NTFS



Bc. Šimon Suchomel

NTFS

- Specifikují k jakým prostředkům má objekt přístup
- Dostupné pouze na NTFS svazcích
- Oprávnění souborů se liší od adresářů
- Příkaz cacls, alternativa xcacls
- Změníme na kartě Security
  - Není karta security vidět?
    - Není svazek na NTFS
    - Je povoleno Simple File Sharing ve Folder Options
- NTFS oprávnění může měnit
  - Člen skupiny Administrators
  - Vlastník
  - Uživatelé s Full Controll

NTFS oprávnění na adresáře

- Read
  - Vidět soubory a podadresáře a vidět oprávnění adresáře a atributy (Read-Only, Hidden, Archive and System)
- Write
  - Vytvořit nový soubor a podadresář, změnit atributy a zobrazit vlastníka a oprávnění
- List Folder Contents
  - Vidět jména souborů a podadresářů
- Read & Execute
  - Jako read a List Folder Contents + dostat se skrz adresáře
- Modify
  - Jako Write a Read & Execute + smazat adresář
- Full Control
  - Jako vše + změnit oprávnění, převzít vlastnictví a mazat podadresáře a soubory
  - Defaultě pro Everyone po formátu svazku NTFS

NTFS oprávnění na soubory

- Read
  - Číst soubor a zobrazit jeho atributy, vlastníka a oprávnění
- Write
  - Přepsat soubor, změnit atributy a zobrazit vlastníka a oprávnění
- Read & Execute
  - Jako Read + spustit aplikaci
- Modify
  - Jako Write a Read & Execute + změnit a smazat soubor
- Full Control
  - Jako vše + změnit oprávnění a převzít vlastnictví

Access Control Lists

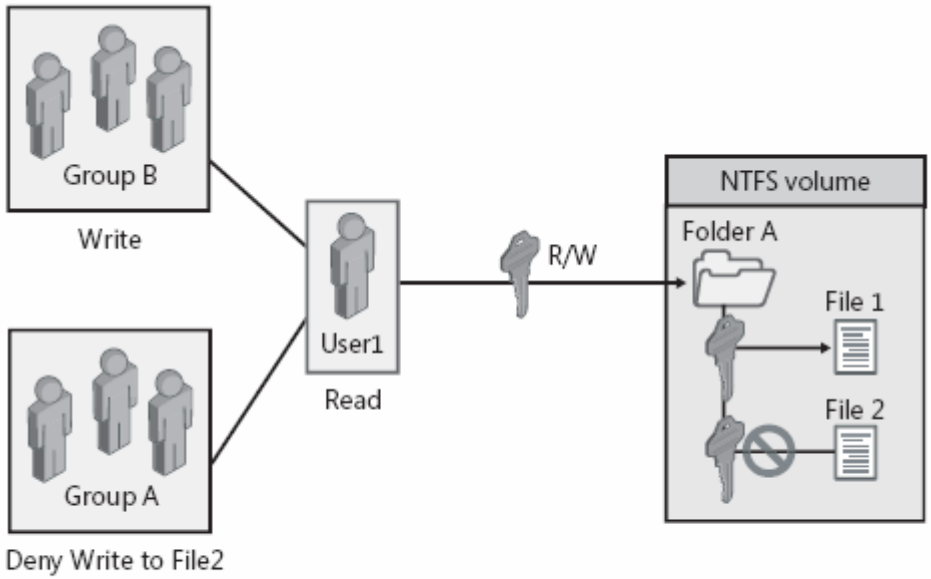
- NTFS spravuje ACL pro každý soubor a adresář na NTFS svazku
- ACL obsahuje seznam všech účtů a skupin, kterým bylo přiděleno oprávnění
- Pro přístup musí ACL obsahovat Access Control Entry (ACE) záznam který musí povolit typ oprávnění, které se uživatel snaží použít

