RSH CONSULTING

# RACF SETROPTS

## KOIRUG - October 2018

# RSH Consulting - Robert S. Hansel

RSH Consulting, Inc. is an IT security professional services firm 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. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050

Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc. He began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He is a leading expert in securing z/OS Unix using RACF. Mr. Hansel has created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel
- http://twitter.com/RSH_RACF

# SETROPTS

- SETROPTS - SET RACF OPTIONS
  - Defines system-wide RACF security and auditing options
  - Options reside in the RACF database Inventory Control Block (ICB)
- TSO Command - SETROPTS option-operand(s) | LIST
  - LIST - display options
  - Use of command always logged
- Authority to execute
  - SPECIAL — List and set security options only
  - AUDITOR — List all options and set auditing options
  - ROAUDIT — List all options
  - Group-AUDITOR — List all options
  - OPERCMDS *racf-subsystem*.SETROPTS — Execute commands via the console
    - READ — LIST
    - UPDATE — All other operands
- Setting options on a particular resource class (e.g., TCICSTRN) affects all classes with the same POSIT value
- ✓ - RSH recommended option settings

# SETROPTS LIST

```
SETROPTS LIST
ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC) TERMINAL(READ) SAUDIT CMDVIOL OPERAUDIT
STATISTICS = DATASET GTERMINL TERMINAL
AUDIT CLASSES = DATASET USER GROUP DASDVOL GDASDVOL GTERMINL TERMINAL
ACTIVE CLASSES = DATASET USER GROUP ACCTNUM ACICSPCT APPL BCICSPCT CCICSCMD
                 CDT CONSOLE DASDVOL DCICSDCT DSNR ECICSDCT FACILITY FCICSFCT
                 FSSEC GCICSTRN GDASDVOL GSDSF GTERMINL HCICSFCT JCICSJCT
                 KCICSJCT LOGSTRM MCICSPPT NCICSPPT OPERCMDS PCICSPSB
                 PMBR PROGRAM PROPCNTL QCICSPSB RACFVARS RRSFDATA RVARSMBR
                 SCICSTST SDSF SERVER STARTED SURROGAT TCICSTRN TEMPDSN
                 TERMINAL TSOAUTH TSOPROC UCICSTST UNIXPRIV VCICSCMD
GENERIC PROFILE CLASSES = DATASET DASDVOL FACILITY PROGRAM TCICSTRN TERMINAL
GENERIC COMMAND CLASSES = DATASET ACCTNUM DASDVOL FACILITY FIELD PERFGRP
                          PROGRAM T@TESTRN TCICSTRN TERMINAL TSOAUTH TSOPROC
GENLIST CLASSES = NONE
GLOBAL CHECKING CLASSES = DATASET FACILITY TERMINAL
SETR RACLIST CLASSES = APPL CDT DSNR FACILITY STARTED TSOAUTH TSOPROC
GLOBAL=YES RACLIST ONLY = TCICSTRN
LOGOPTIONS "ALWAYS" CLASSES =  SURROGAT
LOGOPTIONS "NEVER" CLASSES =  NONE
LOGOPTIONS "SUCCESSES" CLASSES =  NONE
LOGOPTIONS "FAILURES" CLASSES =  FACILITY
LOGOPTIONS "DEFAULT" CLASSES = DATASET ACCTNUM ACICSPCT ALCSAUTH APPCLU
                               ... VTAMAPPL VXMBR WIMS WRITER
AUTOMATIC DATASET PROTECTION IS IN EFFECT
ENHANCED GENERIC NAMING IS IN EFFECT
REAL DATA SET NAMES OPTIONS IS INACTIVE
JES-BATCHALLRACF OPTION IS INACTIVE
JES-XBMALLRACF OPTION IS INACTIVE
JES-EARLYVERIFY OPTION IS INACTIVE
PROTECT-ALL OPTION IS NOT IN EFFECT
TAPE DATA SET PROTECTION IS INACTIVE
SECURITY RETENTION PERIOD IN EFFECT IS  9999 DAYS.
ERASE-ON-SCRATCH IS INACTIVE
SINGLE LEVEL NAME PREFIX IS LVL1X
LIST OF GROUPS ACCESS CHECKING IS ACTIVE.
INACTIVE USERIDS ARE NOT BEING AUTOMATICALLY REVOKED.
NO DATA SET MODELLING IS BEING DONE.
```

