Interpreting Output from the RACF SETR LIST Command

SETR is the command to set options for RACF, IBM's strategic software for mainframe computer security. The SETR LIST command is the version which lists the current setting of all these options. This session will show you how to interpret all these settings. (You may have an actual printout to use along with the presentation.) You will learn recommended values for these settings, as well as the reasons behind these recommendations.

This is the handout for a stand-up presentation by Stu Henderson. Its content is offered on an "as-is", at-your-own-risk, test-it-yourself-first, basis. The opinions expressed are his, and may not be suitable for your installation. This article has been updated May, 2016.

Please direct questions and comments to him at (301) 229-7187 or stu@stuhenderson.com.

- LET'S EXAMINE A SAMPLE SETR LISTING IN 5 PARTS:

    1) THE ATTRIBUTES

    2) RESOURCE CLASS SWITCHES

    3) DATASET AND USERID OPTIONS

    4) PASSWORD OPTIONS

    5) MISCELLANEOUS OPTIONS

1) THE ATTRIBUTES

ATTRIBUTE	MEANING
INITSTATS	SAYS TO TIME-STAMP THE USER RECORD AT TERMINAL SIGN-ON AND AT START OF A BATCH JOB
WHEN (PROGRAM)	ACTIVATES THE PROGRAM RESOURCE CLASS, CHECKING TO SEE WHO IS PERMITTED TO EXECUTE DEFINED PROGRAMS
TERMINAL UACC	DEFAULT TERMINAL ACCESS (READ OR NONE) IF NO MATCHING TERMINAL RESOURCE RULE. (SHOWS ONLY IF TERMINAL CLASS IS ACTIVE)
SAUDIT	SAYS TO LOG EVERY TIME A USER DOES SOMETHING HE OR SHE IS ONLY ABLE TO DO BECAUSE OF THE **SPECIAL** USER ATTRIBUTE
CMDVIOL	SAYS TO LOG EVERY COMMAND VIOLATION
OPERAUDIT	SAYS TO LOG EVERY TIME A USER DOES SOMETHING HE OR SHE IS ONLY ABLE TO DO BECAUSE OF THE **OPERATIONS** USER ATTRIBUTE

RECOMMENDATIONS FOR THE ATTRIBUTE SWITCHES:

LEAVE **TERMINAL** SET AT READ

FOR THE OTHERS,

TURN THEM ALL ON AND LEAVE THEM ON

2) RESOURCE CLASS SWITCHES

THESE SWITCHES DESCRIBE SETTINGS FOR EACH RESOURCE CLASS.

SWITCH	MEANING
STATISTICS	SPECIFIES CLASSES FOR WHICH RACF IS TO KEEP REFERENCE COUNTS IN DISCRETE PROFILES (NUMBER OF CALLS FOR "READ", NUMBER OF CALLS FOR "UPDATE", ETC.)
AUDIT	SPECIFIES CLASSES FOR WHICH RACF IS TO LOG EVERY TIME A RULE IS CREATED, CHANGED (INCLUDING PERMITS) , OR DELETED
ACTIVE	SPECIFIES CLASSES FOR WHICH RACF CHECKING IS TO BE IN EFFECT
GENERIC PROFILE	SPECIFIES CLASSES FOR WHICH % AND * ARE TO TREATED AS WILDCARD CHARACTERS
GENERIC COMMAND	SPECIFIES CLASSES WHICH FOR WHICH RACF COMMANDS TREAT % AND * AS WILDCARD CHARACTERS
GENLIST	SPECIFIES CLASSES FOR WHICH RACF IS TO KEEP ALL THE GENERIC PROFILES LOCKED IN MEMORY (A PERFORMANCE FEATURE) (CONTRAST WITH RACLIST BELOW)
GLOBAL	SPECIFIES CLASSES FOR WHICH RACF IS TO USE GLOBAL CHECKING (SEE THE DSMON REPORT FOR MORE DETAILS)