Effective Permissions

- Pro uživatele je to součet oprávnění přiřazených jeho účtu a skupinám, kterých je členem
- NTFS oprávnění na soubor mají větší prioritu než oprávnění přiřazené na adresář, který obsahuje ten soubor
- Bypass Traverse Checking oprávnění
  - Dostaneme se k souboru na který oprávnění máme, přestože nemáme oprávnění na adresář
  - Windows settings -> Local Policies -> User Rights Assignment -> Bypass Traverse Ch.
- Deny přepíše Allow oprávnění

Příklad

- User1 má Read na adresář A a je členem skupiny A a skupiny B
- Skupina B má Write na adresář A
- Skupina A má denied Write na soubor File2



Dědičnost

- Defaultně se oprávnění dědí z nadřazených adresářů do podadresářů a souborů
- Lze zakázat dědění oprávnění
- Adresář, kterému bylo odebráno dědění od nadřazených adresářů se stává novým kořenem pro dědičnost

Special Permissions

- Full Control
  - Všechna ostatní oprávnění
- Traverse Folder/Execute File
  - Může projít adresářem, ikdyž nemá žádná jiná oprávnění
  - Nemá vliv pokud je povoleno Bypass Traverse Checking
  - Spustit spustitelný soubor
- List Folder/Read Data
  - Vidět podadresáře a soubory
  - Vidět obsah souboru
- Read Attributes
  - Vidět atributy (definované NTFS)
- Read Extended Attributes
  - Vidět další atributy (definované programy)
- Create Files/Write Data
  - Vytvořit nový soubor v adresáři
  - Změnit obsah souboru

Special Permissions

- Create Folders/Append Data
  - Vytvořit adresář v daném adresáři
  - Možnost změnit soubor (pouze přidat data na konec). Nelze přepsat existující
- Write Attributes
  - Změnit atributy definované NTFS
- Write Extended Attributes
  - Změnit atributy definované programy
- Delete Subfolders And Files
  - Smazat podadresář nebo soubor v daném adresáři (ikdyž na něj nemá Delete)
- Delete
  - Smazat konkrétní soubor nebo adresář
- Read Permissions
  - Přečíst oprávnění
- Change Permissions
  - Možnost měnit oprávnění (bez použití Full Control)
- Take Ownership
  - Převzít vlastnictví
- Synchronize
  - Možnost synchronizovat mezi vlákny vícevláknového programu (více procesorů). Není přiděleno uživatelům, ale vícevláknovému programu

