RSH CONSULTING

RACF Protection
CONSOLE & OPERCMDS

CHIRUG - November 2017

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

Topics

- Introduction and Basic Control Concepts
- Console Authority and Control
- Operator Command Protection

Basic Control Concepts

- Operator commands are the commands used to manage the system, control running processes, and dynamically configure the system
- Consoles (physical and logical) are the conduits through which operator commands are entered
- The authority to execute operator commands is governed by:
  - OPERCMDS profiles, or
  - AUTH parameter on the console, which governs use when:
    - There is no protecting OPERCMDS profile, or
    - There is no RACF user logged on at a physical console
- Console logons are governed by:
  - LOGON parameter on the console as defined in PARMLIB(CONSOLxx), and
  - CONSOLE profiles

Console's Role

- Relay system messages to the operator
  - System initialization (IPL) information
  - Device status information
  - Network status information
  - Started task status information
  - Application program status information
  - Requests for replies
- Relay operator commands to the system

Operator Command Functional Overview

- Manage z/OS and its environment
  - Manage the IPL
  - Control and configure hardware
  - Reply to messages
  - Start, modify, and stop tasks
  - Communicate with VTAM and TCPIP
  - Control JES
  - Shutdown z/OS
- Manage flow of work
  - Start initiators
  - Hold, release, and cancel jobs
  - Hold and release output
  - Assign forms
  - Print and route output
  - Purge jobs and output
- Manage system software
  - Load new LNKLST
  - Refresh LNKLST
  - Refresh VLF
  - Change system PARMLIB concatenation
  - Add and delete APF-authorized libraries
  - Activate and deactivate dynamic exits
  - Set software parameters
- Manage the network
  - Establish connections
  - Control lines
  - Control VTAM applications
  - Control nodes
  - Start and stop remote devices

