Sharing & Security

تُعد إدارة الصلاحيات من أهم المهارات الأساسية لمسؤول النظام(System Administrator) ، حيث تضمن:

- حماية البيانات
- تنظيم الوصول للمستخدمين
- منع التلاعب أو الحذف غير المصرح به
- تطبيق مبدأ **Least Privilege**

تعتمد أنظمة Windows Server على نوعين أساسيين من الصلاحيات:

1. **NTFS Permissions (Security Tab)**
2. **Sharing Permissions (Sharing Tab)**

وسيتم في هذه الجلسة شرح كل منهما بالتفصيل، مع بيان العلاقة بينهما، ودور المستخدمين والمجموعات.(Users & Groups)

مقدمة عن File Server

الـ **File Server**هو جهاز (Server) مخصص لتخزين الملفات والبيانات، والسماح للمستخدمين على الشبكة بالوصول إليها ومشاركتها بطريقة منظمة وآمنة.

نستخدم File Server بهدف :

1. مشاركة البيانات بين عدد كبير من المستخدمين.
2. حماية البيانات والتحكم في من يستطيع الوصول إليها.
3. تنظيم الصلاحيات (قراءة – تعديل – حذف) .
4. النسخ الاحتياطي (Backup) وحماية البيانات من الفقدان.
5. الإدارة المركزية بدلاً من تخزين البيانات على أجهزة المستخدمين.

مفهوم Sharing (مشاركة الملفات)

ما المقصود بـ Sharing

هو إتاحة مجلد أو مورد معين على الشبكة بحيث يمكن لأكثر من مستخدم الوصول إليه من أجهزة مختلفة.

فوائد Sharing :

- تسهيل تبادل الملفات.
- العمل الجماعي على نفس البيانات.
- تقليل تكرار الملفات.
- توفير الوقت والجهد.

أنظمة الملفات (File Systems)

ما هو نظام الملفات؟ نظام الملفات هو الطريقة التي يستخدمها نظام التشغيل لتنظيم وتخزين البيانات على القرص الصلب.

نظام FAT32

خصائص:FAT32

- نظام ملفات قديم.
- الحد الأقصى لحجم الملف الواحد.4GB :
- لا يدعم الصلاحيات المتقدمة.
- لا يحتوي على .Security Tab
- يعتمد فقط على .Sharing Permissions

مميزات:FAT32

- بسيط
- متوافق مع أنظمة تشغيل متعددة.

عيوب:FAT32

- ضعف الأمان.
- لا يدعم التحكم الدقيق في الصلاحيات.
- غير مناسب للشبكات الكبيرة أو الخوادم.

نظام NTFS

خصائص:NTFS

- نظام ملفات حديث وقوي.
- يدعم ملفات بأحجام كبيرة جداً.
- يدعم .**Security Permissions**
- يحتوي على:
  - Sharing Tab
  - Security Tab

مميزات:NTFS

- أمان عالي.
- تحكم دقيق في صلاحيات المستخدمين.
- مناسب للـ Servers والشبكات الكبيرة.

الفرق بين Sharing Tab وSecurity Tab

Sharing Tab	Security Tab

• تتحكم في الصلاحيات **عبر الشبكة فقط**.
• تطبق على المستخدمين الذين يصلون من أجهزة أخرى.
• الصلاحيات الأساسية:
  ○ Read
  ○ Change
  ○ Full Control
	• تتحكم في الصلاحيات **محلياً وعبر الشبكة**.
	• تعمل فقط مع NTFS.
	• توفر تحكما أدق في الصلاحيات

سنتعرف على كل منها بالتفصيل :

صلاحيات المشاركة(Sharing Permissions)

هي الصلاحيات التي تتحكم في الوصول إلى المجلد عبر الشبكة فقط.

يتم إعدادها من خلال:

Properties → Sharing → Advanced Sharing

أنواع Sharing Permissions.

Read

- بالنسبة للملف : قراءة الملفات فقط وبالنسبة للمجلدات : فتح المجلدات ورؤية محتواها فقط

Readعلى ملف = فتح الملف
Readعلى مجلد = رؤية المحتوى فقط (لا يمكن فتح الملفات بداخله)

Change

- قراءة
- تعديل
- حذف
- إعادة تسمية

Full Control

- جميع الصلاحيات
- التحكم بالمشاركة نفسها

صلاحيات(NTFS (Security Permissions

هي الصلاحيات التي تُطبق على الملفات والمجلدات المخزنة على أقراص مهيأة بنظام NTFS ، ويتم التحكم بها من خلال:

Properties → Security Tab

أنواع صلاحيات NTFS الأساسية.

