درس سیستم عامل شبکه

قسمت اول:

مشترک در سیستم عاملهای

Windows *2000*

Windows xp

Windows 2003

_ User account :

User name
- حداکثر ۲۰ کاراکتر
- کاراکترهایی که نباید استفاده شود " / \ [ ] : ; | = , + * ? < >

Password — حداکثر ۱۲۸ کاراکتر

_ Builtin users **(کاربران توکار):**

- Administrator — به صورت پیش فرض فعال است(enable)
- Guest — به صورت پیش فرض غیز فعال است(disable)

این دو user غیر قابل حذف هستند ولی میتوان آنها را تغییر نام غیر فعال کرد.

_گروه ها : Groups

_builtin groups : (گروه های توکار):

۱) Administrator
۲) Users
۳) Guests
۴) Back up operators
۵) Power users
۶) Remote desktop users

۱) گروه **administrator**:

اعضای این گروه دسترسی کامل و بدون محدودیت به منابع سیستم دارند.

مثلا
- **ایجاد ، تغییر و حذف user account**
- **ایجاد تغییرات گسترده در سیستم**
- **نصب برنامه های مختلف و دسترسی به همه فایلها**

۲)گروه users:

اعضای این گروه از ایجاد تغییرات گسترده چه به صورت تصادفی و چه عمدی منع می شوند.

بعضی مجوزها
- **اجرای بعضی برنامه های کاربردی**
- **استفاده از چاپگرهای محلی و چاپگرهای شبکه**
- **Start و shut down کردن کامپیوتر**

بعضی محدودیت ها
- **فایلها و پوشه ها را به اشتراک بگذارند**
- **نصب برنامه های کاربردی و چاپگر**

۳)گروه guest : مانند گروه users همان محدودیت ها را دارند و همچنین نمیتوانند تغییرات دایمی در محیط desktop خود ایجاد کنند.

۴)گروه backup operator:

- اعضای این گروه می توانند از فایلها backup تهیه کنند و یا backup گرفته شده را restore کنند بدون آنکه مجوزی برای استفاده از آن فایلها داشته باشند

- همچنین میتوانندshutdown و logon کنند

- ولی نمی توانند تنظیمات security را تغییر دهند.

۵)گروه **power users**:اعضای این گروه بیشتر مجوزهای گروه **administrators** را با برخی محدودیت ها دارند.

بعضی مجوزها
- ایجاد user account و تغییر یا حذف user accountهاییکه خودشان ایجاد کرده اند .
- خارج کردن userها از عضویت در گروه های power users, guests users.

بعضی محدودیتها
- گروه های administratorsوbackup operators را نمی توانند تغییر دهند.
- نمی توانند مالکیت فایل ها را تغییر دهند و آنها را به اشتراک بگذارند.
- Device driversها را نمی توانند loadیا unload کنند.

۶)گروه **remote desktop users**:اعضای این گروه می توانند از راه دور به کامپیوتر logon کنند.

گروه های خاص شناسایی:

گروه هایی هستند که اعضای آنها متغیر بوده و توسط کامپیوتر تعیین می شوند.

۱)گروه Anonymous logon: کاربرهای ناشناخته که دارای account نیستند.یعنی user nameو password ندارند.مثل کاربری که در اینترنت از یک web site دیدن میکند.

۲)گروه Authenticated users : کاربرهای شناخته شده که دارای account هستندیعنی user nameو password دارند.وقتی کاربری از طریق account به کامپیوتر logon میکند این کاربر عضو گروه authenticated users می شوند.

۳)گروه Dial up : کاربرانی که از طریق dial up connection به کامپیوتر logon میکنند عضو این گروه میشوند.

۴)گروه Every one : همه کاربران غیر از anonymous logon ها یعنی Guest و authenticated users .

۵)گروه Interactive :کاربرانی که از پشت کامپیوتر به کامپیوتر logon می کنند.

۶)گروه Network : کاربرانی که از طریق شبکه به کامپیوتر وصل می شوند.

سیاستهای پیکر بندی Account:

(configuring Account policies)

ACCOUNT POLICIES { PASSWORD POLICY
ACCOUNT LOCKOUT POLICY

Password policy {
1) Enforce password history
2) Maximum password age
3) Minimum password age
4) Minimum password length
5) password must meet complexity reuirement

۱) Enforce password history:

در این قسمت کاربررا مجبور می کنیم که از passwordهای قبلی در زمان تغییر password استفاده نکند.

صفر تاریخچه رمزها را نگهداری نمی کند Range :0 → 24

۲) maximum password age :

در این قسمت کاربر را مجبور می کنیم پس از گذشتن یک زمان مشخص password خود را تغییر دهد.

صفر یعنی Not expire Range : 0 → 999 days

۳) minimum password age :

در این قسمت مشخص می کنیم تا مقدار زمان مشخصی نگذرد کاربر نتواند password خود را تغییر دهد.

(نکته:مقدار minimum از مقدار maximum طول عمر باید کمتر باشد)

Range : 0 → 999 days

۴) minimum password length :

در این قسمت کمترین طولی را که یک کاربر می تواند برای password وارد کند مشخص می کنیم.

Range: 0 → 14 characters

صفر یعنی Account می تواند password نداشته باشد

۵) password must meet complexity requirement :

در این قسمت کاربر را مجبور میکنیم که password خود را به صورت پیچیده انتخاب کند.

یک رمز پیچیده باید حداقل سه تا از این چهار قسمت را داشته باشد

1)A→Z
2) a →z
3) 0→9
4) (*, ?, !, :, ...)

Account lockout policy
1)Account lockout threshold
2)Account lockout duration
3)Reset lockout counter after

۱) Account lockout threshold:

در این قسمت مشخص میکنیم که یک user چند بار می تواند password خود را اشتباه وارد کند و اگر موفق نشد password صحیح را وارد کند Account مربوط به آن user قفل شود.attempts 999 → 0 : ange

صفر یعنی Account هرگز قفل نشود

۲)Account lockout duration :

در این قسمت مدت زمان قفل شدن یک Account را مشخص میکنیم.

Range : 0 → 99999 minutes ≈69.4 days

۳)Reset lockout counter after:

در این قسمت مدت زمان لازم برای reset(صفر) شدن شمارنده تعداد دفعات وارد کردن اشتباه password توسط کاربر را مشخص می کنیم.

