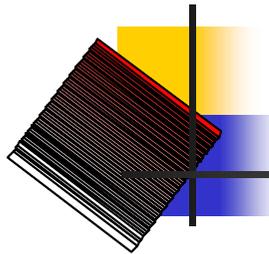




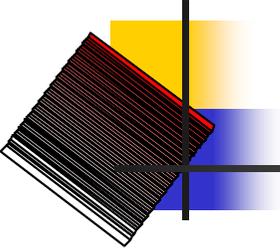
# Corso di Amministrazione di Reti A.A.2002/2003



# Argomenti

---

- ✍ Generalità NTFS
- ✍ Implementare la sicurezza di NTFS
- ✍ Implementare la condivisione di risorse
- ✍ Permessi locali e permessi sulle condivisioni NTFS
- ✍ Solaris: comandi "setfac" e "getfac"



# File system supportati da Windows NT

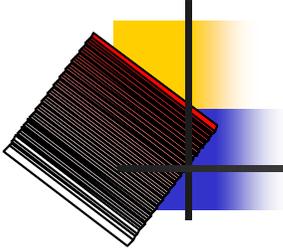
---

## ✎ File system FAT 16

- ✎ Supporta i nomi di file lunghi
- ✎ NON prevede alcuna protezione locale, ogni utente può accedere a tutti i files e directories
- ✎ Dimensione massima partizioni/file: 2.047 MByte

## ✎ File system NTFS

- ✎ Supporta i nomi di file lunghi
- ✎ Supporta la protezione locale
- ✎ Dimensione massima partizioni:
  - ✎ 16 esabyte (teorici)
  - ✎ 2 terabyte (effettivi)



