RSH CONSULTING

RACF
Health Checks

KOIRUG - May 2019

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

IBM Health Checker for z/OS

- Tool developed by IBM to identity common configuration and setup errors
- Components
  - Started Task (HZSPROC) - Requires UID(0) or access to FACILITY BPX.SUPERUSER
  - PARMLIB(HZSPRMxx) - Add, modify, and deactivate checks
  - Health Checks
    - Each check is a "best practice"
    - Written by individual components (e.g., RACF)
    - ISVs and Installations can write their own checks
- Health Check names
  - 1-32 character check name (e.g, RACF_IBMUSER_REVOKED)
  - 1-16 character check owner - IBM-supplied checks begin with IBM (e.g., IBMRACF)
- Health Checks can be viewed via SDSF - option CK on the main panel
- Health Check reports can be printed using PGM=HZSPRNT
- Each check has guidance at the end for interpreting the results

RACF Health Checks - Owner IBMRACF

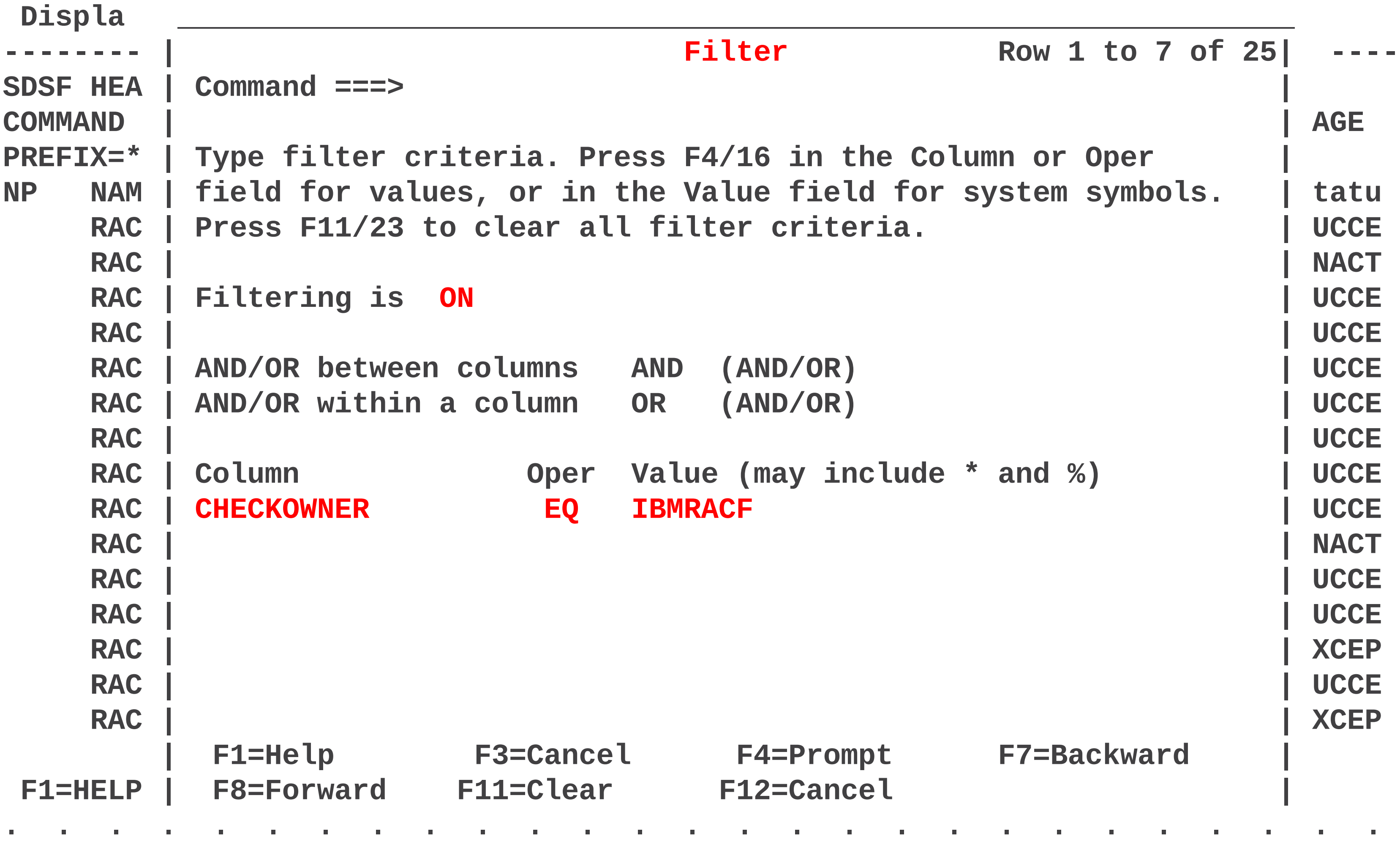
CHECK NAME	FUNCTION
RACF_AIM_STAGE	Verifies the RACF database is at AIM Stage 3
RACF_AUDIT_CONTROLS	Verifies SETROPTS SAUDIT, OPERAUDIT, and CMDVIOL are in effect
RACF_BATCHALLRACF	Verifies the SETROPTS option JES(BATCHALLRACF) is in effect
