Riadenie prístupu v Linuxe pomocou ACL

Tradičné UNIXové práva

- práva: read, write, execute/use
- subjekty: vlastník, skupina, ostatní
- priradené ku každému objektu súborového systému
- problémy:
  - príliš hrubé členenie subjektov
  - nemožnosť definovať default práva pre nové objekty v danom adresári

Tradičné riešenia problémov

- vytvorenie vhodnej množiny skupín
  - vyžaduje zásah administrátora
  - zložité požiadavky na práva vedú k veľkému množstvu skupín
- vhodné používanie umask
  - OK, ak chceme rovnaké default práva
  - problém, ak potrebujeme rôzny default v rôznych adresároch

Access Control List (ACL)

- rozširuje typy subjektov, pre ktoré je možné definovať práva:
  - vlastník
  - priradená skupina
  - ostatní
  - konkrétny používateľ
  - konkrétna skupina
- definuje default práva pre nové objekty v adresári

Access Control List (ACL)

- ku každému objektu súborového systému je priradený zoznam položiek
  - typ položky,
  - identifikátor používateľa/skupiny,
  - práva (read, write, execute/use)

Access Control List (ACL)

- typy položiek
  - ACL_USER_OBJ – práva pre vlastníka
  - ACL_USER – práva pre určeného používateľa
  - ACL_GROUP_OBJ – práva pre skupinu objektu
  - ACL_GROUP – práva pre určenú skupinu
  - ACL_OTHER – práva pre ostatných
  - ACL_MASK – maximálne práva pre ACL_USER, ACL_GROUP a ACL_GROUP_OBJ
- 1, 0 a viac, 0 – 1 (1 ak exist. zelená)

Access Control List (ACL)

- Vyhodnotenie práv
  - ak efektívne UID procesu = UID vlastníka, použijú sa práva z ACL_USER_OBJ
  - inak, ak efektívne UID procesu = identifikátor v niektorej položke ACL_USER, použije sa tá po AND s ACL_MASK
  - inak, sa nájdu všetky položky typu ACL_GROUP_OBJ a ACL_GROUP, ktoré zodpovedajú efektívnemu GID alebo doplnkovej skupine procesu, spraví sa OR ich práv, potom AND s ACL_MASK a výsledok sa použije
  - ak také položky neexistujú, použije sa ACL_OTHER

Access Control List (ACL)

- Vzťah k tradičným UNIX právam
  - práva pre vlastníka zodpovedajú ACL_USER_OBJ
  - práva pre ostatných zodpovedajú ACL_OTHER
  - práva pre skupinu zodpovedajú
    - ACL_GROUP_OBJ, ak neexistuje ACL_MASK
    - ACL_MASK, ak existuje ACL_MASK
  - nastavenie tradičných práv spôsobí aj zmenu ACL a naopak

Access Control List (ACL)

- Textová reprezentácia práv – dlhá verzia
  - jedna položka na riadok
  - typ:id:prava
  - typ
    - user – ACL_USER alebo ACL_USER_OBJ (ak id=“”)
    - group – ACL_GROUP alebo ACL_GROUP_OBJ (ak id=“”)
    - mask – ACL_MASK
    - other – ACL_OTHER
  - prava: 3 znaky z {r, w, x, -}

Access Control List (ACL)

- Textová reprezentácia – krátka verzia
  - položky oddelené čiarkou
  - typ môže byť skrátený na u, g, m, o
  - pomlčky v právach sa môžu vynechať (ale vždy musí zostať aspoň 1 znak)

Zobrazenie ACL

- `getfacl [-R] objekt`
  - -R – rekurzívne celý podstrom
  - vypíše ACL zadaných pre zadané objekty v dlhej textovej forme

```
# file: a
# owner: root
# group: root
user::rw-
user:jerry:---
group::r--
group:users:r--
group:testgroup:-w-
mask::rw-
other::---
```

Nastavenie ACL

- `setfacl [-R] -m acl objekt`
  - -R – rekurzívne pre celý podstrom
  - acl – špecifikácia v krátkej textovej forme
  - pridá/zmení uvedené položky ACL
- `setfacl [-R] -x acl objekt`
  - zmaže položky z ACL
  - acl – špecifikácia bez práv
- `setfacl [-R] -b objekt`
  - zmaže všetky ACL

Nastavenie ACL

- ďalšie parametre setfacl
  - -n – neprepočítať masku
    - normálne setfacl, ak nemá špecifikovanú masku explicitne, vypočíta a nastaví masku na hodnotu OR všetkých ACL_USER, ACL_GROUP a ACL_GROUP_OBJ
- `setfacl --restore=súbor`
  - nastaví ACL podľa obsahu súboru, ktorý je vo formáte výstupu z getfacl

Default ACL

- Adresár môže mať špecifikované default ACL pre nové objekty
  - ACL pre nový objekt vznikne z default ACL adresára
  - z položiek zodpovedajúcich štandardným UNIX právam sa odstránia práva, ktoré neboli pri vytvorení požadované
- Ak adresár nemá default ACL
  - ACL nového objektu bude obsahovať položky zodpovedajúce štandardným právam nastavené podľa požadovaných práv a umask

Nastavenie default ACL

- `setfacl -d -m acl adresar`
  - acl ako pri normálnych ACL
- `setfacl -m defacl adresar`
  - kde položky defacl obsahujú prefix default: alebo d:
- `setfacl -d -x acl adresar`
- `setfacl -x defacl adresar`
- `setfacl -k adresar`
  - odstráni default ACL

Pripojenie súborového systému s podporou ACL

- Pri použití mount, resp. v príslušnom riadku /etc/fstab je potrebné uviesť voľbu **acl**:
  - `mount -t ext3 -o acl /dev/sda2 /home`
- ACL sú v Linuxe pre súborový systém ext3 podporované v jadre 2.6.x

Príklad

```
root@lubka:/tmp/x# umask
0027
root@lubka:/tmp/x# mkdir d
root@lubka:/tmp/x# getfacl d
# file: d
# owner: root
# group: root
user::rwx
group::r-x
other::---
```

```
root@lubka:/tmp/x# setfacl -m g:testgroup:rwx,default:g:testgroup:rwx d
root@lubka:/tmp/x# getfacl d
# file: d
# owner: root
# group: root
user::rwx
group::r-x
group:testgroup:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:group:testgroup:rwx
default:mask::rwx
default:other::---
```

Príklad

```
root@lubka:/tmp/x# touch d/f
root@lubka:/tmp/x# mkdir d/d2
root@lubka:/tmp/x# getfacl d/f
# file: d/f
# owner: root
# group: root
user::rw-
group::r-x                      #effective:r--
group:testgroup:rwx             #effective:rw-
mask::rw-
other::---
```

```
root@lubka:/tmp/x# getfacl d/d2
# file: d/d2
# owner: root
# group: root
user::rwx
group::r-x
group:testgroup:rwx
mask::rwx
other::---
default:user::rwx
default:group::r-x
default:group:testgroup:rwx
default:mask::rwx
default:other::---
```