RSH CONSULTING

SDSF and RACF

RSH RACF Forum
November 2023

RSH Consulting - Robert S. Hansel

RSH CONSULTING

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
- www.linkedin.com/company/rsh-consulting-inc.

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

© 2023 RSH Consulting, Inc. All Rights Reserved.

System Display and Search Facility (SDSF)

- SDSF is a utility for monitoring and managing a z/OS system
  - Manage system components (e.g., start/stop initiators; control the network)
  - Monitor, view, and cancel Started Tasks
  - Monitor, view, cancel, hold, and release jobs
  - View, cancel, hold, and print output
  - View the system log
  - View and manage Healthchecks
  - View system resources (e.g., APF-authorized libraries)
  - Enter system commands
- SDSF functions as an EMCS console with AUTH(MASTER)
- SDSF can optionally be implemented as a server with a Started Task
- SDSF server has a companion address space SDSFAUX that handles data gathering for many Operator Displays (ODSP)
- SDSF can be invoked as a TSO command and in batch, REXX EXECs, and Java

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF

- SDSF configuration parameters - ISFPARMS
  - Govern base options, panel displays, and, optionally in z/OS 2.4(-), security
  - ISFPARMS load module - assembler macros - linked into the SDSF load library (old)
  - ISFPARMS statements - defined in PARMLIB(ISFPRMxx) - used by an SDSF server
    - Multiple SDSF servers can exist, each with a different server name and ISFPRMxx member
- RACF - SDSF | GSDSF classes
  - Profiles control SDSF functions, commands, and fields
  - RACLIST REQUIRED class
- SDSF always calls RACF for authorization for every resource access
- If RACF issues an RC=4 (class not active or no profile found), …
  - z/OS 2.4(-), SDSF uses security parameters in ISFPARMS to determine access
  - z/OS 2.5(+), SDSF denies access (ISFPARMS security parameters are ignored)
  - ISFPARMS CONNECT statement AUXSAF setting may allow access

© 2023 RSH Consulting, Inc. All Rights Reserved.

ISFPARMS - Macros | Statements

- ISFPMAC | OPTIONS - Global initialization options
- ISFGRP | GROUP - Groups - users, authority, options *
- ISFNTBL | NTBLENT and NTBL - Tables of entities (users, destinations) *
- ISFFLD | FLDENT and FLD - Customized displays
- ISFTR | TRDEF and TRTAB - Language, code page
- | PROPLIST and PROPERTY - Customizations
- | CONNECT - Auxiliary server (SDSFAUX) options

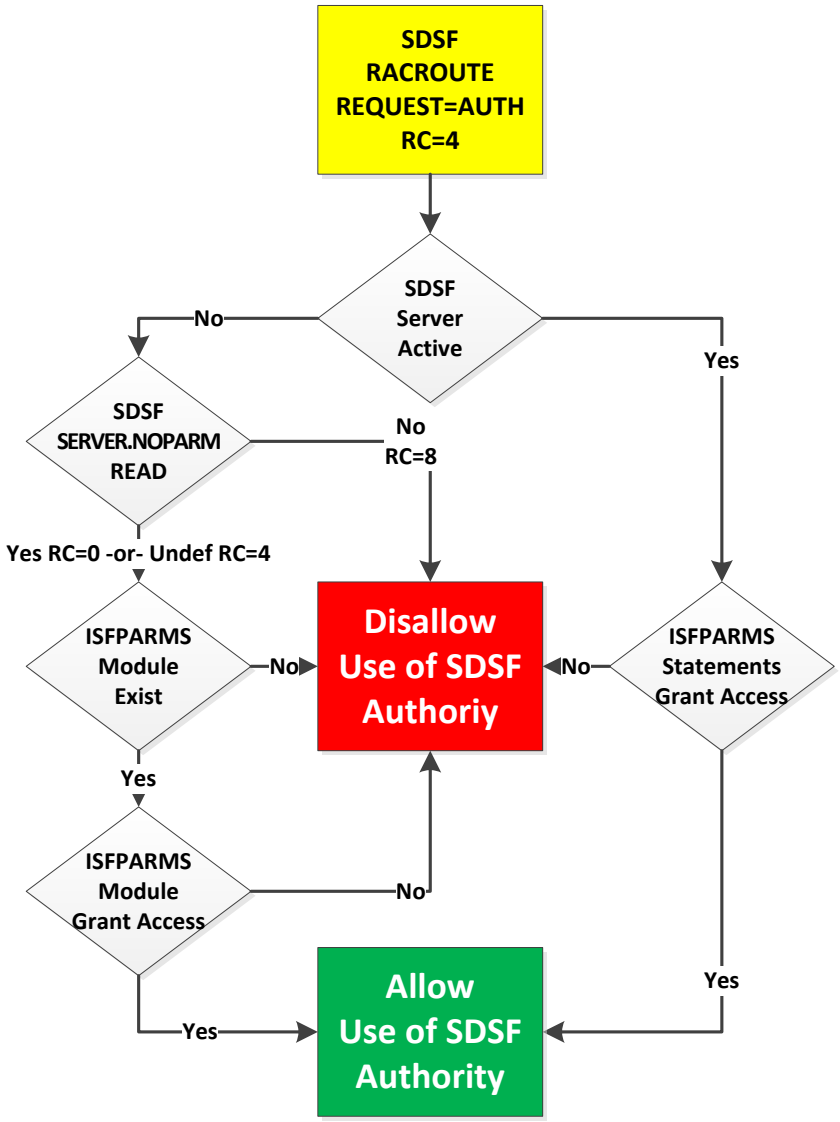
* Includes security options replaceable by RACF

