

HOWTO zur "ACLs" (Access Control Lists) unter UNIX/Linux
 (C) 2008 T.Birnthaler/H.Gottschalk <howtos(at)ostc.de>
 OSTC GmbH, <http://www.ostc.de>
 \$Id: unix-acl-HOWTO.txt,v 1.6 2008-12-22 15:39:07 tsbirn Exp \$

Dieses Dokument beschreibt die Funktionalität und die Einrichtung von
 "Access Control Lists" (ACLs) unter UNIX/Linux

Inhaltsverzeichnis

- 1) Basis-ACL
- 2) Erweiterte ACL
- 3) ACL-Maske
- 4) Hinweise

1) Basis-ACL

Eine ACL ist EIN Satz der Rechte "rwx", die einem Benutzer, einer Gruppe oder "Allen anderen" für eine Datei/Verz. zugeordnet ist. Die 9 UNIX-Standardrechte werden als "degenerierte ACL" bezeichnet, die fix drei Elemente enthält. Diese 3 Elemente werden auch als "Basiseinträge" (base entries) bezeichnet.

Eintrag-Typ	Name
Besitzer	(u)ser
Besitzer-Gruppe	(g)roup
Alle anderen	(o)ther

Solange noch keine weitere ACL gesetzt ist, werden die drei Basiseinträge von "ls -l" folgendermaßen angezeigt (nach "chmod 755 DATEI"):

```
u g o
-rwxr-xr-x tsbirn users ... DATEI
```

Mit "getfacl" werden diese Basiseinträge so dargestellt:

```
# file: DATEI
# owner: tsbirn
# group: users
user::rwx
group::r-x
other::r-x
```

2) Erweiterte ACL

Sobald mit "setfacl" EINE "echte" ACL für einen Benutzer oder eine Gruppe hinzugefügt wird, gibt es neben den Basiseinträgen auch "Benannte Einträge" (named entries) und eine "Maske" (mask). Als Startwert der Maske wird die "Summe" der Einträge verwendet, auf die sie wirkt

Eintrag-Typ	Name	Maske
Basis-Besitzer	basic user	nein
Benannter Benutzer	named user	ja
Basis-Gruppe	basic group	ja
Benannte Gruppe	named group	ja
Basis Alle anderen	basic other	nein
Maske	effective mask	--

Sobald EINE ACL gesetzt ist, hier mit:

```
setfacl -m user:kurs1:-w- DATEI
```

werden die drei Basiseinträge von "ls -l" folgendermaßen angezeigt (d.h. es wird durch ein "+" gekennzeichnet, dass "echte" ACLs vorhanden sind und die Maske STATT den Rechten der Basis-Gruppe dargestellt):

```
u m o
-rwxrwxr-x+ tsbirn users ... DATEI
```

Mit "getfacl" werden die ACL-Einträge so dargestellt:

```
# file: DATEI
# owner: tsbirn
# group: users
user::rwx
```

```
user:kursl:-w-
group::r-x
mask::rwx
other::r-x
```

3) ACL-Maske

Die Maske wird auf ALLE Benannten Einträge (Benutzer + Gruppen) und die Basis-Gruppe angewendet und lässt von der Summe der von diesen Einträgen gesetzten Rechte nur die in der Maske gesetzten Rechte durch ("Effektiv" wirksame Rechte). Nach

```
setfacl -m mask:r-- DATEI
```

ergibt "ls -l" folgende Ausgabe:

```
u m o
-rwxr--r-x+ tsbirn users ... DATEI
```

Mit "getfacl" werden folgende ACL-Einträge angezeigt:

```
# file: DATEI
# owner: tsbirn
# group: users
user::rwx
user:kursl:-w- #effective:---
group::r-x #effective:r--
mask:r--
other::r-x
```

Die Maske wird bei JEDER Änderung eines Eintrages, auf den sie wirkt, auf die "Summe" ALLER Einträge gesetzt, auf die sie wirkt (also "angepasst" = "recalculated"). Nach

```
setfacl -m group:ostc:--x DATEI
```

ergibt "ls -l" folgende Ausgabe:

```
u m o
-rwxrwxr-x+ tsbirn users ... DATEI
```

Mit "getfacl" werden folgende ACL-Einträge angezeigt:

```
# file: DATEI
# owner: tsbirn
# group: users
user::rwx
user:kursl:-w-
group::r-x
group:ostc:--x
mask:rwx
other::r-x
```

Setzt man die Maske anschließend erneut, dann reduziert sie wieder die Rechte der Einträge, auf die sie wirkt. Nach

```
setfacl -m mask:r-- DATEI
```

ergibt "ls -l" folgende Ausgabe:

```
u m o
-rwxr--r-x+ tsbirn users ... DATEI
```

Mit "getfacl" werden folgende ACL-Einträge angezeigt:

```
# file: DATEI
# owner: tsbirn
# group: users
user::rwx
user:kursl:-w- #effective: ---
group::r-x #effective: r--
group:ostc:--x #effective: ---
mask:r--
other::r-x
```

4) Hinweise

* Die Man-Page von "setfacl" beschreibt das Verhalten der Maske falsch. Dort wird behauptet, dass sie nicht mehr an die Summe der Rechte "angepasst" wird, sobald sie einmal manuell gesetzt wurde. Dies ist nicht korrekt.

- * Mit dem Schalter "-no-mask" oder "-n" kann bei Änderung einer ACL die "Anpassung" der Maske an die Summe der Rechte verhindert werden, für die sie relevant ist.
- * Ändern der Gruppenrechte mit "chmod g=w DATEI" ändert die Maske, nicht die Gruppenrechte (solange mindestens EINE ACL vorhanden ist).
- * Ändern der Gruppenrechte kann NUR noch durch "setfacl group::rwx" erfolgen. Dabei wird die Maske wieder "angepasst".