Benutzer- und Gruppeneinstellungen betrachten

whoami	Wer bin ich?
who	Welche Benutzer sind angemeldet?
last	Wer war wann angemeldet?
id	Wie heißt der aktuelle Benutzer? In welchen Gruppen ist er? Angaben von ids und Namen.
id `benutzer`	Wie lauten `uid` und `gid` sowie die zugehörigen Namen von `benutzer`?
groups `benutzer`	In welchen Gruppen ist `benutzer`?
id -gn `benutzer`	

Benutzer wechseln

su -	Zu Benutzer root wechseln
su	Zu Benutzer root wechseln (Umgebungsvariablen werden beibehalten)
su - `benutzer`	Zu `benutzer` wechseln
su -c `cmd` - `benutzer`	Befehl `cmd` als Nutzer `benutzer` ausführen
sudo -i	Zu Benutzer root wechseln mit Login-Shell (springt ins HOME-Directory von root)
sudo -s	Zu Benutzer root wechseln mit einfacher Shell (Umgebungsvariablen werden beibehalten)
sudo -u `benutzer` -i	Zu `benutzer` wechseln
sudo -u `benutzer` `cmd`	Befehl `cmd` als Nutzer `benutzer` ausführen

Benutzerverwaltung

Liste aller Benutzer anzeigen

```
getent passwd
```

Benutzer anlegen

```
useradd -m benutzer
```

Debian

```
adduser benutzer
```

anlegen überprüfen

```
grep ^benutzer /etc/passwd
```

oder

```
getent passwd benutzer
```

Systembenutzer anlegen

RedHat, SuSE, Ubuntu (ab 10.04)

```
useradd -r systembenutzer
```

[1)]

Debian

```
adduser --system --no-create-home --disabled-login systembenutzer
```

Benutzer löschen

[2)]

```
userdel -r benutzer
```

Übrig gebliebene Userfiles nach dem Löschen des Users dem Benutzer root übergeben

```
find / -xdev -uid 1002 -print0 | xargs -0 chown --no-dereference root
```

Nicht zugeordnete Dateien suchen

```
find / -xdev -nouser
find / -xdev -nogroup
```

Passwort vergeben

```
passwd benutzer
```

Benutzer muß Passwort beim nächsten login ändern

SuSE, Debian, RedHat (ab 6.0):

```
passwd -e benutzer
```

oder

```
chage -d 0 benutzer
```

Passwort Ablaufregeln einstellen

für Benutzer nutzer23

```
chage -E 2014-7-31 -M 90 -m 5 -W 21 -I 30 nutzer23
```

für alle zukünftig angelegten Benutzer

`/etc/login.defs` :

```
PASS_MAX_DAYS   90
PASS_MIN_DAYS   5
PASS_WARN_AGE   21
```

Anmerkung: Im Jahr 2020 hat sich auch das BSI vom regelmäßigen, anlasslosen Ändern von Kennwörtern verabschiedet.

Benutzer deaktivieren

[3)]

Passwort sperren:

```
passwd -l benutzer
```

oder

```
usermod -L benutzer
```

Account ungültig setzen:

```
chage -E 0 benutzer
```

oder

```
usermod -e 0 benutzer
```

Benutzer reaktivieren

Passwort entsperren:

```
passwd -u benutzer
```

oder

```
usermod -U benutzer
```

Account gültig setzen:

```
chage -E -1 benutzer
```

oder

```
usermod -e -1 benutzer
```

Gruppenverwaltung

Liste aller Gruppen anzeigen

```
getent group
```

Gruppe anlegen

```
groupadd gruppe
```

anlegen überprüfen

```
grep ^gruppe /etc/group
```

Gruppe löschen

```
groupdel gruppe
```

Benutzer einer Gruppe hinzufügen

```
gpasswd -a nutzer gruppe
```

SuSE

TODO: falsch ~~groupmod -A gruppe nutzer~~

Debian

```
adduser nutzer gruppe
```

RedHat

```
usermod -G gruppe -a nutzer
```

Benutzer aus einer Gruppe entfernen

```
gpasswd -d nutzer gruppe
```

In welchen Gruppen ist ein Nutzer Mitglied?

```
id nutzer
```

Welche Nutzer sind Mitglied einer Gruppe?

CentOS (7)

```
lid -g gruppe
```

Debian (10)

Paket libuser installieren

```
libuser-lid -g gruppe
```

Benutzer aus einer Gruppe entfernen

```
gpasswd -d nutzer gruppe
```

SuSE

TODO openSuSE 13.1 ~~groupmod -R gruppe nutzer~~

Gruppe einer Gruppe hinzufügen

Geht für sssd-Gruppen mit `sss_groupadd`, falls sssd eingesetzt wird.

Weitere Befehle

Weitere Befehle zur Benutzerverwaltung anzeigen:

Debian:

```
dpkg -L passwd | grep bin/
```

SuSE:

```
rpm -ql pwdutils | grep bin/
```

RedHat:

```
rpm -ql shadow-utils | grep bin/
```

Konfigurationsdateien

- `/etc/login.defs`
- `/etc/default/useradd` (Centos 5, openSuSE 11.3, Debian 5.0)

root-Rechte mit sudo

sudo

1)

oder besser:

```
useradd -r -d /tmp -s /bin/false systembenutzer
```

2)

nicht immer eine gute Idee: Was passiert mit den Dateien des Benutzers? Gibt es einen Mechanismus der verhindert, dass die Benutzernummer erneut vergeben wird? Oft ist es besser, den Account nur zu deaktivieren.

3)

Achtung, Falle:

```
grep -r nullok /etc/pam*
```

Wenn bei `pam_unix` `nullok` gesetzt ist, kann man sich mit dem Account jetzt ohne Passwort anmelden! Daher nie -d (Passwort löschen) ohne -l (sperren) benutzen.