

SETROPTS

Cincinnati / Tri-State RACF Users Group - October 23, 2003



Robert S. Hansel

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

SETROPTS

SETROPTS - SET RACF OPTIONS

- Defines system-wide RACF security & auditing options
- Options reside in RACF Database ICB (Inventory Control Block)

TSO Command - SETROPTS *option-operand(s)* | LIST

- LIST - display options
- Use of command always logged

Authority to execute

- SPECIAL List & set security options only
- AUDITOR List all options & set auditing options

Setting options on a particular resource class (e.g., TCICSTRN) effects all classes with the same POSIT value

✓ - RSH recommended option settings

SETROPTS

SETROPTS LIST

```
ATTRIBUTES = INITSTATS WHEN(PROGRAM -- BASIC) TERMINAL(READ) SAUDIT CMDVIOL OPERAUDIT
STATISTICS = DATASET TERMINAL
AUDIT CLASSES = DATASET USER GROUP DASDVOL GDASDVOL TERMINAL GTERMINL
ACTIVE CLASSES = DATASET USER GROUP DASDVOL GDASDVOL TERMINAL GTERMINL APPL
                  TCICSTRN GCICSTRN GLOBAL GMBR DSNR FACILITY SCDMBR SECDATA
                  FCICSFCT HCICSFCT JCICSJCT KCICSJCT DCICSDCT ECICSDCT SCICSTST
                  UCICSTST MCICSPPT NCICSPPT ACICSPCT BCICSPCT PMBR PROGRAM FIELD
                  TSOAUTH TSOPROC ACCTNUM PERFGRP $LMRKTMR T@TESTRN G@TESTRN
GENERIC PROFILE CLASSES = DATASET DASDVOL TERMINAL TCICSTRN FACILITY PROGRAM
GENERIC COMMAND CLASSES = DATASET DASDVOL TCICSTRN FACILITY PROGRAM FIELD
                          TSOAUTH TSOPROC ACCTNUM PERFGRP T@TESTRN
GENLIST CLASSES = NONE
GLOBAL CHECKING CLASSES = DATASET DASDVOL FACILITY
SETR RACLIST CLASSES = APPL DSNR FIELD TSOAUTH TSOPROC ACCTNUM PERFGRP
GLOBAL=YES RACLIST ONLY = TCICSTRN
LOGOPTIONS "ALWAYS" CLASSES = NONE
LOGOPTIONS "NEVER" CLASSES = NONE
LOGOPTIONS "SUCCESSES" CLASSES = NONE
LOGOPTIONS "FAILURES" CLASSES = NONE
LOGOPTIONS "DEFAULT" CLASSES = DATASET RVARSMBR RACFVARS DASDVOL GDASDVOL
                                ... G@TESTRN RMD$FORM
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

PASSWORD PROCESSING OPTIONS

PASSWORD CHANGE INTERVAL IS 45 DAYS.
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-ALPHANUMERIC N-NUMERIC V-VOWEL W-NOVOWEL *-ANYTHING

INSTALLATION DEFINED RVARV PASSWORD IS IN EFFECT FOR THE SWITCH FUNCTION.

DEFAULT RVARV 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

MULTI-LEVEL SECURE 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

EIM REGISTRY = NONE

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)

- Activates PROGRAM Class
- Enables protection of program modules & use of conditional access to datasets via a specific program
- (z/OS 1.4) Mode set via following profile

FACILITY IRR.PGMSECURITY APPLDATA(BASIC | ENHANCED)

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 logons denied

SAUDIT ✓ | NOSAUDIT

- Specifies whether RACF commands issued using SPECIAL authority are logged

CMDVIOL ✓ | NOCMDVIOL

- Specifies whether RACF command violations are logged

OPERAUDIT ✓ | NOOPERAUDIT

- Specifies whether RACF commands issued & resources accessed using OPERATIONS authority are 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 (addressed by SAUDIT)
- Also logs RACFDEFs (Defines) for new resources, including:
 - 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

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)
- Beware activating TEMPDSN - effects temporary dataset access

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 lists to be renewed

GENCMD(*class ... | **) | NOGENCMD(*class ... | **)

- Enables creation of generic profiles in the specified class
- Be sure to active GENCMD before attempted to create profiles with generic characters; otherwise, they will be created as discretetes

SETROPTS

GENLIST(*class* ...) | NOGENLIST(*class* ... ✓) [REFRESH]

- Stores generic profiles in ECSA for authorization checking
- Most appropriate for VM related classes (e.g., VMMDISK)
- To GENLIST, must be defined with GENLIST=ALLOWED in CDT

GLOBAL(*class* ... | *) | NOGLOBAL(*class* ... | *) [REFRESH]

- Activates global access checking for specified class
- Profile matching class name needs to be defined in GLOBAL class

RACLIST(*class* ...) | NORACLIST(*class* ...) [REFRESH]

- Stores all profiles in a data space for authorization checking
- To RACLIST, must be defined with RACLIST=ALLOWED in CDT
- Certain products automatically RACLIST classes (e.g., CICS)
- 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
 - 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 profile audit settings
- ALWAYS and NEVER override profile audit settings
- ALWAYS logs TRUSTED Started Tasks (and everything else)
