

6105 Windows Server og datanett

Leksjon 6b Filsystemet NTFS og rettigheter

- NTFS-rettigheter, ACL og eierskap til filer
- NTFS-rettigheter arves og kombineres
- Avanserte NTFS-rettigheter
- NTFS-rettigheter ved kopiering og flytting
- Komprimerte filer og mapper i NTFS
- Diskkvoter i NTFS



Pensum:

- Kvisli: Windows Server og nettverk, kapittel 9 Filsystemet NTFS og rettigheter

Relevante lenker

Microsoft Docs:

- [Managing Permissions](#)
- [File and folder permissions](#)

Andre kilder

- [Technet Magazine: How IT works NTFS Permission](#)
- [Understanding NTFS permissions](#)
- [Copying and moving files and folders on NTFS partitions](#)

Problemstillinger på filtjener

Vi har nå registrert brukerkontoer og gruppert dem i grupper

Hvordan sikrer vi at brukerne får tilgang til de data de har behov for på filtjeneren?

Hvordan sikrer vi at brukerne ikke har tilgang til mer enn de har behov for?

Hvorfor har vi behov for å begrense tilgangen?

Problemstillinger i Windows

Windows er et flerbruker operativsystem

- Flere brukere kan være innlogget på samme maskin
 - » På samme maskin til forskjellig tidspunkt
 - » På samme tidspunkt f.eks. via fjerntilkobling (terminaltjener)
- Flere brukere kan aksessere data på samme maskin via nettet
 - » F.eks. via delte mapper

Behov for å styre tilgang til data, bl.a.

- Begrense tilgang til "sensitive" data
- Sikre at bruker får tilgang til felles data
- Hindre at andre får innsyn i brukerens "private" data

Løses med tilgangsrettigheter

- Alle flerbruker OS har mekanismer for dette.
- I Windows finnes to typer: NTFS-rettigheter og delingsrettigheter

NTFS-rettigheter

Filsystemet NTFS har innebygget sikkerhet med NTFS-rettigheter

- I motsetning til FAT og FAT32 der alle autentiserte brukere har tilgang til hele filsystemet

NTFS-rettigheter kan settes på

- Mapper (kataloger)
- Filer

NTFS-rettigheter kan gis til

- Brukerkontoer
- Grupper
- Maskiner

NTFS-rettigheter til filer

Read

- Åpne og lese innhold i filen
- Se filens egenskaper, eierskap og rettigheter

Read & Execute

- Alle Read rettigheter
- + Kjøre filen hvis den er en programfil

Write

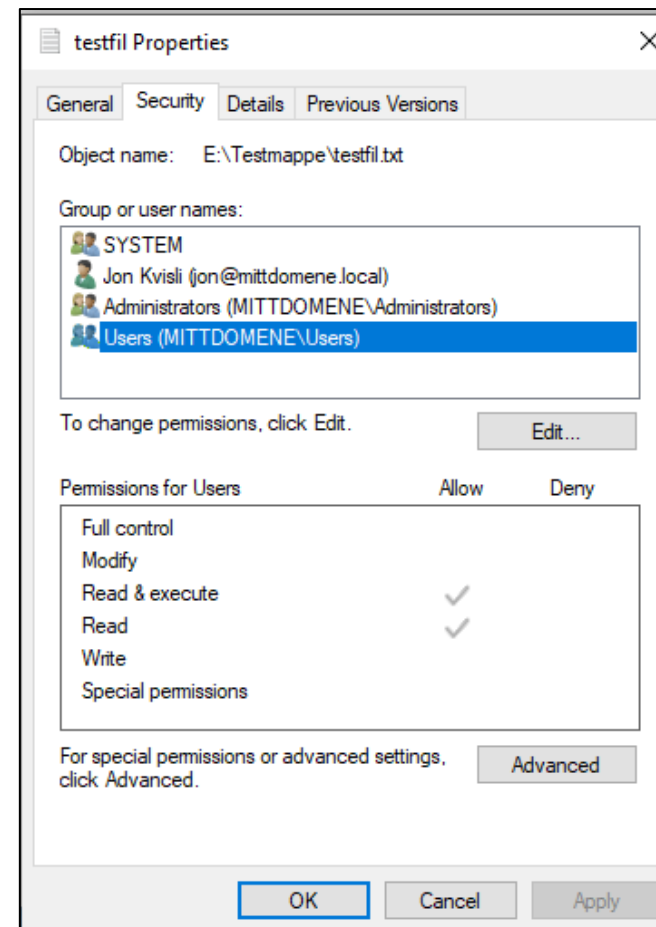
- Endre filen (overskrive med nytt innhold)
- Endre filens egenskaper
- Se filens eierskap og rettigheter
- Obs: Gir ikke Read rettighet !

Modify

- Alle Read & Execute + Write rettigheter
- + Slette filen

Full Control

- Alle rettigheter
- også til å endre filens rettigheter.



NTFS-rettigheter til mapper

List Folder Content

- Se navn på filer og undermapper (ikke innhold)

Read

- Åpne og se innhold i undermapper og filer
- Se mappens egenskaper, eierskap og rettigheter
- Obs: Må ha LFC for å se mappens filer!

Read & Execute

- Som List Folder Content + Read

Write

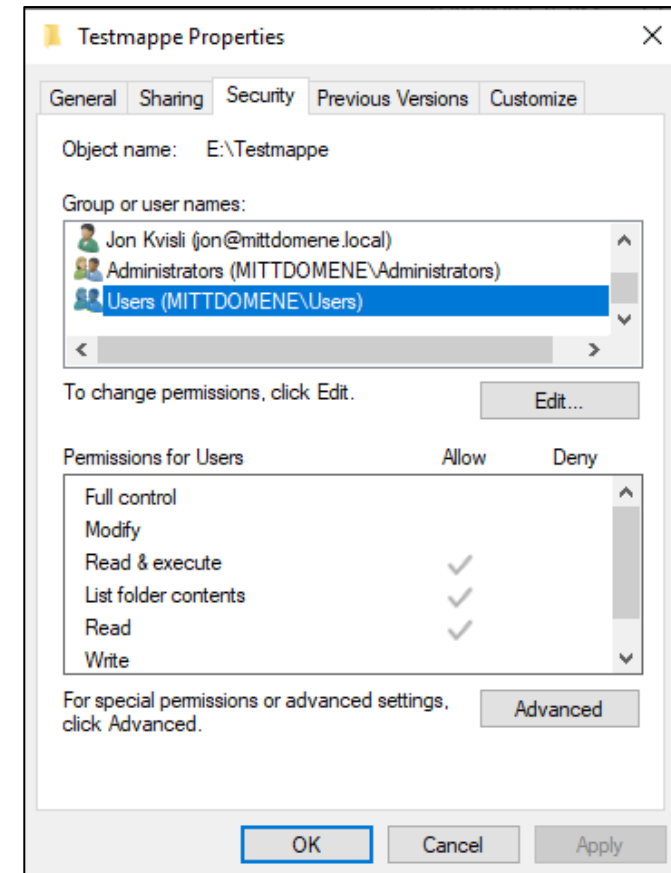
- Lage nye filer og undermapper
- Endre mappens egenskaper
- Se mappens eierskap og rettigheter
- Obs: Gir ikke Read rettighet !

