The Switchuser Command

By George Kraft IV

Any user on the UNIX system can become another user on the system via the switchuser `su` command. This article describes the latest improvements in AIX for the superuser.

The superuser is the privileged administrative account that manages the system for the multipurpose and multiuser UNIX® operating system. Installation and configuration setup of an AIX® system requires superuser authority. For normal operation of the system, the superuser can create and delete accounts, start and stop processes, configure input/output devices, set up networking, and shut down the system. The superuser also can grant privileges to other users on the system.

The privileged superuser account has such a key role in maintaining the UNIX operating system that the system has special allowances for the superuser. Processes run by the superuser bypass runtime and access security restrictions. In addition, when the operating system's process table is full, it reserves some space for the superuser to log in and clean up the system.

The superuser, usually called *root*, has the numeric user ID (UID) of zero (0), shown in the `/etc/passwd` file. The UID 0 indicates the identity of the superuser to the system. Any user with UID 0 has the superuser privileged access, and because of the privileges mentioned above, it is best to run as root as infrequently as possible to prevent accidental system outages due to operator error.

To prevent accidents and to control the use of the root superuser account, by default AIX does not allow programs to execute or library files to be included in the local directory (for example, "."). AIX controls when root can log in and from which TTY ports it can log in. The system can also audit the session of any user including root.

The su Command

With the switchuser `su` command, the superuser can also assume the identity of any user on the system. The `su` command example below assumes the identity of user gk4. The superuser can change its identity from UID 0 to gk4's UID of 1234, which allows the superuser to create and modify files as the user gk4. This is useful for repairing, restoring, and setting up files and directories.

```
/usr/bin/su gk4
```

Although the superuser can assume the identity of user gk4, this does not completely change the environment of the root superuser. To become a completely different user, the superuser must issue the `su` command with the dash (`-`) option, which changes the home directory and initializes its shell environment.

George Kraft IV

The dash option tells the su command to initialize the user shell indicated in /etc/password and to run the user's .profile or .login startup script.

```
/usr/bin/su - gk4
```

In both examples above, the superuser assumed the identity of user gk4 without prompting for the user's password. This takes place because the root user has unrestricted access within the system. However, user gk4 could assume the identity of root—or any other user on the system—by running the su command with a username argument and entering the corresponding user password, when prompted. The su command validates the user account and grants it permission to su.

When using the su command, the non-superuser must authenticate the user's identity by entering the password corresponding to the user. This establishes the user's credentials according to the /etc/passwd and /etc/group databases. However, it is generally recommended that you not divulge account passwords that allow others to assume your identity. If you do share your password with others, then the AIX system administrator could control who can su and who can be "su ed".

The suspend Command

The su command spawns a new shell. When finished, the user can either exit this new shell or suspend the current shell and return to the previous shell. When the shell is suspended in the background, the user can return to the shell in the foreground by using the fg command. This is useful to quickly switch back and forth between the user and root identity, because it is best to run in privilege mode as little as possible.

The su command can spawn a new shell and assume the identity of another user, or it can momentarily change identities while running a specific command. In the example below, a user starts the System Management Interface Tool (SMIT) command as the root user for system administration purposes. Once the smit command exits, the root shell exits and the user's shell is resumed.

```
/usr/bin/su -c /usr/bin/smit
```

A how-to su example appears below in a shell script. The shell's set -x command echos to the screen the command to run. Then the /usr/bin/su -c /usr/bin/smit prints on the screen and prompts the user for the root password to run the smit command.

```
/bin/ksh -c `set -x;
/usr/bin/su -c /usr/bin/smit`
```

Users often find the su command useful in shell scripts to temporarily become the superuser. However, it is prudent to use set -x to show why a prompt appears for the root password.

```
ACTION RebootSU
{
     TYPE          COMMAND
     WINDOW_TYPE   TERMINAL
     EXEC_STRING   /usr/bin/ksh -c 'set -x; \
                   /usr/bin/su - root -c /usr/sbin/shutdown -r now
"Rebooting..."'
DESCRIPTIONThe RebootSU desktop action prompts for the root password,
then shuts down the system for a reboot.
}
```

Figure 1. Desktop action to reboot the system

The Desktop Environment

In the Common Desktop Environment (CDE), it is possible to create a graphical library of administrative commands. However, since the desktop inherits commands from a variety of places, it is dangerous to simply enter the root password in a graphical user interface (GUI) prompt dialog window. Entering the root password prompted by a GUI could actually be coming from a Trojan Horse program trying to gain access to the system.

Figure 1 shows a good example of desktop action which reboots the system. The action opens a terminal emulator window, prints the `shutdown` command to be executed for the user to see, and then prompts the user for the root password.

Conclusion

Any user on the UNIX system can become another user on the system via the `su` command. You can assume the user's home directory and shell initialization by using the dash (`-`) option or simply changing your UID. To return, the user can either exit from or suspend the new shell.

In addition to creating a new shell as another user, you can temporarily become another user to run a command by using the `-c` option. From within a shell script or from a desktop action, you can print to the screen the specific command for which the system is prompting the password.

To change who can issue the `su` command and/or who receives the `su`, run `smit users` command and see the options under Change/Show Characteristics of a User. From the AIX SMIT, the system administrator can control who can and cannot use the switchuser command.

George Kraft IV, IBM Corporation, 11400 Burnet Road, Austin, TX 78758. Mr. Kraft is an advisory software engineer for IBM's Network Computer Division. He recently moved from IBM's RS/6000 Division where he worked on the AIX integration of the IBM Network Station. He has a BS in Computer Science and Mathematics from Purdue University.