z/OS
2.5

SDSF Security Migration Guide

SC27-4942-50

Note

Before using this information and the product it supports, read the information in “Notices” on page 99.

This edition applies to Version 2 Release 5 of z/OS® (5650-ZOS) and to all subsequent releases and modifications until otherwise indicated in new editions.

Last updated: 2023-06-28

Contents

Figures

Tables

About this document

This documentation describes how to migrate from using SDSF security with ISFPARMS (ISFPRMxx or ISFPARMS with assembler macros) to RACF® security. It also describes how to implement recommended SDSF security best practices.

z/OS information

This information explains how z/OS references information in other documents and on the web.

When possible, this information uses cross document links that go directly to the topic in reference using shortened versions of the document title. For complete titles and order numbers of the documents for all products that are part of z/OS, see *z/OS Information Roadmap*.

To find the complete z/OS library, go to IBM Documentation (www.ibm.com/docs/en/zos).

How to send your comments to IBM

We invite you to submit comments about the z/OS product documentation. Your valuable feedback helps to ensure accurate and high-quality information.

Important: If your comment regards a technical question or problem, see instead "If you have a technical problem" on page xiii.

Submit your feedback by using the appropriate method for your type of comment or question:

Feedback on z/OS function
If your comment or question is about z/OS itself, submit a request through the IBM RFE Community (www.ibm.com/developerworks/rfe/).

Feedback on IBM® Documentation function
If your comment or question is about the IBM Documentation functionality, for example search capabilities or how to arrange the browser view, send a detailed email to IBM Documentation Support at ibmdoc@us.ibm.com.

Feedback on the z/OS product documentation and content
If your comment is about the information that is provided in the z/OS product documentation library, send a detailed email to mhvrcfs@us.ibm.com. We welcome any feedback that you have, including comments on the clarity, accuracy, or completeness of the information.

To help us better process your submission, include the following information:

- Your name, company/university/institution name, and email address
- The following deliverable title and order number: z/OS SDSF Security Migration Guide, SC27-4942-50
- The section title of the specific information to which your comment relates
- The text of your comment.

When you send comments to IBM, you grant IBM a nonexclusive authority to use or distribute the comments in any way appropriate without incurring any obligation to you.

IBM or any other organizations use the personal information that you supply to contact you only about the issues that you submit.

If you have a technical problem

If you have a technical problem or question, do not use the feedback methods that are provided for sending documentation comments. Instead, take one or more of the following actions:

- Go to the IBM Support Portal (support.ibm.com).
- Contact your IBM service representative.
- Call IBM technical support.

Summary of changes

This information includes terminology, maintenance, and editorial changes. Technical changes or additions to the text and illustrations for the current edition are indicated by a vertical line to the left of the change.

Note: IBM z/OS policy for the integration of service information into the z/OS product documentation library is documented on the z/OS Internet Library under IBM z/OS Product Documentation Update Policy (www-01.ibm.com/servers/resourcelink/svc00100.nsf/pages/ibm-zos-doc-update-policy?OpenDocument).

Summary of changes for SDSF 2.5

The following content is new, changed, or no longer included in SDSF 2.5.

New

The following content is new.

April 2023 refresh

The ISFNTCNV batch utility was added to assist in translating NTBL/NTBLENT statements during migration. Topics "Migration tools" on page 17 and "Setting up the NTBL conversion utility ISFNTCNV" on page 18 were added.

Information was added about editing the ISFRACEX sample member in the SISFJCL data set instead of running ISFACR to "Group names and owner" on page 23.

Changed

The following content is changed.

June 2023 refresh

Editorial changes were made to the documentation.

April 2023 refresh

Additional details about the ISFACR utility was added to "Setting up the security migration utility ISFACR" on page 20.

The list of parameters was updated in Appendix B, "ISFPARMS parameters not applicable to SAF," on page 57.

The topic Appendix E, "RACF profiles that protect MVS commands," on page 85 was updated.

Chapter 1. Introduction

This documentation describes how to migrate from using SDSF security with ISFPARMS (ISFPRMxx or ISFPARMS with assembler macros) to RACF security. It also describes how to implement recommended SDSF security best practices.

IBM has announced that the next release of the System Display and Search Facility (SDSF) will not support security via the ISFPARMS mechanism. All users of SDSF 2.5.0 must use the Security Authorization Facility (SAF) with an External Security Manager (ESM) such as RACF, ACF2, or TSS. This will simplify SDSF security management and provide the following benefits:

- Centralizes security management in the ESM
- Allows dynamic changes to the security configuration
- Improves auditability

This documentation is not intended to explain how to set up a new SDSF security environment, but might provide suggestions on how to improve your current SDSF security.

This documentation is aimed at mainframe sites that currently use SDSF secured with ISFPARMS, and are planning to migrate to the latest release of SDSF.

This documentation focuses on RACF. SDSF interacts with RACF to control access to several resources (such as SDSF panels, commands, and batch jobs). All references to SAF with an ESM refer to RACF. However, the SDSF security information in this documentation also can be applied to ACF2 and TSS.

The technical person or team implementing this conversion must be proficient in z/OS and RACF.

Chapter 2. How RACF and SDSF work together

SDSF provides users with the ability to securely monitor and control their z/OS system(s), in both JES2 and JES3 environments. Information that is displayed in SDSF includes batch job output, Unix System Services (USS) processes, started tasks, TSO user IDs, system configuration, printers, and other z/OS resources and components. RACF security is used to protect access to these SDSF resources by defining classes and profiles.

SDSF can be invoked via ISPF or TSO. The menu options available to users depends on their security access. Until now, their security access could be defined through either RACF or through ISFPARMS (ISFPRMxx or ISFPARMS with assembler macros). ISFPARMS can also be used as a backup to SAF, for when RACF cannot make a security decision.

Some SDSF functions require users to have access to several RACF classes and profiles with a correct level of authority (READ, CONTROL, UPDATE or ALTER).

With the deprecation of ISFPARMS security support for SDSF, SAF with an ESM (RACF, for example) becomes the only supported security method.

How access is checked

In SDSF version 2.4.0 or earlier, when a user accesses SDSF, the SDSF client program attempts to connect to the SDSF address space (also referred to as the SDSF server). To connect to the SDSF server, the user must have READ access to profile ISF.CONNECT.sysname in the SDSF class.

If the SDSF address space is not active, SDSF provides limited functionality. The user must have READ access to profile SERVER.NOPARM in the SDSF class so that ISFPARMS with assembler macros can be used instead of ISFPRMxx. SDSF panels that require the use of the SDSFAUX data gatherers (such as APF, LPA, and LNK) are not available.