Modify

- = Read & Execute + Write + slette mappen

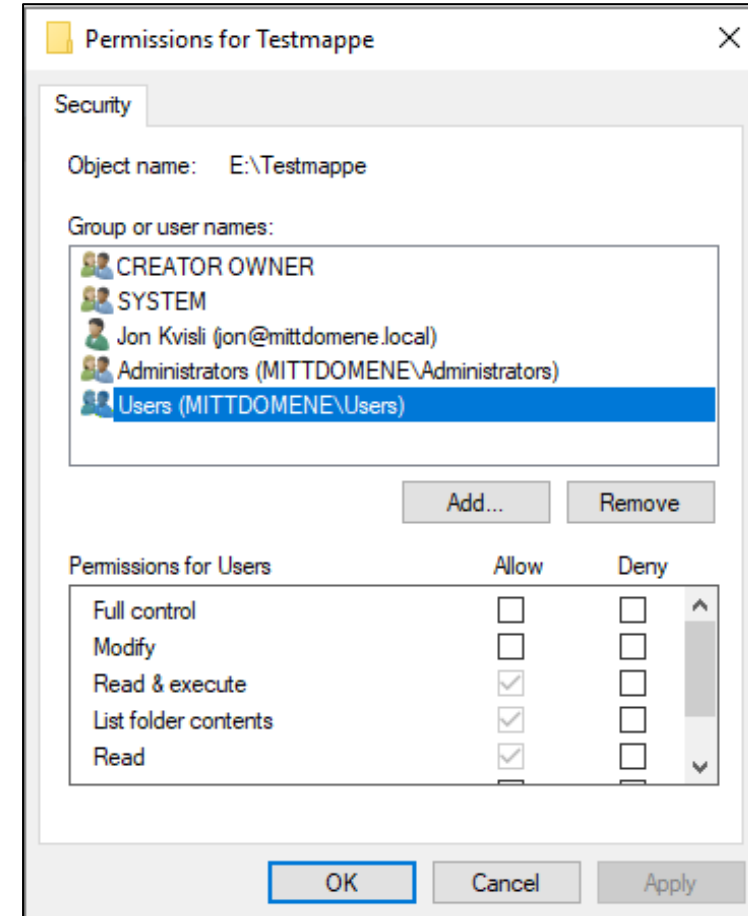
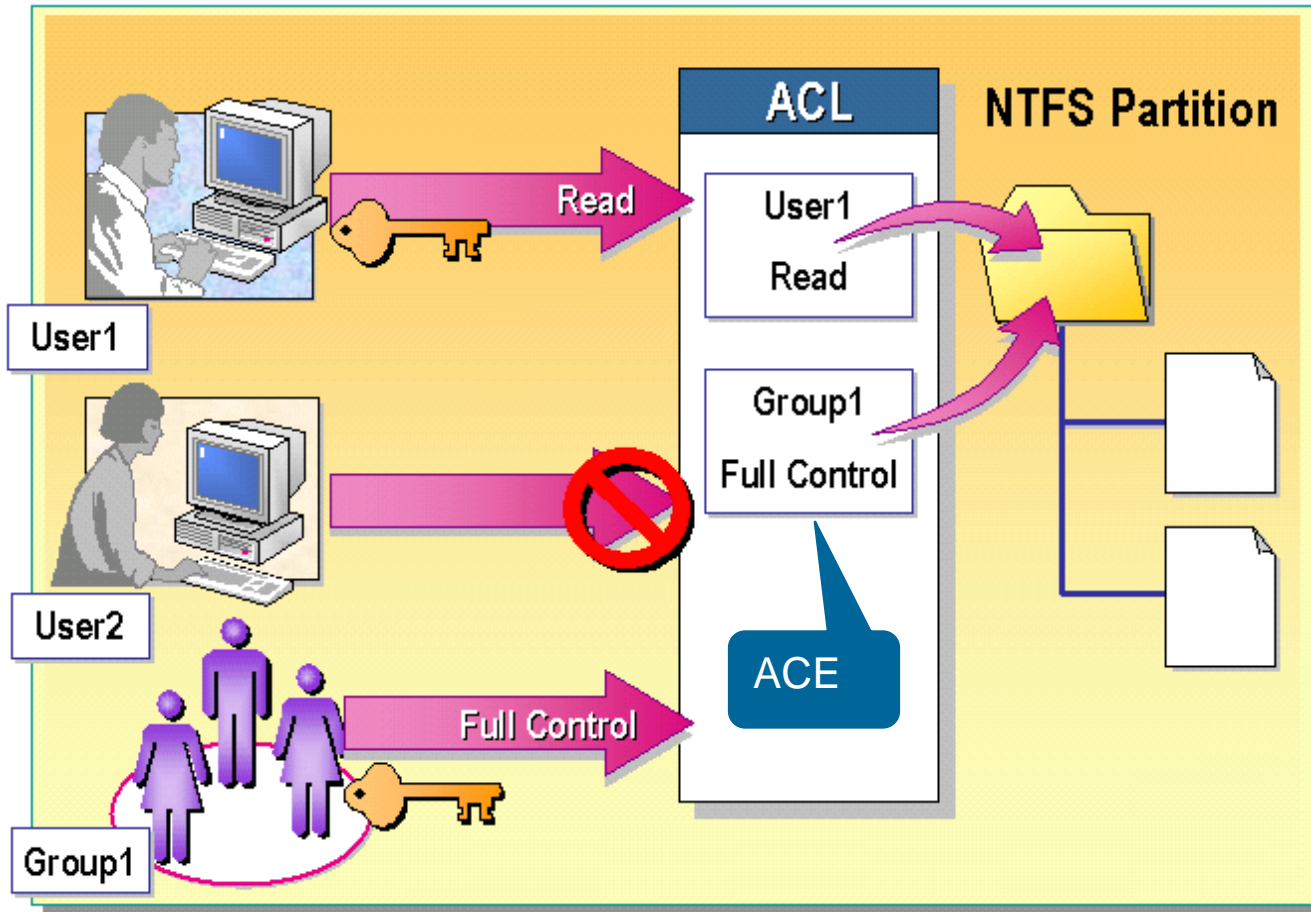
Full Control

- Alle rettigheter, også å endre mappens rettigheter



ACL - Access Control List

ACL editor



ACL - Access Control List

Tilgangskontrolliste

- **Liste over rettigheter for hver mappe og fil i et NTFS filsystem (volum)**
 - Alle filer og mapper har hver sin ACL
 - Lagres som en del av informasjonen i NTFS-filsystemet
- **Lagrer informasjon om:**
 - Alle brukere og grupper som har rettigheter til ressursen
 - Hvilke rettigheter disse har
- **ACL er grunnlaget for autorisering i Windows**
 - Når en bruker aksesserer en fil/mappe sjekkes ACLen for å finne ut om brukeren har rettighet til denne.
- **ACE Access Control Entry**
 - "Rad" i ACL-listen, som knytter en konto og en rettighet til ressursen
- **ACL editor**
 - Vindu/dialogboks for å redigere innholdet i ACL listen (administrere rettigheter)

Eierskap til filer

Alle filer og mapper har en eier (owner)

- Den som oppretter mappen/filen blir automatisk eier
- Eier kan alltid endre rettigheter
- Eierskap kan overføres til andre

