RACF UNIXPRIV Class

SHARE - August 2014
Session 15539

Robert S. Hansel Lead RACF Consultant R.Hansel@rshconsulting.com 617-969-9050

Robert S. Hansel

Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc., an IT security professional services 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, analyst, and consultant. He has reviewed, implemented, and enhanced all manner of RACF controls for major insurance firms, financial institutions, utilities, payment card processors, universities, hospitals, and international retailers. Mr. Hansel is a leading expert in securing z/OS Unix and has pioneered the effective use of many of its security features and functions. He is also highly skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. Mr. Hansel has 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
- www.rshconsulting.com

UNIXPRIV Class

- Allows delegation of specific Superuser privileges

- Superuser (root - Unix system administrator) privileges
  - 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 even without permission
  - If BPX.DAEMON is not defined, can initiate processes with other user's identities

- Superuser authority assigned by ...

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

UNIXPRIV Class - RACF CDT Entry

```
ID          = 1              DFTRETC     = 4
POSIT       = 555            DFTUACC     = NONE
                             OPER        = NO
MAXLNTH     = 246
FIRST       = ANY            GENLIST     = DISALLOWED
OTHER       = ANY            RACLIST     = ALLOWED
KEYQUAL     = 0              RACLREQ     = YES
```

UNIXPRIV Class - Security Administration

- SUPERUSER.FILESYS.CHANGEPERMS - 'chmod' and 'setfacl' 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 duplicate 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 2 or 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 implement FACILITY BPX.NEXT.USER
  - Considered essential if delegating OMVS UID administration via FIELD class resource USER.OMVS.UID to prevent inappropriate assignment of UID(0)

UNIXPRIV Class - Security Administration

- CHOWN.UNRESTRICTED
  - Existence of profile acts as switch to activate functionality - must be Discrete profile
  - z/OS 1.13 and before - if defined, any file or directory owner can chown OWNER or chgrp GROUP to any other user or group respectively
  - z/OS 2.1 or z/OS 1.12 and 1.13 with Security APAR OA41364 - access permission required

READ	Change OWNER to a non-0 ID or change GROUP
UPDATE	Change OWNER to a UID(0) ID

- FILE.GROUPOWNER.SETGID
  - Change method of GROUP inheritance for new files and directories
    - Standard Unix behavior - GROUP taken from parent Directory
    - New optional behavior - GROUP taken from 'effective' gid of creating users' User Security Packet (USP)
  - 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 parent 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', 'chmount', & 'unmount' zFS files
  - READ   With NOSETUID
  - UPDATE   With SETUID

- SUPERUSER.FILESYS.QUIESCE
  - 'quiesce' & 'unquiesce' zFS files
  - READ   With NOSETUID
  - UPDATE   With SETUID

- Limit access to Tech Support staff responsible for maintaining UNIX

- Permit Started Task DFHSM UPDATE access to SUPERUSER.FILESYS.QUIESCE if it backs up Unix File Systems (this is an alternative to assigning it UID(0))

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 to 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 FACILITY profile BPX.DEBUG to trace processes running with either APF-authorization or BPX.SERVER authority

- Require SUPERUSER.PROCESS.GETPSENT
  - WebFocus IADMIN user
  - Tivoli System Automation (Netview) - if not assigned UID(0)
  - Peoplesoft
  - Users of " ps " command (process status) to list dubbed ids and find their attributes [useful for RACF administrators]

- Require SUPERUSER.FILESYS.PFSCTL
  - SAP's sap-system-identifier-ADM ID - READ
  - CA Mainframe Chorus for DB2

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 Access Control Lists (ACLs) [unless ACLOVERRIDE is defined]

