Labo Windows: Opdracht 07: NTFS-rechten

Achtergrond

1. Inleiding

NTFS (New Technology File System) is het standaard bestandssysteem gebruikt door Windows NT en hoger. NTFS is gebaseerd op HPFS (High Performance File System) en dient ter vervanging van het FAT-bestandssysteem dat MS-DOS gebruikte.

NTFS-rechten worden ook wel *permissies* of *machtigingen* genoemd. Deze rechten bepalen wie er bestanden en mappen kan benaderen en wat ze er kunnen mee doen. De rechten zijn enkel beschikbaar op het NTFS-bestandssysteem en voorzien daarop beveiliging voor lokale- en netwerk-toegang.

Rechten kunnen zowel ingesteld worden voor individuele gebruikers (of per groep), voor mappen alsook voor bestanden. De rechten toekennen kan enkel gebeuren door de volgende gebruikers:

- Administrators
- Eigenaars van de mappen en bestanden
- Gebruikers met het recht Volledig beheer

2. Rechten op mappen en bestanden

Bij het toekennen van NTFS rechten wordt er een onderscheid gemaakt tussen mappen en bestanden. Hieronder een overzicht van de verschillende opties welke instelbaar zijn:

2.1 Verschillende toegangsniveaus

Toegangsniveau	**Beschrijving**
Volledig beheer	Gebruikers kunnen de volledige inhoud van een bestand of map bekijken, bestaande bestanden en mappen wijzigen, nieuwe bestanden en mappen maken en programma's in een map uitvoeren.
Wijzigen	Gebruikers kunnen bestaande bestanden en mappen wijzigen,

	maar geen nieuwe maken.
Lezen en uitvoeren	Gebruikers kunnen de inhoud van bestaande bestanden en mappen bekijken en programma's in een map uitvoeren.
Mapinhoud weergeven	Gebruikers kunnen een lijst weergeven van bestanden en mappen (enkel van toepassing bij rechten op mappen).
Lezen	Gebruikers kunnen de inhoud van een map bekijken en bestanden en mappen openen.
Schrijven	Gebruikers kunnen nieuwe bestanden en mappen maken en bestaande bestanden en mappen wijzigen.

3. Access Control List of ACL

Het NTFS-bestandssysteem houdt een ACL bij voor elk bestand of map. Elke ACL bevat een lijst van gebruikers en groepen die toegang hebben tot dat bestand of die map. Verder wordt ook het type toegang dat elke gebruiker en groep heeft bijgehouden. Dit wordt bewaard in een *access control entry* (ACE) per gebruiker en groep.

3.1 Rechten toekennen

Aan een gebruiker of gebruikersgroep kunnen meerdere rechten toegevoegd worden.
Het effectieve recht van een gebruiker is de som van de toegekende rechten aan de gebruiker en van de groep waartoe de gebruiker behoort. Gebruikersrechten worden daarom ook *cumulatief* genoemd.