Rettigheter knyttet til eierskap

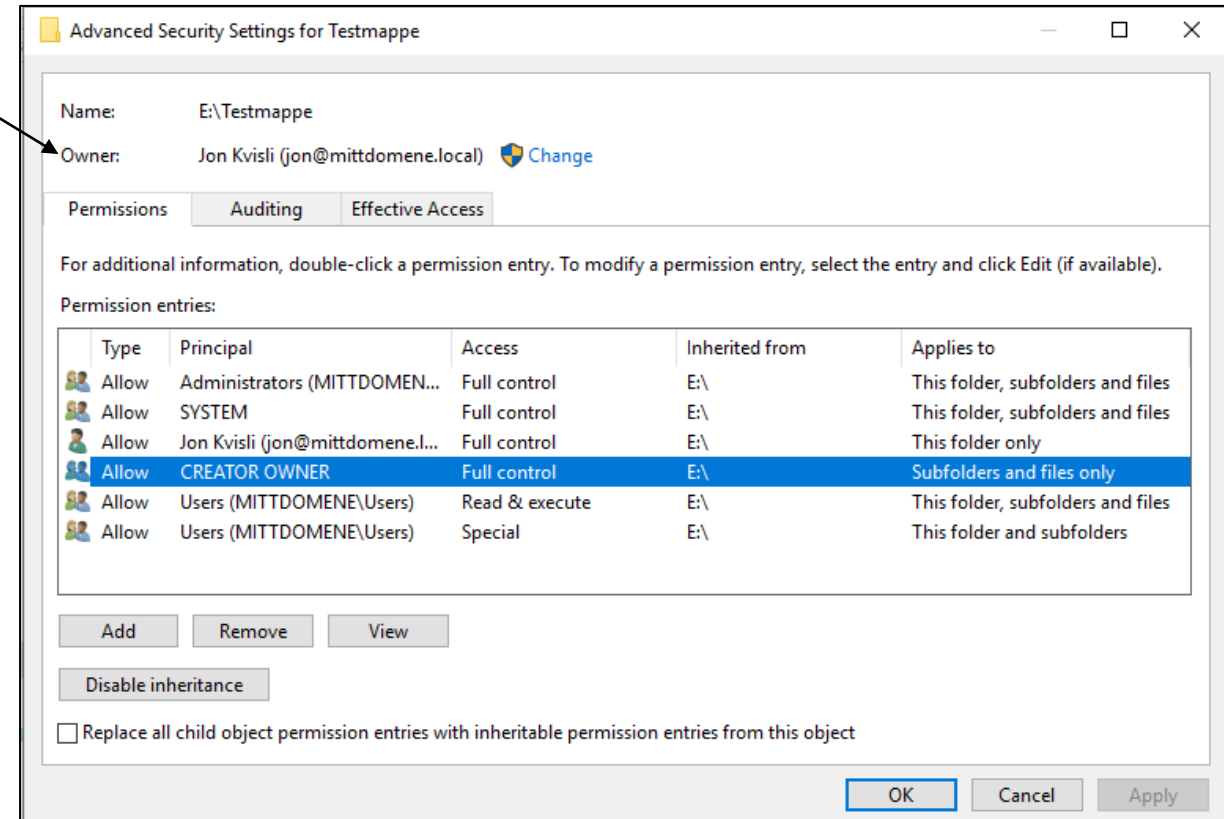
– *Take Ownership*

- » Brukere med denne rettigheten, kan overta eierskap
- » Administrator kan alltid ta eierskap til filer/mapper

Roller knyttet til eierskap

– *CREATOR OWNER*

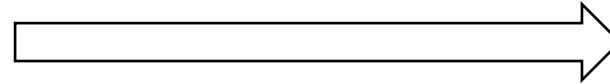
- » Kan gis NTFS-rettigheter som en bruker/gruppe



Administrere NTFS-rettigheter

Hvordan tildele rettigheter?

- Properties for filen/mappen
- Fanen *Security* + knappen **Edit**



Rettigheter kan gis til

- Brukere (lokale og i domenet)
- Grupper (lokale og i domenet)
- Maskiner (i domenet)

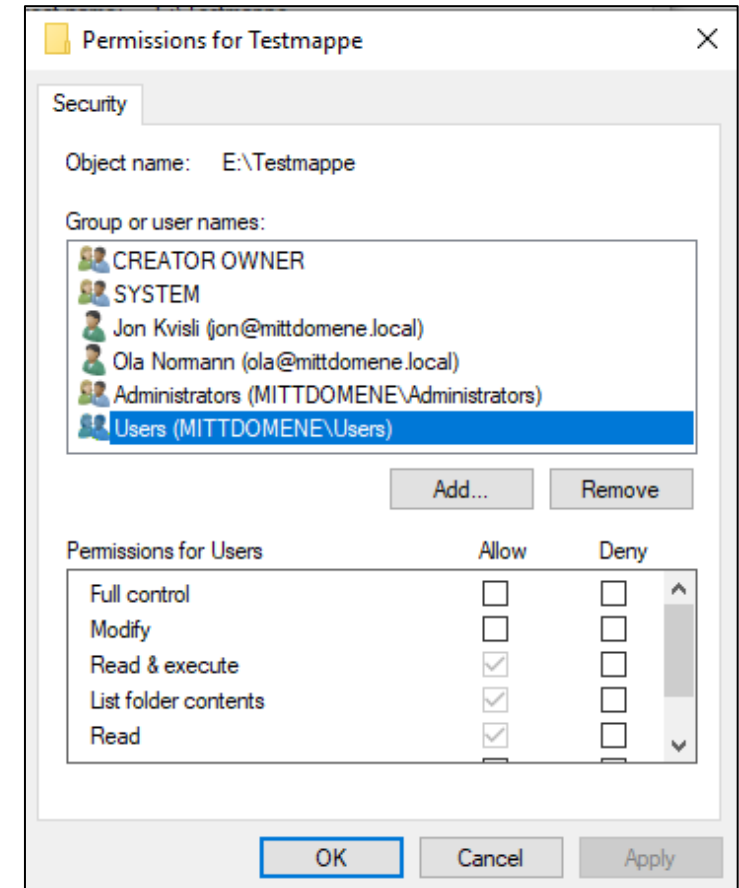
Rettigheter kan:

- Tildeles (*Allow*)
- Nektes (*Deny*)