# SETROPTS LIST

```
PASSWORD PROCESSING OPTIONS
  THE ACTIVE PASSWORD ENCRYPTION ALGORITHM IS KDFAES
  PASSWORD CHANGE INTERVAL IS   45 DAYS.
  PASSWORD MINIMUM CHANGE INTERVAL IS 3 DAYS.
  MIXED CASE PASSWORD SUPPORT IS NOT IN EFFECT
  SPECIAL CHARACTERS ARE ALLOWED.
  10 GENERATIONS OF PREVIOUS PASSWORDS BEING MAINTAINED.
  AFTER   4 CONSECUTIVE UNSUCCESSFUL PASSWORD ATTEMPTS,
      A USERID WILL BE REVOKED.
  PASSWORD EXPIRATION WARNING LEVEL IS   5 DAYS.
  INSTALLATION PASSWORD SYNTAX RULES:
    RULE 1  LENGTH(5:8)   ********
    RULE 2  LENGTH(6:8)   LLLLLLLL
   LEGEND:
    A-ALPHA C-CONSONANT L-ALPHANUM N-NUMERIC V-VOWEL W-NOVOWEL *-ANYTHING
    c-MIXED CONSONANT m-MIXED NUMERIC v-MIXED VOWEL $-NATIONAL s-SPECIAL
    x-MIXEDALL
INSTALLATION DEFINED RVARY PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.
DEFAULT RVARY PASSWORD IS IN EFFECT FOR THE STATUS FUNCTION.
SECLEVELAUDIT IS INACTIVE
SECLABEL AUDIT IS NOT IN EFFECT
SECLABEL CONTROL IS NOT IN EFFECT
GENERIC OWNER ONLY IS NOT IN EFFECT
COMPATIBILITY MODE IS NOT IN EFFECT
MULTI-LEVEL QUIET IS NOT IN EFFECT
MULTI-LEVEL STABLE IS NOT IN EFFECT
NO WRITE-DOWN IS NOT IN EFFECT
MULTI-LEVEL ACTIVE IS NOT IN EFFECT
CATALOGUED DATA SETS ONLY, IS NOT IN EFFECT
USER-ID FOR JES NJEUSERID IS : ????????
USER-ID FOR JES UNDEFINEDUSER IS : ++++++++
PARTNER LU-VERIFICATION SESSIONKEY INTERVAL DEFAULT IS   30 DAYS.
APPLAUDIT IS IN EFFECT
ADDCREATOR IS NOT IN EFFECT
KERBLVL =     0
MULTI-LEVEL  FILE SYSTEM IS NOT IN EFFECT
MULTI-LEVEL  INTERPROCESS COMMUNICATIONS IS NOT IN EFFECT
MULTI-LEVEL  NAME HIDING  IS NOT IN EFFECT
SECURITY LABEL BY SYSTEM IS NOT IN EFFECT
PRIMARY LANGUAGE DEFAULT : ENU / ENGLISH
SECONDARY LANGUAGE DEFAULT : ENU / ENGLISH
```

# SETROPTS

- INITSTATS ✓ | NOINITSTATS
  - Specifies whether user logon statistics are recorded
  - Required with INACTIVE or PASSWORD( REVOKE | HISTORY | WARNING )

- WHEN( PROGRAM ) ✓ | NOWHEN( PROGRAM ) )  [ REFRESH ]
  - Activates PROGRAM Class
  - Enables protection of program modules and use of WHEN(PROGRAM(*program*)) in conditional access permissions for dataset and SERVAUTH profiles
  - Needed to ensure a 'clean' program environment for Unix Daemons
  - SETROPTS displays the mode (i.e., protection level)
    - Default is BASIC
    - Mode can be changed via following profile

      FACILITY IRR.PGMSECURITY APPLDATA( BASIC | ENHANCED | *anything* )

      *anything* - activates ENHANCED-WARNING

# SETROPTS

- TERMINAL( READ ✓ | NONE )
  - Specifies the universal access (UACC) for undefined terminals
  - Only appears if TERMINAL Class is active
  - If set to NONE and no profiles allow access, all terminal logons are denied
- SAUDIT ✓ | NOSAUDIT
  - Specifies whether RACF command execution and resource access using SPECIAL authority is logged
- CMDVIOL ✓ | NOCMDVIOL
  - Specifies whether RACF command violations are logged
- OPERAUDIT ✓ | NOOPERAUDIT
  - Specifies whether resource access and RACF command execution using OPERATIONS authority is logged