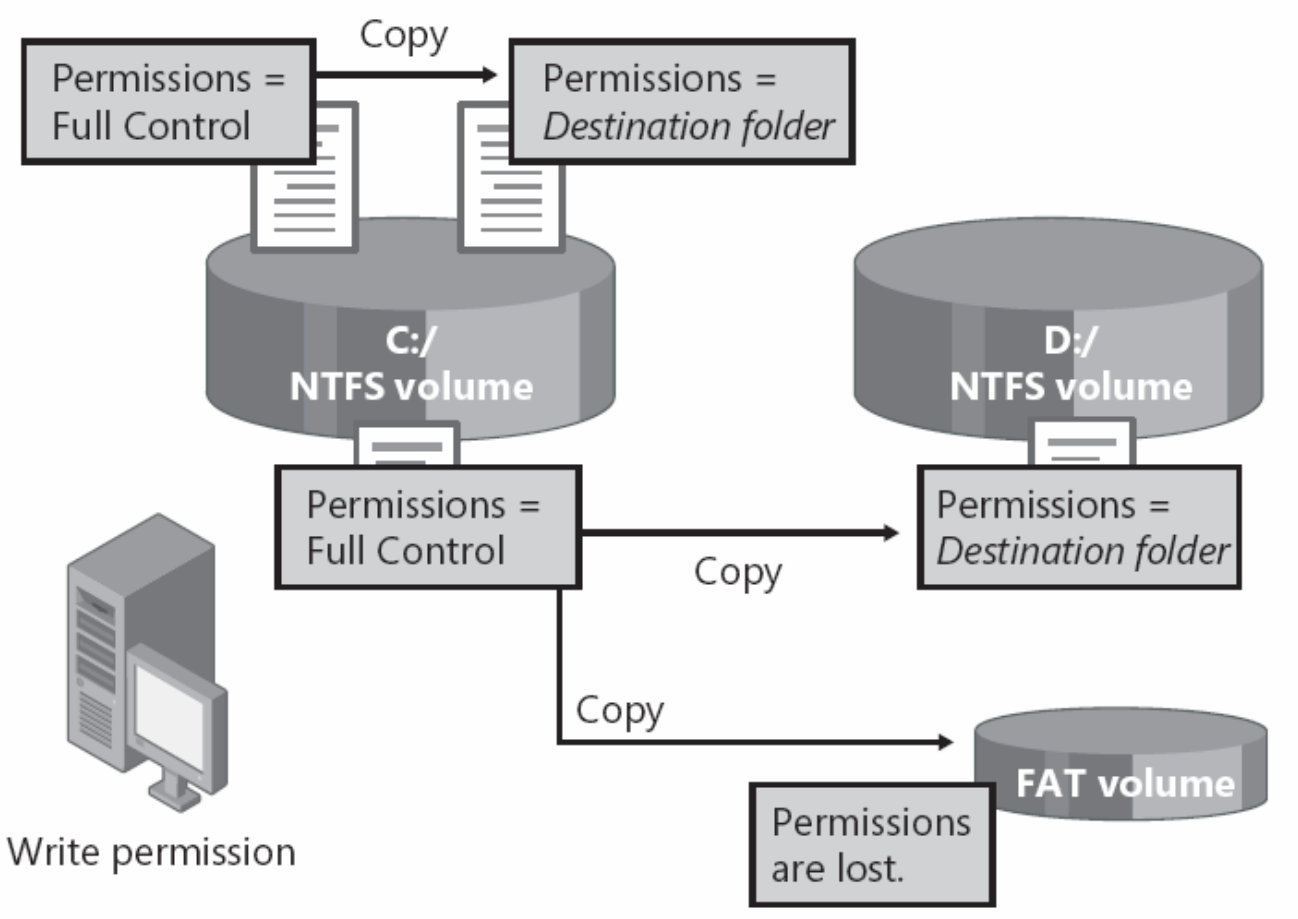
Vlastnictví

- Vlastnictví nelze nikomu přidělit
- Lze si pouze přivlastnit objekt (explicitně změnit vlastnictví na sebe)
- Vlastník může vždy měnit NTFS oprávnění
- Vlastník nebo kdokoliv s Full Control může přiřadit Full Control standardní oprávnění a Take Ownership speciální oprávnění jinému uživateli nebo skupině
- Vlastnictví se počítá do Kvóty (viz další přednášky)

