeuksien tarkistaminen tehdään kahdessa eri vaiheessa. Kun käyttäjä ottaa yhteyttä palvelimen jakamaan verkkoresurssiin, tarkistetaan ensimmäisenä käyttäjän käyttöoikeus verkon kautta jaettua resurssia käytettäessä (kuvan kohta 1). Tämä käyttöoikeus määritetään palvelimen kansion ominaisuuksien jakaminen-välilehdellä (kansio | Properties | Sharing).



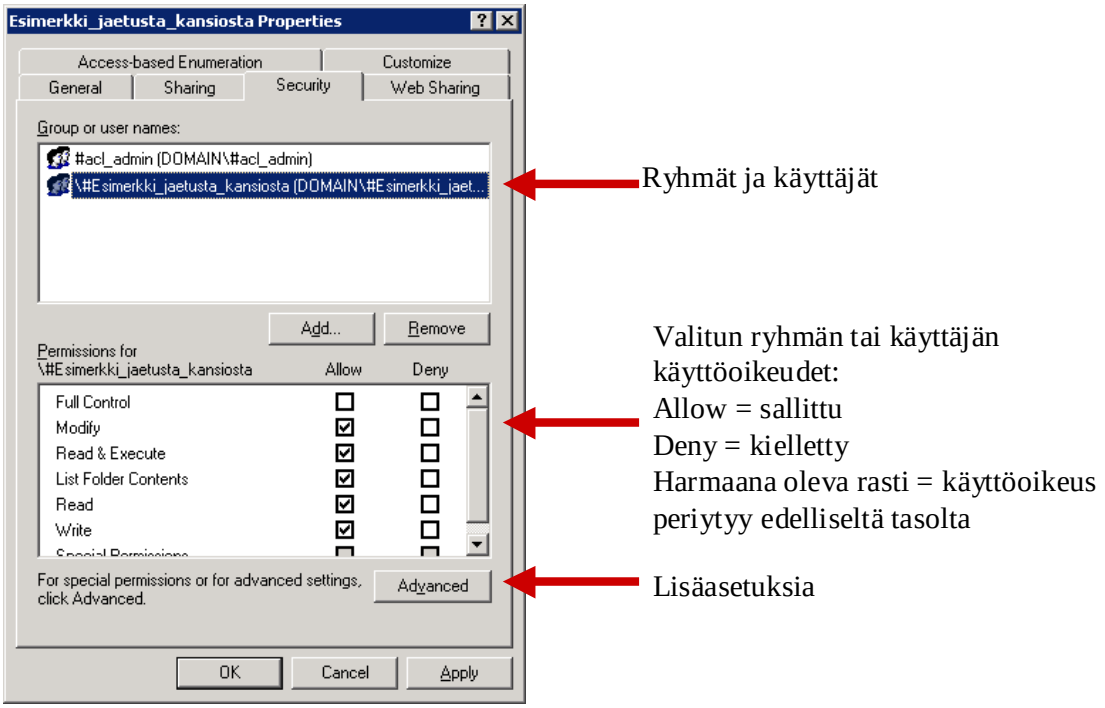
Kuva 12. Kun käyttäjä siirtyy jaettuun verkkokansioon omalta koneelta, ensimmäiseksi tarkistetaan käyttöoikeus verkon kautta (1) ja sen jälkeen mikäli tämä läpäistään, tarkistetaan seuraavana kansion/tiedoston käyttöoikeusdet (2).

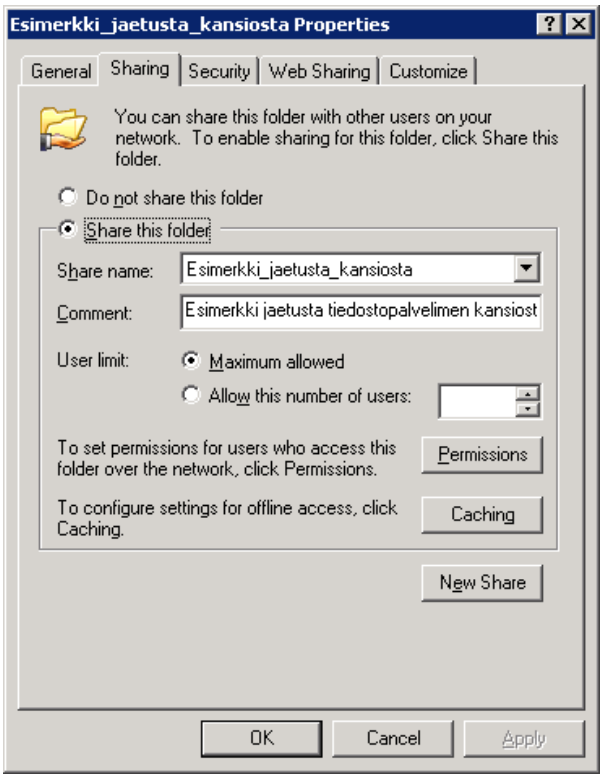
Kun jaettua verkkokansiota käytetään suoraan palvelimelta, voimassa ovat vain kansion/tiedoston käyttöoikeudet. Tällöin ei tarkisteta voimassa olevia verkon kautta olevia käyttöoikeuksia, koska jaettuun resurssiin lähestytään paikallisesti eikä verkon kautta.

Jaettujen resurssien käyttöoikeudet myönnetään siinä vaiheessa kun resurssi laitetaan jakoon. Tällöin pitää antaa kaksi erilaista käyttöoikeutta - oikeus resurssiin verkon kautta sitä käytettäessä - sekä kansio- ja tiedostotason käyttöoikeudet, jotka tarkistetaan sekä verkon kautta että paikallisesti resurssia käytettäessä.



Kuva 13. Sharing-ikkuna eli kansion jakamisen asetukset (yllä) ja Security-ikkuna eli suojausasetukset (alla).





