SDSF Security Introduction – Part 2

Julie Bergh

berghju@gmail.com

- Started Task
- ISFPARMS
- SDSF Panel
- SDSF Profiles / Security

Started Tasks

- The SDSF server is an address space that SDSF uses to:
- Process ISFPARMS statements.
- Provide sysplex support. This consists of sysplex-wide data for JES2 devices and for system resources (APF, AS, CK, CSR, DEV, DYNX, FS, ENC, GT, LNK, LPA, NA, PAG, PARM, PS, RM, SMSG, SMSV, SSI, SYM, SYS, VMAP).
- Manage the starting and stopping of the SDSFAUX address space. SDSFAUX is used to provide data gathering support and other services for SDSF panels.

Started Task

- SDSF Class is RACLISTED
- **MVSADMIN.WLM.POLICY** resource profile.
- PERMIT MVSADMIN.WLM.POLICY ACCESS(READ) CLASS(FACILITY) ID(USERID)
- SDSFAUX and SDSF started task definitions in STARTED class.

SDSF Panels – Remember When – System Programmer

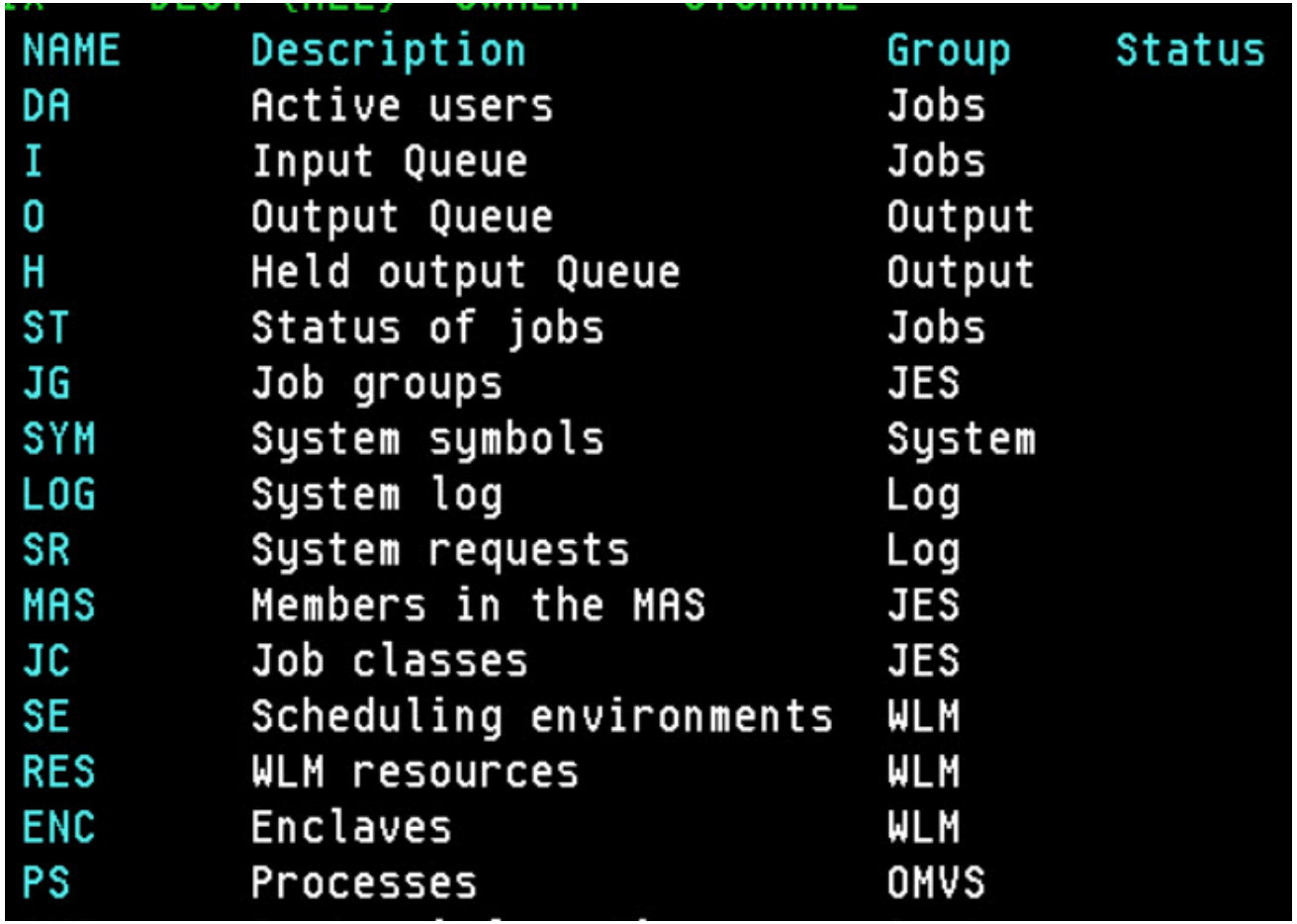
```
HQX7760------- SDSF PRIMARY OPTION MENU -------------
COMMAND INPUT ===>_                    SCROLL ===> PAGE
DA     Active users                    INIT  Initiators
I      Input queue                     PR    Printers
O      Output queue                    PUN   Punches
H      Held output queue               RDR   Readers
ST     Status of jobs                  LINE  Lines
                                       NODE  Nodes
LOG    System log                      SO    Spool offload
SR     System requests                 SP    Spool volumes
MAS    Members in the MAS
JC     Job classes                     RM    Resource monitor
SE     Scheduling environments         CK    Health checker
RES    WLM resources
ENC    Enclaves                        ULOG  User session log
PS     Processes
```

SDSF Panels – Remember When – End User

```
 Display  Filter  View  Print  Options  Help
 -------------------------------------------
HQX7760 ---------  SDSF PRIMARY OPTION MENU ------
COMMAND INPUT ===>

DA     Active users
I      Input queue
O      Output queue
H      Held output queue
ST     Status of jobs
```

SDSF Panels Now – Small Sample



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	

SDSF panels added in z/OS 2.2 & z/OS 2.3

APF Data Sets (APF)
Address Space Storage (AS)
Page Data Sets (PAG)
z/OS Parmlib Data Sets (PARM)
CF Connections (CFC)
CF Structures (CFS)
Device Activity (DEV)
z/OS Unix File Systems (FS)
Generic Tracker (GT)
Network Activity (NA)
SMS Storage Groups (SMSG)
Linklist Data Sets (LNK)
LPA List Data Sets (LPA)
Jobstep Information (JS)
JES2 Proclib Data Sets (PROC)
SMS Volumes (SMSV)
Subsystems (SSI)
Common Storage Remaining (CSR)
Virtual Storage Map (VMAP)
Job Modules (JC)
Job Tasks (JT)
Search Data Set Lists (SRCH)

SDSF Panels added in z/OS 2.4

• EMCS	Extended Consoles
• ENQD	Data Set Enqueues
• JES	JES Subsystems
• JRI	JES2 Resource Information
• JRJ	JES2 Resource Usage By Jobname
• RMA	JES2 Resource Monitor Alerts
• LPD	Link Pack Directory
• OMVS	z/OS Unix Options
• REPC	WLM Report Classes
• RGRP	WLM Resource Groups
• SRVC	WLM Service Classes
• WKLD	WLM Workloads
• WLM	WLM Policy
• XCFM	XCF Groups and Members

- z/OS 2.5 SDSF security needs to be external
- Are you ready?

SDSF Class – Profiles – My Test System

```
CLASS      NAME
-----      ----
SDSF       ISF*.** (G)

GROUP CLASS NAME
----- ----- ----
GSDSF

RESOURCE GROUPS
-------- ------
NONE

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----  --------   ----------------  -----------  -------
 00    SYS1            READ             ALTER     NO

USER      ACCESS
----      ------
ADCDMST   ALTER
IBMUSER   ALTER
```

SDSF Class – Profiles – My Test System

```
CLASS      NAME
 -----      ----
 OPERCMDS   JES%.** (G)

 LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
 -----  --------   ----------------  -----------  -------
  00    IBMUSER        CONTROL          CONTROL    NO


 USER      ACCESS
 ----      ------
 IBMUSER   ALTER
 SYS1      CONTROL
```

SDSF Class – Profiles

- **ISFATTR – over typeable fields**
- **ISFCMD – SDSF Panels and authorized commands**
- **ISFAUTH – used with destination names**
- **ISFOPER – destinations and system operator commands (/)**

Group 1 – Systems Programmers - ISFPROG

Without SAF

```
GROUP NAME(ISFSPROG),
    TSOAUTH(JCL,OPER,ACCT),
    AUTH(ALL),
    CMDAUTH(ALL),
    CMDLEV(7),
    DSPAUTH(ALL),
    DFIELD2(DAFLD2),
    GPLEN(2),
    ACTION(ALL),
    ACTIONBAR(YES),
    APPC(ON),
    OWNER(NONE),
    CONFIRM(ON),
    CURSOR(ON,
    DATE(MMDDYYYY,
    DATESEP(/),
    LOG(OPERACT),
    ISYS(NONE),
    DADFLT(IN,OUT,TRANS,STC,TSU,JOB),
    VALTAB(TRTAB),
    UPCTAB(TRTAB2),
    DISPLAY(OFF)
```

