



MAR1NER



[mar1ner](#)

- [Recent Entries](#)
- [Friends](#)
- [Archive](#)
- [Profile](#)

Add to friends

RSS

Dec						2016	
S	M	T	W	T	F	S	
					1	2	3
4	5	6	7	8	9	10	
11	12	13	14	15	16	17	
18	19	20	21	22	23	24	
25	26	27	28	29	30	31	

Всё не так просто как мы думаем. Всё ещё проще

Законы Мэрфи на практике



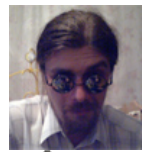
samba + acl = руление доступом из windows

как известно, в linux права описываются формулой "я - мы - они", в смысле, доступ к файлу или директории для создателя, группы и всех остальных. в большинстве случаев этого вполне хватает.

но иногда возникает вопрос - а как бы сделать так, чтобы доать доступ ещё и вот этим товарищам, но не вводить их в группу?

всё просто. есть такой пакет [acl](#).

в пакете хранятся утилиты управления списками доступа.



[mar1ner](#)
June 17th, 2008

ставится этот пакет традиционно:

```
$ sudo apt-get update
$ sudo apt-get install acl
```

теперь объясним системе. что у нас на файловой системе есть расширенное управление правами:

```
$ sudo vi /etc/fstab
# /etc/fstab: static file system information.
#
#
proc          /proc        proc         defaults    0          0
/dev/hda1     /            ext3         defaults,errors=remount-ro 0          1
/dev/hda3     /home        ext3         defaults,acl 0          2
/dev/hda2     /var         ext3         defaults    0          2
/dev/hdd      /media/cdrom0 iso9660      ro,user,noauto 0          0
/dev/fd0      /media/floppy0 auto         rw,user,noauto 0          0
```

в столбик options дописываем параметр acl (выделено красным) после чего либо перемонтируем соответствующие разделы,

```
$ sudo mount -o remount /dev/hda3
```

либо перегружаем всю систему.

ну что, разделы с нужной опцией примонтировались?

как расширенные права выглядят с точки зрения системы можно посмотреть командой

```
$ getfacl tmp
# file: tmp
# owner: root
# group: root
user::rwx
group::rwx
other::rwx
```

это, что называется по умолчанию добавим кому ни будь доступ

```
$ sudo setfacl -m u:username:rx tmp
```

смотрим что получилось

```
$ getfacl tmp
# file: tmp
```

Tags

- :*) :-(antispam debian desktop fallout
- firefox games hardware howto internet
- kinder linux mac macos microsoft photo
- soft spam userpic video virtualbox windows
- windows7 ЖЖ Йошкар-Ола Ксюха Новости Риверт-Сити Славик блогводство бродячие вконтакте дорожное заметки злобное интернет квест ностальгическое одноклассники.ру политика праздник пресса провокационное прохождение ССЫЛОЧНАЯ таньки флешмоб фотография

Powered by [LiveJournal.com](#)

```
# owner: root
# group: root
user::rwx
user:username:r-x
group::rwx
mask::rwx
other::rwx
```

перейдём к более практическому применению - расширенные права в samba.

пробовали назначать права доступа к файлам и каталогам на самбовской шаре? ну как? а с использованием acl всё гораздо интереснее.

добавляем расширенные права в конфиг самбы

```
$ sudo vi /etc/samba/smb.conf
```

```
[global]
...
acl compatibility = auto

[sharename]
comment = Share
path = /path/to/directory
browseable = yes
writable = yes
create mask = 0664
directory mask = 0777
inherit acls = yes
inherit owner = yes
inherit permissions = yes
map acl inherit = yes
```

а вот теперь можно пробовать назначать персональный доступ к файлам и каталогам для отдельных пользователей прямо с виндовой машины. ну совсем такой как в виндах не получится, а вот на предмет читать/писать запросто. особенно для самбы в виндовом домене.

Tags: [debian](#), [linux](#), [samba](#)

(12 comments — [Leave a comment](#))



[shaplov](#)

[2008-06-17 07:53 am \(UTC\)](#)

Скажи мне добрый фей, а может ли при помощи этого, или подобного ему зверя, запретить всем кроме рута убивать симлинк из директории в которой право записи юзера имеют...

