

Linux: Command Line Interface

D. Leeuw

5 april 2025
v.0.9.5



© 2020-2025 Dennis Leeuw

Dit werk is uitgegeven onder de Creative Commons BY-NC-SA Licentie en laat anderen toe het werk te kopiëren, distribueren, vertonen, op te voeren, en om afgeleid materiaal te maken, zolang de auteurs en uitgever worden vermeld als maker van het werk, het werk niet commercieel gebruikt wordt en afgeleide werken onder identieke voorwaarden worden verspreid.

Over dit Document

0.1 Leerdoelen

Na het bestuderen van dit document heeft de lezer kennis van:

- het gebruik van gebruikers en groepen
- waar gebruikers en groepen worden opgeslagen op het systeem
- de commando's: `id`, `adduser`, `deluser`, `usermod`, `passwd`, `gpasswd`

Dit document sluit aan op de volgende onderdelen van de LPI:

- LPI Linux Essentials 010-160 - 6.5.1 Basic Security and Identifying User Types (weight: 2)
- LPI Linux Essentials 010-160 - 6.5.2 Creating Users and Groups (weight: 2)

0.2 Voorkennis

Voor een goed begrip van dit document wordt er van de lezer verwacht dat deze kennis heeft van:

- de commando's: `ls`, `grep`
- omgaan met quoting en escaping en wat dat betekent
- het documentatie systeem (`man`)

Inhoudsopgave

Over dit Document	i
0.1 Leerdoelen	i
0.2 Voorkennis	i
1 Gebruikers, groepen en rechten	1
1.1 Gebruikers	1
1.2 Groepen	3
1.3 UPG	3
2 Werken als root	5
2.1 su	5
2.2 sudo	6
3 Gebruikersbeheer	7
3.1 Gebruikers toevoegen	7
3.1.1 User: wachtwoorden	7
3.2 Groepen toevoegen	7
3.2.1 Group: wachtwoorden	8
3.3 Wijzigen van een gebruiker	8
3.4 Verwijderen van een groep	8
3.5 Verwijderen van een user	8
Index	9

Hoofdstuk 1

Gebruikers, groepen en rechten

Het Unix besturingssysteem en dus ook Linux is altijd bedoeld geweest als multi-user systeem. Het was dus de bedoeling om meer dan één gebruiker op een systeem te laten werken. Bij het ontwerp is er dan ook rekening mee gehouden dat er rechten moesten zijn voor verschillende gebruikers en ook is er van het begin af aan rekening gehouden met dat mensen in groepen zouden moeten kunnen samenwerken.

Dit hoofdstuk gaat over deze gebruikers en groepen en vertelt hoe je de rechten per gebruiker en groep kan zetten.

1.1 Gebruikers

Bij het inloggen heb je een gebruikersnaam en wachtwoord opgegeven en bij de installatie heb je ook een wachtwoord moeten opgeven voor de gebruiker root. Op het systeem zijn dus minimaal al twee gebruikers aanwezig. Op een Linux systeem kunnen ook processen een gebruiker hebben. Dus een proces kan onder een bepaalde gebruiker werken zodat andere gebruikers niet bij dit proces kunnen. Processen zijn taken die op de achtergrond draaien zoals bijvoorbeeld een webserver.

De database met gebruikersnamen is een bestand dat staat in de `/etc` directory. Het bestand heet `passwd` en dat kan je bekijken met `less`.

```
$ less /etc/passwd
```

De wachtwoorden staan in een ander bestand, dat heet `shadow`. Dit bestand kan je met `less` niet bekijken, omdat alleen de beheerder (root) hier rechten voor heeft. De wachtwoorden zijn niet leesbaar, maar ge-encrypt, opgeslagen. Met het `passwd`-commando kan je je wachtwoord wijzigen.

Gebruik `grep` om je eigen gegevens uit `/etc/passwd` te halen:

```
$ grep dennis /etc/passwd
```

vervang hierbij *dennis* door je eigen gebruikersnaam.

