

Managing Non-Login and Locked Solaris 10 Accounts

by: Glenn M. Brunette, Jr., 10/08/2004

<http://www.securitydocs.com/library/2636>

Today's entry will focus on enhancements to the `passwd(1)` command to better support the distinction between locked and non-login accounts. Specifically, we will be looking at the new `-u` and `-N` options to the `passwd(1)` command as well as how they relate to the much older `-l` option. These new capabilities will help administrators obtain better control over how their accounts are accessed and how they can in fact manage those accounts. In the past, some of the interfaces discussed below could only be achieved through manual editing of password files. The addition of these new command line options provides a much safer option for administrators to use.

While the distinction between non-login and locked accounts has existed in Solaris for many years, it became more pronounced in Solaris 9 where the semantics of locked accounts were more rigidly enforced.

Many customers noticed, for example, that locked accounts could no longer execute jobs using cron (1M). This problem was exacerbated by the fact that many commonly referenced security recommendation guides tell users to lock all of the accounts to which interactive access was not needed (which is most of the default accounts). When this was done, cron jobs for accounts such as "sys" (used for collecting system activity records) stopped working. This problem highlighted the intended difference between non-login and locked accounts and the need for additional interfaces to control them.

For those not already aware, a non-login account is one that must exist on the system (to provide a UID for example) but should not be allowed to login to a system interactively. That is, while a non-login account may be able to leverage delayed execution mechanism such as cron(1M), they cannot access the system using `login(1)`, `telnet(1)`, `ftp(1)`, `ssh(1)`, etc. Accounts that are non-login will have the token `NP` as their password. You can also identify non-login accounts using the `passwd(1)` command:

```
# passwd -s daemon
daemon    NL
# grep "^daemon:" /etc/shadow
daemon:NP:6445:::~:
```

In this case, the `daemon` account has been configured as a non-login account.

A locked account on the other hand is one that is not permitted to access the system in any way - it is locked. A locked account differs from one marked as non-login in that locked accounts are not permitted to use delayed execution methods like cron(1M). Locked accounts are those whose password string has the prefix `*LK*`. Further, you can identify locked accounts using the `passwd(1)` command:

```
# passwd -s listen
listen    LK
# grep "^listen:" /etc/shadow
listen:*LK*:::~:
```

In this case, the *listen* account has been locked.

Here is a practical example. In this case, I will add a new account *gmb* to the system. By default, new accounts created using `useradd(1M)` are locked. After assigning a new password, I will demonstrate the use and result of the new `-N` and `-u` options to the `passwd(1)` command in addition to the `-l` option which has been around for ever.

First, let's create a test account called *gmb*. You will notice that by default the account will be locked.

```
# useradd -d /export/home/gmb gmb
# passwd -s gmb
gmb          LK
```

Next, a password will be assigned to the *gmb* account in the usual way using the `passwd(1)` command...

```
# passwd gmb
New Password:
Re-enter new Password:
passwd: password successfully changed for gmb
# passwd -s gmb
gmb          PS
# grep "^gmb:" /etc/shadow
gmb:Onk28eSYhYJ8s:12683::::::
```

You will notice that the "`passwd -s`" command now returns the keyword *PS* for "password set". If the account did not have a password defined, the keyword *NP* (for "no password") would have been returned.

Now that we have a password, let's lock the account and see what happens to the password string in `/etc/shadow` as well as to the output of "`passwd -s`":

```
# passwd -l gmb
passwd: password information changed for gmb
# passwd -s gmb
gmb          LK
# grep "^gmb:" /etc/shadow
gmb:*LK*Onk28eSYhYJ8s:12683::::::
```

You will notice that the account was in fact locked, but what is new in Solaris 10 is that the password string is not replaced with the "`*LK*`" value. Instead, a "`*LK*`" string prefix is prepended to the password so that the original value can be kept if desired. The great thing about this is that it does not depend on the password algorithm used. With the addition of flexible crypt in Solaris 9, you can replace the default crypt algorithm with either others provided by default in Solaris or one of your own and this new locking mechanism will still just work.

To unlock a locked account, you just use the new `-u` option to the `passwd(1)` command:

```
# passwd -u gmb
passwd: password information changed for gmb
# passwd -s gmb
gmb      PS
# grep "^gmb:" /etc/shadow
gmb:Onk28eSYhYJ8s:12683:~::~:
```

The account is now unlocked and the "*LK*" prefix has been removed from the user's password string. The last thing that we will look at today is how you create a non-login account. To do this, simply use the "-N" option to the passwd command:

```
# passwd -N gmb
passwd: password information changed for gmb
# passwd -s gmb
gmb      NL
# grep "^gmb:" /etc/shadow
gmb:NP:12683:~::~:
```

You will notice that the user's original password has been removed and replaced with the string "NP". This account is now a non-login account and the original password has been discarded. You will not be able to login to this account, but the account will be able to make use of delayed execution facilities. To re-enable an account for interactive logins, simply reassign a password to the account using the passwd (1) command.

That's all for this installment. I hope you find this kind of information useful. In future installments, I will continue to highlight some of the lesser known enhancements that contribute to Solaris security in the hopes of raising awareness and their use.

Trackback URL:

http://blogs.sun.com/roller/trackback/gbrunett/Weblog/managing_non_login_and_locked