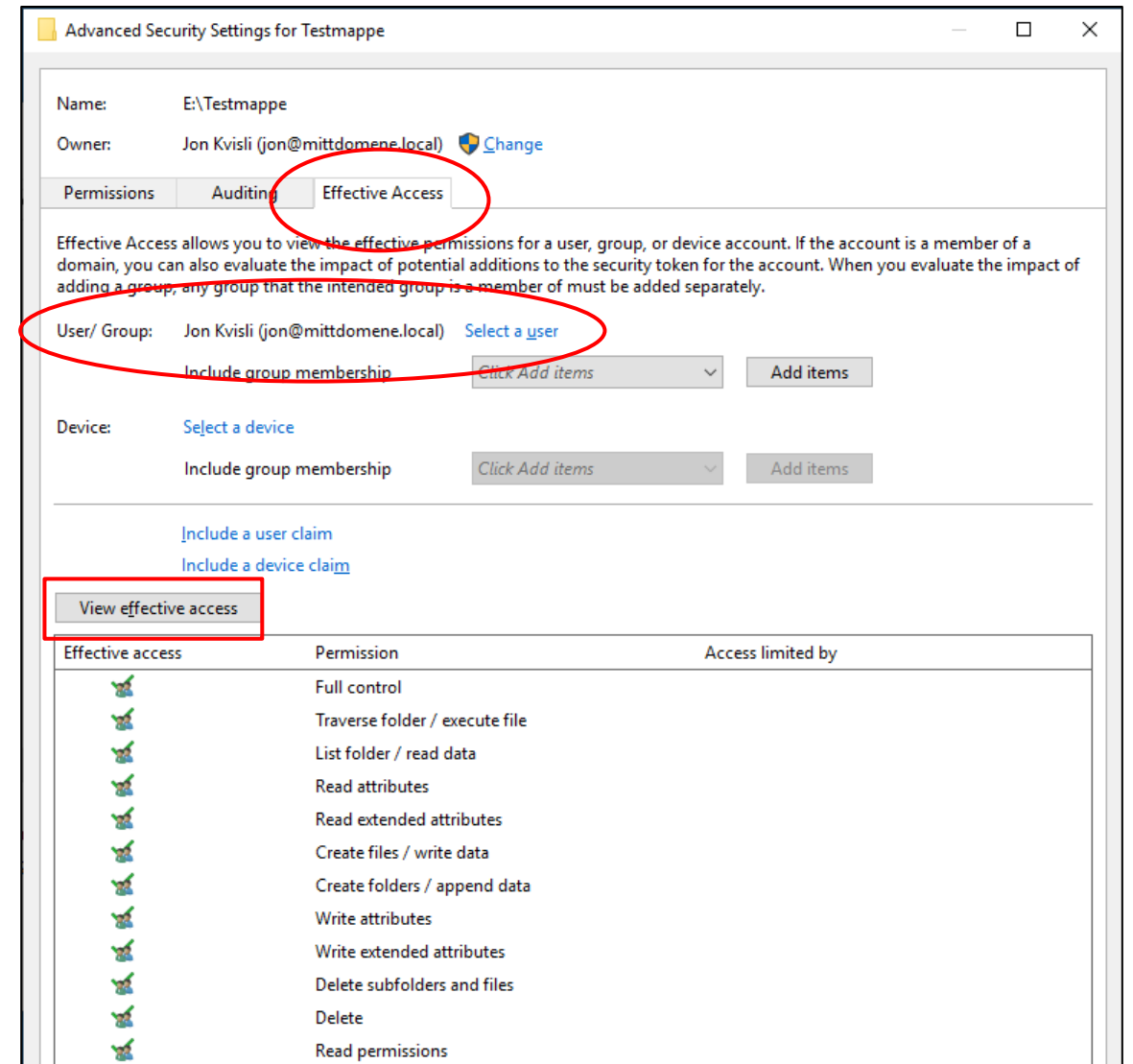
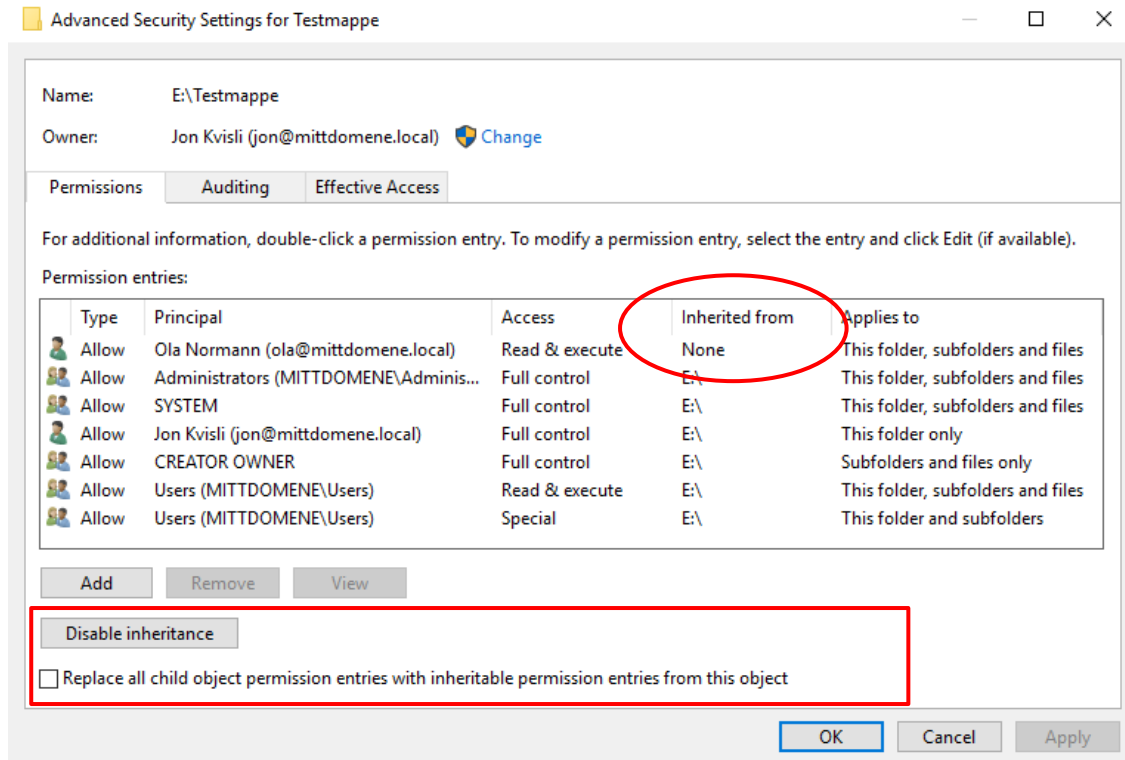
Deny overstyrer allow!

Hvem kan tildele NTFS-rettigheter til filer og mapper?

- Gruppen **Administrators**
- Eier av filen / mappen (**CREATOR OWNER**)
 - » dvs. den som har laget filen / mappen
- Brukere som har fått rettigheten **Full Control** til filen / mappen
 - » Egentlig den avanserte NTFS-rettigheten Change Permissions (se senere foil)



NTFS-rettigheter arves



NTFS-rettigheter arves

Arvede rettigheter

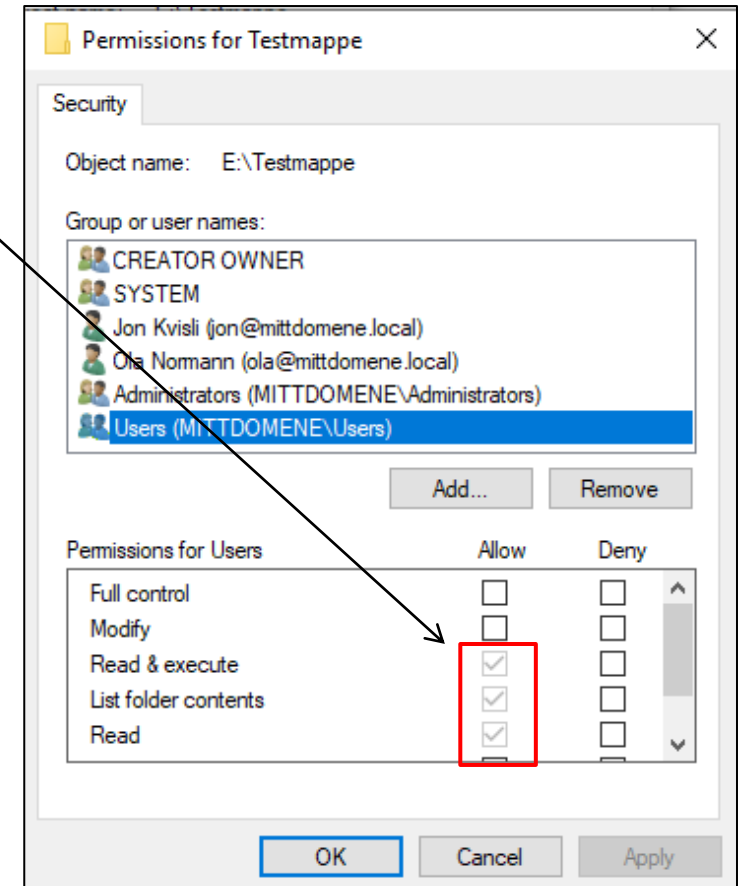
- Nye filer og undermapper arver "mor-mappens" rettigheter
- Endring av rettigheter til "mor-mappe" påvirker også undermappen
- Viser som "grå bokser" i ACL-editoren
- Kan unngås ved å aktivt fjerne arvede rettigheter