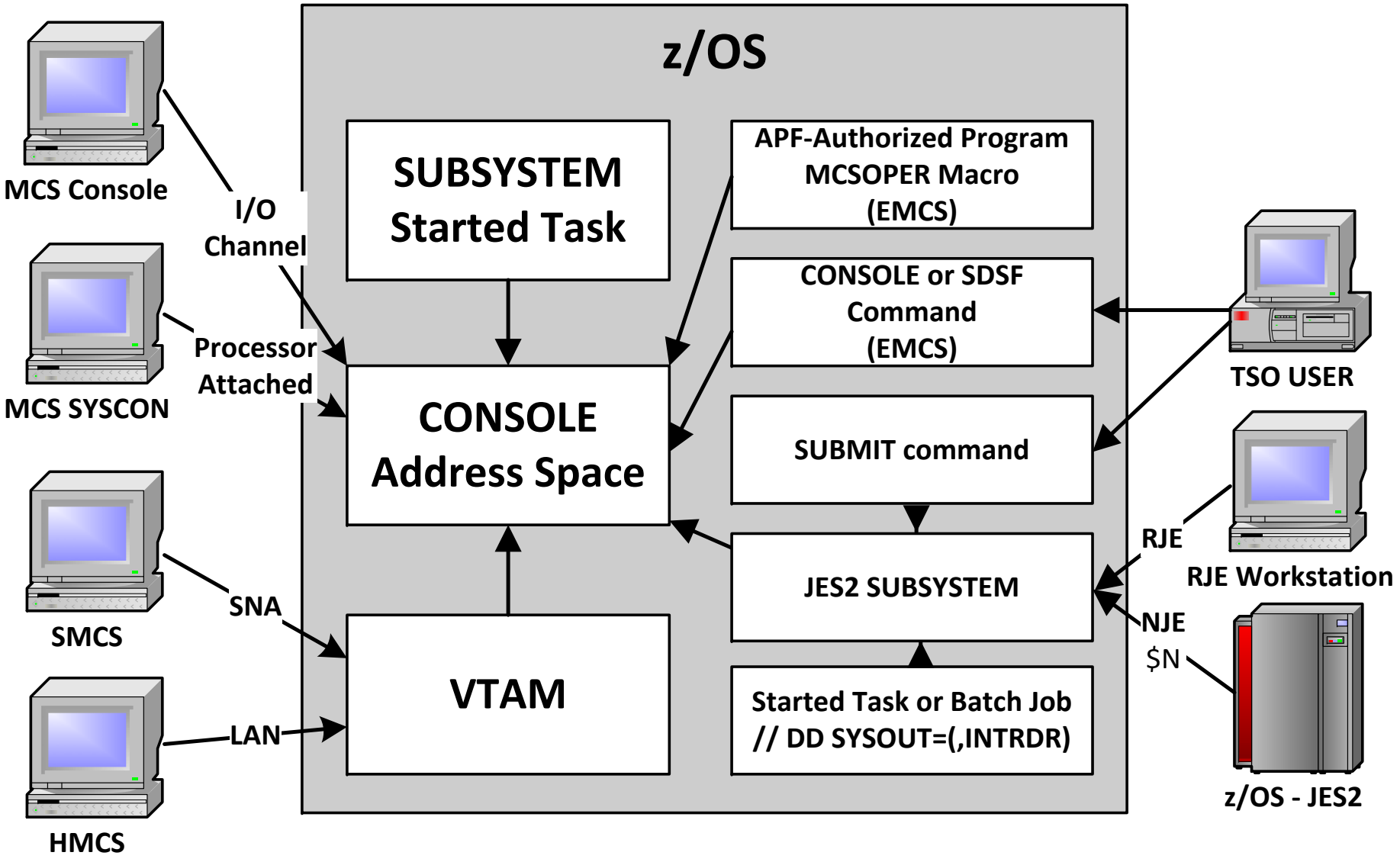
Operator Command Protection Mechanisms

- Physical control of access to console
- Console authorities
- JES2 HASPPARM authorities
- OPERCMDS profiles
- FACILITY CSV-prefixed profiles

Consoles

- MCS - Multiple Console Support (MCS) PARMLIB(CONSOLxx)
  - Physical terminal channel attached to CPU; static device address (DEVNUM)
  - SYSCONS - System Console - MCS console attached to the processor
- SMCS - System Network Architecture (SNA) MCS PARMLIB(CONSOLxx)
  - Physical terminal connected via VTAM; static Logical Unit (LU) name
- HMCS - Hardware Management MCS PARMLIB(CONSOLxx)
  - LAN connection to CPU
- SUBSYSTEM PARMLIB(CONSOLxx)
  - Used by authorized programs; static definition; generally replaced by EMCS
- EMCS - Extended MCS APF-authorized program
  - Defined dynamically using MCSOPER assembly macro
  - Examples - TSO CONSOLE command, SDSF, NetView, and homegrown programs
- Hard Copy console PARMLIB(CONSOLxx)
  - SYSLOG output

Consoles



Consoles - PARMLIB(CONSOLxx)

- Statements and options

INIT

HARDCOPY DEVNUM(SYSLOG | OPERLOG)

DEFAULT LOGON(REQUIRED | OPTIONAL | AUTO)

CONSOLE DEVNUM(*device* | SUBSYSTEM | SYSCONS | SMCS | HMCS)
NAME(*console-name*)
LOGON(REQUIRED | OPTIONAL | AUTO | DEFAULT)
AUTH(INFO | [SYS | IO | CONS] | ALL | MASTER)
TIMEOUT(00 | *nn*)

Ref: z/OS MVS Initialization and Tuning Reference

Consoles - PARMLIB(CONSOLxx) - Sample

```
INIT     AMRF(N)                 /* NO AUTOMATIC MESSAGE RETENTION     */
         CMDDELIM(;)             /* STACKED COMMAND DELIMITER IS ;     */
         CNGRP(00)               /* CONSOLE GROUP MEMBER               */
         CTRACE(CTIOPS00)        /* CTIOPS00 IS THE DEFAULT            */
         LOGLIM(2500)            /* 1000 WTL BUFFERS                   */
         MLIM(5000)              /* 1500 WTO BUFFERS                   */
HARDCOPY CMDLEVEL(CMDS)          /* ALL COMMANDS GO TO HARDCOPY        */
         DEVNUM(SYSLOG,OPERLOG) /*USE SYSLOG AS HARDCOPY              */
         ROUTCODE(ALL)           /* ROUTECODES 1-128 TO HARDCOPY       */
DEFAULT  ROUTCODE(ALL)
         LOGON(AUTO)
         RMAX(400)
         SYNCHDEST(SYNCGRP)
CONSOLE  DEVNUM(D30)
         UNIT(3270-X)
         NAME(&SYSNAME.MSTA)
         AUTH(MASTER)
         MSCOPE(*)
         ROUTCODE(ALL)
CONSOLE  DEVNUM(D40)
         UNIT(3270-X)
         NAME(&SYSNAME.MR)
         AUTH(ALL)
         MSCOPE(*)
         ROUTCODE(1,2,3,4,5,6,7,8,9,10,12,13,14,15,16)
CONSOLE  DEVNUM(SUBSYSTEM)              /* NETVIEW SUBSYS INTERFACE */
         NAME(NETV01)
         AUTH(ALL)
```