With SAF

```
GROUP NAME(ISFSPROG),
    DFIELD2(DAFLD2),
    ACTION(ALL),
    ACTIONBAR(YES),
    APPC(ON),
    CONFIRM(ON),
    CURSOR(ON),
    DATE(MMDDYYYY),
    DATESEP(/),
    LOG(OPERACT),
    DADFLT(IN,OUT,TRANS,STC,TSU,JOB),
    VALTAB(TRTAB),
    UPCTAB(TRTAB2),
    DISPLAY(OFF)
```

Group 1 – Systems Programmers - ISFPROG

CMDLEV	Authorized Commands when CMDAUTH is ALL	MVS/JES2 Commands Authorized for Use with the / Command
0	This is the default.	None authorized
1	Displays information using display and list commands.	$D, $L, D
2	Cancels or purges a job, started task, or TSO user. Releases held output.	$C, $O, $P, C
3	Releases or holds a job.	$A, $H, E
4	JES2 SET command. Restarts a job, or the MVS RESET command.	$E, $T, $TO
5	Routes job output.	$R
6	JES2 printer control commands or any JES2 command.	$B, $F, $I, $S, $Z
7	Any MVS command, the command to stop or withdraw JES2 from the system ($PJES2), or JES2 commands that send commands to other MAS members or nodes.	All MVS/JES2 commands

Group 2 – Operators - ISFOPER

Without SAF

```
GROUP NAME(ISFOPER),
    TSOAUTH(JCL,OPER),
    AUTH(ALLOPER),
    CMDAUTH(ALL),
    CMDLEV(7),
    DSPAUTH(USERID,NOTIFY,AMSG),
    GPLEN(2),
    ACTION(ALL),
    ACTIONBAR(YES),
    APPC(ON),
    OWNER(NONE),
    CONFIRM(ON),
    CURSOR(ON),
    DATE(MMDDYYYY),
    DATESEP(/),
    LOG(OPERACT),
    ISYS(NONE),
    DADFLT(IN,OUT,TRANS,STC,TSU,JOB),
    VALTAB(TRTAB),
    UPCTAB(TRTAB2),
    DISPLAY(OFF)
```

With SAF

```
GROUP NAME(ISFOPER),
    ACTION(ALL),
    ACTIONBAR(YES),
    APPC(ON),
    CONFIRM(ON),
    CURSOR(ON),
    DATE(MMDDYYYY),
    DATESEP(/),
    LOG(OPERACT),
    DADFLT(IN,OUT,TRANS,STC,TSU,JOB),
    VALTAB(TRTAB),
    UPCTAB(TRTAB2),
    DISPLAY(OFF)
```

Group 3 – End Users - ISFUSER

Without SAF

```
GROUP NAME(ISFUSER),
    TSOAUTH(JCL),
    AUTH(ALLUSER),
    CMDAUTH(USERID,NOTIFY),
    CMDLEV(2),
    AUPDT(10),
    DSPAUTH(USERID,NOTIFY),
    PREFIX(USERID),
    ACTION(11,12,USER),
    ACTIONBAR(YES),
    APPC(ON),
    CONFIRM(ON),
    CURSOR(ON),
    DATE(MMDDYYYY),
    DATESEP(/),
    DADFLT(IN,OUT,TRANS,STC,TSU,JOB),
    VALTAB(TRTAB),
    UPCTAB(TRTAB2),
    DISPLAY(OFF)
```

With SAF

```
GROUP NAME(ISFUSER),
    AUPDT(10),
    PREFIX(USERID),
    ACTION(11,12,USER),
    ACTIONBAR(YES),
    APPC(ON),
    CONFIRM(ON),
    CURSOR(ON),
    DATE(MMDDYYYY),
    DATESEP(/),
    DADFLT(IN,OUT,TRANS,STC,TSU,JOB),
    VALTAB(TRTAB),
    UPCTAB(TRTAB2),
    DISPLAY(OFF)
```

SDSF - Options

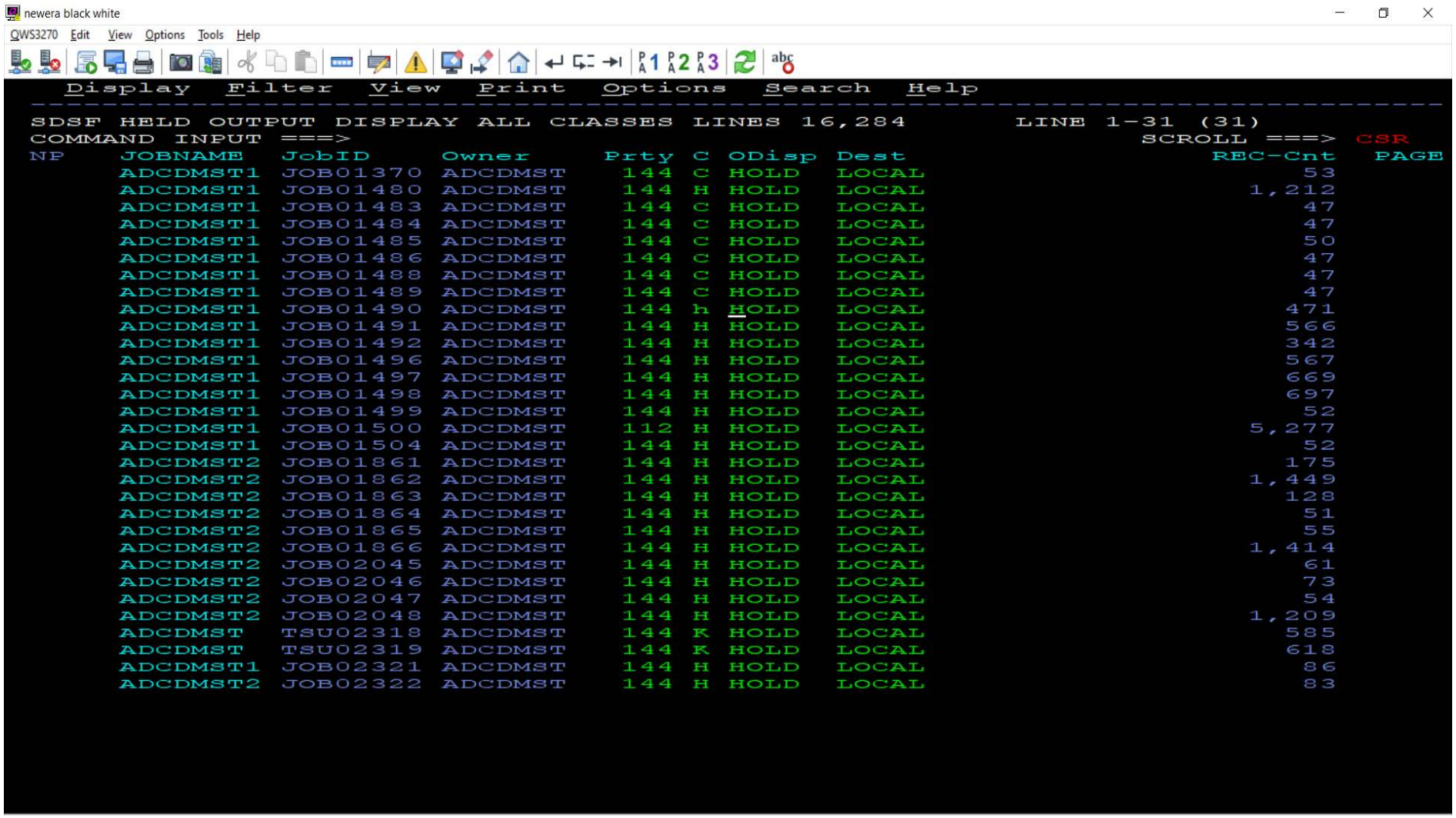
JG	Job groups	JES
MAS	Members in the MAS	JES
JC	Job classes	JES
INIT	Initiators	JES
PR	Printers	JES
PUN	Punches	JES
RDR	Readers	JES
SO	Spool offload	JES
SP	Spool volumes	JES
RM	Resource monitor	JES
PROC	Proclib data sets	JES
RMA	Resource monitor alerts	JES
JES	Job entry subsystems	JES
JRI	JES resource information	JES
JRJ	JES resource by job	JES

SDSF Class – Profiles

ISFDEV - Protecting device activity
ISFDYNX - Protecting dynamic exits
ISFEMCS - Protecting EMCS consoles
ISFENC - Protecting enclaves
ISFENQ - Protecting Enqueue Information
ISFFS - Protecting file systems
ISFGT - Protecting generic tracker events
ISFINIT - Protecting initiators
ISFRM - Protecting JES2 resources
ISFJES - Protecting JES subsystems

