Define Restricted Logins

Special Notices

Information in this document is correct to the best of our knowledge at the time of this writing. Please send feedback by fax to "AIXServ Information" at (512) 823-4009.

Please use this information with care. IBM will not be responsible for damages of any kind resulting from its use. The use of this information is the sole responsibility of the customer and depends on the customer's ability to evaluate and integrate this information into the customer's operational environment.

Note: The information in this document is **not** applicable for AIX 4.1.

About This Document

This document describes two examples of user-defined authentication methods. If these are run as a primary authentication method, they will restrict logins by the root user to a single device while still permitting "su" access to the root account from another port, or limit the number of concurrent logins allowed per user.

About the Procedure

DISCLAIMER:

The authentication methods defined in this document are not supported by IBM AIX support, and are provided only as examples. Furthermore, modification of the included software program may be necessary in order for it to work in a particular environment.

User authentication is used to control access to a RISC System/6000. There are two levels of user authentication in AIX: primary and secondary.

Note: A primary authentication method will prevent login access while a secondary method is purely informational and will **not** restrict access.

It is common practice to install site-specific user verification tests as primary and/or secondary authentication methods. Access by login, su, rlogin, telnet are subject to defined primary and secondary authentication methods. rsh, rexec, and ftp are not subject to these methods.

The methods described in this document, if used as primary authentication will restrict root logins to a specific device, or limit the number of concurrent logins allowed on a per user basis.

Steps to Implement Example I - Restrict root login

The following steps describe how to implement the "console-only" authentication as a primary authentication method. (It must run as a primary authentication method to enforce the restriction.) The steps dexribe how to make the authentication method know to AIX. modify the root user's profile to invoke the validation routine, and compile the "console-only" code.

The module, named "console-only.c", determines if a user is signing onto the specified device (the default is the system console) or executing the "su" command. If either of these conditions are true, the routine returns a status value of zero. Otherwise, it returns a status value of one. If a status value of zero is returned, the login is validated and the user's initial program is executed. invoke the validation routine, and compile the "console-only" code.

1. Edit the /etc/security/login.cfg file and add the following stanza to the file.

   ```
   CONSOLE:
        program = /etc/security/console-only
   ```

   This will make the method known to AIX.

   Note: The program "console-only.c" optionally takes one parameter to indicate a particular device to which root access is restricted. To specify a device other than the console, for instance "tty0", modify the CONSOLE stanza as follows:

   ```
   CONSOLE:
        program = "/etc/security/console-only /dev/tty0"
   ```

2. Now, change the root user's attributes to invoke the new authentication method when the root user attempts to log in. You can do this either from the command line or from smit:

   - From the command line, run the following: (This assumes that "SYSTEM" was the previous setting for auth1.)

     ```
     chuser auth1=SYSTEM,CONSOLE root
     ```

     Note: There cannot be any spaces in the comma-separated list of primary authentication methods.

   - To use smit, enter "smit chuser". Then enter "root" for the user name. In the field "PRIMARY authentication method", add "CONSOLE" to the comma-separated list of primary authentication methods. For example, the field may now read "SYSTEM,CONSOLE". (NOTE: There cannot be any spaces in the comma-separated list of primary authentication methods.) Press Enter to commit the change.

3. Save the text below the "console-only.c" heading as "console-only.c", and compile it with this command:

   ```
   cc -o /etc/security/console-only console-only.c
   ```

   Note: Please note that page headers and footers may appear in the code. They should be removed before the code is used.

4. Finally, verify that the authentication method is working properly by attempting to login, su, rlogin, and telnet as the "root" user. If the user-defined authentication method is working properly, "root" logins will be allowed only on the console or the defined terminal.