# SETROPTS

- STATISTICS( *class* ... | * ) | NOSTATISTICS( *class* ... | * ✓ )
  - Causes access counts to be incremented in discrete profiles
  - Ignored for RACLISTed classes
  - Statistics not incremented for GLOBAL granted access
  - Negative performance impact

- AUDIT( *class* ... | * ✓ ) | NOAUDIT( *class* ... | * )
  - Activates auditing of profile changes for the specified class
  - Ensures auditing of RACF commands entered using an authority other than SPECIAL and OPERATIONS (addressed by SAUDIT and OPERAUDIT)
  - For certain classes, also logs:
    - DATASET creations and deletions of datasets
    - FSOBJ creations and deletions of USS file system objects
    - IPCOBJ creations and deletions of USS objects (e.g., semaphores)
    - PROCESS dubbing and undubbing of a process
    - USER all password changes, even those made during logon and auto-assignment of OMVS segments by BPX.UNIQUE.USER
    - GROUP auto-assignment of OMVS segments by BPX.UNIQUE.USER

# SETROPTS

- CLASSACT( *class ...* | * ) | NOCLASSACT( *class ...* | * )
  - Activates profiles in the specified class
  - Beware activating classes defined with DFTRETC=8 in the CDT; access will be denied when no profile is defined (e.g., JESINPUT)
  - ✓ Activating TEMPDSN turns on protection for temporary datasets
  - ✓ Activating FSSEC causes Unix Extended Access Control Lists to take affect
  - Activating classes PROGRAM and GLOBAL have no effect
- GENERIC( *class ...* | * ) | NOGENERIC( *class ...* | * ) [ REFRESH ]
  - Activates generic profiles in the specified class
  - Also activates GENCMD if not already active
  - REFRESH causes all in-memory address space generic lists and profiles to be discarded
- GENCMD( *class ...* | * ) | NOGENCMD( *class ...* | * )
  - Enables creation of generic profiles in the specified class
  - Be sure to activate GENCMD before attempted to create profiles with generic characters; otherwise, they will be created as discretes

# SETROPTS

- GENLIST( *class* ... ) | NOGENLIST( *class* ... ✓ )
  - Stores generic profiles in ECSA for authorization checking
  - Most appropriate for VM related classes (e.g., VMMDISK )
  - To GENLIST, class must be defined with GENLIST=ALLOWED in CDT
  - To refresh, issue SETROPTS GENERIC(*class*) REFRESH
- GLOBAL( *class* ... | * ) | NOGLOBAL( *class* ... | * ) [ REFRESH ]
  - Activates global access checking for specified class
  - Profile matching class name needs to be defined in the GLOBAL class
- RACLIST( *class* ... ) | NORACLIST( *class* ... ) [ REFRESH ]
  - Stores all profiles in a data space for authorization checking
  - To SETROPTS RACLIST, class must be defined with RACLIST=ALLOWED in CDT
  - Certain products automatically RACLIST classes (e.g., CICS)
    - Appear in SETROPTS LIST under "**`GLOBAL=YES RACLIST ONLY =`**"
  - Required to exploit grouping classes (e.g., DASDVOL/GDASDVOL)
  - Required for some classes (e.g., STARTED ) - RACLREQ=YES in CDT

# SETROPTS

- LOGOPTIONS( *level*( *class* … ) … )
  - Specifies the level of access auditing enforced for a given class
  - Auditing Levels
    - ALWAYS Log all accesses, even if no profile exists (✓ FSSEC SURROGAT )
    - NEVER Do not log any accesses
    - SUCCESSES Log all successful accesses
    - FAILURES ✓ Log all violations
    - DEFAULT Log according to the profile audit settings
  - SUCCESSES and FAILURES augment resource profile audit settings
  - ALWAYS and NEVER override resource profile audit settings
  - ALWAYS logs access by TRUSTED Started Tasks
  - NEVER does not suppress user UAUDIT logging
  - SUCCESSES and ALWAYS
    - Will not log access granted via GLOBAL or where the RACROUTE caller specifed LOG=NONE
    - Does not govern logging for RACROUTE REQUEST=FASTAUTH - only profile log options apply
  - FAILURES( PROCESS PROCACT IPCOBJ ) ✓ activates logging of violations for related Unix events

