evropský sociální fond v ČR
EVROPSKÁ UNIE
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
OP Vzdělávání pro konkurenceschopnost
INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

PSK3-4

Název školy:	Vyšší odborná škola a Střední průmyslová škola, Božetěchova 3
Autor:	Ing. Marek Nožka
Anotace:	Přístupová práva v OS Unix/Linux
Vzdělávací oblast:	Informační a komunikační technologie
Předmět:	Počítačové sítě a komunikační technika (PSK)
Tematická oblast:	Operační systém Linux/Unix
Výsledky vzdělávání:	Žák zjišťuje a nastavuje souborům přístupová práva, vysvětluje jejich význam
Klíčová slova:	Linux, Unix, shell, ls -l, chmod, owner, user, group
Druh učebního materiálu:	Online vzdělávací materiál
Typ vzdělávání:	Střední vzdělávání, 4. ročník, technické lyceum
Ověřeno:	VOŠ a SPŠE Olomouc; Třída: 4L
Zdroj:	Vlastní poznámky, Vilém Vychodil: Linux Příručka českého uživatele

Přístupová práva

Přístupová práva v Unixu umožňují ve víceuživatelském systému definovat přístup k adresářům a souborům na základě uživatelských účtů nebo skupin uživatelů. Kontrola přístupu umožňuje na systémové úrovni zabránit uživatelům, aby záměrně nebo omylem cizí data poškodili nebo zneužili.

Základní oprávnění (označována také jako tradiční unixová oprávnění), která v unixových systémech pocházejí z přelomu 60. a 70. let minulého století, kdy počítače měly velmi málo paměti (řádově desítky kB) a pomalé procesory. Oprávnění byla proto vytvořena co nejjednodušeji, aby se minimalizovala režie operačního systému při jejich interpretaci.

(*Pro pokročilejší a jemnější práci s přístupovými právi slouží tzv. Access control list, který ale musí mít podporu na konkrétním souborovém sytému. Pro manipulaci s přístupovými právy se potom používají programy* `getfacl` *a* `setfacl` *z balíčku* `acl`.)

Pravidla

Každý objekt v souborovém systému (soubor, adresář) má v i-uzlu (inode) uloženy následující informace:

- typ souboru (obyčejný soubor, adresář, symbolický odkaz, soubor zařízení, pojmenovaná roura, socket)
- vlastníka a skupinu, kterému soubor patří
- trojice oprávnění pro vlastníka, skupinu a ostatní uživatele `r` (čtení), `w` (zápis) a `x` (spouštění)

Při práci s objekty v souborovém systému platí tato pravidla:

- nově vytvořený objekt patří uživateli, který ho vytvořil, a primární skupině tohoto uživatele
- nově vytvořený objekt má implicitně oprávnění určená příkazem `umask`
- oprávnění může měnit vlastník objektu nebo správce systému (root)
- vlastníka může měnit pouze `root`, v některých případech i majitel
- skupinu může měnit root, v některých případech i majitel

Operační systém nezasahuje do zapsaných údajů, pokud nemusí. Proto při přejmenování nedojde k ovlivnění oprávnění ani vlastníka či skupiny. Naopak při kopírování patří kopie tomu, kdo si ji vytvořil. Při přesunu záleží na tom, jestli je potřeba vytvořit nový i-uzel (při přesunu mezi různými souborovými systémy jde vlastně o kopírování s následným smazáním originálu) nebo nikoliv (jde vlastně o variantu přejmenování).

Výpis přístupových práv

Přístupová práva lze zjisti příkazem `ls -l`:

```
ls -l soubor
ls -l adresar
ls -dl adresar
```

Výstup příkazu `ls -l /tmp`

```
drwxr-x--x 2 pepa doma 4096 říj 7 18:54 adresar
```

Ve výpisu první znak udává druh souboru

- `d` adresář
- `-` běžný soubor
- `l` symbolický odkaz
- `p` pojmenovaná roura
- `c` znakové zařízení
- `b` blokové zařízení
- `s` socket

Dále je 9 znaků zobrazujících přístupová práva. Dále číslo udává počet jmen souboru. Dále jméno vlastníka `pepa` a skupiny vlastníků

doma. Dále velikost souboru, datum poslední změny a nakonec jméno souboru. Příslušnost uživatele ke skupině nastavuje administrátor sytému.

Přístupová práva se zobrazují ve třech trojicích: vlastník, skupina, ostatní.

- `r` právo pro čtení (read)
- `w` právo pro zápis (write)
- `x` právo pro spouštění (execute)
- `s` SUID bit nebo GUID bit, soubor se bude spouštět s právy vlastníka nebo skupiny
- `t` Sticky bit

```
rwxr-x--x
```

`rwx` – vlastník (`pepa`) může číst psát a spouštět
`r-x` – skupina vlastníků (`doma`) může číst a spouštět
`--x` – ostatní uživatelé mohou spouštět

Změna přístupových práv

Změna přístupových práv se provádí příkazem `chmod` (change mod) podle následujícího schématu:

```
          s
       u + r
chmod  g - w soubor
       o = x
       a   X
           t
```

Příklady použití programu `chmod`

Příkaz	popis
`chmod go-rw soubor`	odebere skupině a ostatním právo pro čtení a zápis
`chmod g=r soubor`	nastaví skupině právo pouze pro čtení
`chmod -R u+w adresar`	přidá vlastníkovy právo pro zápis
	`-R` provede na všech souborech v adresáři a v podadresářích
`chmod a-w soubor`	všem (all) uživatelům se odebere právo pro zápis
`chmod a+X *`	přidá všem právo pro spouštění, ale jen adresářům nebo tam, kde už je nastaveno.

