Am văzut cum se partajează folderele în rețea și cum li se permite clienţilor din rețea accesul la conținutul folderului. Întrebarea este dacă setarea drepturilor Share sunt suficientă pentru ca datele să fie securizate împotriva unei accesări neautorizate.

Unul dintre cele mai grele lucruri atunci când este vorba de protecția reţelei este protecția datelor. Datele sunt cele mai importante pentru o companie. Informațiile cu privire la planurile de viitor, contractele și finanțele pot duce o companie în pragul dezastrului, în cazul în care cineva neautorizat face rost de ele. Deja de ceva vreme, protecția datelor și a informațiilornu se mai referă doar la protecția împotriva atacurilor hackerilor externi, ci este îndreptată din ce în ce mai mult şi către protecția împotriva utilizatorilor interni. Utilizatorii legitimi care sunt nemulțumiți de salariu sau de poziție caută tot mai des în rețeaua companiei informații confidențiale pe care vor putea să le furnizeze mai apoi pe piața neagră și astfel să câștige niște bani în plus sau doar să facă rău companiei.

Din această cauză, dar și din alte motive, pentru partajarea documentelor în reţea nu este suficientă doar setarea drepturilor Share, ci ar trebui ca nivelul de securitate a datelor să fie ridicat şi mai mult prin configurarea permisiunilor și a interdicțiilor NTFS. Sistemul de fișiere NTFS este deja de mai mulți ani lider în acordarea permisiunilor și în interzicerea accesului la resursele partajate în cauză.

Când am vorbit despre partajarea documentelor și despre setarea drepturilor Share, de fapt, am vorbit despre autentificare. Prin urmare, toți utilizatorii cărora le sunt acordate drepturi Share vor putea să se autentifice la sistem și să acceseze folderul partajat și conținutul său. Însă, pentru ca aceiași utilizatori să poată să vizualizeze, să modifice sau să șteargă conținutul, trebuie să fie autorizaţi să facă acest lucru. Prin setarea permisiunilor NTFS pe resursele partajate, se setează de fapt autorizarea.

Spre deosebire de sistemul de fișiere FAT32, NTFS are liste de autorizare cunoscute ca Access Control Lists (ACL). ACL reprezintă o listă cu utilizatorii sau grupurile de utilizatori care au anumite drepturi

asupra unei resurse. Folosind lista ACL, puteți seta drepturile de acces la resursele locale pentru utilizatorii locali, dar doar combinația permisiunilor NTFS și a permisiunilor Sharins, explicate mai devreme, oferă drepturi efective pe care utilizatorii le vor avea asupra resurselor din rețea.

Setarea lui ACL, respectiv a drepturilor NTFS se face în tab-ul Security din meniul Properties al unei resurse. Daţi un clic dreapta pe un folder și selectați Properties. Daţi clic pe tab-ul Security și începeţi setările. Cu un clic pe butonul Edit, aveţi posibilitatea de a adăuga noi utilizatori sau grupuri de utilizatori, sau de a-i elimina pe cei adăugaţi, sau de a adăuga sau modifica drepturile pe care le au.

