Дозволе над системима датотека

Преглед дозвола

Као што смо раније поменули, Слаквер Линукс је вишекориснички оперативни систем. Према томе, његови системи датотека су такође вишекориснички. Ово значи да сваки документ или директоријум има низ дозвола које могу бити укинуте или додељене различитим корисницима. Постоје три основне дозволе и три низа дозвола за сваки документ. Погледајмо на примеру.

```
darkstar:~$ ls -l /bin/ls
-rwxr-xr-x 1 root root 81820 2007-06-08 21:12 /bin/ls
```

Подсетимо се четвртог поглавља, у коме пише да ***ls*** *-l* даје списак свих дозвола над документом или директоријумом поред корисника и групе који *поседују* документ. У овом случају дозволе су **rwxr-xr-x**, корисник је **root**, а група је такође **root**. Одељак са дозволама заиста представља три одвојена дела. Први низ од три знака представља дозволе додељене кориснику који поседује документ. Други низ од три знака су дозволе додељене групи која је власник документа. Последња три знака су дозволе додељене свима.

Табела 10.1. /bin/ls дозволе

Низ	Списак	Значење
Власник	rwx	Власник “root” има дозволе читања, писања, и извршавања (read, write, execute)
Група	r-x	Група “root” има дозволе читања и извршавања (read, execute)
Остали	r-x	Сви остали имају дозволе читања и извршавања (read, execute)

Дозволе над документима говоре све о њиховом значењу. Читање, писање и извршење вам дозвољавају да читате документ, уносите измене (пишете) и извршите га. Али какво онда значење дозволе имају у односу на директоијуме? Просто речено, дозволе читања вам дају могућност увида у садржај директоријума (нпр. командом ***ls***). Дозволе писања вам дају могућност креирања нових докумената унутар директоријума или уклањања читавог директоријума, чак и кад на други начин нисте у могућности да уклоните неке документе унутар датог директоријума. Дозволе извршавања вам дају могућност приступа документу (нпр. уграђеном ***bash*** командом ***cd***).

Погледајмо сада дозволе над директоријумима.

```
darkstar:~$ ls -ld /home/alan
drwxr-x--- 60 alan users 3040 2008-06-06 17:14 /home/alan/
```

Директоријум је под власништвом корисника **alan** и групе **users**. Кориснику су додељена сва права (rwx). Групи су додељене само дозволе читања и извршавања (r-x), а свима осталима је забрањено било какво чињење.

chmod, chown и chgrp

Сада знамо шта су дозволе, али како да их мењамо? И у вези са тим, како приписати власништво кориснику или групи? Одговори се крију управо у овом делу.

Алат о коме ћемо прво говорити је корисни ***chown***. Користећи ***chown***, можете (већ погађате) да промените власништво над одређеним документом или директоријумом. ***chown*** је углавном коришћен за промену власништва у смислу корисника, али можете да мењате и власништво групе такође.

```
darkstar:~# ls -l /tmp/foo
total 0
-rw-r--r-- 1 alan users 0 2008-06-06 22:29 a
-rw-r--r-- 1 alan users 0 2008-06-06 22:29 b
darkstar:~# chown root /tmp/foo/a
darkstar:~# ls -l /tmp/foo
total 0
-rw-r--r-- 1 root users 0 2008-06-06 22:29 a
-rw-r--r-- 1 alan users 0 2008-06-06 22:29 b
```

Користећи простор иза двотачке (:), након корисничког налога, можете одредити нови групни налог.

```
darkstar:~# chown root:root /tmp/foo/b
darkstar:~#  ls -l /tmp/foo
total 0
-rw-r--r-- 1 root users 0 2008-06-06 22:29 a
-rw-r--r-- 1 root root  0 2008-06-06 22:29 b
```

chown можете користити и рекурзивно како бисте променили власништво над свим документима и директоријумима унутар циљаног директоријума. Следећа команда ће променити власништво на root:root над свим документима у директоријуму `/tmp/foo`.

```
darkstar:~# chown -R root:root /tmp/foo/b
```

Уколико одредите само групу без корисника, променићете власништво групе над одређеним документом, док ће власништво корисника остати нетакнуто.

```
darkstar:~# chown :wheel /tmp/foo/a
darkstar:~# ls -l /tmp/foo
ls -l /tmp/foo
total 0
-rw-r--r-- 1 root wheel 0 2008-06-06 22:29 a
-rw-r--r-- 1 root root  0 2008-06-06 22:29 b
```

Млађи брат ***chown***-а је мало мање коришћен ***chgrp***(1). Ова команда ради исто што и ***chown***, с том разликом што може да мења само власништво групе над документом. Пошто ***chown*** ово већ може, зашто досађивати са ***chgrp***? Одговор је једнотаван. Различити ОС-и користе различите верзије ***chown***-а које не могу да мењају власништво групе, тако да уколико

налетите на једну од њих - знате шта да радите.