SWITCH	MEANING
RACLIST	SPECIFIES CLASSES FOR WHICH RACF IS TO KEEP **ALL** PROFILES LOCKED IN MEMORY (ANOTHER PERFORMANCE FEATURE) (CONTRAST WITH GENLIST ABOVE)
LOGOPTIONS ALWAYS	SPECIFIES CLASSES FOR WHICH EVERY REFERENCE IS TO BE LOGGED
LOGOPTIONS NEVER	SPECIFIES CLASSES FOR WHICH NO REFERENCE IS TO BE LOGGED
LOGOPTIONS SUCCESSES	SPECIFIES CLASSES FOR WHICH EVERY SUCCESSFUL REFERENCE IS TO BE LOGGED
LOGOPTIONS FAILURES	SPECIFIES CLASSES FOR WHICH EVERY FAILED REFERENCE IS TO BE LOGGED
LOGOPTIONS DEFAULT	SPECIFIES CLASSES FOR WHICH LOGGING IS BASED ON THE OPTIONS IN THE RACF RULE (GLOBALAUDIT OR AUDIT IN DATASET OR RESOURCE RULE)

RECOMMENDATIONS FOR RESOURCE CLASS SWITCHES

- SINCE **STATISTICS** APPLIES ONLY TO DISCRETE PROFILES, DON'T WORRY ABOUT IT

- TURN ON **AUDIT** FOR EVERY RESOURCE CLASS EXCEPT THE USS (OMVS) RELATED CLASSES, SINCE YOU NEED TO KNOW WHO MADE EACH AND EVERY CHANGE TO A RULE

- MAKE **ACTIVE** ONLY THOSE CLASSES YOU ARE READY TO ADMINISTER (SEE FURTHER RECOMMENDATIONS IN DSMON PRESENTATION)

- TURN ON **GENERIC PROFILE** FOR EVERY CLASS POSSIBLE (NOT POSSIBLE FOR GROUP CLASSES) EXCEPT FOR CLASSES RELATING TO DIGITAL CERTIFICATES

- DON'T WORRY ABOUT **GENERIC COMMAND**, SINCE IT IS USED ONLY TO REPAIR MIXED UP GENERIC PROFILES

- USE **GENLIST** FOR THE VMMDISK RESOURCE CLASS IF YOU USE RACF WITH VM, OTHERWISE USUALLY IGNORE IT

- USE **GLOBAL** FOR DATASETS, SELECTING THE DATASET RULES CAREFULLY BASED UPON ANALYSIS OF FREQUENCY OF USE AND SENSITIVITY. AN ENTRY TO PERMIT ANY ACCESS TO A DATASET WHOSE HIGH LEVEL QUALIFIER IS YOUR USERID WOULD MAKE SENSE. USE **GLOBAL** FOR OTHER CLASSES ONLY IF THE FREQUENCY JUSTIFIES IT

- USE **RACLIST** FOR ALMOST ANY CLASS THAT WILL TAKE IT, SINCE THE MEMORY IT USES IS NO LONGER A PROBLEM.

- SET **LOGOPTIONS** TO DEFAULT FOR ALL CLASSES UNLESS YOU HAVE A SPECIFIC REASON TO SET IT OTHERWISE

3) DATASET AND USERID OPTIONS

OPTION	MEANING
AUTOMATIC DATASET PROTECTION	OBSOLETE. USED TO BE USED TO SPECIFY THAT FOR CERTAIN USERS, EVERY DISK DATASET WHICH THEY CREATE GETS A RACF DISCRETE PROFILE WITH THE RACF BIT TURNED ON
ENHANCED GENERIC NAMING	DETERMINES WHETHER THE "ENHANCED" USE OF ASTERISKS IS USED FOR DSNAMES.
REAL DATASET NAMES	USED WITH DATASET NAMING CONVENTIONS TABLE TO SPECIFY THAT UN-MODIFIED VERSIONS OF DSNAMES ARE TO BE LOGGED
JES-BATCHALL-RACF	USED TO INDICATE THAT EVERY BATCH JOB MUST HAVE A RACF USERID ASSOCIATED WITH IT (EXCEPTING XBM JOBS, SEE NEXT ITEM)
JES-XBMALL-RACF	USED TO INDICATED THAT EVERY BATCH JOB RUN UNDER THE JES EXECUTION BATCH MONITOR MUST HAVE A RACF USERID ASSOCIATED WITH IT