3.2 Rechten weigeren

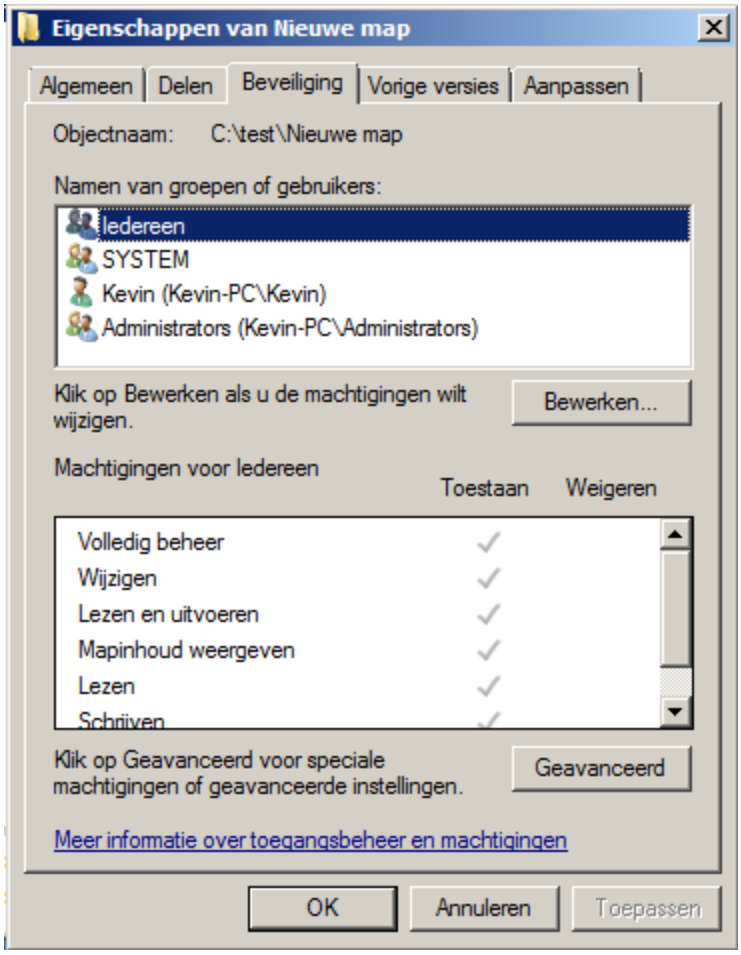
Men kan ook rechten aan een gebruiker weigeren in plaats van toe te staan. *Weigeren heeft telkens voorrang op toestaan*. Weigeren is echter niet de standaard manier om rechten toe te kennen.

3.3 Maprechten overschrijven met bestandsrechten

NTFS bestandsrechten hebben voorrang op rechten op mappen. Een gebruiker met bijvoorbeeld de nodige rechten op een bestand kan dat bestand benaderen in een map waartoe hij niet de nodige rechten heeft. De map die het bestand bevat is echter onzichtbaar als er geen leesrechten zijn op die map. Het bestand benaderen kan dan door het volledige pad op te geven gebruik makende van de UNC (Universal Naming Convention). Een voorbeeld hiervan is:
`\\server\share\file_path\file_name`

3.4 Rechten doorgeven

Standaard worden de rechten van een “ouder-map” doorgegeven naar alle bestaande en nieuwe submappen en bestanden in de map.



Figuur: Overgenomen rechten, te herkennen aan de lichtgrijze vinkjes.

Als in de verschillende onderdelen van de gebruikersinterface voor toegangsbeheer de selectievakjes **Toestaan** en **Weigeren** *grijs worden weergegeven* wanneer je de machtigingen van een object bekijkt, heeft dit object machtigingen van een bovenliggend object overgenomen.

Je kan deze overgenomen **machtigingen instellen** via het **tabblad Machtigingen** van het eigenschappenblad **Geavanceerde beveiligingsinstellingen**.

Er zijn drie aanbevolen manieren waarop je overgenomen machtigingen kan wijzigen:

1. Wijzig het bovenliggende object, waar de machtigingen specifiek zijn gedefinieerd. Deze machtigingen worden vervolgens door het onderliggende object overgenomen.

2. Schakel het selectievakje Toestaan in om de *overgenomen machtiging Weigeren* op te heffen.

3. Schakel het selectievakje Overneembare machtigingen van het bovenliggende object opnemen uit. Je kan nu de machtigingen wijzigen, of gebruikers of groepen uit de lijst bij Machtigingen verwijderen. Voor het object worden echter geen machtigingen van het bovenliggende object meer overgenomen.

4. Administratie van rechten

4.1 Goede aanpak (vereenvoudigen)

Om de administratie te vereenvoudigen kan men de volgende punten in acht nemen:

- Rangschik bestanden volgens: toepassingen, data, ...
- Centraliseer werk- en publieke mappen op een apart volume.
- Ken enkel rechten toe op mappen, niet op bestanden.
- Isoleer toepassingen en het OS op een apart volume.
- Weiger enkel rechten als het echt nodig is.