Console Control

- Establish an identity for the user at the console and operator command authority

- Control options:
  - Determine whether logon at a console is required
  - Determine who can log on at a specific console
  - Establish the native-MVS authority of the console

Console Logon Control

- Console logon sequence
  - At console command line, enter:

    LOGON

  - System issues prompt:

    LOGON **PASSWORD**

    GROUP **SECLABEL**

  - After entry of ID and password, system issues message:

    IEE185I LOGON *userid* COMPLETE FOR DEVNUM=*devnum*

    CN=*console-name*

  - At command line, enter:

    LOGOFF

  - After logoff, system issues message:

    IEE185I LOGOFF *userid* COMPLETE FOR DEVNUM=*devnum*

    CN=*console-name*

Console Logon Control

- Console logon requirement
  - Defined in PARMLIB(CONSOLxx)
  - Applies to MCS and SMCS consoles only
  - Set using the LOGON(*option*) parameter
  - LOGON is specified in DEFAULT and/or CONSOLE statements
    - DEFAULT LOGON
      - Applies to all consoles unless overridden
      - Optional parameter
    - CONSOLE LOGON
      - Applies to just the one console
      - Overrides the DEFAULT setting
      - Optional parameter

Console Logon Control

- Console logon requirement
  - LOGON(REQUIRED | AUTO | OPTIONAL | DEFAULT)
    - REQUIRED Logon is mandatory, no commands accepted until logon
    - AUTO Console automatically logged on with ID matching its name
    - OPTIONAL Console logon is optional; if no logon, console AUTH active
    - DEFAULT Use DEFAULT statement setting (CONSOLE statement only)
  - With LOGON(REQUIRED), commands may be entered at the Master Console without logging on when RACF is not yet active
  - With LOGON(AUTO)
    - Must define a USERID matching the 'console-name'
    - Must permit this USERID READ access to corresponding CONSOLE 'console-name' profile
    - Can logon with another USERID to temporarily override
  - Default settings when LOGON is not specified in DEFAULT or CONSOLE statement
    - MCS OPTIONAL
    - SMCS REQUIRED

Console Logon Control

- Console logon permission - controls who can log on at console
  - CONSOLE class profiles
  - Resource name - console identifier (e.g., name)
  - Restricts logon to MCS and SMCS consoles
  - Optionally checked for logical consoles
    - CICS - INTERNAL and INSTREAM
  - Logon permission - UACC or PERMIT
    - READ Logon permitted
    - NONE Logon denied
  - Example:
    - RDEFINE CONSOLE CN70 UACC(NONE)
    - PERMIT CN70 CLASS(CONSOLE) ID(OPERGRP) ACCESS(READ)
  - Consider UACC(READE) for consoles in computer room (rely on physical security)

CONSOLE Class CDT Entry

- ID = 68
- POSIT = 107

- MAXLNTH = 8
- FIRST = ANY
- OTHER = ANY
- CASE = UPPER

- DFTRETC = 8
- DFTUACC = NONE
- OPER = NO

- GENLIST = DISALLOWED
- RACLIST = ALLOWED
- RACLREQ = NO

Console Logon Control

- CONSOLE Class - Console Identifier
  - Resource name is the 'console-name' (e.g. PRD1MSTA)
  - Resource name used to also be a 2-digit console number
    - Previously, if no 'console-name' was defined, console's identifier was its initialization sequence number assigned during IPL (e.g., 04)
    - Sequence number was not reliable - identity could change each IPL
    - Sequence number identifiers did not work well with Sysplex
    - Present-day requirement is all consoles must have a 'console-name'
    - Any console number profiles are now obsolete (unless you gave them a 2-digit number as a name)
  - To avoid confusion, IBM recommends you not assign consoles names that might match a physical unit address