OPTION	MEANING
JES-EARLYVERIFY	OBSOLETE, JES NOW ALWAYS ASSUMES THAT THIS SWITCH IS ON. USED TO INDICATE THAT JOBS SHOULD HAVE THEIR PASSWORD CHECKED WHEN THEY ARE READ IN, NOT LATER WHEN THEY ARE EXECUTED
PROTECT-ALL	REQUIRES EVERY DATASET TO HAVE A RACF RULE COVERING IT. IF TAPEDSN IS SET, APPLIES TO TAPE DATASETS, AS WELL
TAPE DATA SET PROTECTION (TAPEDSN)	TELLS RACF TO PROCESS TAPE DATASETS THE SAME WAY THAT DISK DATASETS ARE PROCESSED (THAT IS, BY CHECKING THE DSNAME AT OPEN TIME AGAINST THE APPROPRIATE RACF DATASET PROFILE)
SECURITY RETENTION PERIOD	USED WITH TAPE DATASETS TO SPECIFY THE DEFAULT NUMBER OF DAYS A TAPE DATASET IS KEPT BEFORE THE REEL OR CARTRIDGE IS SENT TO THE "SCRATCH" POOL.
ERASE-ON-SCRATCH	SPECIFIES WHETHER SCRATCHING A DISK DATASET CAUSES ZEROES TO BE WRITTEN OVER THE DATA BEFORE THE DISK SPACE IS FREED UP. FOUR OPTIONS: NOT ACTIVE, ACTIVE FOR ALL DATASETS, FOR DATASETS WITH A SPECIFIED SECURITY LEVEL OR HIGHER, OR FOR DATASETS WHOSE RACF PROFILES HAVE THE "ERASE" FLAG TURNED ON.

OPTION	MEANING
SINGLE LEVEL NAME PREFIX	SPECIFIES PREFIX WHICH RACF PRETENDS IS THE HIGH LEVEL QUALIFIER OF DSNAMES WHICH OTHERWISE HAVE JUST ONE QUALIFIER. FOR EXAMPLE, DSNAME=PASSWORD IS TREATED AS IF IT WERE DSNAME=prefix.PASSWORD
LIST OF GROUPS	SPECIFIES THAT EACH USER IS TO BE TREATED AS BEING ACTIVE IN ALL GROUPS TO WHICH THE USER IS CONNECTED
INACTIVE USERIDS	SPECIFIES THE NUMBER OF DAYS OF INACTIVITY AFTER WHICH A USERID WILL BE AUTOMATICALLY REVOKED
MODELLING (USER, GROUP, GDG)	OBSOLETE. USED TO SPECIFY THAT MODEL DATASET PROFILES WILL BE USED TO FILL IN THE PERMIT LISTS OF USER, GROUP, OR GDG DATASET PROFILES

RECOMMENDED DATASET AND USERID OPTIONS

- LEAVE **AUTOMATIC DATASET PROTECTION** INACTIVE
- SET **ENHANCED GENERIC NAMING** ON OR OFF FOR ALL OF YOUR INSTALLATION. NEITHER WAY IS RIGHT OR WRONG.
- USE **REAL DATASET NAMES** IF YOU CHOOSE, BUT IT ONLY MATTERS IF YOU USE THE DATASET NAMING CONVENTIONS EXIT
- ACTIVATE **BATCHALLRACF** AND **XBMALLRACF** TOGETHER
- DON'T WORRY ABOUT **EARLYVERIFY**
- TURN ON **PROTECTALL** IN FAIL MODE
- TURN ON **TAPE DATA SET PROTECTION OR USE TAPE MANAGEMENT SOFTWARE OR THE DEVSUPxx MEMBER OF PARMLIB**
- DON'T WORRY ABOUT **RETENTION PERIOD** IF YOU USE TAPE MANAGEMENT SOFTWARE
- ACTIVATE **ERASE-ON-SCRATCH** FOR SELECTED DATASETS (NOTE HOW IBM DESCRIBES THIS: "BY SECURITY LEVEL IS INACTIVE"!) OR FOR ALL DATASETS. THE PERFORMANCE PROBLEM HAS BEEN FIXED. THE STIGS (Security Technical Information Guides) FROM THE FEDERAL GOVERNMENT NOW SAY TO SPECIFY THIS FOR ALL DATASETS.
- SET **SINGLE LEVEL PREFIX** TO SUIT YOUR TASTE, OR STANDARDS