Resource Name	Description
ISFATTR.OUTPUT.**	Modify output group fields on the Held Output (H) and Output Queue (O) panels
ISFATTR.OUTPUT.BURST	Modify burst indication field on H and O panels
ISFATTR.OUTPUT.CLASS	Modify JES2 output class on H and O panels
ISFATTR.OUTPUT.DEST	Modify JES2 print destination name on H and O panels
ISFATTR.OUTPUT.FCB	Modify output FCB ID on H and O panels
ISFATTR.OUTPUT.FLASH	Modify output flash ID on H and O panels
ISFATTR.OUTPUT.FORMS	Modify output form number on H and O panels
ISFATTR.OUTPUT.PRMODE	Modify printer process mode on H and O panels
ISFATTR.OUTPUT.UCS	Modify output UCS ID on H and O panels
ISFATTR.OUTPUT.WRITER	Modify output external writer name on H and O panels
ISFATTR.RDR.**	Modify fields on the Readers (RDR) panel

Resource Name	Description
ISFATTR.RDR.**	Modify fields on the Readers (RDR) panel
ISFCMD.DSP.ACTIVE.jesx	Display Active users (DA) panel command
ISFCMD.DSP.HELD.jesx	Held Output (H) panel command
ISFCMD.DSP.INPUT.jesx	Input Queue (I) panel command
ISFCMD.DSP.OUTPUT.jesx	Output Queue (O) panel command
ISFCMD.DSP.STATUS.jesx	Status (ST) panel command
ISFCMD.ODSP.INITIATOR.jesx	Initiator (INIT) panel command
ISFCMD.ODSP.JOBCLASS.jesx	Job Class (JC) panel command
ISFCMD.ODSP.LINE.jesx	Line (LI) panel command
ISFCMD.ODSP.PRINTER.jesx	Printer (PR) panel command
ISFCMD.ODSP.PROCESS	Process (PS) panel command
ISFCMD.ODSP.PUNCH.jesx	Punch (PUN) panel command
ISFCMD.ODSP.READER.jesx	Reader (RDR) panel command
ISFCMD.ODSP.RESOURCE.system	Resource (RES) panel command
ISFCMD.ODSP.SR.system	System Request (SR) panel command
ISFINIT.Ixx.jesx	Display information about an initiator
ISFINIT.Ixx.jesx	All other functions such as start, stop, and drain an initiator
ISFJOBCL.class.jesx	Display information about a job class
ISFJOBCL.class.jesx	Modify job class characteristics


newera black white
QWS3270 Edit View Options Tools Help
Display Filter View Print Options Search Help
SDSF HELD OUTPUT DISPLAY ALL CLASSES LINES 16,284 LINE 1-31 (31)
COMMAND INPUT ===> SCROLL ===> CSR
NP JOBNAME JobID Owner Prty C ODisp Dest REC-Cnt PAGE
ADCDMST1 JOB01370 ADCDMST 144 C HOLD LOCAL 53
ADCDMST1 JOB01480 ADCDMST 144 H HOLD LOCAL 1,212
ADCDMST1 JOB01483 ADCDMST 144 C HOLD LOCAL 47
ADCDMST1 JOB01484 ADCDMST 144 C HOLD LOCAL 47
ADCDMST1 JOB01485 ADCDMST 144 C HOLD LOCAL 50
ADCDMST1 JOB01486 ADCDMST 144 C HOLD LOCAL 47
ADCDMST1 JOB01488 ADCDMST 144 C HOLD LOCAL 47
ADCDMST1 JOB01489 ADCDMST 144 C HOLD LOCAL 47
ADCDMST1 JOB01490 ADCDMST 144 h HOLD LOCAL 471
ADCDMST1 JOB01491 ADCDMST 144 H HOLD LOCAL 566
ADCDMST1 JOB01492 ADCDMST 144 H HOLD LOCAL 342
ADCDMST1 JOB01496 ADCDMST 144 H HOLD LOCAL 567
ADCDMST1 JOB01497 ADCDMST 144 H HOLD LOCAL 669
ADCDMST1 JOB01498 ADCDMST 144 H HOLD LOCAL 697
ADCDMST1 JOB01499 ADCDMST 144 H HOLD LOCAL 52
ADCDMST1 JOB01500 ADCDMST 112 H HOLD LOCAL 5,277
ADCDMST1 JOB01504 ADCDMST 144 H HOLD LOCAL 52
ADCDMST2 JOB01861 ADCDMST 144 H HOLD LOCAL 175
ADCDMST2 JOB01862 ADCDMST 144 H HOLD LOCAL 1,449
ADCDMST2 JOB01863 ADCDMST 144 H HOLD LOCAL 128
ADCDMST2 JOB01864 ADCDMST 144 H HOLD LOCAL 51
ADCDMST2 JOB01865 ADCDMST 144 H HOLD LOCAL 55
ADCDMST2 JOB01866 ADCDMST 144 H HOLD LOCAL 1,414
ADCDMST2 JOB02045 ADCDMST 144 H HOLD LOCAL 61
ADCDMST2 JOB02046 ADCDMST 144 H HOLD LOCAL 73
ADCDMST2 JOB02047 ADCDMST 144 H HOLD LOCAL 54
ADCDMST2 JOB02048 ADCDMST 144 H HOLD LOCAL 1,209
ADCDMST TSU02318 ADCDMST 144 K HOLD LOCAL 585
ADCDMST TSU02319 ADCDMST 144 K HOLD LOCAL 618
ADCDMST1 JOB02321 ADCDMST 144 H HOLD LOCAL 86
ADCDMST2 JOB02322 ADCDMST 144 H HOLD LOCAL 83

SDSF Security

- SDSF interacts with SAF to control access to the following resources:
  - Membership in SDSF groups
  - SDSF panels
  - SDSF authorized commands
  - Use of the / command to issue MVS and JES commands and receive responses
  - Overtypeable fields
  - Destination names
  - Operator authority by destination

SDSF Security

- RACF logs access attempts to protected SDSF resources according to the audit setting in the RACF profile for the resource. Logging is performed for all access attempts except for the following resource names in the SDSF class:
  - ISFOPER.DEST.*jesx*
  - ISFAUTH.DEST.*destname*
  - ISFAUTH.DEST.*destname.*DATASET.*dsname*
  - ISFOPER.ANYDEST.*jesx*
  - All resource names beginning with ISFATTR.
  - Logging is not performed for these access attempts because the user is not specifically trying to gain access to those resources.

SDSF Class – Profiles

- **ISFATTR – over typeable fields**
- **ISFCMD – SDSF Panels and authorized commands**
- **ISFAUTH – used with destination names**
- **ISFOPER – destinations and system operator commands (/)**

SDSF Class – Profiles

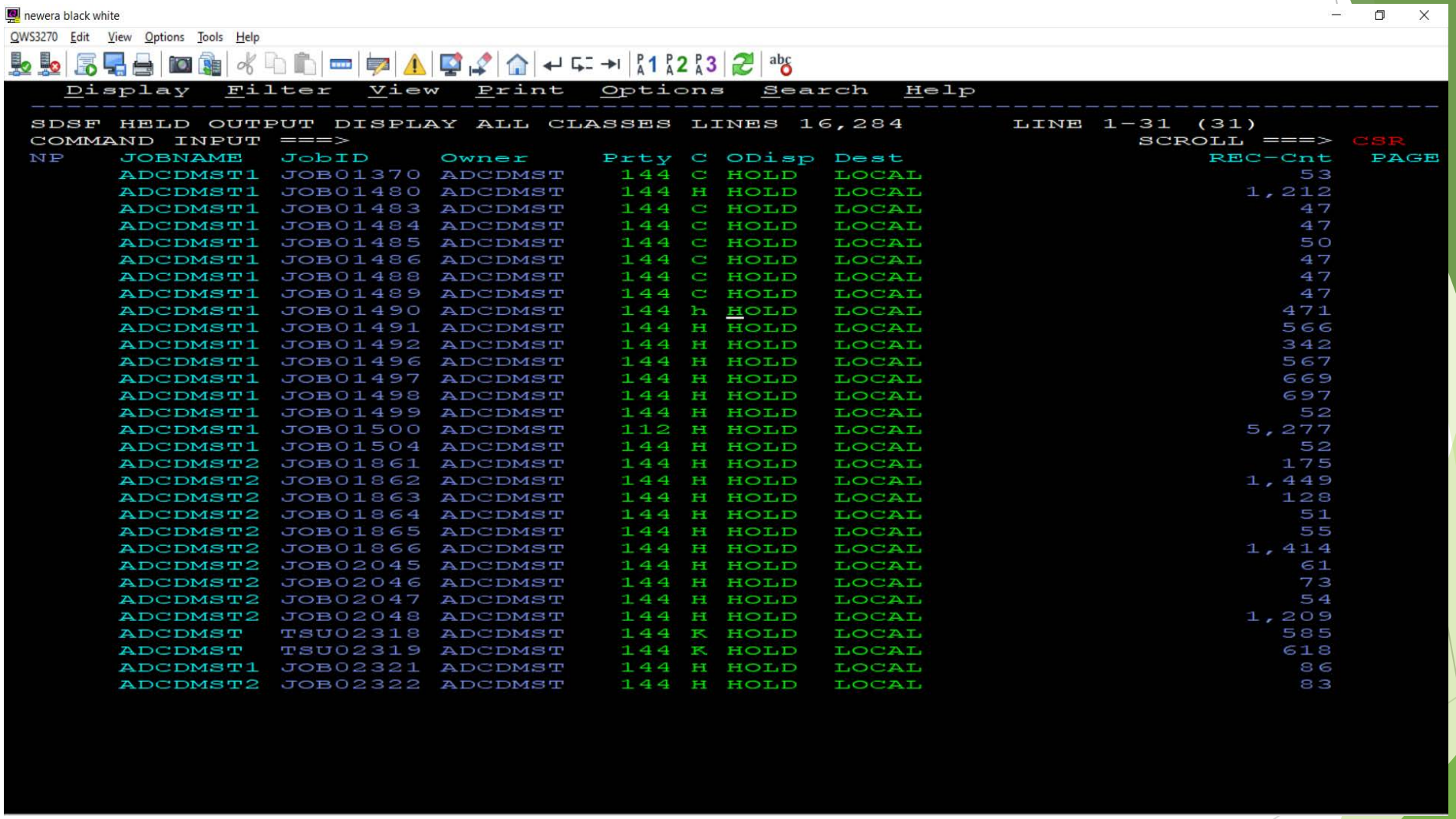
Action Characters	SDSF Actions, or MVS and JES2 Commands Issued	Where Valid
A	$TO (Set output)	H O
C	$C (Cancel) $CO (Cancel) See notes 1 and 2.	DA H I JDS O ST LI NO PR PUN RDR SO H O
C	$C	JG
CA	$C,ARMRESTART	DA I ST