Console Command Authority

- Authority level for an individual console - CONSOLxx
  - AUTH(INFO | [SYS | IO | CONS] | ALL | MASTER)
    - INFO — Any informational command (included in all others)
    - SYS — System control command
    - IO — I/O control command
    - CONS — Console control command
    - ALL — SYS, IO, and CONS
    - MASTER — Same as ALL and eligible to be a master console

- Master Console
  - Can only have one Master Console at a time
  - First eligible online MCS console becomes the Master Console
    - Can be switched to another console with AUTH(MASTER) after the IPL
  - Used to communicate with system until other consoles are initialized
  - Can enter commands prior to RACF initialization regardless of LOGON
  - Can enter default password for certain RACF RVARY command operations

Console Command Authority

- Authority level for EMCS Consoles
  - Governed by the MCSOPER macro and user OPERPARM segment

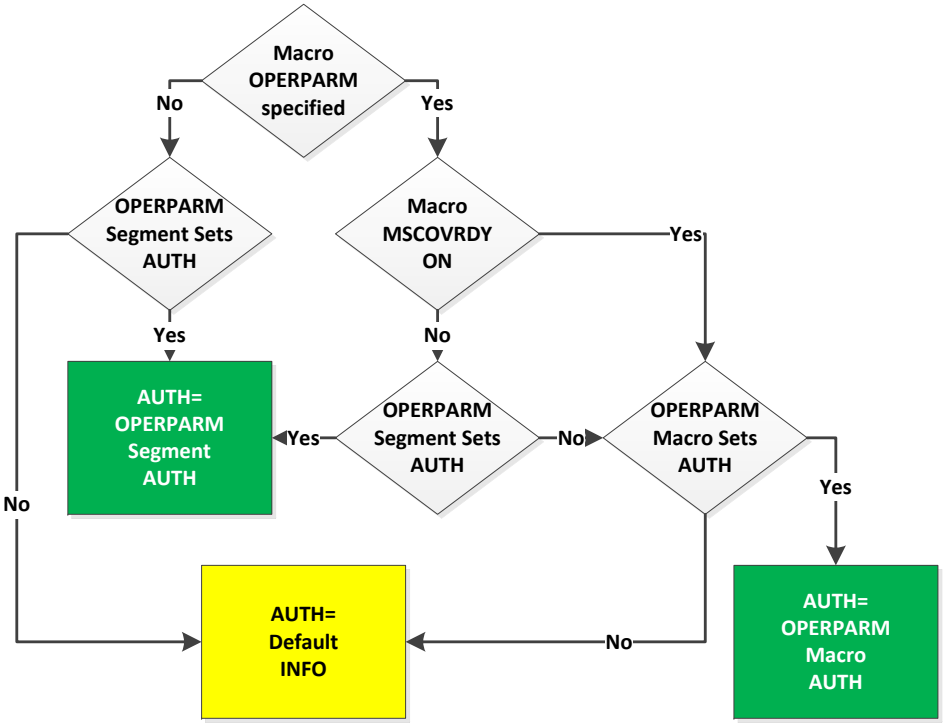
```
MCSOPER  REQUEST=ACTIVATE,
             NAME=console-name,              (Required)
             OPERPARM=parm-area-addr,        (Optional)
             CONSID=id-area,
             TERMNAME=vtam-luname
```

  - To use a console with a given NAME, even a console matching the user's own USERID, the user needs READ access to resource MVS.MCSOPER.*console-name* in the OPERCMDS class
    - To facilitate users' use of console names matching their own USERID and reduce the number of OPERCMDS profiles, implement the following Global Access Table Entry

```
RDEF GLOBAL OPERCMDS OWNER(owner)
RALT GLOBAL OPERCMDS ADDMEM(MVS.MCSOPER.&RACUID*/READ)
```