4.2 Veiligheid binnen een NTFS systeem

Om een NTFS systeem echt veilig te maken is het nodig om de *rechten in te perken*, ken dus enkel de nodige rechten toe en niet meer. Creëer groepen overeenkomstig de nodige rechten en ken vervolgens rechten toe aan die groepen, vermijdt hierbij toekenning van rechten aan individuele gebruikers. Moedig de gebruikers wel aan om rechten toe te kennen aan de mappen die ze creëren.

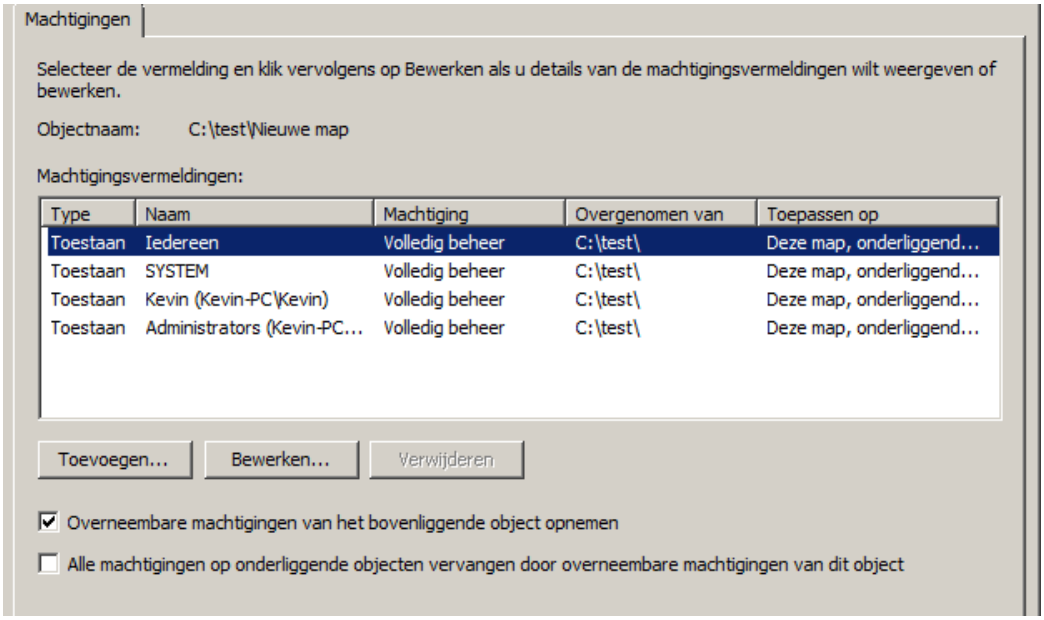
4.3 NTFS rechten toekennen

Rechten kunnen ingesteld worden via eigenschappen en beveiliging van een bestand of map. Als men geen lid is van een domein kan men het tabblad beveiliging weergeven door in het venster Deze Computer bij mapopties e*n weergave* het selectievakje *Eenvoudig delen van bestanden gebruiken* uit te schakelen.

Bij *beveiliging* kan men per gebruiker of groep de rechten instellen (als men daar het recht toe heeft). Een gebruiker of groep kan eventueel toegevoegd worden in het lijstje, er wordt dan een nieuwe ACE aangemaakt voor die gebruiker.

4.4 Geavanceerde NTFS rechten toekennen

Selecteer hiervoor *Geavanceerd* bij *eigenschappen en beveiliging* van een map of bestand. Kies vervolgens de gebruiker waarvoor je de rechten wilt toekennen en selecteer bewerken. Een uitgebreide lijst met rechten kan nu ingesteld worden.



