Gestionarea drepturilor de acces la fisiere si dosare in SO (Windows, Linux)

Indicații teoretice

Un cont de utilizator determină cum interacționați cu PC-ul și cum îl personalizați. De exemplu, contul dvs. determină ce aplicații, fișiere și foldere puteți să utilizați, ce modificări puteți să faceți la PC și care sunt preferințele dvs. personale, cum ar fi aspectul ecranului Start, fundalul pentru desktop sau economizorul de ecran. În cazul în care creați conturi separate pentru alte persoane, ele nu trebuie să partajeze aceleași setări, ceea ce înseamnă că puteți să restricționați accesul la inboxul de e-mail, la lucrul în rețelele sociale și la alte fișiere și să utilizați imagini de cont diferite, culori sau fundaluri pentru desktop pentru fiecare cont.

Există trei tipuri de conturi. Fiecare tip vă oferă un alt nivel de control asupra PC-ului:

- **Conturile de administrator** oferă control maxim asupra unui PC și ar trebui utilizate mai rar. Probabil că ați creat acest tip de cont atunci când ați utilizat pentru prima dată PC-ul.
- **Conturile standard** sunt destinate pentru lucrul de zi cu zi. În cazul în care configurați conturi pentru alte persoane de pe PC-ul dvs., este o idee bună să le oferiți conturi standard.
- **Conturile de copil** sunt utile pentru părinții care doresc să monitorizeze sau să seteze limite pentru modul în care copilul lor utilizează PC-ul, cu setările din Siguranța familiei din Windows. Pentru mai multe informații despre Siguranța familiei, consultați Configurați Siguranța familiei.

În plus față de alegerea unuia dintre aceste tipuri de conturi, puteți alege, de asemenea, o metodă de conectare pentru fiecare tip: persoanele se pot conecta la Windows cu un **cont Microsoft** sau cu un **cont local**.

Utilizatorii (atât de domeniu cît și locali), grupuri de utilizatori, și calculatoare (le vom numi pe toate entități) au identificatoare de securitate unice - SID. Cu ajutorul acestui identificator sistemul și "știe" entitatea. SID are o valoare unică în domeniu și se formează în timpul creării unui utilizator sau grup, sau atunci când calculatorul este înregistrat în domeniu.

Atunci când un utilizator la conectare introduce numele de utilizator și parola , sistemul de operare verifică dacă parola este corectă, iar în cazul în care parola este corectă, creează un token de acces pentru utilizator. Token-ul include SID și toate SID-urile grupurilor utilizatorului în care utilizatorul face parte.

Pentru obiectele care urmează să fie protejate (cum ar fi fișiere, foldere, registru Windows) se creează un descriptor de securitate. Cu el se asociază ACL(Access Control List - ACL), care conține informații despre modul în care subiecților le sunt date anumite drepturi de acces la obiect. Pentru a determina dacă să se acorde tipul solicitat de acces la obiect, sistemul de operare compară SID în token-ul de acces al subiectului cu SID, cuprins în ACL.

Permisiunile sunt sumate, iar **interdicția este o prioritate mai mare decât permisiunea**. De exemplu, în cazul în care utilizatorul are permisiunea de a citi dosarul, și în grupul din care face parte - de a scrie, ca urmare utilizatorul poate citi și scrie. În cazul în care utilizatorul are permisiunea de a citi, și grupul din care face parte, citirea este interzisă, utilizatorul nu poate citi fișierul.

Dacă vorbim despre fișiere și foldere, mecanismele de securitate din sistemele de fișiere sunt acceptate numai pe discuri cu sistem de fișiere NTFS. Sistemul de fișiere FAT (și varianta sa - FAT32) nu implică posibilitatea de a stoca ACL, asociat cu fișierul.

Politicile de securitate Windows sunt foarte eficiente în protejarea mașinilor Windows prin asigurarea accesului restricționat la utilizatori. Dacă politicile de securitate Windows nu sunt configurate corect, utilizatorii pot manipula ușor registrul, applet-urile panoului de control, și alte setări de sistem critice, ceea ce poate duce la blocarea sistemului. Prin urmare, configurarea în mod corespunzător a politicilor de securitate pentru Windows în fiecare mașină windows din rețea este foarte important.

