

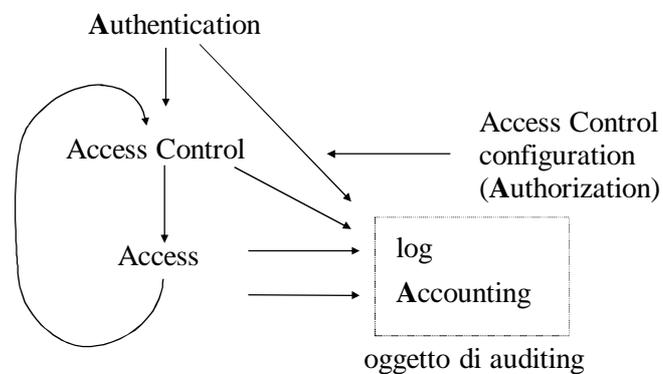
Filesystem e permessi NTFS

Bernardo Palazzi

 UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

AAA

- Authentication, Authorization (access control), Accounting
 - AAA Working Group, IETF
- logging, auditing



 UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

2

Controllo degli accessi discrezionario

- Gli utenti possono proteggere le risorse di cui hanno la proprietà.
- Il proprietario può consentire l'accesso agli altri utenti.
- Il proprietario può stabilire il tipo di accesso (read/write/execute) permesso agli altri.

Politica chiusa

- Assegnato a Mario l'accesso read a "rapporti"
- Assegnato a Bob l'accesso r/w a "missioni"
 - Mario: desidera leggere "rapporti"
 - L'accesso è permesso
 - Mario: desidera leggere "missioni"
 - L'accesso è negato

Politica aperta

- Negato a Mario l'accesso read a "rapporti"
- Negato a Bob l'accesso r/w a "missioni"
 - Mario: desidera leggere "rapporti"
 - L'accesso è negato
 - Mario: desidera leggere "missioni"
 - L'accesso è permesso



UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

Politica chiusa con autorizzazioni negative e priorità della negazione

- Assegnato a Mario l'accesso r/w a "rapporti"
- Negato a Mario l'accesso w a "rapporti"
 - Mario: desidera leggere "rapporti"
 - L'accesso è permesso
 - Mario: desidera scrivere "rapporti"
 - L'accesso è negato



UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

Panoramica sul File System

- NTFS – formato nativo del file system di Windows NT
- Include supporto per:
 - CDFS
 - UDF
 - FAT12, FAT16 e FAT32

NTFS

- Utilizza cluster con indici a 64-bit
- NTFS ha la capacità di indirizzare volumi grandi fino a 16 exabyte 10^{15}
- Window limita la taglia di un volume NTFS a cluster indirizzabili con cluster a 32-bit
 - 128 TB (utilizzando cluster a 64KB)

