

z/OS V1R13

RACF: UNIX file system access

Session objectives

- Introduce new file system access control
- Show RACF setup

Overview

- Problem Statement / Need Addressed
 - Ability for the RACF administrator to control access to UNIX System Services mounted file systems without needing to use UNIX semantics.
- Solution
 - Implement a new FASTAUTH call in ck_access that checks user's permission to file system profile in a new class (FSACCESS).
 - Supported for zFS and NFS.
- Benefit / Value
 - Provides a coarse-grained file system access control for use by the RACF administrator.
 - Does not require UNIX command expertise (setfac) for administration.
 - Provides compliance and audit verification for RACF-centric customers.

Usage and invocation

- Mount point traversal triggers one-time check to the container
 - Access failure prevents any operation within file system, regardless of permission bits, acls, file ownership, or UID(0)
 - Successful access (or no covering profile) simply continues with existing UNIX-style checks which may or may not allow access to file system object
 - RACF AUDITOR attribute bypasses FSACCESS check
- UPDATE access required to (new) FSACCESS class resource name which equals the containing data set name
 - Only performed in FSACCESS class is active

Usage and invocation

- RACF setup:

```
RDEFINE FSACCESS IBMUSER.ZFS.SRC UACC(NONE)

PERMIT IBMUSER.ZFS.SRC CLASS(FSACCESS) ID(IBMUSER) ACCESS(UPDATE)

SETROPTS CLASSACT(FSACCESS)

SETROPTS RACLIST(FSACCESS)
```

Interactions and dependencies

- Exploiters
 - UNIX System Services at APAR level OA35970.

Migration and coexistence considerations

- New function available in Releases 12 and 13.
- New function enabled when FSACCESS class is activated.

Installation

- The following set of APARs are required:
 - OA35973 RACF
 - OA35974 SAF
 - OA35970 UNIX

Session summary

- RACF administrator can now control zFS and NFS file system access by managing FSACCESS profile permissions

Appendix - References

- SA22-7691 Security Server RACF Callable Services
- SA22-7684 Security Server RACF Auditor's Guide
- GA22-7800 UNIX System Services Planning