Eksplisitte rettigheter

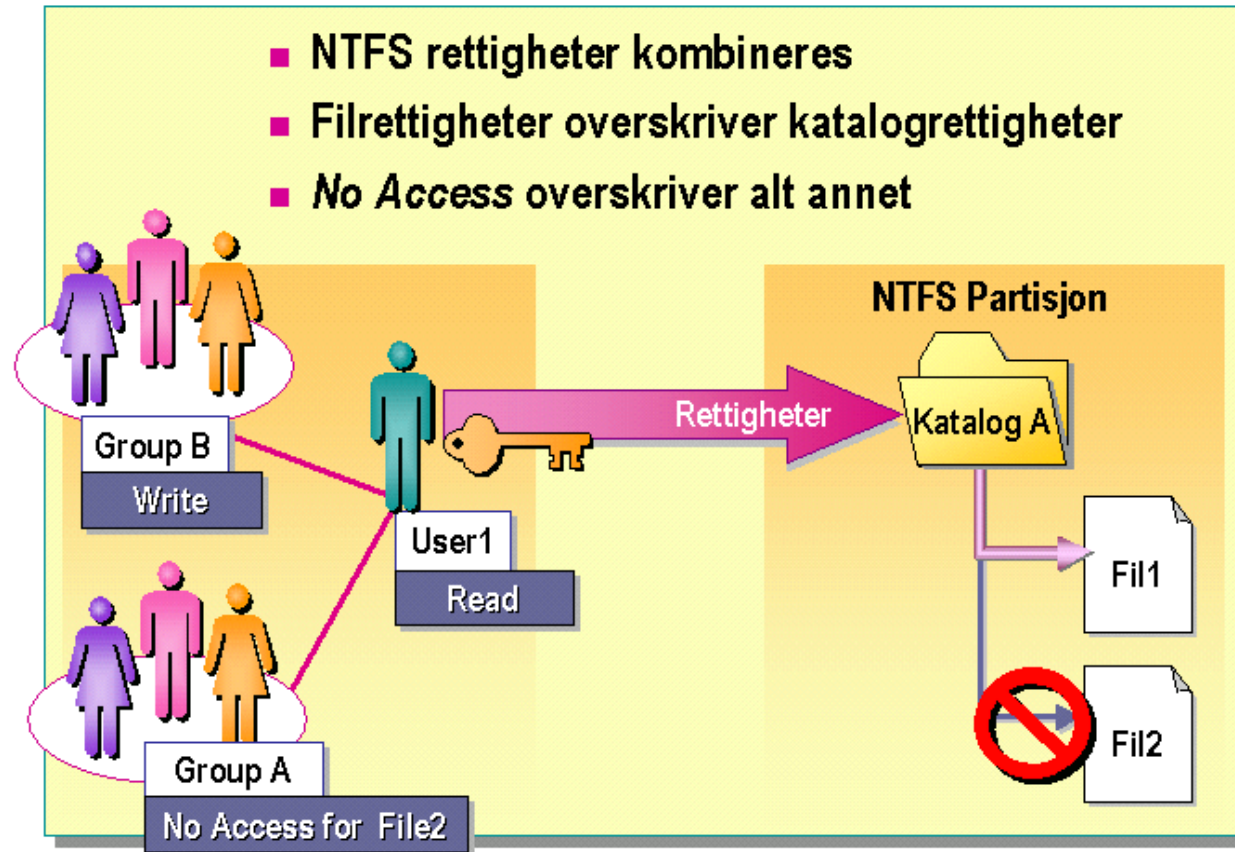
- Gis direkte til hver fil/mappe
- Kommer i tillegg til arvede rettigheter
- Overstyrer arvede rettigheter hvis konflikt

Effektive rettigheter

- "Summen" av arvede og eksplisitte rettigheter
- Bestemmer hva man faktisk får tilgang til.



NTFS-rettigheter kombineres



Brukerens rettigheter kombineres med rettighetene til alle grupper som brukeren er medlem av.

NTFS-rettigheter kombineres

Rettighetene er *kumulative*, dvs:

- En brukers *effektive rettigheter* =
 - » rettighetene gitt til brukeren + rettighetene gitt til grupper som brukeren tilhører
- Eksempel: **User1**'s effektive rettighet blir *Read* og *Write* til **Katalog A**
 - » Fordi **User1** er medlem i **Group B** som har *Write* til **Katalog A**

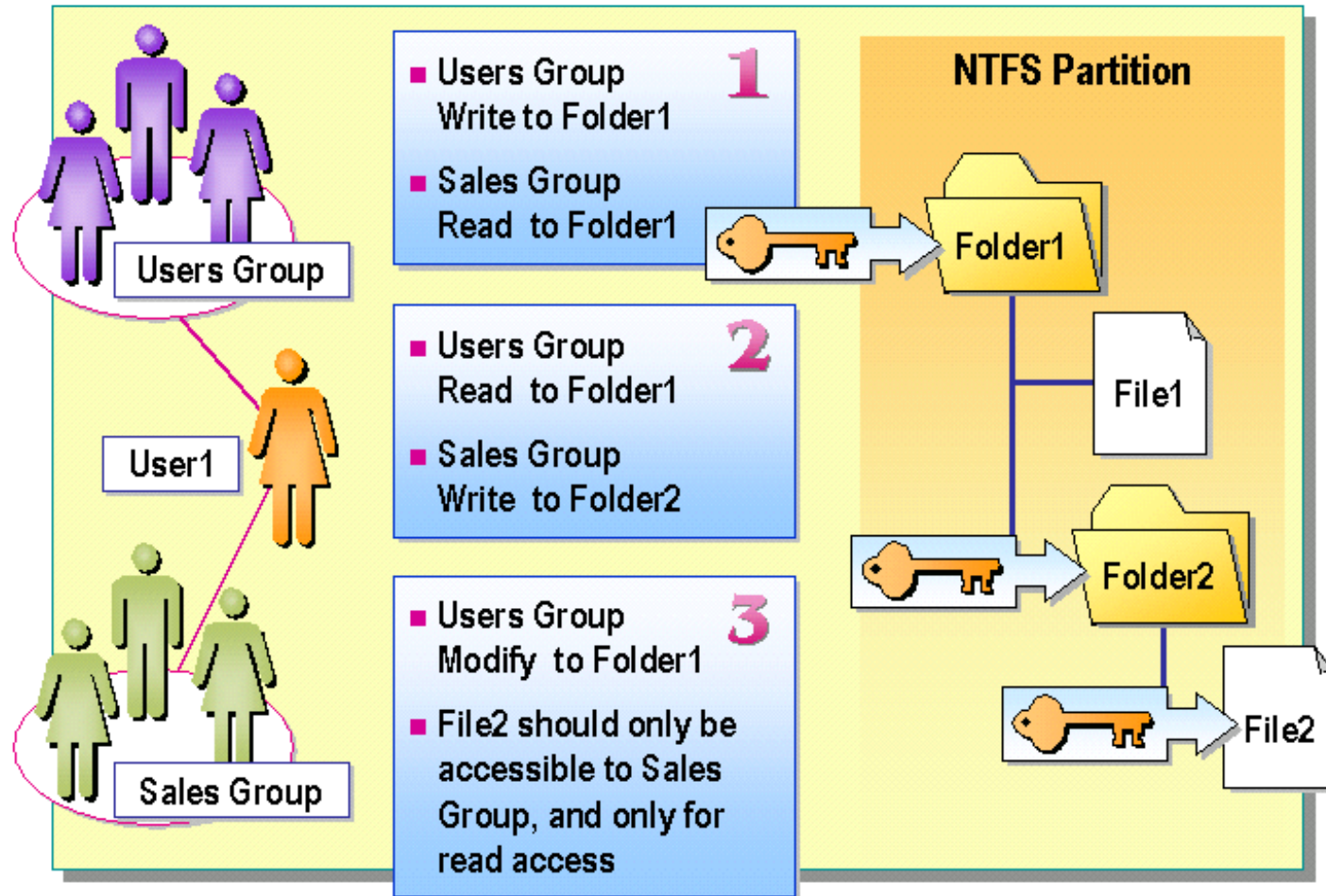
Deny overstyrer Allow

- *Deny Full Control* = *No access*
 - » overstyrer alle andre rettigheter

Rettigheter på filer overstyrer rettigheter på mappen

- Eksempel: **User1** har *No Access* (= *Deny Full Control*) til **Fil2**
 - » Fordi **User1** er medlem i **Group A** som har *No Access* til **Fil2**
 - » Fordi rettigheter til filer overstyrer mapperettigheter

Oppgaver



Oppgave 1: Hvilken rettighet har *User1* til *Folder1*?