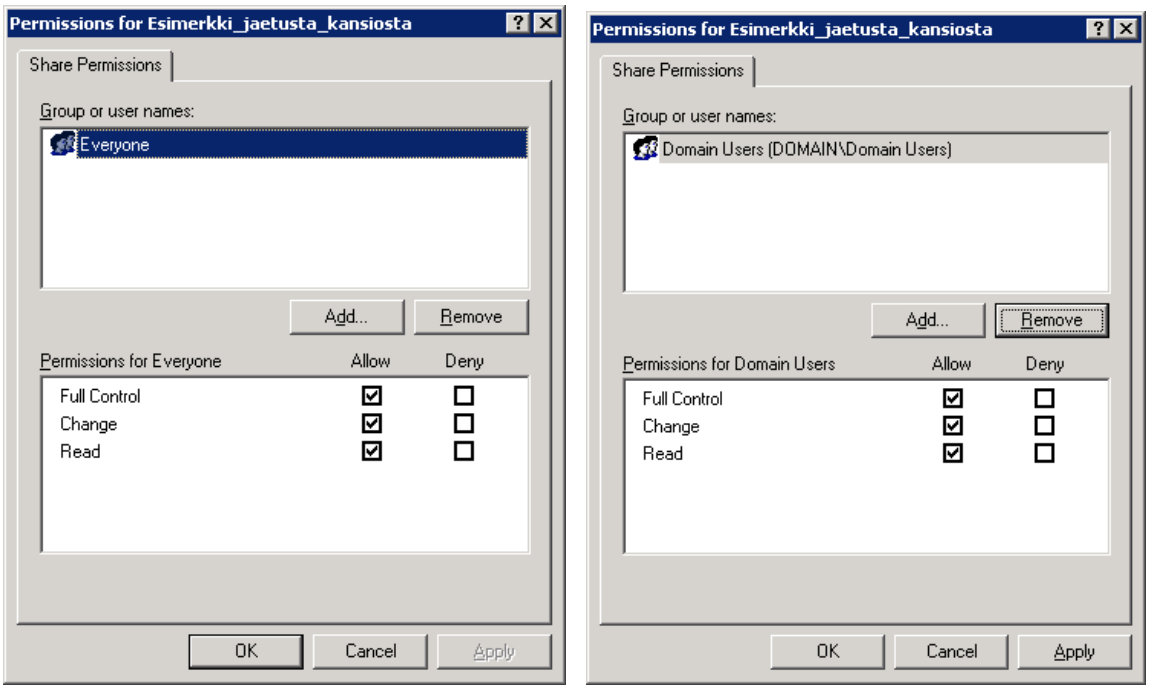
Kuva 14. Kansion jakamisen perusnäkymä, jaetut verkkokansiot tulee kommentoida huolellisesti.

a) Samanaikaisten käyttäjien rajoittaminen - user limit

Kansiota jaettaessa voit rajoittaa samanaikaisten käyttäjien lukumäärää. Huomaa, että Windows 2000/XP-työasemissa on 10 samanaikaisen verkkokäyttäjän raja, jota ei voi kiertää. Älä käytä tämän takia työasemaa tiedostojen jakamiseen vaan verkkopalvelinta. Samanaikaisten käyttäjien asetusta voit hyödyntää esimerkiksi sellaisten verkkopalvelimille asennettavien sovellusten jakamisessa, joiden lisensöintimalli pohjautuu samanaikaisten käyttäjien lukumäärään. Jos sovelluksella saa olla esimerkiksi maksimissaan 20 samanaikaista käyttäjää, valitse kohta ”Allow this number of users” sekä asetuksen arvoksi 20.

b) Käyttöoikeudet verkon kautta - permissions

Jaetun kansion asetusten ikkunan kohdasta ”Permissions” pääset hallitsemaan verkon kautta annettavia käyttöoikeuksia.



Kuva 15. Käyttöoikeudet verkon kautta resurssia käytettäessä – kaksi erilaista vaihtoehtoa.

Oletuksena Windows 2003-palvelinympäristössä kaikille käyttäjille (everyone) annetaan vain lukuoikeus (read). Mikäli käytössä on Windows 2000, oletuksena kaikille annetaan täydet oikeudet jaetun resurssin käyttämiseen verkon kautta.

Normaalisti tässä kohdassa voit toimia kolmella eri tavalla:

- jos tiedät tarkalleen, että tätä resurssia ei tule käyttämään kuin jokin tietty ryhmä, poista everyone Remove-painikkeella ja lisää se ryhmä, jolle tähän halutaan sallia käyttöoikeus. Anna ryhmälle Change-oikeus, mikäli ryhmän jäsenille pitää sallia kirjoitusoikeus.

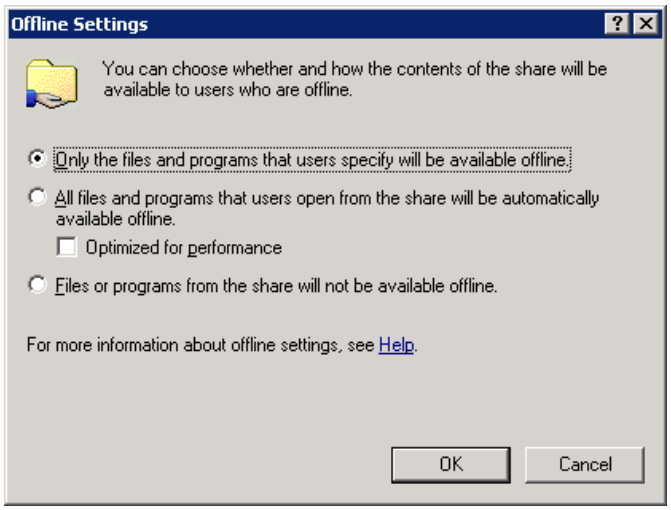
- mikäli jaettua kansiota tulee käyttämään useat erilaiset käyttäjät ja käyttäjäryhmät sekä käyttöoikeudet vaihtelevat ryhmittäin, muuta Everyone-ryhmälle Full Control eli täydet oikeudet. Huolehdi tämän jälkeen kansion käyttöoikeuksista, siten että jokainen ryhmä saa tarvitsemansa käyttöoikeudet.

- mikäli kaikki käyttäjät lisätään automaattisesti Domain Users-ryhmän jäseniksi, poistetaan everyone ja annetaan Domain Users-ryhmälle kaikki oikeudet. Tällöin Domain Users-ryhmän tulee sisältää myös järjestelmänvalvojien käyttämät suojausryhmät.

Näiden lisäksi voit tarvittaessa kaventaa käyttöoikeuksia deny- eli kielto-oikeudella. Huomaa, vaikka käyttäjällä tai käyttäjäryhmällä olisi täydet oikeudet jonkin toisen ryhmäjäsenyyden kautta, deny-oikeus ohittaa ne ja estää resurssin käyttämisen.