De output van de vorige commando zal er ongeveer zo uit zien:

```
dennis:x:1000:1000:Dennis Leeuw,,,:/home/dennis:/bin/bash
```

Het **passwd** bestand is een soort database waarin de verschillende elementen (velden) gescheiden zijn door een **:**. Computers werken met getallen, het zijn rekenaars, dus elke gebruiker en elke groep heeft een nummer. De gebruikersnaam en groepsnaam zijn er voor ons mensen, de nummers voor de computer. Het nummer voor de gebruiker noemen we het UID of User ID en het getal voor de groep het GID of Group ID.

De verschillende velden van het **/etc/passwd** bestand bevatten, van voor naar achter, deze informatie:

1. gebruikersnaam (login-naam)
2. dit veld werd vroeger gebruikt voor het wachtwoord, nu staat er altijd een **x**. Wachtwoorden staan nu in het **shadow** bestand.
3. numerieke ID van de gebruiker (UID: User ID). De UID's 0-999 zijn gereserveerd voor het systeem en 1000 en hoger zijn vrij te gebruiken voor gebruikers. Het root-account heeft altijd UID 0.
4. numerieke ID van de primaire groep van de gebruiker (GID: Group ID). De GID's 0-999 zijn gereserveerd voor het systeem.
5. extra informatie over de gebruiker, met komma's gescheiden. Heet ook wel het GECOS-field en kan dan de volgende informatie bevatten:
 - (a) Volledige naam van de gebruiker
 - (b) Adres gegevens van de gebruiker (gebouw en kamernummer)
 - (c) Werk telefoonnummer
 - (d) Thuis telefoonnummer
 - (e) Overige contact informatie (fax, prive e-mail adres, pager, social media)
6. de home-directory van de gebruiker
7. de shell die wordt opgestart als de gebruiker inlogt

1.2 Groepen

Elke gebruiker is ook lid van minimaal 1 groep, de primaire groep zoals opgegeven in `/etc/passwd`. Op sommige systemen is dat de groep **users** op andere systemen is dat een andere groep. Om te zien van welke groepen je lid bent kan je `id` gebruiken.

```
$ id
```

De output geeft weer dat je maar één UID hebt en één of meer GID's. Je kan dus lid zijn van meer groepen. De eerste groep is de standaard (default) groep waarvan je lid bent.

In de output zie je ook dat elk UID en elke GID eigenlijk een nummer is. Computers kunnen alleen met getallen werken, terwijl wij mensen beter met namen om kunnen gaan. Vandaar dat het besturingssysteem steeds een vertaling maakt van naam naar getal.

Zoek uit hoe je `id` alleen het numerieke ID terug kunt laten geven en hoe je `id` alleen de naam van je primaire groep kan laten weergeven.

De “database” met groep informatie vind je in `/etc/group`. Je kan de naam van bijvoorbeeld je primaire groep terug vinden door een `grep` te doen op `:GID:`, dus in het voorgaande voorbeeld zou dat betekenen:

```
$ grep :1000: /etc/group
```

de dubbele punten om het id is om te voorkomen dat je bijvoorbeeld ook groep ID 10000 of 10001 terug krijgt.

1.3 UPG

User Personal Group of UPG is een gecombineerd gebruik van de user-ID en de group-ID voor het opslaan van data. Er is bij gebruik van UPG ook een groepsnaam met de gebruikersnaam.

In de voorgaande voorbeelden zag je het gebruik van UPG. De gebruiker dennis heeft een UID van 1000 en een GID van 1000 en beide zijn gekoppeld aan de naam dennis. Dus de groepsnaam is gelijk aan de gebruikers naam (de numerieke ID's hoeven niet gelijk te zijn, maar zijn dat vaak wel). De gebruiker is dus niet lid van de groep **users** waar op sommige andere systemen elke gebruiker lid van is.