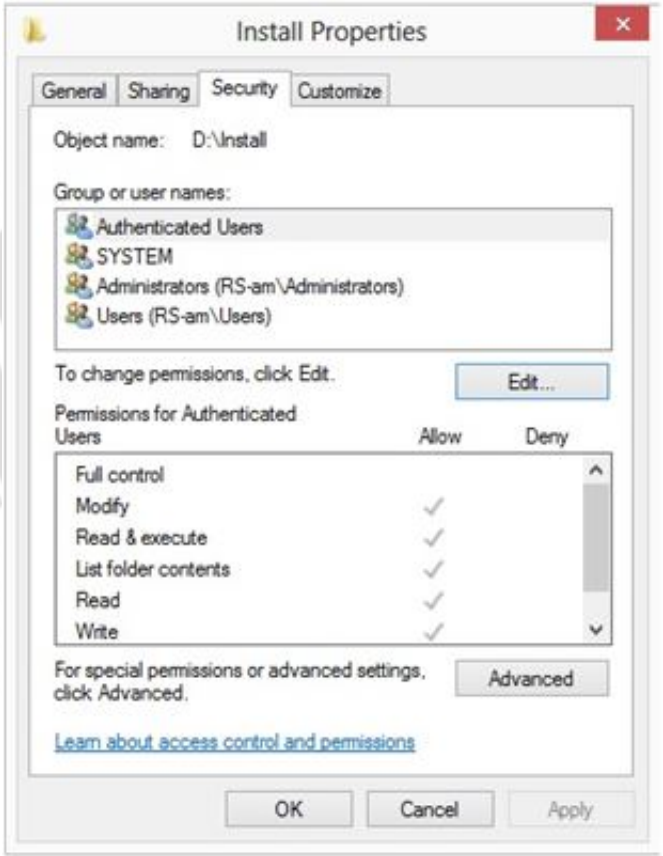

Figura 16.1 Setarea permisiunilor NTFS

Utilizatorilor li se pot acorda următoarele permisiuni:

Permisiune	Descriere
Full Control	Controlul complet asupra folderului şi al conţinutului
Modify	Posibilitatea de citire a conţinutului folderului şi de scriere în el
Read and Execute	Posibilitatea de citire a fişierelor şi de pornirea aplicaţiilor
Read	Este posibilă doar citirea fişierelor
Write	Este posibilă modificarea conţinutului folderului şi a fişierelor, precum şi ştergerea fişierelor
Special Permissions	O configurare specială

Tabel 16.1 Nivelurile permisiunilor

NTFS aduce încă un supliment important: moștenirea. Toate drepturile setate pe folder sunt moștenite de către fișierele care se află în acel folder. Acest lucru va economisi foarte mult din timpul necesar pentru setarea permisiunilor de acces, deoarece nu va trebui să setaţi drepturile pe fiecare fișier în parte, ci doar pe folderul în care se află toate fişierele. Moștenirea, în afară de fișiere, se aplică şi pe subfoldere.

Permisiunile NTFS se clasifică în două tipuri:

- Permisiuni Explicit- cele care sunt stabilite direct pe un obiect fișier sau folder.
- Permisiuni Inherited– cele care sunt moștenite de la obiectul în care se află fişierul.

Permisiunile Explicit sunt mai puternice decât cele Inherited. Prin urmare, dacă un fișier a moștenit interdicţia de acces pentru un anumit utilizator, dar are setată o permisiune directă de acces pentru același utilizator, utilizatorul respectiv va putea să acceseze fișierul. Atunci când adăugați permisiuni și interdicțiinoi în lista ACL, veți

observa că lângă câmpurile de introducere se află nişte permisiuni marcate cu gri ce nu se pot modifica. Acestea sunt permisiunile moștenite care nu pot fi modificate.

Deși moștenirea NTFS este un lucru foarte bun și vă poate ajuta foarte mult în accelerarea muncii, uneori vă poate provoca probleme, în special în situațiile în care creați o locație partajată. Folderul partajat va conține subfoldere pentru fiecare departament în parte. Prin urmare, va trebui să creați subfoldere care pot fi accesate doar de angajații dintr-un anumit departament, caz în care vi se pot anula drepturile moștenite din folderul părinte.

Pentru a întrerupe moștenirea, aveţi nevoie de fereastra Properties a ferestrei pe care doriți să o deconectați. Daţi clic pe tab-ul Security, apoi pe butonul Advanced. În partea de jos a ferestrei noi, aveți opțiunea Disable inheritance.

