RSH CONSULTING

RACF & TSO

NYRUG - April 2015

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, and consultant. He has reviewed, implemented, and enhanced RACF controls for major insurance firms, financial institutions, utilities, payment card processors, universities, hospitals, and international retailers. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He has also 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

Topics

- Introduction to TSO
- TSO Configuration
- TSO Commands
- TSO Logon
- TSO Resource Protection
- TSO Segment Administration
- Performance & Monitoring
- Miscellaneous

RACF, z/OS, TSO/E, DB2, and CICS are Trademarks of the International Business Machines Corporation

Introduction to TSO

- Time Sharing Option (TSO)
  - Interactive, time-sharing end-user processing environment
  - Each TSO user is provided with an individual address space
  - TSO interacts with users in either a line-by-line mode or in a full screen, menu-driven mode

- History
  - First introduced as an "optional feature" for OS/360 MVT in 1971
  - Became a standard component with the introduction of MVS in 1974
  - Licensed program for MVS through MVS/ESA
  - Time Sharing Option Extensions (TSO/E) added features to TSO
  - Part of the base element of OS/390 and z/OS

- Components
  - Started Task TCAS (Terminal Control Address Space) or VTAM APPL definitions
  - User Account Data Set - SYS1.UADS
  - Interactive System Productivity Facility/ Program Development Facility (ISPF/PDF)
  - Information Center Facility (ICF)
  - CLIST and REstructured eXtended eXecutor (REXX)
  - Batch programs IKJEFT01, IKJEFT1A, or IKJEFT1B

TSO Configuration - PARMLIB(IKJTSO*xx*)

- PARMLIB(IEASYSxx)
  - IKJTSO=00 | *xx*[,*xx*] - Identifier (*xx*) of IKJTSO TSO configuration member

- PARMLIB(IKJTSO*xx*) - TSO commands and programs
  - AUTHCMD NAMES(*cmd1*,*cmd2*...) - Authorized TSO/E commands (ADDSD)
  - AUTHPGM NAMES(*pgm1*,*pgm2*...) - Authorized programs (GIMSMP)
  - AUTHTSF NAMES(*name1*,*name2*...) - Authorized using service facility (ICHDSM00)
  - HELP *language*(*dsname1*[, ...)[[,...]) | ENU(SYS1.HELP)
  - LOGON LOGONHERE(ON | OFF) - Use RECONNECT even if not disconnected
    PASSPHRASE(ON | OFF) - Allows password of up to 100 characters
    VERIFYAPPL(ON | OFF) - Check permission to APPL resource at logon
  - SEND OPERSEND(ON | OFF) USERSEND(ON | OFF) ... - Allow use of SEND
    BROADCAST (DATASET(*dataset-name* | SYS1.BRODCAST) ...)
  - TRANSREC CIPHER(ALWAYS | YES | NO) ... - TRANSMIT options
  - TEST TSOCMD(*cmd1*,*cmd2*...) ... - Commands allowed to execute under TEST

TSO Configuration - TCAS

- TCAS Started Procedure

```
//TCAS    PROC MBR=TSOKEY00
//TCAS    EXEC PGM=IKTCAS00,TIME=1440
//PARMLIB  DD  DSN=LVL0.PARMLIB(&MBR),DISP=SHR,FREE=CLOSE
//PRINTOUT DD  SYSOUT=W,FREE=CLOSE
```

- TCAS PARMLIB DD - TSO/VTAM time sharing parameters (TCAS options)
  - Member defaults to PARMLIB(TSOKEY00)
  - USERMAX=0 | 40 | *n* - Maximum number of users that may be logged onto TSO(1)
  - RECONLIM=0 | 3 | 32767 - Minutes within which a user may reconnect
  - GNAME=*name* - Optional generic name for one or more TSO systems in a SysPlex

(1) The maximum number of users is also governed by IEASYS*xx* parameters RSVNONR, RSVSTRT, and MAXUSER, and if using VTAM APPL statements for TSO instead of TCAS, by the number of APPL statements

TSO Configuration - PARMLIB(SMFPRM*xx*)

- PARMLIB(IEASYSxx)
  - SMF=<u>00</u> | *xx*[,*xx*] - Identifier (*xx*) of SMFPRM SMF*n* member