If the SDSF address is active, but no ISFPRMxx is in effect (for instance, when a syntax error is found during startup), SDSFAUX is not started. The user requires access to RACF profile SERVER.NOPARM to fall back to ISFPARMS with assembler macros and requires READ access to RACF profile ISF.CONNECT.sysname to continue. SDSF panels that require the use of SDSFAUX are not available.

If the SDSF address space is active, but the RACF class SDSF is not active or not RACLISTed, the SDSF server allows requests based on the ISFPRMxx CONNECT definition. When AUXSAF(FAILRC4) is in effect (which is the default), the request is denied. The user cannot connect to the SDSF server and the SDSFAUX-related panels are not available. SDSF falls back to ISFPARMS with assembler macros because access to RACF profile SERVER.NOPARM results in a return code 04 (cannot determine the result).

When AUXSAF(NOFAILRC4) is in effect, the server allows the request, but access to the panel is controlled through the definitions in ISFPARMS with assembler macros.

RACF classes that protect SDSF

Several RACF classes are used to secure the SDSF environment.

Table 1. RACF classes used to secure SDSF

RACF Class	**Description**
JESSPOOL	Controls access to job data sets on the JES spool (that is, SYSIN and SYSOUT data sets).
LOGSTRM	Controls access to system logger resources, such as log streams and the coupling facility structures associated with them.
OPERCMDS	Controls who can issue operator commands.

Table 1. RACF classes used to secure SDSF (continued)	
RACF Class	**Description**
SDSF	Controls the use of authorized commands and functions in SDSF.
WRITER	Controls the user of JES2 printers and outbound NJE processing.
XFACILIT	General purpose class similar to FACILITY class but supporting longer resource and profile names (up to 246 characters).

A more detailed view of the SDSF functions and resources being protected by these RACF classes can be found in the table below.

Table 2. SDSF functions and resources and corresponding RACF classes			
Function	**Specific Function**	**RACF CLASS**	**Resources to Protect**
Jobs and output	Display job and output queues	SDSF	DA, H, I, O, and ST authorized commands
	Issue action characters	JESSPOOL	Job or output group
		OPERCMDS	Generated MVS or JES command
		SDSF	JD, JM and JY action characters for job devices, memory and delays
	Overtype fields	SDSF	Overtypeable field
		JESSPOOL	Job or output group
		OPERCMDS	Generated MVS or JES command
	Browse output	JESSPOOL	SYSIN/SYSOUT data sets
Printers	Display printers	SDSF	PR authorized command
	Issue action characters	WRITER	Printer
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Overtypeable field
		WRITER	Printer
		OPERCMDS	Generated MVS or JES command

Table 2. SDSF functions and resources and corresponding RACF classes (continued)

Function	Specific Function	RACF CLASS	Resources to Protect
Initiators	Display initiators	SDSF	INIT authorized command
	Issue action characters	SDSF	Initiator
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Overtypeable field
		SDSF	Initiator
		OPERCMDS	Generated MVS or JES command
Lines	Display lines	SDSF	LI authorized command
	Issue action characters	SDSF	Line
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Overtypeable field
		SDSF	Line
		OPERCMDS	Generated MVS or JES command
Nodes	Display nodes	SDSF	NO authorized command
	Issue action characters	SDSF	Node
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Overtypeable field
		SDSF	Node
		OPERCMDS	Generated MVS or JES command
Spool offloaders (JES2 only)	Display spool offloaders	SDSF	SO authorized command
	Issue action characters	SDSF	Offloader
		OPERCMDS	Generated MVS or JES2 command
	Overtype fields	SDSF	Overtypeable field
		SDSF	Offloader
		OPERCMDS	Generated MVS or JES2 command

Table 2. SDSF functions and resources and corresponding RACF classes (continued)			
Function	**Specific Function**	**RACF CLASS**	**Resources to Protect**
MAS and JESPLEX members	Display the MAS or JESPLEX members	SDSF	MAS or JP authorized command
	Issue action characters	SDSF	MAS or JESPLEX members
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Overtypeable field
		SDSF	MAS or JESPLEX members
		OPERCMDS	Generated MVS or JES command
Network connections	Display network connections	SDSF	NC authorized command
	Issue action characters	SDSF	Network connection
		OPERCMDS	Generated JES command
Network servers	Display network servers	SDSF	NS authorized command
	Issue action characters	SDSF	Network server
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Overtypeable field
		SDSF	Network server
		OPERCMDS	Generated MVS or JES command
Punches	Display punches	SDSF	PUN authorized command
	Issue action characters	SDSF	Punch
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Overtypeable field
		SDSF	Punch
		OPERCMDS	Generated MVS or JES command

Table 2. SDSF functions and resources and corresponding RACF classes (continued)			
Function	**Specific Function**	**RACF CLASS**	**Resources to Protect**
Readers	Display readers	SDSF	RDR authorized command
	Issue action characters	SDSF	Reader
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Overtypeable field
		SDSF	Reader
		OPERCMDS	Generated MVS or JES command
Checks	Display checks	SDSF	CK authorized command
	Display check history	LOGSTRM	Log stream
	Issue action characters	XFACILIT	Check
		OPERCMDS	Generated MVS command
	Overtype fields	SDSF	Overtypeable field
		XFACILIT	Check
		OPERCMDS	Generated MVS command
Enclaves	Display enclaves	SDSF	ENC authorized command
	Issue action characters	SDSF	Enclave
	Overtype fields	SDSF	Overtypeable field
		SDSF	Enclave
JES2 resources (JES2 only)	Display JES2 resources	SDSF	RM authorized command
	Issue action characters	SDSF	Resource
		OPERCMDS	Generated MVS or JES2 command
	Overtype fields	SDSF	Overtypeable field
		SDSF	Resource
		OPERCMDS	Generated MVS or JES2 command

Table 2. SDSF functions and resources and corresponding RACF classes (continued)			
Function	**Specific Function**	**RACF CLASS**	**Resources to Protect**
Job classes	Display job classes	SDSF	JC authorized command
	Issue action characters	SDSF	Job class
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Overtypeable field
		SDSF	Job class
		OPERCMDS	Generated MVS or JES command
Job devices	Display job devices	SDSF	JD action character
	Issue action characters	SDSF	Job devices
		OPERCMDS	Generated MVS or JES command
Spool volumes	Display spool volumes	SDSF	SP authorized command
	Issue action characters	SDSF	Spool volume
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Overtypeable field
		SDSF	Spool volume
		OPERCMDS	Generated MVS or JES command
WLM resources	Display WLM resources	SDSF	RES authorized command
	Issue action characters	SDSF	WLM resource
		OPERCMDS	Generated MVS command
	Overtype fields	SDSF	Overtypeable field
		SDSF	WLM resource
		OPERCMDS	Generated MVS command
Scheduling environments	Display scheduling environments	SDSF	SE authorized command
	Issue action characters	SDSF	Scheduling environment Generated MVS command
System requests	Display system requests	SDSF	SR authorized command
	Issue action characters	SDSF	System request Generated MVS command

