# 23. Uživatelé v Unixu

## Obsah

- Definice uživatele
- Vnější a vnitřní identita
- Skupiny uživatelů
- Vztah mezi uživatelem, procesem a souborem
- Lokální soubory definující uživatele
- Základní principy administrace uživatelů

## Definice uživatele

V unixových systémech představuje uživatel entitu, která může: - Přihlásit se do systému - Spouštět procesy - Vlastnit soubory a adresáře - Mít přidělena specifická práva a omezení

Unixové systémy jsou víceuživatelské, což znamená, že umožňují současnou práci více uživatelů, přičemž každý má své vlastní prostředí a přístupová práva. Tento koncept je základním stavebním kamenem bezpečnostního modelu Unixu.

## Vnější a vnitřní identita

Každý uživatel má v systému Unix dvě základní identity:

#### Vnitřní identita (UID - User ID)

- Číselný identifikátor uživatele
- Pro systém je primární (systém pracuje s UID, nikoliv se jmény)
- Nemění se po celou dobu existence uživatelského účtu
- Je uvedena v souboru `/etc/passwd`

#### Vnější identita (username)

- Textový identifikátor (přihlašovací jméno)
- Slouží pro interakci s uživatelem
- Může být změněna bez změny UID

#### Rozsahy UID

Unixové systémy tradičně používají různé rozsahy UID pro různé typy uživatelů:

- **0**: root (superuživatel, administrátor)
- **1-99**: systémoví uživatelé (daemon, bin, sys, ...)
- **100-999**: systémové účty a skupiny
- **1000+**: běžní uživatelé (v moderních distribucích)

Příklady speciálních uživatelů: - **root (UID 0)** - superuživatel s neomezenými právy - **nobody** - uživatel s minimálními právy, používaný některými službami - **daemon** - používaný démonovými procesy - **www-data** - používaný webovým serverem

## Skupiny uživatelů

Skupiny slouží k organizaci uživatelů a usnadnění správy přístupových práv. Místo přidělování práv jednotlivým uživatelům lze práva přidělit skupině, a tím i všem jejím členům.

#### Typy skupin

#### Primární skupina

- Každý uživatel patří do jedné primární skupiny

- Určena v souboru `/etc/passwd` jako GID (Group ID)
- Nově vytvořené soubory jsou automaticky přiřazeny této skupině

#### Sekundární skupiny

- Uživatel může patřit do libovolného počtu sekundárních skupin
- Definovány v souboru `/etc/group`
- Umožňují uživateli přístup k prostředkům sdíleným v rámci těchto skupin

#### Specifikace skupin v `/etc/group`

Formát záznamu v souboru `/etc/group`:

```
nazev_skupiny:heslo:GID:seznam_uzivatelu
```

Příklad:

```
admin:x:100:john,mary,tom
```

Význam polí: 1. **Název skupiny**: textový identifikátor skupiny 2. **Heslo**: většinou nepoužívané (historický relikt), označeno `x` 3. **GID**: číselný identifikátor skupiny 4. **Seznam uživatelů**: uživatelé, kteří mají tuto skupinu jako sekundární (oddělení čárkami)

## Vztah mezi uživatelem, procesem a souborem

Vztah mezi uživateli, procesy a soubory je klíčový pro bezpečnostní model Unixu.

#### Uživatel a proces

- **Identita procesu**: Každý proces běží pod identitou konkrétního uživatele (EUID - Effective User ID)
- **Dědičnost identity**: Proces dědí identitu od uživatele, který ho spustil, nebo od rodičovského procesu
- **Práva procesu**: Proces má stejná práva jako uživatel, pod jehož identitou běží
- **Přístup k procesům**: Uživatel může zasahovat pouze do svých vlastních procesů (s výjimkou roota)

#### Speciální případy

- **SUID (Set User ID)**: Když je u spustitelného souboru nastaven bit SUID, proces spuštěný tímto souborem poběží pod identitou vlastníka souboru, nikoliv spouštějícího uživatele
- **SGID (Set Group ID)**: Podobné jako SUID, ale týká se skupiny

#### Uživatel a soubor

- **Vlastnictví souborů**: Každý soubor a adresář má svého vlastníka (uživatele) a skupinu
- **Přístupová práva**: Určují, kdo a jak může se souborem pracovat (čtení, zápis, spuštění)
- **Tvorba souborů**: Při vytvoření souboru se stává jeho vlastníkem uživatel, který jej vytvořil
- **Skupina souboru**: Nově vytvořené soubory jsou přiřazeny primární skupině uživatele, který je vytvořil (výjimka: adresář s nastaveným SGID - soubory dědí skupinu adresáře)

**Přístupová práva k souborům** Základní přístupová práva se vztahují na tři kategorie: - **Vlastník** (u) - **Skupina** (g) - **Ostatní** (o)

Pro každou kategorii lze nastavit tři typy práv: - **Čtení** (r) - hodnota 4 - **Zápis** (w) - hodnota 2 - **Spuštění/vstup** (x) - hodnota 1

Příklad zápisu práv:

```
-rw-r--r--
```

Význam: - První znak: typ souboru (`-` běžný soubor, `d` adresář, ...) - Následující tři znaky: práva vlastníka (`rw-`) - Další tři znaky: práva skupiny (`r--`) - Poslední tři znaky: práva ostatních (`r--`)

## Lokální soubory definující uživatele

V unixových systémech existuje několik klíčových souborů pro definici uživatelů a skupin:

### Samostatná stanice

U samostatných stanic (nikoliv v síti) jsou uživatelé definováni v lokálních souborech.