Politica de securitate locală a unui sistem este un set de informații cu privire la securitatea al unui calculator local. Informațiile politicii de securitate locale include următoarele:

1. Domeniile de încredere pentru a autentifica încercări de conectare.
2. Care conturi de utilizator pot accesa sistemul și cum. De exemplu, interactiv, printr-o rețea, sau ca un serviciu.
3. Drepturile și privilegiile atribuite conturilor.
4. Politica de audit de securitate.

Sarcina

Pentru a efectua lucrarea va avea nevoie de două conturi - *cont_administrator* și *cont_utilizator*, care nu face parte din grupul de administratori. De asemenea, vom avea nevoie de o grupă (*cont_grupă*). Toate grupurile și conturile sunt de domeniu, astfel încât managementul se va efectua cu ajutorul **Active Directory Users and Computers**.

Lucrînd sub contul **administrator**, vom crea un nou folder(**Test**). În proprietățile sale, selectați fila **Security** (Figura 1). Puteți vizualiza doar autorizația existentă. Pentru a le modifica, trebuie să faceți clic pe Edit, ceea ce va permite de a modifica lista de control al accesului la dosar (Figura 2).

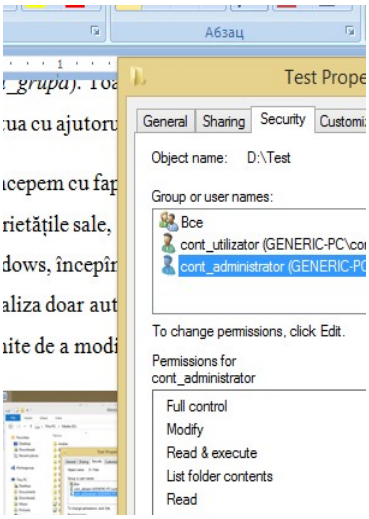

Fig. 1

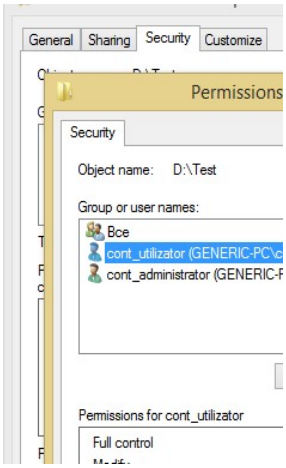

Fig. 2

Sarcina

Urmați etapele similare celor descrise mai sus. Asigurați-vă că utilizatorul cont_utilizator nu este în lista de acces la dosar, dar este membru al grupului Users. Efectuați comutarea utilizatorilor, conectați-vă la contul cont_utilizator, încercați să deschideți folderul și să creați un nou dosar în el. Care dintre aceste acțiuni au avut succes? De ce?

Efectuați din nou comutarea utilizatorilor. Sub contul de cont_administrator adauga la lista de utilizatori accesul la fișiere pentru contul cont_utilizator și dați-i permisiunea de a efectua modificări (Modify). Încercați din nou să creați folderul.

După cum s-a văzut, puteți adăuga utilizatori la lista de acces. Sub contul cont_administrator să ștergem grupul Users. Nu veți putea face acest lucru, va apărea avertismentul (Figura 3) că aceste permisiuni sunt moștenite de la obiectul părinte. În scopul de a anula moștenirea ar trebui în fila Security (Figura 1), să faceți clic pe Advanced. În fereastra apărută (Figura 4) se observă că este inclusă proprietatea Include inheritable permissions from this object's parent. Acest lucru înseamnă că obiectul moștenește ACL de la părinte, dar în ACL-ul propriu pot fi adăugate doar pentru permisiuni sau interdicții. Dacă faceți clic pe butonul Edit și a reseta această bifă, va apărea întrebarea, ce să se facă cu lista de moștenire - se poate face copiate (Copy), în ACL obiectului sau să fie eliminat (Eliminare). Cel mai des, pentru a nu se pierde setările, se efectuiază copiere, iar apoi lista este corectată.