- RACF controls only supersede the security related parameters; non-security parameters are still used and needed

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF - RC=4 Processing

- z/OS 2.4(-), if RACF responds with a Return Code of 4 (RC=4), SDSF uses ISFPARMS for controlling access in the following order of precedence
  - If the SDSF server is active, use ISFPARMS statements in PARMLIB(ISFPRMxx)
  - If the SDSF server is not active, ...
    - If SDSF resource SERVER.NOPARM is not protected, use ISFPARMS load module (if exists)
    - If a profile for SDSF resource SERVER.NOPARM is defined, ...
      - If the user has READ access, use ISFPARMS load module (if exists)
      - If the user does not have READ, SDSF access is denied
    - If ISFPARMS load module does not exist, SDSF access is denied
- z/OS 2.5(+), RC=4 denies access



© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF - CONNECT AUXSAF

- Handling of RC=4 is also determined by ISFPARMS CONNECT statement parameter AUXSAF
  - AUXSAF(FAILRC4) Fail request (Default)
  - AUXSAF(NOFAILRC4) Allow request

- z/OS 2.4(-), AUXSAF governs access only for resources processed by SDSFAUX
  - ISFPARMS governs access for resources not processed by SDSFAUX and without regard for the AUXSAF setting
  - Commonly set to NOFAILRC4 at installations that had not yet implemented SDSF class profiles for SDSFAUX resources

- z/OS 2.5(+), AUXSAF governs access for all resources and will allow access to any unprotected resource (e.g., JESSPOOL, SDSF)

- Recommendation - set AUXSAF to FAILRC4

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF WHO, SET, SECTRACE, and ULOG

```
COMMAND INPUT ===> WHO
USERID=RSH,PROC=DBPROCCG,TERMINAL=TCP00004,GRPINDEX=1,GRPNAME=ISFSPROG,
MVS=z/OS 02.05.00,JES=z/OS 2.5,SDSF=HQX77D0,ISPF=7.5,RMF/DA=HSF,SERVER=YES,
SERVERNAME=SDSF,JESNAME=JES2,MEMBER=S0W1,JESTYPE=JES2,SYSNAME=S0W1,
SYSPLEX=SVSCPLEX,COMM=NOTAVAIL,COMMX=ENABLED,JOBID=TSU06363,XCFGROUP=SVSCJES2,
SESSID=1,NUMSESS=1


COMMAND INPUT ===> SET DISPLAY ON
PREFIX=*  DEST=(ALL)  OWNER=RSH  SYSNAME=


COMMAND INPUT ===> SET SECTRACE ON  -or-  WTP          (ON goes to ULOG, WTP to SYSLOG)
COMMAND INPUT ===> ULOG              (Requires READ access to ISFCMD.ODSP.ULOG.jes-name)
 SDSF ULOG  CONSOLE RSH                              LINE 0       COLUMNS 02- 81
 COMMAND INPUT ===> RIGHT 71                                    SCROLL ===> PAGE
******************************** TOP OF DATA ***********************************
SAFRC=0 ACCESS=READ CLASS=SDSF RESOURCE=ISFCMD.ODSP.SYSLOG.JES2 Reqstor=ISFUNCTN
SAFRC=0 ACCESS=READ CLASS=SDSF RESOURCE=ISFCMD.DSP.STATUS.JES2 Reqstor=ISFUNCTN
SAFRC=0 ACCESS=UPDATE CLASS=SDSF RESOURCE=ISFATTR.JOB.PRTY Reqstor=ISFUATTR
SAFRC=0 ACCESS=UPDATE CLASS=SDSF RESOURCE=ISFATTR.JOB.CLASS Reqstor=ISFUATTR
SAFRC=0 ACCESS=UPDATE CLASS=SDSF RESOURCE=ISFATTR.JOB.SYSAFF Reqstor=ISFUATTR
SAFRC=0 ACCESS=READ CLASS=SDSF RESOURCE=ISFAUTH.DEST.LOCAL.DATASET.JESMSGLG Reqs
SAFRC=0 ACCESS=READ CLASS=JESSPOOL RESOURCE=SVSCJES2.RSH.RSHDSMON.JOB05617.D0000
```


© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF - RACF Classes

- SDSF _ GSDSF - SDSF functions, commands, and overtypeable fields
- JESSPOOL - Jobs, Started Tasks, and output
- OPERCMDS - Operator commands
- WRITER - Printer management
- LOGSTRM - Log streams
- XFACILIT - Health Checks (HZS-prefix)
- CONSOLE - Conditional access

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Connection

- z/OS 2.4(-), to use many newer SDSF functions primarily provided by the SDSFAUX address space, users must "connect" to the SDSF server

- To connect, access is required to the following resource

  SDSF ISF.CONNECT.*system* READ

- To facilitate viewing information for all systems in a Sysplex, common practice is to define a profile like ISF.CONNECT.* and give UACC or ID(*) READ access

- In addition to connect access, permission to the individual function is also required

- z/OS 2.5(+), access to ISF.CONNECT.*system* is required to use SDSF on a specific system

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Group Assignment

- SDSF Groups
  - SDSF parameters include definitions for Groups (GROUP or ISFGRP)
  - Group definitions specify display attributes, and in z/OS 2.4(-), group membership and access authorities
  - A user must be assigned an SDSF Group to be permitted to use SDSF
  - The SDSF "WHO" command displays a user's SDSF Group (troubleshooting aid)

- Each SDSF Group has a name
  - Statement: GROUP NAME(*group-name*)
  - Macro: *group-name* ISFGRP
  - If an SDSF group is not assigned a name, SDSF generates a name of ISF*nnnnn*, where '*nnnnn*' is the group's sequence number as it appears in the ISFPARMS
    - A group's generated name can change if GROUP statements are added, deleted, or rearranged in ISFPARMS
  - Recommendation - Assign a NAME to every group