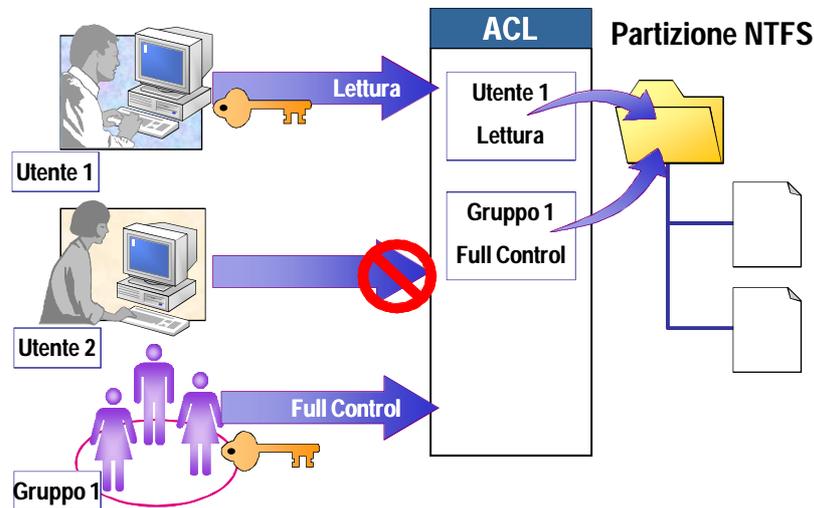
Caratteristiche avanzate NTFS

- **Recuperabilità (Recoverability)**
 - Le "strutture" del file system può essere riportata a uno stato consistente (nessuna perdita di informazioni su file o struttura delle directory – i dati possono essere persi)
- **Sicurezza di file e directory**
 - File e directory sono protetti da accesso non autorizzato utilizzano una combinazione di ID di sicurezza (immagazzinate come parte di un file ACL) e la password inserita...
- **Compressione File**
 - Transparente alle applicazioni
 - Compressione delle directory possibile

Caratteristiche avanzate NTFS (2)

- **Quote Disco**
 - Quote del disco per utente
 - NTFS segna file e directory con l'ID di sicurezza dell'utente che lo ha creato...
- **Crittazione**
 - Supporta EFS – Encrypting File System
 - Transparente alle applicazioni
 - Si può accedere ai file tramite la chiave privata di una coppia di chiavi pubblico/privato di EFS ...
- **Ereditarietà delle autorizzazioni**

Autorizzazioni NTFS



 UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

Permessi per le cartelle NTFS

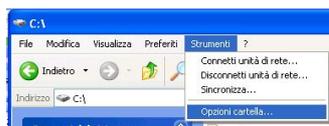
- Read
 - Vedere i file e le sottocartelle presenti nella cartella con gli attributi, le proprietà e i permessi
- Write
 - Creare nuovi file e sottocartelle dentro la cartella, cambia gli attributi, si possono vedere permessi e proprietà nelle cartelle
- List Folders Contents
 - Vedere i nomi di file e sottocartelle nella cartella
- Read & Execute
 - Traversa le cartelle, in più effettua azioni permesse dalle autorizzazioni di Read e List Folder Contents
- Modify
 - Cancellare la cartella ed effettuare l'insieme dell'unione dei permessi Write e Read & Execute
- Full Control
 - Cambiare i permessi, può prendere la proprietà, cancellare le sottocartelle e i file, è l'unione di tutti i precedenti permessi

 UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

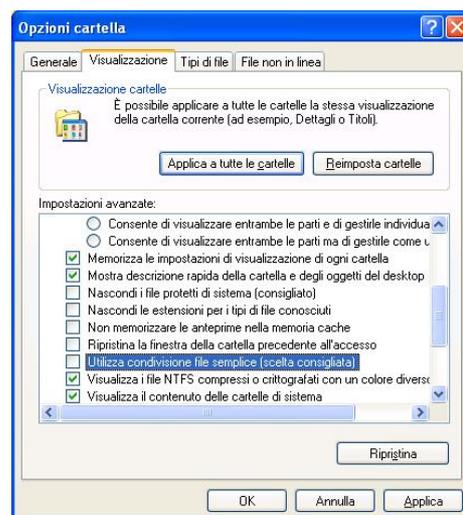
Permessi per i file NTFS

- Read
 - Vedere i file con gli attributi, le proprietà e i permessi
- Write
 - Creare nuovi file, cambiare gli attributi, si possono vedere permessi e la proprietà nei file
- List Folders Contents
 - Vedere i nomi di file e le sottocartelle nella cartella
- Read & Execute
 - Caricare le applicazioni ed effettuare le azioni permesse dalle autorizzazioni di Read
- Modify
 - Modificare e cancellare il file ed effettuare l'insieme dei permessi Write e Read & Execute
- Full Control
 - Cambiare i permessi, può prendere la proprietà, è l'insieme di tutti i permessi NTFS del file