Range:1 → 99999 minutes

راههای دسترسی به Account policy روی یک client:

راه اول:

1)start/Run →type⇒GPEDIT.MSC ↙

2)local computer policy/computer configuration/windows setting/security setting/account policies

راه دوم:

۱)START/RUN→TYPE ⇒MMC ↙ (Microsoft Management Concole)

۲)در پنجره باز شده (یعنیconsole)روی منوی فایل و سپس روی Add/remove snap-in کلیک کنید

۳)در پنجره Add remove snap-in روی Add کلیک کنید.

۴)در پنجره Add stand alone snap in روی group policy و سپس روی Add کلیک کنید.

۵)در پنجره select group policy object روی finish کلیک کنید.

۶)در پنجره Add stand alone snap in روی close کلیک کنید.

۷) در پنجره Add remove snap-in روی OK کلیک کنید.

۸)در پنجره console به شاخه زیر بروید:

local computer policy/computer configuration/windows setting/security setting/account policies

:NTFS PERMISSION

خواص NTFS
- 1)File-level and Folder level security(NTFS PERMISSION)
- 2)Disk compression
- 3)Disk quatas
- 4)File encryption

NTFS folder permission
- 1)Read
- 2)Write
- 3)List folder contents
- 4)Read & execute
- 5)Modify
- 6)Full control

۱)READ:
- دیدن فایلها وزیر فولدرها در یک فولدر
- دیدن permissionها و صفات یک پوشه

READ
- List folder
- Read attributes
- Read permissions

۲)write:
- create files — ایجاد فایلهای جدید
- create folder — ایجاد subfolder های جدید
- write Attributes — تغییر صفات folder

۳) List Folder Contents: فقط میتواند محتویات folder را ببیند.

۴) READ & EXECUTE:
- Read
- List Folder Content
- Read & execute (فایلهای اجرایی را هم میتواند اجرا کند)

۵) Modify :
- Read
- Write
- Delete

Modify
- Read
- Write
- List folder contents
- Read & execute
- Modify

۶) full control : کنترل کامل

FULL CONTROL
- Read
- Write
- List Folder contents
- Read & execute
- Modify
- Full control → change permission
- Full control → take ownership

NTFS FILE PERMISSION
- Read
- Write
- Read & execute
- Modify
- Full control

1)READ
- Read data
- Read Attribute
- Read permission

2)WRITE
- Write data
- Append data
- Write attribute
- Read permission

3) Read & execute
- Execute file
- Read data
- Read Attribute
- Read permission

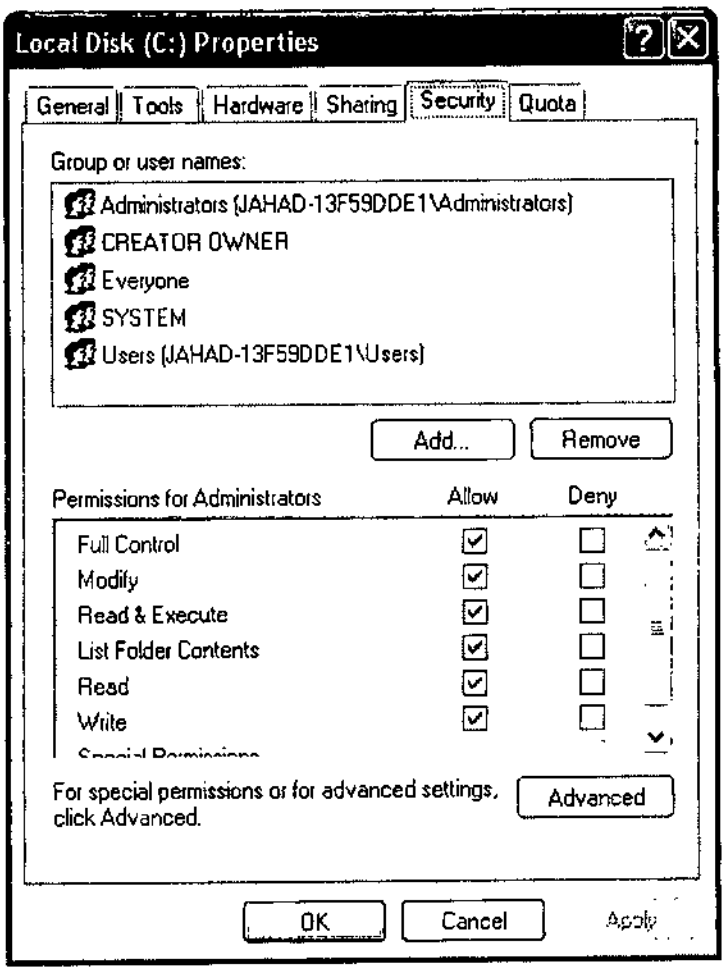
4) Modify:
- Read
- Write
- Delete

5)Full control→ از جمله→همه چیز Change permissions , take ownership

ACCESS CONTROL LIST (ACL) :

لیست کنترل دسترسی یا لیست **permission** های یک فایل یا پوشه

همان سرپوشه **security** در کادر محاوره ای **properties** یک فایل یا پوشه



Effective permissions : (۱) جمع شدن مجوزها (جمع مجوزهای گروه هایی که user عضو آن است یا مجوزهای خود user)

مجوزهای موثر

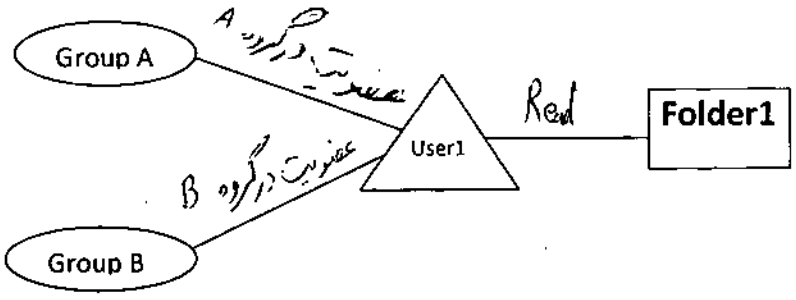
(۲) **overriding folder permission with file permission**

