[pam\_tally2 command – lock & unlock ssh failed logins in linux](http://shabbathster.blogspot.com/2014/07/pamtally2-command-lock-unlock-ssh.html)

pam\_tally2 command – lock & unlock ssh failed logins in linux

**pam\_tally2** command is used to lock and unlock **ssh failed logins** in linux like operating system. To implment a security feature  like a user's account must be locked after  a number of failed login attempts . We can achieve this security via **pam module** called **pam\_tally2**. This module  can display user's login attempts,set counts on individual basis, unlock all user counts.

pam\_tally2 comes in two parts: **pam\_tally2.so** and **pam\_tally2.** The former is the PAM module and the latter, a stand-alone program. **pam\_tally2** is an  application which can be used to interrogate and manipulate the counter file

In this article we will discuss how to lock and unlock user's account after reaching a fixed number of failed ssh attempts in**RHEL 6.X**  / **CentOS 6.X**

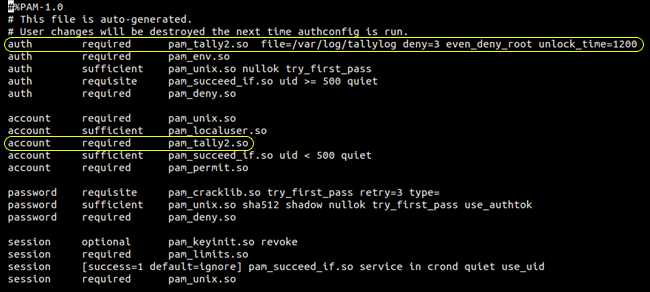
By default pam\_tally2 module is already installed in linux. To set the lock and unlock rules, edit  the  two files :  '**/etc/pam.d/system-auth**' & **'/etc/pam.d/password-auth**' and add the below line  at the starting of auth section in both the files

auth     required   pam\_tally2.so  file=/var/log/tallylog deny=3 even\_deny\_root unlock\_time=120

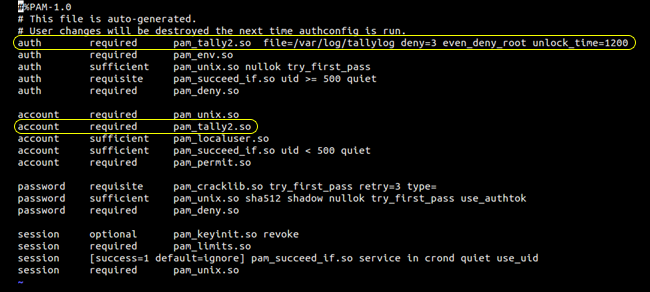
And then add the below line in the account Section in both the files

account required   pam\_tally2.so

Sample File of /etc/pam.d/system-auth



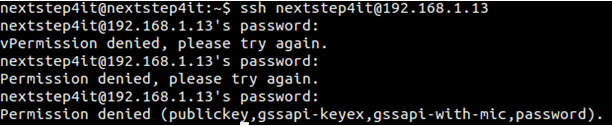
Sample File of /etc/pam.d/password-auth



**whereas :**

* **file=/var/log/tallylog** – Default log file whic keep login counts.
* **deny=3** – Deny access after 3 attempts and lock down user.
* **even\_deny\_root** – Policy is also apply to root user.
* **unlock\_time=1200** – Account will be locked till 20 Min after that it will be unlocked

**Now Try to Login the linux box with incorrect password :**

****

**Now check user's login attempts using pam\_tally2 Command**

[root@localhost ~]# pam\_tally2 -u nextstep4it

Login        Failures Latest failure From

nextstep4it      3 06/14/14 02:01:25  192.168.1.8

**Now reset or unlock user's account's using pam\_tally2 command :**

[root@localhost ~]# pam\_tally2 --user nextstep4it --reset

Login        Failures Latest failure From

nextstep4it      4 06/14/14 02:20:42  192.168.1.8

**Now Verify the login Attempt is reset or not**

[root@localhost ~]# pam\_tally2 --user nextstep4it

Login        Failures Latest failure     From

nextstep4it      0