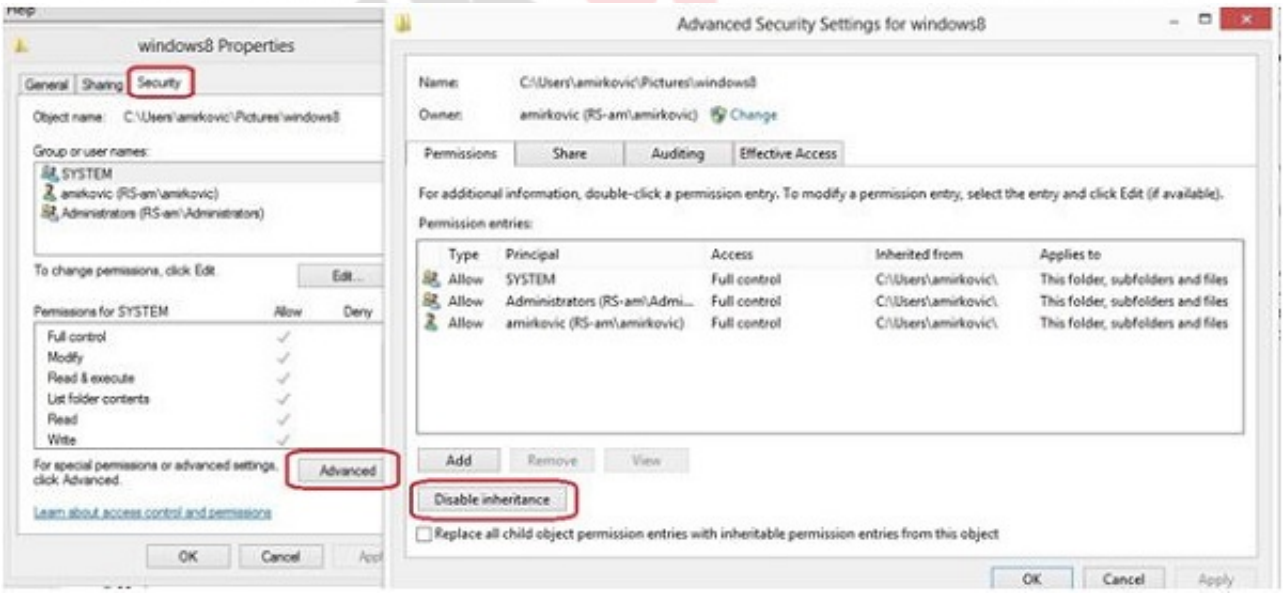

Figura 16.2 Setarea avansată a permisiunilor NTFS

Când daţi clic pe Disable inheritance, trebuie să determinaţi ce doriţi să faceţi cu drepturile deja moștenite. Cele două opțiuni oferite sunt:

- Convert inherited permissions into explicit permissions on this object – cu care veţi converti toate permisiunile moştenite în unele directe. Totul va rămâne aplicat pe folderul respectiv, doar că acum veţi avea dreptul să le modificaţi.

- Remove all inherited permissions from this object – prin care veţi şterge toate permisiunile moștenite şi veţi începe de la zero cu adăugarea și setarea drepturilor.

În procesul de copiere și mutare a fișierelor și a folderelor, se produc anumite schimbări în configurarea drepturilor NTFS.

- Când copiați un fișier sau un folder pe o altă locaţie, în cadrul aceleiași partiții NTFS, fișierele și folderele copiate vor moșteni setările folderului de destinație.
- Când copiați un fișier sau un folder pe o altă locație, într-o altă partiție NTFS, fișierele și folderele copiate vor moșteni setările folderului de destinație.
- Când copiați un fișier sau un folder pe o partiție care nu este NTFS, toate permisiunile sunt pierdute, deoarece sunt acceptate doar pe partiţiile NTFS.
- Când mutați un fișier sau un folder într-o altă locaţie, în cadrul aceleiași partiții NTFS, fișierele transferate îşi vor păstra toate setările și vor moşteni permisiunile suplimentare ale folderului de destinație.
- Când mutați un fișier sau un folder într-o altă locație, pe o altă partiție NTFS, fișierul mutat va moșteni permisiunile și interdicţiile folderului de destinație.
- Când mutați un fișier sau un folder pe o partiție care nu este NTFS, toate setările vor fi pierdute, deoarece acestea sunt acceptate doar pe partiții NTFS.

