

RACF UNIXPRIV CLASS

November 2011



Robert S. Hansel

Lead RACF Specialist - RSH Consulting, Inc.

R.Hansel@rshconsulting.com - 617-969-9050 - www.rshconsulting.com

RSH INSTRUCTOR



Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc., a firm he established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. He has worked with IBM mainframes since 1976 and in information systems security since 1981. Mr. Hansel began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. He has reviewed, implemented, and enhanced RACF controls for major insurance firms, financial institutions, utilities, payment card processors, universities, hospitals, and international retailers. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He has also created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

Contact and background information:

- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel

UNIXPRIV CLASS

Allows delegation of specific Superuser privileges

Superuser (root - Unix system administrator)

- Full access to all Unix directories and files (like OPERATIONS)
- Can change directory/file owners and permissions (like SPECIAL)
- Can perform privileged Unix functions
- Can use privileges related to most unprotected FACILITY BPX resources and to some protected ones without permission
- If BPX.DAEMON is not defined, can assume other user's identities

Superuser authority assigned by ...

- | | |
|--------------------------------------|-------------------------|
| • OMVS(UID(0)) | OMVS STCs & Daemons |
| • FACILITY - BPX.SUPERUSER | Unix Tech Support staff |
| • PRIVILEGED / TRUSTED Started Tasks | Still require uid & gid |

UNIXPRIV CLASS CDT ENTRY

ID = 1

POSIT = 555

MAXLNTH = 246

FIRST = ANY

OTHER = ANY

KEYQUAL = 0

DFTRETC = 4

DFTUACC = NONE

OPER = NO

GENLIST = DISALLOWED

RACLIST = ALLOWED

RACLREQ = YES

UNIXPRIV CLASS - SECURITY ADMIN

SUPERUSER.FILESYS.CHANGEPERMS - 'chmod' any permit

SUPERUSER.FILESYS.CHOWN - 'chown' any file or directory

- READ access required
- Also require x (search) authority to upper directories of target directory or file
- Limit access to CHANGEPERMS and CHOWN to security administration staff and use in lieu of BPX.SUPERUSER

SHARED.IDS

- Prevents assignment of existing uid or gid to keep them unique
- Existence of profile acts as switch to activate restriction - must be Discrete
- Requires Application Identity Mapping (AIM) Stage 3
- Can be overridden using SHARED keyword when creating or changing OMVS segment
`ADDUSER FTPD OMVS(UID(0) SHARED)`
- Requires System-SPECIAL or READ access to use SHARED keyword
- Required to use FACILITY BPX.NEXT.USER
- Considered essential if delegating OMVS UID administration via FIELD class profiles

UNIXPRIV CLASS - SECURITY ADMIN

CHOWN.UNRESTRICTED

- Existence of profile acts as switch to activate - must be Discrete
- Allow any user to 'chown' their files & directories to any other user

FILE.GROUPOWNER.SETGID

- Change method of GROUP inheritance for new files and directories
 - Standard Unix behavior - GROUP taken from parent Directory in which new subdirectory or file is created
 - New optional behavior - GROUP taken from 'effective' gid in User Security Packet (USP) of the creating process
- Existence of profile acts as switch to activate - must be Discrete
- Behavior depends on set-gid bit for the parent directory
 - If bit OFF (default) - GROUP taken from USP
 - If bit ON - GROUP taken from Directory as before
 - Must use 'chmod' command to turn on set-gid bit for directory in order for it to revert to original behavior
 - 'ls' display shows 's' ('x' on) or 'S' ('x' off) in x-bit place for GROUP
- Currently running processes do not recognize the change

UNIXPRIV CLASS - MAINTENANCE

SUPERUSER.FILESYS.MOUNT

- 'mount' and 'chmount' HFS files

READ **With NOSETUID only**

UPDATE **With SETUID or NOSETUID**

SUPERUSER.FILESYS.QUIESCE

- 'quiesce' and 'unquiesce' HFS files

READ **With NOSETUID only**

UPDATE **With SETUID or NOSETUID**

Limit access to Tech Support staff responsible for maintaining UNIX

UNIXPRIV CLASS - SERVICE PROCESSES

SUPERUSER.FILESYS.PFSCTL	Physical File System services
SUPERUSER.FILESYS.VREGISTER	Register as VFS server (e.g. NFS)
SUPERUSER.IPC.RMID	Release IPC resources ('ipcrm')
SUPERUSER.PROCESS.GETPSENT	Get process status info
SUPERUSER.PROCESS.KILL	Issue kill to processes
SUPERUSER.PROCESS.PTRACE	Use ptrace through dbx debugger
SUPERUSER.SETPRIORITY	Increase own priority

Require READ access to use

Typically, limit access to UNIX processes or users performing debugging

UNIXPRIV CLASS - SERVICE PROCESSES

To debug daemons, users need access to ...