Console Command Authority

- Authority level for EMCS Consoles
  - OPERPARM=*parm-area-addr* operand on MCSOPER macro
    - Optional - specifies location of set of parameters, including AUTH
    - If not specified, AUTH is set to the value in AUTH operand in OPERPARM segment of ID matching console-name
    - If specified, depends on MCSOVRDY bit in parm-area-addr
      - If MCSOVRDY is on (OI MCSOFLAG,MCSOVRDY), AUTH is set to value specified in parm-area-addr
      - If MCSOVRDY is off, AUTH is set to (in order of precedence):
        - Value in AUTH operand in OPERPARM segment of ID matching console-name
        - If no OPERPARM AUTH, then the AUTH value specified in parm-area-addr
    - If no AUTH value is set, defaults to INFO



Console Command Authority

- USER profile OPERPARM segment fields
  - ALTGRP(alternate-console-group)
  - **AUTH(INFO | MASTER | ALL | SYS | IO | CONS)**
  - AUTO(YES | NO)
  - CMDSYS(system-name | *)
  - DOM(NORMAL | ALL | NONE)
  - HC(YES | NO)
  - INTIDS(YES | NO)
  - KEY(searching-key)
  - LEVEL(NB | ALL | R | I | CE | E | IN)
  - LOGCMDRESP(SYSTEM | NO)
  - MFORM(message-format)
  - MIGID(YES | NO)
  - MONITOR(JOBNAMES | JOBNAMEST | SESS | SESST | STATUS)
  - MSCOPE(system-names | * | *ALL)
  - ROUTCODE(ALL | NONE | routing-codes)
  - STORAGE(amount)
  - UD(YES | NO)
  - UNKNIDS(YES | NO)

```
LU RSHTEST OPERPARM

OPERPARM INFORMATION
--------------------
STORAGE= 00000
AUTH= ALL
```

TSO CONSOLE Command

- Use controlled by TSOAUTH resource CONSOLE
- Console-name defaults to user's own USERID
- User can change console-name with NAME(*console-name*) operand

  CONSOLE NAME(*consname*)

- User must be permitted to use the console-name

  OPERCMDS MVS.MCSOPER.*consname* - READ

- If a command is not protected by an OPERCMDS profile, user's command authority is determined by AUTH parameter associated with console-name
  - If set to the user's own USERID - uses user's OPERPARM AUTH
  - If set to another USERID - uses other user's OPERPARM AUTH
  - If set to the name of inactive MCS or SMCS - uses console's CONSOLxx AUTH
  - Restrict what console-names users may specify; perhaps to only their own USERID

Operator Commands Entered via JES2

- JES Ports of Entry (POEs)
  - Internal Reader (e.g., DD SYSOUT=(,INTRDR))
  - Remote Job Entry (RJE)
  - Network Job Entry (NJE)
  - Card Reader

- Job Stream

```
/*$VS,'mvs-system-commands'
/*$jes2-commands
//jobname  JOB statement
/*jes2-routing-commands
//   mvs-system-commands
```

Related HASPPARMs

```
INTRDR, RDR
INTRDR, RDR


JOBCLASS
```

- Internal Reader - INTRDR Parms

  AUTH = (JOB= NO | YES , DEVICE = NO | YES , SYSTEM = NO | YES)

- Reader - RDRnn Parms

  AUTH = (JOB= NO | YES , DEVICE = NO | YES , SYSTEM = NO | YES)

Operator Commands Entered via JES2

- JOBCLASS(v) Parms - Batch Jobs
- JOBCLASS(STC) Parms - Started Tasks
- JOBCLASS(TSU) Parms - TSO Logons

COMMAND = VERIFY | IGNORE | DISPLAY | EXECUTE

AUTH = ALL | CONS | INFO | IO | SYS

- AUTH MVS Commands

SYS	- System
CONS	- Console
IO	- Input/Output
INFO	- Display

COMMAND Actions

VERIFY	- Confirm with Operator
IGNORE	- Do not Execute
DISPLAY	- Console Display and Execute
EXECUTE	- Execute with no Display

- OPERCMDS protection for a command supersedes AUTH authority

Operator Commands Entered via JES2

- Network Job Entry (NJE) - NODE(nnnnn(-nnnnn)) Parms

  AUTH = (JOB = YES | NO , DEVICE = YES | NO , NET = NO | YES , SYSTEM = YES | NO)