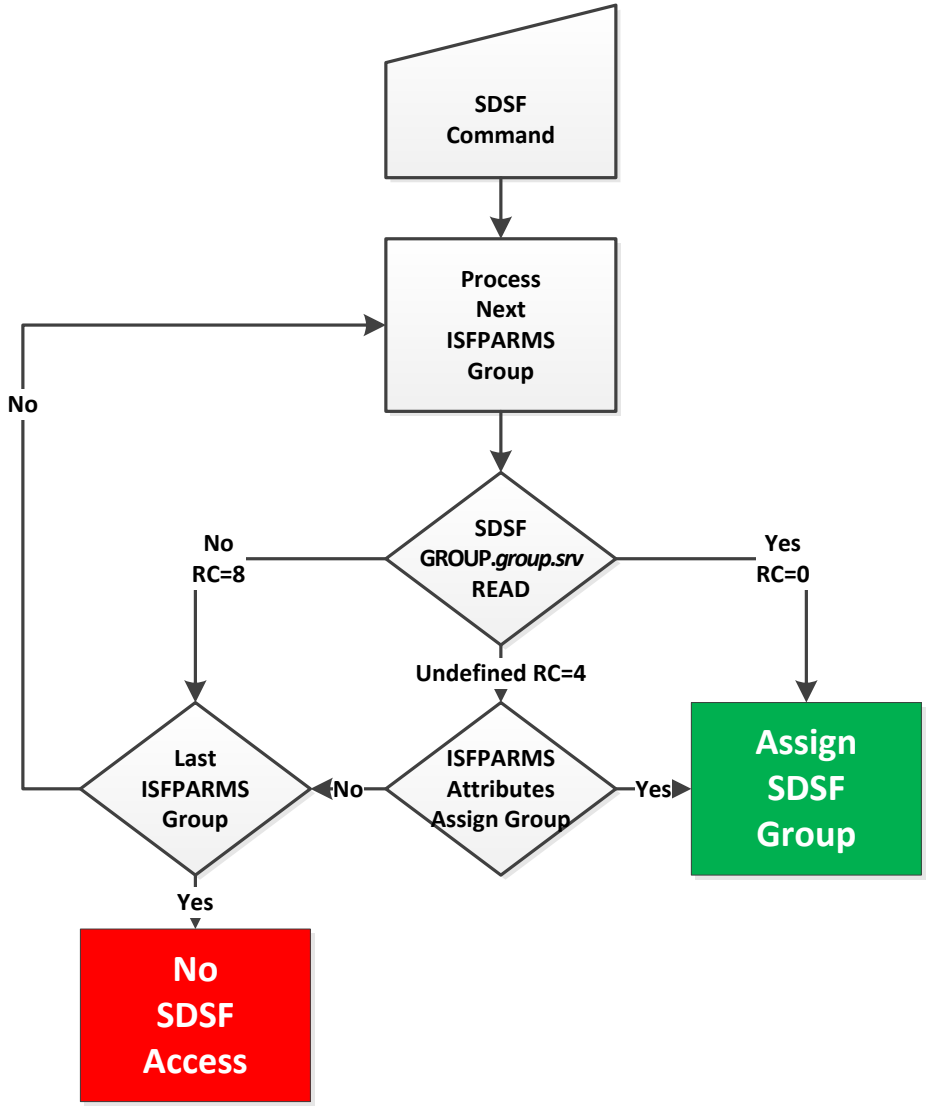
© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Group Assignment

- Upon entry, SDSF attempts to assign a group to a user
  - Assignment is made by checking the user's authority to each SDSF group in the sequence they appear in the ISFPARMS
  - SDSF first calls RACF for group assignment authorization

    SDSF GROUP.*group-name.server-name* READ

    (RACROUTE LOG=NONE)
  - z/OS 2.4(-), if RACF RC=4, SDSF checks ISFPARMS parameters TSOAUTH, IUID, XUID, ITNAME, XTNAME, ILPROC, and XLPROC in ISFPARMS for user assignment
  - z/OS 2.5(+), if RACF RC=4, SDSF checks AUXSAF for FAILRC4 | NOFAILRC4
  - The first group the user is authorized to use is assigned (do not use WARN mode)
  - If the user is not authorized to any group, access to SDSF is denied



© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Commands

- SDSF commands govern the use of panels, filters, and options
  - SDSF ISFCMD.*category.option*[.*jes-name*] READ
  - ISFCMD *Categories*
    - ISFCMD.DSP.*option* End-User Display
    - ISFCMD.FILTER.*option* Display Filtering
    - ISFCMD.MAINT.*option* Maintenance
    - ISFCMD.ODSP.*option* Operator Display
    - ISFCMD.OPT.*option* Option
- Upon entry, SDSF determines what DSP and ODSP commands (i.e., panels) a user is permitted to use and builds the user's Primary Option Menu based on what options are authorized
  - SDSF calls RACF for authorization to every individual command

    SDSF ISFCMD.[DSP | ODSP].*option* READ (RACROUTE LOG=NONE)
  - If RACF issues RC=4 …
    - z/OS 2.4(-), SDSF looks at parameter AUTH in ISFPARMS
    - z/OS 2.5(+), access is denied unless AUXSAF is set to NOFAILRC4
  - Do not use WARNING on profiles for DSP or ODSP resources