(۳) **overriding other permission with deny**

۱)جمع شدن مجوزها: مثال:

لیست کنترل دسترسی برای Folder1

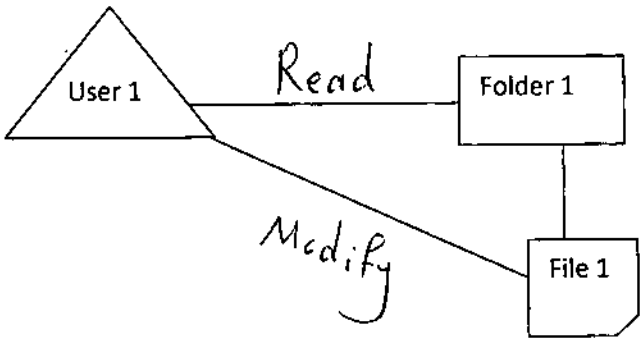
- user1→Read
- Group A→Write
- Group B→Modif



effective permission=MODIFY

۲) نوشته شدن file permissionها بر روی folder permission

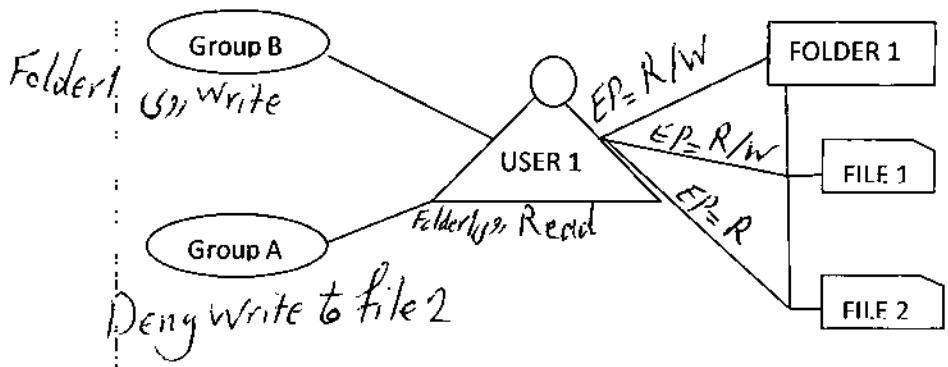
مثال



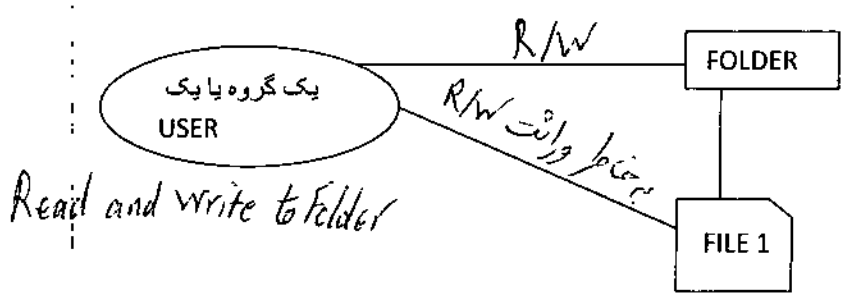
Effective permission=modify

۳) نوشته شدن denyها بر روی دیگر permissionها

برای مشخص کردن permission موثر باید permission های allow را با هم جمع کنیم و بعد deny ها را از ان کم کنیم