  - NJE nodes act as local consoles
  - If NET=NO, SYSTEM = is ignored
  - If all are set to NO, INFO commands can still be sent
  - Route command format: $N *node*, '*command*'

Operator Commands Entered via JES2

- Network Job Entry (NJE) - NODE(nnnnn(-nnnnn)) Parms (continued)
  - Can restrict commands using NODES class 'RUSER' profile and OPERCMDS
    - Define NODES profiles *submitting-nodename*.RUSER.*submitting-nodename* UACC(READ)
    - Define FACILITY profile NJE.*submitting-nodename*
      - If no matching FACILITY profile exists, authority reverts to NODE AUTH parameters
    - Define USERID matching *submitting-nodename*
      - Specify RESTRICTED and NOPASSWORD (to make PROTECTED)
    - If no matching USERID or if USERID is REVOKED, operator commands fail
    - Permit NJE nodename USERID READ permission to JESINPUT *nodename* profile if protected
    - Permit NJE nodename USERID permission to OPERCMDS profiles as desired
  - To block commands from other foreign NJE NODES
    - Define NODES profile *.RUSER.* UACC(NONE)
    - Define FACILITY profiles NJE.*all-foreign-jes-nodenames*
    - Define *foreign-jes-nodenames* as IDs and REVOKE them

Operator Commands Entered via JES2

- RJE Workstation command entry
  - To enable use of operator command ...
    - RJE workstation must be configured to transmit a workstation sign-on with a USERID and password

      (BSC) /*SIGNON RMTnnnn linepswd newpswd rmtpswd

      (SNA) LOGON APPLID(JES2) LOGMODE(name) DATA(RMTnnnn,linepswd,rmtpswd,newpswd)
    - Define FACILITY profile RJE.*rje-workstation-name* (e.g., RJE.RMT1)
    - Define USERID matching *rje-workstation-name* (e.g., RMT1)
      - Set PASSWORD to match that used in RJE transmit sign-on with NOEXPIRE
      - Make ID PASSWORD NOINTERVAL
    - If no matching USERID or if USERID is REVOKED, RJE sign-on fails
    - Permit RJE workstation USERID READ permission to JESINPUT *rje-workstation-name* profile if protected
    - Permit RJE workstation USERID permission to OPERCMDS profiles as desired
    - Last Access and Connect Dates are not updated by workstation sign-on and misleadingly appear to be inactive

Operator Command Protection

- The authority to execute operator commands is governed by:
  - OPERCMDS profiles, or
  - AUTH parameter on the console, which governs use when:
    - There is no protecting OPERCMDS profile, or
    - There is no RACF user logged on at a physical console
  - AUTH parameter on JES POE, which governs use when:
    - There is no protecting OPERCMDS profile, or
    - There is no RACF user logged on for an NJE connection

- OPERCMDS Resources
  - MVS commands
  - JES subsystem commands
  - RACF subsystem commands
  - Other subsystem commands

OPERCMDS Class - CDT Entry

- ID = 63
- POSIT = 112
- MAXLNTH = 39
- FIRST = ANY
- OTHER = ANY
- CASE = UPPER
- DFTRETC = 4
- DFTUACC = NONE
- OPER = NO
- GENLIST = DISALLOWED
- RACLIST = ALLOWED
- RACLREQ = YES

OPERCMDS Profiles

- Resource name is based on subsystem, command, and operands
  - Subsystem prefix - MVS, JESx, and others - first qualifier
  - Example: V CN(*console-name*),AUTH=ALL
  - Resource: MVS.VARY.CN UPDATE
    MVS.VARYAUTH.CN CONTROL
- JES resource names do not include target of the command
  - Cancel job: $C J 2534
  - Resource: JES2.CANCEL.BAT UPDATE (no reference to job #)
- Access levels are generally based on sensitivity of function
  - READ Display Equivalent to CONSOLE AUTH(INFO)
  - UPDATE Manage work Equivalent to CONSOLE AUTH(SYS,IO,CONS)
  - CONTROL Manage system Equivalent to CONSOLE AUTH(MASTER)