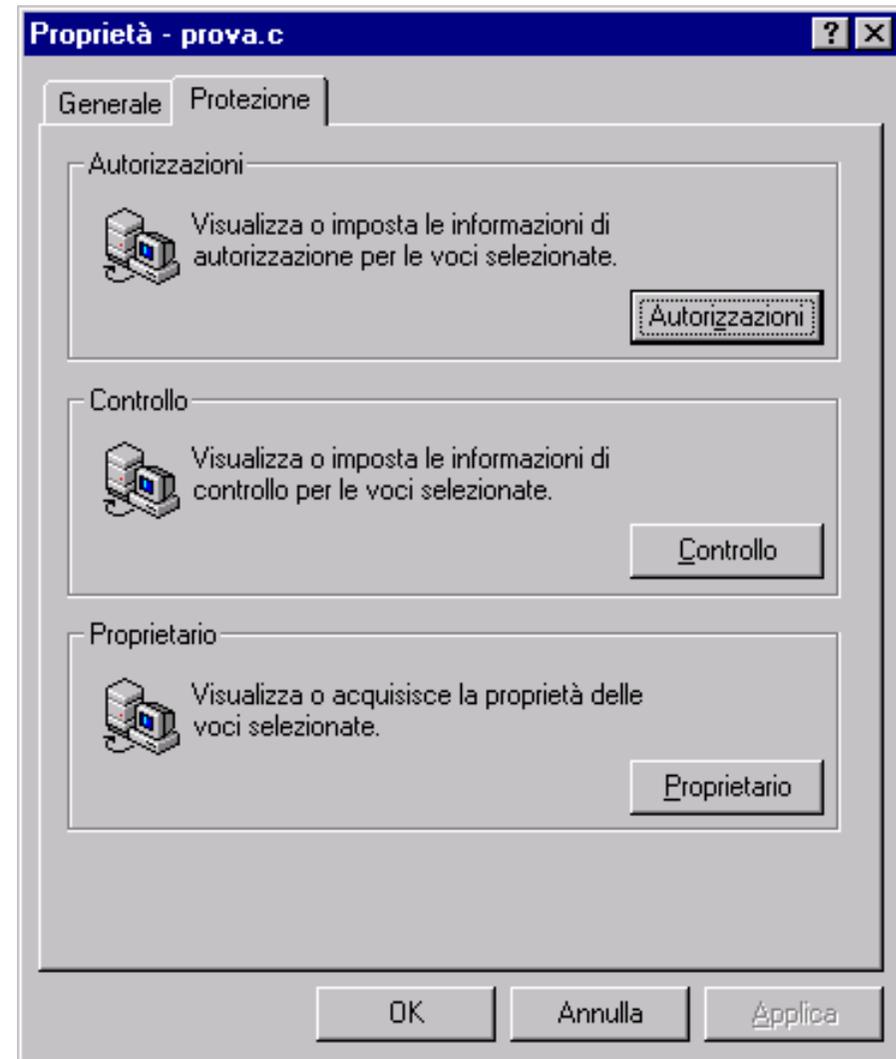
# Implementare la sicurezza di NTFS

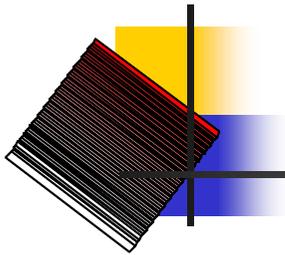
---

- ✍ Settare Directory o File Permissions
- ✍ Auditing

# Sicurezza NTFS: requisiti

- Disponibile solo su partizioni NTFS
- Settare le Permissions richiede:
  - 'Full Control'
  - 'Change Permissions'
  - 'Ownership'

