21. Управление на права за достъп до файлове и директории за различни потребители

Специални права за достъп

В Linux съществуват още и специални права за достъп **SUID (Set User ID root)** и **SGID (Set Group ID root)**, които позволяват на обикновените потребители да пускат програми, изискващи за своята работа root права.

В съвременните дистрибуции на Linux навярно ще ви се налага да променяте тези права за достъп изключително рядко (а може би дори и никога), но все пак вие трябва да знаете как може да ги промените. Например, ако желаете да разрешите програмата **/usr/sbin/program** да може да бъде пускана с root права от обикновен потребител, задайте нейните права за достъп така:

```
# chmod u+s /usr/sbin/program
```

Използването на SUID е лошо решение от гледна точка на сигурността. По-правилно е да се използва команда **sudo**, ако на някой потребител са му нужни root права.

Команда chattr

В Linux освен права за достъп има и атрибути на файла, подобно на файловите атрибути в останалите операционни системи. Атрибутите на файла могат да бъдат променени с командата chattr:

chattr +/-<атрибути> <файл>

Зададените атрибути могат да се видят с командата lsattr:

lsattr <файл>

Някои полезни атрибути на файловете са приведени в таблицата.

Атрибут	Описание
i	Този атрибут забранява модифицирането, промяната на името и изтриването на файла. Може да го зададете за критични конфигурационни файлове или за други критични данни. Този атрибут може да бъде зададен (или премахнат) само от root потребител или от процес с възможност CAP_LINUX_IMMUTABLE. С други думи, този атрибут не може да бъде премахнат току-така - необходими са root права.
u	При изтриване на файл с атрибут и неговото съдържание продължава да се пази на твърдия диск, което позволява лесното му възстановяване.

c	Файлът ще се компресира. Може да зададете този атрибут за големи файлове, съдържащи некомпресирани данни. Достъпът до компресирани файлове ще бъде по-бавен, отколкото към обикновените, затова не е добро решение да задавате такъв атрибут на файлове с бази данни. Този атрибут не може да бъде задаван за файлове, които вече съдържат компресирани данни - архиви, JPEG картинки, MP3/MP4 файлове и т.н. С това вие не само няма да намалите техните размери, но и ще забавите производителността.
S	Данните, записвани на файла, веднага ще бъдат прехвърляни на диска. Аналогично на изпълнението на команда sync веднага след всяка операция за запис във файла.
s	Противоположен на атрибута и. След изтриването на файла принадлежащите му блокове ще бъдат нулирани и възстановяването им вече ще бъде невъзможно.

Пример за задаване на атрибут:

 # chattr +i /etc/pam.d/time.conf

Пример за премахване на атрибут:

 # chattr –i /etc/pam.d/time.conf