- PARMLIB(SMFPRM*xx*) - SMF options
  - SID(<u>*processer-model#*</u> | *sysid* ...) - System Identifier (up to 4 characters)
  - JWT(*hhmm* | <u>0010</u>) - Time a job or TSO/E user may be inactive before termination
    - Note: Coding TIME=1440 on the JOB statement or the EXEC statement bypasses this limit

TSO Configuration - JES2

- JES2 PROC

```
//JES2      PROC  PROC01=PAY.PROCLIB
//IEFPROC   EXEC  PGM=HASJES20
//PROC00    DD  DSN=SYS1.PROCLIB,DISP=SHR
//          DD  DSN=TECHSPT.PROCLIB,DISP=SHR
//PROC01    DD  DSN=USER1.PROCLIB,DISP=SHR
//          DD  DSN=&PROC01,DISP=SHR
//HASPPARM DD  DSN=SYS1.PARMLIB(JES2PARM),DISP=SHR
//HASPLIST DD  DDNAME=IEFRDER
```

- HASPPARM JES2 Parameter Statements
  - PROCLIB *ddname*,DD(*sequence#*),DSNAME(*dsname*)
  - JOBCLASS(TSU)   (formerly TSUCLASS)
    - PROCLIB = 00 | *nn*
    - BLP = NO | YES
    - COMMAND = VERIFY | IGNORE | DISPLAY | EXECUTE
    - AUTH = ALL | CONS | INFO | IO | SYS

TSO Configuration - JES2

- TSO Logon PROC

```
//IKJACCNT PROC
//IKJACCT  EXEC PGM=IKJEFT01,DYNAMNBR=100
//SYSPRINT DD  TERM=TS,SYSOUT=*
//SYSTERM  DD  TERM=TS,SYSOUT=*
//SYSIN    DD  TERM=TS
//*
```

TSO Configuration - MSTJCL*xx*

- Master Scheduler Job - MSTJCL*xx*
  - PARMLIB(IEASYS*xx*) - MSTRJCL=*xx*[,*xx*] - Identifier (*xx*) of MSTJCL member, either ...
    - PARMLIB(MSTJCL*xx*)
    - SYS1.LINKLIB(MSTJCL*xx* | <u>MSTJCL00</u>)

```
//MSTJCLSV JOB MSGLEVEL=(1,1),TIME=1440
//         EXEC PGM=IEEMB860,DPRTY=(15,15)
//STCINRDR DD SYSOUT=(A,INTRDR)
//TSOINRDR DD SYSOUT=(A,INTRDR)
//IEFJOBS  DD DISP=SHR,DSN=VENDOR.STCJOBS
//         DD DISP=SHR,DSN=SVTSC.STCJOBS
//         DD DISP=SHR,DSN=LVL0.STCJOBS
//IEFPDSI  DD DISP=SHR,DSN=VENDOR.PROCLIB
//         DD DISP=SHR,DSN=SVTSC.PROCLIB
//         DD DISP=SHR,DSN=LVL0.PROCLIB
//         DD DISP=SHR,DSN=SYS1.PROCLIB
//SYSUADS  DD DSN=SYS1.UADS,DISP=SHR       (Optional)
```

TSO Commands - User

- CANCEL Ends the processing of batch jobs submitted at your terminal
- EDIT Creates, modifies, stores, submits, retrieves, and deletes datasets
- EXEC Executes a CLIST or REXX exec (e.g., EXEC EXEC.RACF.CLIST)
- HELP Gets information about command functions, syntax, and operands
- LISTALC Lists data sets that are currently allocated to the TSO/E session
- LISTBC Displays messages of general interest (from SYS1.BRODCAST)
- LISTCAT Lists entries from a catalog by name or entry type
- LOGOFF Ends your terminal session
- LOGON Starts your terminal session
- OUTPUT Display, route, print, and delete output (JOBNAME must start with user's USERID)
- PROFILE Changes or lists your user TSO profile (e.g., PREFIX)
- PROTECT Manage MVS password for datasets (will fail if PASSWORD dataset does not exist)
- RECEIVE Retrieves and restores transmitted files
- SEND Sends a message to another terminal user or system operator
- STATUS Displays the status of a job
- SUBMIT Submits batch jobs for processing
- TRANSMIT Sends a copy of a dataset to another user in the network