Read

- قراءة محتوى الملف

- فتح الملف فقط
- ❌ لا يمكن التعديل أو الحذف

اما على مجلد تعني :

- فتح المجلد
- رؤية أسماء الملفات
- ❌ **لا يمكن فتح الملفات نفسها**

Read & Execute

- قراءة الملفات
- تشغيل الملفات التنفيذية
- استعراض المجلدات

اما على مجلد تعني :

- الدخول إلى المجلد
- تشغيل الملفات التنفيذية داخله
- فتح الملفات المسموح بها

List Folder Contents

- عرض محتويات المجلد فقط
- تُستخدم غالبا مع المجلدات

Write

- إنشاء ملفات جديدة
- تعديل محتوى الملفات
- ❌ **لا يسمح بالحذف أو إعادة التسمية**

اما على مجلد تعني :

- إنشاء ملفات جديدة داخل المجلد
- إنشاء مجلدات فرعية
- ❌ **لا يسمح بحذف الملفات أو تعديل ملفات موجودة**

Modify

تشمل : Read , Write , Delete , Rename

- لا تشمل تغيير الصلاحيات

Full Control

- جميع الصلاحيات السابقة
- تغيير الصلاحيات
- أخذ الملكية(Take Ownership)

الصلاحية	الوصف
Read	قراءة الملفات فقط
Read & Execute	قراءة وتشغيل الملفات
List Folder Contents	عرض محتويات المجلد
Modify	قراءة + تعديل + حذف
Write	إضافة ملفات أو تعديلها
Full Control	تحكم كامل (قراءة، تعديل، حذف، تغيير الصلاحيات)

الفرق بين Modify وFull Control

المقارنة	Modify	Full Control
قراءة الملفات	✓	✓
التعديل	✓	✓
الحذف	✓	✓
إعادة التسمية	✓	✓
تغيير الصلاحيات	✗	✓
أخذ الملكية	✗	✓

ملاحظة:
لا يُنصح بإعطاء Full Control إلا للمسؤولين.(Administrators)

العلاقة بين Sharing وSecurity

قاعدة مهمة جداً:

الصلاحية النهائية للمستخدم = أقل صلاحية بين Sharing وSecurity

مثال:

- Sharing = Full Control
- Security = Read

الصلاحية النهائية ← Read

ملاحظة : الصلاحية تكون ممنوعة ضمنيا... وعند الرغبة بمنحها لاحد المستخدمين ، يجب التصريح علنا بانها مسموحة عن طريق تفعيل الخيار allow .وبالتالي حتى يحصل مستخدم على صلاحية ما يجب ان يتم التصريح علنا انها مسموحة ضمن ال sharing وضمن ال security معا.

المستخدمون والمجموعات(Users & Groups)

نستخدم Groups من اجل :

- سهولة الإدارة
- تقليل الأخطاء
- إدارة جماعية للصلاحيات

.أنواع المجموعات:

- Administrators
- Domain Users
- Custom Groups (Group1, Group2…)

.مبدأ العمل:

- لا نعطي الصلاحيات مباشرة للمستخدم
- نعطي الصلاحيات للمجموعة
- نضيف المستخدم إلى المجموعة

ملاحظة :

Administrator يمتلك صلاحيات كاملة افتراضياً.

سيناريو عملي :

1. إنشاء مجلد

```
C:\Folder
```

2. مشاركة المجلد

```
Properties → Advanced Sharing → Share this folder
Share Name: my_share
```

3. Sharing Permissions

- Everyone → Read

4. Security Permissions

- Group1 → Modify
- Group2 → Read

5. إضافة المستخدمين

- Ahmad → Group1
- Shadi→ Group2

6. النتيجة:

- Ahmad: يستطيع التعديل والحذف
- Shadi: يستطيع القراءة فقط

أفضل الممارسات(Best Practices)

1. استخدام NTFSدائماً في الخوادم.
2. ضبط الصلاحيات من Security Tab.
3. تقليل استخدام Full Control.
4. الاعتماد على Groups بدلاً من Users.

5. مراجعة الصلاحيات بشكل دوري.
6. تفعيل النسخ الاحتياطي.(Backup)

تحديد الصلاحيات ضمن ال groups :

ادا كان لدي Group1 , Group2 وكان احمد مستخدم ينتمي الى كلا الغروبين

سيحصل احمد على الصلاحيات وفق الجدول التالي :

الصلاحية في group1	الصلاحية في group2	صلاحيات احمد
مسموحة بشكل صريح	غير محددة (لم يتم تفعيل allow ولا حتى تفعيل deny)	سيحصل على الصلاحية
مسموحة بشكل صريح	ممنوعة بشكل صريح	ممنوعة
ممنوعة بشكل صريح	مسموحة بشكل صريح	ممنوعة
مسموحة بشكل صريح	مسموحة بشكل صريح	مسموحة
غير محددة (لم يتم تفعيل allow ولا حتى تفعيل deny)	غير محددة (لم يتم تفعيل allow ولا حتى تفعيل deny)	ممنوعة

اي ان احمد سيحصل على تجميع الصلاحيات التي لم يتم الاعلان عنها صراحة انها ممنوعة ...