RACF_CERTIFICATE_EXPIRATION	Reports certificates expiring in 60 days and checks if expired certificates are trusted or associated with any keyrings
RACF_*class*_ACTIVE	Verifies the class is active: CFSKEYS, CFSSERV, FACILITY, JESJOBS, JESSPOOL, OPERCMDS, TAPEVOL, TEMPDSN, TSOAUTH, UNIXPRIV
RACF_ENCRYPTION_ALGORITHM	Verifies password encryption algorithm KDFAES is in use
RACF_GRS_RNL	Verifies none of the RACF ENQ names are on a Global Resource Serialization (GRS) resource name exclusion list (RNL) which changes the scope of the RACF ENQ
RACF_IBMUSER_REVOKED	Verifies user IBMUSER is revoked
RACF_ICHAUTAB_NONLPA	Reports non-LPA resident ICHAUTAB programs
RACF_PASSWORD_CONTROLS	Verifies mixed-case passwords are allowed, INITSTATS is active, invalid password attempts are 3 or less, and password expiration is no more than 90 days
RACF_RRSF_RESOURCES	Verifies RRSF INMSG and OUTMSG datasets are defined and protected
RACF_SENSITIVE_RESOURCES	Verifies critical system datasets and general resources are properly protected
RACF_UNIX_ID	Checks if FACILITY BPX.DEFAULT.USER exists, and if defined, BPX.UNIQUE.USER is fully implemented - UNIXPRIV SHARE.IDS and FACILITY BPX.NEXT.USER are defined and active
ZOSMIGV2R1_DEFAULT_UNIX_ID	Same as RACF_UNIX_ID