Table 2. SDSF functions and resources and corresponding RACF classes (continued)

Function	Specific Function	RACF CLASS	Resources to Protect
Enqueues	Display enqueues	SDSF	ENQ authorized command
	Issue action characters	SDSF OPERCMDS	Enqueue Generated MVS command
System symbols	Display system symbols	SDSF	SYM authorized command
	Issue action characters	SDSF OPERCMDS	Symbol Generated MVS command
z/OS UNIX processes	Display processes	SDSF	PS authorized command
	Issue action characters	SDSF OPERCMDS	Process Generated MVS command
Display the system log	Display the LOG panel	SDSF	LOG authorized command
	Access the logical log (SYSLOG)	JESSPOOL	JESSPOOL
	Access the log stream (OPERLOG)	LOGSTRM	LOGSTRM
Destination operator authority	Issue action characters	SDSF	Operator authority
		SDSF	Jobs or output based on destination name
		OPERCMDS	Generated MVS or JES command
	Overtype fields	SDSF	Operator authority
		SDSF	Overtypeable field
		SDSF	Jobs or output based on destination name
		OPERCMDS	Generated MVS or JES command
	Browse output	SDSF	Operator authority
		SDSF	Data sets based on job or output group destination

Table 2. SDSF functions and resources and corresponding RACF classes (continued)			
Function	**Specific Function**	**RACF CLASS**	**Resources to Protect**
System commands and responses	Use / command	SDSF SDSF	ULOG authorized command / command
		OPERCMDS	MVS and JES require authorisation to OPERCMDS resources for MVS and JES commands issued.
SDSF commands	Use DEST command	SDSF	DEST authorized command
		SDSF	Destination names
	Use authorized SDSF commands	SDSF	SDSF authorized commands
SDSF server	Refresh ISFPARMS or change server options, start and stop the server and server communications	OPERCMDS	START, MODIFY, and STOP commands

For a list of RACF profiles involved in protecting SDSF, see Appendix C – RACF Classes and Profiles to Protect SDSF.

Chapter 3. Analyzing your current SDSF environment

Before beginning to convert ISFPARMS to RACF, validate and analyze your current SDSF security position.

Consider the following:

- How is SDSF security currently set up?
  - Is it using ISFPARMS?
  - Does it use RACF classes and profiles?
- Who uses SDSF?
  - How are these user IDs grouped?
  - What access do these users and groups currently have?
  - What access will users and groups require?
- Is the SDSF class RACLISTed?

To answer these questions, collect and document information about the current state of the mainframe system as pertaining to SDSF security.

Understanding the SDSF user population is critical for planning and migration steps, and may vary from system to system. From a high-level perspective, the SDSF user population typically is divided into the following general areas:

- System programmers
- Operators
- End users

To facilitate security management, users with the same role or level of access are grouped together.

With ISFPARMS, users can be assigned to groups in either RACF or ISFPARMS.

Ways to assess the current SDSF security setup

There are several programs and commands that you can use to assess the current SDSF security configuration.

Option 1: IBM Health Checker for z/OS

You can use SDSF and IBM Health Checker for z/OS. The following is an example of the SDSF Health Checker display:

```
SDSF HEALTH CHECKER DISPLAY  RSMG                       LINE 102-120 (184)
COMMAND INPUT ===>                                          SCROLL ===> CSR
NP   NAME                              CheckOwner       State              Status
     SDSF_CLASS_SDSF_ACTIVE            IBMSDSF          ACTIVE(ENABLED)    SUCCESSFUL
     SDSF_ISFPARMS_IN_USE              IBMSDSF          ACTIVE(ENABLED)    SUCCESSFUL
```

Select the option **SDSF_CLASS_SDSF_ACTIVE** to view details about the SDSF class.

```
CHECK(IBMSDSF,SDSF_CLASS_SDSF_ACTIVE)
SYSPLEX:    LOCAL     SYSTEM: RSMG
START TIME: 10/15/2020 08:45:28.058636
CHECK DATE: 20080324  CHECK SEVERITY: LOW

ISFH1015I The class SDSF is active.

END TIME: 10/15/2020 08:45:28.067733  STATUS: SUCCESSFUL
```

Select option **SDSF_ISFPARMS_IN_USE** to view information about the ISPPARMS.

```
CHECK(IBMSDSF,SDSF_ISFPARMS_IN_USE)
SYSPLEX:    LOCAL     SYSTEM: RSMG
START TIME: 10/15/2020 08:45:28.058170
CHECK DATE: 20170105  CHECK SEVERITY: LOW

ISFH1001I SDSF server SDSF is using statements from member ISFPRM00 of
data set SYS1.PARMLIB.LOCAL.

END TIME: 10/15/2020 08:45:28.062913  STATUS: SUCCESSFUL
```

Option 2: RACF command SETROPTS LIST

If you don't have access to IBM Health Checker, you can issue the RACF command SETROPTS LIST to see if the SDSF class is active. The following example shows the results from this command:

```
ACTIVE CLASSES = DATASET USER GROUP ACCTNUM APPL CSFKEYS CSFSERV DIGTCERT
                 DIGTCRIT DIGTNMAP DIGTRING EJBROLE FACILITY GCSFKEYS
                 GEJBROLE GSDSF GXCSFKEY GXFACILI GZMFAPLA JESSPOOL LOGSTRM
                 NODES NODMBR OPERCMDS PTKTDATA PTKTVAL RACFVARS RVARSMBR
                 SDSF SERVAUTH SERVER STARTED SURROGAT TSOAUTH TSOPROC
                 UNIXPRIV WBEM XCSFKEY XFACILIT ZMFAPLA
ZMFCLOUD
```

Option 3: SDSF started task message or DISPLAY command

Another way to identify which ISFPRMxx member is in use is by checking the SDSF started task job output for message IEE252I.

```
IEE252I MEMBER ISFPRM00 FOUND IN SYS1.PARMLIB.LOCAL
```