Oppgave 2: Hvilken rettighet har *User1* til mappen *Folder2*?

Oppgave 3: Hva kan du gjøre for at gruppen *Sales* har rettigheten *Read* til filen *File2*?

Avanserte NTFS-rettigheter (advanced permissions)

NTFS-rettighetene er egentlig sammensatt av mer detaljerte (avanserte) rettigheter

Avanserte NTFS-rettigheter:

- Full control
- Traverse folder / execute file
- List folder / read data
- Read attributes
- Read extended attributes
- Create files / write data
- Create folders / append data
- Write attributes
- Write extended attributes
- Delete subfolders and files
- Delete
- Read permissions
- Change permissions
- Take ownership

Sjeldent behov for dette nivået

- Kan settes med *Edit* under *Advanced Security Settings* og **Show advanced permissions**

Permission Entry for Testmappe

Principal: Ola Normann (ola@mittdomene.local) [Select a principal](#)

Type: Allow

Applies to: This folder, subfolders and files

Advanced permissions: [Show basic permissions](#)

<input type="checkbox"/> Full control	<input type="checkbox"/> Write attributes
<input checked="" type="checkbox"/> Traverse folder / execute file	<input type="checkbox"/> Write extended attributes
<input checked="" type="checkbox"/> List folder / read data	<input type="checkbox"/> Delete subfolders and files
<input checked="" type="checkbox"/> Read attributes	<input type="checkbox"/> Delete
<input checked="" type="checkbox"/> Read extended attributes	<input checked="" type="checkbox"/> Read permissions
<input type="checkbox"/> Create files / write data	<input type="checkbox"/> Change permissions
<input type="checkbox"/> Create folders / append data	<input type="checkbox"/> Take ownership

Only apply these permissions to objects and/or containers within this container [Clear all](#)

Add a condition to limit access. The principal will be granted the specified permissions only if conditions are met.

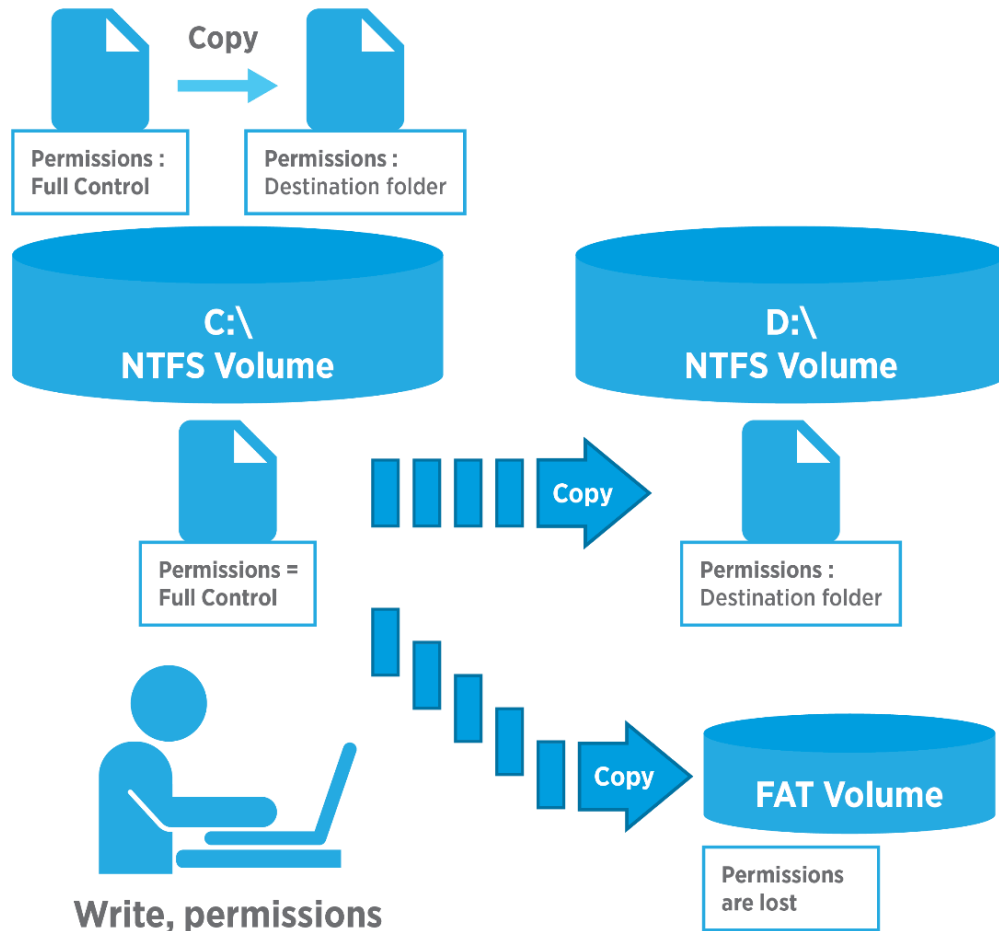
[Add a condition](#)

OK Cancel

Avanserte NTFS-rettigheter

Avanserte NTFS-rettigheter på mapper/filer	Full Control	Modify	Read & Execute	List Folder Contents	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