SDSF Class – Profiles

Overtypeable Fields	MVS and JES2 Commands Issued	Where Valid
ACTIVE	$T (Set)	JC
ADISC	$T (Set)	LI
ANODE	$T (Set)	LI NC
APPL	$T (Set)	NS
APPLID	$T (Set)	LI
ARCHIVE	$T (Set)	SO
ASIS	$T (Set)	PR
AUTH	$T (Set)	JC

SDSF Class – Profiles

Action Character	SDSF Panel	Command, JES2 Command, JES3	OPERCMDS Resource, JES2 OPERCMDS Resource, JES3	OPERCMDS Required Access
A	H O	$TO	*jesx*.MODIFY.*type*OUT	UPDATE
		-	-	-
A	DA I ST	$A	*jesx*.MODIFYRELEASE.*type*	UPDATE
		*F	*jesx*.MODIFY.JOB	


newera black white
QWS3270 Edit View Options Tools Help
Display Filter View Print Options Search Help
SDSF HELD OUTPUT DISPLAY ALL CLASSES LINES 16,284 LINE 1-31 (31)
COMMAND INPUT ===> SCROLL ===> CSR
NP JOBNAME JobID Owner Prty C ODisp Dest REC-Cnt PAGE
ADCDMST1 JOB01370 ADCDMST 144 C HOLD LOCAL 53
ADCDMST1 JOB01480 ADCDMST 144 H HOLD LOCAL 1,212
ADCDMST1 JOB01483 ADCDMST 144 C HOLD LOCAL 47
ADCDMST1 JOB01484 ADCDMST 144 C HOLD LOCAL 47
ADCDMST1 JOB01485 ADCDMST 144 C HOLD LOCAL 50
ADCDMST1 JOB01486 ADCDMST 144 C HOLD LOCAL 47
ADCDMST1 JOB01488 ADCDMST 144 C HOLD LOCAL 47
ADCDMST1 JOB01489 ADCDMST 144 C HOLD LOCAL 47
ADCDMST1 JOB01490 ADCDMST 144 h HOLD LOCAL 471
ADCDMST1 JOB01491 ADCDMST 144 H HOLD LOCAL 566
ADCDMST1 JOB01492 ADCDMST 144 H HOLD LOCAL 342
ADCDMST1 JOB01496 ADCDMST 144 H HOLD LOCAL 567
ADCDMST1 JOB01497 ADCDMST 144 H HOLD LOCAL 669
ADCDMST1 JOB01498 ADCDMST 144 H HOLD LOCAL 697
ADCDMST1 JOB01499 ADCDMST 144 H HOLD LOCAL 52
ADCDMST1 JOB01500 ADCDMST 112 H HOLD LOCAL 5,277
ADCDMST1 JOB01504 ADCDMST 144 H HOLD LOCAL 52
ADCDMST2 JOB01861 ADCDMST 144 H HOLD LOCAL 175
ADCDMST2 JOB01862 ADCDMST 144 H HOLD LOCAL 1,449
ADCDMST2 JOB01863 ADCDMST 144 H HOLD LOCAL 128
ADCDMST2 JOB01864 ADCDMST 144 H HOLD LOCAL 51
ADCDMST2 JOB01865 ADCDMST 144 H HOLD LOCAL 55
ADCDMST2 JOB01866 ADCDMST 144 H HOLD LOCAL 1,414
ADCDMST2 JOB02045 ADCDMST 144 H HOLD LOCAL 61
ADCDMST2 JOB02046 ADCDMST 144 H HOLD LOCAL 73
ADCDMST2 JOB02047 ADCDMST 144 H HOLD LOCAL 54
ADCDMST2 JOB02048 ADCDMST 144 H HOLD LOCAL 1,209
ADCDMST TSU02318 ADCDMST 144 K HOLD LOCAL 585
ADCDMST TSU02319 ADCDMST 144 K HOLD LOCAL 618
ADCDMST1 JOB02321 ADCDMST 144 H HOLD LOCAL 86
ADCDMST2 JOB02322 ADCDMST 144 H HOLD LOCAL 83

SDSF – OPERCMDS

You can set up two generic profiles to allow use of all action characters

JES Commands *jesx*.** OPERCMDS CONTROL
MVS Commands MVS.** OPERCMDS CONTROL

SDSF – OPERCMDS – Conditional Access

- Permit users to issue JES2 commands while running in SDSF.
- RDEFINE OPERCMDS JES2.** UACC NONE
- PERMIT JES2.** CLASS(OPERCMDS)ID(*userid* or *groupid*) ACCESS(CONTROL) WHEN(CONSOLE(SDSF))
- To permit users unconditionally to issue all JES2 commands:
- PERMIT JES2.** CLASS(OPERCMDS)ID(*userid* or *groupid*) ACCESS(CONTROL)

SDSF Profiles

OPERCMDS Resource Name	Required Access	Action Character	JES/MVS Command	SDSF Panel
***jesx*.DISPLAY.INITIATOR**	READ	D, DL	$D	INIT
***jesx*.DISPLAY.JOB**	READ	D, DL	$D	JC
***jesx*.DISPLAY.JOB**	READ	D, L, LB, LH, LT	*I	DA I ST

Group 1 – Systems Programmers - ISFPROG

CMDLEV	Authorized Commands when CMDAUTH is ALL	MVS/JES2 Commands Authorized for Use with the / Command
0	This is the default.	None authorized
1	Displays information using display and list commands.	$D, $L, D
2	Cancels or purges a job, started task, or TSO user. Releases held output.	$C, $O, $P, C
3	Releases or holds a job.	$A, $H, E
4	JES2 SET command. Restarts a job, or the MVS RESET command.	$E, $T, $TO
5	Routes job output.	$R
6	JES2 printer control commands or any JES2 command.	$B, $F, $I, $S, $Z
7	Any MVS command, the command to stop or withdraw JES2 from the system ($PJES2), or JES2 commands that send commands to other MAS members or nodes.	All MVS/JES2 commands

Function	JES	Class	Resource Profile	Access
Action characters for CMDLEV=2	JES2	OPERCMDS	*jesx*.DISPLAY.BAT	READ
			jesx.DISPLAY.TSU	READ
			jesx.DISPLAY.STC	READ
			jesx.DISPLAY.INITIATOR	READ
			jesx.DISPLAY.DEV	READ
			jesx.MSEND.CMD	READ
			jesx.DISPLAY.BATOUT	READ
			jesx.DISPLAY.TSUOUT	READ
			jesx.DISPLAY.STCOUT	READ
			jesx.DISPLAY.GROUP	READ
			MVS.DISPLAY.WLM	UPDATE
			jesx.MODIFY.BATOUT	UPDATE
			jesx.MODIFY.TSUOUT	UPDATE

- z/OSMF

ISF.SISFEXEC(ISFRAC)

```
/*************************************************************/
/*  Do not execute these commands until you have verified they   */
/*  will secure things in an appropriate way for your installation,  */
/*  and have constructed the necessary lists of user IDs.        */
/*************************************************************/
/*  These commands will secure SDSF-only facilities to prevent end   */
/*  users and operators from using restricted functions by defining  */
/*  RACF profiles in the SDSF class.  These profiles provide a       */
/*  different view of security than the resource grouping profiles   */
/*  in the GSDSF class.  However, the two classes can also be used   */
/*  together.                                                        */
/*                                                                   */
```

ISF.SISFEXEC(ISFRAC)