- ACTIVATE **LIST-OF-GROUPS**

- REVOKE **INACTIVE USERIDS** AFTER SOME TIME, BUT USE SEARCH COMMAND WITH CLIST OPTION TO REVOKE THEM PROPERLY

- LEAVE **MODELLING** TURNED OFF

4) PASSWORD OPTIONS

PASSWORD OPTION	MEANING
ENCRYPTION ALGORITHM	KDFAES IS MORE ROBUST THAN LEGACY
CHANGE INTERVAL	NUMBER OF DAYS AFTER WHICH A USER MUST CHANGE HIS OR HER PASSWORD
NUMBER OF GENERATIONS MAINTAINED	NUMBER OF RECENTLY USED PASSWORDS (UP TO 32) MAINTAINED IN EACH USER PROFILE (TO PREVENT PASSWORD RE-USE)
PASSWORD MINIMUM CHANGE INTERVAL	MINIMUM DAYS BEFORE A PASSWORD CAN BE CHANGED AGAIN
MIXED CASE PASSWORD SUPPORT	SUPPORTS BOTH UPPER AND LOWER CASE CHARACTERS IN PASSWORDS
SPECIAL CHARACTERS	ALLOWED OR NOT
NUMBER OF CONSECUTIVE UNSUCCESSFUL	NUMBER OF BAD PASSWORDS IN A ROW WHICH WILL CAUSE RACF TO REVOKE A USERID
EXPIRATION WARNING LEVEL	NUMBER OF DAYS BEFORE A PASSWORD EXPIRES THAT A USER IS WARNED

PASSWORD OPTION	MEANING
SYNTAX RULES	LENGTH AND CONTENT RULES (POSSIBLE VALUES ARE: *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*)

RECOMMENDATIONS FOR PASSWORD OPTIONS

- IMPLEMENT **KDFAES ENCRYPTION ALGORITHM**
- SET **PASSWORD CHANGE INTERVAL** TO SOMETHING IN THE AREA OF 30 DAYS (COMMON PRACTICE)
- SET **MINIMUM PASSWORD CHANGE INTERVAL** TO ONE DAY
- CONSIDER IMPLEMENTING **MIXED CASE PASSWORDS**, BUT ONLY AFTER TRAINING USERS PROPERLY AND FIXING ALL PROGRAMS WITH SIGN-ON SCREENS
- ALLOW **SPECIAL CHARACTERS** IN PASSWORDS
- KEEP 32 PASSWORD **GENERATIONS**, BUT ALSO MONITOR RE-USE AND FORBID RE-USE IN SECURITY STANDARDS
- REVOKE USERIDS AFTER 3 **UNSUCCESSFUL PASSWORDS**
- SET **PASSWORD EXPIRATION** LEVEL TO SUIT TASTE AND STANDARDS
- SET **SYNTAX RULES** TO INCLUDE AT LEAST ONE NUMBER AND AT LEAST ONE LETTER (ALPHANUMERIC) WITH A LENGTH OF AT LEAST 7.
- CONSIDER IMPLEMENTING **MIXED CASE** AND/OR **PASS PHRASES**, BUT ONLY AFTER SUFFICIENT TRAINING OF USERS.AND ADJUSTMENT OF ALL SIGNON SCREENS

5) MISCELLANEOUS OPTIONS

OPTION	MEANING
RVARY PASSWORDS	PASSWORDS OPERATOR IS TO ENTER TO CONFIRM USE OF RVARY COMMAND
SECURITY LEVEL AUDIT	SPECIFIES THAT RACF IS TO LOG ALL CHECKS OF ITEMS WITH A SPECIFIED SECURITY LEVEL
SECLABEL AUDIT	USED WITH B1. CAUSES LOGGING FOR ENTITIES WITH SECURITY LABELS BASED ON THE AUDIT OPTIONS IN THE SECLABEL RULES
SECLABEL CONTROL	USED WITH B1. RESTRICTS WHO CAN SPECIFY SECURITY LABELS IN RACF COMMANDS.
GENERIC OWNER	RESTRICTS SCOPE OF USER ATTRIBUTE CLAUTH(resource class name) TO PREVENT UNDERCUTTING
COMPATIBILITY MODE	USED WITH B1. ALLOWS CERTAIN USERIDS THAT DON'T HAVE SECURITY LABELS TO USE THE SYSTEM, EVEN THOUGH SECURITY LABELS ARE BEING CHECKED
MULTI-LEVEL OPTIONS	USED WITH B1 TO SPECIFY DEGREE OF RIGOR FOR LABEL CHECKING
CATALOGUED DATASETS ONLY	REQUIRES EVERY DATASET TO BE CATALOGUED, (WITH SOME EXCEPTIONS)
NJEUSERID	DEFAULT USERID FOR JESSPOOL PROFILE NAMES FOR NJE JOBS
UNDEFINEDUSER	DEFAULT USERID FOR JESSPOOL PROFILE NAMES FOR LOCAL JOBS