RACF Health Checks - SDSF

```
 Display  Filter  View  Print  Options  Search  Help
-------------------------------------------------------------------------------
SDSF MENU V2R3M0    SVSCPLEX  S0W1                      LINE 31-45 (48)
COMMAND INPUT ===>                                             SCROLL ===> PAGE
PREFIX=*  DEST=(ALL)  OWNER=*  SYSNAME=
NP   NAME     Description              Group    Status
     CK       Health checker           System
     LNK      Link list data sets      System
     LPA      Link pack data sets      System
     APF      APF data sets            System
     PAG      Page data sets           System
     PARM     Parmlib data sets        System
     PROC     Proclib data sets        JES
     CFC      CF Connections           Sysplex
     CFS      CF Structures            Sysplex
     VMAP     Virtual storage map      Memory
     SMSG     SMS storage groups       Devices
     SMSV     SMS volumes              Devices
     FS       File systems             OMVS
     CSR      Common storage remaining Memory
     GT       Generic tracker          System
```

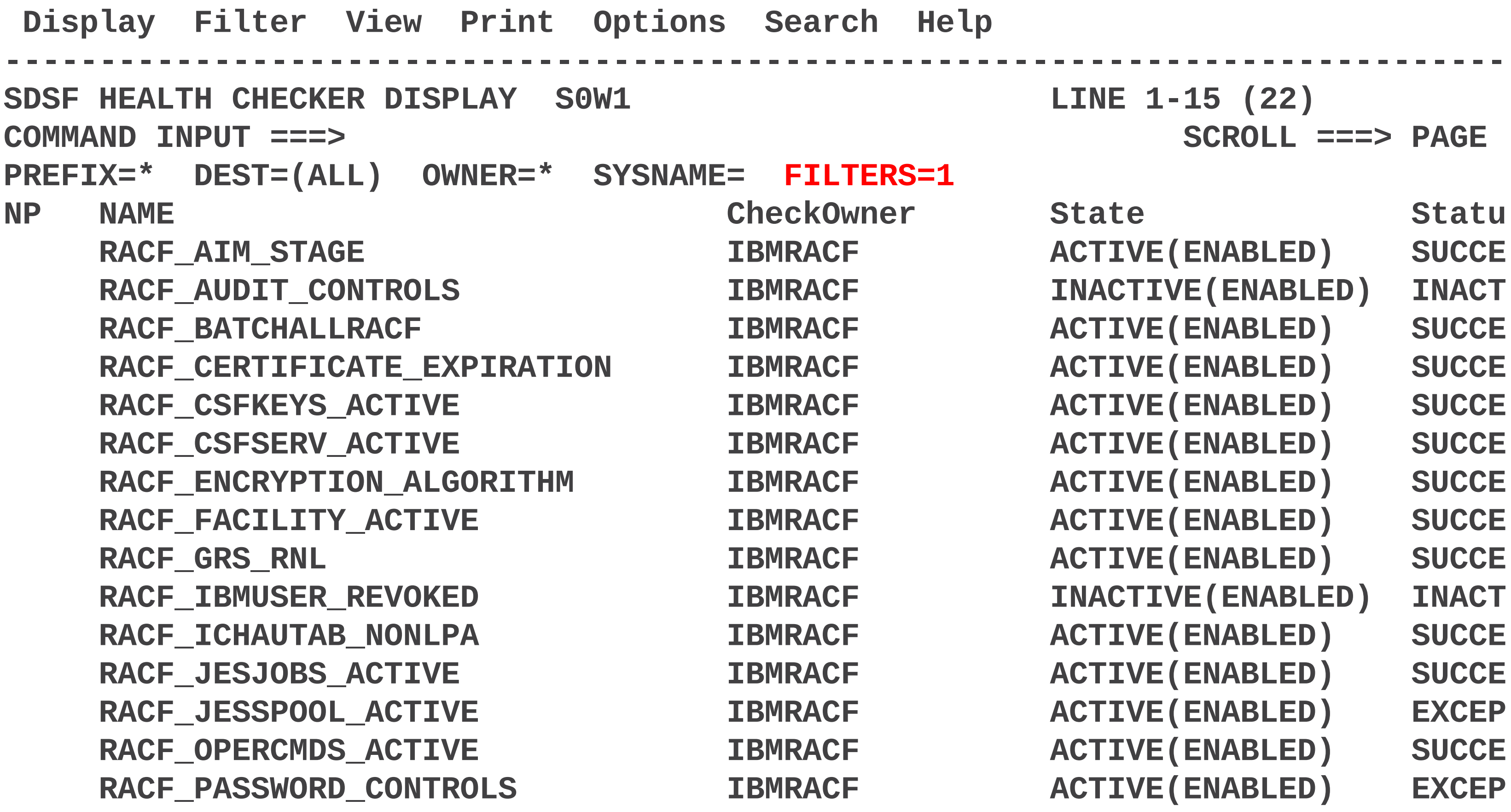
SDSF ISFCMD.ODSP.HCHECKER.*system* - READ access required to use CK command
LOGSTRM *health-check-history-log-stream-name* - READ access

