# Решение проблемы с копящимся faillog при использовании sudo

По умолчанию в ОС для фиксации числа неверных попыток входа пользователей применяется PAM-модуль pam_tally. Использование pam_tally в секции auth в файле /etc/pam.d/common-auth обеспечивает увеличение счетчика неверных попыток входа пользователя при начале процесса аутентификации.

В PAM-стеке sudo по умолчанию подключается common-auth:

```
#%PAM-1.0
@include common-auth
@include common-account
@include common-session-noninteractive
```

В свою очередь в common-auth вызывается модуль pam_tally:

```
auth [success=ignore default=die] pam_tally.so per_user deny=10
```

На стадии аутентификации (auth) модуль pam_tally проверяет не заблокирован ли пользователь, и если нет, то он инкрементирует счётчик attempted login. Если аутентификация прошла успешно, то тот же самый модуль pam_tally должен сбросить этот счётчик на стадии account. Счётчик должен сбрасываться на вызове функции pam_setcred. Но в случае с sudo этого не происходит. В auth.log выводится warning:

```
Mar 30 14:31:41 dcm14 sudo: pam_tally(sudo:setcred): Tally underflowed for user root
```

Для обхода этой проблемы необходимо добавить в PAM-стек sudo ещё один вызов pam_tally:

```
account required pam_tally.so
```

Важно!
Вызов pam_tally в фазе account должен быть после его вызова в фазе auth. В нашем случае после:

```
@include common-auth
```

Например, с таким PAM-сценарием для sudo счётчик attempted logins должен сбрасываться в случае успешной аутентификации:

```
#%PAM-1.0
@include common-auth
@include common-account
@include common-session-noninteractive
account required pam_tally.so
```