:NTFS PERMISSION IMHERITANCE

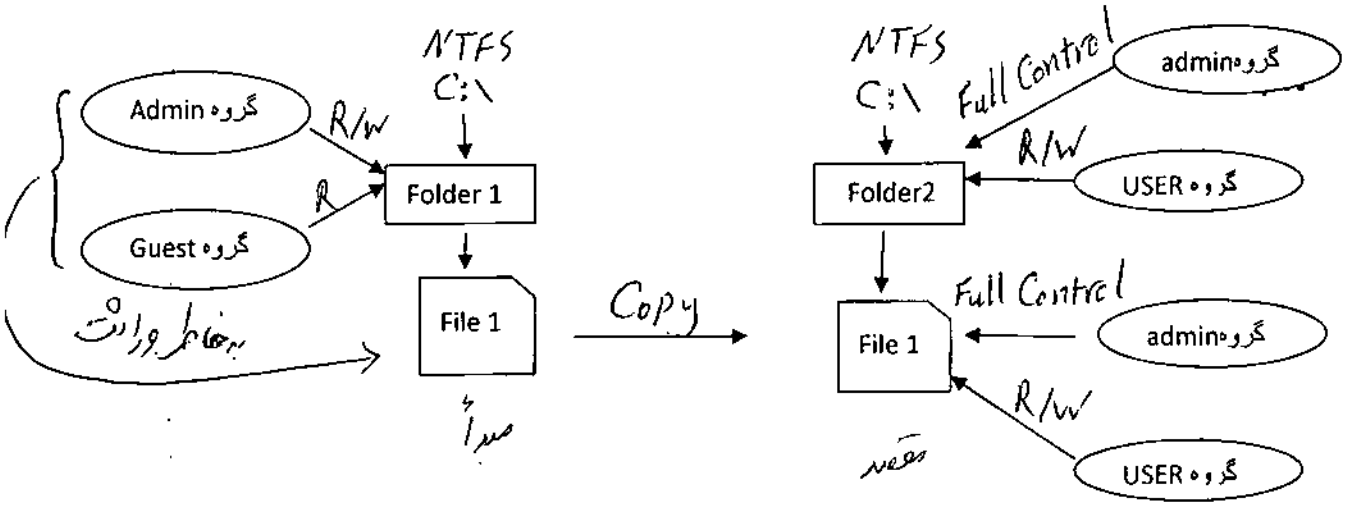


Special permission یا مجوزهای خاص

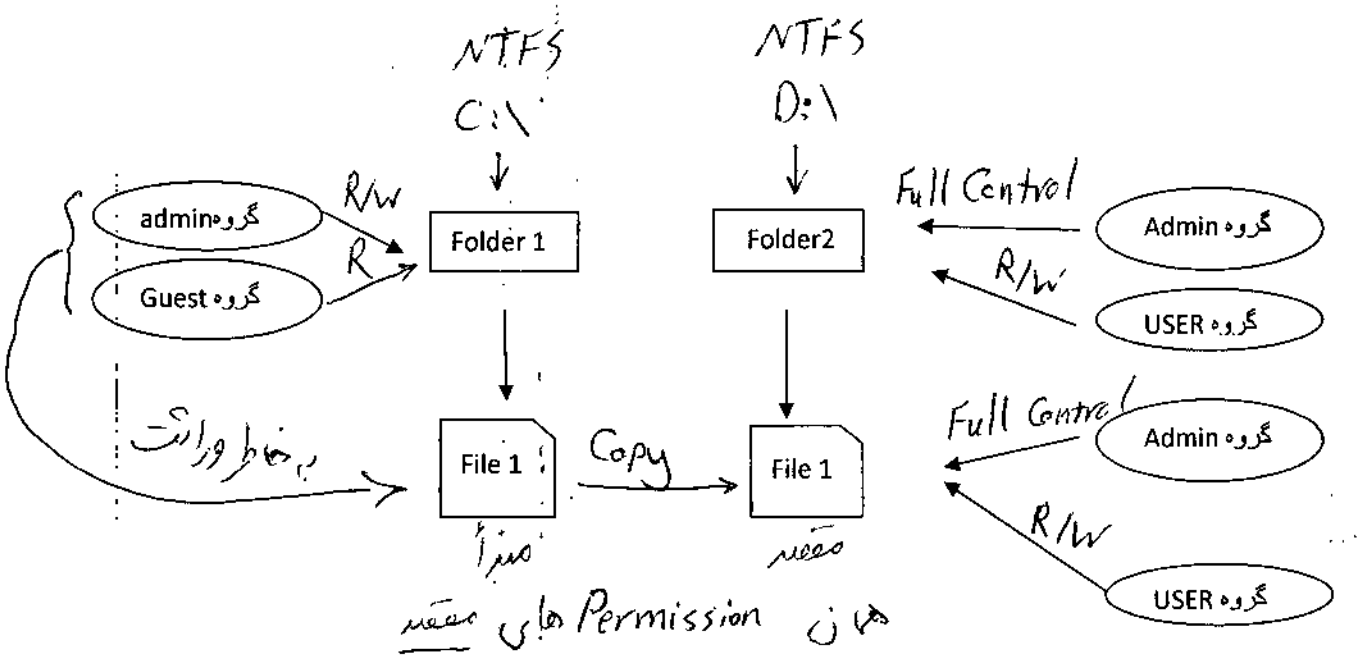
جزئی تر کردن permission ها

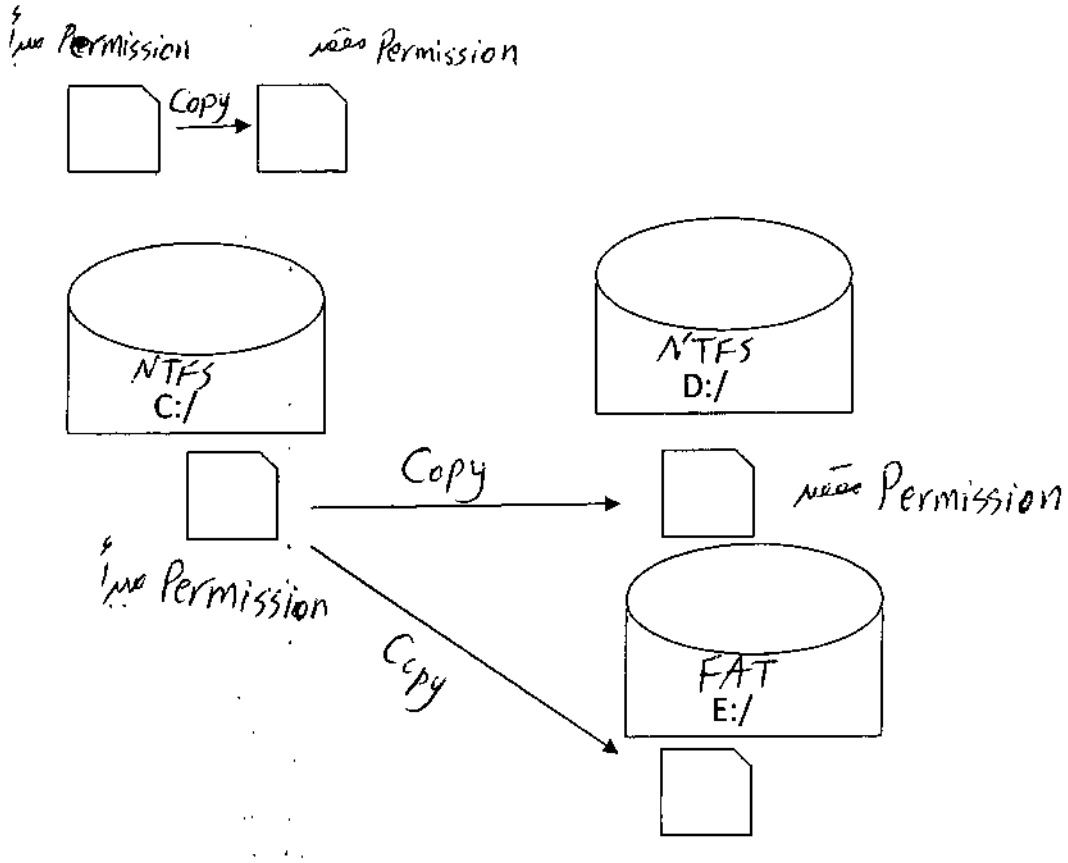
1) Read attributes
2)Read extended attributes
3)Create file / write data
4)Create folders/ append data
5)Write attributes
6)Write extended attributes
7)Delete sub folders and files
8)Delete
9)Read permission
10)Change permission
11)Take owner ship
12)Full control
13)Traverse folder/ execute file
14)List folder/ read data