# SETROPTS

- ADSP | NOADSP ✓
  - Will automatically create a discrete dataset profile when a dataset is created for any user whose ID also has the ADSP attribute
  - To create a discrete group dataset profile, the user must be connected to the group with at least CREATE authority

- EGN ✓ | NOEGN
  - Enables use of enhanced generic naming for datasets, including the ** generic character
  - When first enabled, profiles formerly ending in * display as *.**

- REALDSN | NOREALDSN
  - Applicable when the Naming Conventions Table ICHNCV00 is used
  - Causes RACF messages and SMF records to display the true dataset name rather than the converted name

# SETROPTS

- JES ( BATCHALLRACF ✓ | NOBATCHALLRACF )
  - Requires all batch jobs to have an associated USERID
  - RJE and NJE jobs must have RACF IDs

- JES ( XBMALLRACF ✓ | NOXBMALLRACF ) (JES2 only)
  - Requires all batch jobs run under an Execution Batch Monitor to have an associated USERID

- JES ( EARLYVERIFY | NOEARLYVERIFY ✓ )
  - Requires JES to verify batch job users (ID and password) at the time of submission rather than waiting until execution
  - Obsolete legacy option - only applies to pre-3.1.3 versions of JES (circa 1990)
  - Newer releases of JES behave as if EARLYVERIFY is active

# SETROPTS

- PROTECTALL( FAILURES ✓ | WARNING ) | NOPROTECTALL
  - Requires all datasets to be 'defined' to RACF to gain access
  - Only applies to datasets
  - Mode Options
    - WARNING Allows and logs access to undefined datasets
    - FAILURES Denies access to undefined datasets
  - Privileged/Trusted Started Tasks and System-SPECIAL users can access undefined datasets

- TAPEDSN | NOTAPEDSN
  - Activates DATASET profile protection for tape datasets
  - ✓ - Any of the following options
    - RACF SETROPTS TAPEDSN
    - z/OS PARMLIB(DEVSUPxx) parameter TAPEAUTHDSN=YES
    - CA-1 configuration option OCEOV is set to YES

- RETPD( *nnnnn* | 0 ✓ )
  - Default security retention period in days for tape dataset profiles
  - *nnnnn* values can be 0 - 65533 or 99999 (never)
  - Typically handled by tape management system

# SETROPTS

- ERASE( ALL | SECLEVEL(*seclevel*) | NOSECLEVEL ) | NOERASE
  - ✓ ALL or NOSECLEVEL
  - Enables overwriting of datasets upon deletion to protect against scavenging of residual data
  - NOSECLEVEL - uses ERASE option setting on dataset profile
  - Applies to DASD datasets only
  - Significant performance improvements have been made in recent z/OS releases
  - Alternative - Pervasive Encryption

- PREFIX( *prefix* ✓ ) | NOPREFIX
  - Activates RACF protection for single-qualifier datasets
  - Appends pseudo-HLQ prefix to the dataset name before checking authorization
  - Prefix should match name of predefined group
    - ✓ Create a unique, standalone group to be used solely for the prefix
  - Enables protection via normal dataset profiles (e.g., *prefix*.** )
  - With NOPREFIX and EGN active, profiles like HLQ.** will protect single-level named datasets whose name matches the HLQ

# SETROPTS

- GRPLIST ✓ | NOGRPLIST
  - Determines whether all a user's connected groups are used for access authorization -or- just the user's current logon group
  - When authorization checking uses all a user's groups (GRPLIST), access authority is based on highest level of access allowed by any of the groups

- INACTIVE( *nnn* ) | NOINACTIVE (✓* <= 90)
  - Specifies the number of days ( up to 255 ) that a USERID can remain unused and still be considered active
  - First logon attempt after limit has been crossed results in the ID being revoked
  - PROTECTED IDs are exempt from inactive checking
  - Alternative - automated process to identify and eliminated IDs of terminated users
  - * - Can be problematic in an RRSF environment
    - Logon statistics are only maintained on the system(s) where the user logs on
    - Users who logon infrequently to certain systems can get revoked on all systems if the inactive threshold is crossed on any of those other systems