"console-only.c"

```
/* Console-only root login authentication method.
 *
 *   Written By: John F. Haugh, II        Date:  18 March 93 */

#include <sys/types.h>
#include <utmp.h>
#include <stdio.h>
#define CONSOLE "/dev/hft/0"

/* console-only - TTY Port access control authentication method
 *
 *    console-only permits root logins on the console device (defined
 *    with the CONSOLE macro above).  It allows su's from any device. */

main (int argc, char **argv)
{
        char    *user;
        char    *console;
        char    *tty, *ttyname ();
        struct  utmp    utmp, *putmp;

        /* Usage is "console-only <user>".  This would typically be
         * only for root, but we allow other users to use this method. */

        if (argc < 2)
                exit (1);
        user = argv[argc - 1];

        /* If there are 3 arguments, #2 is the name of the device.  */

        if (argc == 2)
                console = CONSOLE;
        else
                console = argv[1];

        /* Get the TTY name.    */

        if ((tty = ttyname (0)) == (char *) 0)
```

```
                exit (1);

        /* Clear the utmp structure so I can fetch this line's utmp
         * record.     */

        memset ((void *) &utmp, 0, sizeof utmp);
        strncpy (utmp.ut_line, tty + 5, sizeof utmp.ut_line);
        setutent ();
        putmp = getutline (&utmp);

        /* See if my PPID is the same as the PID in the utmp record.
         * That would mean that login is calling me.  This is what
         * distinguishes between "login" and "su".     */

        if (putmp == (struct utmp *) 0 || putmp->ut_pid != getppid ())
                exit (0);
        exit ((strcmp (console, tty) == 0) ? 0:1);
}
```

How to Implement Example II - Limit User Logins

In order to limit the number of logins per user, you will have to create a script and update two files: /etc/security/login.cfg and /etc/security/user.

1. Using an editor create a script, such as:

```
vi /usr/bin/Block_user   * name isn't important, just be consistent
```

```
#!/bin/ksh

USER=$1
NUM= who | grep $USER |cut -c1-8 | wc -l
# The above   is not a single quote but back quote(accent)
if ⅛ $NUM -lt 1 ‘
then
   exit 0
fi
   echo "permission denied ...$NUM is the limit of logins"
   exit 1
```

   Save this file and then change its permissions. Make sure this file is owned by root and does not have write permission for group or other.

```
   chmod 755 /usr/bin/Block_user        * make script executable
```

2. Edit /etc/security/login.cfg

```
   vi /etc/security/login.cfg
```

   Add the following lines:

```
* auth_method:
*     program =
```

   you will need to change it to look as follows:

```
auth_method:
program = /usr/bin/Block_user
```

3. Edit /etc/security/user

```
admin = false
login = true
su = true
daemon = true
rlogin = true
sugroups = ALL
ttys = ALL
auth1 = SYSTEM
auth2 = NONE
tpath = nosak
umask = 022
expires = 0

root:                   admin = true
user1:                  admin = false
```

Change the auth1 line to:

```
default:                   auth1 = SYSTEM, auth_method
```

This change will affect all users logging into the system.

```
   user1:                   auth1 = SYSTEM, auth_method
   user2:                   auth1 = SYSTEM, auth_method
   user3:
```

The above changes to the individual user stanza's would limit user1 and user2 to the login restrictions defined in the script above.

Reader's Comments

Please fax this form to (512) 823-4009, attention "AIXServ Information". You may also e-mail comments to: elizabet@austin.ibm.com. These comments should include the same customer information requested below.

Use this form to tell us what you think about this document. If you have found errors in it, or if you want to express your opinion about it (such as organization, subject matter, appearance) or make suggestions for improvement, this is the form to use.

If you need technical assistance, contact your local branch office, point of sale, or 1-800-CALL-AIX (for information about support offerings). These services may be billable. Faxes on a variety of subjects may be ordered free of charge from 1-800-IBM-4FAX. Outside the U.S. call 415-855-4329 using a fax machine phone.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you.

Note: If you have a problem report or item number, supplying that number may help us determine why a procedure did or did not work in your specific situation.

Problem Report or Item #: Branch Office or Customer #:

Be sure to print your name and fax number below if you would like a reply:

Name: Fax Number:

END OF DOCUMENT (JH) (restrict.login.dev.cmd, 4FAX# 2561)