12. Správa uživatelů a oprávnění

**1. Správa uživatelů a skupin v OS Windows**

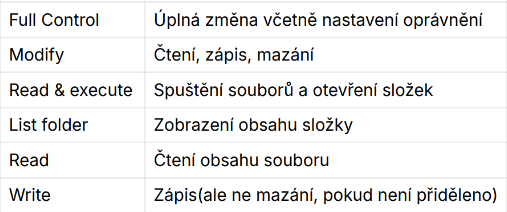
**1.1 Lokální správa uživatelů a skupin**

* **Nástroje:**
  + **Správa počítače (Computer Management):**
    - V konzoli najdete položku „Místní uživatelé a skupiny“, kde můžete vytvářet, mazat a upravovat **účty a skupiny**.
  + **Příkazový řádek a PowerShell:**
    - Příkazy jako net user, net localgroup nebo cmdlety jako New-LocalUser, Add-LocalGroupMember umožňují automatizovat správu účtů.
* **Principy:**
  + **Vytváření uživatelských účtů:** Nastavení jména, hesla, popisných údajů a členství ve skupinách.
  + **Delegace správy:** Umožňuje přidělovat správu určitých uživatelů nebo skupin lokálním administrátorům bez plného přístupu k systému.
* **Uživatelské účty**
  + K přihlášení – ověření identity, oprávnění (k čemu můžem přistupovat)
  + Místní a doménové účty (AD).
* **Profil uživatele**
  + Soubor složek a dat obsahující prostředí plochy a nastavení aplikací
  + Aby měl uživatel stejnou konfiguraci (např. plochy)
* **Skupiny**
  + Množina či seznam uživatelských účtů
  + Výhoda – hromadné spravování oprávnění a práv
  + (nějaké jsou již inte´grované v OS W, jako Domain admins, Domain users, Authenticated users, everyone atd…

**1.2 Správa v prostředí Active Directory (AD)**

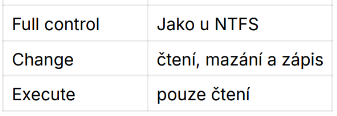
* **Centralizovaná správa:**
  + U větších organizací se využívá Active Directory, kde se účty spravují centrálně.
  + Administrátoři mohou využívat nástroje jako **Active Directory Users and Computers (ADUC)**, kde se nastavují vlastnosti účtů, organizační jednotky (OU) a skupinové členství.
* **Delegace a zásady:**
  + Umožňuje delegovat správu konkrétních OU, což pomáhá v hierarchické správě a rozdělení odpovědnosti.
  + Skupinové politiky (Group Policy) lze využít k nastavení bezpečnostních pravidel, jako je vypršení hesla nebo omezení přístupu.

**2. Přehled oprávnění ve Windows na úrovni souborového systému a sdílení**

**2.1 Oprávnění na úrovni souborového systému (NTFS)**

* **NTFS oprávnění:**
  + **Základní oprávnění:** Čtení, zápis, modifikace, úplná kontrola a speciální oprávnění.
  + **Dědičnost:** Oprávnění mohou být děděna z nadřazených složek, což usnadňuje správu v hierarchické struktuře.
  + **Vlastnictví:** Každý soubor či složka má vlastníka, který může udělovat nebo měnit oprávnění.
* **Nástroje:**
  + Vlastnosti souborů a složek ve Windows Explorer, kde v záložce „Zabezpečení“ lze nastavovat oprávnění pro různé uživatele a skupiny.

**2.2 Oprávnění na úrovni sdílení**

* **Sdílené složky:**
  + Sdílení souborů přes síť se konfiguruje pomocí sdílených složek, kde se nastavují **sdílené oprávnění** (čtení, zápis, úplná kontrola). 
  + Sdílená oprávnění se kombinují s NTFS oprávněními – výsledné přístupové právo je nejostřejší z obou nastavení.
* **Správa přístupu:**
  + Uživatelé přistupují k síťovým zdrojům na základě přidělených sdílených oprávnění a bezpečnostních nastavení uložených v NTFS.
* **Nástroje:**
  + Sdílení lze konfigurovat přes vlastnosti složky v Průzkumníku souborů nebo pomocí PowerShell cmdletů jako New-SmbShare.