Permisiunile și restricțiile pentru accesul la anumite resurse le puteţi seta pe mai multe niveluri şi ele se pot referi la diferite metode de accesare. Am văzut că puteți seta permisiunile NTFS pentru a permite utilizatorilor să se autentifice și să lucreze cu fișiere. Permisiunile NTFS le puteţi atribui atât utilizatorilor individuali, cât și grupurilor de utilizatori, aşa că introducerea unui utilizator în mai multe grupuri de utilizatori v-ar putea îngreuna combinarea permisiunilor. De asemenea, utilizatorilor le puteţi acorda şi permisiuni Sharing, și să le permițeţi să se conecteze în rețea și să lucreze cu fișierele. Doar o combinație a tuturor acestor setări dă permisiunile efective și arată ce fel de drepturi va avea, în final, utilizatorul.

Unl dintre cele mai importante lucruri pe care trebuie să le aveţi mereu în vedere, atunci când este vorba de crearea permisiunilor eficiente pentru utilizatori, este acela că setarea Deny este întotdeauna mai puternică decât Allow.

În orice moment puteţi verifica ce drepturi efective are un anumit utilizator deschizând fereastra Properties a unui folder. Poziționaţi-vă pe tab-ul Security, daţi clic pe Advanced și poziţionaţi-vă pe tab-ul Effective Permissions. Selectați utilizatorul și veți obține o listă cu permisiunile și interdicțiile valide pentru acesta.

EFS – Encripted File System

Setarea permisiunilor NTFS și a permisiunilor Sharing este un mod excelent de a preveni accesul utilizatorilor neautorizați la documente. Însă, hackerii vor găsi întodeauna o cale de a ocoli aceste interdicții. Vor obţine numele de utilizator și parola unui utilizator autorizat sau vor accesa documentele de pe un calculator care nu este Windows și vor folosi anumite aplicații pentru a evita interdicțiile.

EFS - Encripted File Systemeste un sistem pe care Microsoft îl oferă utilizatorilor ca opţiune de criptare a datelor. Criptarea sau codificarea a fost în trecut unul dintre cele mai importante instrumente pentru trimiterea mesajelor confidențiale de la o locație la alta și datorită

căruia nu era nevoie să vă faceți griji că cineva le va intercepta și le va citi.

Windows 8 vine cu sistemul EFS integrat în ediţiile Pro si Enterprise. EFS foloseşte o cheie unică pentru a cripta documentul și doar acea cheie se poate folosiulterior pentru decriptare. Când criptaţi datele, acestea devin imposibil de citit și utilizatorul care nu are cheia poate să vadă fişierul, dar nu-l poate citi și înțelege.

Pe lângă criptarea şi securizarea documentelor în acest fel, va trebui să aveţi în vedere şi de furnizarea cheii cu care sunt criptate documentele. Dacă rămâneţi fără cheie nu veţi putea să decriptaţi datele și să le utilizaţi, iar cel care intră în posesia cheii, va putea să facă orice doreşte cu ele.

Când începeţi cu criptarea datelor, fiţi atenţi la următoarele:

- Nu păstraţi cheia EFS pe același calculator pe care îl utilizați pentru criptare.
- Când reinstalați Windows-ul, folosiţi cheia veche și pe noul sistem de operare.
- Dacă protecția EFS nu vă mai este necesară, decriptaţi datele înainte de a șterge cheia EFS.
- Ștergând un cont de utilizator, nu veţi putea accesa documentele până când nu acordaţi noului cont dreptul de a utiliza cheia EFS.