Figuur: geavanceerde NTFS Rechten

Figuur: geavanceerde NTFS Rechten

In volgende tabel worden de toegangsbeperkingen voor elke set speciale NTFS-machtigingen aangegeven:

Speciale	*Volledig*	*Wijzigen*	*Lezen en*	*Mapinhoud*	*Lezen*	*Schrijven*

machtigingen	*beheer*		*uitvoeren*	*weergeven (alleen voor mappen)*		
Door map bladeren/bestand uitvoeren	x	x	x	x		
Map weergeven/gegevens lezen	x	x	x	x	x	
Kenmerken lezen	x	x	x	x	x	
Uitgebreide kenmerken lezen	x	x	x	x	x	
Bestanden maken/gegevens schrijven	x	x				x
Mappen maken/gegevens toevoegen	x	x				x
Kenmerken schrijven	x	x				x
Uitgebreide kenmerken schrijven	x	x				x
Submappen en bestanden verwijderen	x					
Verwijderen	x	x				
Machtigingen lezen	x	x	x	x	x	x
Machtigingen wijzigen	x					
Eigenaar worden	x					

Synchroniseren	x	x	x	x	x	x

Groepen of gebruikers die de machtiging **Volledig beheer** hebben voor een map, kunnen alle bestanden in deze map verwijderen, ongeacht de machtigingen die voor de bestanden zijn ingesteld. Een administrator kan steeds eigenaar worden, onafhankelijk van de ingestelde rechten. Niemand, zelfs niet de eigenaar of administrator kan iemand anders “het eigenaarsschap” toekennen.

5. Kopiëren en verplaatsen van bestanden

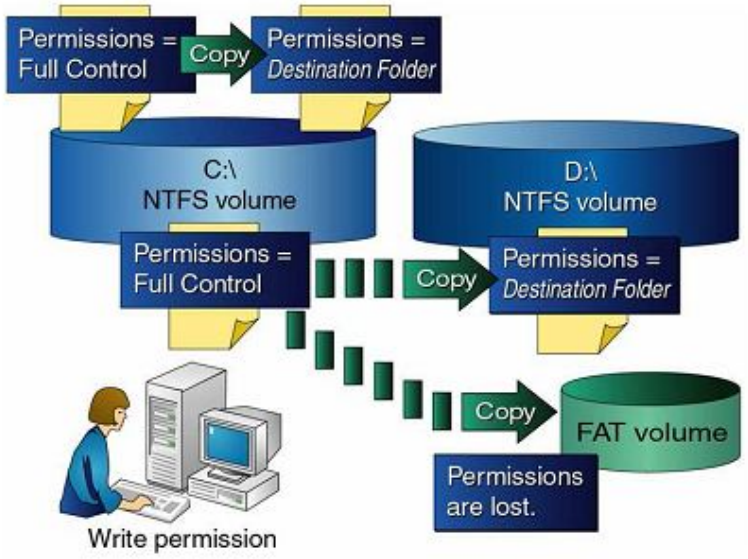
Als bestanden verplaatst of gekopieerd worden dan kunnen de rechten veranderen. Speciale regels controleren hoe deze rechten veranderen. Problemen kunnen voorkomen worden door de regels te kennen. Deze regels moeten in acht worden genomen om gebruikers niet buiten spel te zetten of om bestanden niet onbeveiligd te maken.

5.1 Kopiëren van bestanden

Bij het kopiëren van een NTFS volume naar een NTFS volume geldt:

- Bestanden krijgen de rechten van de doelmap waarnaar gekopieerd wordt.
  (dit geldt ook voor een doelmap op eigen volume)

- Je moet schrijfrechten hebben op de doelmap.



