19. Създаване на потребители и групи - Linux Ubuntu

Командата visudo

За да направите един обикновен потребител администратор (т.е. да му предоставите правото да използва командата sudo), може или да използвате графични инструменти, или командата visudo.

Файлът **/etc/sudoers** може да бъде редактиран само с командата visudo:

export EDITOR=joe

sudo visudo

Първата команда определя променливата на средата EDITOR, задаваща удобен текстов редактор, който да бъде използван за /etc/sudoers. Втората команда извиква инструмента за редактиране на файла /etc/sudoers.

Да си представим, че имаме потребителя eva, на когото трябва да разрешим да прави всичко, каквото може да прави и потребителят root. За целта трябва да добавим в /etc/sudoers запис от вида:

eva ALL=(ALL:ALL) ALL

Може също да добавим и записа:

%sudoALL=(ALL:ALL) ALL

Това означава, че членовете на групата sudo могат да правят всичко, което прави и потребителят root. Тогава всички помощник-администратори трябва да бъдат добавени в групата sudo.

Запазате файла и излезте от редактора. Влезте като потребителя, на когото предоставихте sudo права. В нашия случай това е потребителят eva. След това въведете команда, която изисква root права чрез команда sudo:

sudo <команда>

Например:

sudo apt install nano

Може да контролирате получаването на sudo права с командата:

 # tail /var/log/auth.log | grep sudo

Сесиите sudo са по-сигурни от su сесиите, тъй като те се затварят автоматично - може потребителят да стане за малко от компютъра и през това време някой друг да се възползва от неговите права.

Изтриване на акаунт

За да изтриете акаунт, трябва да го селектирате и да натиснете бутона в прозореца **User Accounts.** В командния ред за изтриването на потребител се използва командата **userdel.**

Форматът на командата userdel (погледнете таблицата) е следният:

sudo userdel [параметри] потребител

Параметър	Описание
-f, --force	Изтрива акаунта дори ако потребителят работи в системата. Също така ще бъдат изтрити домашната папка и пощенската кутия дори ако друг потребител използва същата домашна папка. Ако във файла /etc/login.defs параметърът USERGROUPS_ENAB е yes, ще бъде изтрита и първичната група на потребителя дори и ако тя се явява първична за друг потребител. Много опасен параметър, който може да доведе системата до неработещо състояние.
-r, --remove	Изтрива домашната папка и пощенската кутия на потребителя. Файловете на този потребител, създадени на други файлови системи, трябва да се търсят и изтриват ръчно.
-R, --root chroot	Извършва промени в папка chroot и използва конфигурационните файлове от тази папка.

Пример за изтриване на акаунта eva. Домашната папка и пощенската кутия също ще бъдат изтрити:

sudo userdel -r eva

Модули за автентификация

Запознаване с PAM (Pluggable Authentication Modules)

Модулите за автентификация PAM (Pluggable Authentication Modules) предоставят на администраторите допълнителни методи за удостоверяване автентичността на потребителя.

Промяната на настройките на PAM е необходима далеч не на всички домашни потребители. В повечето случаи те така и ще си останат по подразбиране. Ако обаче ви е грижа за сигурността на вашите данни, то задължително трябва да се запознаете с представения в този раздел материал.

PAM модулите позволяват използването на няколко схеми за автентификация. Повечето приложения, които се нуждаят от проверка на автентичността на потребителя, използват PAM. Тези модули позволяват реализирането на алтернативна автентификация, например, по пръстов отпечатък или по ретината на очите, но за това е необходимо допълнително оборудване, например четец на отпечатъци.