Pentru a cripta datele prin EFC, daţi clic dreapta pe folderul care trebuie criptat și selectați Properties (se va cripta întregul conținut al folderului). În tab-ul General, daţi clic pe butonul Advanced. Selectați opţiunea Encript content to secure data şi daţi clic pe OK.

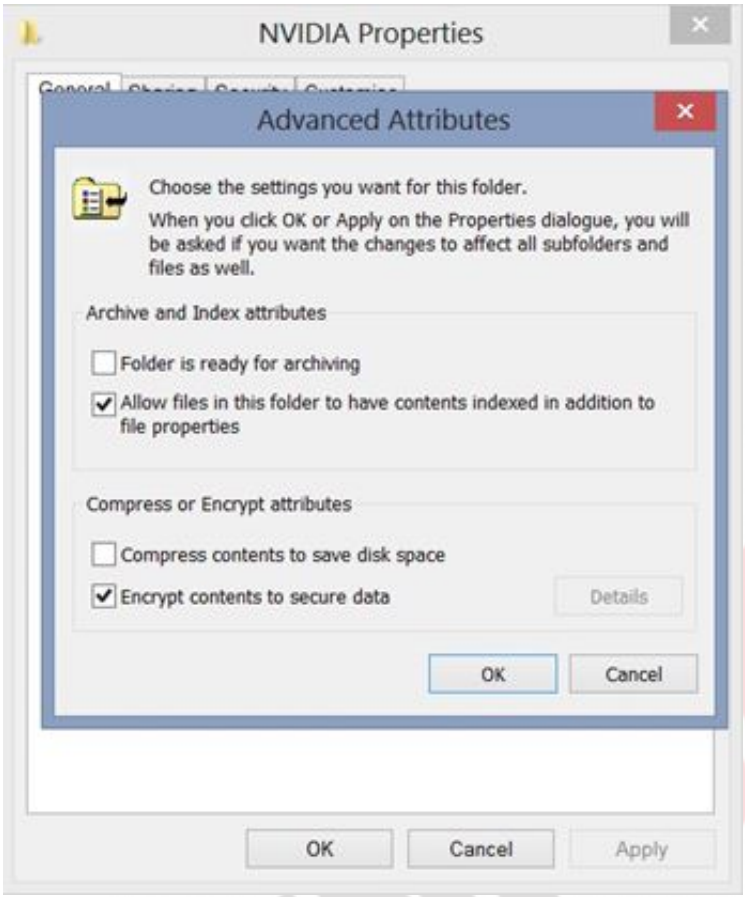

Figura 16.3 Setarea criptării

Când porniți prima oară procesul de criptare a documentelor, Windows creează automat un certificat cu o cheie de criptare și vă oferă posibilitatea de a face un backup al cheii. Backup-ul nu trebuie făcut în mod obligatoriu, deoarece certificatul şi cheie respectivă sunt setate automat pe calculator, dar în situațiile pe care le-am menționat mai sus, trebuie să aveţi o copie a cheii, de aceea recomandarea este să creaţi una imediat.

Ar trebui să efectuaţi şi o mică verificare pentru a vedea dacă datele au fost criptate cu succes:

- Folderul care este criptat ar trebui să se înverzească
- Opțiunea Encript Contents To Secure Data ar trebui să rămână bifată

- Niciun alt utilizator nu ar trebui să poată accesa datele

Cotele

Cotele (Disk Quotas)reprezintă un instrument foarte util atunci când este vorba de controlul cantităţii de date pe care utilizatorii o introduc pe hard disk-uri. În general se setează în mediul Client-Server, unde utilizatorii îşi păstrează datele într-o locație partajată central.

În condiţiile de mediului de acasă, cotele sunt utile în situațiile în care mai mulți utilizatori folosesc un singur calculator și îşi stochează datele doar pe acel calculator, doar pe o singură partiție sau doar pe un singur volum.

Cotele implicite sunt dezactivate și va trebui mai întâi să le activaţi și să le configuraţi pentru a le folosi.