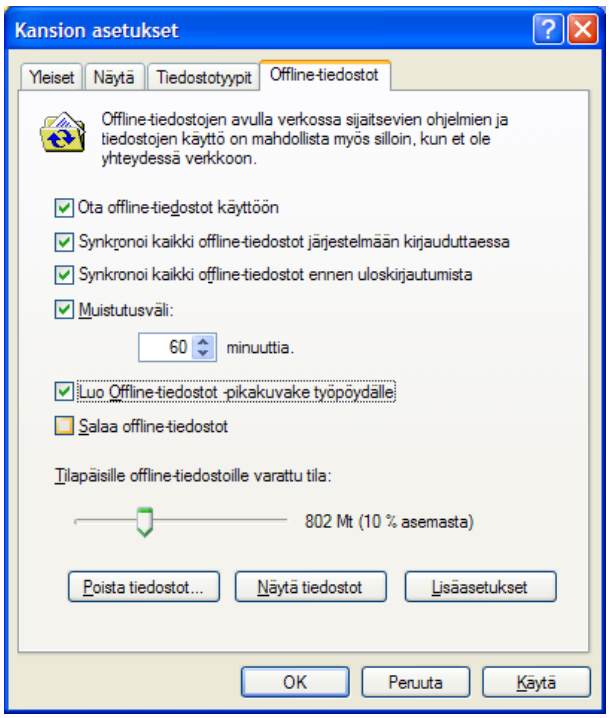
c) *Välimuistitoiminto - caching*

Valinnalla Caching voit määrittää, miten tiedostojen offline-käyttö on mahdollista. Offline-käyttö mahdollistaa jaetun verkkoresurssin käyttämisen esimerkiksi kannettavalla tietokoneella ilman, että kannettavalta tietokoneelta on minkäänlaista fyysistä verkkoyhteyttä palvelimelle. Tämä tapahtuu siten, että työasema synkronoi eli lataa palvelimelta offline-tilaa varten jaetussa resurssissa olevat tiedostot työaseman paikalliselle tietokoneelle.



Kuva 16. Verkkokansiolle laitetaan oletuksena päälle asetus, että käyttäjä voi itse halutessan valita välimuistiin sijoitettavat tiedostot ja kansiot. Valinnalla "All files and programs that users open from the share will be automatically available offline" kaikki mitä käyttäjä tästä verkkokansiosta avaa, ladataan automaattisesti käytettäväksi offline-tilassa. Alimmalla valinnalla "Files or programs from the share will not be available offline" estetään offline-käyttö kokonaan.

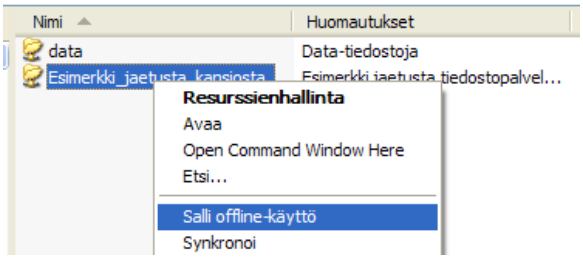
Offline-tiedostot pitää ottaa erikseen käyttöön työasemissa. Voit vaikuttaa siihen Windows 2000/XP-työasemassa resurssienhallinnan Työkalut-valikon | Kansion asetukset | Offline-tiedostot-kohdasta (Tools | Folder Options | Offline-files).



Kuva 17. Offline-tiedostojen asetukset, laita rasti ylimpään kohtaan sekä kaikkiin muihin alapuolelle paitsi ”Salaa offline-tiedostot”. Salaus pohjautuu Windowsin käyttämään EFS-salaukseen, jonka käyttöönotto pitää toteuttaa erillisenä käyttöönottoprojektina.

Offline-käytön suhteen pitää noudattaa organisaation voimassa olevaa käytäntöä sen hyödyntämisessä! Offline-tila voi muodostaa tietoturvariskin, mikäli tietokoneen kiintolevy ei ole salakirjoitettu, koska käyttäjän muulloin normaalisti palvelimella olevat tiedostot saattavat aueta murtautujalle offline-tilassa.

Tiedostot valitaan käytettäväksi offline-tilassa joko jaetun resurssien kohdassa ”Caching” olevien asetusten kautta automaattisesti tai käyttäjän toimesta napauttamalla hiiren oikealla painikkeella jaetun resurssin kohdalla ja valitsemalla ”Salli offline-käyttö” (Allow offline-use).

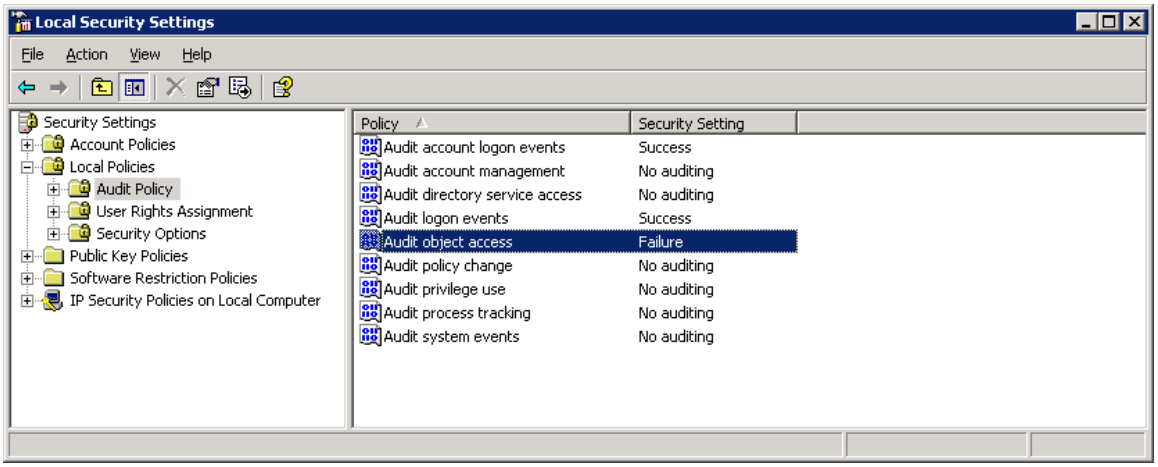


Kuva 18. Verkkoresurssi otetaan käyttöön offline-tilaan hiiren oikealla painikkeella jaetun kansion kohdalta valinnalla Salli offline-käyttö.