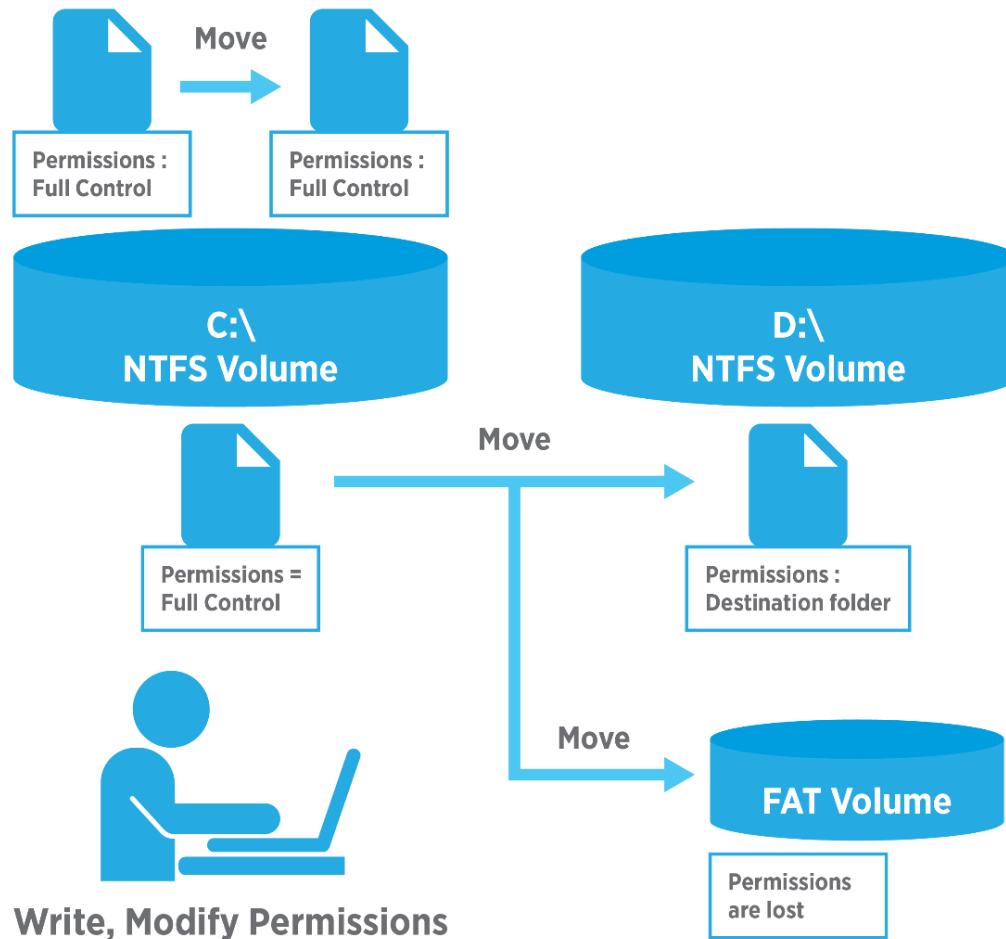
NTFS-rettigheter ved kopiering



- Rettigheter kopieres **ikke** fra originalen til kopien!
- Kopien overtar (arver) **alltid** rettigheter fra målmappen (*destination folder*)

- Hvis du kopierer filer/mapper til et volum med FAT eller FAT32 filsystem, mister kopien alle NTFS-rettigheter (ingen NTFS-rettigheter å arve)

NTFS-rettigheter ved flytting



- Hvis en fil flyttes innen **samme** NTFS-volum:
 - » Filen **beholder** sine *eksplisitte* rettigheter
 - » I tillegg arver den rettigheter fra målmappen (*destination folder*)
 - » Og: filen mister eventuelle *arvede* rettighetene fra fra-mappen
- Flytting til annet volum = kopiering, dvs. kopien får kun arvede rettigheter fra målmappen
- Hvis en fil flyttes til et volum med FAT eller FAT32 filsystem, mister kopien alle NTFS-rettigheter

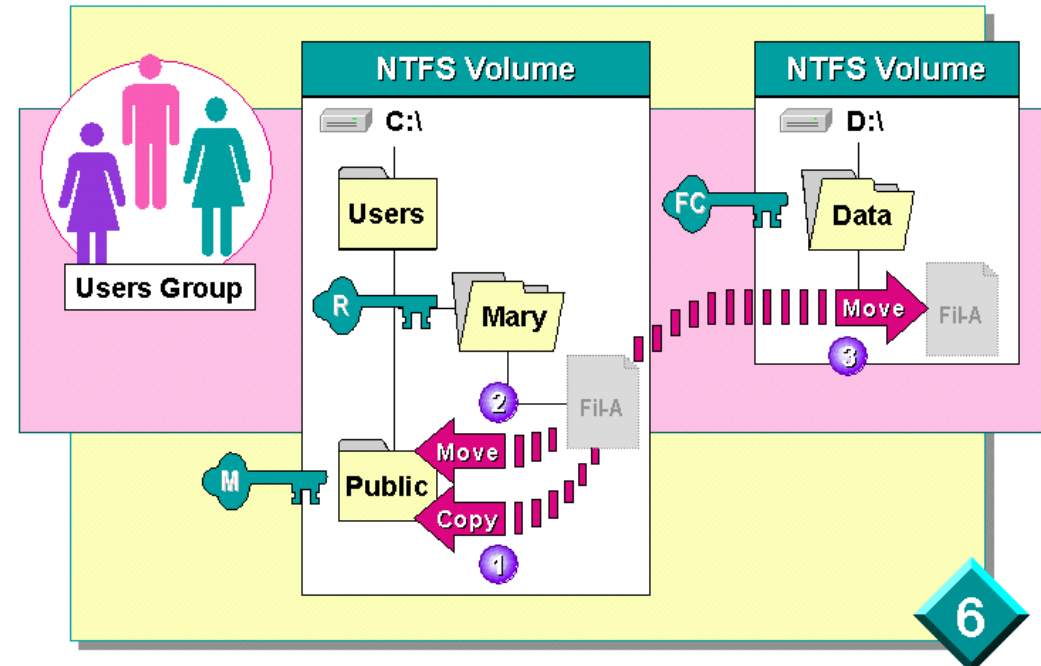
Oppgaver

Rettigheter for gruppen Users

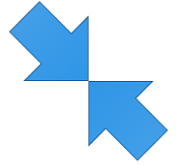
- Rettigheten *Read* for mappen **C:\Users\Mary** og alle filene i den
- Rettigheten *Modify* for mappen **C:\Public**
- Rettigheten *Full Control* for mappen **D:\Data**

Oppgaver:

- Hvilken tilgangsrettighet har gruppen **Users** til **Fil-A** hvis den kopieres til **C:\Public** ?
- Hvilken tilgangsrettighet har gruppen **Users** til **Fil-A** hvis at den flyttes til **C:\Public** ?
- Hvilken tilgangsrettighet har gruppen **Users** til **Fil-A** hvis den er flyttes til **D:\Data** ?



Komprimerte filer og mapper



Komprimere

- På NTFS-volumer kan filer og mapper komprimeres
- Windows utfører komprimering og dekomprimering automatisk
- Skjult for bruker og programmer

Hensikt

- Spare diskplass

Ulempe

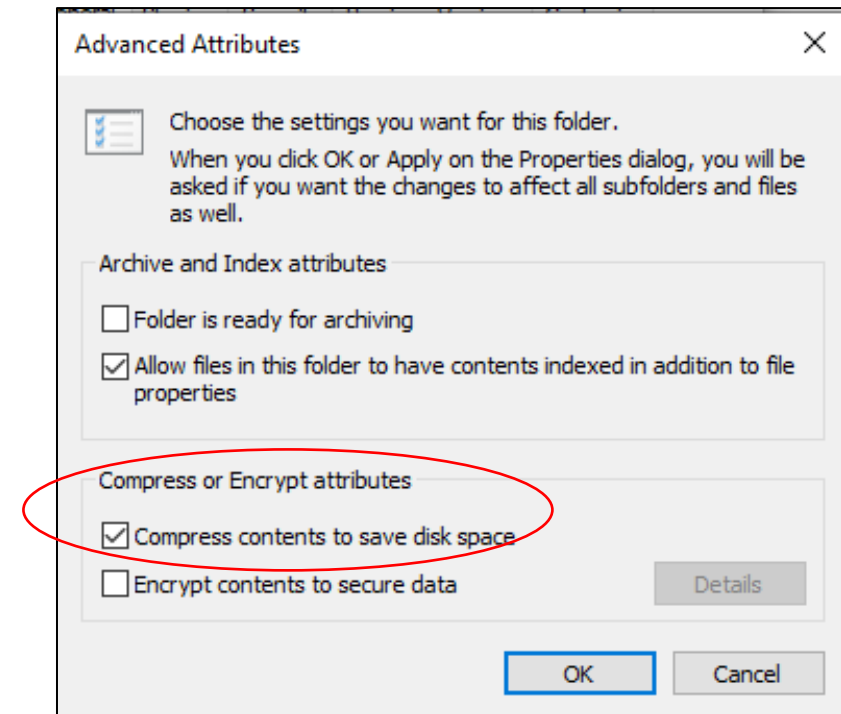
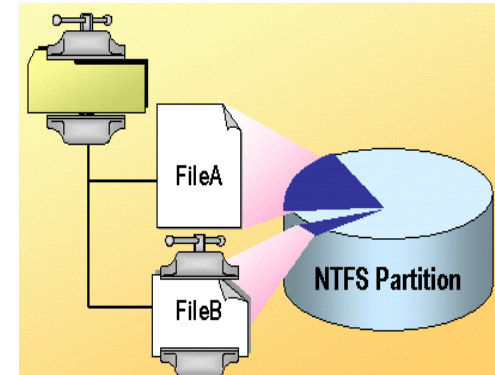
- Skrivning og lesing går langsommere