You can also use the MVS F SDSF, DISPLAY command to see which ISFPRMxx member is in use.

```
 RESPONSE=SS01      ISF304I Modify DISPLAY command accepted.
 RESPONSE=SS01      ISF312I SDSF Display
 RESPONSE=SS01         Server status:  Active       Default: Yes
 RESPONSE=SS01         Communications: Active
 RESPONSE=SS01         Parms: ISFPRMRS / STSUV.PARMLIB
 RESPONSE=SS01         XCF Communications: Configured
 RESPONSE=SS01         AuxName: SDSFAUX
```

Option 4: SDSF WHO command

The SDSF WHO command can also be used to check how SDSF security is set up for your own user ID.

```
USERID=SYS001,PROC=RSMPROC,TERMINAL=A05TCP20,GRPINDEX=1,GRPNAME=ISFSPROG,
MVS=z/OS 02.04.00,JES=z/OS 2.4,SDSF=HQX77C0,ISPF=7.4,RMF/DA=HSF,SERVER=YES,
SERVERNAME=SDSF,JESNAME=JES2,MEMBER=RSMG,JESTYPE=JES2,SYSNAME=RSMG,
SYSPLEX=LOCAL,COMM=NOTAVAIL,COMMX=ENABLED,JOBID=TSU00826
```

ISFPARMS with assembler macros

You must determine if your system still uses ISFPARMS with assembler macros. ISFPARMS was previously defined to SDSF by using assembler macros, and is still supported in JES2 for compatibility reasons. This method is not supported by JES3.

By default, the ISFPARMS module is located in LINKLST data set ISF.SISFLOAD.

If ISFPARMS with assembler macros is still in use, review the module and note the configuration parameters that are defined to SDSF.

Understanding the users and groups

The following parameters are used in ISFPARMS with assembler macros to define groups and users:

Table 3. Parameters for ISFPARMS with assembler macros	
Parameter	**Description**
macro label	Group name, used in SAF resource.
ILPROC=ISFNTBL-label	Includes users by logon procedure.
XLPROC=ISFNTBL-label	Excludes users by logon procedure.
ITNAME=ISFNTBL-label	Includes users by terminal name.
XTNAME=ISFNTBL-label	Excludes users by terminal name.
IUID=ISFNTBL-label	Includes users by user ID.
XUID=ISFNTBL-label	Excludes users by user ID.
TSOAUTH=attributes	Includes users by TSO authority.

Example 1 – Group of users defined with IUID parameter

```
ISFGRP IUID=GRPACC,
     PREFIX=USERID,
     AUTH=(ALLUSER)
GRPACC ISFNTBL TEST,1,DEV,1
```

The IUID parameter works with ISFNTBL macro GRPACC. This means that any user whose user ID that starts with the string TEST or DEV will be included in this group (for example: TEST01, TESTUSR, DEVUSR, DEV001, or DEV002).

The PREFIX parameter specifies that the users will only be able to see jobs in SDSF under their own prefix name (such as DEV001*).

The AUTH parameter identifies the SDSF panels that users of this group are allowed to display, and the SDSF commands that they are allowed to issue.

Example 2 – Group of users defined in RACF

```
GRPSDSF1 ISFGRP
AUTH=(DA,I,O,H,ST,DEST,PREF),
     PREFIX=USERID
```

In this example, group GRPSDSF1 is defined through the label on the ISFGRP macro. All members of this group will be authorized in RACF to profile GROUP.*group-name.server-name*. If SDSF is the server name, this translates to GROUP.GRPSDSF1.SDSF.

The PREFIX parameter set to USERID means that users only can see jobs in SDSF under their own prefix name (such as DEV001*).

ISFPRMxx statements

After you identify which ISFPRMxx member SDSF is using, you can determine how security is set up and assess how users are grouped and what they are authorized to do in SDSF.

Note: Consider that when RACF class SDSF is active and RACLISTed, and profiles are defined to it, this security supersedes ISFPRMxx.

The following parameters are used in ISFPRMxx to define groups and users:

Table 4. ISFPRMxx parameters	
Parameter	**Description**
NAME (*group-name*)	Group name, used in SAF resource.

Table 4. ISFPRMxx parameters (continued)	
Parameter	**Description**
ILPROC (*NTBL-name*)	Includes users by logon procedure.
XLPROC (*NTBL-name*)	Excludes users by logon procedure.
ITNAME (*NTBL-name*)	Includes users by terminal name.
XTNAME (*NTBL-name*)	Excludes users by terminal name.
IUID (*NTBL-name*)	Includes users by user ID.
XUID (*NTBL-name*)	Excludes users by user ID.
TSOAUTH (*attributes*)	Includes users by TSO authority.

Example 1 – Group of users defined with IUID parameter

```
GROUP IUID(GRPACC),
     PREFIX(USERID),
     AUTH(ALLUSER)
NTBL NAME(GRPACC)
     NTBLENT STRING(TEST),OFFSET(1)
     NTBLENT STRING(DEV),OFFSET(1)
```

The IUID parameter defines the NTBL statement labelled GRPACC. This means that any user whose user ID that starts with the string TEST or DEV will be included in this group (for example: TEST01, TESTUSR, DEVUSR, DEV001, DEV002).

The PREFIX parameter specifies that users will only be able to see jobs in SDSF under their own prefix name (such as DEV001*).

The AUTH parameter identifies the SDSF panels that users belonging to this group are allowed to display, and the SDSF commands that they are allowed to issue.

Example 2 – Group of users defined in RACF

```
GROUP NAME(GRPSDSF1) AUTH(DA,I,O,H,ST,DEST,PREF),
      PREFIX(USERID)
```

In this example, group GRPSDSF1 is being defined through the NAME parameter on the GROUP statement. All members of this group will be authorized in RACF to profile GROUP.*group-name.server-name*. If SDSF is the server name, this translates to GROUP.GRPSDSF1.SDSF.

The PREFIX parameter set to USERID means that users will only be able to see jobs in SDSF under their own prefix name (such as DEV001*).

RACF profiles

It is important to determine if certain RACF classes are active.

Note: Consider that when RACF class SDSF is active and RACLISTed, and profiles are defined to it, this security supersedes ISFPRMxx.

Determine whether RACF classes are active.

- The SDSF RACF class must be active and RACLISTed throughout the migration process.
- The following RACF classes are recommended to be active. If they are inactive, before activating them you should consider the impact on other resources (such as JES) and plan accordingly.
  - JESSPOOL
  - LOGSTRM
  - OPERCMDS

- WRITER
- XFACILIT

You can determine which profiles are defined in class SDSF and who has access to them by looking at the UACC and Access Control List.

Chapter 4. Planning for migration

Once you have an understanding of your system's current position, you can begin planning the steps to perform the migration.