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Primary Options Menu Panel

```
SDSF MENU V2R5M0     SVSCPLEX  S0W1                        LINE 1-18 (73)
COMMAND INPUT ===>                                          SCROLL ===> PAGE
PREFIX=*  DEST=(ALL)  OWNER=++++*  SYSNAME=
NP    NAME      Description              Group     Status
      DA        Active users             Jobs
      I         Input queue              Jobs
      O         Output queue             Output
      H         Held output queue        Output
      ST        Status of jobs           Jobs
      JG        Job groups               JES
      SYM       System symbols           System
      LOG       System log               Log
      SR        System requests          Log
      MAS       Members in the MAS       JES
      JC        Job classes              JES
      SE        Scheduling environments  WLM
      RES       WLM resources            WLM
      ENC       Enclaves                 WLM
      PS        Processes                OMVS
      SYS       System information       System
```

DA ISFCMD.DSP.ACTIVE.*jes-name*

LOG ISFCMD.ODSP.SYSLOG.*jes-name*

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Primary Options Menu Panel

```
SDSF MENU V2R5M0    SVSCPLEX  S0W1                        LINE 17-32 (73)
COMMAND INPUT ===>                                          SCROLL ===> PAGE
PREFIX=*  DEST=(ALL)  OWNER=++++*  SYSNAME=
NP    NAME      Description              Group     Status
      ENQ       Enqueues                 System
      ENQC      Enqueue contention       System
      ENQD      Enqueued data sets       Sysplex
      DYNX      Dynamic exits            System
      AS        Address space memory     Jobs
      INIT      Initiators               JES
      PR        Printers                 JES
      PUN       Punches                  JES
      RDR       Readers                  JES
      LINE      Lines                    Network
      NODE      Nodes                    Network
      SO        Spool offload            JES
      SP        Spool volumes            JES
      NS        Network servers          Network
      NC        Network connections      Network
      RM        Resource monitor         JES
```


© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Primary Options Menu Panel

```
SDSF MENU V2R5M0    SVSCPLEX  S0W1                        LINE 33-48 (73)
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
     SSI      Subsystem information    System
     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
```


© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Primary Options Menu Panel

```
SDSF MENU V2R5M0    SVSCPLEX  S0W1                        LINE 49-64 (73)
COMMAND INPUT ===>                                          SCROLL ===> PAGE
PREFIX=*  DEST=(ALL)  OWNER=++++*  SYSNAME=
NP   NAME     Description               Group    Status
     NA       Network activity          Network
     DEV      Device activity           Devices
     EMCS     Extended consoles         Sysplex
     BPXO     OMVS options              OMVS
     LPD      Link pack directory       System
     XCFM     XCF groups and members    Sysplex
     WLM      WLM policy data           WLM
     SRVC     Service classes           WLM
     REPC     WLM report classes        WLM
     RGRP     WLM resource groups       WLM
     WKLD     WLM workloads             WLM
     RMA      Resource monitor alerts   JES
     JES      Job entry subsystems      JES
     JRI      JES resource information  JES
     JRJ      JES resource by job       JES
     LLS      Link list sets            System
```


© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Primary Options Menu Panel

```
SDSF MENU V2R5M0    SVSCPLEX  S0W1                          LINE 65-73 (73)
COMMAND INPUT ===>                                          SCROLL ===> PAGE
PREFIX=*  DEST=(ALL)  OWNER=++++*  SYSNAME=
NP    NAME      Description               Group    Status
      MEM       Memory contents           Memory
      CFD       Couple data sets          Sysplex
      SVC       SVC routines              System
      SYSP      System parameters         System
      CS        Common storage subpools   Memory
      PC        PC routines               System
      AD        Address space diagnostic  Jobs
      ULOG      User session log          Log
      HELP      SDSF help facility        SDSF
```


© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Primary Menu Command Panels