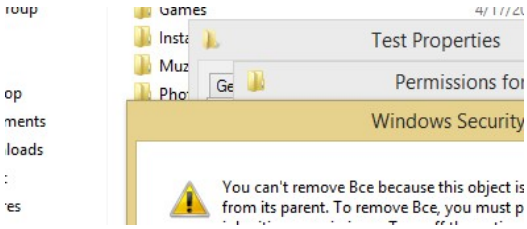

Fig. 3

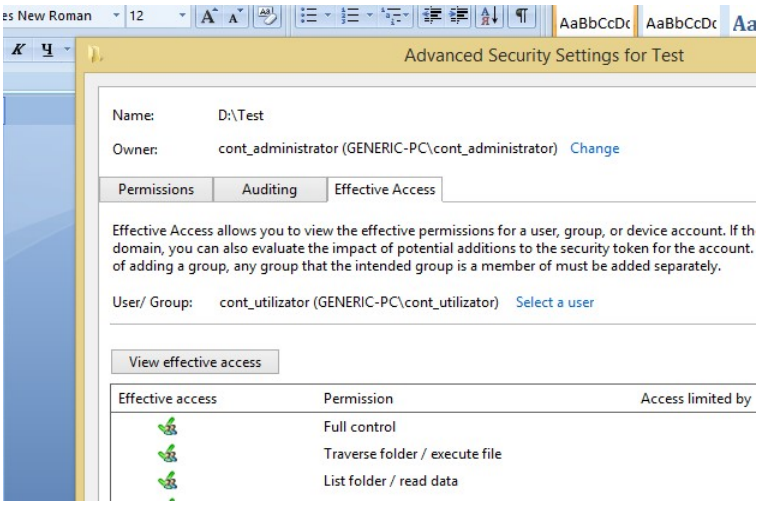

Fig. 4

Sarcina

Scoateți grupul de utilizatori din ACL pentru dosar.

Dacă editați permisiunile utilizatorului din fereastra de setări suplimentare de securitate, veți vedea o listă de permisiuni, care sunt diferite de ceea ce a fost anterior (Fig. 5).

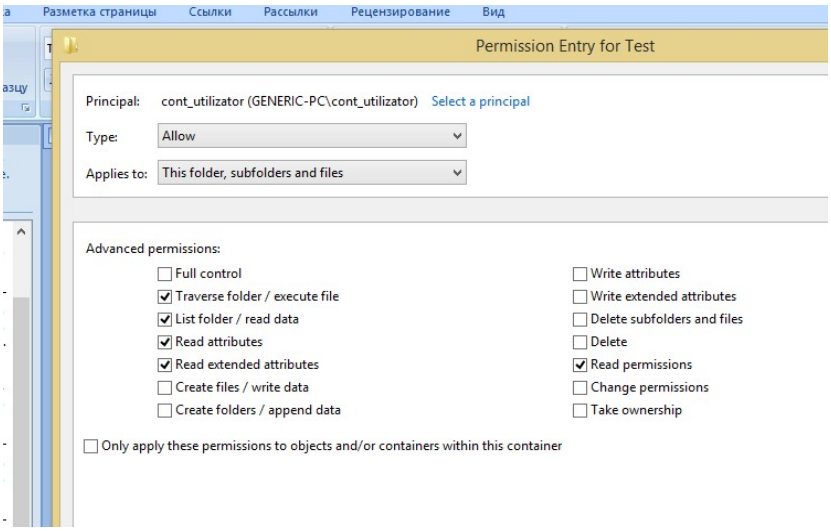

Fig. 5

Acestea sunt așa-numitele permisiuni speciale. Văzute anterior, permisiunile implicite (citire / read, scriere / write etc) constau din permisiuni speciale. Interacțiunile dintre ele sunt descrise în Fig. 6. Informații mai detaliate cu privire la acest subiect pot fi găsite, de exemplu, cu ajutorul sistemului Help din Windows.

Special Permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

Fig. 6

După cum s-a menționat mai devreme, în determinarea permisiunilor de acces se i-au în vedere activarea sau dezactivarea drepturile, atât pentru utilizator cît și pentru toate grupurile din care face parte. În scopul de a afla permisul valabil (efectiv), aveți posibilitatea să utilizați fila Effective Permissions (Fig. 4). Tastînd tasta Select, puteți selecta un utilizator sau grup pentru care va fi afișat efectiv persmisiunea.

Sarcina

Verificați dacă utilizatorul TestUser, la dosarul în care se desfășoară activitatea, a avut permisiunea de a modifica. Verificați rezoluția efectivă curentă.

Fără a termina sesiunea de utilizator, treceţi la sesiunea utilizatorului Administrator. Adauga la permisiunile folder-ului lista pentru interzicerea grupului TestGroup, orice acces (selectare Deny permisiunea de Control total). Introduceţi la membrii grupului TestGroup utilizatorul TestUser. Uitaţi-vă soluție eficientă pentru utilizatorul TestUser.