To help with the SDSF security migration from ISFPARMS to RACF, refer to the checklist in ISFPARMS Security Migration to RACF – Checklist.

Migration tools

SDSF provides some tools to assist with migration.

The following utilities are included with SDSF in the ISF.SISFEXEC data set:

- ISFACR is an ISPF dialog-driven migration tool that interactively reads ISFPRMxx statements and generates a sequence of RACF commands that can act as a starter set for the migration effort.
- ISFNTCNV is a batch utility that helps you create RACF commands based on the NTBL/NTBLENT statements in ISFPRMxx. It generates the following:
  - A sequence of RACF ADDGROUP and CONNECT statements, assuming that the NTBL is used on the IUID keyword for one or more SDSF groups.
  - A sequence of RACF RDEFINEs for JESSPOOL profiles, assuming that the NTBL is used on the IDSP keyword for one or more SDSF groups.

Use of the ISFNTCNV batch utility provides a simpler alternative to using the ISFACR tool. ISFACR has several limitations based on the complexity of your security definitions and may not be appropriate at your installation. However, ISFACR generates a more comprehensive set of commands that those created by ISFNTCNV.

Instructions for using these utilities are provided in the topics that follow.

User ID access requirements

The user ID that performs the migration must have access to certain mainframe resources and other specific authorizations.

The user ID must be able to:

- Access TSO
- Access ISPF
- Access SDSF
- Access ULOG
- Access the ISFPARMS configuration, including:
  - ISFPRMxx residing in the PARMLIB
  - ISFPARM with assembler macros member
- Review IBM Health Checker results for SDSF
- Issue RACF commands, including SETROPTS LIST
- Modify its own TSO logon procedure
- Have TSO authority for JCL, ACCT, and OPER, and be able to run the ISFACR utility
- Run the ISFACR migration utility
- Have access to SMF or zSecure Access Monitor
- Modify ISFPRMxx
- Issue MVS DISPLAY and MODIFY commands

If a single user ID cannot perform all of these functions, the help of other user IDs with the correct level of access is required to complete the implementation of the SDSF security migration.

Setting up the NTBL conversion utility ISFNTCNV

The ISFNTCNV conversion utility can be used to process NTBL/NTBLENT statements in your ISFPRMxx and generate corresponding RACF commands.

Before you begin

ISFNTCNV is not intended to handle all security configurations, but to provide you with a starter set of RACF commands that you can modify based on your security implementation.

The conversion tool consists of sample members ISF.SISFJCL(ISFRACNT) and ISF.SISFEXEC(ISFNTCNV). ISFRACNT contains sample JCL to run the tool and ISFNTCNV is a REXX exec to process your ISFPRMxx statements.

The ISFNTCNV conversion utility ISFNTCNV tool reads your ISFPRMxx member, processes all of the NTBL/NTBLENT statements, and then generates the following :

- Generates a RACF ADDGROUP command for every NTBL statement. The RACF group name is taken from the NTBL statement. Following the ADDGROUP command is a set of RACF CONNECT commands for user IDs that match the associated NTBLENTs. These generated commands are written to the // CONNECT DD that is specified in the run JCL.
- A sequence of RDEFINEs for JESSPOOL profiles, built assuming that the NTBLENTs are used to define job names. These NTBLENTs would typically be referenced by group keywords such as IDSP. The generated commands are written to the //RDEFINE DD that is specified in the run JCL.

Important: ISFNTCNV does not assess the NTBL usage on the GROUP statements; it unconditionally generates both types of statements. You must determine whether the generated statements are accurate and edit the statements accordingly.

Note: ISFNTCNV ignores TYPE(DEST) NTBLs.

Procedure

1. Ensure that the submitting user ID has sufficient RACF authority to list all of the USERIDs in the system.
2. Ensure that the submitting user ID has READ access to the data set specified on the ISFPRM DD statement.
3. Check that the ISFPRMxx member is valid and able to be activated by the SDSF server without errors.

   The member need not be active when the ISFNTCNV tool is run.
4. In the ISFPRMxx member, ensure that each NTBL statement is on one line, including any TYPE keywords.
5. In the ISFPRMxx member, ensure that each NTBLENT statement is on one line.
6. Make a private copy of the ISFRACNT member of the SISFJCL data set and modify it for your site.

   Instructions are contained in the JCL comments. Refer to the following sample:

```
//ISFRACNT JOB <job card parameters>
//*
//********************************************************************
//* Licensed Materials - Property of IBM                             *
//* 5650-ZOS                                                         *
//* Copyright IBM Corp. 2021.                                        *
//* Copyright Rocket Software Inc. 2021.                             *
//*                                                                  *
//* Status = HQX77D0                                                 *
//*                                                                  *
//********************************************************************
//*                                                                  *
//* Sample JCL to run the ISFNTCNV conversion tool                   *
//*                                                                  *
```

```
//* Before using this job, note the following:                          *
//*                                                                     *
//*  1. Add the job parameters to meet your system requirements         *
//*                                                                     *
//*  2. Change the //SYSEXEC DD statement to reference your            *
//*     ISF.SISFEXEC data set name                                      *
//*                                                                     *
//*  3. Change the //ISFPRM DD statement to reference your              *
//*     ISFPRMxx member to process                                      *
//*                                                                     *
//*  4. Review the invocation of the ISFNTCNV exec and update the       *
//*     arguments as necessary.                                         *
//*                                                                     *
//*       %ISFNTCNV owner supgroup                                      *
//*                                                                     *
//*       where                                                         *
//*                                                                     *
//*         owner -    specifies the OWNER value to be used             *
//*                    on the generatsed ADDGROUP command               *
//*                    (default ISF)                                    *
//*                                                                     *
//*         supgroup - specifies the SUPGROUP value to be used          *
//*                    on the generated ADDGROUP command                *
//*                    (default ISF)                                    *
//*                                                                     *
//*  5. After running the conversion tool, review the generated         *
//*     commands and update as necessary before running them.           *
//*                                                                     *
//*********************************************************************
//*                                                                     *
//* EXTERNAL CLASSIFICATION = OTHER                                     *
//* END OF EXTERNAL CLASSIFICATION:                                     *
//*                                                                     *
//*********************************************************************
//*
//*--------------------------------------------------------------------*
//* Create a list of all userids defined to the system                 *
//*--------------------------------------------------------------------*
//LISTUSER  EXEC PGM=IKJEFT01,REGION=0M
//SYSPRINT  DD SYSOUT=*
//SYSTSPRT  DD DSN=&&USERS,
//             DISP=(,PASS),UNIT=SYSALLDA,
//             SPACE=(CYL,(10,10)),
//             DCB=(RECFM=VBA,LRECL=133,BLKSIZE=0)
//SYSIN     DD DUMMY
//SYSTSIN   DD *
  SEARCH CLASS(USER)
//*
//*--------------------------------------------------------------------*
//* Generate sample ADDGROUP, CONNECT, and RDEFINE statements          *
//*--------------------------------------------------------------------*
//NTBLCONV  EXEC PGM=IKJEFT01,REGION=0M
//*
//SYSEXEC   DD DISP=SHR,DSN=ISF.SISFEXEC            <=== Note 2
//SYSPRINT  DD SYSOUT=*
//SYSTSPRT  DD SYSOUT=*
//*
//USERS     DD DSN=&&USERS,DISP=OLD
//*
//ISFPRM    DD DISP=SHR,DSN=SYS1.PARMLIB(ISFPRM00)  <=== Note 3
//*
//CONNECT   DD SYSOUT=*
//RDEFINE   DD SYSOUT=*
//*
//SYSIN     DD DUMMY
//SYSTSIN   DD *         <=== Note 4
 %ISFNTCNV ISF ISF
//
******************************** Bottom of Data ************************
```