- **SAMPLE RACF COMMANDS**

ISF.SISFEXEC(ISFRAC)

```
/*********************************************************************/
/*  Other functions of SDSF can be protected both by defining them   */
/*  in the SDSF (or GSDSF) class and in another class (OPERCMDS,     */
/*  WRITER, or JESSPOOL).  Commands to protect them in other classes */
/*  are not included below, so these resources will not be completely*/
/*  secured by these commands.                                       */
/*                                                                   */
/*  There are two groups of RDEFINE commands.  The first group       */
/*  uses a relatively small number of profiles to protect SDSF       */
/*  functions using generic profiles in the SDSF class.  The second  */
/*  group uses discrete profiles to protect SDSF resources.  If      */
/*  your installation needs many generic profiles to protect SDSF    */
/*  functions, you should consider using discrete profiles instead   */
/*  for improved RACF performance.  Generally, you should be able    */
/*  to use the generic profiles with a few of the discrete profiles  */
/*  to protect SDSF.                                                 */
/*                                                                   */
```

ISF.SISFEXEC(ISFRAC)

```
/*                                                                  */
/*------------------------------------------------------------------*/
/* Restrict operator SDSF functions.                                */
/*------------------------------------------------------------------*/
/*                                                                  */
RDEFINE SDSF ISFATTR.** UACC(NONE)
RDEFINE SDSF ISFAUTH.** UACC(NONE)
RDEFINE SDSF ISFCDE.**  UACC(NONE)
RDEFINE SDSF ISFCMD.**  UACC(NONE)
RDEFINE SDSF ISFCSR.**  UACC(NONE)
RDEFINE SDSF ISFDEV.**  UACC(NONE)
RDEFINE SDSF ISFJES.**  UACC(NONE)
RDEFINE SDSF ISFFS.**  UACC(NONE)
RDEFINE SDSF ISFGT.**  UACC(NONE)
```

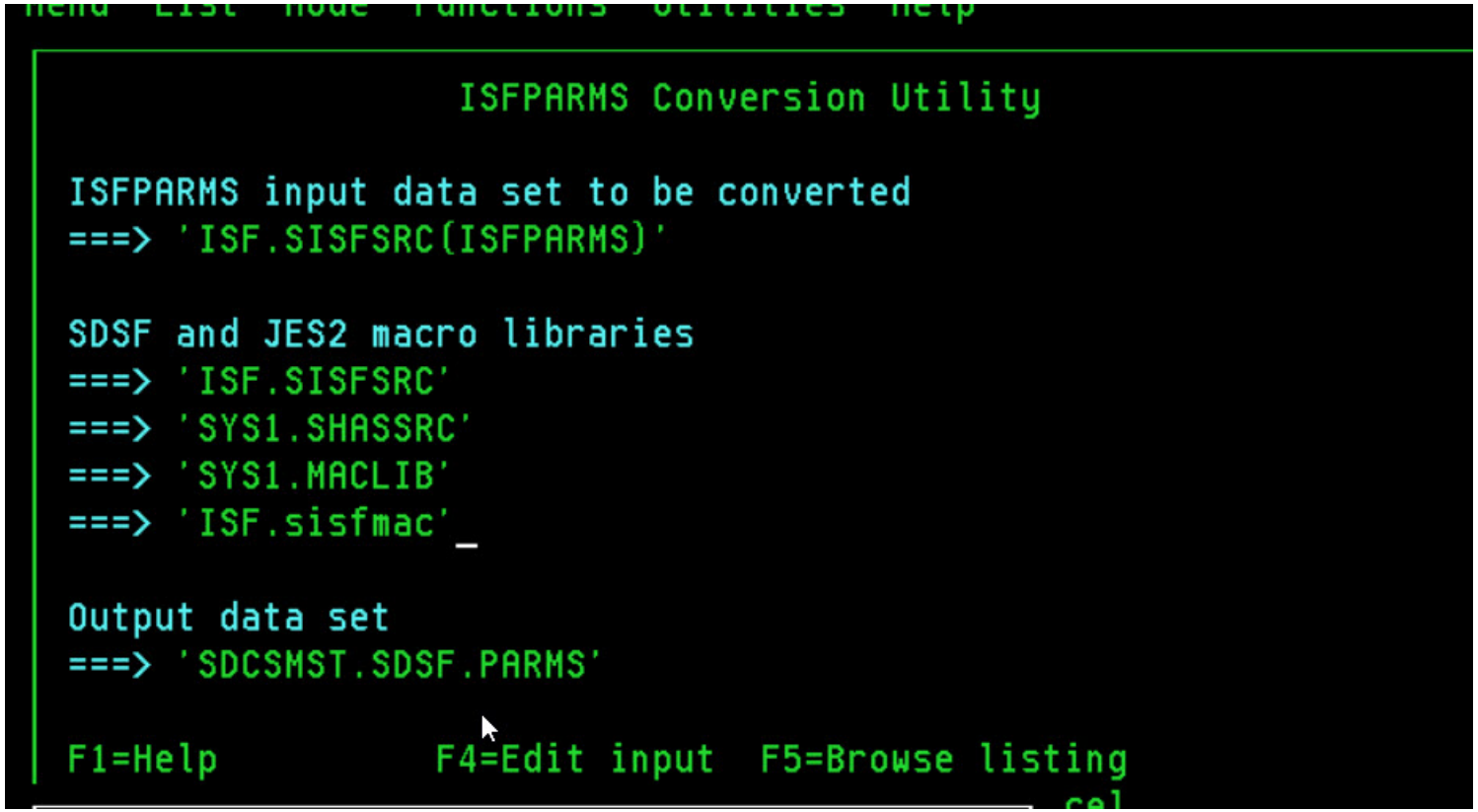
ISF.SISFEXEC(ISFRAC)

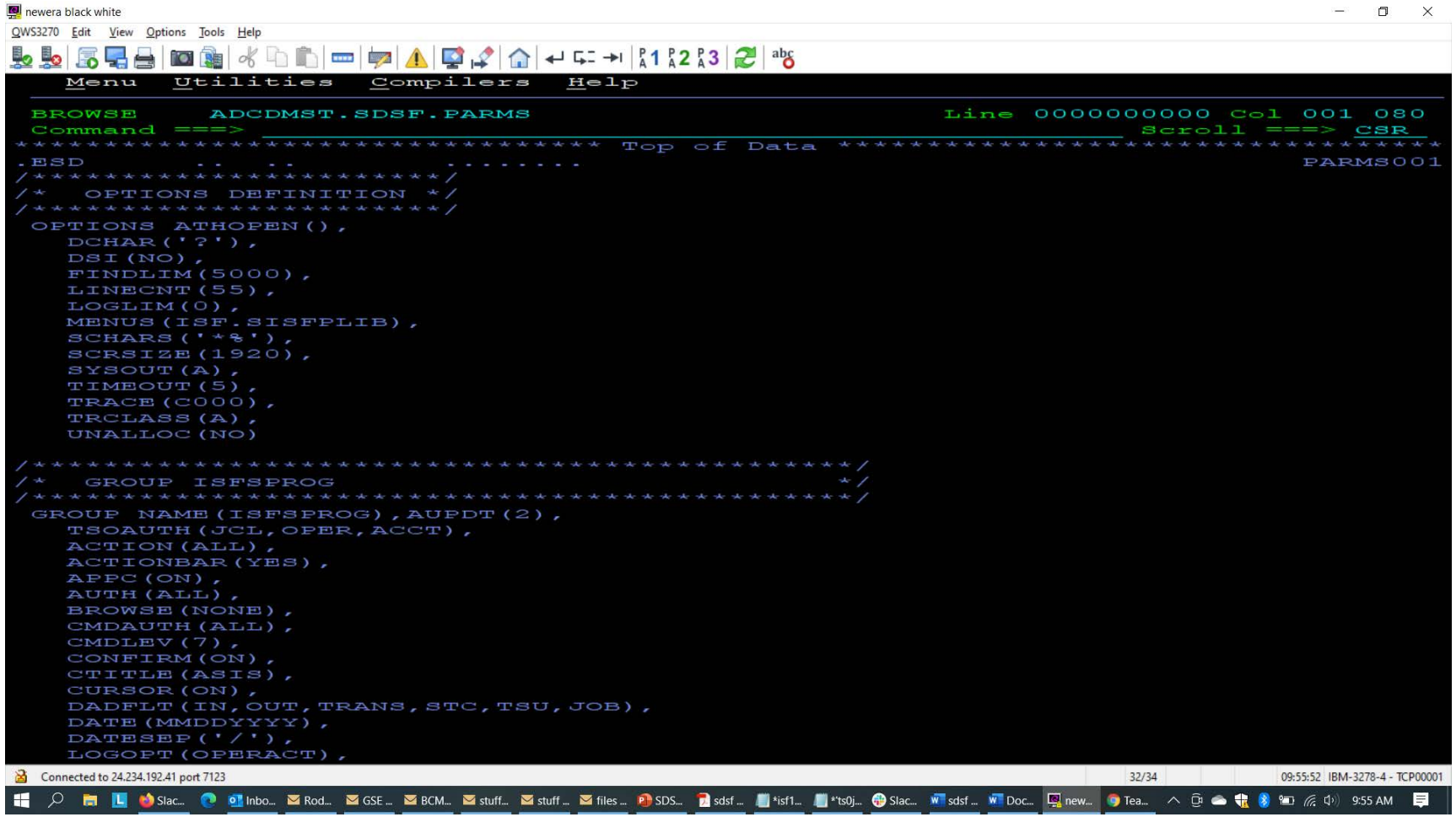
```
/*-------------------------------------------------------------*/
/* Create UACC(READ) profiles for end users.  To keep functions     */
/* from being made available, remove the appropriate profiles       */
/* from the list below, or create more specific profiles for        */
/* specific functions with UACC(NONE).  To allow functions that are  */
/* restricted above to be used, change the universal access above or */
/* create additional profiles below that are more specific with the  */
/* appropriate universal access (UACC).                             */
/*-------------------------------------------------------------*/
/*                                                               */
RDEFINE SDSF ISF.CONNECT.*       UACC(READ)
RDEFINE SDSF ISFATTR.JOB.OUT*.*  UACC(READ)
RDEFINE SDSF ISFATTR.JOB.PRTDEST UACC(READ)
RDEFINE SDSF ISFCMD.DSP.**       UACC(READ)
RDEFINE SDSF ISFCMD.FILTER.*     UACC(READ)
RDEFINE SDSF ISFOPER.ANYDEST.*   UACC(READ)
```