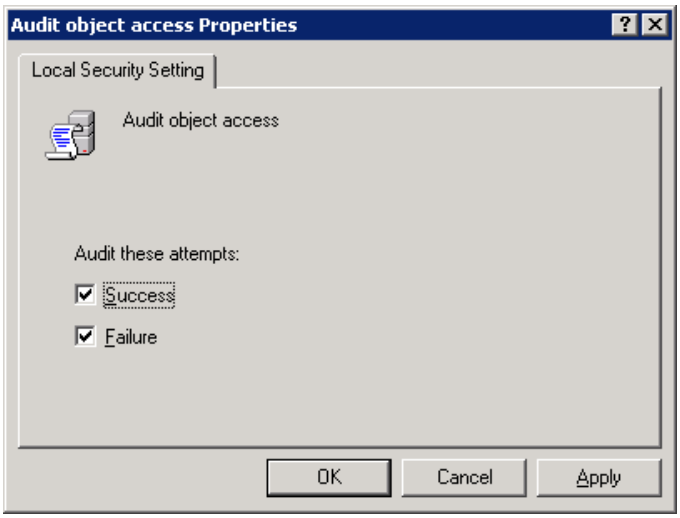
5 KÄYTTÖOIKEUKSIEN AUDITOINTI ELI VALVONTA

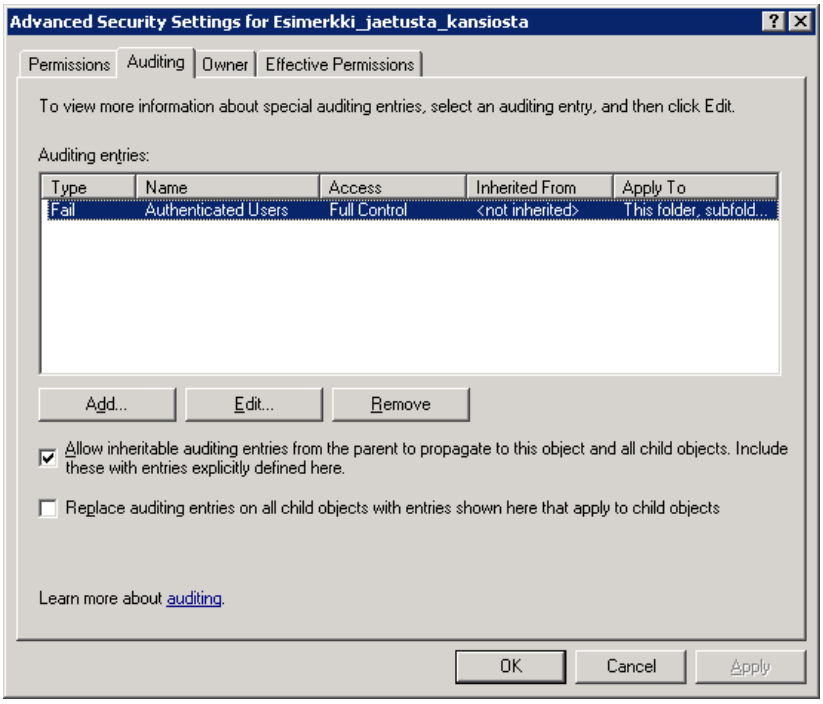
Hyvään tiedonhallintatapaan kuuluu käyttöoikeuksien valvonta. Tämä tarkoittaa sitä, että esimerkiksi organisaation kriittisimpien tietojen käyttöä voidaan valvoa sekä niiden käyttäjien osalta, joille tietojen käyttö on sallittu sekä etenkin sellaisten käyttöoikeusyritysten varalta, jolloin kyseisiin tietoihin yrittävällä taholla ei ole tarvittavaa käyttöoikeutta.

Auditoinnin käytöönotto on kaksivaiheinen prosessi. Ensimmäiseksi palvelimen tietoturva-asetuksista pitää sallia auditointi. Active Directory-ympäristössä voidaan käyttää myös Domain Security Policy ja Domain Controller Security Policy-asetuksia. Kun tämä asetus on voimassa, voidaan audtiointi laittaa päälle erikseen jokaiseen jaettuun resurssiin tarkemmalla tasolla käyttäjittäin/ryhmittäin sekä määrittää, mitä asioita halutaan valvoa.

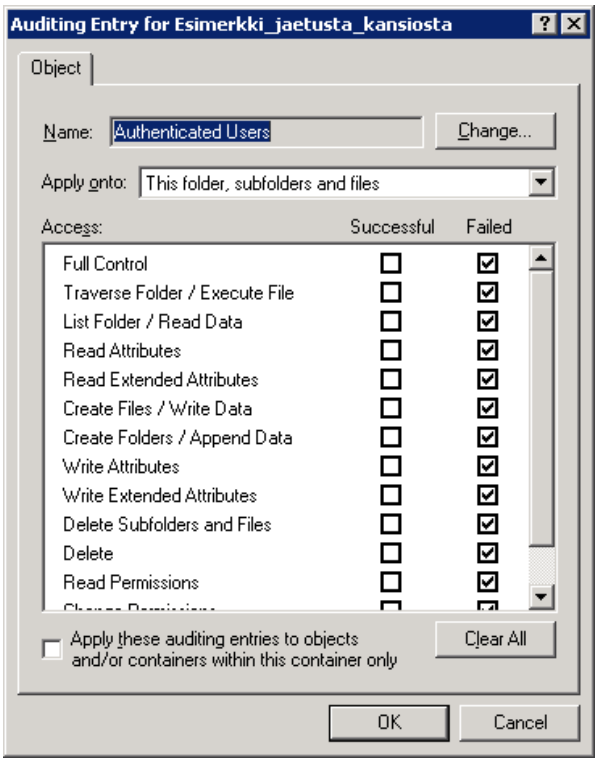


Kuva 19. Palvelimen paikallisista suojausasetuksista (secpol.msc-ohjelma) on laitettu päälle Audit object access-kohtaan Failure – tämä mahdollistaa jatkossa kaikkien epäonnistuneiden käyttöyritysten lokittamisen tapahtumienvalvonta-ohjelman (event viewer) suojaus-välilehdelle (security). Mikäli myös sallittua käyttöä halutaan valvoa, määritetään myös success-asetus voimaan samaan paikkaan (kuva alla).

