KI/OPS

UŽIVATELÉ, SKUPINY A JEJICH (S)PRÁVA

Uživatelé I

- **Bežní uživatelé (kubera, test)**
- **Adminnistrátor (root)**
- **Služby (sshd)**
  - >less /etc/passwd

```
root:x:0:0:root:/root:/bin/bash
sshd:x:74:74:Privilege-separated SSH:/var/empty/sshd:/sbin/nologin
kubera:x:1000:1000:Petr Kubera:/home/kubera:/bin/bash
test:x:1001:1001::/home/test:/bin/bash
```

    - Jméno uživatele, x-heslo
    - UID – identifikátor uživatele
    - GUID – identifikátor primární skupiny
    - Informace o uživateli
    - Domovský adresář
    - Přihlašovací shell (/sbin/nologin ,/bin/false =nelze se přihlásit)

Uživatelé II

- **Informace o heslech /etc/shadow**

sshd:!!:16576::::::
test:
6EPKgSKgu$AlJ3LHzoABJSLNpbQ3p.lMSsJ1sCUWqX99LlRz3UBt7KjmxvT2RPwL0ejnH2OP4/qi2o/W/XrsUK/p3bevMK/1:16870:0:99999:7:::

Otisk hesla (typicky MD5)
Informace o platnosti hesla, jak dlouho s musí, nesmí změnit, doba do zablokování účtu apod.

- **Uživatelé mají různá práva**
  - Přidělení práv jiného uživatele su (substitute user)
    - > su test ---> přihlášení se jako uživatel test
    - > su ---> přihlášení se jako root
  - Provedení akce s právy superuživatele sudo
    - > sudo whoami ---> root
    - > sudo -i ---> spustí shell s právy superuživatele (roota)
    - Doba přihlášení je omezená
    - exit pro odhlášení

Uživatelé III správa uživatelů

- **Přes GUI**
- **V příkazové řádce**
  - Přidání uživatele: useradd, adduser
    - > sudo useradd milan
    - > sudo useradd -m petr -d /home/pavel -s /usr/bin/octave
  - Odstranění uživatele: userdel, deluser
    - > sudo userdel -r milan --->odstraní včetně „home“
  - Modifikace /etc/passwd -> blokace uživatele
    - test:*:1001:1001::/home/test:/bin/bash ---> uživatel test se nebude moci přihlásit
  - Změna hesla passwd
    - > sudo passwd petr ---> změní heslo uživatele petr
    - > passwd ---> změna vlastního hesla
  - Modifikace uživatelů usermod
  - Konfigurace sudo: /etc/sudoers
    - Kdo, kde může spouštět co s právy roota
    - Nástroj visudo
    - Více např: http://www.linuxsoft.cz/article.php?id_article=493

Skupiny

- **Organizace uživatelů do skupin**
- **Informace o skupinách /etc/group**

```
root:x:0:
sshd:x:74:
kubera:x:1000:kubera
test:x:1001:
```

  - Formát: jméno skupiny:x:GID:seznam členů
  - Vytvoření skupiny : groupadd
    - > sudo groupadd devel
  - Přidání existujícího uživatele do skupiny
    - > sudo usermod -g devel test --->přidá do primární skupiny
    - > sudo usermod -G petr test ---> přidá do sekundární skupiny
  - Přidání nového uživatele useradd -g skupina
  - Odstranění skupiny: groupdel
    - > sudo groupdel devel
  - > id -a test ---> výpis skupin uživatele test

Práva souborů a adresářů I

- **Rozlišujeme práva:**
  - Uživatel (u)
  - Skupina (g)
  - Ostatní (o)
  - u+g+o=a

-rw-rw-r--. 1 kubera kubera 0 10. bře 05.54 test.txt

chmod a-r,u+x,g=rwx test.txt

--wxrwx---. 1 kubera kubera 0 10. bře 14.49 test.txt

- **Práva u souborů:**
  - r -může soubor číst
  - w -může do souboru zapisovat (odstraňovat NE??)
  - x -může soubor spouštět, **program má práva toho kdo jej spustil !**
- **Práva u adresářů: chmod -R ... aplikuje rekurzivně**
  - r –může číst obsah adresáře
  - w -může modifikovat obsah adresáře
  - X -může do adresáře vstupovat

Práva souborů a adresářů II

- **Číselné vyjádření práv**
  - Pro každou akci a skupinu číslo
    - r – 4
    - w – 2
    - x – 1
  - > chmod 764 test.txt --->-rwx|rw-|r-- .....
- **Defaultní maska umask --->0002**
  - Adresáře: 0777-0002--->0775=rwx|rwx|r-x
  - Soubory: 0666-0002--->0664=rw-|rw-|r--

Práva souborů a adresářů III

- **Příznak suid (set user ID) - číselně 4**
  - Program má práva vlastníka programu, nikoliv toho kdo jej spustil: např. passwd

    -rwsr-xr-x. 1 root root 27864 18. srp 2014 /usr/bin/passwd číselně: 4655
  - **> chmod u+s ...**
- **Příznak sgid (set group ID) - číselně 2**
  - Program přebírá práva skupiny
  - Nově vytvořený dresář „dědí“ práva od skupiny rodiče, nikoliv od tvůrce.
  - > chmod g+s ...
- **Sticky bit - číselně 1**
  - Umožňuje výmaz souboru pouze jeho vlastníkovi, nikoliv tomu kdo může zapisovat do adresáře
  - Do adresáře tmp mohou zapisovat všichni, mazat však jen vlastníci souborů
  - >chmod +t

Další libůstky

- **ACL – jemnější systém práv**
  - Možnost přidělit práva jmenovitě uživatelům
  - setfacl, getfacl
- **Změna vlastníka – chown**
  - >sudo chown uzivatel soubor
  - Rekurzivní změna -R
- **Změna skupiny – chgrp**
  - >sudo chown skupina soubor
  - Rekurzivní změna -R

Atributy

- **Specifické chování k souborům**
  - Podpora na většině linuxových file systémů
  - Výpis lsattr (podobně jako ls)
  - Nastavení atributů chattr
    - Pouze append: +a, -a (root)
    - Neměnnost souboru: +i, -i (root)
    - Automatická komprese: +c, -c
    - Přepsání dat nulami při výmazu: +s
  - > sudo chattr +aic soubor.txt
  - > lsattr soubor.txt ---> ----ia--c----e-- soubor.txt