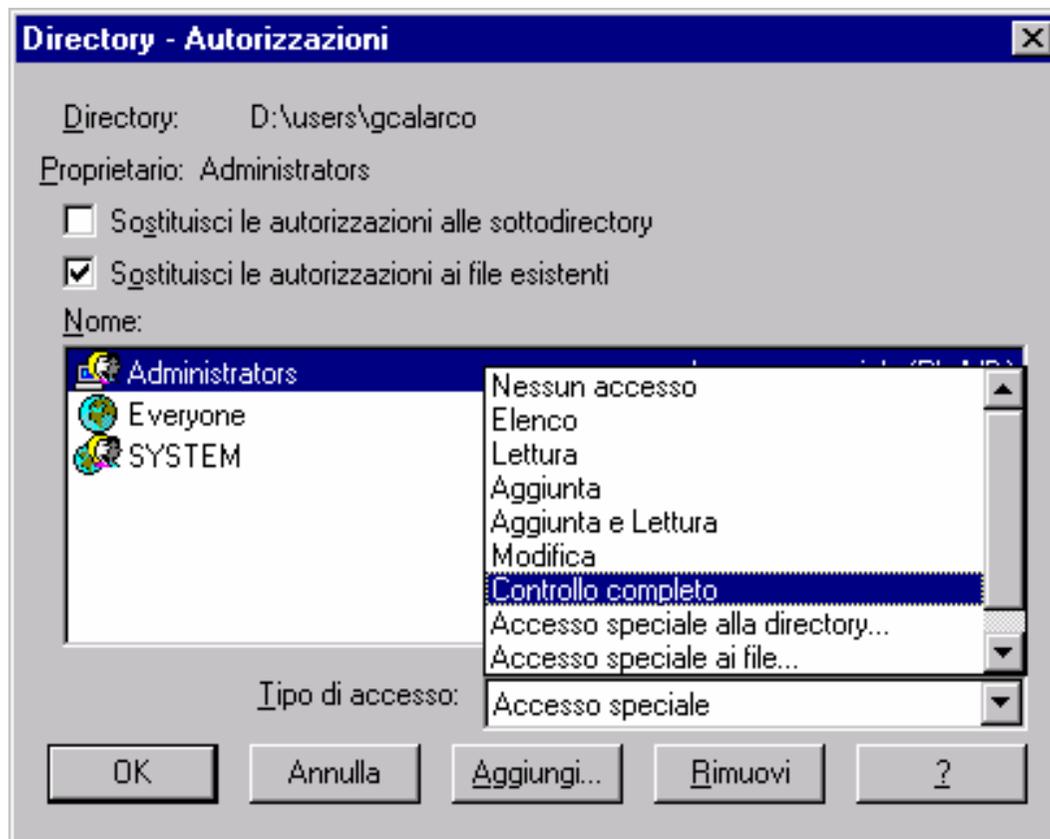




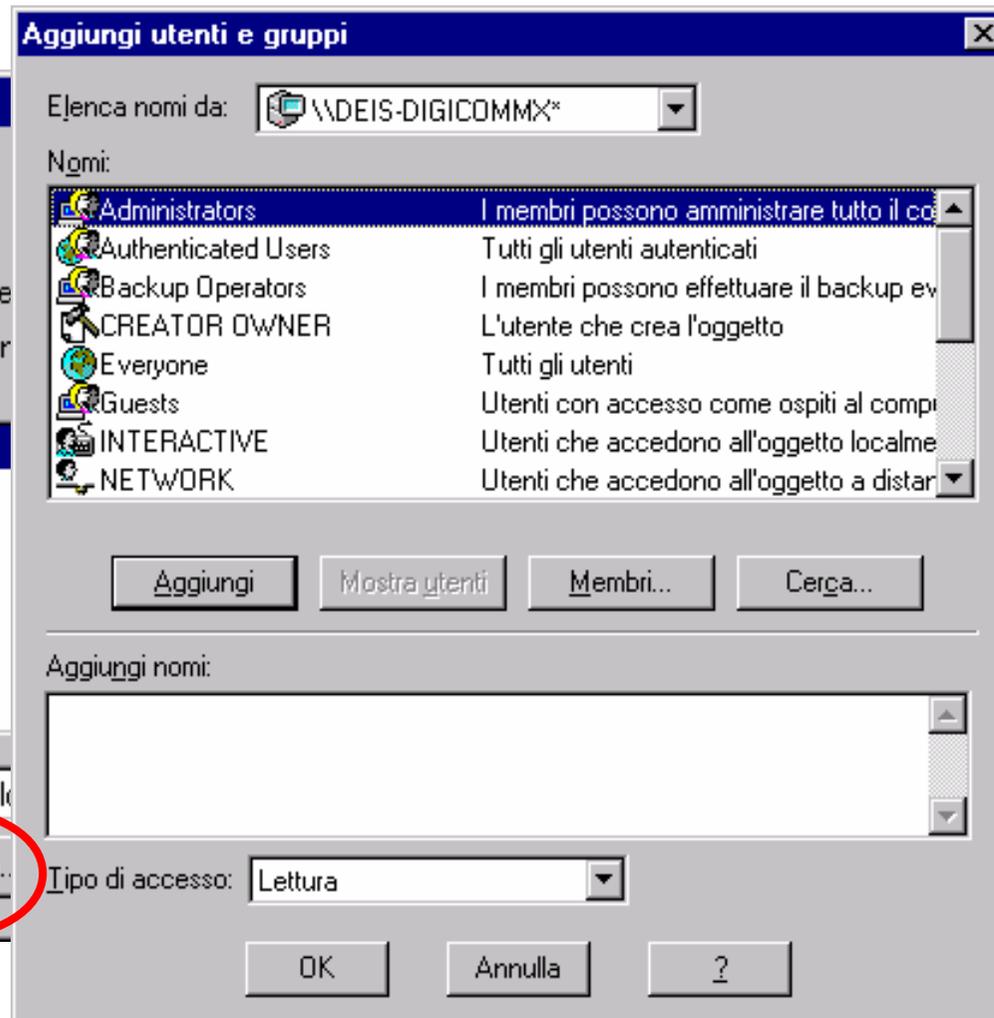
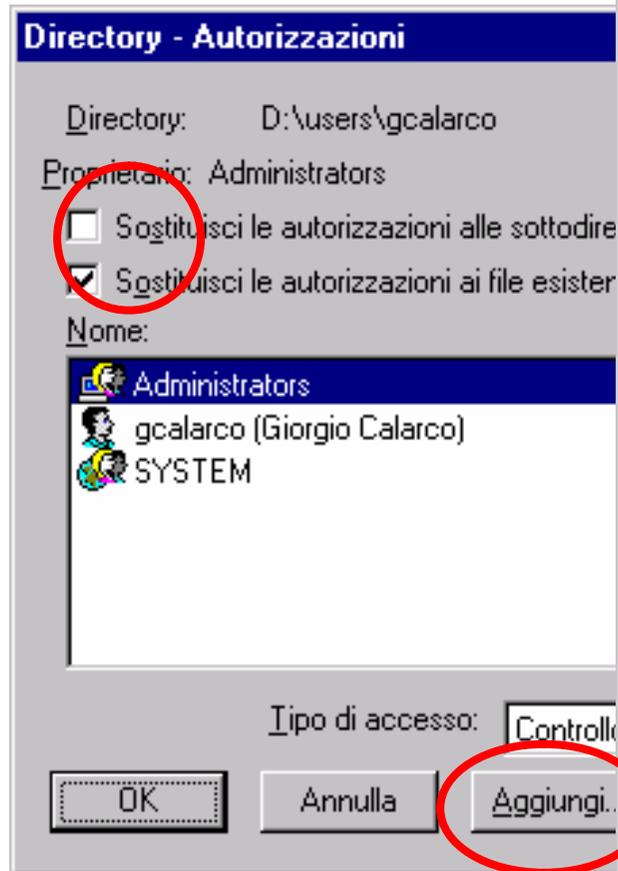
# Autorizzazioni di accesso alle cartelle