# SETROPTS

- MODEL( *options* ) | NOMODEL
  - Options
    - GDG | NOGDG ✓
      - If a MODEL profile exists that matches the GDG base name (e.g., PAY.BACKUP), RACF will use this profile to govern access to all RACF-indicated the GDG generations (e.g., PAY.BACKUP.G0982V00)
      - The GDG base itself can be protected with its own discrete profile
    - GROUP | NOGROUP
      - If a group profile specifies MODEL(*model-profile-name*) and the corresponding model profile exists, when a new group dataset profile is created, RACF automatically copies the UACC and access list from the model into the new profile; specifying FROM(*profile*) overrides the model
    - USER | NOUSER
      - If a user profile specifies MODEL(*model-profile-name*) and the corresponding model profile exists, when a new user dataset profile is created, RACF automatically copies the UACC and access list from the model into the new profile; specifying FROM(*profile*) overrides the model
  - A non-generic profile is defined as a model by specifying the MODEL operand on the ADDSD command
  - The profile assigned as the MODEL for a user or group must have an HLQ matching the user or group and either be a discrete or a MODEL profile
  - When assigning the MODEL profile, do not enclose it in quotes or include the HLQ

# SETROPTS

- PASSWORD( *suboperand …* )
  - ALGORITHM(KDFAES) ✓ | NOALGORITHM
    - Directs RACF to use the KDFAES algorithm to encrypt new passwords and password phrases instead of DES
  - INTERVAL( *nnn* | 30 ) ( ✓ <= 90)
    - Number of days ( 1 to 254 ) before user must change password
  - MINCHANGE( *nnn* | 0 ) ( ✓ => 1)
    - Number of days ( 0 to 254 ) before user can change password again
  - MIXEDCASE ✓ | NOMIXEDCASE
    - Specifies whether passwords are to be mixed case
  - SPECIALCHAR ✓ | NOSPECIALCHAR
    - Enables use of special characters in passwords, including: . < + | & ! * - % _ > ? : =
  - HISTORY( *nn* ) | NOHISTORY ( ✓ => 12)
    - Number of previous passwords ( up to 32 ) that cannot be reused
  - REVOKE( *nnn* ) | NOREVOKE ( ✓ <= 5)
    - Number of consecutive incorrect password attempts ( up to 255 ) before USERID is revoked
  - WARNING( *nnn* ) | NOWARNING ( ✓ <= 5)
    - Specifies the number of days ( up to 255 ) before a password expires to begin issuing an upcoming expiration notice to the user
    - Warnings are only displayed by applications designed to process this setting (e.g., TSO)

# SETROPTS

- PASSWORD( suboperand … ) - continued
  - RULE*n*( LENGTH( *m1* [ :*m2* ] ) [ *content-keyword*(*position*) … ] ) | NORULE*n* | NORULES
    - Specifies password syntax for new user-selected passwords
    - Up to 8 separate rules - a password must match one rule for acceptance
    - Does not apply to ADDUSER or ALTUSER PASSWORD(*password*) unless NOEXPIRED is specified
    - Length - 'm1' minimum to (optional) 'm2' maximum (e.g., 6 or 5:7 ) - from 1 to 8
    - Content-Keywords ( Defaults to ANYTHING - * )
      - ALPHA ALPHANUM VOWEL NOVOWEL CONSONANT NUMERIC NATIONAL SPECIAL
      - MIXED CONSONANT MIXED NUMERIC MIXED VOWEL (MIXEDCASE options)
      - MIXEDALL ✓
    - Content position - position number or range (e.g., 3 or 5:8)
    - Alternatives (use ALPHANUM instead of MIXEDALL if special characters cannot be used)

```
RULE1( LENGTH(7:8) )
-----------------------------------------------------------------------------------------------------------------------
RULE1( LENGTH(7:8) MIXEDALL(7:8) )
-----------------------------------------------------------------------------------------------------------------------
RULE1( LENGTH(7) ALPHA(1,7) MIXEDALL(2:6) )
RULE2( LENGTH(8) ALPHA(1,8) MIXEDALL(2:7) )
-----------------------------------------------------------------------------------------------------------------------
RULE1( LENGTH(8) ALPHANUM(8) )              <- Most common rule
```