Attivare permessi NTFS in Windows XP

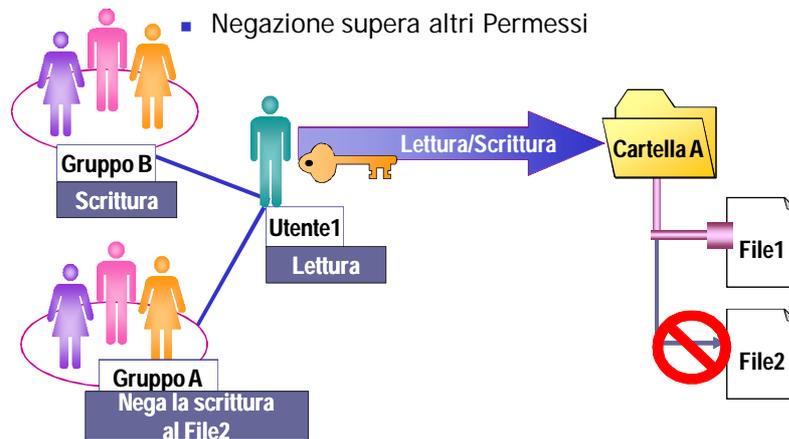


- I permessi NTFS in Windows XP Pro sono disabilitati di default
- Tramite la voce **Opzioni Cartella...** del menu **Strumenti** di una finestra dell'**Esplora Risorse** è possibile abilitare le funzionalità NTFS avanzate



Autorizzazioni NTFS Multiple

- Le autorizzazioni NTFS sono cumulative
- Autorizzazioni sui File sovrascrivono le autorizzazioni sulle cartelle
- Negazione supera altri Permessi



 UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

Ereditarietà permessi NTFS

Ereditarietà Permessi

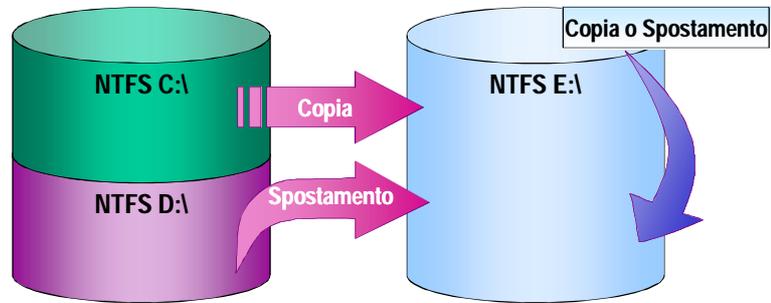


Prevenzione Eredità



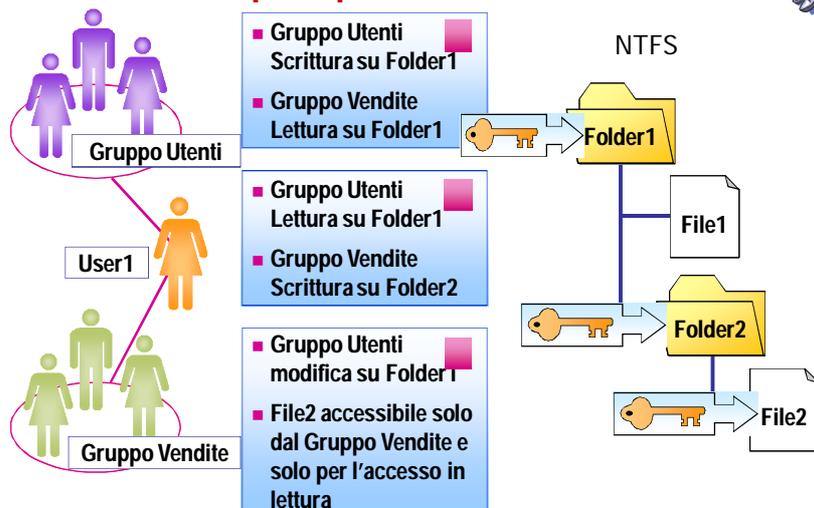
 UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

Copia e spostamento in NTFS



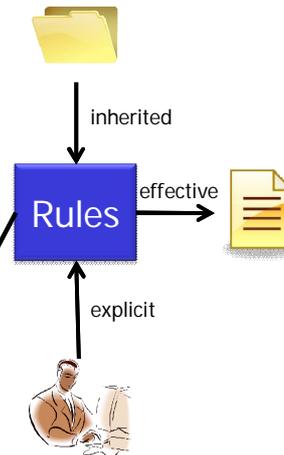
- Tutto ciò che si copia eredita le autorizzazioni
- Solo nello spostamento all'interno della stessa partizione si mantengono le autorizzazioni