Číselný zápis přístupových práv

Práva `rwxr-x--x` bychom mohli zapsat jako `111101001`. Každou trojici binárních znaků může interpretovat jako osmičkovou číslici -- tedy `751`. Příkaz `chmod` potom může vypadat takto:

```
chmod 640 spubor
```

Interpretace přístupových práv

Přístupová práva se rozdílně interpretují pro soubory a pro adresáře.

Interpretace pro soubory

Právo `r` umožňuje uživateli číst obsah souboru a právo `w` měnit jeho obsah. Ale právo `w` u souboru není rozhodující při jeho mazání nebo přepsání. Jde spíše o "příznak ochrany proti zápisu".

Právo `x` umožňuje uživateli soubor spustit. Spustitelný soubor může být buď binární nebo může jít o skript. O možnosti jeho spuštění nerozhoduje přípona, ale právě jeho přístupová práva.

Speciální přístupová práva

Právo `s` pro uživatele nebo skupinu je označované jako tzv. SUID a SGUI. Pokud je nastaveno je program spuštěn tak jako by ho spustil jeho vlastník nebo skupina vlastníků.

Příkladem použití může být například změna hesla: Hesla uživatelů jsou uložena v souboru /etc/passwd nebo /etc/shadow, do kterých běžný uživatel nemůže zapisovat (soubor shadow nemůže dokonce ani číst). Při změně hesla je ale potřeba změněné heslo do těchto souborů zapsat. Proto má program /usr/bin/passwd nastaven SUID bit a patří uživateli root. Po spuštění běží program passwd s právy roota a heslo může být do příslušného souboru zapsáno.

Nebo: Některé hry zapisují dosažené skóre do souboru, aby mohli hráči své výkony porovnat. Takový soubor by musel mít právo zápisu pro všechny uživatele v systému. Hráči by pak snadno mohli tento soubor měnit a své dosažené skóre neférově zvyšovat. Proto je program s hrou svěřen speciální skupině (např. games) a je mu nastaven SGID bit. Soubor se skóre pak bude mít právo zápisu přidělené jen skupině games. Do souboru se skóre tak spuštěná hra může zapisovat, kdežto uživatelé nemohou soubor měnit.

Pokud je nastaven Sticky bit `t` ponechává se jeho obsah ve vyrovnávací paměti, což urychlí jeho další spuštění. V současné době se příliš nepoužívá.

Interpretace pro adresáře

U adresářů právo `w` znamená možnost v adresáři vytvářet nebo mazat soubory. Nerozhoduje tedy právo zápisu pro soubor, ale pro adresář ve kterém je umístěn.

Právo `r` říká, že uživatel může vypsat jména souborů v adresáři a právo `x` říká, že do adresáře může vstoupit nebo jím "proplout" k podadresáři. Pro "normální" pří stup k adresáři je zapotřebí právo `r` i `x`.

Chceme-li například sdílet adresář s ostatními uživateli provedeme následující:

```
mkdir ~/public
chmod 711 ~
ls -ld ~
    drwx--x--x 2 pepa doma 4096 říj 7 18:59 /home/pepa
chmod -R go-rwx ~/*
chmod 755 public
ls -ld ~/public
    drwxr-xr-x 2 pepa doma 4096 říj 7 18:59 /home/pepa/public
```

Tím je domovský adresář nastaven tak, že v něm nelze nic číst, ale zároveň jím lze "proplout" do adresáře public, kde je čtení již povoleno.

Speciální přístupová práva

Je li nastaveno právo `s` pro skupinu (GUID) budou nově vytvořené soubory v adresáři náležet skupině, které náleží adresář.

Pokud je nastaven sticky bit `t` může uživatel v adresáři mazat jen své vlastní soubory. Jinak by mohl (pod by měl v adresáři právo zápisu) smazat i soubory vlastněné jiným uživatelem.

Výchozí přístupová práva

O přístupových právech nově vytvořených souborů rozhoduje uživatelská maska (user mask). Tu lze zobrazit a nastavit příkazem `umask`.

```
umask
    026
```

Pokud je vytvářen nový adresář jsou jeho přístupová práva logickým rozdílem čísla `777` a uživatelské masky. Nově vytvořený adresář tedy bude mít práva `rwxr-x--x`

```
  777
- 026
-------
  751
```

Pokud je vytvářen nový soubor jsou jeho přístupová práva logickým rozdílem čísla `666` a uživatelské masky. Nově vytvořený soubor tedy bude mít práva `rw-r-----`.

```
  666
- 026
-------
  640
```

Nastavení uživatelské masky na hodnotu `022` provedeme příkazem

```
umask 022
```