Задаване на минимална дължина на паролата

От съображения за сигурност съвременните дистрибуции не позволяват задаването на прекалено къса парола (по-малка от 8 символа). За промяна на дължината на паролата трябва да редактирате файла **/etc/pam.d/common-password:**

sudo joe /etc/pam.d/common-password

Намерете в този файл следния ред:

password [success=1 default=ignore] pam_unix.so obscure sha512

Заменете го със следния:

password [success=1 default=ignore] pam_unix.so sha512 minlen=10

Тук ние **премахнахме опцията obscure,** която изисква въвеждането на сложна парола (при желание може да я оставите), но зададохме минимална дължина на паролата 10 символа.

Запазете файла и излезте от редактора. Повече никакви действия не са необходими.

Ограничаваме достъпа до системата

Параметрите на PAM, отнасящи се до ограничаването на достъпа, се намират в папка **/etc/security**. В нея има много и най-различни конфигурационни файлове, затова ние ще разгледаме само някои от тях. Ще започнем с файла **access.conf,** в който се декларират **ограниченията за достъп до системата.**

Форматът на този файл е следният:

разрешения : потребители : източници

Разрешението може да започва със символа „+“ (достъпът е разрешен) или „-“ (достъпът е забранен). Ако трябва да бъдат зададени няколко потребители, имената им се разделят с интервал. Ако трябва да бъде направено изключение за някои потребители, пред имената им се поставя служебната дума **EXCEPT.**

Третото поле може да съдържа списък с едно или няколко **имена па конзоли (tty)** - за немрежов достъп до системата, **имена на възли (за мрежов достъп), имена на домейни** (започват с **„.“**), **IP адреси на възли, IP адреси на мрежи** (завършват с **„.“**). Също така може да бъдат зададени всички източници (ALL), нито един източник (NONE) или само локални източнnци (LOCAL).

А сега няколко примера:

-:ALL EXCEPT root: ttyl

Първата конзола ще бъде само конзола за root. На другите потребители е забранено да я използват. Hue забраняваме достъпа (-) на всички потребители (ALL) освен (EXCEPT) потребителя root за конзолата ttyl.

Следващият пример - разрешаване на регистрация като root от определени IP адреси:

+ : root : 192.168.1.1 192.168.1.4 192.168.1.9

+ : root : 127.0.0.1

Ако е необходимо да бъде разрешена регистрация като root от всички подмрежи 192.168.1.0, тогава задайте адреса на тази подмрежа, поставяйки точка вместо 0:

+ : root : 192.168.1.

Най-строгият пример - забраняваме на root въобще да влиза в системата:

-: root : ALL

Малко по-нагоре разрешихме вход на потребителя root от определени IP адреси. За съжаление, само редактирането на access.conf няма да бъде достатъчно за това. Трябва да бъдат редактирани още и съответните файлове в /etc/pam.d. Интересува ни регистрация no SSH (telnet вече не се използва, затова ще се регистрирате no SSH) и обикновена регистрация в системата. Затова трябва да редактираме файловете /etc/pam.d/sshd и /etc/pam.d/system-auth. В тези файлове трябва да добавите следния ред:

account required /lib64/security/pam_access.so

Ако системата ви е 32-битова, тогава трябва да добавите малко по-различен ред:

account required /lib/security/pam_access.so

Разрешаваме регистрация само в работно време

Най-добре е да управлявате сигурността на системата в работно време. Затова, ако настройвате корпоративен уеб сървър, който потребителите могат да използват само в работно време, има смисъл да разрешите регистриране в системата само тогава, например от 8:00 до 20:00 часа (в случай че някой трябва да остане до малко по-късно).

Отворете файла **/etc/security/time.conf** и добавете в него следния ред:

login;tty* & !ttyp*; !root & admin & ; !A10800-2000

Тук разрешаваме на потребителите да влизат в системата само от 8:00 до 20:00 ч. За потребителите root и admin това правило не важи.

След това трябва да промените файловете **/etc/pam.d/sshd** и **/etc/pam.d/system-auth**, в които трябва да добавите следния ред:

acount required /lib64/security/pam_time.so

или (за 32-битови системи):

account required /lib/security/pam_time.so