Door gebruik te maken van een groep **users** waar elke gebruiker lid van is maak je het delen van informatie met andere gebruikers makkelijker omdat iedereen een gedeelde groep heeft. Data die toegankelijk is voor de groep **users** is dus toegankelijk voor iedereen.

UPG is meer gericht op veiligheid. Omdat elke gebruiker alleen in zijn eigen groep zit kan er standaard geen data gedeeld worden. Data kan alleen gedeeld worden als er een groep aangemaakt wordt waaraan gebruikers worden toegevoegd. Die groep kan dan data met elkaar delen. Verder is alle data die je maakt alleen toegankelijk voor jezelf.

Hoofdstuk 2

Werken als root

De root-gebruiker is op een Linux-systeem almachtig. Deze gebruiker mag alles inclusief het systeem stuk maken en dat is helemaal niet zo moeilijk om te doen. Juist omdat root alles mag is het niet verstandig om als de root gebruiker op een systeem te werken. Doe zoveel mogelijk als een normale gebruiker. Pas als het echt niet anders kan doe je het als root.

Inloggen als root zou je eigenlijk nooit moeten doen. Als je iets als root wilt doen gebruik je **sudo** (Super User Do), zie daarvoor de volgende sectie.

Om te werken als een andere gebruiker is er **su** (switch user), dit kan je natuurlijk ook gebruiken om root te worden en die verleiding is waarschijnlijk groot. Maar wen jezelf aan om dat niet te doen en **sudo** te gebruiken om handelingen als root uit te voeren.

2.1 su

Met het commando **su** (switch user) kan je een werken als een andere gebruiker, mits je het wachtwoord weet van die gebruiker.

Om ook alle omgevingsvariabelen van die gebruiker mee te krijgen moet je aan **su** het min-teken(-) meegeven. Dat ziet er dan zo uit:

```
$ su - mies
```

De kans dat mies bestaat op ons systeem is niet zo groot. De gebruiker waarvan we zeker weten dat deze wel bestaat is onze root gebruiker:

```
$ su -
```

We hebben bij de switch naar root niet opgegeven dat we de root gebruiker willen worden. Als er bij **su** geen naam wordt opgegeven gaat **su** ervan uit dat je root wil worden. Met het **exit** commando kom je weer terug naar je eigen omgeving.

Voor het installeren van software moet je root zijn. Een gewone gebruiker mag dat niet. We gaan nu eenmalig het **sudo** packet installeren als root gebruiker, zodat we hierna **sodu** kunnen gebruiken.

```
$ su -  
# apt-get install sudo  
# usermod -a -G sudo dennis
```

We hebben het sudo-packet geïnstalleerd en de gebruiker (dennis, die je natuurlijk weer vervangen hebt door je eigen gebruikersnaam) toegevoegd (-a is append) aan de groep sudo (-G sudo) die rechten heeft om **sudo** te gebruiken.

Als we met **exit** de omgeving van root verlaten en weer terug zijn in ons eigen account dan typen we nog een keer **exit** zodat we uitgelogd zijn. Als we daarna weer inloggen kunnen we met **id** zien dat we nu een extra (sudo) groep hebben waarvan we lid zijn.

2.2 sudo

Met het **sudo** (super user do) commando kan je commando's uitvoeren alsof ze van root zijn, je moet daar dan natuurlijk wel de rechten voor hebben niet iedereen mag dat doen. Wie die rechten heeft wordt bepaald door het **/etc/sudoers** bestand of door bestanden in de **/etc/sudoers.d** directory of, zoals we eerder gezien hebben, door lid te zijn van de sudo-groep.

Om te zien wat er in de home-directory van root staat kan je het volgende commando geven:

```
$ sudo ls /root
```

Hiermee hebben we aangetoond dat we commando's als root kunnen uitvoeren.