Comutaţi-vă la sesiune utilizatorului TestUser. Încercați să deschideți folderul și să creaţi un document. Log off sesiunea TestUser și conectați-vă din nou. Apoi, încercați să deschideți un folder și să creaţi un document. Cum putem explica acest rezultat (indiciu este la începutul descrierii lucrării de laborator)?

Acum, să luăm în considerare problemele legate de dreptul de proprietate asupra unui folder sau fișier. Utilizatorul care a creat fișierul sau folderul devine proprietarul acestuia. Posesorul curent al obiectului,îl puteți vedea dacă în setările de securitate avansate (Figura 4), selectați fila Owner.

Proprietarul fișierului poate schimba permisiunile la acest fișier, chiar dacă şi lui i se refuză accesul.

Procedura de schimbare a proprietarului unui fișier în Windows Server 2008 este diferit de ceea ce a fost în versiunile anterioare ale sistemului de operare. Anterior, administratorul sau un utilizator care are proprietate la un dosar (folder) chiar ar putea deveni proprietari de fișier. Mai mult decât atât, proprietarul poate fi fie un anumit utilizator sau un grup de administratori (Adminisrators) - un alt proprietar de grup nu a fost atribuit.

În Windows Server 2008 administratorul (sau un membru al grupului de administratori), poate deveni nu numai proprietarul, ci, de asemenea, să transfere dreptul de proprietate pentru un utilizator arbitrar sau de grup. Dar acest lucru este considerat ca privilegiat și nu este disponibil

pentru orice utilizator care are dreptul la folder. Fig. 7 arată că administratorul a făcut proprietarul folderului Test pe grupul TestGroup.

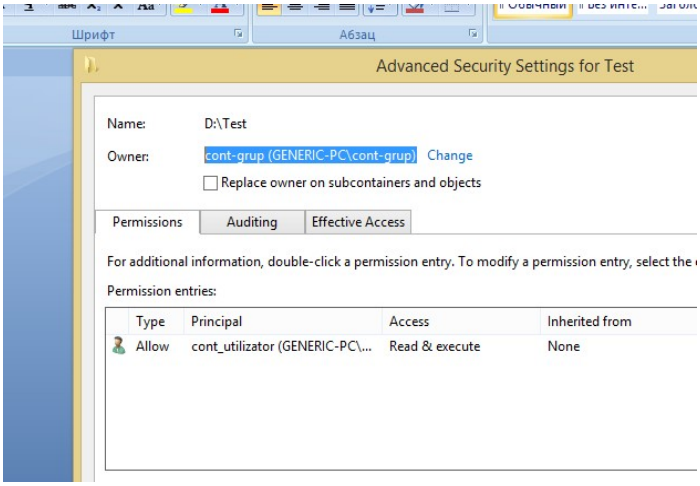

Fig. 7

Sarcina

Să petrecem transferul proprietății grupui TestGroup, care include utilizatorul TestUser. Accesînd acest cont, modificați permisiunile, astfel încât TestUser ar putea lucra cu dosarul.

Când se folosește un calculator care rulează Windows Server 2008 ca un server de fișiere , este important să se ia în considerare faptul că prevăzut în folderul partajat , separa permisiunile care reglementează accesul la rețea . Puteți să faceţi aceasta în Partajare tab Sharing (Fig. 9.8). În acest caz, accesul la rețea și permisiunea de a opera o permisiune de folder comune și NTFS. Rezultatul este cel mai restrictiv. De exemplu, în cazul în care directorul partajat este setat pentru "doar a citi" şi în permisiunile NTFS - "schimbare", apoi, în cele din urmă, utilizatorul care se conectează la rețea, poate doar citi fișiere. Și același utilizator de acces local primeste dreptul de a schimba (permisiunea la folderul partajat nu vor fi afectate).

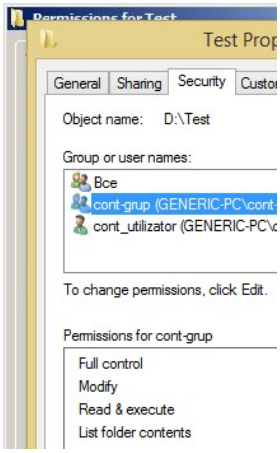
Test Prop
General
Sharing
Security
Object name: D:\Test
Group or user names:
Bce
cont_utilizator (GENERIC-PC\c
To change permissions, click Edit.
Permissions for cont-grup
Full control
Modify
Read & execute
List folder contents

Fig. 8