Постоји разлог зашто смо разговарали о промени власништва пре промене дозвола. Прво концепт је много лакши за разумевање. Алат за промену дозвола над документом или директоријумом је ***chmod***(1). Синтакса је скоро идентична оној за ***chown***, али уместо да одредите корисника и групу, овде ћете као администратор морати да одредите или сет окталних или сет абецедних дозвола. Ниједан од ова два концепта није једноставан за разумевање кад се сретнете први пут, тако да ћемо кренути од мало једноставнијег концепта окталних дозвола.

Окталне дозволе су добиле име по томе што се означавају цифрама. Наиме, додељује им се једна од осам цифара, од 0 до 7. Свакој дозволи се додаје број који је помножен са 2, и ови бројеви сабрани заједно дају коначне дозволе за један сет дозвола. Уколико ово звучи збуњујуће, можда ће вам ова табела помоћи у разумевању.

Табела 10.2. Окталне дозволе

Дозвола	**Значење**
Read (читање)	4
Write (писање)	2
Execute (извршење)	1

Сабирајући ове бројеве, можете добити било који број од 0 до 7 и одредити све могуће комбинације дозвола. На пример, како бисте доделили привилегије читања и писања, а одбили привилегију извршења, доделићете број 6. Број 3 би доделио дозволе писања и извршења, а забранио могућност читања документа. Морате одредити број за сваки од три сета када користите окталне дозволе. На пример, на овај начин није могуће одредити само сет корисничких и групних дозвола.

```
darkstar:~# ls -l /tmp/foo/a
-rw-r--r-- 1 root root  0 2008-06-06 22:29 a
darkstar:~# chmod 750 /tmp/foo/a
darkstar:~# ls -l /tmp/foo/a
-rwxr-x--- 1 root root  0 2008-06-06 22:29 a
```

chmod може користити и словне вредности поред тастера + и − за додељивање или ускраћивање дозвола. Мада је овај начин лакши за памћење, често је једноставније користити окталне дозволе.

Табела 10.3. Абецедне дозволе

Дозволе	**Словна вредност**
Read (читање)	r
Write (писање)	w
Execute (извршење)	x

Табела 10.4. Абецедне вредности корисника и група

Циљани налози	**Словна вредност**
User/Owner (Корисник/Власник)	u
Group (Група)	g

Циљани налози	Словна вредност
Others/World (Сви остали/Свет)	o

Да бисте користили словне вредности са ***chmod***, морате одредити сет на који се односе, или *u* за корисника, или *g* за групу, или *o* за све остале. Такође морате одредити да ли додајете или одузимате дозволе, са + и -. Ово можете применити и на више сетова одједном тако што ћете сваки одвојити зарезом.

```
darkstar:/tmp/foo# ls -l
total 0
-rw-r--r-- 1 alan users 0 2008-06-06 23:37 a
-rw-r--r-- 1 alan users 0 2008-06-06 23:37 b
-rw-r--r-- 1 alan users 0 2008-06-06 23:37 c
-rw-r--r-- 1 alan users 0 2008-06-06 23:37 d
darkstar:/tmp/foo# chmod u+x a
darkstar:/tmp/foo# chmod g+w b
darkstar:/tmp/foo# chmod u+x,g+x,o-r c
darkstar:/tmp/foo# chmod u+rx-w,g+r,o-r d
darkstar:/tmp/foo# ls -l
-rwxr--r-- 1 alan users 0 2008-06-06 23:37 a*
-rw-rw-r-- 1 alan users 0 2008-06-06 23:37 b
-rwxr-x--- 1 alan users 0 2008-06-06 23:37 c*
-r-xr----- 1 alan users 0 2008-06-06 23:37 d*
```

Који начин од ових ћете користити, зависи искључиво од вас самих. У неким случајевима је један начин бољи од другог, тако да као прави корисник Слаквера треба да познајете оба.