7. Submit the JCL.
8. Examine the RACF statements produced in the CONNECT and JESPPOOL ddnames and customize as required. Note that the statements should not be run as is; you must examine the statements carefully and modify them as needed.

Setting up the security migration utility ISFACR

The ISFACR security migration utility is provided with SDSF. It can be used to help convert ISFPARM security into RACF profiles in the SDSF class.

Before you begin

Important: ISFACR does not provide comprehensive coverage of all migration actions required. This utility serves only as a starting point to provide you with sample RACF commands based on your current security settings. All generated commands should be thoroughly reviewed and tested before being implemented. It is likely that adjustments to the RACF commands will be required for a successful migration.

For sites with a large number of USERIDs and GROUPs in the production RACF database, the tool might encounter 31-bit storage constraints due to the REXX implementation. If that occurs, consider running ISFACR against a smaller test system RACF database to generate the starter set of RACF commands. You might also consider using the ISFNTCNV tool outlined in "Setting up the NTBL conversion utility ISFNTCNV" on page 18.

ISFACR provides ISPF panels that assist with SDSF security conversion. The migration utility can be found in data set ISF.SISFEXEC.

Important: SDSF APAR PH13974 must be applied before running ISFACR. This APAR fixes a potential error that might result in message `Error running ISFDC42M - line xxxx Invalid Expression` when running the migration utility.

Procedure

1. Update your TSO logon procedure to include the data sets listed in the following table.

Table 5. DDs required in TSO logon procedure

TSO logon procedure DD card	SDSF data set
ISPMLIB	ISF.SISFMLIB
ISPPLIB	ISF.SISFPLIB
ISPSLIB	ISF.SISFSLIB
ISPTLIB	ISF.SISFTLIB
SYSEXEC	ISF.SISFEXEC

This example shows the data sets in the procedure RSMPROC.

```
//RSMPROC EXEC PGM=IKJEFT01,
//         DYNAMNBR=99,PARM='%TSOLOGON'
//ISPMLIB DD DSN=ISP.SISPMENU,DISP=SHR
//         DD DSN=SYS1.SBPXMENU,DISP=SHR
//         DD DSN=ISF.SISFMLIB,DISP=SHR
//ISPPLIB DD DSN=SYS1.ISPPLIB.LOCAL,DISP=SHR
//         DD DSN=ISP.SISPPENU,DISP=SHR
//         DD DSN=SYS1.SBPXPENU,DISP=SHR
//         DD DSN=ISF.SISFPLIB,DISP=SHR
//ISPSLIB DD DSN=ISP.SISPSENU,DISP=SHR
//         DD DSN=ISP.SISPSLIB,DISP=SHR
//         DD DSN=ISF.SISFSLIB,DISP=SHR
//ISPTLIB DD DSN=ISP.SISPTENU,DISP=SHR
//         DD DSN=SYS1.SBPXTENU,DISP=SHR
//         DD DSN=ISF.SISFTLIB,DISP=SHR
//SYSEXEC DD DSN=ISP.SISPEXEC,DISP=SHR
//         DD DSN=SYS1.SBPXEXEC,DISP=SHR
//         DD DSN=ISF.SISFEXEC,DISP=SHR
//ISPEXEC DD DISP=SHR,DSN=ISP.SISPEXEC
//         DD DISP=SHR,DSN=SYS1.SBPXEXEC
//SYSLBC DD DSN=SYS1.BRODCAST,DISP=SHR
//SYSPROC DD DSN=SYS1.ISPCLIB.LOCAL,DISP=SHR
//         DD DSN=ISP.SISPCLIB,DISP=SHR
```

```
//        DD DSN=SYS1.SBPXEXEC,DISP=SHR
//SYSUADS DD DSN=SYS1.UADS,DISP=SHR
//SYSIN DD TERM=TS
//SYSPRINT DD TERM=TS,SYSOUT=Z
//SYSTERM DD TERM=TS,SYSOUT=Z
```

2. The user ID must log off and log back on for the changes to take effect.
3. Invoke the ISPF panels of the ISFACR security migration utility by issuing the TSO ISFACR command. The panel that is displayed shows the SDSF security conversion steps.

```
          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
```

What to do next

Details about how to use the ISFACR security migration utility are provided in the topic Migrating from ISFPARMS into RACF.

The following table lists two other SDSF data sets provided by IBM that contain sample jobs that might be useful during security conversion.

Table 6. Data sets that contain sample jobs for security conversion

SDSF Data set	Description
ISF.SISFJCL	Contains sample jobs for SDSF and SDSFAUX started tasks, SMP/E and ISFPRMxx samples (ISFPRM00 and ISFPRM01).
ISF.SISFSRC	Contains sample ISFPARMS with assembler macros and sample SDSF user exit module.

Establishing ISFACR parameters

When using the ISFACR security migration utility, you must define a set of parameters that will be used by the utility to perform the SDSF security conversion from ISFPARMS to RACF.

The following table provides the list of the parameters and a set of examples. Use the "Value for your migration" column to fill in the appropriate values for your migration.

Table 7. ISFACR migration utility parameters

Task	Example	Value for your migration
ISFPARMS input data set	SYS1.PARMLIB.LOCAL(ISFPRM00)	
Profile description data set	SYS001.SDSF.PROFILES	
CLIST library	ISF.SISFEXEC	
RACF commands data set	SYS001.SDSF.RACF	
Prefix for generated GROUP names	ISF	
Owner group name for resource profiles	ISF	

Table 7. ISFACR migration utility parameters (continued)		
Task	**Example**	**Value for your migration**
JES names for use in RACF resources – JES2	JES2	
JES names for use in RACF resources – JES3	JES3	

For more information, see the topic Running ISFACR - Step 1 - Define profile.