**3. Správa uživatelů, skupin a oprávnění v UNIX-like OS**

**3.1 Správa uživatelských účtů a skupin**

* **Základní soubory:**
  + **/etc/passwd:** Obsahuje základní informace o uživatelích (uživatelské jméno, UID, domovský adresář, shell).
    - Formát:
    - 
  + **/etc/shadow:** Uchovává šifrovaná hesla a informace o expiraci hesel.
  + **/etc/group:** Obsahuje informace o skupinách a jejich členství.
* **Příkazy pro správu:**
  + **useradd, usermod, userdel:** Přidávání, modifikace a odstraňování uživatelů.
    - usermod -aG (neboli --append --groups) — přidá uživatele do dalších skupin (oddělené čárkou)
  + **groupadd, groupmod, groupdel:** Správa skupin.
  + **passwd:** Nastavení nebo změna hesla uživatele.

**3.2 Správa souborových oprávnění**

* **Tradiční oprávnění:**
  + **Vlastník, skupina a ostatní:** Každý soubor a adresář má přiřazeného vlastníka, skupinu a přístupová práva (čtení, zápis, spuštění).
  + **Příkazy:**
    - **chmod:** Nastavení oprávnění (např. chmod **755** soubor) **(vlastník, skupina, ostatní**) (**rwx**(4+2+1)**r-xr-x**).
    - **chown:** Změna vlastníka souboru (např. chown uživatel:soubor).
    - **chgrp:** Změna skupiny.
* **Speciální bity:**
  + **setuid a setgid:** Umožňují spouštění souboru s oprávněními vlastníka či skupiny.
  + **Sticky bit:** Používá se především u adresářů, aby uživatelé nemohli odstranit soubory patřící jiným uživatelům (např. /tmp).
* Atributy souborů lze zobrazit pomocí ls -l
  + - — označuje soubor
  + d — označuje složku
  + l — označuje symbolický odkaz
  + c — zařízení typu char device (terminál)
  + b — zařízení typu block device (úložiště)

**4. ACL a kvóty v UNIX-like OS**

**4.1 Access Control Lists (ACL)**

* **Definice:**

ACL poskytují jemnější kontrolu nad přístupovými právy, než jakou umožňují tradiční vlastnická práva (vlastník, skupina, ostatní).

* **Nástroje:**
  + **getfacl a setfacl:**
    - getfacl zobrazí aktuální ACL u souboru či adresáře.
    - setfacl umožňuje nastavovat nebo upravovat ACL (např. přidání oprávnění pro specifického uživatele či skupinu).
* **Použití:**
  + Umožňují definovat specifická práva pro jednotlivé uživatele a skupiny, což je užitečné zejména v prostředích s víceúrovňovým přístupem.
* Pro soubory:
  + R (čtení souboru), W (zápis do souboru), X (exe script)
* Pro složky:
  + R (obsahu složky), W (úprava souborů ve složce), X (přístup do složky??)

**4.2 Kvóty (Disk Quotas)**

* **Definice:**

Kvóty slouží k omezení množství diskového prostoru, který může uživatel nebo skupina využívat. Pomáhají předcházet situacím, kdy jeden uživatel spotřebuje všechny dostupné zdroje.

* **Nástroje a konfigurace:**
  + **Quotaon, edquota, repquota:**
    - quotaon aktivuje kvóty na souborovém systému.
    - edquota slouží k nastavení limitů pro uživatele nebo skupiny.
    - repquota zobrazuje aktuální stav využití a limity.
* **Implementace:**
  + Kvóty jsou často nastaveny v souborovém systému, jako je ext4, pomocí úprav v konfiguračních souborech a následné inicializace kvótového systému.

**Shrnutí**

* **Windows:**
  + Správa uživatelů a skupin se provádí pomocí lokálních nástrojů (Computer Management, příkazový řádek, PowerShell) nebo centrálně v Active Directory.
  + Oprávnění se nastavují na úrovni NTFS (s dědičností a vlastnictvím) a při sdílení pomocí sdílených oprávnění, které se kombinují s NTFS právy.
* **UNIX-like OS:**
  + Uživatelé a skupiny jsou spravováni pomocí základních systémových souborů (/etc/passwd, /etc/shadow, /etc/group) a příkazů jako useradd a groupadd.
  + Přístupová práva se konfigurují pomocí příkazů chmod, chown a chgrp, přičemž speciální bity (setuid, setgid, sticky bit) rozšiřují možnosti zabezpečení.
  + ACL umožňují granulárnější řízení přístupu, zatímco kvóty chrání systém před nadměrným využitím diskových zdrojů.