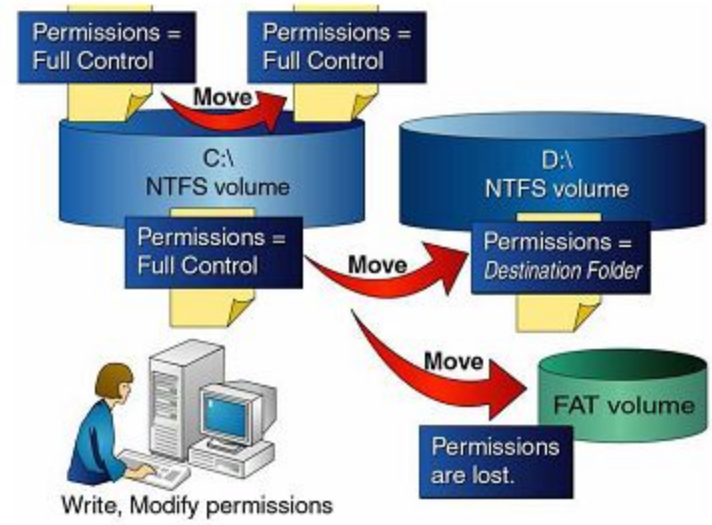
Figuur: Kopiëren van bestanden en de gevolgen qua permissies ervan.

5.2 Verplaatsen van bestanden

Bij het verplaatsen van bestanden naar hetzelfde NTFS volume blijven de rechten behouden.

Bij het verplaatsen naar een ander NTFS volume krijgen de bestanden daarentegen de rechten van de doelmap. Opmerking: de bestandseigenaar blijft dezelfde.

Voor het verplaatsen moet je minstens schrijfrechten hebben op de doelmap en wijzigingsrechten op de bronmap.



Figuur: Verplaatsen van bestanden en de gevolgen qua permissies ervan.

6. De opdrachtprompt

Met de opdracht `cacls` kan men op de opdrachtprompt rechten van bestanden of mappen beheren. Het algemene gebruik van de opdracht is : `cacls` *`bestandsnaam /optie`*.

De change access control list (`cacls`) bezit echter een aantal tekortkomingen. Het is bijvoorbeeld niet simpel om rechten toe te kennen aan een overgeërfde folder. Hiervoor heeft Microsoft `icacls` in het leven geroepen. Deze opdracht bezit praktisch dezeflde opties als zijn voorganger, maar doet net wat meer.

De opdracht zonder optie geeft de huidige permissie instellingen van een bestand of map weer.
vb. `icacls test.txt`

6.1 Opties van icacls

Een aantal mogelijke schakelopties zijn:

- `/grant[:r] Sid`

  Machtiging geeft de opgegeven toegangsrechten aan de gebruiker. Met `:r` vervangen

de machtigingen alle eerdere uitdrukkelijk toegewezen machtigingen. Zonder `:r` worden de machtigingen aan alle eerdere uitdrukkelijk toegewezen machtigingen toegevoegd.

- `/deny Sid`

  Machtiging: weigert uitdrukkelijk de opgegeven toegangsrechten. Een ACE voor uitdrukkelijk weigeren wordt aan de opgegeven machtigingen toegevoegd, en dezelfde machtigingen in elke uitdrukkelijke toewijzing worden verwijderd.

- `/remove[:[g|d]] Sid`

  Verwijdert alle exemplaren van `Sid` in de ACL. Met `:g` worden alle exemplaren van aan die `Sid` toegewezen machtigingen verwijderd. Met `:d` worden alle aan die `Sid` geweigerde machtigingen verwijderd.

6.2 Mogelijk toe te kennen rechten

Hieronder een overzicht van de toe te kennen rechten met `icacls`:

- **F** (full access)
- **M** (modify access)
- **RX** (read and execute access)
- **R** (read-only access)
- **W** (write-only access)

6.3 Rechten op mappen

Wanneer `icacls` toegepast wordt op een map kan men ook het volgende zien en eventueel wijzigen:

Uitvoer	ACE(recht) is van toepassing op
OI	deze map en bestanden
CI	deze map en submappen
IO	niet op huidig bestand of map
geen uitvoer	alleen deze map
(IO)(CI)	deze map, submappen en bestanden
(OI)(CI)(IO)	alleen submappen en bestanden