Esempi: permessi NTFS



NTFS file permissions

- **Explicit:** set by the *owner* for each user/group.
- **Inherited:** dynamically inherited from the explicit permissions of ancestor folders.
- **Effective:** obtained by combining the explicit and inherited permission.
- ◆ Determining effective permissions:
 - By default, a user/group has no privileges.
 - Explicit permissions override conflicting inherited permissions.
 - Denied permissions override conflicting allowed permissions.



Condivisione Cartelle

Requisiti per le cartelle condivise

I requisiti sono diversi a seconda:

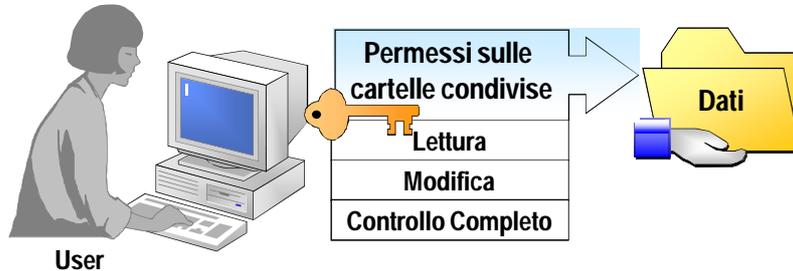
- se le cartelle condivise siano in un dominio o in un gruppo di lavoro
- del tipo di sistema operativo sul computer dove risiede la cartella condivisa

Condividere una cartella	Bisogna essere Membri di:
In un dominio Windows	Administrators o Server Operators
In un Workgroup Windows	Administrators o Power Users
Su un Computer Client con Windows	Administrators o Power Users

Condividere una cartella



Permessi Cartelle Condivise



User

- I permessi sulle cartelle condivise sono cumulativi
- Negazione:
 - Sovrascrive tutti gli altri permessi
 - Da utilizzare solo se necessario



UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

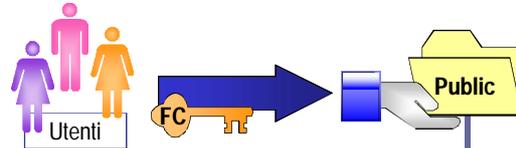
Gestione cartelle condivise

- Assegnare permessi a una cartella condivisa:
 - la cartella condivisa può risiedere su un hard disk formattato con NTFS, FAT o FAT32
 - gli utenti necessitano di permessi appropriati per accedere a file su un volume NTFS
- Si possono modificare i permessi di condivisione sulle cartelle:
 - Annullando la condivisione
 - Modificando il nome per la condivisione
 - Modificando i permessi
 - Creando condivisioni multiple per una cartella condivisa (per condivisioni multiple)
 - Rimuovere condivisioni (per condivisioni multiple)



UNIVERSITÀ DEGLI STUDI ROMA TRE
Dipartimento di Informatica e Automazione

Combinazione permessi NTFS e Cartelle Condivise



Regole da ricordare:

- I permessi NTFS sono richiesti su unità NTFS
- Gli utenti per accedere devono possedere i corretti permessi NTFS e di condivisione
- Si applica il più restrittivo dei permessi tra i permessi di condivisione cartella o i permessi NTFS

Cartelle amministrative condivise

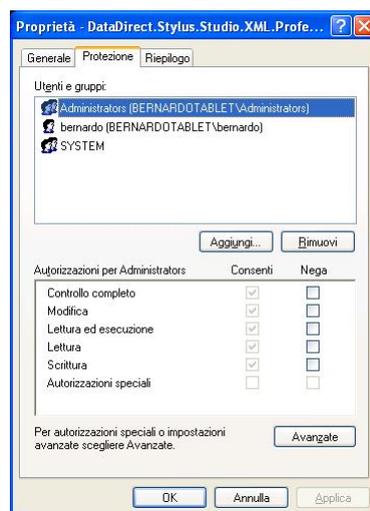
- Gli amministratori usano cartelle amministrative condivise per effettuare attività amministrative
- Le cartelle amministrative condivise sono nascoste dai normali utenti
- Gli amministratori dispongono del controllo completo