- Each command on the Primary Menu displays a unique resource panel

```
SDSF HELD OUTPUT DISPLAY ALL CLASSES LINES 17,027      LINE 1-16 (74)
 COMMAND INPUT ===>                                      SCROLL ===> PAGE
NP   JOBNAME  JobID    Owner    Prty C ODisp Dest                Tot-Rec  Tot-
      RSHAPPL  JOB04227 RSH       144 H HOLD  LOCAL                   220
      RSHAPPL  JOB04228 RSH       144 H HOLD  LOCAL                   311
      RSHAPPL  JOB04229 RSH       144 H HOLD  LOCAL                   152


SDSF INITIATOR DISPLAY  S0W1                           LINE 1-15 (20)
COMMAND INPUT ===>                                       SCROLL ===> PAGE
NP     ID Status       Classes  JobName  Stepname ProcStep JobID    C ASID ASID
        1 INACTIVE     KAB74                                        27 001B
        2 INACTIVE     L74HAB                                       46 002E
        3 INACTIVE     74AB                                         47 002F


SDSF JOB CLASS DISPLAY ALL CLASSES                     LINE 1-15 (38)
COMMAND INPUT ===>                                       SCROLL ===> PAGE
NP   CLASS    Status   Mode Wait-Cnt Xeq-Cnt  Hold-Cnt ODisp          QHld Hold
     A        NOTHELD  JES                             ()             NO   NO
     B        NOTHELD  JES                             ()             NO   NO
```


© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Primary Menu Command Panels

- Most panels allow the entry of action characters (NP - Input column)
  - Depending on the panel, the use of individual action characters on a specific object is controlled by SDSF, OPERCMDS, JESSPOOL, WRITER, and/or XFACILIT class profiles
  - Each action character has a required level of access, where READ is typically needed for Display actions and UPDATE, CONTROL, and ALTER are for management actions
- Many panels have overtypeable fields (e.g., Dest)
  - Upon panel entry, SDSF determines what fields a user is authorized to overtype and displays the authorized ones in highlighted font
  - SDSF calls RACF for authorization to every field - UPDATE access is required

    SDSF ISFATTR.*panel.field* UPDATE (RACROUTE LOG=NONE)
  - Do not use WARNING on profiles for ISFATTR resources
  - Depending on the field, entering a value by overtyping a field is further controlled by SDSF, OPERCMDS, WRITER, and/or JESSPOOL class profiles
- Most action characters and overtype actions cause SDSF to generate MVS and JES operator commands, which are governed by OPERCMDS class profiles
  - Recommend OPERCMDS permissions include WHEN(CONSOLE(SDSF))

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Action and Resource Access Examples

- Purging a job on the Hold queue ('P') requires the following permissions
  - SDSF ISFCMD.DSP.HOLD.*jesname* READ
  - OPERCMDS *jesname*.CANCEL.BAT UPDATE
  - JESSPOOL *nodename.ownerid.jobname.jobid.dsnumber.ddname* ALTER

- Overtyping the output class on a job in the Hold queue requires the following permissions
  - SDSF ISFCMD.DSP.HOLD.*jesname* READ
  - SDSF ISFATTR.OUTPUT.CLASS UPDATE
  - OPERCMDS *jesname*.MODIFY.BATOUT UPDATE
  - JESSPOOL *nodename.ownerid.jobname.jobid.dsnumber.ddname* ALTER

© 2023 RSH Consulting, Inc. All Rights Reserved.

Action Character Resource Permission Examples

PANEL	CLASS	RESOURCE	ACCESS	ACTION
APF	SDSF	ISFAPF.dsname	READ	All
CK CKH	XFACILIT	HZS.sysname.checkowner.checkname.action	READ UPDATE CONTROL	D S X A H R All others
	LOGSTRM	health-check-history-log-stream-name	READ	
DYNX	SDSF	ISFDYNX.exitname	READ UPDATE ALTER	All others H P PF U
INIT	SDSF	ISFINIT.Inn.jes-name	READ CONTROL	D All others
PR	WRITER WRITER	jes-name.LOCAL.device-name jes-name.RJE.device-name	READ CONTROL ALTER	D All others C
SR	SDSF	ISFSR.type.system.jobname ISFSR.ACTION.system.jobname ISFSR.REPLY.system.jobname	READ READ READ	D C AI, R

© 2023 RSH Consulting, Inc. All Rights Reserved.

Jobs, Output Groups, SYSIN/SYSOUT

- SDSF uses the JESSPOOL class to protect jobs, Started Tasks, and output
  - READ View jobs and output
  - ALTER Modify, cancel, or delete jobs or output
- Use of action characters and overtypeable fields varies by panel and depending on the action to be taken requires access to these resources
  - JESSPOOL *nodeid.userid.jobname.jobid* READ, ALTER
  - JESSPOOL *nodeid.userid.jobname.jobid.*D*dsid.dsname* READ, ALTER
  - JESSPOOL *nodeid.userid.jobname.jobid.*GROUP.*ogroupid* READ, ALTER
- *jobid* prefixes - *localnodeid.userid.jobname.**jobid**.dsnumber.ddname*
  - JOB Batch job
  - TSU TSO User
  - STC Started Task
- Standard JES output *ddnames* - JESYSMSG, JESJCL, JESMSGLG, JESJCLIN
- If a job has multiple spool outputs, an access authorization check is made for each one individually

© 2023 RSH Consulting, Inc. All Rights Reserved.