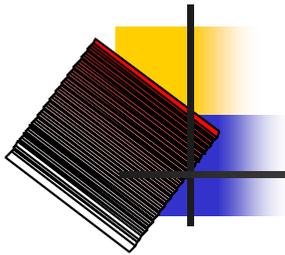
- ✎ Sulle cartelle è possibile impostare le seguenti **autorizzazioni standard**:
  - ✎ Nessun accesso (Nessuno)(Nessuno)
  - ✎ Elenco (RX)(Non specificato)
  - ✎ Lettura (RX)(RX)
  - ✎ Aggiunta (WX)(Non specificato)
  - ✎ Aggiunta e Lettura (RWX)(RX)
  - ✎ Modifica (RWXD)(RWXD)
  - ✎ Controllo completo (Tutti)(Tutti)
- ✎ Le autorizzazioni sono **cumulative**, ad eccezione dell'autorizzazione 'No Access' che ha la precedenza su tutte le altre. Se ad esempio un utente è membro di un gruppo a cui è stata concessa l'autorizzazione Lettura e di un gruppo a cui è stata concessa l'autorizzazione Modifica, l'utente disporrà dell'autorizzazione Modifica.
- ✎ **Nota:** I gruppi o gli utenti a cui è stata concessa l'autorizzazione 'Controllo completo' su una cartella sono in grado di eliminarne i file, indipendentemente dall'autorizzazione che li protegge.

# Settare i permessi di cartelle

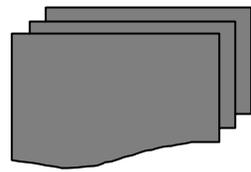


# Assegnazione di autorizzazioni

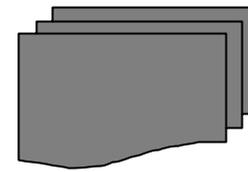
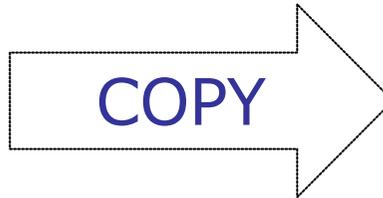




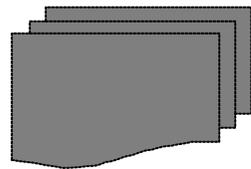
## Permessi dopo un copy/move di file (e directory)



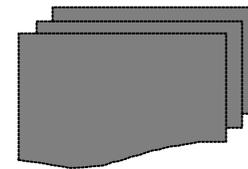
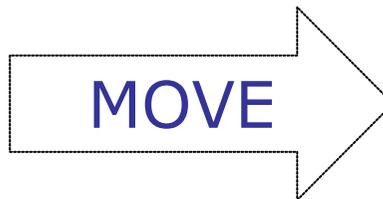
File1 = RWX



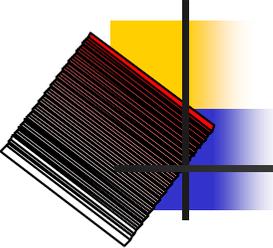
File1 = diritti del  
direttorio



File1 = RWX



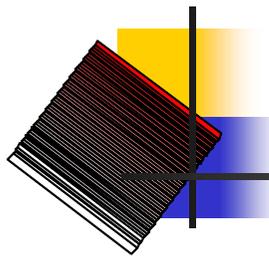
File1 = RWX



# Autorizzazioni di accesso ai files

---

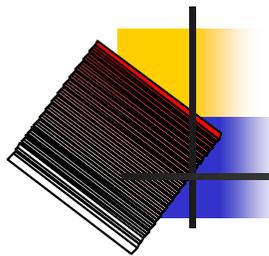
- ☞ Sui file è possibile impostare le seguenti **autorizzazioni standard**:
  - ☞ Nessun accesso (Nessuno)
  - ☞ Lettura (RX)
  - ☞ Modifica (RWXD)
  - ☞ Controllo completo (Tutti)
- ☞ Impostando le autorizzazioni di accesso a un file sarà possibile specificare il tipo di accesso al file consentito a un gruppo o a un utente. Altrimenti, un file eredita le autorizzazioni proprie della cartella in cui è stato creato.
- ☞ Le autorizzazioni sono **cumulative**, ad eccezione dell'autorizzazione 'Nessun accesso' che ha la precedenza su tutte le altre. Se ad esempio un utente è membro di un gruppo a cui è stata concessa l'autorizzazione Lettura e di un gruppo a cui è stata concessa l'autorizzazione Modifica, l'utente disporrà dell'autorizzazione Modifica.