1. Accesaţi instrumentul Disk Management prin apăsarea simultană a tastelor Win și X de pe tastatură
2. Daţi un clic dreapta pe drive, pe volum sau pe partiția pe care doriți să activați cotele şi selectaţi Properties
3. Daţi clic pe tab-ul Quota
4. Selectaţi Enable Quota Management

Configurarea cotelor trebuie de asemenea făcută, deoarece setările implicite cu siguranță nu vă vor oferi ceea ce vă doriţi.

1. Deny Disk Space To Users Exceeding Quota Limit - vă va permite să interziceţi salvarea datelor pentru utilizatorii care ajung la o anumită limită. În caz contrar, utilizatorii vor putea să continue să salveze, dar vor primi un avertisment că au depășit limita.
2. Limit Disk Space To - vă permite să limitaţi cantitatea de spațiu care este disponibilă utilizatorului.
3. Set Warning Level To – reprezintă configurarea alertei la un anumit nivel. Utilizatorii care ajung la acest nivel vor fi atenţionaţi

că le-a mai rămas puţin spațiu liber.

WIN8_16 - Windows 8

1. Autentificare pentru accesul la foldere şi la conţintul lor se setează prin adăugarea pemisiunilor şi a interzicerilor într-unul dintre tab-urile meniului Properties al folderului cu pricina. Care este acesta?

- ◯ a) General
- ◯ b) Security
- ◯ c) Share
- ◯ d) Advanced

2. Pentru ca un utilizator să fie autorizat să vizualizeze, să modifice sau să șteargă conținutul unui anumit folder, acesta trebuie să aibă setate:

- ◯ a) drepturile Share
- ◯ b) drepturile NTFS
- ◯ c) drepturile Advanced

3. Listele Access Control sunt disponibile pe unul dintre tipurile de sisteme de fişiere menţionate. Care este acesta?

- ◯ a) FAT16
- ◯ b) FAT32
- ◯ c) NTFS
- ◯ d) Ext2

4. Moştenirea este o opţiune disponibilă pe sistemul de fişiere:

- ◯ a) FAT16
- ◯ b) FAT32
- ◯ c) NTFS
- ◯ d) Ext2

5. În care dintre ediţiile sistemului de operare Windows 8 este disponibil EFS?

- ☐ a) Windows 8

- [ ] b) Windows 8 Pro
- [ ] c) Windows 8 Enterprise

6. Instrumentul care vă permite să limitaţi utilizarea hard disk-ului şi capacitatea care poate fi ocupată cu datele de utilizator este:

- ◯ a) Encripted File System
- ◯ b) Disk Quotas
- ◯ c) Disk Partitioning
- ◯ d) Encapsulated System

7. Când se utilizează EFS, se creează o cheie pentru criptarea datelor şi încă o cheie pentru decriptarea lor.

- ◯ a) adevărat
- ◯ b) fals

1. Autentificare pentru accesul la foldere şi la conţintul lor se setează prin adăugarea pemisiunilor şi a interzicerilor într-unul dintre tab-urile meniului Properties al folderului cu pricina. Care este acesta?

c

2. Pentru ca un utilizator să fie autorizat să vizualizeze, să modifice sau să șteargă conținutul unui anumit folder, acesta trebuie să aibă setate:

b

3. Listele Access Control sunt disponibile pe unul dintre tipurile de sisteme de fişiere menţionate. Care este acesta?

c

4. Moştenirea este o opţiune disponibilă pe sistemul de fişiere:

c

5. În care dintre ediţiile sistemului de operare Windows 8 este disponibil EFS?

b, c

6. Instrumentul care vă permite să limitaţi utilizarea hard disk-ului şi capacitatea care poate fi ocupată cu datele de utilizator este:

b

7. Când se utilizează EFS, se creează o cheie pentru criptarea datelor şi încă o cheie pentru decriptarea lor.

b