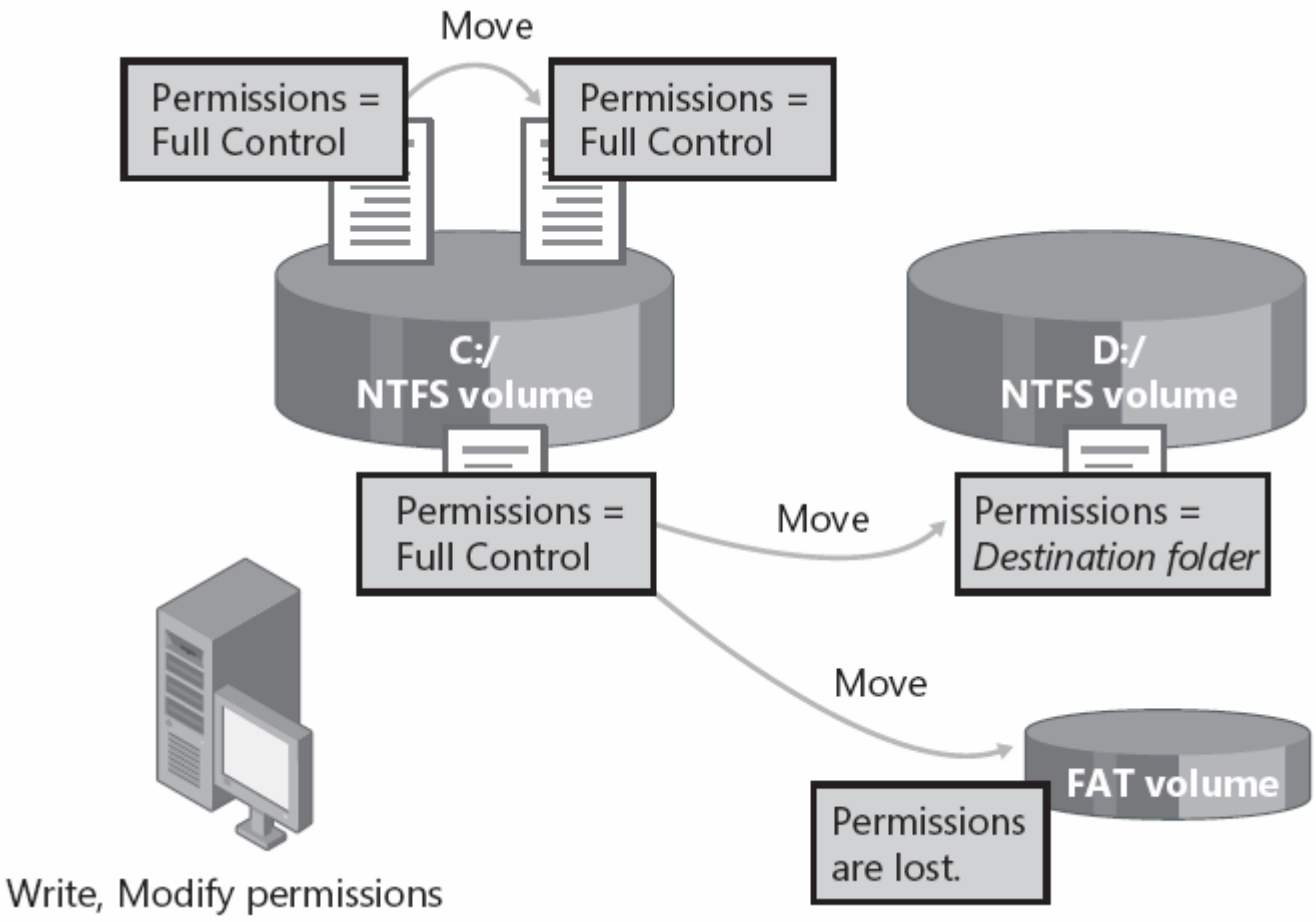
Jak plánovat NTFS

- Organizovat soubory do adresářů a těm pak přidělovat oprávnění místo oprávnění přímo na soubory
- Princip nejnižšího oprávnění
- Vytvářet skupiny podle typu přístupu, oprávnění přiřazovat skupinám, uživatelé jako členy skupin
- Adresáře s aplikacemi by měly mít Read & Execute pro skupiny Users i Administrators
- Pro veřejná místa Full Control pro skupinu Creator Owner
- Nepoužívat Deny jako součást plánu!!!!!
- Poučit uživatele aby si měnily oprávnění na svoje složky ☺

Když jsou soubory a složky kopírovány



Když jsou soubory a složky přesouvány



Standardní problémy

- Uživatel nemůže přistoupit ke zdroji
- Přidali jsem uživatele do skupiny s oprávněním ke zdroji, ale stále tam přístup nemá
- Uživatel má Full Control na adresář, smaže tam soubor, přestože neměl právo mazat soubor jako takový

Standardní problémy a řešení

- Uživatel nemůže přistoupit ke zdroji
  - Zkontrolujeme oprávnění jestli se nezměnilo při kopírování či přesunu
- Přidali jsem uživatele do skupiny s oprávněním ke zdroji, ale stále tam přístup nemá
  - Aby se znovu vyhodnotilo ACL musí se uživatel znovu ověřit
- Uživatel má Full Control na adresář, smaže tam soubor, přestože neměl právo mazat soubor jako takový
  - Odebereme oprávnění Delete Subfolders and Files