Angis i Windows Utforsker

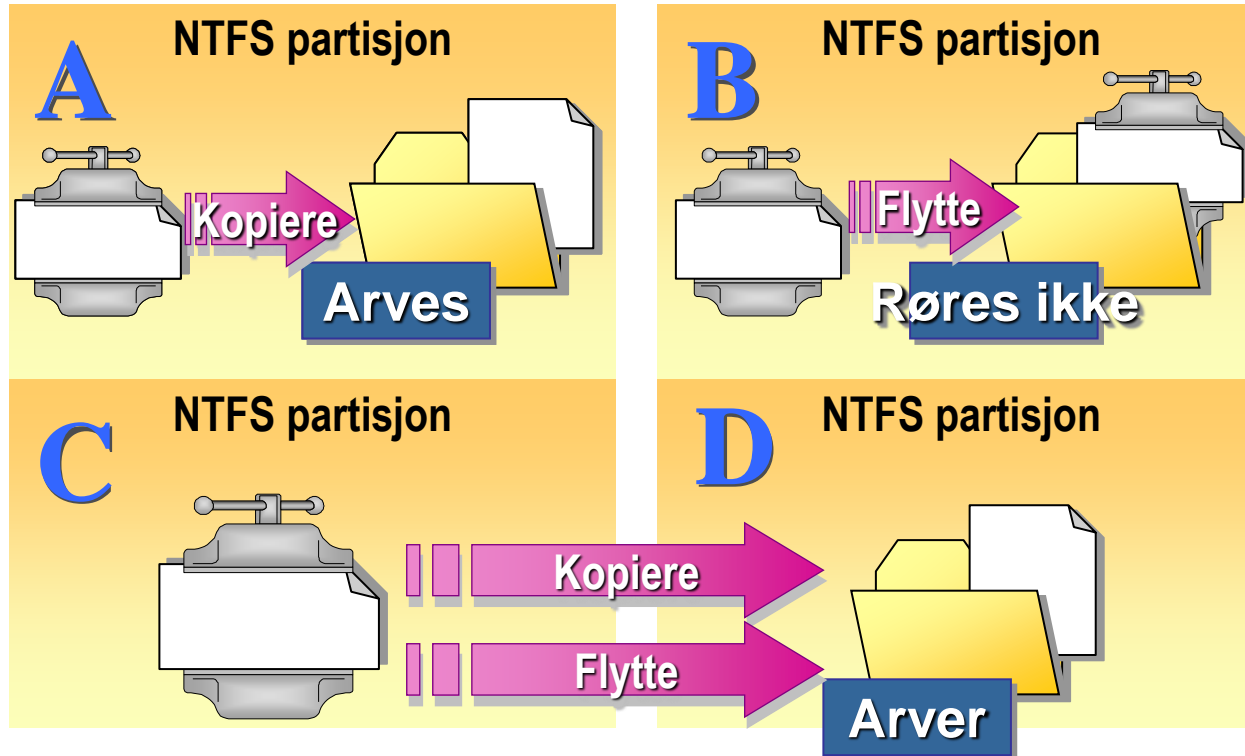
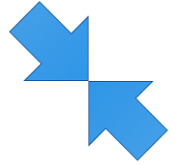
- Avanserte egenskaper

Kan angis for:

- Filer
- Mapper
- Undermapper



Komprimerte filer og mapper



Hovedregel for flytting/kopiering:

- Målmappe bestemmer komprimeringsstatus når filer/mapper flyttes eller kopieres.

Unntak:

- Ved flytting innen samme partisjon beholdes alltid komprimeringsstatus.

Disk kvoter

Disk kvote (Disk Quota)

- Begrense på hvor mye lagringsplass hver bruker kan benytte på en disk
- Alle filer og mapper som brukeren er eier av, teller med i kvoten

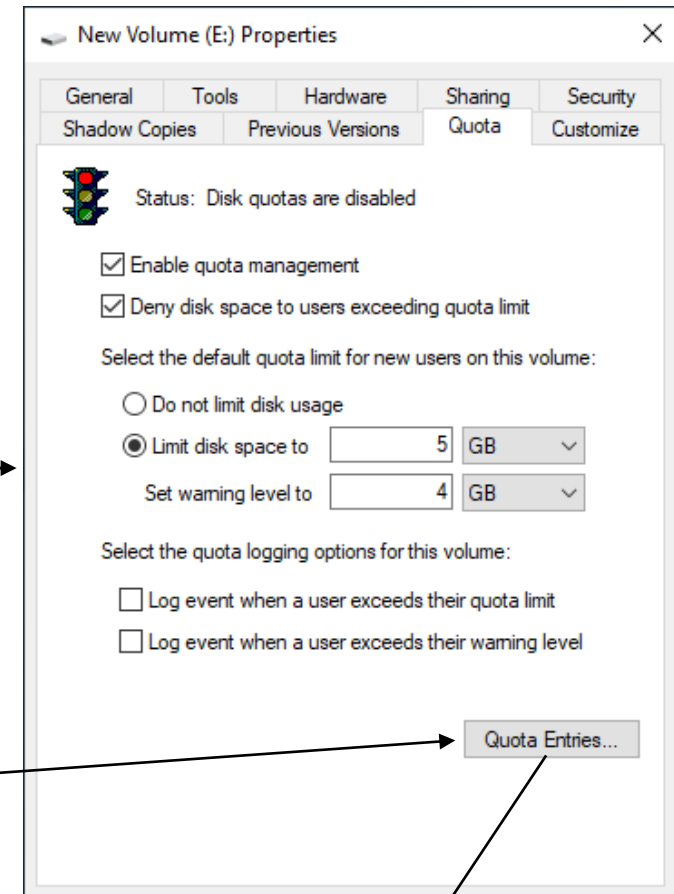
Kvote kan settes på hver disk

- Quota under Properties for disken
- Gjelder da for alle brukere
- Gjelder bare data på denne disken

Kan settes på hver brukerkonto

- Gjelder da kun for disse brukerne
- Knappen Quota Entries...
- Menyvalg Quota | New Quota Entry

Kvoter kan ikke settes på grupper



The screenshot shows the 'Quota Entries for New Volume (E:)' window with a table of quota entries. The table has columns for Status, Name, Logon Name, Amount Used, Quota Limit, Warning Level, and Percent Used. The entries are as follows:

Status	Name	Logon Name	Amount Used	Quota Limit	Warning Level	Percent Used
OK	Jon Kvisli	jon@mittdomene.local	0 bytes	10 GB	9 GB	0
Warning	Test Domenebruker1	testbruker1@mittdomene.local	1,02 MB	2 MB	500 KB	51
OK	BUILTIN\Administrators	BUILTIN\Administrators	74 KB	No Limit	No Limit	N/A
OK	NT AUTHORITY\SYSTEM	NT AUTHORITY\SYSTEM	6 MB	No Limit	No Limit	N/A

4 total item(s), 1 selected.