SUID, SGID и "лепљиви" бит

Још није готово са дозволама. Постоје још три ,,посебне дозволе, поред поменутих. Оне су SUID, SGID и лепљиви бит. Када документ има једну или више ових посебних дозвола, специфично се понаша. SUID и SGID дозволе мењају начин на који апликација функционише, док лепљиви бит онемогућује уклањање докумената. Ове дозволе су примењене и са ***chmod*** командом као читање, писање и извршавање, али обрнуто. SUID и SGID представљају *Set User ID* односно *Set Group ID*. Када је на апликацију примењен један од ових сетова, апликација се покреће са корисничким и групним дозволама саме апликације, без обзира који је корисник стварно покренуо апликацију. Погледајте уобичајену SUID апликацију ***passwd*** и фајлове које она мења. <code> darkstar:~# ls -l /usr/bin/passwd /etc/passwd /etc/shadow -rw-r—r— 1 root root 1106 2008-06-03 22:23 /etc/passwd -rw-r—— 1 root shadow 627 2008-06-03 22:22 /etc/shadow -rws—x—x 1 root root 34844 2008-03-24 16:11 /usr/bin/passwd* </code> Обратите пажњу на дозволе везано за ***passwd***. Уместо X у корисничком извршном одељку стоји S. Ово значи да је ***passwd*** SUID програм, и када се покрене, процес се покреће од стране *root* корисника, а не корисника који је уствари покренуо програм. Разлог за ово је очигледан уколико погледате два фајла које овај програм мења. Нико нема дозволу писања ни у /etc/passwd ни у /etc/shadow осим root корисника. Када корисник има потребу да промени личне информације, ***passwd*** мора бити покренут од стране кореног корисника како би изменио поменута два фајла. А шта са лапљивим битом? Лапљиви бит одузима могућност померања или уклањања докумената и постављен је само на директоријумима. Обичан корисник не може да

помери или уклони документе унутар директоријума са лепљивим битом, осим уколико није власник датог документа. У нормалним ситуацијама, свако ко има дозволу писања над документом, може да уради ово, али лепљиви бит онемогућује свакога у овоме, осим власника (и `root` корисника, наравно). Баците поглед на уобичајени ,,лепљиви директоријум.

```
darkstar:~# ls -ld /tmp
drwxrwxrwt 1 root root   34844 2008-03-24 16:11 /tmp
```

Природно, будући да је директоријум за складиштење привремених фајлова на системском нивоу, свако треба да има дозволе писања, читања и извршавања у `/tmp` директоријуму. С обзиром да сваки корисник у сваком тренутку овде има фајл или два, исправно је спречити друге корснике да те фајлове уклоне. Зато се овде поставља лепљиви бит. Можете га уочити по присуству слова T на место слова X у делу који се односи на дозволе за све остале (свет).

Табела 10.5. SUID, SGID и “Лепљиве” дозволе

Врста дозволе	Октална вредност	Словна вредност
SUID	4	s
SGID	2	s
Sticky	1	t

Када користите октални дозволе, морате одредити додатну водећу октални вредност. На пример, да бисте поново креирали дозволу над `/tmp` директоријумом, морате користити 1777. Да бисте то исто учинили са `/usr/bin/passwd`, морате користити 4711. У сваком случају, када ова четврта водећа октална вредност није одређена, ***chmod*** ће као вредност узети 0.

```
darkstar:~# chmod 1777 /tmp
darkstar:~# chmod 4711 /usr/bin/passwd
```

Коришћење абецедних вредности дозвола је донекле другачије. Претпоставимо да два поменута фајла имају дозволе 0000 (уствари немају никакве дозволе), овако ћемо их поставити.

```
darkstar:~# chmod ug+rwx,o+rwt /tmp
darkstar:~# chmod u+rws,go+x /usr/bin/passwd
```

Кретање кроз поглавља

Претходно поглавље: Корисници и групе

Следеће поглавље: Рад са системима датотека

Извори

- Оригинални извор: http://www.slackbook.org/beta

- Изворно писали Alan Hicks, Chris Lumens, David Cantrell, Logan Johnson

From:
https://docs.slackware.com/ - **SlackDocs**

Permanent link:
https://docs.slackware.com/sr:slackbook:filesystem_permissions

Last update: **2014/09/07 12:42 (UTC)**