(CI)(IO)	alleen submappen
(OI)(IO)	alleen bestanden

LABO-GEDEELTE

Doelstellingen

- Rechten op bestanden en mappen kunnen instellen
- Gebruik van de opdracht `icacls` (command prompt)

Opgaven

7.1 Rechten op mappen en bestanden

1. Log in als een gebruiker met beperkte rechten
2. Maak in uw map Mijn Documenten een submap Labo7 aan
3. Controleer de rechten van de map Labo7 via eigenschappen en beveiliging.
4. Welke gebruikers hebben allemaal volledig beheer op de map “Labo7”?
5. Controleer hetzelfde via de opdrachtprompt. Welk commando gebruik je?
6. Voeg een nieuwe gebruiker toe aan het lijstje op het tabblad beveiliging. Welke rechten krijgt deze standaard toegekend?
7. Log nu in als deze toegevoegde gebruiker, kan deze eigenaar worden van deze map?
8. Welke recht(en) moet men daarvoor toekennen? Test dit ook effectief uit.
9. Log terug in als originele gebruiker en ken jezelf opnieuw het eigenaarsschap toe.

7.2 Doorgeven van rechten

1. Creëer in de map Labo7 een tekstbestand tekst1.txt
2. Worden de rechten van de map doorgegeven?
   Ga dit na, voor de toegevoegde gebruiker aan het lijstje in het tabblad beveiliging.
3. Zorg ervoor als je nu nog een nieuw tekstbestand (tekst2.txt) creëert dat ditmaal niet de rechten van de map doorgegeven krijgt (enkel die voor de toegevoegde gebruiker).
4. Verandert deze instelling ook de rechten van tekst1.txt?
5. Stel via de opdrachtprompt in dat de rechten van de map Labo7 terug doorgegeven wordt aan mappen en bestanden erin, verwijder hiervoor eerst de rechten van de toegevoegde gebruiker en ken ze nadien terug toe.

   LET OP: wis de rechten van de andere gebruikers niet!

7.3 Speciale rechten

1. Weiger het schrijfrecht aan de eigenaar van tekst1.txt
2. Selecteer Geavanceerd op het tabblad Beveiliging en kies daar het tabblad Machtigingen
3. Welke speciale rechten (machtigingen) houdt het schrijven in?
4. Voeg een machtigingsvermelding toe voor de map Labo7 en dit voor de Beheerder, zorg ervoor dat deze geen nieuwe submap kan aanmaken, test dit uit.

5. Kan ik met de opdracht icacls deze speciale rechten zien en verwijderen?
6. Kijk na wat het verschil is tussen de rechten “RX” en “W” bij de opdracht icacls.

7.4 Kopiëren en verplaatsen van bestanden

1. Zet de rechten van de map Labo7 op enkel lezen voor de Beheerder.
2. Controleer of dat de bestanden erin ook enkel leesrechten hebben voor de Beheerder.
3. Creëer een map Labo7bis in Mijn Documenten zonder de rechten te wijzigen, ga ze wel na voor de Beheerder.
4. Kopieer de bestanden uit de map Labo7 naar de map Labo7bis.
5. Welke rechten hebben de gekopieerde bestanden voor de Beheerder?
6. Wis de bestanden in de map Labo7bis.
7. Herhaal nu het bovenstaande maar verplaats i.p.v. kopieer. Dit zal niet lukken, waarom niet?
8. Maak de volgende aanpassingen:
    a. Zet de rechten terug op volledig beheer voor de map Labo7 voor de eigenaar.
    b. Weiger volledig beheer op de map Labo7bis voor de groep administrators.
9. Verplaats nu de bestanden van de map Labo7 naar de map Labo7bis
10. Wat is er gebeurd met de rechten van de administrators voor deze bestanden?
11. Op welke manier kan je de machtigingsinstellingen op de map Labo07 terug naar de beginwaarden brengen?