RACF Health Checks - SDSF - Filter



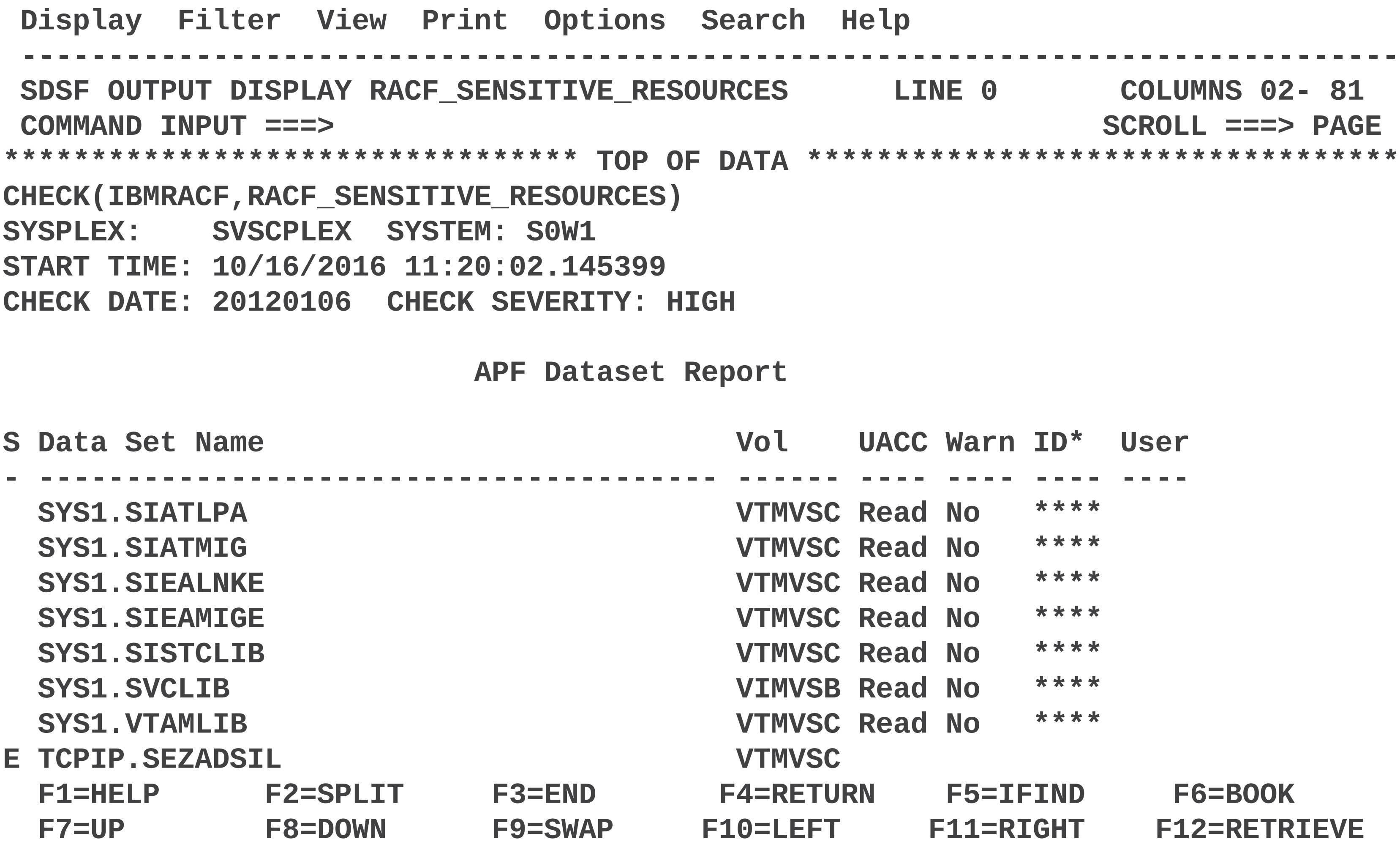
```
 Displa  ________________________________________________________________
-------- |                            Filter           Row 1 to 7 of 25|  ----
SDSF HEA | Command ===>                                                |
COMMAND  |                                                             | AGE
PREFIX=* | Type filter criteria. Press F4/16 in the Column or Oper     |
NP   NAM | field for values, or in the Value field for system symbols. | tatu
     RAC | Press F11/23 to clear all filter criteria.                  | UCCE
     RAC |                                                             | NACT
     RAC | Filtering is  ON                                            | UCCE
     RAC |                                                             | UCCE
     RAC | AND/OR between columns   AND  (AND/OR)                      | UCCE
     RAC | AND/OR within a column   OR   (AND/OR)                      | UCCE
     RAC |                                                             | UCCE
     RAC | Column                 Oper  Value (may include * and %)    | UCCE
     RAC | CHECKOWNER              EQ   IBMRACF                        | UCCE
     RAC |                                                             | NACT
     RAC |                                                             | UCCE
     RAC |                                                             | UCCE
     RAC |                                                             | XCEP
     RAC |                                                             | UCCE
     RAC |                                                             | XCEP
         |  F1=Help        F3=Cancel       F4=Prompt       F7=Backward |
 F1=HELP |  F8=Forward    F11=Clear      F12=Cancel                    |
 .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .  .
```