ISF.SISFEXEC(ISFRAC)

```
/*-------------------------------------------------------------*/
/* Permit system programmers to use all SDSF functions.        */
/*-------------------------------------------------------------*/
/*                                                             */
PERMIT ISF*.**             CLASS(SDSF) ID(SYSPROG) ACC(ALTER)
PERMIT ISFATTR.**          CLASS(SDSF) ID(SYSPROG) ACC(UPDATE)
PERMIT ISFATTR.JOB.OUT*.*  CLASS(SDSF) ID(SYSPROG) ACC(ALTER)
PERMIT ISFATTR.JOB.PRTDEST CLASS(SDSF) ID(SYSPROG) ACC(UPDATE)
PERMIT ISFAUTH.**          CLASS(SDSF) ID(SYSPROG) ACC(ALTER)
PERMIT ISFCDE.**           CLASS(SDSF) ID(SYSPROG) ACC(READ)
PERMIT ISFCMD.**           CLASS(SDSF) ID(SYSPROG) ACC(READ)
PERMIT ISFCMD.DSP.**       CLASS(SDSF) ID(SYSPROG) ACC(READ)
PERMIT ISFCMD.FILTER.*     CLASS(SDSF) ID(SYSPROG) ACC(READ)
PERMIT ISFCMD.MAINT.**     CLASS(SDSF) ID(SYSPROG) ACC(READ)
PERMIT ISFDEV.**           CLASS(SDSF) ID(SYSPROG) ACC(READ)
PERMIT ISFJES.**           CLASS(SDSF) ID(SYSPROG) ACC(READ)
```

ISFACP

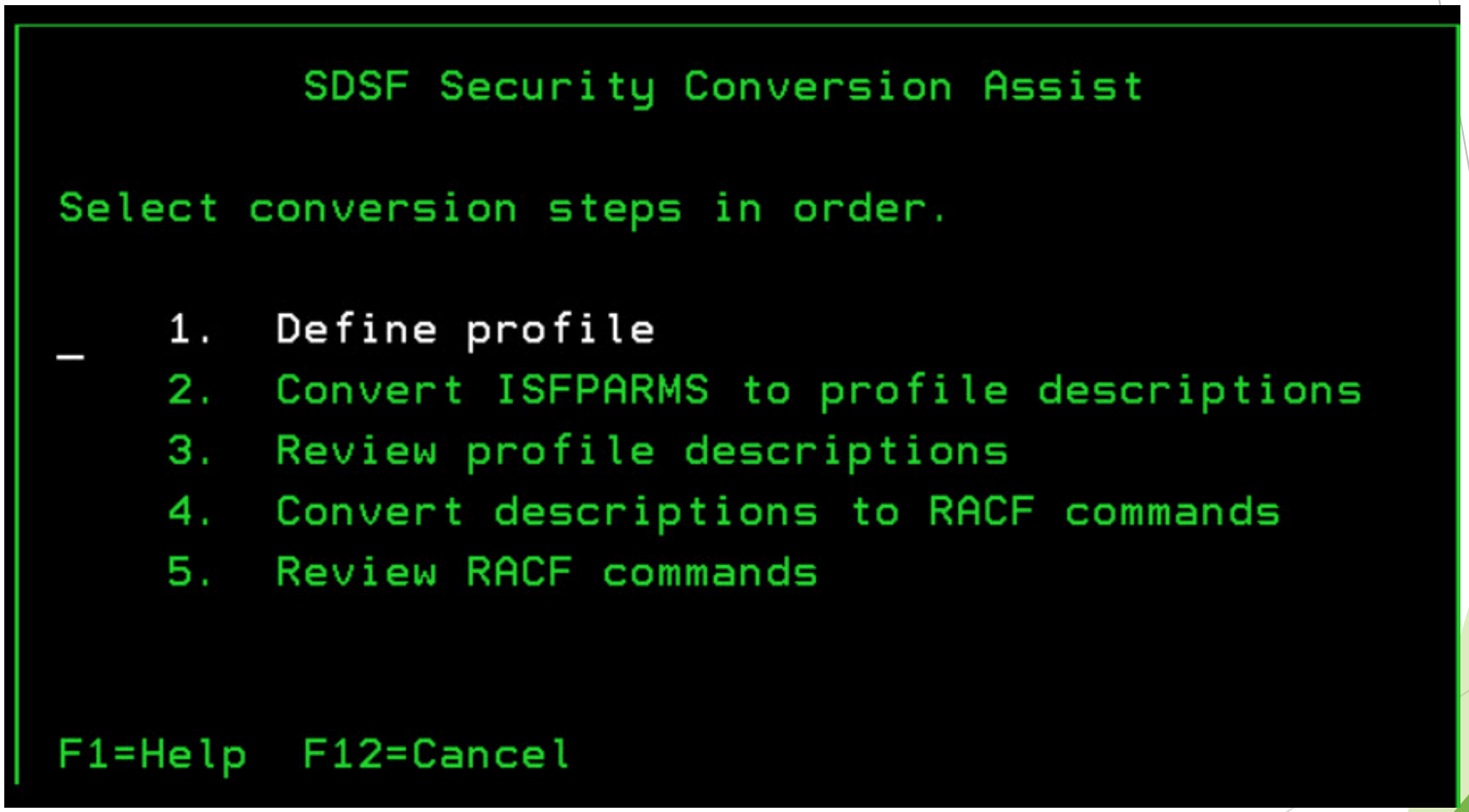

ISFPARMS Conversion Utility
ISFPARMS input data set to be converted
===> 'ISF.SISFSRC(ISFPARMS)'
SDSF and JES2 macro libraries
===> 'ISF.SISFSRC'
===> 'SYS1.SHASSRC'
===> 'SYS1.MACLIB'
===> 'ISF.sisfmac'
Output data set
===> 'SDCSMST.SDSF.PARMS'
F1=Help
F4=Edit input
F5=Browse listing


newera black white
QWS3270 Edit View Options Tools Help
Menu Utilities Compilers Help
BROWSE ADCDMST.SDSF.PARMS Line 0000000000 Col 001 080
Command ===> Scroll ===> CSR
Top of Data
.ESD PARMS001
/*********************/
/* OPTIONS DEFINITION */
/*********************/
OPTIONS ATHOPEN(),
DCHAR('?'),
DSI(NO),
FINDLIM(5000),
LINECNT(55),
LOGLIM(0),
MENUS(ISF.SISFPLIB),
SCHARS('*%'),
SCRSIZE(1920),
SYSOUT(A),
TIMEOUT(5),
TRACE(C000),
TRCLASS(A),
UNALLOC(NO)
/***/
/* GROUP ISFSPROG */
/***/
GROUP NAME(ISFSPROG),AUPDT(2),
TSOAUTH(JCL,OPER,ACCT),
ACTION(ALL),
ACTIONBAR(YES),
APPC(ON),
AUTH(ALL),
BROWSE(NONE),
CMDAUTH(ALL),
CMDLEV(7),
CONFIRM(ON),
CTITLE(ASIS),
CURSOR(ON),
DADFLT(IN,OUT,TRANS,STC,TSU,JOB),
DATE(MMDDYYYY),
DATESEP('/'),
LOGOPT(OPERACT),
Connected to 24.234.192.41 port 7123
32/34
09:55:52 IBM-3278-4 - TCP00001
9:55 AM

ISFACR


SDSF Security Conversion Assist Menu
More: +
The Security Conversion Assist gives you a head start on the conversion to RACF security. It does not provide a complete, automated conversion. It supports most of the ISFGRP/GROUP parameters of ISFPARMS. For a complete list of supported parameters, tab the cursor to the highlighted ISFGRP/GROUP and press Enter.
You may want to simply use the generated commands as a sample to help you understand RACF security. Or, after carefully reviewing and modifying the commands, you may want to issue them to provide RACF security. Use the conversion assist in conjunction with SDSF Operation and Customization, SA22-7670, which describes both ISFPARMS and RACF security for SDSF.