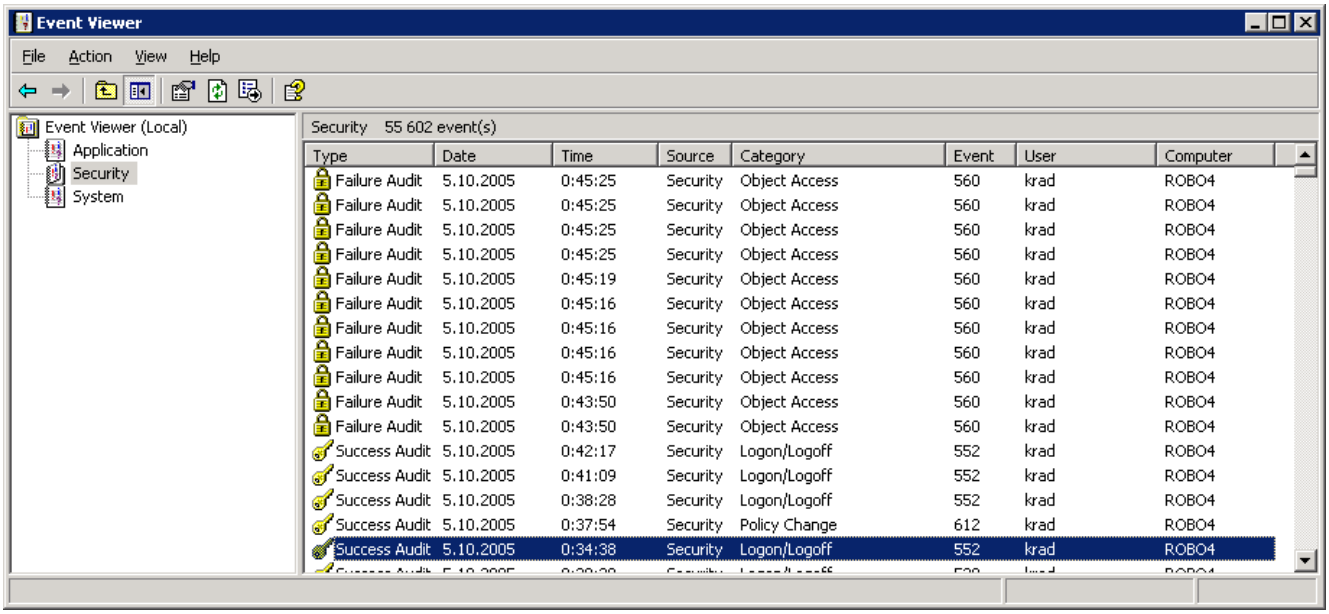




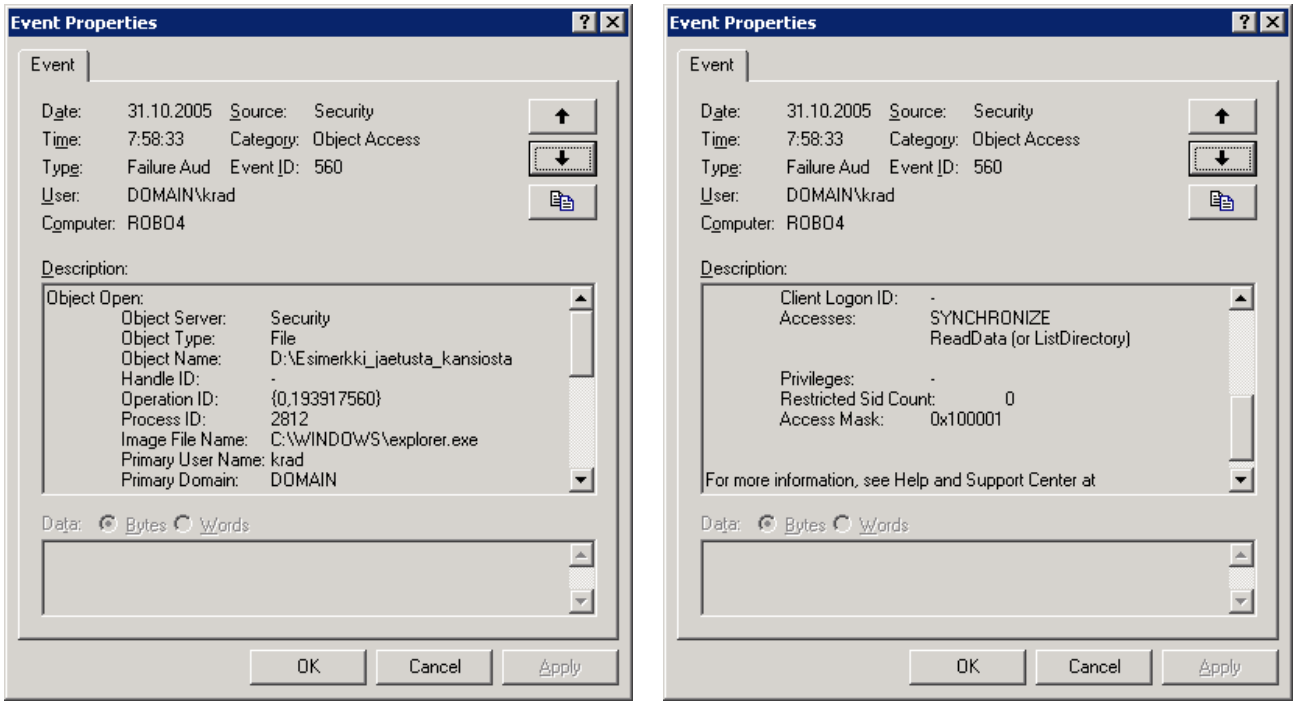
Kuva 20. Kansion suojaus-ominaisuuksista laitetaan auditing-välilehdeltä päälle authenticated users-ryhmälle Full control eli kaikkien käyttöoikeuksien valvonta päälle koskien Fail-tyyppisiä eli epäonnistuneita käyttöoikeuksia.



Kuva 21. Mikäli valvonta halutaan ulottaa myös sallittuihin asioihin, laitetaan rasti kohtaan Succesful-sarakkeen Full Control kohtaan tai rajataan valvottavia asioita tarkemmalla tasolla yksittäisillä rasti ruutuun valinnoilla.



Kuva 22. Kun auditointi on laitettu päälle, tuottaa se välittömästi kyseisen palvelimen tapahtumienvalvonnan suojaus-lokiin merkintöjä, valitettavasti lokien tulkitseminen on hieman hankalaa.