RACF Health Checks - SDSF - CK Display



```
 Display  Filter  View  Print  Options  Search  Help
--------------------------------------------------------------------------------
SDSF HEALTH CHECKER DISPLAY  S0W1                          LINE 1-15 (22)
COMMAND INPUT ===>                                                SCROLL ===> PAGE
PREFIX=*  DEST=(ALL)  OWNER=*  SYSNAME=  FILTERS=1
NP   NAME                             CheckOwner       State                Statu
     RACF_AIM_STAGE                   IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_AUDIT_CONTROLS              IBMRACF          INACTIVE(ENABLED)    INACT
     RACF_BATCHALLRACF                IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_CERTIFICATE_EXPIRATION      IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_CSFKEYS_ACTIVE              IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_CSFSERV_ACTIVE              IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_ENCRYPTION_ALGORITHM        IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_FACILITY_ACTIVE             IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_GRS_RNL                     IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_IBMUSER_REVOKED             IBMRACF          INACTIVE(ENABLED)    INACT
     RACF_ICHAUTAB_NONLPA             IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_JESJOBS_ACTIVE              IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_JESSPOOL_ACTIVE             IBMRACF          ACTIVE(ENABLED)      EXCEP
     RACF_OPERCMDS_ACTIVE             IBMRACF          ACTIVE(ENABLED)      SUCCE
     RACF_PASSWORD_CONTROLS           IBMRACF          ACTIVE(ENABLED)      EXCEP
```

RACF Health Checks - Sensitive Resources



```
 Display  Filter  View  Print  Options  Search  Help
 -------------------------------------------------------------------------------
 SDSF OUTPUT DISPLAY RACF_SENSITIVE_RESOURCES      LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===>                                            SCROLL ===> PAGE
********************************* TOP OF DATA **********************************
CHECK(IBMRACF,RACF_SENSITIVE_RESOURCES)
SYSPLEX:    SVSCPLEX  SYSTEM: S0W1
START TIME: 10/16/2016 11:20:02.145399
CHECK DATE: 20120106  CHECK SEVERITY: HIGH

                           APF Dataset Report

S Data Set Name                            Vol    UACC Warn ID*  User
- ---------------------------------------- ------ ---- ---- ---- ----
  SYS1.SIATLPA                             VTMVSC Read No   ****
  SYS1.SIATMIG                             VTMVSC Read No   ****
  SYS1.SIEALNKE                            VTMVSC Read No   ****
  SYS1.SIEAMIGE                            VTMVSC Read No   ****
  SYS1.SISTCLIB                            VTMVSC Read No   ****
  SYS1.SVCLIB                              VIMVSB Read No   ****
  SYS1.VTAMLIB                             VTMVSC Read No   ****
E TCPIP.SEZADSIL                           VTMVSC
  F1=HELP      F2=SPLIT     F3=END       F4=RETURN    F5=IFIND     F6=BOOK
  F7=UP        F8=DOWN      F9=SWAP     F10=LEFT     F11=RIGHT    F12=RETRIEVE
```