OPTION	MEANING
SESSIONKEY INTERVAL	DEFAULT NUMBER OF DAYS SESSION KEY FOR APPC IS VALID
PRIMARY AND SECONDARY LANGUAGES	DEFAULT LANGUAGES (FRENCH AND GERMAN, NOT COBOL AND FORTRAN) FOR MVS TO PRINT ERROR MESSAGES
ADDCREATOR	SPECIES THAT THE CREATOR OF A DATASET OR RESOURCE RULE SHOULD BE AUTOMATICALLY PERMITTED TO IT AT CREATION TIME WITH ALTER PERMISSION

RECOMMENDATIONS FOR MISCELLANEOUS OPTIONS

- PROVIDE **RVARY PASSWORDS**, DOCUMENT THEM, TRAIN AND TEST OPERATORS
- LEAVE **SECURITY LEVEL**, **SECLABEL AUDIT**, AND **SECLABEL CONTROL** INACTIVE UNLESS YOU NEED A B1 LEVEL OF SECURITY FOR THE MILITARY OR YOU HAVE SOME OTHER NEED
- CONSIDER TURNING ON **GENERICOWNER** AS PART OF AN OVERALL STRATEGY FOR DELEGATION OF AUTHORITY
- LEAVE **COMPATIBILITY MODE** AND **MULTI-LEVEL OPTIONS** NOT IN EFFECT, UNLESS YOU WANT B1 LEVEL SECURITY
- CONSIDER TURNING ON **CATALOGUED DATA SETS ONLY**, BUT RECOGNIZED THAT THIS MAY HAVE NOTHING TO DO WITH

SECURITY

- LEAVE THE REST TO THEIR DEFAULT VALUES: **NJEUSERID** (????????), **UNDEFINEDUSER** (++++++++), **SESSIONKEY INTERVAL** (30 DAYS), AND **LANGUAGES** (ENU FOR "ENGLISH AS SPOKEN IN THE UNITED STATES")

- SET **NOADDCREATOR**

NOTE: B1 REFERS TO A HIGHER THAN COMMON LEVEL OF SECURITY AS DEFINED BY THE US FEDERAL GOVERNMENT. MOST COMMERCIAL INSTALLATIONS ARE COMFORTABLE WITH THE SOMEWHAT LOWER C2 LEVEL, WHICH REQUIRES: BATCHALLRACF, XBMALLRACF, TAPE PROTECTION, PROTECTALL, ERASE-ON-SCRATCH FOR ALL DISK DATASETS, AND MORE.

SUMMARY

- WE HAVE SHOWN YOU HOW TO UNDERSTAND THE SETR LIST OUTPUT, AND PROVIDED YOU WITH RECOMMENDATIONS TO CONSIDER. MORE IMPORTANT THAN WHAT IS LISTED HERE IS THAT YOUR ORGANIZATION FORMALLY DECIDES HOW IT WANTS THESE OPTIONS TO BE SET. YOUR ORGANIZATION SHOULD DOCUMENT THIS AS A BASELINE DOCUMENT.

- YOU SHOULD HAVE A STANDARD IN WRITING FOR EVERY FIELD IN SETR LIST

- YOU SHOULD HAVE PERIODIC AUDITS OR REVIEWS TO ENSURE THAT THE STANDARD IS OBSERVED

- THIS WILL HELP YOU TO KNOW THAT YOUR RACF OPTIONS ARE SET THE WAY YOU WANT THEM TO BE. THIS WILL BE THE FOUNDATION FOR AN EFFECTIVE RACF IMPLEMENTATION, AND FOR EFFECTIVE INFORMATION SECURITY.

For More Info:

Questions to Stu Henderson at (301) 229-7187, stu@stuhenderson.com.
More whitepapers: http://www.stuhenderson.com/XARTSTXT.HTM
Newsletters at http://www.stuhenderson.com/Newsletters-Archive.html

The NIST STIGs (Security Technical Information Guides) for various types of computer, including mainframes https://web.nvd.nist.gov/view/ncp/repository

Useful guidelines for knowing that your InfoSec is comprehensive comprehensive (Note especially Publication 800-53): http://csrc.nist.gov/publications/PubsSPs.html#800-53