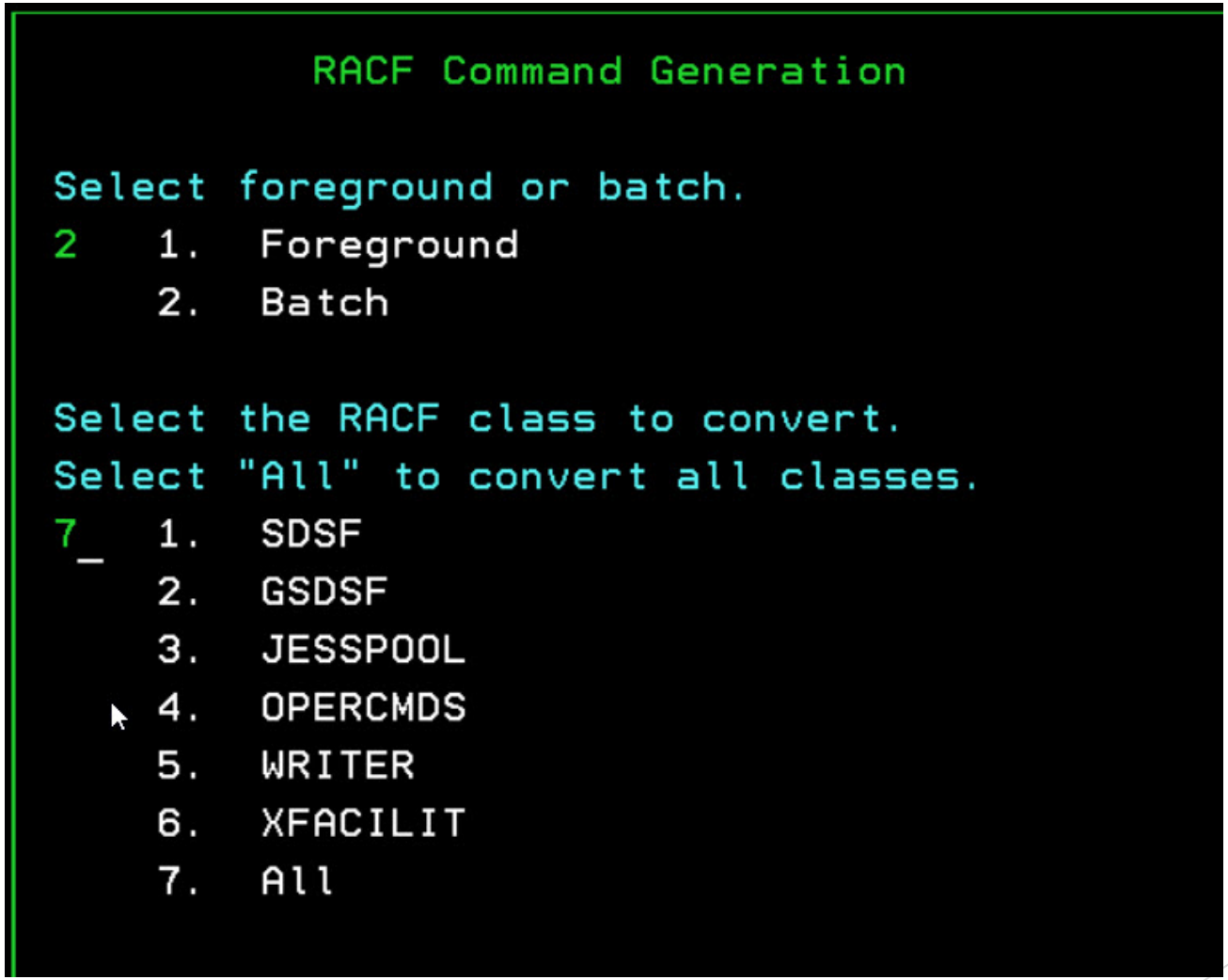
ISFACR


SDSF Security Conversion Assist
Select conversion steps in order.
1. Define profile
2. Convert ISFPARMS to profile descriptions
3. Review profile descriptions
4. Convert descriptions to RACF commands
5. Review RACF commands
F1=Help F12=Cancel

ISFACR


SDSF Security Conversion Assist Profile
ISFPARMS input data set
===> 'SYS1.PARMLIB(ISFPRM00)'
Profile description data set
===> 'adcdmst.in.sdsf'
CLIST library
===> 'ISF.AISFEXEC'
RACF commands data set
===> 'adcdmst.sdsfracf.clist'
Prefix for generated GROUP names
===> ISF
Owner group name for resource profiles
===> ISF
JES names for use in RACF resources
JES2 name ===> JES2
JES3 name ===> JES3

ISFACR


RACF Command Generation
Select foreground or batch.
2 1. Foreground
2. Batch
Select the RACF class to convert.
Select "All" to convert all classes.
7_ 1. SDSF
2. GSDSF
3. JESSPOOL
4. OPERCMDS
5. WRITER
6. XFACILIT
7. All

ISFACR

```
95 profiles in class SDSF
102 profiles in class SDSF
6 profiles in class GSDSF
203 profiles in class OPERCMDS
4 profiles in class WRITER
connect users to tsoauth group
JCL 0
OPER 0
ACCT 0
AUTH = ALL
CMDAUTH = ALL
CMDLEV = 7
DSPAUTH = ALL
```

ISFACR

```
/* ********************************************** */
 /* Note:  The set of RACF commands contained in this  */
 /* exec should be considered a sample.  Do not invoke */
 /* the exec before carefully reviewing its contents.  */
 /* You may need to add, modify and delete RACF        */
 /* commands.  See SDSF Operation and Customization,   */
 /* SA22-7670, for information on using the Security   */
 /* Conversion Assist and on SDSF security.            */
 /* ********************************************** */
  CONTROL MAIN NOFLUSH

 SETROPTS GENERIC(SDSF WRITER JESSPOOL OPERCMDS XFACILIT)
 SETROPTS GENCMD(SDSF WRITER JESSPOOL OPERCMDS XFACILIT)
```

ISFACR

- /* Commands for GLOBAL profiles */
- RDEFINE GLOBAL JESSPOOL OWNER(ISF) UACC(NONE) DATA('JESSPOOL') AUDIT(ALL)
- RALTER GLOBAL JESSPOOL NOWARNING
- RALTER GLOBAL JESSPOOL ADDMEM(*.&RACUID.*/ALTER)
- RALTER GLOBAL JESSPOOL ADDMEM(*.*.&RACUID*/ALTER)

ISFACR

- /* Commands for JESSPOOL profiles */
- RDEFINE JESSPOOL *.*.$JESNEWS.*.D*.JESNEWS OWNER(ISF) UACC(READ) DATA('JESNEWS') AUDIT(ALL)
- RALTER JESSPOOL *.*.$JESNEWS.*.D*.JESNEWS NOWARNING
- PERMIT *.*.$JESNEWS.*.D*.JESNEWS CLASS(JESSPOOL) ID(CHANGE) ACCESS(ALTER)
- RDEFINE JESSPOOL *.*.*.*.*.JESTRACE OWNER(ISF) UACC(NONE) DATA('JESTRACE') AUDIT(ALL)
- RALTER JESSPOOL *.*.*.*.*.JESTRACE NOWARNING
- PERMIT *.*.*.*.*.JESTRACE CLASS(JESSPOOL) ID(CHANGE) ACCESS(ALTER)

ISFACR

```
/* Commands for  GSDSF  profiles */
 RDEFINE  GSDSF ATTR.CMD2 OWNER(ISF) UACC(NONE) DATA('COMMAND_LEVEL') AUDIT(ALL)
 RALTER GSDSF ATTR.CMD2 NOWARNING
 RALTER GSDSF ATTR.CMD2  ADDMEM(ISFATTR.OUTPUT.BURST)
 RALTER GSDSF ATTR.CMD2  ADDMEM(ISFATTR.OUTPUT.CLASS)
 RALTER GSDSF ATTR.CMD2  ADDMEM(ISFATTR.OUTPUT.COPYCNT)
 RALTER GSDSF ATTR.CMD2  ADDMEM(ISFATTR.OUTPUT.DEST)
 RALTER GSDSF ATTR.CMD2  ADDMEM(ISFATTR.OUTPUT.FCB)
 RALTER GSDSF ATTR.CMD2  ADDMEM(ISFATTR.OUTPUT.FLASH)
 RALTER GSDSF ATTR.CMD2  ADDMEM(ISFATTR.OUTPUT.FORMS)
 RALTER GSDSF ATTR.CMD2  ADDMEM(ISFATTR.OUTPUT.ODISP)
```

