Utility "rxxfind" V1.1

The tool "rxxfind" has been designed for putting together z/OS UNIX security related file structure information in two different ways that can be combined as well. Like "xfind" it can be used efficiently in a z/OS UNIX sysplex sharing environment and only file systems that are owned locally are used for searching.

- In case of zFS the search is done on the zFS-owning system, otherwise on the USS-owning system. Doing all this avoids unnecessary XCF traffic and overhead.
- Important: NFS file systems, as being "remote" file systems, are not searched. Just "local" z/OS file systems are searched.
- You can call the utility using two possibilities.

  (a) It can be executed as a SYSREXX routine, named RXXFIND, from a console locally or on all systems in parallel.

  (b) It can be started with name "rxlfind" locally from z/OS UNIX. You will normally use the UNIX tool from within a batch job as this allows best to process the functions and commands.

Functions of the utility...

- "Find for Generic User and Group specifications" is used to list z/OS UNIX access of users or groups within the current file system structure (permission bits, ACLs, directory default ACLs and file default ACLs). Users and groups can be specified generically to combine lots of users or groups.
- "List specific attributes out of a list of supported attributes" lists the specific attributes as requested.
- You can combine both functions but the output looks better and clearer when you do not do it.

Using "rxlfind" from within a batch job (according to ccsid 1141)

Following an BPXBATCH/SL based job that can be nicely used to run "rxlfind"...

```
//UNIXJ65  JOB ,'USS job',NOTIFY=&SYSUID.,REGION=0M,SYSTEM=SC65
//* ------------------------------------------------------------------
//RXLFIND  EXEC PGM=BPXBATSL,PARM='PGM /bin/sh -c $STDIN!$ICONV!sh'
//STDIN    DD DATA,DLM=##
rxlfind /usr/sbin -s0 -lugep -p !0011 -d -f -x -a dd:usrgrps
RC=$?
echo "We are done..." >&2
if [ $RC -ne 0 ]; then; echo "\nRC= $RC"; exit 1; else; exit 0; fi
##
//USRGRPS  DD DATA,DLM=##
G USS*
U *TST*
U *ROOT
G SYS*
##
//STDENV   DD DATA,DLM=##
STDIN=/bin/cat //dd:STDIN
ICONV=iconv -f1141 -t1047
_BPX_SHAREAS=MUST
_EDC_ADD_ERRNO2=1
_BPX_BATCH_UMASK=0022
PATH=/usr/local/bin:/bin
##
//STDOUT   DD SYSOUT=*,LRECL=136,RECFM=VB
//STDERR   DD SYSOUT=*,LRECL=136,RECFM=VB
//* ------------------------------------------------------------------
```

Here are more detailed explanations about the options and values for rxlfind...

Specifying generic values in ddname USRGRPS used when option "-a" is specified ...

- Specifying "G USS*" means to look for access of all groups starting with string "USS".
- Specifying "U *TST*" means to look for access of all users with string "TST". Some within the user name. Using "*TST" is equivalent.

You can start such a job on every LPAR in the sysplex in parallel as only locally managed or mounted file systems are searched to avoid XCF overhead.

Details for listing specific attributes with option "-l"...

- Using "u" with option "-l" means to list the userid or uid (if no user for the uid is set) information.
- Using "g" with option "-l" means to list the group or gid (if no group or gid is set) information.
- Using "e" with option "-l" means to list the extended attributes information.
- Using "p" with option "-l" means to list the permission bit settings.
- Using "i" with option "-l" means to list the inode number.
- Using "f" with option "-l" means to list the auditid (FID) value.
- If no specific attribute is given the default is "ugepi".

If leaving out option "-a" or "-l" you simply get listed all the z/OS UNIX entries found.

The syntax for using "rxlfind"

The syntax for using "rxlfind" is shown next via calling it from z/OS UNIX without parameters.

```
$> rxlfind
Syntax: rxlfind start [-parm [parmvalue]] [...] ...

start -- The z/OS UNIX entry to start with, normally a directory
-u [!]userid -- Search for user 'userid' or ( ! ) avoid hitting user 'userid'
-g [!]group -- Search for group 'group' or ( ! ) avoid hitting group 'group'
-e [!]extattr -- Search for extended attributes 'extattr' or ( ! ) avoid it
-p [!]mode -- Search for permission bits 'mode' or ( ! ) avoid it
-d -- Only search for directory entries
-f -- Only search for regular file entries
-x -- Only search within the initial file system
-s nn -- Only search nn directory sub-levels; 0 means the start directory only
-l [[u][g][e][p][i][f]] -- List specific attributes
-a [dd:ddname|dsn]-- Search for generic user and group entries in a data set

Using "-d -f" searches for directories and files.
Using "i" with "-l" means to list the inode number.
Using "f" with "-l" means to list the auditid (FID) value.
For more details see the documentation as provided.
$>
```

Output of the job

Following an actual output for the job is provided.

```
Mode Exta User     Group    Name
---- ---- -------- -------- ------------------------------------------------...
0744 ap-- BPXROOT  8512     /Z23RE1/usr/sbin/sshd
BPXROOT  RWX USER  /Z23RE1/usr/sbin/sshd
```

```
0744 -p-- BPXROOT  8512     /Z23RE1/usr/sbin/chroot
BPXROOT  RWX USER  /Z23RE1/usr/sbin/chroot
0744 -p-- BPXROOT  8512     /Z23RE1/usr/sbin/cron
BPXROOT  RWX USER  /Z23RE1/usr/sbin/cron
0744 --s- BPXROOT  8512     /Z23RE1/usr/sbin/init
BPXROOT  RWX USER  /Z23RE1/usr/sbin/init
0744 -p-- BPXROOT  8512     /Z23RE1/usr/sbin/inetd
BPXROOT  RWX USER  /Z23RE1/usr/sbin/inetd
0744 -ps- BPXROOT  8512     /Z23RE1/usr/sbin/rlogind
BPXROOT  RWX USER  /Z23RE1/usr/sbin/rlogind
```

More details and information about the output data...

- Normally it is useful to use just "-l" or "-a" and not both. It is allowed and shown here for demonstration but it be confusing to have it mixed.
- On using "-a" column1 shows a userid or group, column 2 is the type of access, in column3 you see the source of the access and finally column 4 lists the z/OS UNIX entry itself. The source types are self explaining; USER (base permission of a user), GROUP (group owner permission), ACL-U (User ACL), ACL-G (Group ACL), DDACL (directory default ACL) and FDACL (file default ACL).

More examples of options specified with rxlfind and what you get in the output...

- Using **`-e!a -e!p`** lists all enrtries with no APF and no PGMCTL extended attribute while **`-e!ap`** only avoids to show entries with APF and PGMCTL extended attribute at the same time.
- Using **`-p 1000`** lists all entries with the sticky bit set on.
- Using **`-ubpxroot`** lists all entries with owner being the superuser (if BPXROOT is defined with UID=0).
- Using **`-u!0`** lists all entries with owner not being the superuser.
- Using **`-p 0755 -p !0020 -p !0002`** lists all entries having exactly permission bits set to 755.
- Using **`-p !0755`** lists all entries having not set permission bits 755 or higher, so not 755, not 775, not757 and not 777.
- Note, currently all select criteria is meant to be logically interpreted as AND. There is no OR at the moment.