TSO Commands - User - PROFILE

```
profile list
 CHAR(0)  LINE(0)    PROMPT   INTERCOM   NOPAUSE NOMSGID MODE    WTPMSG    NORECO
VER PREFIX(RSH)     PLANGUAGE(ENU) SLANGUAGE(ENU) VARSTORAGE(LOW)
 DEFAULT LINE/CHARACTER DELETE CHARACTERS IN EFFECT FOR THIS TERMINAL
```

- PROFILE command operands:
  - LIST - List current PROFILE
  - RECOVER | NORECOVER - Use EDIT RECOVER option

    -- Uses datasets *userid*.EDITUTL1 and *userid*.EDITUTL2
  - PROMPT | NOPROMPT - Prompt for missing information
  - MSGID | NOMSGID - Include message identifiers with diagnostic message
  - PREFIX(*userid* |*dsname-prefix*) | NOPREFIX - Prefix DSNAME if no quotes

- PROFILE options are kept in the User Profile Table (UPT) control block, which is retained in the user's SYS1.UADS member or in the TUPT field of the user's TSO segment (cannot be listed or changed using RACF commands, nor is it included in IRRDBU00 unload output)

TSO Commands - System Programmer

- ACCOUNT Manage user attribute dataset (SYS1.UADS) and broadcast dataset
- CONSOLE Enter MVS operator commands
- CONSPROF Establish, change, or display your console characteristics
- OPERATOR Monitor TSO, cancel users, and perform SLIP
- PARMLIB Display and dynamically change TSO configuration
- RACONVRT Convert SYS1.UADS entries to RACF profiles
- SYNC Synchronize the broadcast dataset with either or both UADS and RACF TSO segments
- TESTAUTH Test authorized programs

TSO Logon

```
------------------------------- TSO/E LOGON -----------------------------------


   Enter LOGON parameters below:                RACF LOGON parameters:

   Userid    ===> RSHTEST

   Password  ===>                               New Password ===>

   Procedure ===> SPFPROCE                      Group Ident  ===>

   Acct Nmbr ===> FB3

   Size      ===> 100000

   Perform   ===>

   Command   ===>

   Enter an 'S' before each option desired below:
           -Nomail         -Nonotice        -Reconnect        -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
```

TSO Logon

- TSO checks RACF before SYS1.UADS
- If USERID is defined to RACF with a TSO Segment
  - Retrieve user's logon characteristics from the segment
  - Validate password with RACF
  - Verify user is authorized to use TSO resources via RACF profiles
- If USERID is defined to RACF without a TSO Segment
  - Retrieve user's logon characteristics from SYS1.UADS
    - If user is not defined to SYS1.UADS: IKJ56420I Userid *userid* not authorized to use TSO
  - Validate password with RACF
- If USERID is not defined to RACF, but is defined to SYS1.UADS
  - Retrieve user's logon characteristics from SYS1.UADS
  - Validate password with SYS1.UADS (can have null password)
- Recommendations:
  - Have a few RACF IDs with entries in SYS1.UADS and no TSO segment to enable TSO logon if either the TSO classes or RACF is disabled
  - Ensure senior RACF administrators can log onto the system console to fix RACF issues if TSO logon is not possible

SYS1.UADS

- SYS1.UADS
  - PDS with members associated with USERIDs
  - Allocated with LRECL=80,BLKSIZE=8000
  - Members are stored in a single block
  - Member names are *useridn*, where '*n*' is a sequential numeric suffix, starting with 0 (e.g., IBMUSER0)
    - If a user is assigned many TSO attributes, multiple members may be needed to store them
    - Length of TSO USERIDs is restricted to 7 characters to accommodate the member suffix
  - Managed with ...
    - TSO ACCOUNT command - if permitted access to TSOAUTH ACCT
      - LISTIDS subcommand - list all IDs
      - LIST subcommand - list details about an ID
    - TSO EDIT command - if permitted UPDATE access to SYS1.UADS
      - If creating a new UADS entry (e.g., by copying another member), must execute SYNC command to synchronize UADS with SYS1.BRODCAST

SYS1.UADS - ACCOUNT command

```
account
 ACCOUNT
listids
 IBMUSER   RSHUADS   SVTSCU
 IKJ56590I LISTED
list (rshuads)
 RSHUADS  USER ATTRIBUTES:  NOOPER  NOACCT  NOJCL  NOMOUNT    RECOVER
          INSTALLATION ATTRIBUTES, IN HEX: 0000
           MAXSIZE: NOLIM
           USER PROFILE TABLE:
           00000000000000000000000000000000 RSHUADS
           DESTINATION  =  CENTRAL SITE DEFAULT
           HOLD MSGCLASS=  (DEFAULT)
           JOB CLASS    =  (DEFAULT)
           MESSAGE CLASS=  (DEFAULT)
           SYSOUT CLASS =  (DEFAULT)
           NO PERFORMANCE GROUPS
    SEEPSWD
      (*)
        TSOTRSH   PROCSIZE=       0K, UNIT NAME= (NONE)
 IKJ56590I LISTED
end
```