الوراثة (Inheritance) في المجلدات

الوراثة هي آلية في نظام NTFS تقوم بـ:

نقل الصلاحيات من المجلد الأب(Parent Folder) إلى:

- المجلدات الفرعية(Subfolders)
- الملفات الموجودة داخلها

أي صلاحية تُطبّق على مجلد، **تنتقل تلقائيا** إلى كل ما بداخله.

لماذا تُستخدم الوراثة؟

الوراثة تحقق:

- سهولة إدارة الصلاحيات
- تقليل الأخطاء البشرية

- توحيد مستوى الأمان
- تقليل الحاجة لتعيين صلاحيات لكل ملف يدويا

مثال:
إذا كان لديك 1000 ملف داخل مجلد
←الوراثة تغنيك عن تعيين 1000 صلاحية منفصلة.

كيف تعمل الوراثة عمليا؟

مثال بنية مجلدات:

```
D:\Company
│
├── HR
│   └── employees.xlsx
│
└── IT
```

صلاحيات المجلد الأب:(Company)

- Group1 → Modify
- Group2 → Read

النتيجة:

- مجلد HR يرث نفس الصلاحيات
- ملف employees.xlsx يرث نفس الصلاحيات

أنواع الصلاحيات من حيث الوراثة

عند الدخول إلى:

`Security → Advanced`

ستجد نوعين من الصلاحيات:

Inherited

- صلاحيات موروثة من المجلد الأب
- لا يمكن تعديلها مباشرة

Explicit

- صلاحيات أُضيفت يدويا
- يمكن تعديلها أو حذفها

تمييز مهم:

- الصلاحيات الموروثة تكون غالبا **باللون الرمادي**

التحكم بالوراثة(Disable Inheritance)

المسار:

```
Properties → Security → Advanced → Disable Inheritance
```

عند الضغط على **Disable Inheritance** تظهر نافذة تحتوي خيارين مهمين جدا.

الخيار الأول

Convert inherited permissions

ماذا يعني Convert ؟

يعني: تحويل الصلاحيات الموروثة إلى صلاحيات صريحة(Explicit)

ماذا يحدث فعليا؟

- يتم قطع الوراثة
- تبقى نفس الصلاحيات
- لكن تصبح قابلة للتعديل والحذف

أي: " احتفظ بالصلاحيات الحالية لكن اجعلها مستقلة عن الأب"

متى نستخدم Convert ؟

✓عندما نريد:

- تعديل بعض الصلاحيات فقط
- منع تأثر المجلد بتغييرات مستقبلية في الأب
- تخصيص الصلاحيات لمجلد معين

مثال عملي:

```
Company (Full Control)
└── HR
```

نريد:

- HR بدون Full Control
- لكن مع Modify فقط

→ Disable Inheritance
→ Convert
→تعديل Full Control إلىModify

الخيار الثاني

Remove all inherited permissions

ماذا يعنيRemove ؟

يعني: حذف جميع الصلاحيات الموروثة بالكامل

ماذا يحدث؟

- المجلد يصبح بدون أي صلاحيات تقريبا
- قد تفقد القدرة على الدخول إليه

⚠تحذير خطير: قد تقفل المجلد على نفسك

متى يُستخدم؟

✓في حالات خاصة جدا مثل:

- إنشاء مجلد سري
- مجلد أمني عالي الحساسية
- عزل كامل عن الهيكل العام

بعد استخدامه: يجب إضافة صلاحيات جديدة يدويا فورا

مقارنة بين Convert وRemove

المقارنة	Convert	Remove
الاحتفاظ بالصلاحيات	✓	✗
قطع الوراثة	✓	✓
الأمان	آمن	خطر
الاستخدام الشائع	✓ جدًا	نادر
مناسب للطلاب	✓	✗

أولوية الصلاحيات مع الوراثة

ترتيب الأولوية:

1. Explicit Deny
2. Explicit Allow
3. Inherited Deny
4. Inherited Allow

أي:

- الصريح أقوى من الموروث
- Deny أقوى منAllow

مثال امتحاني شائع

السؤال:

مجلد فرعي يرث Full Control من الأب
أردنا منعه من الحذف فقط
ما الحل الصحيح؟

الإجابة النموذجية:

1. Disable Inheritance
2. Convert inherited permissions
3. تعديل الصلاحية من Full Control إلىModify

الوصول من جهاز Client لمجلد مشارك على الشبكة

1. تسجيل الدخول بمستخدم Domain
2. تشغيل : windows run ← \\ServerIP\ my_share

يتم تطبيق الصلاحيات تلقائيا حسب:

- Group
- NTFS
- Sharing

..... انتهت الجلسة مع تمنياتي لكم بالتوفيق والنجاح .....