# SETROPTS

- RVARYPW( SWITCH( *password* ) ✓ | STATUS( *password* ) ✓ )
  - Sets console password that must be entered to execute RVARY
  - Default password is YES
- SECLEVELAUDIT( *seclevel* ) | NOSECLEVELAUDIT
  - Activates auditing of all access attempts to resources at or above a specified security level
  - The specified *seclevel* must be defined in a SECDATA SECLEVEL profile
- SECLABELAUDIT | NOSECLABELAUDIT
  - Specified that SECLABEL profile auditing options are to be used in addition to the resource profile auditing options in logging access
- SECLABELCONTROL | NOSECLABELCONTROL
  - Restricts who can change the SECLABEL on a profile to only those users with System and Group SPECIAL

# SETROPTS

- GENERICOWNER | ENHANCEDGENERICOWNER ✓ | NOGENERICOWNER
  - Applies to users with CLAUTH for general resource class
  - Restricts creation of more specific, undercutting profiles and (enhanced) members
  - To create a more specific profile, user must:
    - Have System-SPECIAL
    - Be the Owner of the existing profile
    - Have Group-SPECIAL over the group owning the existing profile
- COMPATMODE | NOCOMPATMODE
  - Allows users and jobs not using SECLABELs to be on a system enforcing SECLABELs (using RACROUTE pre-1.9 keywords)
- MLQUIET | NOMLQUIET
  - Allows only Started Tasks, console operators, or users with SPECIAL attribute to logon or access resources
- MLSTABLE | NOMLSTABLE
  - Prevents alter of SECLABELs unless system is in MLQUIET mode

# SETROPTS

- MLS( FAILURES | WARNING ) | NOMLS
  - Prevents users from de-classifying data
- MLACTIVE( FAILURES | WARNING ) | NOMLACTIVE
  - Requires SECLABELs for all work entering system and on USER, DATASET and classes requiring SECLABELs ( SLBLREQ= in CDT )
- CATDSNS( FAILURES | WARNING ) | NOCATDSNS
  - Requires all DFP-managed datasets to be catalogued in order to access them
  - Uncataloged datasets are only accessible to users with:
    - Privileged/Trusted Started Task or SPECIAL attribute
    - Access to FACILITY Profile 'ICHUNCAT.dsname'
    - Access to FACILITY Profile 'ICHUSERCAT' when using a private catalog (JOBCAT or STEPCAT)
    - Access authority to datasets protected by Discrete Profiles
- JES ( NJEUSERID( *non-existing-userid* | ???????? ✓ ) )
  - Designates the owner assigned to NJE SYSOUT and jobs that arrive through the network without an RTOKEN or UTOKEN

# SETROPTS

- JES ( UNDEFINEDUSER( *non-existing-userid* | ++++++++ ✓ ) )
  - Designates the owner assigned to local jobs and Started Tasks that enter the system without a user ID (e.g., RJE)

- SESSIONINTERVAL( *nnnnn* | 30 ) | NOSESSIONINTERVAL
  - Sets the maximum value in minutes ( up to 32767 ) that can be specified for RDEFINE or RALTER session key expiration intervals on APPCLU profiles
  - NOSESSIONINTERVAL sets the value to 0 ( no limit )

- APPLAUDIT ✓ | NOAPPLAUDIT
  - Enables user verification auditing for APPC transactions
  - AUDIT settings on associated APPL class profiles govern SMF record generation

- ADDCREATOR | NOADDCREATOR ✓
  - Determines whether the USERID of the creator of a new dataset or general resource profile is automatically placed on the access list with ALTER access when the profile is created

# SETROPTS

- KERBLVL( 0 | 1 )
  - Specifies whether DES alone (0) or DES, DES3, and DESD (1) can be used in creating Kerberos keys
  - Obsolete option - ignored beginning with z/OS 1.9
- MLFSOBJ( ACTIVE | INACTIVE )
  - Specifies whether security labels are required for Unix files and directories
- MLIPCOBJ( ACTIVE | INACTIVE )
  - Specifies whether security labels are required for Unix interprocess communication
- MLNAMES | NOMLNAMES
  - Specifies whether users are restricted to viewing only the names of datasets and Unix files and directories that their security labels would allow them to read
- LANGUAGE(PRIMARY(*language*) SECONDARY(*language*) )
  - Sets default for system-wide national languages
  - Default is ENU (U.S. English)