وقتی فایل یا فولدری را کپی می کنیم permission های آن چه می شود؟



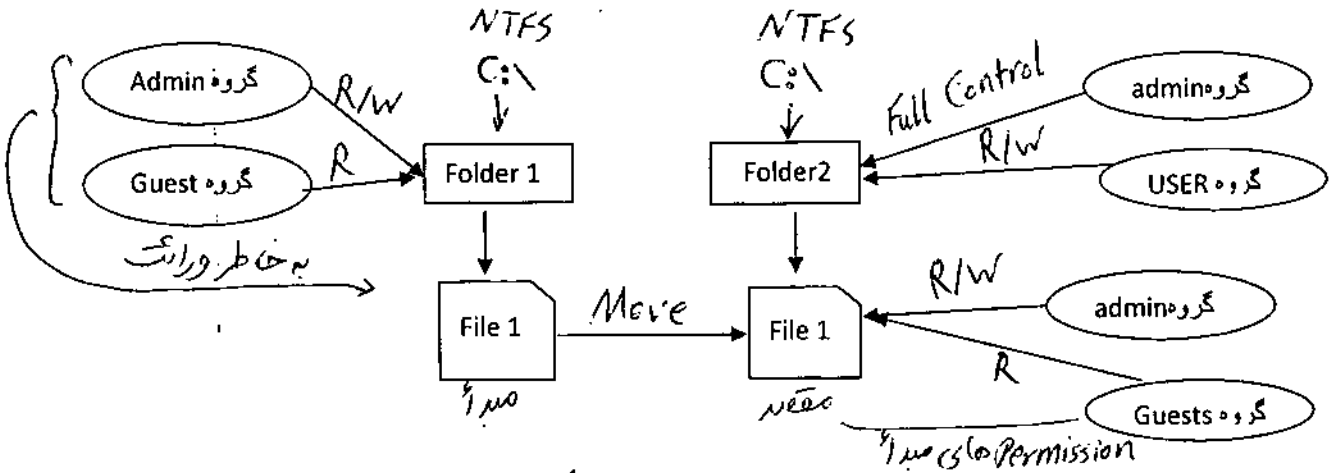
همان Permission های مقصد

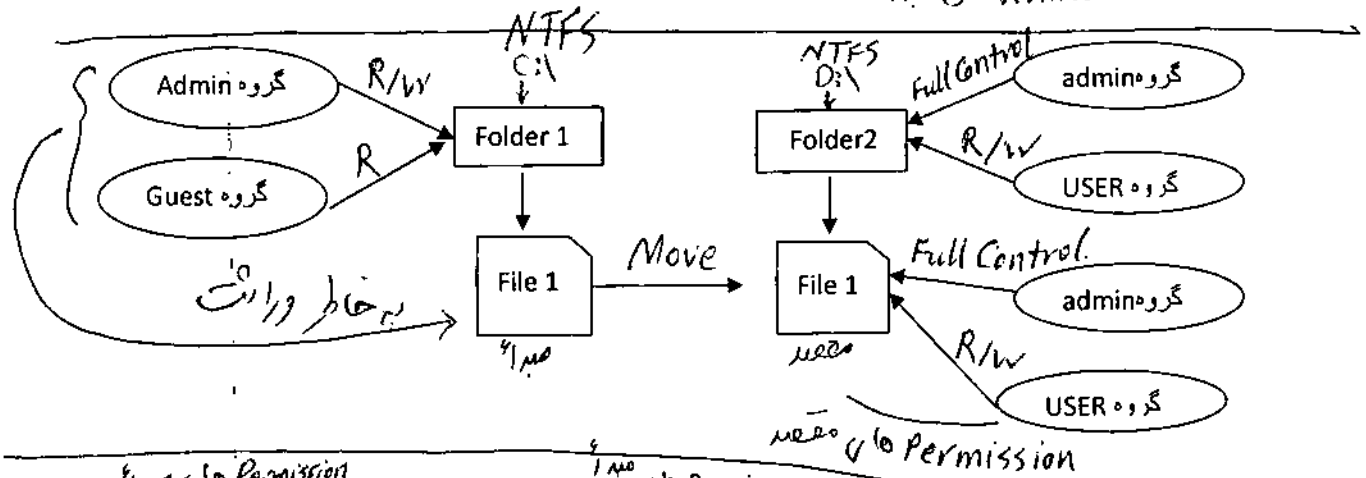


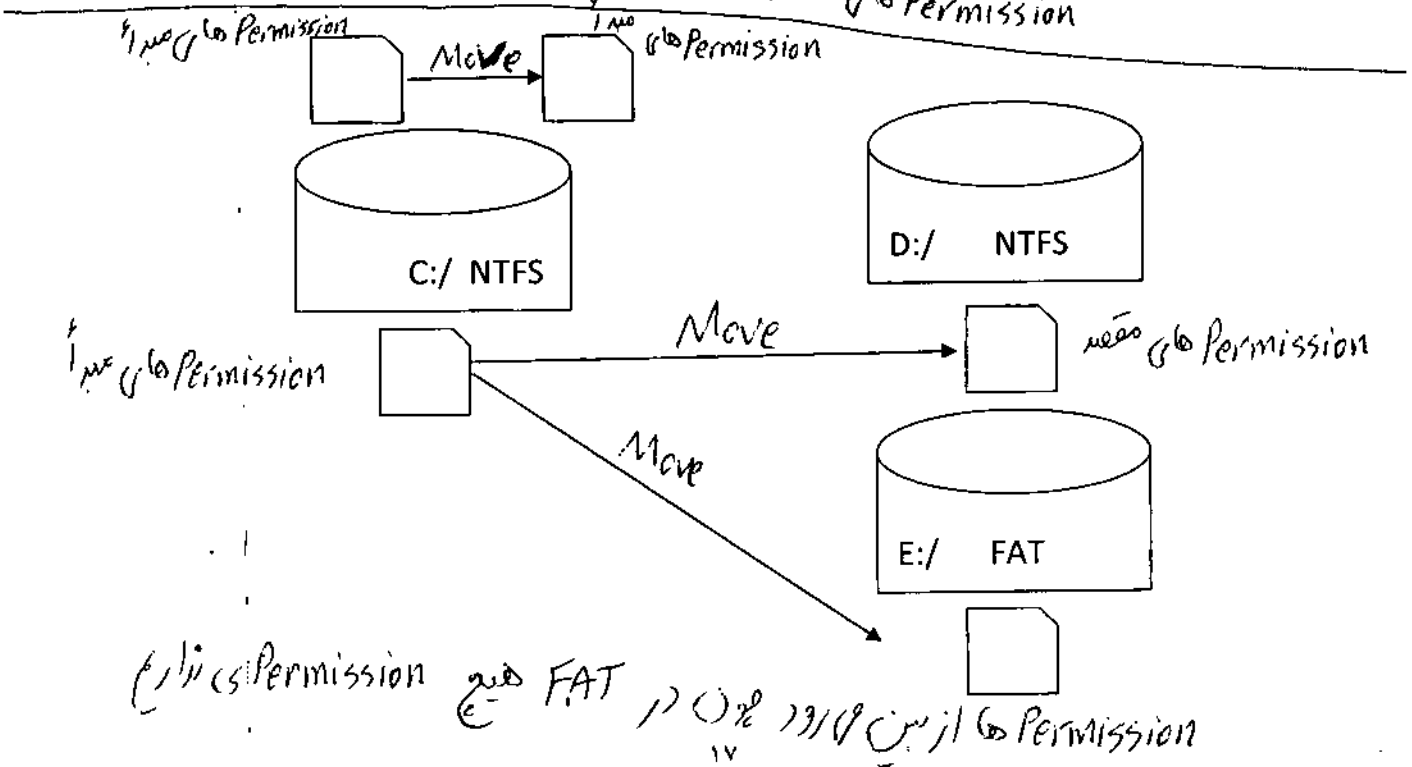


PERMISSIONها از بین میرود چون در FAT هیچPERMISSION ی نداریم

وقتی فولدر یا فایلی را MOVE میکنیم PERMISSIONهای آن چه می شود؟







فشرده سازی Compression

زمانی که احتیاج به فضای بیشتری برای ذخیره سازی اطلاعات روی دیسک داریم یا به عبارت دیگر با کمبود ظرفیت و فضا روبرو میشویم میتوانیم اطلاعات را فشرده کنیم.

اصول کار نرم افزارهای فشرده سازی

۱)جلوگیری از هدر رفتن فضا

واحد تخصیص فایل یا کلاستر را تغییر میدهدو چند فایل کوچک را در یک کلاسترقرار میدهد

۲) حذف کاراکتر های تکراری:

به دنبال کاراکترهای تکرار شده در فایل میگردد و به جای انکه انها را چند بار تکرار کند

تعداد دفعات تکرار آنها نشان میدهد

چه اطلاعاتی را باید فشرده کنیم

۱) اطلاعاتی که پس از فشرده سازی حجم آنها کمتر میشود

۲)اطلاعاتی که کمتر با انها سر و کار داریم(به دلیل زمان لازم برای

(compress، uncompress

