ACL Konzept NEU 11.2016

Das Problem bei den ACLs ist immer die Übertragung über Inodelevel hinaus, und auch über die Maske selbst hinaus. Da dies ja nicht geht hier ein neues Konzept das genau dieses Problem umgeht. Funktionieren kann das nur wenn die Maske von Quelle und Ziel immer gleich ist.

Wir erstellen uns einen Ordner Dokumente1 in home und setzen hierfür die Rechte.

```
mkdir /home/Dokumente1
chgrp dokumente /home/Dokumente1
setfacl  -m group:dokumente:rwX,other:rwX /home/Dokumente1  # setzt die ACL
des Ordners
setfacl -d -m group:dokumente:rwX,other:rwX /home/Dokumente1  # setzt die
Default ACL des Ordners
chmod g+s /home/Dokumente1
chmod 770 /home/Dokumente1
```

Die Rechte sehen jetzt so aus:

```
getfacl /home/Dokumente1
# file: Dokumente1
# owner: root
# group: dokumente
# flags: -s-
user::rwx
group::rwx
group:dokumente:rwx
mask::rwx
other::---
default:user::rwx
default:group::rwx
default:group:dokumente:rwx
default:mask::rwx
default:other::rwx
```

Wie man sieht darf in diesem Ordner jeder Schreiben und lesen. Das ist aber kein Sicherheitsproblem da man Mitglied der Gruppe „Dokumente“ sein muss um überhaupt in dem Ordner zu gelangen. Wichtig ist hier bei „getfacl“, rwX zu schreiben und nicht rwx. Der Unterschied ist bei großem X nur die Auflistung des Ordnerinhaltes gewährt wird, was natürlich auch einem möglichem Schreiben im Ordner gleicht. Es gewährt aber keinesfalls „Ausführen“ von Dateien in diesem Ordner. Diese dürfen natürlich von jedem Benutzer gesetzt werden, aber es ist kein Standard bei neuen Dateien.

Unix ACL's ganz einfach und ohne Aufwand (ACL-Observer)

ACL's sind bekanntlich ja nicht gerade einfach. Dann muss man auch noch aufpassen das man mit dem richtigen Share drauf zugreift. Also NFS mit ACL, tut man mit SSHFS ist's schon wieder vorbei. Mit dem folgenden Konzept übergeht man das alles.

Weitere Probeleme können Programme verursachen. Dolphin regt sich hier bei jedem ACLbreich übergreifenden Kopieren oder Verschieben auf das die Rechte nicht geschrieben werden können auf. Das nervt. Um das ganze zu umgehen setzen wir die ACLs wie folgt:

```
mkdir /home/firmendaten
chown -R root:nogroup /home/firmendaten
find /home/firmendaten -type d -exec chmod 777 {} +
find /home/firmendaten -type f -exec chmod 666 {} +
setfacl -R -m other:rwX /home/firmendaten  # setzt die ACL des Ordners (-R
vor -m für recursiv)
setfacl -R -d -m other:rwX /home/firmendaten  # setzt die Default ACL des
Ordners  (-R vor -m für recursiv)
chmod 770 /home/firmendaten
chgrp firmendaten /home/firmendaten
```

```
/home/ getfacl firmendaten
# file: firmendaten
# owner: root
# group: firmendaten
user::rwx
group::rwx
other::---
default:user::rwx
default:group::rwx
default:other::rwx
```

Wir können die Gruppe getrost weglassen, da wir diese ja nur beim Eingang (spricht den Ordner) der ACL benötigen. Natürlich müssen alle anderen ACLbereiche (auch Homeverzeichnisse) so gesetzt sein. Damit bekommt man die Fehlermeldung in Dolphin nicht mehr. Sieht man sich den Inhalt an, irritiert dieser ein wenig. Passt aber definitiv zum Rechtesystem.

```
drwxrwxrwx+  4 root   nogroup    4096 Dez  2 20:36 Testordner
-rw-rw-rw-   1 root   nogroup  757681 Jul 11 08:35 Testdatei.txt
```

Neue Dateien werden mit der Gruppe und dem Eigentümer des Users angelegt. Probleme hat man mit dem Konzept dann, wenn z.B. Daten mit einer anderen Dateimaske von einem USBstick kopiert werden. Da die Maske mantürlich nicht angpasst wird.

Die AllinOne-Lösung bietet ACL-Observer. Das ist ein Systemd Service das Dateien und Verzeichnisse auf ACL's und Masken überwacht und die auch beim Verschieben von Dateien setzt. Im Prinzip arbeitet es wie Incron. Ist nur wesentlich leichtgewichtiger und einfacher zu konfiguruieren.

Installation von ACL-Observer

Installation über unsere Paketquelle für Ubuntu:

```
apt-key adv --recv-keys --keyserver keyserver.ubuntu.com 2FAB19E7CCB7F415
echo "deb http://styrion.at/apt/ ./" > /etc/apt/sources.list.d/styrion.list
```

```
apt update
apt install facl-observer
```

Konfiguration

Hier ein Beispiel:

```
cat /etc/facl-observer/config
[MAIN]

# Folders to observer
WATCH_DIRS = /home/bilderarchiv, /home/Dokumente

# Disable file execute permissions on changes
WATCH_DISABLE_FILE_EXECUTE = True
```

Danach den Dienst neu starten, und man braucht sich um Berechtigungen keine Sorgen mehr machen :)

```
systemctl restart facl-observer.service
```

Neue Homeverzeichnisse setzen

Das Folgende ist nicht mehr nötig wenn man schon ACL-Observer einsetzt.

Dies ist nur möglich wenn sich im Homeverzeichnis keine Daten befinden. Hiervon sind versteckte Dateien unberührt.

```
chmod 777 /home/user
chmod 777 /home/user/*
setfacl -d -m other:rwX /home/user
setfacl -m other:rwX /home/user
setfacl -m other:rwX /home/user/*
setfacl -d -m other:rwX /home/user/*
chmod 700 /home/user
```