OPERCMDS Profiles - Examples

- Commands to manage system availability
  - Reconfigure I/O — ACTIVATE IODF=03,CFID=COMPUT22 — MVS.ACTIVATE
  - Cancel TSO users — CANCEL U=RSHUSER — MVS.CANCEL.TSU.**
  - Force started tasks — FORCE CICSTASK,ARM — MVS.FORCE*.STC.**
  - Quiesce the system — QUIESCE — MVS.QUIESCE
- Commands to reconfigure system software
  - Change PARMLIBs — SETLOAD 03,PARMLIB,DSN=RSH.PARMLIB — MVS.SETLOAD.LOAD
  - Add APF library — SETPROG APF,ADD,DSN=SYS1.DATA,VOL=RV1 — MVS.SETPROG
  - Start tasks — START LLA,SUB=MSTR — MVS.START.STC.**
- Commands to alter workflow
  - Start Initiators — $S I14 — JES%.START.INITIATOR
  - Start Spool Offload — $S OFFLOAD1,TYPE=TRANSMIT — JES%.START.DEV
- Commands to manage network
  - Add connections — $ADD CONNECT,NODEA=BOS,MEMBA=1,NODEB=SEA,MEMBB=2 — JES%.ADD.CONNECT
  - Add lines — $ADD LINE=66,UNIT=SNA — JES%.ADD.LINES
  - Start lines — $S LINE66 — JES%.START.LINE

Dynamic Configuration Changes

- Control who can make dynamic changes to LLA, APF, LPA, Exits, and Linklist

- OPERCMDS - Protect operator commands (UPDATE access)
  - SET command MVS.SET.PROG
  - SETPROG command MVS.SETPROG

- FACILITY - Protect use of CSV-prefixed MACROs (UPDATE access)
  - Access is only required if the user is not APF-authorized
  - CSVAPF.library-name
  - CSVAPF.MVS.SETPROG.FORMAT.[DYNAMIC | STATIC]
  - CSVDYLPA.[ADD | DELETE].modname
  - CSVDYNEX.LIST (READ access)
  - CSVDYNEX.exitname.[DEFINE | UNDEFINE | ATTRIB | CALL | RECOVER | modname]
  - CSVDYNL.linklstname.[ADD | DEFINE | DELETE | ACTIVATE | UNDEFINE]
  - CSVDYNL.linklstname. TEST (READ access)
  - CSVLLA.lladataset

RACF Subsystem - Console Commands

- Requires RACF subsystem
- Execution sequence at console

  LOGON *userid* - will be prompted for password

  #racf-command - include prefix character (e.g., #)

  LOGOFF
- Logged-on ID is shown at bottom of console display
- Prefix character determined by PARMLIB(IEFSSNxx) INITPARM operand on RACF subsystem definition

```
SUBSYS SUBNAME(RACF)
  INITRTN(IRRSSI00) INITPARM('#')
```

- If no prefix is specified, the prefix defaults to the RACF subsystem name plus a blank - e.g., 'RACF '

```
RACF LISTUSER IBMUSER
```

RACF Subsystem - Console Commands

- Can optionally register prefix with Command Prefix Facility (CPF) to ensure it is reserved
  - INITPARM('*prefix*,*scope*')*scope* = M or X
    - M - Reserve within system image
    - X - Reserve within Sysplex (only one subsystem in Sysplex can use)
  - If registered, can be listed with operator command:

    DISPLAY OPDATA,PREFIX

- Commands are protected by OPERCMDS profiles
  - *racf-subsystem-name.racf-command*
    - READ Execute SETROPTS LIST and all other RACF commands (e.g., PERMIT)
    - UPDATE Execute SETROPTS with parameters other than LIST (e.g., REFRESH)
    - Normal RACF authority (e.g., SPECIAL) is also required

- Periodically test to ensure other subsystems do not interfere with command execution

RACF Subsystem - Console Commands

- Control who can manage RACF subsystem and RRSF (READ access)
  - DISPLAY *racf-subsystem*.DISPLAY.SIGNON
  - RESTART *racf-subsystem*.RESTART
  - SET *racf-subsystem*.SET.parameter (e.g., LIST, INCLUDE)
  - SIGNOFF *racf-subsystem*.SIGNOFF
  - STOP *racf-subsystem*.STOP
  - TARGET *racf-subsystem*.TARGET.parameter (e.g., LIST, NODE)