TSO Segment - Logon Attributes

- TSO Segment - ADDUSER and ALTUSER TSO Operands
  - **ACCTNUM(account-number)**
  - COMMAND(command-issued-at-logon)
  - DEST(destination-id)
  - HOLDCLASS(hold-class)
  - JOBCLASS(job-class)
  - MAXSIZE(maximum-region-size)
  - MSGCLASS(message-class)
  - **PROC(logon-procedure-name)**
  - SECLABEL(security-label)
  - **SIZE(default-region-size)**
  - SYSOUTCLASS(sysout-class)
  - UNIT(unit-name)
  - USERDATA(user-data)

```
LU RSH TSO NORACF


USER=RSH


TSO INFORMATION
---------------
ACCTNUM= 1
PROC= IKJRSH
SIZE= 00000000
MAXSIZE= 00000000
UNIT= 3390
USERDATA= 0000
COMMAND= ISPF
```

TSO Segment - Logon Attributes

- The contents of the TSO segment are merely used to automatically fill in the TSO Logon Panel fields for the user; the segment entries do not permit access to the resources named
- At LOGOFF, TSO saves the attributes specified at logon to the TSO segment
  - In z/OS 2.1, TSO only saves the attributes if any were changed
- ACCTNUM syntax and coding
  - An ACCTNUM field value can contain any special character
    - UADS account number can contain any character except a blank, comma, semicolon, apostrophe, or tab
  - If defining an ACCTNUM resource containing parentheses, commas, blanks, or semicolons (*invalid*), enclose the string in single quotation marks
  - If defining an ACCTNUM resource containing a single quotation mark, put two single quotation marks together and enclose the string in single quotation marks
  - The ACCTNUM field value has a maximum length of 40 characters
    - The TSO logon panel allows the entry of account numbers of 40 characters in length
    - RACF ACCTNUM class profiles have a maximum of 39 characters
    - TSO truncates the account number entered to 39 characters for authorization checking

TSO Segment - Logon Attributes

- Syntax and coding

COMMAND	1-80 characters, case-sensitive - Same rules as for ACCTNUM if entering special characters
DEST	1-7 alphanumeric characters, beginning with alpha or national
HOLDCLASS	1 alphanumeric character, excluding nationals
JOBCLASS	1 alphanumeric character, excluding nationals
MAXSIZE	0-2096128 of 1024-byte units of virtual storage
MSGCLASS	1 alphanumeric character, excluding nationals
PROC	1-8 alphanumeric characters, beginning with alpha
SIZE	0-2096128 of 1024-byte units of virtual storage (minimum size) - ignored if greater than MAXSIZE
SYSOUTCLASS	1 alphanumeric character, excluding nationals
UNIT	1-8 alphanumeric characters
USERDATA	4 characters comprised of 0-9 and A-F

TSO Resource Protection

- Controls ...
  - What TSO account number, logon PROC, and performance group a user may use
  - What TSO privileged authorities are assigned to a user

- TSO-specific Resource Classes

TSOPROC	- Logon procedure name
ACCTNUM	- Account number
PERFGRP	- Performance group name
TSOAUTH	- Authorities

- Classes must be activated to enable protection
  - SETROPTS CLASSACT(*class*)

- Classes can optionally be activated for generics
  - SETROPTS GENCMD(*class*) - Enables creation of profiles
  - SETROPTS GENERIC(*class*) - Activates profiles

TSO Resource Protection - CDT

CDT ATTRIBUTES	TSOPROC	ACCTNUM	PERFGRP	TSOAUTH
ID =	45	46	47	48
FIRST =	ALPHA	ANY	NUMERIC	ALPHANUM
MAXLENX =	8	39	3	8
MAXLNTH =	8	39	3	8
OTHER =	ALPHANUM	ANY	NUMERIC	ALPHANUM
POSIT =	127	126	125	124

