

Lektionstillfälle 5

Användare och rättigheter
med Mikael Larsson

Återblick

Sist jobbade vi mer direkt med boken än tidigare.

Vi pratade om:

- Linux-distributioner och pakethanterare
- Linux filstruktur
- Filsystem-kommandon
- Länkar
- Rättigheter
- Att söka efter filer

Dagens lektion

Mål: Att kunna hantera användare, grupper och rättigheter

- Mer om filrättigheter
- Processrättigheter
- Lägga till användare
- Hantera grupper
- Olika slags användare
- su och sudo

Termer och begrepp

- Hashade lösenord
- /etc/passwd och /etc/shadow
- Primär grupp och sekundära grupper
- Numeriska ID
- Process, barnprocess och förälderprocess

Lite mer om filrättigheter

Användare och grupper

Alla användare är medlemmar i en **primär** grupp. I Ubuntu skapas en grupp per användare med samma namn som användaren.

Användare kan också vara med i ett antal sekundära grupper. De används ofta till att ge användaren tillgång till vissa program och systemresurser.

Grupptillhörighet, shell, etc. sätts vid inloggning.

Vem är jag?

- whoami
- groups
- id

Var bor användarna?

Användardatabasen är **/etc/passwd** som standard.

/etc/passwd anger

- Användarnamn
- Användar-ID
- Primär grupp-ID
- Hemkatalog
- Shell

..men inte lösenord!

Linux använder ett plugin-system för autentifiering som heter "pam" – "Pluggable Authentication Modules".

Det finns många olika sätt att hantera användare centralt på, istället för lokalt i **/etc/passwd**.

Ett sådant sätt är LDAP, som använder modulen ***pam_ldap***.

Grupper och lösenord

- Grupperna definieras i **/etc/group**
- Lösenord ligger i **/etc/shadow**, som bara "root" kan läsa.

Lösenord lagras alltid hashade och saltade, aldrig i klartext. Hashade lösenord får inte innehålla '*', så användare som inte ska logga in har lösen-hash '*'.

Numeriska ID

- Root har användar-ID noll.
- Vanliga användare börjar på 1000.
- Det är numeriska ID som spelar roll, namnet bara i /etc/passwd.

? Kan en användare byta namn?

? Kan filer ägas av användare som inte finns i /etc/passwd?

? Vad händer med användarna och deras filer om jag flyttar en hårddisk från ett Linux-system till ett annat?

Processer och användare

- Alla processer körs som en användare.
- Processen ärver samma rättigheter som användaren har.
- Alla processer har också ett numeriskt ID, "pid".
- Processer kan skapa nya processer, som då blir barnprocesser.
- Alla processer har en förälderprocess, förutom "systemd", den första processen som startar.

Använd "ps" för att lista processer, och "pstree" för att se trädet med processer från "systemd" och nedåt.

"ps -ef" listar alla systemets processer, inklusive kärntrådar.

"pstree 0" visar motsvarande bild som ett träd

Processer och filer

Allting är filer i Linux – men för att göra någonting med en fil behövs en process.

När en fil används säger man att den **hålls öppen** av en process.

- För att se vilka processer som använder en fil, används "fuser".
- För att se vilka filer en viss process använder, används "lsof". Ofta används "lsof -p <pid>".

Laboration 1

Tre uppgifter för att undersöka filer, numeriska ID och processer.

Se studentportalen.

Administrera användare

Kommandon för att administrera användare:

- useradd
- usermod
- userdel
- passwd

Kommandon för att administrera grupper:

- groupadd
- groupmod
- groupdel

Tips: Det finns ett hjälpverktyg för att lägga till användare som heter "adduser", som i sin tur använder:

```
useradd --create-home <user>
```

```
passwd <user>
```

```
chfn <user>
```

Olika slags användare

Systemanvändare – ”system account”

- Inget hem
- Användar-ID under 1000
- Ingen login

Används för att köra specifika tjänster och avgränsa rättigheter så mycket som möjligt

Systemparametrar för login sätts i

- `/etc/login.defs` och `/etc/default/useradd` resp. `/etc/adduser.conf`
- `/etc/pam.d`

su och sudo

TLCL s101

"su" = **"substitute user"**, byter ut nuvarande användare. Kräver lösenord för den användare man byter till.

"sudo" = **"su do"**, exekverar ett kommande som en annan användare. Kräver nuvarande användares lösenord.

Bara användare godkända i **/etc/sudoers** får göra **"sudo"**.

Laboration 2

Labb baserad på "Excercising Our Privileges"
TLCL s106-108.

Följ instruktionerna för att sätta upp en delad musik-katalog.

Följande skillnader:

- Använd kommandoraden istället för GUI
- Lägg till de användare som behövs, se till att de får hemkataloger och "bash" som shell.
- Verifiera att du kan logga in som användarna
- "umask" behöver inte justeras, den är 0002 som standard på Ubuntu
- Efter setup, testa att det funkar som tänkt genom att lägga upp och läsa filer i den delade mappen.

Laboration 3

Se studentportalen.

Summering

Idag har vi behandlat:

- Mer om filrättigheter
- Processrättigheter
- Användare, filer och processer
- Att lägga till användare och grupper
- Olika slags användare
- su och sudo

Frågor?

Nästa gång

Mål: Att veta hur program startas, pausas och avbryts

- PATH
- Argument
- Inmatning, utmatning och omdirigering
- Förgrunds- och bakgrundsprocesser
- Jobbkontroll
- Exit codes
- Signaler*

**överkurs*

Stort tack!