Hoofdstuk 3

Gebruikersbeheer

3.1 Gebruikers toevoegen

Om gebruikers toe te voegen aan het systeem zijn er twee tools. De eerste is **useradd** en de andere is **adduser**. Het programma **useradd** is een low-level tool, de standaard manier om gebruikers aan te maken is via **adduser** en dat is dan ook wat we gaan gebruiken.

```
$ sudo adduser eengebruiker
```

Om gebruikers te kunnen aanmaken hebben we root-rechten nodig, dus we gebruiken het **sudo** commando.

Het **adduser** commando maakt bijna alles automatisch aan. Het enige dat je hoeft te doen is te vertellen wat het wachtwoord van de gebruiker is en welke informatie er in het GECOS-veld terecht moet komen.

Je mag aan **adduser** ook meegeven dat zaken anders moeten zijn. Bijvoorbeeld dat een gebruiker een andere shell gebruikt dan bash. Dat kan door de optie **-shell /bin/chsh** mee te geven. Lees de man-page van **adduser** eens door met wat er nog meer mogelijk is.

Als op het systeem UPG gebruikt wordt dan zal je zien dat er ook gelijk een groep voor de gebruiker aangemaakt is. Gebruik **id** om te zien wat de ID is van de nieuwe gebruiker.

3.1.1 User: wachtwoorden

3.2 Groepen toevoegen

We gaan nu een extra groep aanmaken:

```
$ sudo addgroup specialgroup
```

deze groep is nu toegevoegd aan het `/etc/group` bestand.

3.2.1 Group: wachtwoorden

Om een gebruiker toe te voegen aan een groep, gebruiken we `gpasswd`. `gpasswd` is een tool om groepen te beheren.

Om een gebruiker aan een groep toe te voegen gebruiken we:

```
$ sudo gpasswd -a eengebruiker specialgroup
```

om diezelfde gebruiker weer uit de groep te halen gebruiken we:

```
$ sudo gpasswd -d eengebruiker specialgroup
```

3.3 Wijzigen van een gebruiker

Om de instellingen van een gebruiker te wijzigen gebruiken we `usermod`.

Er zijn vele zaken die we kunnen instellen voor een gebruiker. De man-page van `usermod` vermeldt ze allemaal.

3.4 Verwijderen van een groep

Om een groep weer te verwijderen is er `delgroup`. Het verwijderen van een groep betekent dat gebruikers uit de groep verdwijnen, maar eventuele bestanden op disk die van deze groep zijn veranderen niet. Je houdt dus bestanden over die numeriek nog van de groep zijn, maar waar geen groepsnaam voor is. Dus alleen de owner kan er nog bij (en root natuurlijk).

3.5 Verwijderen van een user

Het verwijderen van gebruikers kan heel simpel gedaan worden met `deluser`. Het heeft echter wel wat gevolgen. Als een gebruiker niet meer bestaat op het systeem dan kunnen er nog wel bestanden zijn die van deze gebruiker waren (zoals in zijn of haar home-directory). Numeriek zijn deze bestanden dan ook nog van het UID van de voormalige gebruiker. Alleen root kan nog bij deze bestanden, maar wat ook kan gebeuren is dat het UID opnieuw toegewezen wordt aan een nieuwe gebruiker die aangemaakt wordt. Deze gebruiker wordt dan opeens de eigenaar van de nog aanwezige bestanden. Zorg er dus voor dat de bestanden van eigenaar veranderd zijn voordat je een gebruiker verwijderd.

Index

/etc/passwd, 1

addgroup, 7

adduser, 7

commando

 addgroup, 7

 adduser, 7

 gpasswd, 8

 id, 3

 passwd, 1

 usermod, 8

commandos

 useradd, 7

delgroup, 8

deluser, 8

gpasswd, 8

grep, 1

id, 3

passwd, 1

root-gebruiker, 5

shadow, 1

su, 5

sudo, 6

super user do, 6

switch user, 5

UPG, 3

User Personal Group, 3

useradd, 7

usermod, 8