CASE = UPPER

DFTRETC = 4

DFTUACC = NONE

DYNAMIC = NO

GENLIST = DISALLOWED

RVRSMAC = NO

KEYQUAL = 0

OPER = NO

PROFDEF = YES

RACLIST = ALLOWED

RACLREQ = NO

SLBLREQ = NO

TSO Resource Protection - TSOPROC

- TSOPROC class
  - Resource - *procname* - 1-8 characters (e.g., PGMRP1)
  - Access level - READ - permits use

- RACF SAG states TSOPROC profiles must be discrete, but generics work

- If the TSOPROC class is inactive, users cannot logon and TSO displays ...
  - IKJ56482I THE PROCEDURE NAME TSOTRSH HAS NOT BEEN DEFINED FOR USE

- If a user enters a TSOPROC that is not defined to RACF, TSO displays ...
  - IKJ56482I THE PROCEDURE NAME UNKPROC1 HAS NOT BEEN DEFINED FOR USE
  - User must change it to a valid PROC to logon

- If a user attempts to use an unauthorized TSOPROC, TSO displays ...
  - IKJ56483I THE PROCEDURE NAME TPR1 HAS NOT BEEN AUTHORIZED FOR THIS USERID
  - User must change it to a valid PROC to logon

TSO Resource Protection - TSOPROC

- If a user attempts to logon without specifying a PROC (e.g., NOPROC), ...
  - If TSOPROC is not RACLISTED , TSO displays ...
    - IKJ56497I DEFAULT PROCEDURE NAMES COULD NOT BE OBTAINED - ENTER PROCEDURE NAME
    - User must enter an authorized PROC
  - If TSOPROC is RACLISTED, TSO will check the TSOPROC profiles and ...
    - If the user is permitted access to a single discrete TSOPROC profile, TSO will automatically assign this PROC to the user and log the user on
    - If the user is permitted access to more than one TSOPROC profile, one of which is a discrete, TSO will insert the first authorized discrete profile found on the logon panel and display ...
      - IKJ56485I THE ACCOUNT NUMBER FB3 IS A DEFAULT NAME - YOU MAY CHANGE IT
      - The user can keep this entry and logon, or change it to another authorized TSOPROC
    - If the user is not permitted access to any discrete profiles, but is permitted access to one or more generic profiles, TSO will insert the first generic profile found on the logon and display ...
      - IKJ56480I THE PROCEDURE NAME TSOT* IS A GENERIC NAME - PLEASE COMPLETE IT
      - The user must change it to an authorized PROC
    - If the user is not permitted access to any profiles, TSO will display ...
      - IKJ56495I LOGON TERMINATED. USER IS NOT DEFINED TO ANY PROCEDURE NAMES
      - TSO then ejects the user

TSO Resource Protection - ACCTNUM

- ACCTNUM class
  - Resource - *account-number* - 1-39 characters (e.g., FIN2245ACCTPAY)
    - The TSO segment ACCTNUM field allows the use of special characters that cannot be coded in an ACCTNUM profile; generic masking characters must be used to allow their use
  - Access level - READ - permits use

- If the ACCTNUM class is inactive, users cannot logon and TSO displays ...
  - IKJ56486I THE ACCOUNT NUMBER ABC123 HAS NOT BEEN DEFINED FOR USE

- If a user enters an ACCTNUM that is not defined to RACF, TSO displays ...
  - IKJ56486I THE ACCOUNT NUMBER XXX HAS NOT BEEN DEFINED FOR USE
  - User must change it to a valid account number to logon

- If a user attempts to use an unauthorized ACCTNUM, TSO displays ...
  - IKJ56487I THE ACCOUNT NUMBER FB3 HAS NOT BEEN AUTHORIZED FOR THIS USERID
  - User must change it to a valid account number to logon

