How To Check if Any Users Were Added or Deleted on Your Linux System

Yesterday in my post on numeric userids instead of usernames, I touched briefly the problem of recovering the username if you only know the userid it once had. Today I would like to show you another option which may be available to you when it comes to recovering the usernames of removed users by their userid.

useradd and userdel logs in Ubuntu

Both **useradd** and userdel commands keep logs in many Unix-like systems. This means that every newly created user gets the whole procedure documented in appropriate logs with lines similar to this (it's an Ubuntu example, **/var/log/auth.log** file):

```
Jan  6 04:24:27 simplyunix useradd[1456]: new group: name=mike, GID=1006
Jan  6 04:24:27 simplyunix useradd[1456]: new user: name=mike, UID=1006, GID=1006, home=/home/mike, shell=/bin/sh
```

Similarly, deleting a file doesn't go unnoticed neither:

```
Jan  6 04:29:21 simplyunix userdel[1516]: delete user `mike'
Jan  6 04:29:21 simplyunix userdel[1516]: delete `mike' from group `admin'
Jan  6 04:29:21 simplyunix userdel[1516]: removed group `mike' owned by `mike'
```

So, there's a chance that by simply going through /var/log/auth.log you will find the userid of a local Unix user which was recently removed. But the reason I won't say "there's a really good chance" is because most of the logs in /var/log are rotated on a weekly and monthly basis, and this

means the information about new users created or deleted may not be there at the time you go looking for it – anyone who was added or deleted more than few months ago will not show up.

useradd and userdel in RedHat Enterprise Linux

Similar to Ubuntu, you can find recent user management activity logged in RHEL system, in /var/log/secure file.

useradd will produce something link this:

```
Jan  8 00:18:36 rhel5 useradd[2674]: new group: name=newuser, GID=501
Jan  8 00:18:36 rhel5 useradd[2674]: new user: name=newuser, UID=501, GID=501, home=/home/newuser, shell=/bin/bash
```

… while **userdel** will document its actions with the following:

```
Jan  8 00:18:40 rhel5 userdel[2682]: delete user `newuser'
Jan  8 00:18:40 rhel5 userdel[2682]: removed group `newuser' owned by `newuser'
```

How to check if any users were added on your Unix system

Based on the information above, all you have to do is something like this:

ubuntu$ **grep useradd /var/log/***

This is bound to return you a list of all the recently added users.

How to confirm local users which were recently removed

Similarly, use a command like this to find out if any users were recently removed:

ubuntu$ **grep userdel /var/log/***

Hope this helps! Enjoy!

See also:

- **What to do if numerid userids are shown instead of usernames in file ownership**
- **Creating new users in Unix with useradd**