Kuva 23. Esimerkki tapahtumienvalvonnan auditointi-merkinnästä: krad-niminen käyttäjä on yrittänyt avata palvelimella sijaitsevaa d:\esimerkki_jaetusta_kansiosta-kansiota, mutta hänellä ei ole ollut siihen tarvittavaa käyttöoikeutta (Type: Failure Audit). Käyttäjä on yrittänyt avata tiedostoa (ReadData) tai avata kansiota (or ListDirectory).

6 WINDOWS 2003 SP1 ACCESS BASED ENUMERATION

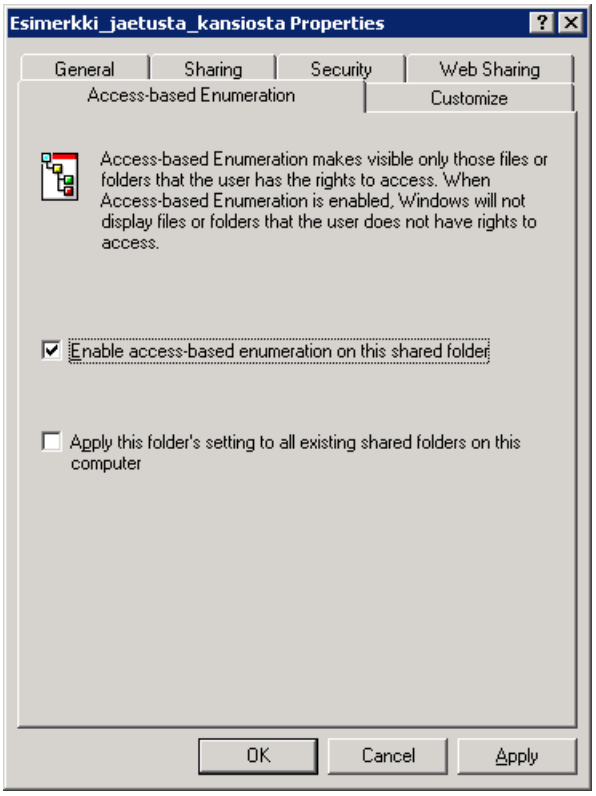
Microsoft Windows 2003 SP1-päivityskorjaus tuo mukanaan kokonaan uuden lisäominaisuuden käyttöoikeuksien hallintaan – ABE – Access Based Enumeration. Ominaisuus mahdollistaa sen, että jaetuista resursseista näytetään käyttäjälle vain ne käyttäjät ja kansiot, joihin hänellä on käyttöoikeus.

Aikaisemmissa Windows-versioissa on se ongelma, että ne näyttävät kaikki jaetut resurssit ja niissä olevat kansiot ja tiedostot, vaikka käyttäjällä ei olisi niihin varsinaista luku- tai suoritusoikeutta (read). Tämä lisää kiinnostavuutta tietoihin ja joissain tapauksissa pelkkien tiedostojen ja kansioiden nimistä voidaan päätellä asiakkaiden tai henkilöiden nimiä, joiden pitäisi säilyä luottamuksellisena.

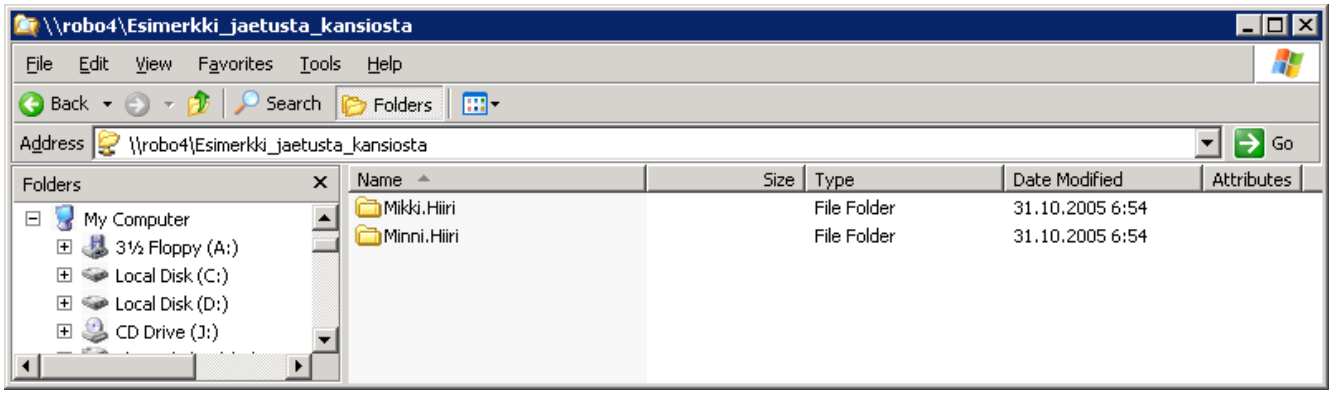
Lataa Windows 2003 SP1-versioon abe-apuohjelma osoitteesta:

http://www.microsoft.com/windowsserver2003/techinfo/overview/abe.mspx

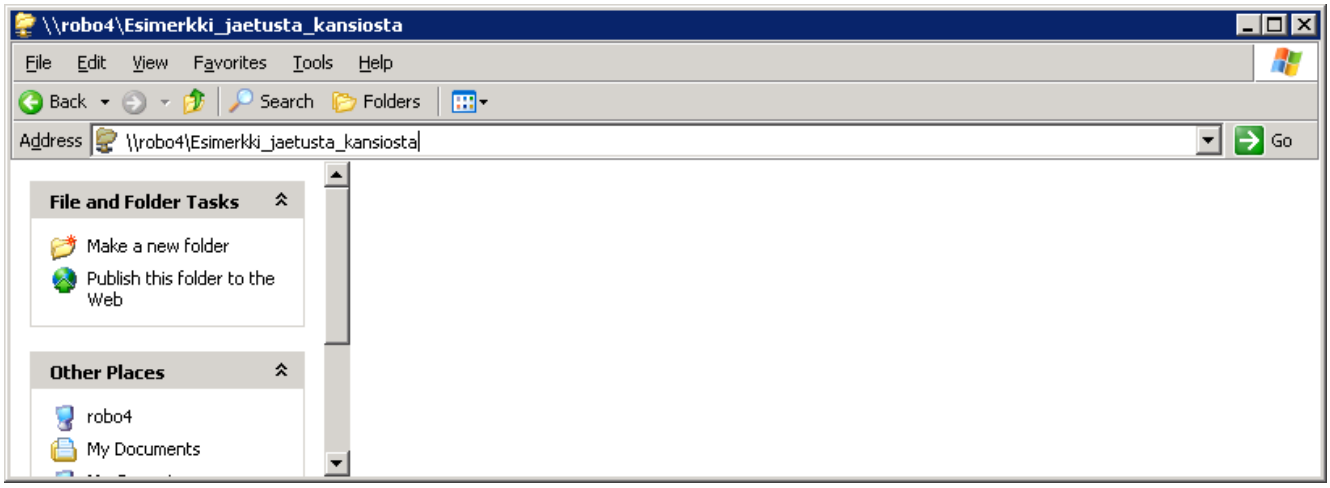
Asennettuasi ohjelman Windows 2003-palvelimelle saat esille jaetun kansion ominaisuuksista uuden välilehden Access-based Enumeration:



Kuva 24. Voit valita ABE:n päälle kansioittain tai kerralla kaikkiin jaettuna oleviin resursseihin.