## Autorizzazioni di accesso ai files

---

- ✎ Quando si imposta un'autorizzazione standard, accanto a questa viene visualizzato un insieme di **autorizzazioni individuali**. Quando ad esempio per un file viene impostata l'autorizzazione Lettura, verrà visualizzata la sigla (RX), indicante le autorizzazioni Lettura e Esecuzione sul file.
- ✎ **Nota**  
I gruppi o gli utenti cui si concede l'autorizzazione Controllo completo su una cartella possono eliminarne i file, indipendentemente dall'autorizzazione che li protegge.



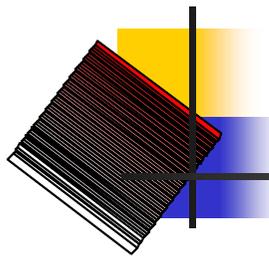
## Interazione permessi utente e gruppi

Permessi di Michael	Permessi di Research	Permessi di Development	Permessi di Michael (effettivi)
Read	Read	-	Read
Write	-	Read	Read & Write
-	Change	Read	Change
Take Ownership	Read	Change	Take Ownership & Change
No Access	Read	Change	No Access
Change	No Access	Change	No Access

RWX = Read, Write, Execute

DPO = Delete, Permissions, Ownership

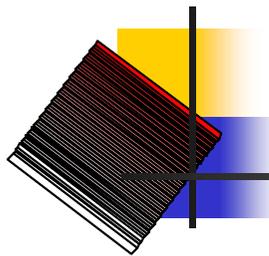
Change = RWXD



## Ownership di files e directories

---

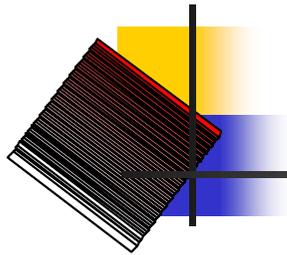
- ✍ L'Owner di files e directories ha il pieno controllo (Full Control)
- ✍ Administrator può sempre prendere l'ownership
- ✍ L'Owner può assegnare le permissions per prendere l'Ownership
- ✍ Nota bene:
  - ✍ Gli utenti che creano un file o una directory ne detengono l' Ownership



# Assegnazione di autorizzazioni NTFS

---

- ✎ Autorizzazioni NTFS predefinite:
  - ✎ A Everyone viene assegnato automaticamente Full Control
  - ✎ I nuovi file ereditano le autorizzazioni della cartella in cui vengono creati (questo vale anche per i files che vengono copiati in un direttorio)

