Resetting File Permissions

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 several possible mechanisms for restoring incorrect file permissions:

- Manually determine correct permissions by examining mksysb tape or another system, and manually set permissions.
- Manually determine correct permissions by examining mksysb or install tape and manually set permissions.
- Automatically determine and set permissions based on mksysb or tape.
- Automatically determine and set permissions based on sysck.cfg file.

The sections on the manual methods and the sysck.cfg method apply to all AIX 3.x versions but have not been verified with AIX 4.1 or later. The section on automatically setting permissions from a mksysb tape will not work with AIX 4.1 or later as 4.1 mksysb uses Backup & Restore and the table of contents does not show permissions and owners

Notes:

1. If you use ACLs (access control lists), using the chmod numerical parameters will erase the ACLs. The document "Backup and Restore Access Control Lists During mksysb" may be helpful. It is available in these locations:
   - Document number 2685 from 1-800-IBM-4FAX within the U.S. or from 415-855-4FAX outside the U.S. Outside the U.S., the number must be dialed from a fax machine phone.

- World-wide web http://aix.boulder.ibm.com. (Follow menu choices for AIX/USA/Electronic Services.)

2. Before using the methods in this document, you may wish to save a record of your current permissions by redirecting the output of the following to a file:

```
ls -lR /
```

Manually Setting Permissions

Examining a mksysb Image or Instal Tape

If you have a recent mksysb, you can examine the permissions of the backed up files by skipping to the file storage portion of the tape and performing a tape listing. Assuming the archive device is /dev/rmt0, the following commands will produce a listing of all files on the tape. You can refer to InfoExplorer for documentation on the chown, chmod, tar, and tctl commands.

```
tctl -f /dev/rmt0.1 fsf 3
tar -tvf /dev/rmt0 > /tmp/mksysb.listing
```

The file /tmp/mksysb.listing will contain the tar listing of every file on the tape. You can use the grep command to locate the line in which you are interested and then use the chown and chmod commands to set the file ownership and permissions.

Examining Another System

If you have a similar system you may examine the permissions of the file in question on the other system. Differences in file ownership or permissions can then be corrected with the chown and chmod commands.

Automatically Setting Permissions

Setting Permissions With a mksysb or Install Tape

Symptom: All the permissions and/or ownerships on my files (or the whole system) are changed! How do I reset all permissions and ownership?

Answer: This solution depends upon having a mksysb tape. If you have a system backup that was not made by mksysb (using tar format) you will have to make modifications to the script.

Note when using an Install tape, only the bos protion is in tar format and can be used by this process.

Steps

1. In the following script, replace "rmtx" with the name for your tape drive, such as "rmt0".
2. Insert the mksysb tape and run the following script, which will create another script called reset.perms.out.
3. Carefully examine reset.perms.out and modify it if needed before running it on your system.
4. Run reset.perms.out to change all ownership, group, and permissions to what they were at the time of the last mksysb backup.

The Script

Notes:

1. Please note that page headers and footers may appear in the following code. They should be removed before the code is used. Also, revision bars (vertical bars in the left margin which mark changes in the document) may appear to the left of the code and should be removed before the code is used.
2. Be sure that the string "#!/bin/ksh" starts in the first column on the first line of the file containing the code.

Here is the script:

```
#!/bin/ksh
rm reset.perms.out 2>/dev/null
cd /tmp
tctl -f /dev/rmtx rewind
tctl -f /dev/rmtx.1 fsf 3
tar -tvf /dev/rmtx |
awk '{
        if ( NF == "9" )
        {
                printf ("chown %s.%s %s\n",$2,$3,$9)
                {
                perms=0
                if(substr($1,2,1) == "r")
                        perms = perms + 400
                if(substr($1,3,1) == "w")
                        perms = perms + 200
                if(substr($1,4,1) == "x")
                        perms = perms + 100
                if(substr($1,4,1) == "S")
                        perms = perms + 4000
                if(substr($1,4,1) == "s")
                        perms = perms + 4100

                if(substr($1,5,1) == "r")
                        perms = perms + 40
                if(substr($1,6,1) == "w")
```

```
                perms = perms + 20
            if(substr($1,7,1) == "x")
                perms = perms + 10
            if(substr($1,7,1) == "S")
                perms = perms + 2000
            if(substr($1,7,1) == "s")
                perms = perms + 2010

            if(substr($1,8,1) == "r")
                perms = perms + 4
            if(substr($1,9,1) == "w")
                perms = perms + 2
            if(substr($1,10,1) == "x")
                perms = perms + 1

            if(substr($1,10,1) == "T")
                perms = perms + 1000
            if(substr($1,10,1) == "t")
                perms = perms + 1001

            printf("chmod %d %s     # %s\n",perms,$9,$1)
            }
        }
}' >reset.perms.out
chmod 755 reset.perms.out
```

Automatically Setting Permissions Using sysck.cfg

sysck or tcbck Command

The sysck command was renamed to tcbck in AIX 3.2, but is referred to as sysck in this document for historical consistency.

The sysck command was designed to strictly enforce file ownership and permissions according to file descriptions in /etc/security/sysck.cfg. When file contents are found to disagree with file size and checksum information, sysck revokes access to the file by removing all permission attributes. For this reason, "sysck" may be unsuited to many environments.