TSO Resource Protection - ACCTNUM

- If a user attempts to logon without specifying an account number (e.g., NOACCTNUM), ...
  - If ACCTNUM is not RACLISTED , TSO displays ...
    - IKJ56496I DEFAULT ACCOUNT NUMBERS COULD NOT BE OBTAINED - ENTER ACCOUNT NUMBER
    - User must enter an authorized account number to logon
  - If ACCTNUM is RACLISTED, TSO will check the ACCTNUM profiles and ...
    - If the user is permitted access to a single discrete ACCTNUM profile, TSO will automatically assign this ACCTNUM to the user and log the user on
    - If the user is permitted access to more than one ACCTNUM profile, one of which is a discrete, TSO will insert the first authorized discrete profile found on the logon panel and display ...
      - IKJ56485I THE ACCOUNT NUMBER FB3 IS A DEFAULT NAME - YOU MAY CHANGE IT
      - The user can keep this entry and logon, or change it to another authorized ACCTNUM
    - If the user is not permitted access to any discrete profiles, but is permitted access to one or more generic profiles, TSO will insert the first generic profile found on the logon and display ...
      - IKJ56484I THE ACCOUNT NUMBER ABCDEF* IS A GENERIC NAME - PLEASE COMPLETE IT
      - The user can keep this entry as is and logon, or change it to another authorized ACCTNUM
    - If the user is not permitted access to any profiles, TSO will log the user in with no account number

TSO Resource Protection - PERFGRP

- PERFGRP class
  - Resource - *performance-group-name* - 3 digits
  - Access level - READ - permits use

- Message if PERFGRP inactive or there is no group defined
  - IKJ56488I NO PERFORMANCE GROUPS EXIST FOR THIS USERID
  - User can simply delete the performance group and logon

- Performance Groups are obsolete, and their functionality has been replaced by WLM

- Logon is permitted when PERFGRP is inactive as long as the user does not enter a performance group number
  - Many installations deactivate this class

TSO Resource Protection - TSOAUTH

- TSOAUTH class
  - Resource - *tso-authority* - specific names, up to 8 characters (e.g., ACCT)
  - Access level - READ - permits use
    - UPDATE - permits PARMLIB update (load new IJKTSO*xx* member)

- Messages if the user attempts to use an authority when (a) TSOAUTH is inactive, (b) no profile is defined, or (c) the user is not permitted access
  - IKJ56553I COMMAND NOT AUTHORIZED FOR RSHTEST+
  - IKJ56553I YOUR INSTALLATION MUST AUTHORIZE USE OF THIS COMMAND

- TSOAUTH checking
  - TSO automatically checks a user's permission to every authority at logon (using RACROUTE with LOG=NONE) and notes which authorities the user is permitted to use in the Protected Step Control Block (PSCB) maintained by TSO for the user
  - Following logon, TSO uses the bit settings in the PSCB to govern a user's authority to use a TSO authority; it does not check RACF
  - No violation is recorded if user attempts to use an authority that is not allowed

TSO Resource Protection - TSOAUTH

- TSOAUTH resources

ACCT	- Execute ACCOUNT and SYNC commands
CONSOLE	- Execute CONSOLE and CONSPROF commands
JCL	- Execute SUBMIT command
MOUNT	- Issue allocation requests needing a volume to be mounted
OPER	- Execute OPERATOR command
PARMLIB	- Execute PARMLIB command
RECOVER	- Recover from EDIT errors
TESTAUTH	- Execute TESTAUTH command

- If RACF is installed, user must have SPECIAL authority to execute RACNVRT; otherwise, user must have access to ACCT

- Use of CONSOLE also requires access to OPERCMDS MVS.MCSOPER.*userid*, where '*userid*' typically matches the ID of the invoking user

TSO Resource Protection - TSOAUTH

- Common / Best Practices
  - All users typically need JCL and RECOVER
    - Usually defined with UACC(READ)
    - Often have corresponding entries in the Global Access Table allowing READ
  - Few users would ever need MOUNT
  - Avoid coding profiles ACCOUNT and OPERATOR as they are not substitutes for ACCT and OPER
  - Restrict access to ACCT, CONSOLE, OPER, and PARMLIB
  - Disallow all access to TESTAUTH, except perhaps on System Test LPAR and only for installation TSO command development
  - Avoid the use of TSO authorities for granting SDSF authorities
    - ISFPARMS - GROUP TSOAUTH(JCL,OPER,ACCT)
    - Instead use permissions to SDSF resources GROUP.*group-name*.*sdsf-server-name*

TSO Resource Protection - JESJOBS

- Controls who can cancel jobs other than their own using the TSO CANCEL command

- JESJOBS Class (DFTRETC=8 class)
  - Resource - CANCEL.*local-nodename.userid.jobname*
    - Example: CANCEL.PRDNDE1.HRBATID.HR00737
      CANCEL.*.HRBATID.HR* - PERMIT ID(PRODCNTL) ACC(ALTER)
    - *Userid* is the job's execution ID
  - Access level - ALTER - permits cancel