- Enables logging of Unix System Services events
 - DIRSRCH DIRACC FSOBJ FSSEC PROCESS PROCACT IPCOBJ

SETROPTS

ADSP | NOADSP ✓

- Will automatically create a discrete dataset profile when a dataset is first created for any user whose ID also has the ADSP attribute

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 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
- Legacy option - only applies to pre-3.1.3 versions of JES
- 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 & System-SPECIAL users can access undefined datasets

SETR TAPEDSN ✓ | NOTAPEDSN

- Activates DATASET profile protection for tape datasets

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

- 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
- Newer DASD devices eliminate performance concerns

PREFIX(*prefix* ✓) | NOPREFIX

- Activates RACF protection for single-qualifier datasets
- Appends pseudo-HLQ prefix to the dataset name before checking authorization
- Prefix should match existing USERID or Group
- Enables protection via normal dataset profiles (e.g., *prefix.***)
- With **NOPREFIX** & **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 (Recommend <= 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

SETROPTS

MODEL(*options*) | NOMODEL ✓

- Identifies whether discrete dataset profile modeling is in effect
- Options
 - GDG | NOGDG
 - ◆ Allows each member of a GDG to use a common profile
 - ◆ Discrete profile defined for GDG base is used to protect all members
 - GROUP | NOGROUP
 - ◆ For new group datasets, RACF uses model profile associated with the group to create new discrete profiles
 - ◆ Group profile must have MODEL(*model-profile-name*)
 - USER | NOUSER
 - ◆ For new user datasets, RACF uses model profile associated with the USERID to create new discrete profiles
 - ◆ User profile must have MODEL(*model-profile-name*)
- Model dataset profiles are created using ADDSD MODEL operand

SETROPTS

PASSWORD(*suboperand ...*)

- **INTERVAL(*nnn* | 30) | NOINTERVAL** (✓ ≤ 90)
 - Number of days (up to 254) before user must change password
- **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 revoke
- **WARNING(*nnn*) | NOWARNING** (✓ ≤ 5)
 - Specifies the number of days (up to 255) before a password expires to beginning issuing an upcoming expiration notice to the user
 - Only applies to applications that recognize it (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 for acceptance
 - Does not apply to ADDUSER or ALTUSER PASSWORD(*password*), unless NOEXPIRED is also specified
 - Length - 'm1' minimum to (optional) 'm2' maximum (e.g., 6 or 5:7) - up to 8
 - Content-Keywords (Defaults to ANYTHING - *)
ALPHA ALPHANUM VOWEL NOVOWEL CONSONANT NUMERIC
 - Content position - position number or range (e.g., 3 or 5:8)
 - Alternative recommendations ✓

RULE1(LENGTH(6:8))

RULE1(LENGTH(6:8) ALPHANUM(6:8))

RULE1(LENGTH(6) ALPHA(1,6) ALPHANUM(2:5))

RULE2(LENGTH(7) ALPHA(1,7) ALPHANUM(2:6))

RULE3(LENGTH(8) ALPHA(1,8) ALPHANUM(2:7))

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
- Must be defined in 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 ✓ | NOGENERICOWNER

- Applies to users with CLAUTH for general resource class
- Restricts creation of more specific, undercutting profiles
- 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

SETROPTS

COMPATMODE | NOCOMPATMODE

- Allows users & 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

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)

SETROPTS

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 authority to FACILITY Profile 'ICHUNCAT.dsname'
 - Access authority to FACILITY Profile 'ICHUSERCAT' when using a private catalog (JOB CAT or STEP CAT)
 - Access authority to datasets protected by Discrete Profiles

JES (NJEUSERID(*non-existing-userid* | ????????? ✓))

- Defines the owner to be associated with NJE SYSOUT or jobs that arrive through the network without an RTOKEN or UTOKEN

JES (UNDEFINEDUSER(*non-existing-userid* | +++++ ✓))

- Defines the owner to be associated with local jobs that enter the system without a user ID (e.g., RJE)

SETROPTS

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 auditing of APPC transactions
- Depends on AUDIT settings on associated APPL class profiles

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

EIMREGISTRY | NOEIMREGISTRY

- Activates the RACF registry name for Enterprise Identity Mapping (EIM) services
- Registry name is defined in FACILITY IRR.PROXY.DEFAULTS

LANGUAGE(PRIMARY(*language*) SECONDARY(*language*))

- Sets default for system-wide languages
- Default is ENU (U.S. English)