Considerations for mapping ISFPRMxx statements to RACF profiles

When planning, consider these factors and recommendations.

A good initial goal is a one-to-one conversion from ISFPARMS security to RACF. A one-to-one conversion might cause more profiles to be created profiles than are needed. You should analyze the profiles and combine them where practical.

Your first task is to analyze your current security system to determine the kind of protection and authorization you need. In addition to making your SDSF security system easier to maintain, this analysis may result in improvements in the general security and auditability of your installation.

The conversion of SDSF security to RACF might require the cooperation of different groups in your organization. If you are not familiar with SDSF and its functions, seek assistance from your system programmers. It is very important that the person or team implementing the migration understand not only SDSF functions, but also how ISFPARMS security works.

Details on how to use the ISFACR security migration utility are provided in Chapter 5, “Migrating from ISFPARMS into RACF,” on page 23.

RACF environment requirements

To secure SDSF with RACF, several requirements need to be met.

- The RACF classes are already defined for RACF.
- Depending on the RACF classes, the SDSF class may need to be RACLISTed.
- RACF profiles must be defined in the appropriate classes using the **RDEFINE** command to protect the SDSF functions and resources.
- As a rule of thumb, when defining RACF profiles, start with the most generic profiles for broad access to resources and then define more specific profiles to setup a more granular access.
- Provide access to users (preferably in groups) to the appropriate RACF profiles in each class with the necessary access levels, using the **PERMIT** command.
- Generic processing must be activated before defining RACF profiles using the **SETROPTS** command.
- Activate the classes using the **SETROPTS** command.

Because the ISFACR security migration utility will help with the generation of the RACF commands, you need only to review the generated RACF commands and ensure they meet your requirements.

Details on how to use the ISFACR security migration utility are provided in the topic Migrating from ISFPARMS into RACF.

For more information on the required RACF classes, see the topic RACF Classes Protecting SDSF.

For more information on RACF commands, see *Security Server RACF Command Language Reference*.

Chapter 5. Migrating from ISFPARMS into RACF

Architecting a RACF group structure

It is important to establish your RACF group tree structure, determine who should be connected to those groups, and decide what access they require in SDSF.

The IBM-provided ISFPRM00 default member is used as an example of migrating from ISFPARMS security into RACF throughout this documentation. See the topic Default Member ISFPRM00 for more information. This ISFPRMxx statements member contains a typical common description of the types of users (groups) that access SDSF.

Table 8. Typical ISFPARMS groups and descriptions in ISFPRMxx statements

ISFPARMS Group	**Description**
ISFSPROG	System programmers
ISFOPER	Operators
ISFUSER	End users

Your case may be more specific and more granular, but the principle is the same. To simplify the examples and the SDSF security migration process, this documentation uses the default group types in the preceding table.

Group names and owner

Unless the groups are already defined in RACF, during the security migration process you will be asked to enter information related to the groups.

The default group tree structure, as used by the ISFACR security migration utility for the default ISFPRM00 member, is:

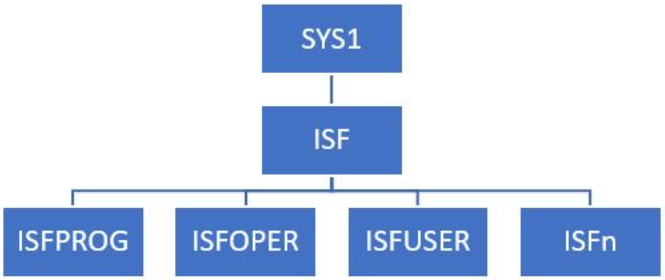

Figure 1. Default RACF group tree structure

The groups defined in ISFPRM00 are added to the RACF group tree structure (ISFSPROG, ISFOPER, and ISFUSER). Any other groups that the migration utility requires are added using the prefix for generated group names, followed by a number. For example, if the default prefix for generated group names is ISF, then the generated group names will follow the naming standard ISFn, where n is a number (for example: ISF4).

Member ISFRACEX in the SISFJCL data set contains sample JCL and RACF statements that establish a simple example of the definitions that are required for the groups described in ISFPRM00. Depending on the complexity of your security configuration, you can refer to this member and edit as required, instead of running ISAFCR.

You can define the prefix for generated group names and the owner/superior group in step 1 of the ISFACR security migration process.

```
             SDSF Security Conversion Assist Profile

ISFPARMS input data set
===> 'SYS1.PARMLIB.LOCAL(ISFPRM00)'
Profile description data set
===> 'SYS001.SDSF.PROFILES'
CLIST library
===> 'ISF.SISFEXEC'
RACF commands data set
===> 'SYS001.SDSF.RACF'

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
```

When you start the migration process using the ISFACR security migration utility, step 4 will generate the required RACF commands including the commands to create the RACF group tree structure. An example of these commands is as follows:

```
/* Commands for  GROUP  profiles */
ADDGROUP  ISF OWNER(SYS1) SUP(SYS1 ) DATA('ISFPARMS GROUP OWNER#GROUP')
ADDGROUP  ISFSPROG OWNER(ISF) SUP(ISF ) DATA('ISFPARMS GROUP JCL,OPER,ACCT')
ADDGROUP  ISFOPER OWNER(ISF) SUP(ISF ) DATA('ISFPARMS GROUP JCL,OPER')
ADDGROUP  ISFUSER OWNER(ISF) SUP(ISF ) DATA('ISFPARMS GROUP JCL')
ADDGROUP  ISF4 OWNER(ISF) SUP(ISF ) DATA('ISFPARMS GROUP SLIST')
```

Using the ISFACR security migration utility

Using the IBM-provided migration utility ISFACR is recommended to assist you with the SDSF security conversion from ISFPARMS to RACF.

The ISFACR security migration utility generates RACF commands based on your current ISFPARMS. Because the utility generates the RACF commands for you, you need only to review the generated RACF commands to ensure they meet your requirements.

ISFACR conversion steps

When running the ISFACR security migration utility, there are five steps that must be completed in sequence.

```
         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
```

The following table describes these steps.