- **SUPERUSER.PROCESS.GETPSENT**
- **SUPERUSER.PROCESS.KILL**
- **SUPERUSER.PROCESS.PTRACE**
 - **Also requires access to BPX.DEBUG to trace processes running with APF-authorization or BPX.SERVER authority**

Requires SUPERUSER.PROCESS.GETPSENT

- **WebFocus IADMIN user**

UNIXPRIV CLASS - ACCESS

SUPERUSER.FILESYS

- Grants access to all Unix files and directories at specified permit level, even if denied access by permission bits and ACLs (unless ACLOVERRIDE is defined)

READ Read all files and search all directories
UPDATE Write to any files
CONTROL Write to any directory

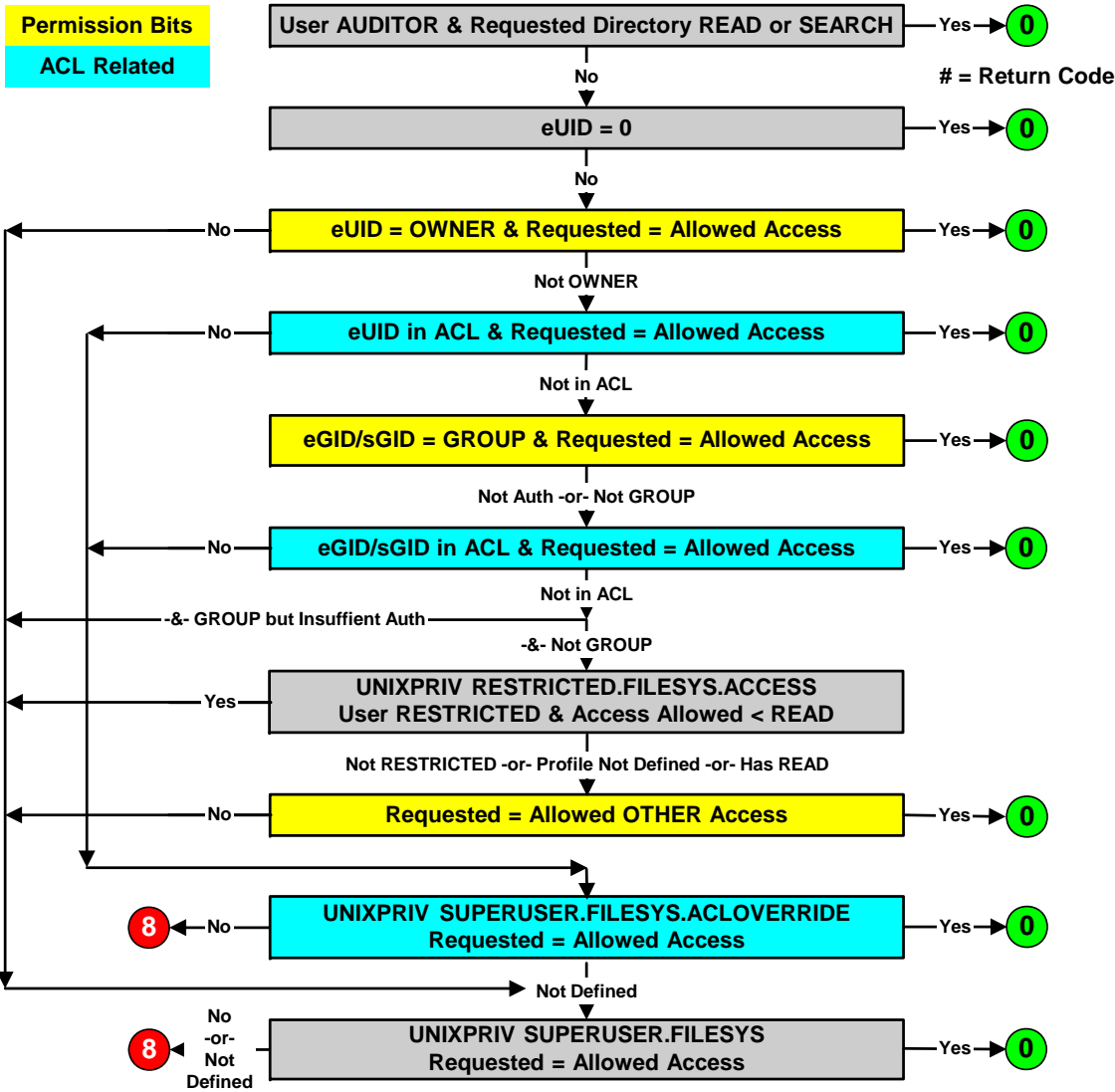
SUPERUSER.FILESYS.ACLOVERRIDE

- Causes ACL permissions to overrule access SUPERUSER.FILESYS would otherwise grant
- Permitting access grants access like SUPERUSER.FILESYS

RESTRICTED.FILESYS.ACCESS

- Prohibits RESTRICTED users from gaining access via OTHER permission bits
- Permitting READ access bypasses the restriction

ACCESS AUTHORIZATION - ACL



(c) 2011 RSH Consulting, Inc.

UNIXPRIV CLASS

Checked after other authorities - AUDITOR, uid(0), permission bits, ACLs

- **Cannot be used to supersede or limit other authorities**

Can log successful accesses, but not failures

- **RACROUTE LOG=NOFAIL is used**
 - **Except for profile SHARED.IDS**
- **To monitor, specify ...**
 - **RALT UNIXPRIV profile AUDIT(SUCCESS(level))**
- **Cannot monitor with LOGOPTIONS**
 - **Bypassed due to RACROUTE REQUEST=FASTAUTH**

Catch-all * or ** profile not recommended