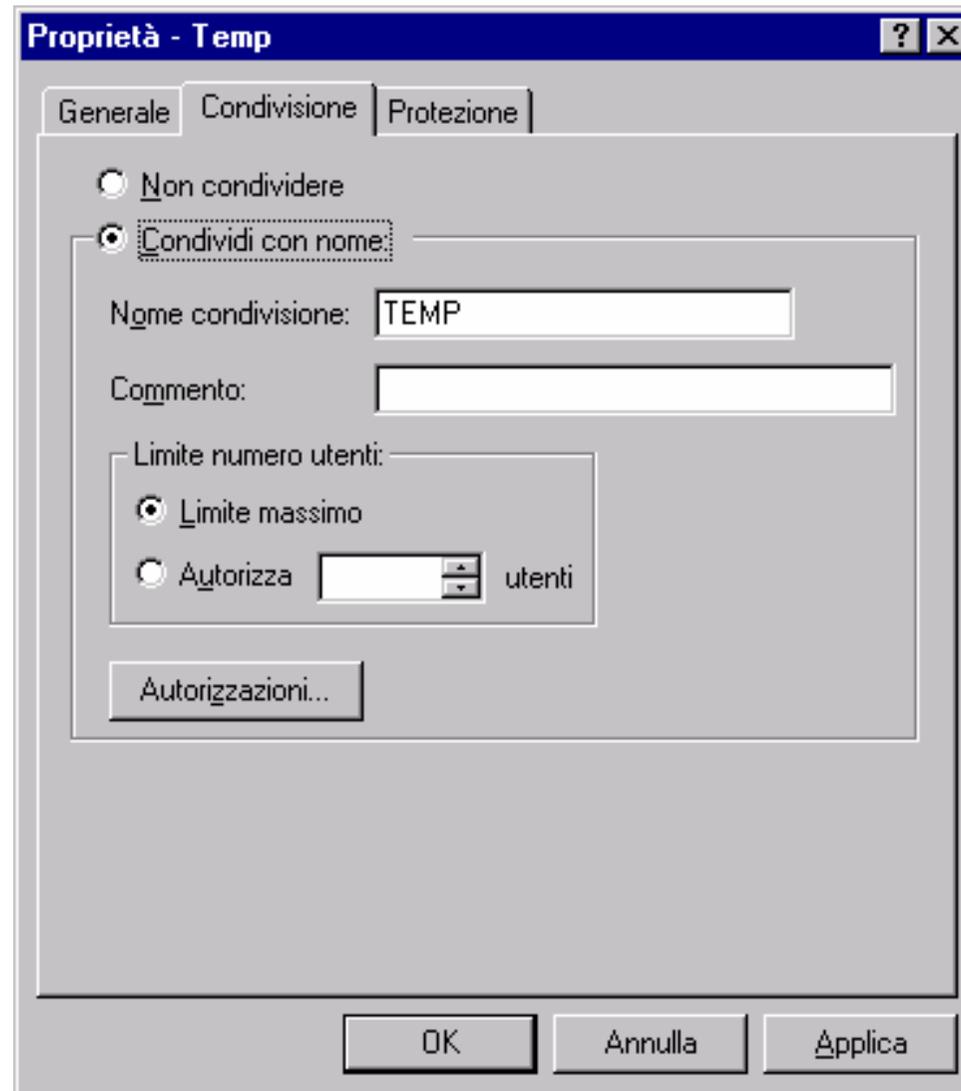


## Condivisione di risorse

---

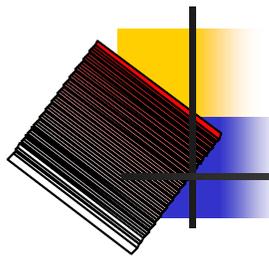
- ✍ Share = directory (folder) condivisa
- ✍ Diritti necessari per attivare le condivisioni:
  - ✍ Administrators
  - ✍ Server Operators (se in un dominio)
  - ✍ Power Users (se in un workgroup)
- ✍ Gli Users devono avere almeno il permesso List per fruire della directory condivisa

# Condividere un direttorio



# Permessi di una share

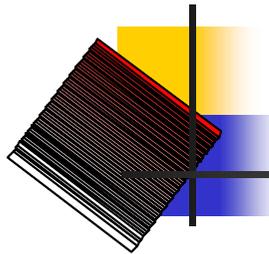




## Permessi locali vs. Permessi sulla condivisione

	Permessi Assegnati	Permessi di Michael
Permessi Share C:\temp	Everyone: Read Michael: Change	<b>Change</b> (RWXD)
Permessi locali	Everyone: Read Michael: Read	<b>Read</b> (RX)
Permessi effettivi		<b>Read</b> (RX)

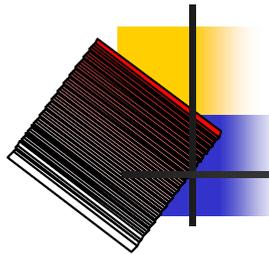
L'autorizzazione effettiva è quella più restrittiva !



# Setfacl

---

- ✎ Modifica l'Access Control List (ACL)  
Sintassi: `setfacl -s acl_entries file`
- ✎ `acl_entries` sono ACL separate da virgole
- ✎ Affinché l'ACL venga effettivamente applicata occorre essere l'owner del file
- ✎ Es.: `setfacl -s user:www:rwX,user::rwX,group::r-x,mask:rwX,other:r-x download/`
- ✎ Attenzione a `mask`: filtra i diritti di `user` aggiuntivo e `group`. Se `user:www:rw-` e `mask:r--` -> l'effetto è che `www:r--`
- ✎ Più comoda l'opzione `-m`, che aggiunge l'`acl` ai diritti preesistenti. Es. `setfacl -m user:www:rwX foo`



# Getfac

---

- ✎ Sintassi: getfac file
- ✎ Esempio: getfac download/

# file: download/

# owner: help

# group: suexec

user::rwx

user:www:rwx                   #effective:rwx

group::r-x                   #effective:r-x

mask:rwx

other:r-x