Warning

sysck can render a system unusable.

If the "-y" option will be used, the system administrator should verify that the sysck.cfg file has the correct information. If the checksum and size for any file are not correct in the sysck.cfg, that file will be made inaccessible.

To update a single file using sysck, enter the command

```
sysck -t <file>
```

where <file> is the name of the file being changed. If you receive any messages indicating that the file size or checksum is incorrect, you must answer the prompt "no" to indicate that you do not wish the changes for that value made.

If you wish for every file listed in sysck.cfg to be checked, replace <file> with the keyword "ALL".

fileck Script

Warning

This script automatically applies the values in /etc/security/sysck.cfg without concern for the actual file contents (it does not check checksum and size). The checksum and size information in sysck.cfg exists to prevent Trojan horses and other security violations from occurring. Using this script may prevent your system from detecting certain types of security-related problems.

The attached script should be copied to a local directory and named "fileck".

This script implements many of the rules used by sysck but does not perform file-size or checksum tests. Since these two tests in sysck can result in the disabling of a file-system object, the potential for damage using "fileck" is much less than that of sysck. However, fileck may prevent the system from detecting certain security-related problems.

fileck operates in single-file or "ALL" mode, similar to sysck. The syntax is

```
fileck { ALL | <file(s)> }
```

Files must be specified with the full path as found in /etc/security/sysck.cfg.

When called with one or more file names on the command line, fileck will examine the sysck.cfg to determine the correct owner, group, permissions, hard links, and symbolic links. In "ALL" mode, fileck checks all files listed in sysck.cfg. fileck returns a message for each file that is processed and reports the names of any files specified on the command line that could not be found in sysck.cfg.

Notes:

1. Please note that page headers and footers may appear in the following code. They should be removed before the code is used. Also, revision bars (vertical bars in the left margin which mark changes in the document) may appear to the left of the code and should be removed before the code is used.
2. Be sure that the string "#!/bin/ksh" starts in the first column on the first line of the file containing the code.

3. You must be logged in as the root user to run this command.

Here is the fileck script:

```
#!/bin/ksh
#
#   fileck -- perform sysck-like processing without the grief
#
fixmode()
{
   file=${1}
   modes=$(echo ${2} | tr ',' ' ')
   TCB=N
   SUID=u-s
   SGID=g-s
   SVTX=-t

   for mode in ${modes} ; do
      case ${mode} in
         TCB) TCB=Y ;;
         [0-9]*) PERM=${mode} ;;
         [-r]*)  u=${mode%%??????}
                 r=${mode##???}
                 g=${r%%???}
                 o=${r##???}
                 PERM=$(echo u=${u},g=${g},o=${o} | tr -d '-')
                 ;;
         SUID)   SUID=u+s ;;
         SGID)   SGID=g+s ;;
         SVTX)   SVTX=+t ;;
      esac
   done
   chmod ${PERM},${SUID},${SGID},${SVTX} ${file}
   if [ ${TCB} = Y ]; then
      chtcb on ${file}
   else
      chtcb off ${file}
   fi
}

fixsymlinks()
{
   file=${1}
   links=$(echo ${2} | tr ',' ' ')

   for link in ${links} ; do
      if [ -L ${link} ]; then
         rm -f ${link}
         ln -s ${file} ${link}
      fi
   done
}
```

```
fixlinks()
{
   file=${1}
   links=$(echo ${2} | tr ',' ' ')

   ls -i ${file} | read inum_a junk

   for link in ${links} ; do
      if [ -f ${link} ]; then
         ls -i ${link} | read inum_b junk
      else
         inum_b=0
      fi
      if [ ${inum_a} != ${inum_b} ]; then
         ln -f ${file} ${link}
      fi
   done
}

fixall()
{
   scratch=/tmp/fixall$$
   file=${1}

   grep -p "^${file}:" /etc/security/sysck.cfg > ${scratch}
   read real_file junk < ${scratch}
   real_file=${real_file%%:}

   if [ ! -s ${scratch} ]; then
      echo "no matches for ${file}" 1>&2
      return
   fi
   echo "checking ${file}"
   while read attr junk value ; do
      case ${attr} in
         owner)          chown ${value} ${file} ;;
         group)          chgrp ${value} ${file} ;;
         links)       fixlinks ${file}  ${value} ;;
         symlinks) fixsymlinks ${file}  ${value} ;;
         mode)         fixmode ${file}  ${value} ;;
      esac
   done < ${scratch}
   /usr/bin/rm -f ${scratch}
}

if [ $# = 0 ] ; then
   echo "usage: fileck { ALL | file ... }"
   exit 1
elif [ "${1}" = "ALL" ]; then
   list=/tmp/fileck$$
   grep '^/.*:$' /etc/security/sysck.cfg | sed -e 's/://' > ${list}
```

```
   while read FILE ; do
      fixall ${FILE}
   done < ${list}
   /usr/bin/rm -f ${list}
else
   for FILE in $* ; do
      fixall ${FILE}
   done
fi
```

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 (reset.file.perms.cmd, 4FAX# 4253)