Share	Purpose
C\$, D\$, E\$	La root di ogni partizione è condivisa automaticamente
Admin\$	La cartella C:\Winnt è condivisa come Admin\$
Print\$	La cartella contenente i driver per la stampante è condivisa come Print\$ (creata con la prima stampante)

Permessi NTFS Avanzati

NTFS Avanzato

- Impostazioni Avanzate ci si accede tramite le proprietà di un file o di una cartella
- La finestra delle **Impostazioni Avanzate** è suddivisa in **4** schermate
 - **Autorizzazioni**
 - **Controllo**
 - **Proprietario**
 - **Autorizzazioni Valide**



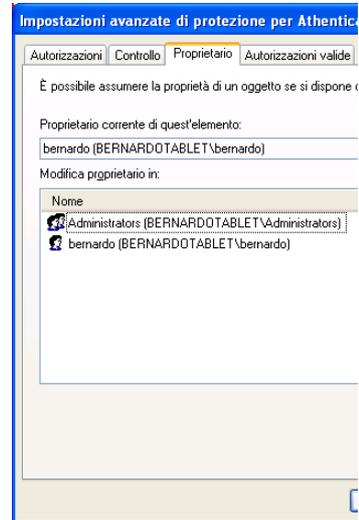
Impostazioni avanzate NTFS

- **Autorizzazioni**

Da qui e' possibile aggiungere, modificare o rimuovere **ACL**. Le due caselle di controllo in basso invece specificano le opzioni di **Ereditarieta'** dei permessi, permettendo all'oggetto di ereditare le impostazioni dall'oggetto in cui e' contenuto, e propagandole agli oggetti in esso contenuti.

- **Controllo**

Se e' stata abilitata la **Policy** relativa ai controlli sugli accessi, specifica in che modo attuare questo controllo.



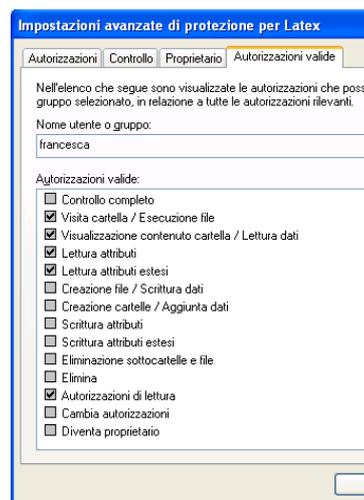
Impostazioni avanzate NTFS (2)

- **Proprietario**

Permette di specificare il proprietario dell'oggetto. Anche qui e' possibile apportare la modifica anche ad oggetti figli.

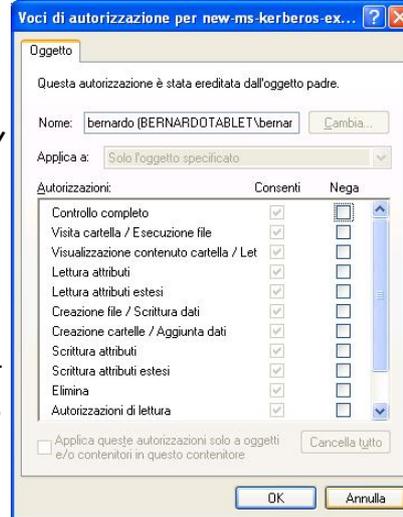
- **Autorizzazioni Valide**

Permette, una volta selezionato un utente o un gruppo, di visualizzare quali siano le effettive autorizzazioni applicate all'utente o gruppo per quell'oggetto. E' molto utile verificare le autorizzazioni, in modo da essere certi che non ci siano autorizzazioni troppo "elastiche" su oggetti che dovrebbero rimanere privati.