Kuva 25. Lähtötilanne ennen kuin ABE on päällä.



Kuva 26. ABE on käytössä ja kirjautuneella käyttäjällä ei ole kansiossa oikeuksia, joten hän ei näe muiden käyttäjien sinne tallentamia tiedostoja tai kansioita.

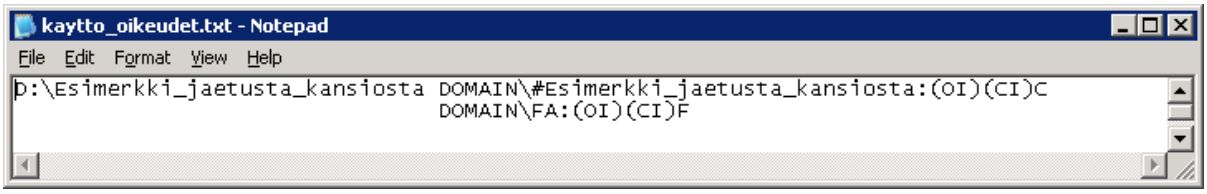
7 MUUTA HUOMIOITAVAA & PARHAITA KÄYTÄNTÖJÄ

a) Käyttöoikeuksien dokumentoiminen

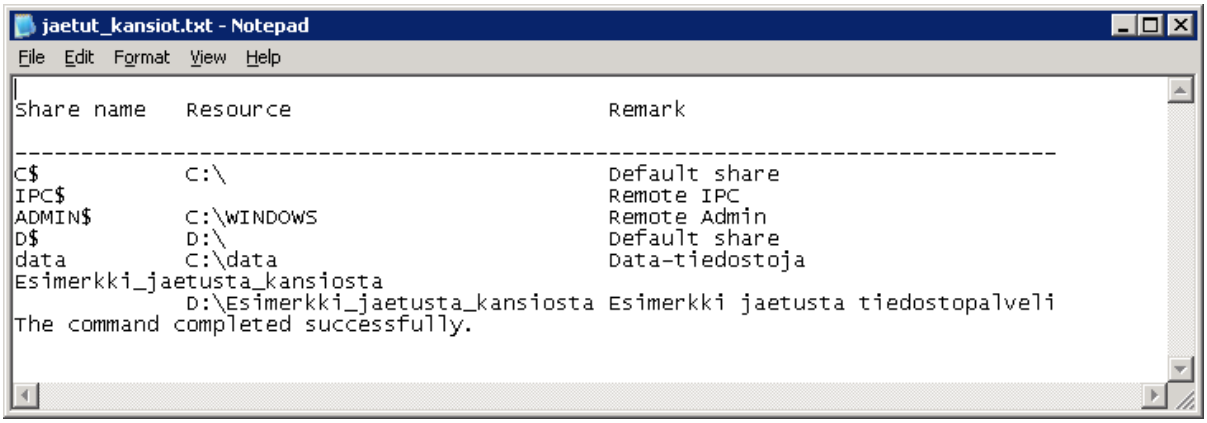
Ennen kuin teet laajemman käyttöoikeuksien muutoksen, varmista että sinulla on dokumentoituna olemassa olevat käyttöoikeudet ja jaetut verkkoresurssit. Voit tehdä tämän esimerkiksi palvelimella komentokehotetasolla ajamalla seuraavien kahden komennon tulokset tiedostoon:

net share > palvelimen_jakamat_kansiot.txt

cacls e:\esimerkki_jaetusta_kansiosta >kaytto_oikeudet.txt



Kuva 27. Cacls-komennolla voidaan tarkastella ja myös muuttaa komentokehotetasolla kansioiden ja tiedostojen käyttöoikeuksia.



Kuva 28. Net share-komento näyttää palvelimen jakamat kansiot.

Voit myös varmuuskopioida kansiorakenteen toiseen paikkaan ennen käyttöoikeuksien suurempaa muutosta. Tätä ei voi tehdä hiirellä eli graafisella käyttöliittymällä, koska silloin kansioiden/tiedostojen käyttöoikeudet eivät kopioidu mukana! Tee kopiointi esimerkiksi komentokehotetasolla xcopy-komennolla:

xcopy lähde kohde /S /E /C /O
- kopioi lähde-kansiosta kaikki kansiot ja tiedostot alikansioineen kohdekansioon, /o valitsin kopioi myös kansioiden käyttöoikeus- eli acl-tiedot.

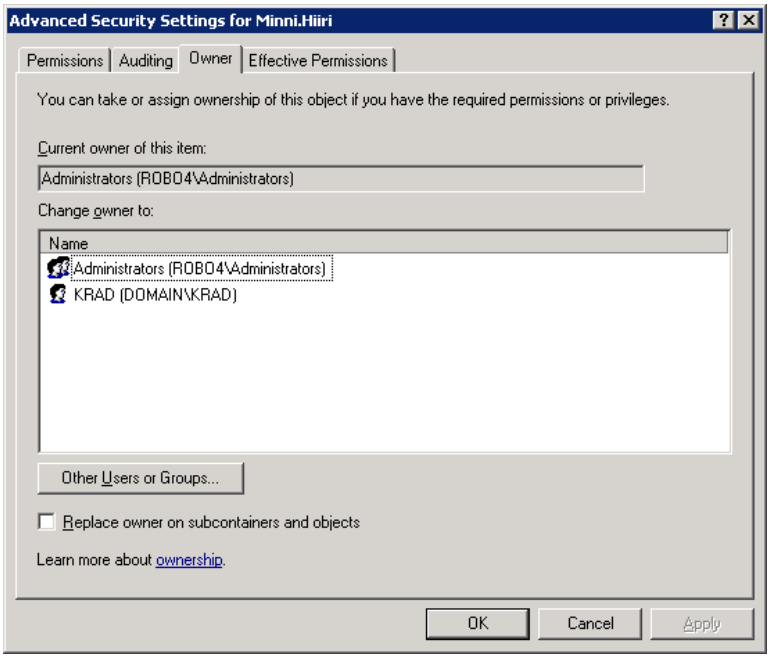
Voit myös käyttää palvelimen varmuuskopiointi-ohjelmaa (ntbackup) kansioiden ja tiedostojen varmistamiseen, se tallettaa varmuuskopioon käyttöoikeustiedot varmistettavista kansioista ja tiedostoista.