- فایلهایی که ذات انها فشرده است پس از فشرده سازی حجم آنها کمتر نمیشود مثل jpg,gif,mpg,mp3

- فایلهایی مثل . TXTو BMPپس از فشرده سازی حجم آنها از ۵۰ تا ۷۰ درصد کم میشود

- نباید فایلها را چند بار COMPRESSکرد چون عملا در دفعات بعدی نه تنها حجم آنها کم نمیشود بلکه زیاد تر هم میشود

فشرده سازی در WIN XP

۱)استفاده از COMPRESSED(ZIPPED) FOLDER

۲) فشرده کردن فایلها و فولدر ها در درایو NTFS

۳)فشرده کردن درایو NTFS

ویژگیهای COMPRESSED(ZIPPED) FOLDER

۱)قابل ساختن هم روی درایو FAT وهم روی درایو NTFS

۲) فایلها و فولدر های درون آن را میتوان دید و بعضی فایلهای اجرایی آن را اجرا کرد ولی نمیتوان فایلهای آن را تغییر دهد

۳) این فولدر قابل جا به جایی از هر درایو یا فولدر به درایوها و فولدرهای دیگر است و سازگار با دیگر نرم افزارهای ZIP مثل WINZIP و PKZIP است

۴)اگر فایلی را درون آن قرار دهیم COMPRESSمیشود واگر فایلی را از آن خارج کنیم ودر یک محل UNCOMPRESS قرار دهیم آن فایل UNCOMPRESS میشود

راه ایجاد COMPRESSED(ZIPPED) FOLDER:

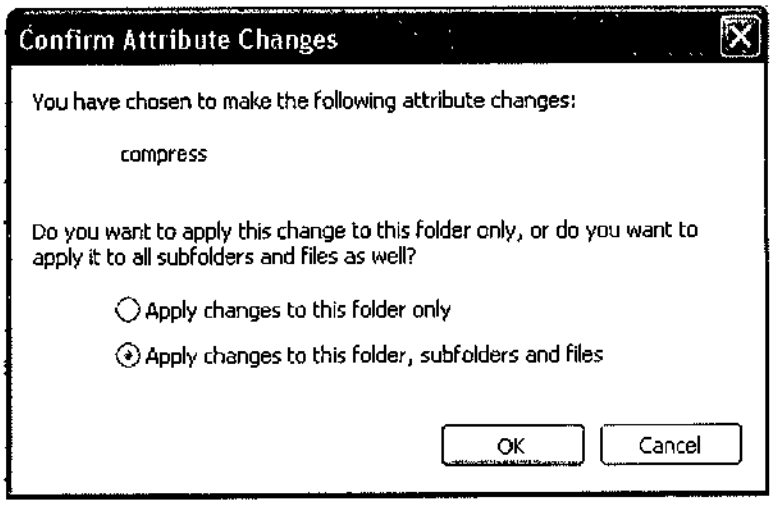
راست کلیک در قسمت خالی پنجره←NEW←COMPRESSED(ZIPPED) FOLDER