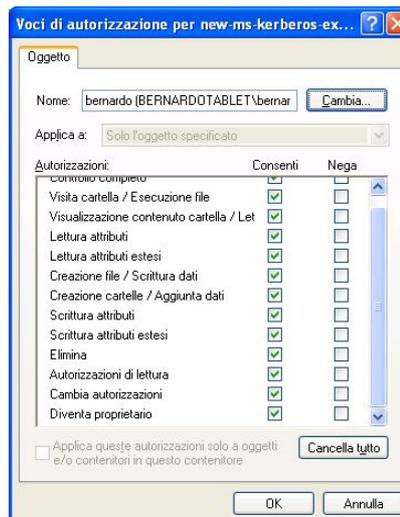
Impostazioni avanzate NTFS (3)

- **Controllo Completo**
L'insieme di tutti i permessi
- **Visita Cartelle/Esecuzione File**
Permette di attraversare le directory ed eseguire i file.
- **Visualizzazione contenuto cartella / Lettura dati**
Consente di visualizzare il contenuto di una directory o di leggere un file.
- **Lettura Attributi**
Permette di visualizzare le proprietà di un file o di una directory.
- **Creazione file / Scrittura dati**
Permette di creare file all'interno di una directory o di scrivere altri dati in un file.
- **Creazione cartelle / Aggiunta dati**
Consente di creare nuove sottocartelle o di aggiungere dati alla fine di un file.
- **Scrittura attributi**
Consente di modificare gli attributi di un file



Impostazioni avanzate NTFS (4)

- **Scrittura attributi estesi**
Consente di impostare gli attributi estesi su file o cartelle
- **Eliminazione sottocartelle e file**
Si applica solo alle cartelle e consente di cancellare gli oggetti contenuti in esse.
- **Elimina**
Consente di eliminare l'oggetto.
- **Lettura Autorizzazione**
Consente di leggere le autorizzazioni di un file.
- **Cambia autorizzazioni**
Consente la modifica delle ACL
- **Diventa proprietario**
Consente di ottenere la proprietà di un oggetto.
Il proprietario può sempre modificare le ACL degli oggetti



Proprietà (Ownership) di un file

- L'utente che crea un file ne è anche il Proprietario (Owner)
- Il proprietario del file è l'unico, oltre agli utenti del gruppo Administrators, che ha diritto di impostarne le autorizzazioni
- Attraverso la scheda *Proprietario*, presente nelle impostazioni avanzate, è possibile visualizzare la proprietà del file o della cartella
- La proprietà può essere modificata in due modi:
 - Un amministratore può diventare proprietario dell'oggetto in qualsiasi momento attraverso la scheda proprietario
 - Il proprietario corrente può concedere l'Autorizzazione speciale *Diventa proprietario* al nuovo proprietario che potrà assumerla in qualsiasi momento

Impostazioni avanzate di protezione per Docs

Autorizzazioni | **Proprietario** | Autorizzazioni valide

È possibile assumere la proprietà di un oggetto se si dispone

Proprietario corrente di quest'elemento:
bernardo (BERNARDOTABLET\bernardo)

Modifica proprietario in:

Nome
francesca (BERNARDOTABLET\francesca)

Sostituisci proprietario in sottocarterni ed oggetti

Autorizzazioni di base e avanzate

Autorizzazioni speciali	Controllo completo	Modifica	Lettura/esecuzione	Visualizza contenuto cartella (solo cartelle)	Lettura	Scrittura
Attraversa cartelle/Esecuzione file	x	x	x	x		
Visualizzazione contenuto cartella/Lettura dati	x	x	x	x	x	
Lettura attributi	x	x	x	x	x	
Lettura attributi estesi	x	x	x	x	x	
Creazione file/Scrittura dati	x	x				x
Creazione cartelle/Aggiunta dati	x	x				x
Scrittura attributi	x	x				x
Scrittura attributi estesi	x	x				x
Eliminazione sottocartelle e file	x					
Eliminazione	x	x				
Autorizzazioni di lettura	x	x	x	x	x	x
Cambia autorizzazioni	x					
Diventa proprietario	x					