ISFACR

- /* Commands for SDSF profiles */
- RDEFINE SDSF ISFCMD.DSP.ACTIVE.JES2 OWNER(ISF) UACC(NONE) DATA('SDSF_COMMANDS') AUDIT(ALL)
- RALTER SDSF ISFCMD.DSP.ACTIVE.JES2 NOWARNING
- PERMIT ISFCMD.DSP.ACTIVE.JES2 CLASS(SDSF) ID(ISFOPER) ACCESS(READ)
- PERMIT ISFCMD.DSP.ACTIVE.JES2 CLASS(SDSF) ID(ISFSPROG) ACCESS(READ)
- PERMIT ISFCMD.DSP.ACTIVE.JES2 CLASS(SDSF) ID(ISFUSER) ACCESS(READ)

ISFACR

```
/* Commands for  WRITER  profiles */
 RDEFINE  WRITER JES2.LOCAL.PU* OWNER(ISF) UACC(NONE) DATA('WRITER_COMMANDS') AUDIT(ALL)
 RALTER WRITER JES2.LOCAL.PU* NOWARNING
 PERMIT JES2.LOCAL.PU* CLASS(WRITER) ID(ISFOPER) ACCESS(READ)
 PERMIT JES2.LOCAL.PU* CLASS(WRITER) ID(ISFSPROG) ACCESS(READ)
 RDEFINE  WRITER JES2.LOCAL.PR* OWNER(ISF) UACC(NONE) DATA('WRITER_COMMANDS') AUDIT(ALL)
 RALTER WRITER JES2.LOCAL.PR* NOWARNING
 PERMIT JES2.LOCAL.PR* CLASS(WRITER) ID(ISFOPER) ACCESS(READ)
 PERMIT JES2.LOCAL.PR* CLASS(WRITER) ID(ISFSPROG) ACCESS(READ)
```

ISFACR

```
/* Commands for  OPERCMDS  profiles */
 RDEFINE  OPERCMDS JES2.* OWNER(ISF) UACC(NONE) DATA('SDSF_OPERCOMMANDS') AUDIT(ALL)
 RALTER OPERCMDS JES2.* NOWARNING
 PERMIT JES2.* CLASS(OPERCMDS) ID(CHANGE) ACCESS(ALTER)
 PERMIT JES2.* CLASS(OPERCMDS) ID(ISFOPER) ACCESS(ALTER)
 PERMIT JES2.* CLASS(OPERCMDS) ID(ISFSPROG) ACCESS(ALTER)
 RDEFINE  OPERCMDS JES2.CANCEL.BAT OWNER(ISF) UACC(NONE) DATA('SDSF_OPERCOMMANDS') AUDIT(ALL)
 RALTER OPERCMDS JES2.CANCEL.BAT NOWARNING
 PERMIT JES2.CANCEL.BAT CLASS(OPERCMDS) ID(ISFOPER) ACCESS(UPDATE)
 PERMIT JES2.CANCEL.BAT CLASS(OPERCMDS) ID(ISFSPROG) ACCESS(UPDATE)
 PERMIT JES2.CANCEL.BAT CLASS(OPERCMDS) ID(ISFUSER) ACCESS(UPDATE)
```

SDSF Class – Profiles

```
CLASS      NAME
-----      ----
SDSF       ISF*.** (G)

GROUP CLASS NAME
----- ----- ----
GSDSF

RESOURCE GROUPS
-------- ------
NONE

LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
-----  --------   ----------------  -----------  -------
 00    SYS1            READ              ALTER    NO

USER      ACCESS
----      ------
ADCDMST   ALTER
IBMUSER   ALTER
```

SDSF Class – Profiles

```
CLASS      NAME
 -----      ----
 OPERCMDS   JES%.** (G)

 LEVEL  OWNER      UNIVERSAL ACCESS  YOUR ACCESS  WARNING
 -----  --------   ----------------  -----------  -------
  00    IBMUSER        CONTROL          CONTROL    NO


 USER      ACCESS
 ----      ------
 IBMUSER   ALTER
 SYS1      CONTROL
```

SDSF Security Introduction

Julie Bergh

berghju@gmail.com

BACKUP SLIDES

SDSF - Options

SMSG	SMS storage groups	Devices
SMSV	SMS volumes	Devices
DEV	Device activity	Devices
DA	Active users	Jobs
I	Input Queue	Jobs
ST	Status of jobs	Jobs
AS	Address space memory	Jobs

SDSF - Options

JG	Job groups	JES
MAS	Members in the MAS	JES
JC	Job classes	JES
INIT	Initiators	JES
PR	Printers	JES
PUN	Punches	JES
RDR	Readers	JES
SO	Spool offload	JES
SP	Spool volumes	JES
RM	Resource monitor	JES
PROC	Proclib data sets	JES
RMA	Resource monitor alerts	JES
JES	Job entry subsystems	JES
JRI	JES resource information	JES
JRJ	JES resource by job	JES

SDSF - Options

LOG	System log	Log
SR	System requests	Log
ULOG	User session log	Log
VMAP	Virtual storage map	Memory
CSR	Common storage remaining	Memory
LINE	Lines	Network
NODE	Nodes	Network
NS	Network servers	Network
NC	Network connections	Network
NA	Network activity	Network
O	Output Queue	Output
H	Held output Queue	Output

SDSF - Options

PS	Processes	OMVS
FS	File systems	OMVS
BPXO	OMVS options	OMVS
ENQD	Enqueued datasets	Sysplex
CFC	CF Connections	Sysplex
CFS	CF Structures	Sysplex
EMCS	Extended consoles	Sysplex
XCFM	XCF groups and members	Sysplex

SDSF - Options

SYM	System symbols	System
SYS	System information	System
ENQ	Enqueues	System
ENQC	Enqueue contention	System
DYNX	Dynamic exits	System
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
SSI	Subsystem information	System
GT	Generic tracker	System
LPD	Link pack directory	System

SDSF - Options

SE	Scheduling environments	WLM
RES	WLM resources	WLM
ENC	Enclaves	WLM
WLM	WLM policy data	WLM
SRVC	Service classes	WLM
REPC	WLM report classes	WLM
RGRP	WLM resource groups	WLM
WKLD	WLM workloads	WLM

SDSF Class – Profiles

- **ISFAPF - Protecting authorized program facility data sets**
- **ISF.CONNECT - Connection to SDSFAUX**
- **ISFXCFM - XCF groups and members**
- **ISFCFC - Protecting CF connections**
- **ISFCFS - Protecting CF structures**
- **HZS. - Checks on the CK and CKH panels**
- **ISFOPER - Protecting destination names**
- **ISFAUTH - Protecting destination names.**

SDSF Class – Profiles

ISFDEV - Protecting device activity
ISFDYNX - Protecting dynamic exits
ISFEMCS - Protecting EMCS consoles
ISFENC - Protecting enclaves
ISFENQ - Protecting Enqueue Information
ISFFS - Protecting file systems
ISFGT - Protecting generic tracker events
ISFINIT - Protecting initiators
ISFRM - Protecting JES2 resources
ISFJES - Protecting JES subsystems

SDSF Class – Profiles

ISFJOBCL - Protecting job classes and job class members

ISFJDD – Protecting job devices - Jobs, job groups, output groups, and SYSIN/SYSOUT data sets – JES uses the JESSPOOL class to protect SYSIN/SYSOUT data sets and the EVENTLOG, which SDSF uses to display job step information. SDSF extends the use of the JESSPOOL class to protect SDSF job and output group resources as well.

SDSF Class – Profiles

ISFJRI - Protecting JESInfo resources
ISFJRJ - Protecting JESInfo by job resources
ISFLINES - Protecting lines
ISFLNK - Protecting link list data sets
ISFMEMB - Protecting MAS and JESPLEX members

GROUP – (SDSF class) - You can control membership in groups defined by ISFPARMS using SAF. This is an alternative to using ISFPARMS to control membership in the groups. Controlling membership in groups

SDSF Class – Profiles

ISFOPER - MVS and JES commands on the command line (/)
ISFNETACT - Protecting network activity
ISFAPPL - Protecting network connections
ISFSOCK Protecting network connections
ISFNS - Protecting network servers
ISFNODE - Protecting nodes
ISFOMVS - Protecting OMVS options
SYSPLEX.OPERLOG (LOGSTRM)
ISFATTR - Overtypable fields

SDSF Class – Profiles

ISFPAGE - Protecting page data sets
ISFPARM - Protecting PARM data sets
WRITER class - Protecting printers / Punches
ISFPROG - Protecting processes
ISFPLIB - Protecting proclibs
ISFRDR - Protecting readers
ISFRMA - Protecting resource monitor alerts
ISFRES - Protecting WLM resources
ISFSE - Protecting scheduling environments
SERVER - Protecting the SDSF server
ISFSTORGRP - Protecting SMS storage groups
ISFSMSVOL - Protecting SMS volumes
ISFSO - Protecting spool offloaders

SDSF Class – Profiles

ISFSP - Protecting spool volumes
ISFSUBSYS - Protecting subsystems
SYSLOG – JESSPOOL - Protecting the logical log
ISFSYM- Protecting system symbol information
ISFSYS - Protecting system information
ISFSR - Protecting system requests
ULOG – user log - OPERCMDS
ISFXCFM - Protecting XCF groups and members