[\(Reply\)](#) [\(Thread\)](#)



[mar1ner](#)

[2008-06-17 08:21 am \(UTC\)](#)

и если что то делать с правами на симлинк, то реально права меняются на то место, на которое он ссылается. так что судя по всему облом :(

[\(Reply\)](#) [\(Parent\)](#) [\(Thread\)](#)



[moose_kazan](#)

[2008-06-17 08:58 am \(UTC\)](#)

Так:

```
> $ sudo umount /dev/hda3
```

```
> $ sudo mount /dev/hda3
```

не правильно. Правильно так:

```
$ sudo mount -o remount /dev/hda3
```

Заодно проблема с используемыми разделами решается:)

[\(Reply\)](#) [\(Thread\)](#)



[mar1ner](#)

2008-06-17 09:03 am (UTC)



спасибо, подправил

[\(Reply\)](#) [\(Parent\)](#) [\(Thread\)](#)

[pofiq_kto](#)

2008-06-17 12:10 pm (UTC)

вообще в SAMBA

Default: acl compatibility = Auto

+ на остальные директивы inherit *

у меня

mbd --version

Version 3.0.25b-1.el5_1.4

вообще ругается :o/

[\(Reply\)](#) [\(Thread\)](#)



[mar1ner](#)

2008-06-17 12:22 pm (UTC)

```
# nmbd --version
```

```
Version 3.0.23c
```

это на рабочем файлсервере, откуда конфиги

а дистрибутив какой?

[\(Reply\)](#) [\(Parent\)](#) [\(Thread\)](#)

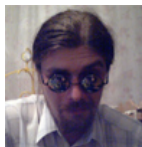
[pofiq_kto](#)

2008-06-18 03:20 am (UTC)

хम्म... странно

CentOS 5.1

[\(Reply\)](#) [\(Parent\)](#) [\(Thread\)](#)



[mar1ner](#)

2008-06-18 05:12 am (UTC)

хм...

<http://yandex.ru/yandsearch?text=CentOS+samba+acl>

<http://linuxforum.ru/index.php?showtopic=66222> немного ниже по треду

ну и

<http://mar1ner.livejournal.com/316108.html>

[\(Reply\)](#) [\(Parent\)](#) [\(Thread\)](#)



[skonstantin](#)

2009-04-20 06:27 am (UTC)

Огромное спасибо!!!

[\(Reply\)](#) [\(Thread\)](#)



[rootadmin](#)

2009-10-28 01:54 pm (UTC)

Благодарю, поднял на днях файлопомойку, а все описания "чтоб с винды, да галочками" были про фриБСД.

[\(Reply\)](#) [\(Thread\)](#)

(Anonymous)

[2012-03-26 03:03 pm \(UTC\)](#)

Что-то не могу сообразить как сделать. Конфиг взят без изменений отсюда.
Есть папка /share зашаренная в samba.
Права доступа для нее и вложенных подпапок 770.
Задача 1

Проблема: файл не редактируем, но удаляем

```
# file: file.xls
# owner: root
# group: smbusers
user::rwx
user:my_user:rw-
group::r--
mask::rw-
other::---
```

Задача 2

Нужно сделать доступ на папку для всех групп и пользователей read-only, и двум пользователям full access.

Проблема: Создаваемые файлы (думаю и папки) пользователем full access имею права 770, что дает возможность группе редактировать.

```
# file: my_share
# owner: root
# group: smbusers
user::rwx
user:my_user1:rwx
user:my_user2:rwx
group::r-x
mask::rwx
other::---
```

Понятно, что маска обрабатывает, но непонятно где копать. Если я правильно понял у smb своя маска у fs acl своя?

[\(Reply\)](#) [\(Thread\)](#)



[mar1ner](#)

[2012-03-27 02:28 am \(UTC\)](#)

Да, у самбы свой взгляд на права доступа к файлам. Можно в описании шары поиграть параметрами valid users и write users. вроде так.

- 1) для самбы и ниса не разницы между удалением и редактированием.
 - 2) можно завести группу редакторов на эту папку, и включать туда нужных пользователей. А права дать 664
- И рекомендую поменять 770 права на 660

Давно я этим не занимался. Вспоминать надо.

[\(Reply\)](#) [\(Parent\)](#) [\(Thread\)](#)

(12 comments — [Leave a comment](#))