Linux Password & Shadow File Formats

Archived: 2026-04-05 13:24:46 UTC

Traditional Unix systems keep user account information, including one-way encrypted passwords, in a text file called ``/etc/passwd''. As this file is used by many tools (such as ``ls'') to display file ownerships, etc. by matching user id #'s with the user's names, the file needs to be world-readable. Consequentally, this can be somewhat of a security risk.

Another method of storing account information, one that I always use, is with the shadow password format. As with the traditional method, this method stores account information in the /etc/passwd file in a compatible format. However, the password is stored as a single "x" character (ie. not actually stored in this file). A second file, called ``/etc/shadow'', contains encrypted password as well as other information such as account or password expiration values, etc. The /etc/shadow file is readable only by the root account and is therefore less of a security risk.

While some other Linux distributions forces you to install the Shadow Password Suite in order to use the shadow format, Red Hat makes it simple. To switch between the two formats, type (as root):

```
/usr/sbin/pwconv      To convert to the shadow format
/usr/sbin/pwunconv    To convert back to the traditional format
```

With shadow passwords, the ``/etc/passwd'' file contains account information, and looks like this:

```
smithj:x:561:561:Joe Smith:/home/smithj:/bin/bash
```

Each field in a passwd entry is separated with ":" colon characters, and are as follows:

- Username, up to 8 characters. Case-sensitive, usually all lowercase
- An "x" in the password field. Passwords are stored in the ``/etc/shadow'' file.
- Numeric user id. This is assigned by the ``adduser'' script. Unix uses this field, plus the following group field, to identify which files belong to the user.
- Numeric group id. Red Hat uses group id's in a fairly unique manner for enhanced file security. Usually the group id will match the user id.
- Full name of user. I'm not sure what the maximum length for this field is, but try to keep it reasonable (under 30 characters).
- User's home directory. Usually /home/username (eg. /home/smithj). All user's personal files, web pages, mail forwarding, etc. will be stored here.

- User's "shell account". Often set to ``/bin/bash" to provide access to the bash shell (my personal favorite shell).

Perhaps you do not wish to provide shell accounts for your users. You could create a script file called ``/bin/sorrysh", for example, that would display some kind of error message and log the user off, and then set this script as their default shell.

> **Note:** Note: If the account needs to provide "FTP" transfers to update web pages, etc. then the shell account will need to be set to ``/bin/bash" -- and then special permissions will need to be set up in the user's home directory to prevent shell logins. See Section 7.1 for details on this.

The ``/etc/shadow" file contains password and account expiration information for users, and looks like this:

```
smithj:Ep6mckrOLChF.:10063:0:99999:7:::
```

As with the passwd file, each field in the shadow file is also separated with ":" colon characters, and are as follows:

- Username, up to 8 characters. Case-sensitive, usually all lowercase. A direct match to the username in the /etc/passwd file.
- Password, 13 character encrypted. A blank entry (eg. ::) indicates a password is not required to log in (usually a bad idea), and a ``*" entry (eg. :*:) indicates the account has been disabled.
- The number of days (since January 1, 1970) since the password was last changed.
- The number of days before password may be changed (0 indicates it may be changed at any time)
- The number of days after which password *must* be changed (99999 indicates user can keep his or her password unchanged for many, many years)
- The number of days to warn user of an expiring password (7 for a full week)
- The number of days after password expires that account is disabled
- The number of days since January 1, 1970 that an account has been disabled
- A reserved field for possible future use