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

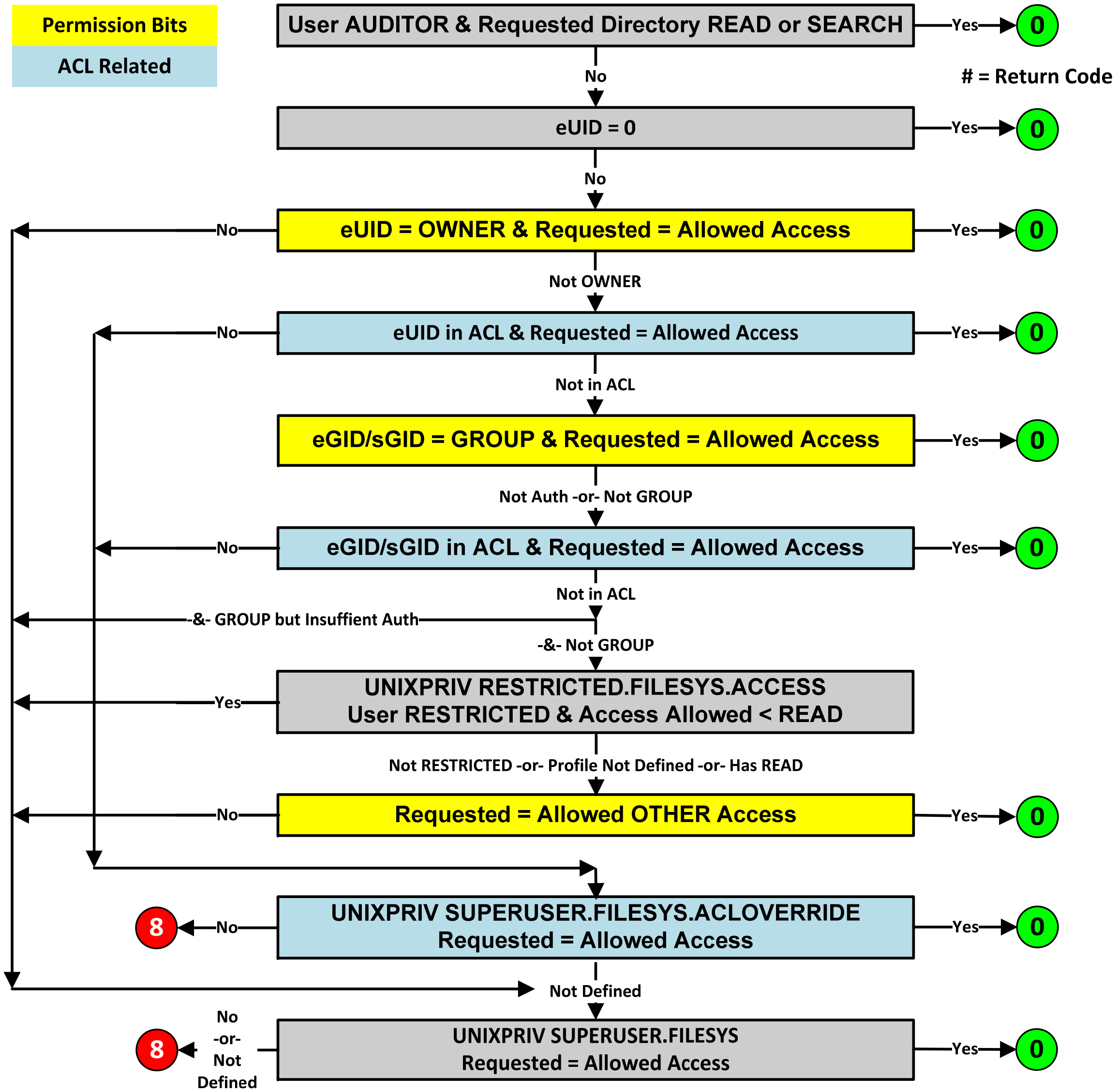
  - Can replace UID(0) with SUPERUSER.FILESYS access

❖ READ	Sterling (now CA) Solve NetMaster
❖ READ	Tivoli Asset Discovery - Inquisitor
❖ READ	Tivoli System Automation (Netview)
❖ CONTROL	Tivoli Directory Server (LDAP) [or substitute with specific permits]

- 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

UNIXPRIV Class - Access



Permission Bits

ACL Related

= Return Code

User AUDITOR & Requested Directory READ or SEARCH — Yes → 0
No

eUID = 0 — Yes → 0
No

eUID = OWNER & Requested = Allowed Access — Yes → 0; No
Not OWNER

eUID in ACL & Requested = Allowed Access — Yes → 0; No
Not in ACL

eGID/sGID = GROUP & Requested = Allowed Access — Yes → 0
Not Auth -or- Not GROUP

eGID/sGID in ACL & Requested = Allowed Access — Yes → 0; No
Not in ACL

-&- GROUP but Insuffient Auth

-&- Not GROUP

UNIXPRIV RESTRICTED.FILESYS.ACCESS
User RESTRICTED & Access Allowed < READ — Yes
Not RESTRICTED -or- Profile Not Defined -or- Has READ

Requested = Allowed OTHER Access — Yes → 0; No

UNIXPRIV SUPERUSER.FILESYS.ACLOVERRIDE
Requested = Allowed Access — Yes → 0; No → 8
Not Defined

UNIXPRIV SUPERUSER.FILESYS
Requested = Allowed Access — Yes → 0; No -or- Not Defined → 8

UNIXPRIV Class

- Checked after other authorities - AUDITOR, eUID(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