فشرده کردن فایلها و فولدر ها در درایو NTFS

این کار از طریق پنجره PROPERTIES مربوط به FILE یا FOLDER امکان پذیر است

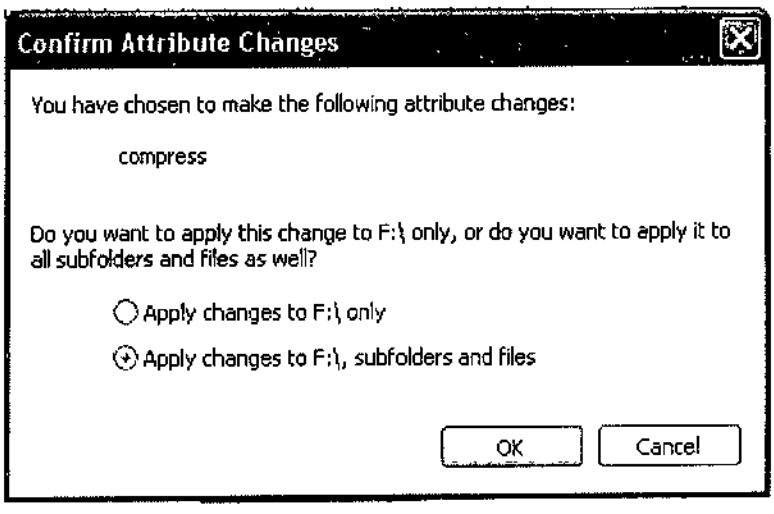
پنجرهPropertiesمربوط به پوشه مورد نظر / GENERALسرپوشه/دکمه ADVANCE/گزینه/COMPRESS CONTENTS

وقتی گزینه COMPRESSرا برای یک FOLDER انتخاب میکنیم و دکمه OKرا میزنیم در پنجره PROPERTIESکادر با دو گزینه ظاهر میشود

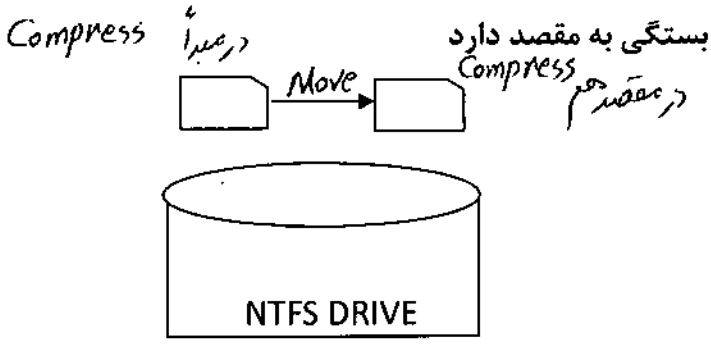


فشرده کردن درایو NTFS

پنجرهPropertiesمربوط به درایو مورد نظر / GENERALسرپوشه/دکمه ADVANCE/گزینه/COMPRESS Drive to Save Disk Space



فقط در حالتی که فایل یا پوشه ای را از مکانی روی درایو NTFS که COMPRESS شده به مکان دیگری روی همان درایو NTFSانتقال دهیم ان فایل یا پوشه در مقصد هم compress باقی می ماند در حالتهای دیگر بستگی به مقصد دارد



ENERYPTING FILE SYSTEM (EFS)

رمز کردن فایلها و فولدر ها در یک درایو NTFS

گزینه ENERYPT CONTENTS TO SECUREDATA/دکمه ADVANCE /سربوشه GENERAL/ پنجرهProperties مربوط به فایل یا فولدر مورد نظر

در آن واحد فقط میتوان یک فایل یا پوشه را COMPRESS یا ENERYPTکرد

یعنی این که فایل نمیتواند هم فشرده هم رمز شده باشد

RECOVERY AGENT مامور نجات

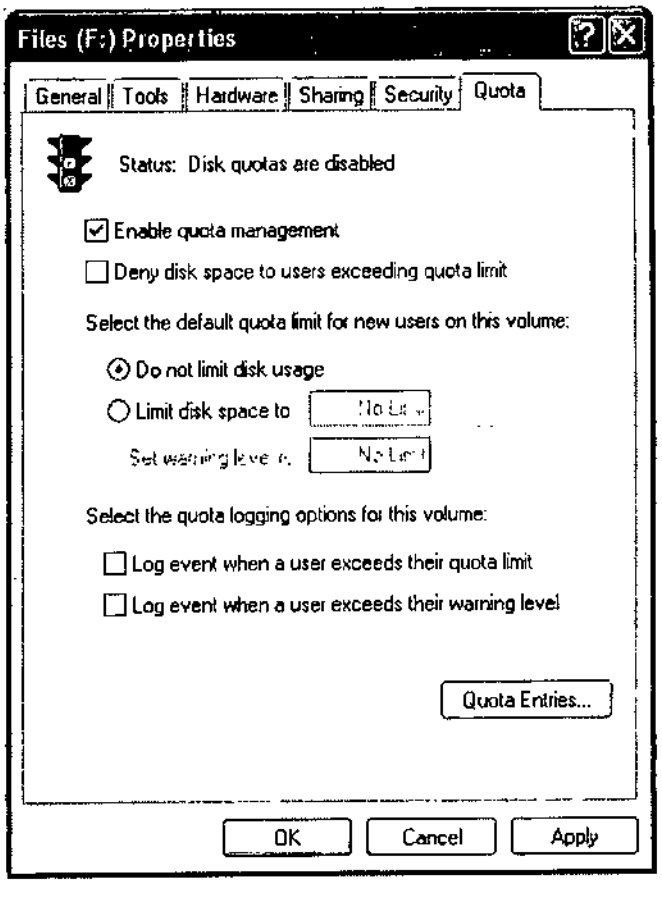
گزینه ای در FOLDER OPTION در قسمت VIEW برای رنگی نشان دادن:

SHOW ENCRYPTED OR COMPRESSED NTFS FILE IN COLOR

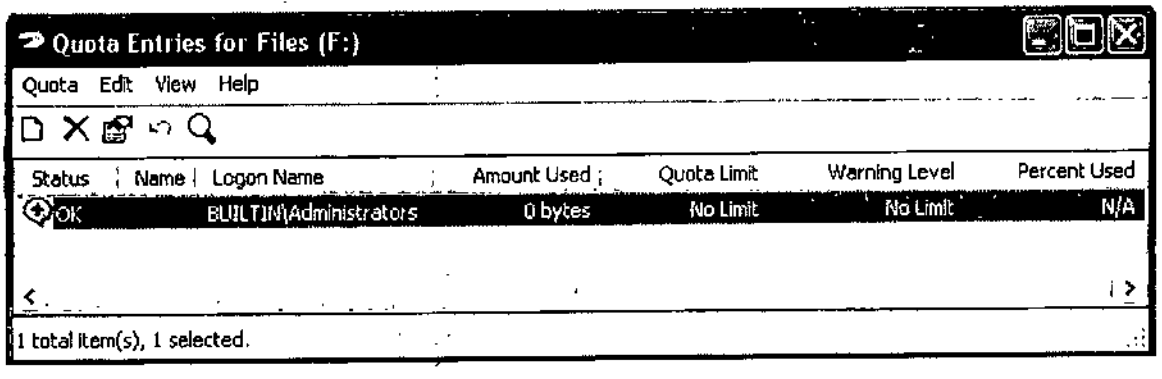
رنگ ابی ←COMPRESS

رنگ سبز ←ENERYPT

سهمیه بندی کردن دیسک Disk Quota



اگر دکمه Quota Entries را انتخاب کنیم:



برای وارد کردن یک user جدید در قسمت Quota Entries می توان از منوی Quota گزینه New Quota Entryرا انتخاب کرد

درس سیستم حامل شبکه

قسمت دوم:

ACTIVE DIRECTORY

در

WINDOWS 2003 SERVER

DOMAIN FUNCTIONAL LEVELS

WINDOWS 2000 MIXED

وقتی ACTIVE DIRECTRY را روی ویندوز 2003نصب میکنیم ویا وقتی که سیستم عامل یک DOMAIN CONTROLLERرا به WINDOWS 2003 SERVER ارتقائ میدهیم این DOMAIN CONTROLLER روی WINDOWS 2000 MIXEDتنظیم میشود

WINDOWS 2000 MIXEDاجازه کار با DOMAIN CONTROLLERهای WINDOWS NT WIN 2000,WIN2003,را میدهد

WIN 2000 NATIVE

اگر DOMAIN CONTROLLER های موجود در FOREST همه روی سیستم عاملهای WINDOWS SERVER,WIN 2003باشند(یعنی Domain Controller ی با ویندوز NT نداشته باشیم) میتوان FUNCTION LEVEL مربوط به DOMAIN CONTROLLER روی WIN SERVER2003 را بالا برد و به NATIVEتبدیل کرد

بنابر این WIN 2000 NATIVE فقط ا جازه کار با DOMAIN CONTROLLER ها ی روی سیستم عامل SERVER 2003,WIN SERVER2000 را میدهد

WIN SERVER 2003 INTERIM

زمانی که DOMAIN CONTROLLERروی NTرا به DOMAIN CONTROLLERروی WIN 2003ارتقائ میدهیم و یک FOREESTجدید ایجاد میکنیم میتوان به طور موقت این LEVEL FUNCTION را انتخاب کرد

WIN SERVER 2003 INTERIM فقط اجازه کار با DOMAIN CONTROLLERهای WIN NT4وwin server2003 را میدهدیعنی domain controller های win 2000 را پشتیبانی نمیکند

Win server 2003

اگر سیستم عامل تمام domain controller های یک domain ,ویندوز سرور ۲۰۰۳ باشد میتوان functional level آنها را به Win server 2003 تبدیل کرد. این functional level فقط اجازه کار باdomain controller های ویندوز ۲۰۰۳ را میدهد.

گروهها در DOMAIN :

GROUP TYPES:

۱) SECURITY GROUP:گروههایی هستند که میتوان به آنها PERMISSIONهایی برای دسترسی به منابع داد.این گروهها می توانند نقش گروههای توزیع شده (Distribution Group) را نیز بازی کنند.

۲)Distribution Group :گروههایی هستند که هیچ PERMISSIONی روی آنها نمیتوان اعمال کرد.فقط برنامه هایی که برای کار با Active directory طراحی شده اند میتوانند از این گروهها استفاده کنند مثل exchange server (مخصوص کارهای توزیعی)

Group scopes
- Global groups
- Domain local Groups
- Universal Groups

Global Groups:

فقط userها ,گروهها و کامپیوترهای domain ی که این گروه روی آن تعریف شده می توانند عضو آن شوند.

اعضای این گروه می توانند به تمام منابع داخل یک forest دسترسی داشته باشند(Global)

Domain local Groups :

userها ,گروهها و کامپیوترهای هر domain در forest میتوانند عضو آن شوند

اعضای این گروه فقط اجازه دسترسی به منابع domain ی که این گروه روی آن تعریف شده را دارند. (Local)

Universal Groups :

ترکیب هر دو گروهDomain local وGlobal می باشد یعنی اعضای این گروه میتوانند همه userها ,گروهها و کامپیوترها در تمام forest باشند و دسترسی به همه منابع در سراسر forest داشته باشند

Universal Groups فقط درdomain هایی که دارایdomain functional level های Windows 2000 native و windows server 2003 هستند قابل دستیابی و استفاده می باشند بنابراین در domain ی با FUNCTIONAL LEVEL هایWindows 2000 mixed وinterim قابل دستیابی نمی باشند

اعضای گروه ها:

Group scope	Windows 2000 mixed	Windows 2000 native and Windows server 2003
Global	user ها و کامپیوترها از همان Domain	user ها و کامپیوترها و global group از همان Domain
Domain local	user ها و کامپیوترها و global group از هر Domain	user ها و کامپیوترها و global group و universal group از هر Domain ی وdomain local group ها از همان domain
Universal	قابل دستیابی در FUNCTIONAL LEVEL نمیباشد	user ها و کامپیوترها و global group و universal group از هر Domain ی در forest

گروه های پیش ساخته در Active Directory:

در Active Directory سه دسته گروه به صورت پیش فرض وجود دارند:

۱)گروهها در پوشه built-in

۲) گروهها در پوشه User

۳)گروههای خاص شناسایی

گروههای پیش فرض در پوشه built-in:

نام گروه	توضیحات
ACCOUNT OPERATORS	اعضای این گروه اپراتور ACCOUNT هستند و به صورت پیش فرض این گروه هیچ عضوی ندارد اعضای این گروه میتوانند Group count و User count و computer account ایجاد کنند، تغییر دهند و یا حذف کنند ولی اجازه تغییر گروههای Administrator و Domain Admins را ندارند یعنی نمی توانند عضوی را به این گروهها اضافه کنند یا تغییر دهند و یا حذف کنند