Access Permission Guidelines

- All MVS and JES commands
  - Master console operators
  - System programmers
  - Automation tasks
- Job management commands
  - Production control
  - Automation tasks
  - End-users - own jobs
- Dynamic software change commands
  - Automation tasks
  - System programmers
- Initiator control commands
  - Scheduling
  - Production control
  - Performance and tuning
  - Automation tasks
- Printer control commands
  - Local printer operators
  - Remote printer operators
  - Production control
- RACF commands
  - Security staff
  - RACF system programmers

Implementation Suggestions

- Identify command “owner” to approve protection mechanisms
- Create an authority matrix to fit your organization
- Assign individual USERIDs to started tasks for use in granting appropriate access
- Initially, log and review existing usage
  - SETROPTS LOGOPTIONS(ALWAYS(OPERCMDS))
- Check for started tasks that submit commands on behalf of users and implement compensating controls (e.g., OPS/MVS, ZEKE, NETVIEW, CA-7)
- Consider assigning UACC(READ) for all display commands
  - MVS.DISPLAY.**
  - JES%.DISPLAY.**

Implementation Suggestions

- Restrict the entry of MVS commands via JES devices using the $VS command
  - JES%.VS
- Unknown commands - RACF SAG UACC guidelines
  - MVS.UNKNOWN UACC(READ) AUDIT(ALL)
  - JES%.UNKNOWN UACC(NONE) AUDIT(ALL)
  - *racf*.UNKNOWN UACC(NONE) AUDIT(ALL)
  - *subsystem.*UNKNOWN UACC(READ | NONE) AUDIT(ALL)
- Restrict use of certain commands to specific physical consoles in the computer room
  - JES%.HALT.**
  - MVS.FORCE*.**
  - MVS.HALT.**
  - MVS.QUIESCE
  - MVS.VARYAUTH.CN
  - MVS.VARYLOGON.CN

Implementation Suggestions

- Consider using RACFVARS variables to group started task PROC names or sets of related OPERCMDS commands

```
RACFVARS  &NETSTC  ADDMEM( NETVIEW  TCPIP  FTPSERVE  HTTPSRV )
        ... either ...
OPERCMDS  MVS.CANCEL.STC.&NETSTC
OPERCMDS  MVS.FORCE.STC.&NETSTC
OPERCMDS  MVS.FORCEARM.STC.&NETSTC
OPERCMDS  MVS.MODIFY.STC.&NETSTC
OPERCMDS  MVS.START.STC.&NETSTC
OPERCMDS  MVS.STOP.STC.&NETSTC
        ... or ...
RACFVARS  &ACTION  ADDMEM( CANCEL FORCE FORCEARM MODIFY START STOP )
OPERCMDS  MVS.&ACTION.STC.&NETSTC
```

Implementation Suggestions

- Include a backstop for all subsystem names now in use and a ** backstop with no permissions to block access to newly introduced resources
  - MVS.**
  - JES%.**
  - *racf*.**
  - ** UACC(NONE) No permissions

- For SDSF users, permit access using WHEN(CONSOLE(SDSF))
  - Requires CONSOLE class to be active

- Remember that lack of an OPERCMDS backstop profile will result in fallback to your MVS console AUTH authority

Common Findings - Consoles and OPERCMDS

- LOGON not set to AUTO or REQUIRED in CONSOLxx definitions
- OPERCMDS resources not fully protected
- Excessive access granted to commands that can alter the system configuration, especially those affecting APF library authorization
- System shutdown commands not properly restricted
- Access granted to very broad generics (e.g., MVS.**)
- OPERCMDS MVS.MCSOPER.* defined with default access of READ
- WHEN(CONSOLE(SDSF)) restrictions not used
- Security staff console logons and RACF command entry tests not performed

Operator Command References

- Security Server RACF Security Administrator's Guide

- MVS Initialization and Tuning Reference
- MVS Planning: Operations
- MVS System Commands

- Authorized Assembler Services Guide
- Authorized Assembler Services Reference (Volume 3)

- JES2 Commands
- JES2 Initialization and Tuning Guide
- JES2 Initialization and Tuning Reference

- JES3 Commands
- JES3 Initialization and Tuning Guide
- JES3 Initialization and Tuning Reference

- RSH RACF Tips newsletters and surveys - www.rshconsulting.com