- Comments / Best Practices
  - USERID assigned to the job is the "owner" of the job and the owner will be allowed to cancel the job without explicit authorization - only need to define profiles where one user is to be allowed to cancel the jobs of another user
  - Most installations use other facilities (SDSF) for canceling jobs
  - Recommendation - Create JESJOBS profile CANCEL.* with UACC(NONE) and no permissions to block all use of CANCEL except by job owner

TSO Resource Protection - APPL

- Controls who can log onto TSO on this system or set of systems
- APPL Class
  - Resource - either …
    - TSO*ssss* - where '*ssss*' is the SMF system ID from PARMLIB member SMFPRM*xx*
    - *VTAM-generic-name* - name specified by the GNAME parameter of the Terminal Control Address Space (TCAS) started task when VTAM generic resources are being used for TSO
  - Access level - READ - permits logon
- APPL checking is activated by setting PARMLIB member IKJTSO*xx* parameter VERIFYAPPL to YES (default setting is NO) - Option introduced in z/OS 1.10
- If the user is not authorized to log onto TSO's APPL resource, TSO displays the following and then ejects the user ...
  - IKJ56420I USERID userid NOT AUTHORIZED TO USE TSO
  - IKJ56418I CONTACT YOUR TSO ADMINISTRATOR
- If the user logs on with UADS credentials alone, no APPL resource access authorization check is performed

TSO Segment Administration - FIELD

- Delegate maintenance of profile segments (e.g., TSO segment)

- FIELD Class
  - Profile - *profile-type.segment.field* (e.g., USER.TSO.TACCNT)
  - Access Levels
    - READ - list settings
    - UPDATE - change settings

- Applies to all profiles, no Scope-of-Groups limitation

- &RACUID can be used to permit users access to just their own USER segment(s) - usually to allow viewing (READ)

- May combine with CLAUTH(*tso-class*) to enable TSO profile creation

- Best Practice - Limit UPDATE access to those individuals responsible for management of the segment's related product (e.g., TSO) when such users are better able to manage the segments than RACF administration

TSO Segment - FIELD Class Resources

USER.TSO.	
USER.TSO.TACCNT	ACCTNUM
USER.TSO.TCOMMAND	COMMAND
USER.TSO.TDEST	DEST
USER.TSO.THCLASS	HOLDCLASS
USER.TSO.TJCLASS	JOBCLASS
USER.TSO.TLPROC	PROC
USER.TSO.TLSIZE	SIZE
USER.TSO.TMCLASS	MSGCLASS
USER.TSO.TMSIZE	MAXSIZE
USER.TSO.TSCLASS	SYS
USER.TSO.TSOSLABL	SECLABEL
USER.TSO.TUDATA	USERDATA
USER.TSO.TUNIT	UNIT

Performance

- SETROPTS RACLIST(*tso-classes*)
  - Loads TSO-related profiles into a dataspace to expedite authorization checking
  - Recommended for all TSO-related classes

- SETROPTS GLOBAL - Recommended entries

DATASET	&RACUID.*.**/ALTER	
DATASET	ISF.*.**/READ	
DATASET	ISP.*.**/READ	
DATASET	SYS1.BRODCAST/READ	(assumes this is the BROADCAST dataset)
TSOAUTH	JCL/READ	
TSOAUTH	RECOVER/READ	

- Dataset profile refresh - TSO user can execute the following command to refresh profiles for a particular HLQ (avoids re-logon and GENERIC REFRESH)

```
LISTDSD DA('hlq.anything') GENERIC
```

Miscellaneous

- SETROPTS AUDIT(*tso-classes*)
  - Audits all changes to RACF profiles in the associated resource class
  - Captures administrative events not covered by SAUDIT
  - Recommended for all classes

- TSO warns users of an upcoming requirement to change their password based on SETROPTS PASSWORD(WARNING(*nn*))

- TSO users have unrestricted authority to add, delete, and change dataset profiles whose HLQs match their USERID, even if the profile is owned by another user or group (unless RACF commands are controlled)

- RACF and TSO segment administrators require UPDATE access permission to the BROADCAST dataset (SYS1.BRODCAST) to add and delete TSO segments

- If z/OS systems share a RACF database but not the BROADCAST dataset (SYS1.BRODCAST) and a TSO segment is added on one system, the SYNC command must be run on the others to synchronize their individual BROADCAST datasets with RACF; otherwise, users may not receive their notify messages