Destination Operator Authority

- Destination Operator Authority enables a user to manage and view all output associated with a destination without requiring JESSPOOL permission
- To serve as a Destination Operator, a user requires the following permission
  - SDSF ISFOPER.DEST.*jes-name* READ
- Use of action characters and overtypeable fields varies by panel and depending on the action to be taken requires access to these resources
  - SDSF ISFAUTH.DEST.*destname*.DATASET.*dsname*
  - SDSF ISFAUTH.DEST..DATASET.*dsname* (embedded .. is valid)
  - SDSF ISFAUTH.DEST.*destname*
  - SDSF ISFAUTH.DEST. (ending . is valid)
  - Access required
    - READ View jobs and output (use case - see all output with a specific destination)
    - ALTER Modify, cancel, or delete jobs or output
  - Access to these resources is <u>not</u> logged
    - LOGSTR field in SMF records for JESSPOOL events indicate use of dest operator authority
  - To allow job management or review without access to application output, permit access to ISFAUTH.DEST.*.DATASET.JESMSGLG | JESJCL |JESYSMSG

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Profiles Governing Overtypeable Fields

- ISFATTR profile prefixes and panel - resource name suffix is *.fieldname*

ISFATTR.CHECK	CK	Health checks
ISFATTR.CKPT	CKPT	JES Checkpoint
ISFATTR.EMCS	EMCS	Extended Console
ISFATTR.ENCLAVE	ENC	Enclaves
ISFATTR.INIT	INIT	Initiators
ISFATTR.JOB	DA, I, ST	Jobs
ISFATTR.JOBCL	JC	Job classes
ISFATTR.JOBGROUP	JG	Job groups
ISFATTR.LINE	LI	Lines
ISFATTR.LOGON	NS	Network servers
ISFATTR.MEMBER	MAS	MAS members
ISFATTR.MODIFY	SO	Spool offloaders
ISFATTR.NETOPTS	NC, NS	Network Connections
ISFATTR.NODE	NO, NC	Nodes
ISFATTR.OFFLOAD	SO	Spool offloaders
ISFATTR.OUTDESC	OD	Job output descriptors

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF Profiles Governing Overtypeable Fields

- ISFATTR profile prefixes and panel (continued)

• ISFATTR.OUTPUT	H, O	Job output datasets
• ISFATTR.PROPTS	LI, NC, NS, PR, PUN	Lines, networks, printers, punches
• ISFATTR.RDR	RDR	Readers
• ISFATTR.RESMON	RM	JES2 resources
• ISFATTR.RESOURCE	RES	WLM resources
• ISFATTR.SELECT	INIT, LI, NC, NS, PR, PUN, SO	Device selection criteria
• ISFATTR.SPOOL	SP	Spool volumes

- UPDATE access is required to use an overtypeable field

- TSO users are usually permitted UPDATE access to the following
  - ISFATTR.JOB.OUT*.**
  - ISFATTR.JOB.PRTDEST

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF - Miscellaneous Resources

- Control use of the slash "/" command used to enter operator commands
  - SDSF ISFOPER.SYSTEM READ
  - OPERCMDS MVS.MSCOPER.*userid* READ
  - SDSF ISFCMD.ODSP.ULOG.*jes-name* READ
  - Commands enter via / as not subject to WHEN(CONSOLE(SDSF)) permissions
- Control access to SYSLOG
  - SDSF ISFCMD.ODSP.SYSLOG.*jes-name* READ
  - JESSPOOL *localnodeid*.+MASTER+.SYSLOG.*jobid.dsidentifier.sysid* READ
- Control access to merged, sysplex-wide system message log
  - LOGSTRM SYSPLEX.OPERLOG READ
- Control selection of Destination names - all or restricted
  - SDSF ISFOPER.ANYDEST.*jes-name* READ All destinations (usually ID(*))
  - SDSF ISFAUTH.DEST.*destname* READ Specific destinations
    - *destnames* are defined in JES PARMs - defaults to LOCAL
  - To allow users to specify which destination they wish to see using the DEST command, permit READ to ISFCMD.FILTER.DEST