b) *Käyttöoikeuksien eli omistajuuden ryöstäminen*

Mikäli käyttöoikeuksien asettaminen ei ole tarkkaan hallittua ja ohjeistettua, saattaa syntyä sellainen tilanne, että palvelimella on kansio tai tiedostoja, joille ei ole olemassa enää omistajaa. Tällöin kukaan ei pääse käsittelemään kyseisiä tietoja. Tällöin ainoaksi keinoksi jää orpona olevien kansioiden / tiedostojen käyttöoikeuksien omistajuuden (ownership) kaappaaminen järjestelmänvalvojille, jotka voivat sen jälkeen antaa niille tarvittavat oikeudet.

Käyttöoikeus otetaan Security | Advanced | Owner-välilehdeltä valitsemalla käyttäjä tai ryhmä, kenelle omistajuus halutaan antaa ja valitsemalla Ok. Oletuksena omistajuus otetaan vain valittuna olevaan kansioon tai tiedostoon, mutta mikäli kaikki alikansiot ja tiedostot halutaan ottaa myös hallintaan, pitää laittaa rasti kohtaan ”Replace owner on subcontainers and objects”.

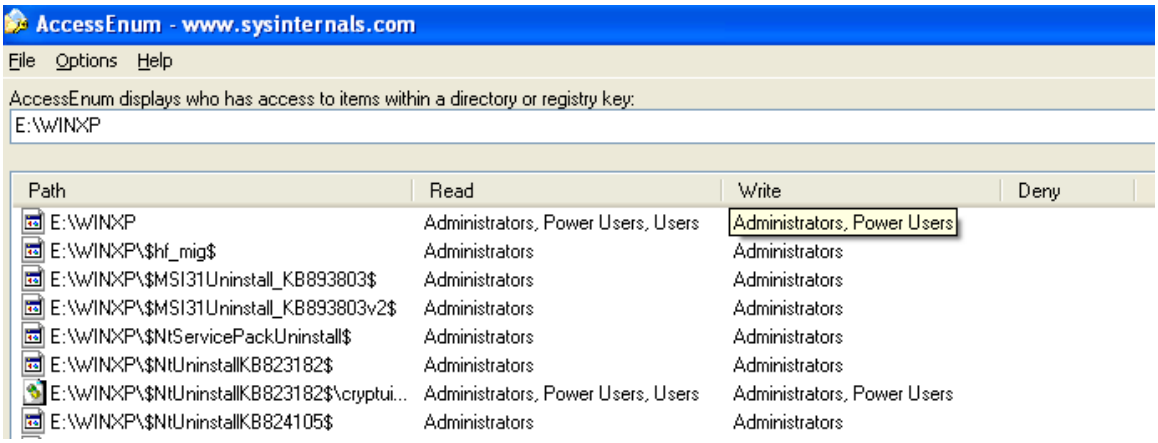
Huomaa, oletuksena tämä tarkoittaa sitä, että kaikki olemassa olevat aikaisemmat käyttöoikeudet häviävät ja vain valitulle käyttäjälle / ryhmälle tulevat täydet käyttöoikeudet. Usein tällaisissa tilanteissa kannattaa ensisijaisesti päästä kyseiseen kansiorakenteeseen kiinni sellaisen käyttäjän koneelta, jolla on kohteeseen täydet oikeudet ja tehdä hänen tunnuksen kautta tarvittavat muutokset.



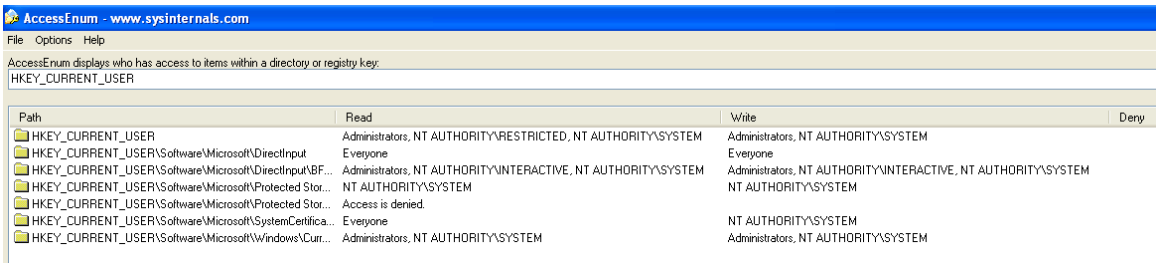
Kuva 29. Omistajuutta tarjotaan oletuksena administratros-ryhmälle tai kirjautuneena olevalle järjestelmänvalvojalle, voit antaa sen myös Other Users or Groups-valinnalla myös jollekin muulle taholle. Muista laittaa rasti kohtaan ”Replace owner on subcontainers and objects”.

c) Linkkejä:

Apuohjelma kansioiden käyttöoikeuksien tarkastamiseksi:
http://www.sysinternals.com/Utilities/AccessEnum.html



Kuva 30. Ohjelma näyttää määrittelemistäsi kansioista erikseen luku- ja kirjoitusoikeiden omaavat käyttäjät sekä ne, joilla on käyttö kokonaan kielletty (deny).



Kuva 31. Ohjelma osaa näyttä sama tiedot myös rekisteriavaimista.

Apuohjelma jaettujen verkkoresurssien käyttöoikeuksien tarkistamiseksi:
http://www.sysinternals.com/Utilities/ShareEnum.html

Windows 2000 Security Hardening Guide
http://www.microsoft.com/technet/security/prodtech/windows2000/win2khg/

Windows Server 2003 Security Guide
http://www.microsoft.com/technet/security/prodtech/windowsserver2003/w2003hg/