### Stanice v síti

U stanic v síti je běžná kombinace lokálních souborů (pro systémové uživatele) a sdílené databáze (pro běžné uživatele), jako jsou NIS, LDAP nebo Active Directory.

### Hlavní konfigurační soubory

`/etc/passwd` Základní soubor s informacemi o uživatelích.

Formát záznamu:

```
username:x:UID:GID:GECOS:home_directory:login_shell
```

Příklad:

```
mark:x:1001:1001:Mark Smith,,,:/home/mark:/bin/bash
```

Význam polí: 1. **Username**: přihlašovací jméno 2. **Password**: dříve obsahoval zašifrované heslo, nyní většinou `x` (heslo je v `/etc/shadow`) 3. **UID**: číselný identifikátor uživatele 4. **GID**: číselný identifikátor primární skupiny 5. **GECOS**: plné jméno a další informace (čárkami oddělené) 6. **Home directory**: domovský adresář uživatele 7. **Login shell**: shell spouštěný po přihlášení

`/etc/shadow` Obsahuje zašifrovaná hesla a informace týkající se platnosti účtů.

Formát záznamu:

```
username:encrypted_password:last_change:min_days:max_days:warn_days:inactive_days:expire_date
```

Příklad:

```
mark:$6$.n.:17736:0:99999:7:::
```

Význam polí: 1. **Username**: přihlašovací jméno 2. **Encrypted password**: zašifrované heslo ve formátu `$alg$salt$hash` - `$6$` označuje algoritmus SHA-512 - Pokud je zde `*` nebo `!`, účet je uzamčen 3. **Last change**: den poslední změny hesla (počet dnů od 1.1.1970) 4. **Min days**: minimální počet dnů mezi změnami hesla 5. **Max days**: maximální platnost hesla ve dnech 6. **Warn days**: počet dnů před vypršením hesla, kdy je uživatel varován 7. **Inactive days**: počet dnů neaktivity po vypršení hesla, po kterých je účet uzamčen 8. **Expire date**: datum vypršení platnosti účtu (počet dnů od 1.1.1970)

`/etc/group` Definuje skupiny a jejich členy.

Formát záznamu:

```
group_name:password:GID:user_list
```

Příklad:

```
developers:x:1005:john,mark,lisa
```

Význam polí: 1. **Group name**: název skupiny 2. **Password**: většinou nepoužívané, označeno `x` 3. **GID**: číselný identifikátor skupiny 4. **User list**: seznam uživatelů, kteří jsou členy této skupiny (mimo jejich primární skupinu)

`/etc/gshadow` Obsahuje zašifrovaná hesla skupin a informace o administrátorech skupin.

`/etc/sudoers` Definuje, kteří uživatelé mohou používat příkaz `sudo` a s jakými oprávněními.

Formát záznamu:

```
user host=(run_as) command
```

Příklad:

```
john ALL=(root) /usr/sbin/shutdown
```

Tento soubor by měl být editován pouze pomocí příkazu `visudo`, který kontroluje správnost syntaxe.

## Základní principy administrace uživatelů

### Příkazy pro správu uživatelů

### Vytvoření uživatele

```
# Základní vytvoření uživatele
useradd username

# Vytvoření s dalšími parametry
useradd -m -g primary_group -G secondary_groups -s /bin/bash username
```

Parametry: - `-m`: vytvoří domovský adresář - `-g`: specifikuje primární skupinu - `-G`: specifikuje sekundární skupiny (oddělené čárkami) - `-s`: specifikuje login shell

### Úprava existujícího uživatele

```
# Změna údajů uživatele
usermod -G new_groups username

# Uzamčení účtu
usermod -L username

# Odemčení účtu
usermod -U username
```

### Smazání uživatele

```
# Smazání uživatele
userdel username

# Smazání včetně domovského adresáře
userdel -r username
```

### Správa hesel

```
# Nastavení hesla uživatele
passwd username

# Změna vlastního hesla
passwd

# Nastavení vypršení hesla
chage -d 0 username  # Vynutí změnu hesla při dalším přihlášení
```

### Přepínání uživatelů

```
# Přepnutí na jiného uživatele
su username
```

```
# Přepnutí na jiného uživatele včetně prostředí
su - username

# Spuštění příkazu jako jiný uživatel
su -c "command" username
```

### Příkaz sudo

Příkaz `sudo` umožňuje spouštět příkazy s právy jiného uživatele (typicky roota).

```
# Spuštění příkazu jako root
sudo command

# Spuštění příkazu jako jiný uživatel
sudo -u username command

# Seznam příkazů, které může aktuální uživatel spouštět přes sudo
sudo -l
```

