ACL Konzept für Ordner und Gruppen

Nautilus ACL mit apt-get install eiciel, oder noch besser http://sourceforge.net/projects/nautilusadvacl/

Man legt für den gemeinsam benutzen Ordner zuerst zwei Gruppen in LDAP an. Hier als Beispiel „Dokumente“

Gruppe zum Schreiben und Lesen: „dokumente“ Gruppen zum Lesen: „dokumente_ro“

```
mkdir /home/Dokumente
ls -ld /home/Dokumente
drwxr-xr-x 2 root root 4096 Mär 22 22:47 Dokumente
```

Festlegen des Eigentümers und der Gruppe und setzen der Rechte

```
chown root:dokumente /home/Dokumente
chmod 770 /home/Dokumente
```

WICHTIG: Setzt man auf eine bestehenden Ordner mit bereits vorhandenen Daten auf, muss natürlich auch einmalig die Rechte gleichsetzen:

```
find /home/Dokumente -type f -exec chmod 660 {} +
find /home/Dokumente -type d -exec chmod 770 {} +
```

Setzen der Default ACL

```
setfacl -R -d -m group:dokumente:rwx /home/Dokumente
setfacl -R -d -m group:dokumente_ro:r-x /home/Dokumente
```

Setzen der ACLs

```
setfacl -R -m group:dokumente_ro:r-x /home/Dokumente
setfacl -R -m group:dokumente:rwx /home/Dokumente
```

```
find /home/Dokumente -type f -exec chmod 660 {} +
find /home/Dokumente -type d -exec chmod 770 {} +
```

Nun betrachten wir den fertigen Ordner:

```
getfacl /home/Dokumente

# file: Dokumente/
# owner: root
# group: dokumente
user::rwx
```

```
group::rwx
group:dokumente_ro:r-x
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:dokumente:rwx
default:group:dokumente_ro:r-x
default:mask::rwx
default:other::---
```

A C H T U N G
Wenn man Daten mit grafischen Dateimanagern wie Nautilus oder Dolphin (nach Ubuntu 12.04 LTS) verschiebt oder kopiert, werden immer die DefaultACLs des Zielordners angewendet (Gilt nicht für den Befehl „mv“ Bei „mv“ verbleiben alle ACL-Rechte der Quelle). Das soll so sein und das ist auch gut so. Zu beachten ist aber wenn man Daten verschiebt (Nautilus, Dolphin) werden die bestehenden Unixgruppenrechte von der Quelle mit übernommen. Das heist also es werden zwar die ACLs des Ziels übernommen, aber es werden weder Unixgruppengrechte vom User der kopiert, noch Gruppenrechte vom Ziel übernommen. Das heist, wenn man eine Datei verschiebt die der Gruppe „tux“ gehört, dann gehört sie am Ziel auch der Gruppe „tux“. Vorausgesetzt das man Rechte auf die Gruppe „tux“ hat. Hat man die nicht wird die Gruppe in die eigene Hauptgruppe umgewandelt. Dann kommen wir auch schon zum Nächsten Punkt.Dies ist relevant wenn man bestehende Daten migriert. Werden von Usern neue Dateien angelegt, werden auch seine Rechte durch die DefaultACL gesetzt. Es wird also empfohlen eine sogenannte Migrationsgruppe (z.B. „daten-firma“) anzulegen diese Gruppe den Besitz der migrierten Daten zu zuweisen. In dieser Gruppe darf natürlich niemand Mitglied sein. Die Gruppe darf auch nur immer auf den Inhalt des jeweiligen Berrechtigungspunktes angewendet werden. Denn hat ein Berrechtigungspunkt keine ACLs, was sehr oft vorkommt, können die Benutzer diesen Punkt nicht mehr betreten. Werden jetzt solche Dateien verschoben, wird immer mit der Hauptgruppe des Benutzer angelegt. Jetzt kann nichts passieren da ja niemand Mitglied der Gruppe „daten-firma“ ist.Das hat seinen Vorteil, da Benutzer sehr oft den Sinn und die Funktion von UnixACLs nicht richtig verstehen, und so unbeabsichtigt vom User falsche Rechte vergeben werden.