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF - ISFPARMS - PROPLIST and PROPERTY

- An ISFPARMS PROPLIST statement, along with associated PROPERTY statements, defines customized values for certain SDSF properties

- The PROPLIST statement is associated with a group of users through the CUSTOM parameter on the GROUP statement

```
GROUP NAME(SYSPROG)
    CUSTOM(USERPROP)
...
PROPLIST NAME(USERPROP)
    PROPERTY NAME(property) VALUE( FALSE | TRUE )
```

- Security-related PROPERTY
  - Security.Browse.LogNOFAIL(FALSE | TRUE)
    - TRUE avoids violations for every JOB output file when 'S' is specified to select entire job
      - No ICH408I message or SMF violation record

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF - Implementation Recommendations

- Ensure every ISFPARMS SDSF group has an assigned name to facilitate use SDSF GROUP-prefixed profiles to control their assignment
- Remove security options from ISFPARMS once RACF control is implemented
  - May be able to consolidate all ISFPARMS groups into one group with common display options
- Implement RACF classes in this sequence
  - CONSOLE, XFACILIT, WRITER, (if needed) LOGSTRM - simultaneously or in any order
  - OPERCMDS
  - JESSPOOL
  - SDSF / GSDSF
- GSDSF profiles are sometimes used for sets of overtypeable field resources
- RACF Administrators should be given READ access to almost all SDSF resources to be able to monitor the configuration of the system

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF - Implementation Recommendations

- Use WHEN(CONSOLE(SDSF)) for OPERCMDS permissions for end-users
  - PERMIT JES2.CANCEL.BAT CLASS(OPERCMDS) ID(*) ACCESS(UPDATE) +
    WHEN(CONSOLE(SDSF))
  - CONSOLE class must be active to use the feature (*** DFTRETC=8 class ***)

- Be careful with overly generic SDSF profiles - fully specify the first qualifier when permitting ID(*) access or access higher than READ
  - ISF*.* - Permit ALTER only to Operations and Tech Support
  - ISFOPER.DEST.** - Permit no access to exclude Destination Operator authority
  - ** UACC(NONE) - Recommended to disallow new or unprotected functions

- If deemed non-sensitive, consider providing all users with the ability to view processing results of all jobs using the Global Access Table

  RDEFINE GLOBAL JESSPOOL +

  ADDMEM(**.JESYSMSG/READ **.JESJCL/READ **. JESMSGLG/READ)
  - Can exclude certain jobs with overriding entries (e.g., *.PAYID.**/NONE)

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF - Implementation Recommendations

- Sample profile definition and permit commands
  - ISF.SISFEXEC(ISFRAC) - REXX EXEC
  - Assumes three categories of users
    - SYSPROG All access - Includes Destination Operator with ALTER
    - OPERATOR Extensive access - Includes Destination Operator with READ
    - Users Limited access - UACC(READ)
  - Dangerous - do not execute commands as generated - deletes existing profiles (e.g., OPERCMDS, XFACILIT) and rebuilds them as if only SDSF access matters
  - Use output only as a guide at best

- Existing ISFPARMS are often outdated, convoluted, and grant excessive authority, so it is generally best to start fresh and design SDSF profiles from the ground up using Role Based Access Control (RBAC) principles without trying to mimic the existing ISFPARMS
  - Existing OPERCMDS, JESSPOOL, WRITER, and XFACILIT profiles often require extensive remediation as well

© 2023 RSH Consulting, Inc. All Rights Reserved.

SDSF - References

- RSH RACF Tips newsletter
  - *Sharing Output in SDSF (Without JESSPOOL Permission)* - April 2008
  - *SDSF Destination Operators* - April 2014
  - *SDSF SECURITY TRACE* - July 2016
  - *Recent SDSF RACF Changes* - January 2018

- IBM manuals
  - z/OS SDSF Operation and Customization
  - z/OS 2.5 SDSF Security Migration Guide

© 2023 RSH Consulting, Inc. All Rights Reserved.