Výhody použití sudo: - Detailní kontrola nad tím, které příkazy může uživatel spouštět - Zaznamenávání všech příkazů pro účely auditu - Není nutné sdílet heslo roota - Zvýšení bezpečnosti systému

### Správa skupin

```
# Vytvoření nové skupiny
groupadd groupname

# Úprava existující skupiny
groupmod -n new_name old_name

# Smazání skupiny
groupdel groupname

# Přidání uživatele do skupiny
usermod -a -G groupname username
gpasswd -a username groupname

# Odebrání uživatele ze skupiny
gpasswd -d username groupname

# Zobrazení skupin aktuálního uživatele
groups

# Zobrazení skupin konkrétního uživatele
groups username
```

### Kontrola identity a příslušnosti ke skupinám

```
# Zobrazení identity aktuálního uživatele
id

# Zobrazení identity konkrétního uživatele
id username

# Zobrazení aktuálního uživatelského jména
whoami

# Zobrazení efektivního UID
id -u
```

```
# Zobrazení efektivního GID
id -g
```

### Proces přidání nového uživatele

Manuální proces: 1. Přidání řádku do `/etc/passwd` 2. Přidání řádku do `/etc/shadow` (nastavení hesla) 3. Vytvoření domovského adresáře 4. Nastavení vlastnictví a oprávnění domovského adresáře 5. Kopírování výchozích souborů do domovského adresáře (z `/etc/skel`)

Automatizovaný proces:

```
useradd -m -g users -G wheel,developers -s /bin/bash john
passwd john
```

### Správa přístupových práv

```
# Změna vlastníka souboru
chown username:groupname file

# Rekurzivní změna vlastníka adresáře a jeho obsahu
chown -R username:groupname directory

# Změna skupiny souboru
chgrp groupname file

# Změna přístupových práv
chmod 644 file  # rw-r--r--
chmod 755 directory  # rwxr-xr-x

# Symbolický zápis
chmod u+x file  # Přidá právo spouštění pro vlastníka
chmod g-w file  # Odebere právo zápisu pro skupinu
chmod o=r file  # Nastaví ostatním pouze právo čtení
```

### Pokročilé koncepty

### SUID, SGID a Sticky bit

```
# Nastavení SUID bitu (spuštění s právy vlastníka)
chmod u+s file  # nebo chmod 4755 file

# Nastavení SGID bitu (spuštění s právy skupiny)
chmod g+s file  # nebo chmod 2755 file

# Nastavení SGID na adresář (nové soubory dědí skupinu adresáře)
chmod g+s directory

# Nastavení sticky bitu (jen vlastník může mazat soubory v adresáři)
chmod +t directory  # nebo chmod 1777 directory
```

**Změna identity procesu** V programech:

```
// Změna efektivního UID
#include <unistd.h>

int seteuid(uid_t euid);
```

### Praktické příklady

#### Skript pro vytvoření více uživatelů

```
#!/bin/bash
# bulk_create_users.sh - vytvoří více uživatelů ze seznamu

# Seznam uživatelů ve formátu: username:full_name:groups
USERS_FILE="users.txt"

if [ ! -f "$USERS_FILE" ]; then
    echo "Soubor $USERS_FILE neexistuje!"
    exit 1
fi

while IFS=: read -r username fullname groups; do
    # Přeskočit prázdné řádky nebo komentáře
    if [ -z "$username" ] || [[ "$username" == \#* ]]; then
        continue
    fi

    echo "Vytvářím uživatele: $username"
    useradd -m -c "$fullname" -s /bin/bash "$username"

    if [ -n "$groups" ]; then
        echo "Přidávám do skupin: $groups"
        usermod -a -G "$groups" "$username"
    fi

    # Nastavení náhodného hesla a vynutí jeho změnu při prvním přihlášení
    password=$(openssl rand -base64 12)
    echo "$username:$password" | chpasswd
    passwd -e "$username"

    echo "Uživatel $username vytvořen s heslem: $password"
    echo "----------------------------------------"
done < "$USERS_FILE"

echo "Hotovo!"
```

#### Skript pro audit uživatelských účtů

```
#!/bin/bash
# audit_users.sh - kontroluje neaktivní a nezabezpečené účty

echo "Kontrola účtů bez hesla:"
awk -F: '($2 == "" || $2 == " ") {print $1}' /etc/shadow

echo -e "\nÚčty s UID 0 (rootovská oprávnění):"
awk -F: '($3 == 0) {print $1}' /etc/passwd

echo -e "\nNeaktivní účty (nepřihlášeni > 90 dnů):"
THRESHOLD=$(date --date="90 days ago" +%s)
while IFS=: read -r username _ _ _ _ _ _ last_change _; do
    if [ -z "$last_change" ] || [ "$last_change" == " " ]; then
        continue
    fi

    last_login=$(date --date="1970-01-01 + $last_change days" +%s)
```

```
    if [ "$last_login" -lt "$THRESHOLD" ]; then
        echo "$username (poslední aktivita: $(date --date="@$last_login" "+%Y-%m-%d"))"
    fi
done < /etc/shadow
```