RACF Health Checks - Sensitive Resources

- Ensures UACC and ID(*) access levels are appropriate and profiles are not in WARNING
- Dataset checks (also confirms they are on the indicated volume and profile-protected if PROTECTALL is not in effect)
  - APF
  - RACF
  - PARMLIB
  - Link List
  - System REXX
  - ICSF
- Resource checks
  - FACILITY BPX.unix-authority
  - FACILITY IEAABD.dump-authority
  - FACILITY ICHBLP
  - FACILITY IRR.PASSWORD.RESET
  - OPERCMDS SET.PROG and SETPROG
  - OPERCMDS SLIP
  - SURROGAT BPX.SRV.userid
  - TSOAUTH authority
  - UNIXPRIV SUPERUSER.unix-authority
- ICHAUTAB check

RACF Health Checks - Sensitive Resources

- Status flags in "S" field
  - E Exception - excessive authority or no dataset profile (NOPROTECTALL)
  - V Dataset not on indicated volume (could be SMS migrated)
  - M Migrated dataset
  - U Dataset in Use - could not be checked
- If there is no corresponding RACF profile, the UACC, WARN, and ID(*) columns are blank
- If a valid user ID was specified as a parameter to the check, that user's authority to the dataset is checked and flagged if above READ
- Modules which are flagged in the ICHAUTAB report as exceptions must be either removed from ICHAUTAB or the module must be moved to a non-LPA location and protected by a PROGRAM class profile

RACF Health Checks - HZSPRNT Batch Print

```
//jobname JOB (account),'username',CLASS=x,MSGCLASS=x
//STEP0001 EXEC PGM=HZSPRNT,PARM='CHECK(IBMRACF,*)'
//SYSOUT DD SYSOUT=*,DCB=LRECL=256

 ************************************************************************
 *                                                                      *
 * Start: CHECK(IBMRACF,RACF_BATCHALLRACF)                              *
 *                                                                      *
 ************************************************************************

 CHECK(IBMRACF,RACF_BATCHALLRACF)
 SYSPLEX:    SVSCPLEX  SYSTEM: S0W1
 START TIME: 03/01/2019 05:17:01.402348
 CHECK DATE: 20160202  CHECK SEVERITY: MEDIUM

 IRRH330I SETROPTS JES(BATCHALLRACF) is in effect.

 END TIME: 03/01/2019 05:17:01.402670  STATUS: SUCCESSFUL

 ************************************************************************
 *                                                                      *
 * End:   CHECK(IBMRACF,RACF_BATCHALLRACF)                              *
 *                                                                      *
 ************************************************************************

 No messages exist      <- indicates check is not active
```

RACF Protection for Health Checker

- RACF controls who can view, initiate, print, and manage checks
- XFACILIT / GXFACILI class profiles
- Resources (depends on use of wildcarding in request)
  - READ (HZSQUERY) *reqtype* MESSAGES, QUERY
  - UPDATE (HZSCHECK) *reqtype* ACTIVATE, UPDATE, DEACTIVATE, RUN
  - CONTROL (HZSCHECK, HZSADDCK) *reqtype* DELETE, REFRESH
  - HZS.*sysname*.*reqtype*
  - HZS.*sysname*.*check_owner*.*reqtype*
  - HZS.*sysname*.*check_owner*.*check_name*.*reqtype*
- RACF related health-check resources - checked in the following sequence
  - HZS.*sysname*.*reqtype* - applies to all checks
  - HZS.*sysname*.IBMRACF.*reqtype*
  - HZS.*sysname*.IBMRACF.*check-name*.*reqtype*
- Authorization checking using FASTAUTH - XFACILIT must be RACLISTed

EX: HZS.SYSA.IBMRACF.RACF_SENSITIVE_RESOURCES.QUERY