Table 9. ISAFCR steps and descriptions		
Step	**Action**	**Description**
1	Define profile	Set up options for the security migration utility. Define ISFPARMS input data set, output data sets, prefixes, and more.
2	Convert ISFPARMS to profile descriptions	Analyzes ISFPARMS input file and creates output file with profile descriptions. This step also checks if the user IDs that are found in name tables in ISFPARMS exist in RACF.
3	Review profile descriptions	Allows you to manually review and modify profile descriptions.
4	Convert descriptions to RACF commands	Converts the profile descriptions into RACF commands.
5	Review RACF commands	Allows you to manually review and modify the generated RACF commands.

Migration considerations

When migrating SDSF security from ISFPARMS to RACF, there are several factors to keep in mind.

Table 10. Considerations when migrating	
Consideration	**Description**
OWNER command	The OWNER keyword on the ISFGRP macro or GROUP statement can be used to limit the jobs that appear on the displays. There is no protection for the OWNER command using ISFPARMS. This command can only be protected using SAF. If the command is not protected using SAF, then all users can use the OWNER command to further restrict the jobs that appear on their displays.
Destinations	When a user has no IDEST list in ISFPARMS, that user must have READ authority to the SDSF class resource ISFOPER.ANYDEST.jesx. Otherwise, no jobs will appear on the queues and the user's DEST value, when queried, will be displayed as either blanks or the character string ????????, depending on the JES release. When an IDEST list is provided for a user, the user must have READ authorization to each SDSF class resource (ISFAUTH.DEST.destname) protecting the destination names in the IDEST list.
NOTIFY	There is no one-to-one RACF equivalent for setting CMDAUTH or DSPAUTH to NOTIFY in ISFPARMS. To obtain similar functions, a user must have access to the appropriate person's output by way of the JESSPOOL resource.
CMDLEV	Although you can migrate command protection from ISFPARMS CMDLEV protection to RACF OPERCMDS protection on a one-to-one basis, it is not necessarily advisable to keep the hierarchy restriction of CMDLEV when using RACF. RACF provides a more flexible means of authorizing users to access various commands. Decide which commands your users need, and then authorize the proper users, or groups of users, to access the appropriate OPERCMDS resources.

Running ISFACR

The tasks in this set of topics correspond to the ISAFCR security migration steps.

About this task

To invoke the ISFACR security migration utility, enter **TSO ISFACR** from the ISPF command line.

Step 1: Define the profile

The first step of the SDSF security migration is to set up the parameters that will be used by the ISFACR migration utility.

Procedure

1. On the **SDSF Security Conversion** panel, select option 1.
   The **SDSF Security Conversion Assist Profile** panel is displayed:

```
             SDSF Security Conversion Assist Profile

ISFPARMS input data set
===> 'SYS1.PARMLIB.LOCAL(ISFPRM00)'
Profile description data set
===> 'SYS001.SDSF.PROFILES'
CLIST library
===> 'ISF.SISFEXEC'
RACF commands data set
===> 'SYS001.SDSF.RACF'

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
```

2. Enter the parameter values required for your migration, as described in the following list:

   ISFPARMS input data set
   Type the name of the ISFPARMS data set to be converted. The ISFPARMS can be in either assembler macro or statement format.

   Profile description data set
   Type the name of the profile descriptions data set. The default name of the data set is prefix.IN.SDSF. You must allocate the data set before running the conversion assist. It must be a sequential data set with a record length of at least 80.

   CLIST library
   Type the name of the library containing any CLISTS to be used in the conversion.

   RACF commands data set
   Type the name of the RACF commands data set. This data set will contain the generated RACF commands. The data set must be sequential with a record length of at least 133 and it needs to be allocated before running the utility.

   Prefix for generated GROUP names
   Type the prefix to be used for RACF groups generated by the conversion assist. The default is ISF. The conversion assist appends Tn to the prefix, where n is the number of the group in ISFPARMS.

   Owner group name for resource profiles
   Type the owner group name for the resource profiles generated by the conversion assist. The default is ISF.

JES names for use in RACF resources
Type the JES2 and JES3 names to be used in generated resource names. Only one is required. For example, if you specify JESA, then the resource jes.MODIFY.DEV will be JESA.MODIFY.DEV

Step 2: Convert ISFPARMS to profile descriptions

Once the ISFACR parameters are set, you can convert the ISFPARMS to profile descriptions.

Procedure

1. On the **SDSF Security Conversion** panel, select option 2.
   The **ISFPARMS Conversion Environment** panel is displayed:

```
ISFPARMS Conversion Environment

1   1.  Foreground
    2.  Batch
```

2. Select option 1 to do the conversion in the foreground or option 2 to do the conversion in as a batch job.
   - Selecting option 1 to process in the foreground automatically starts the conversion process and issues reporting messages as in the following example:

```
 EXEC NAME = ISFDC42M

    DESCRIPTIVE NAME = Conversion Processing Part 1

    PROPRIETARY STATEMENT =

      LICENSED MATERIALS - PROPERTY OF IBM

      5650-ZOS

      Copyright IBM CORP. 1997, 2019.
      Copyright Rocket Software Inc. 2015, 2019.

      STATUS = HQX77C0

IBMUSER is an empty group
IZUUSER is an empty group
TSGTS is an empty group
RSMJ is an empty group
RSMP is an empty group
SYS001 is an empty group
SYS002 is an empty group
SYS003 is an empty group
SYS004 is an empty group
SYS005 is an empty group
SYS006 is an empty group
SYS007 is an empty group
SYS008 is an empty group
SYS009 is an empty group
SYS010 is an empty group
SYS011 is an empty group
SYS012 is an empty group
SYS013 is an empty group
SYS014 is an empty group
SYS015 is an empty group
SYS016 is an empty group
SYS017 is an empty group
SYS018 is an empty group
SYS019 is an empty group
SYS020 is an empty group
IBMUSER is an empty group
IZUUSER is an empty group
#GENUSER is an empty group
#TESTUSR is an empty group
IBMUSER is an empty group
IZUUSER is an empty group
IBMUSER is an empty group
IZUUSER is an empty group
```

```
#GENUSER is an empty group
#TESTUSR is an empty group
IBMUSER is an empty group
IZUUSER is an empty group
IBMUSER is an empty group
IZUUSER is an empty group
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 37
OPER 39
ACCT 3
AUTH = ALL
CMDAUTH = ALL
CMDLEV = 7
DSPAUTH = ALL
connect users to tsoauth group
JCL 37
OPER 39
AUTH = ALLOPER
CMDAUTH = ALL
CMDLEV = 7
DSPAUTH = USERID,NOTIFY,AMSG
connect users to tsoauth group
JCL 37
AUTH = ALLUSER
CMDAUTH = USERID,NOTIFY
CMDLEV = 2
DSPAUTH = USERID,NOTIFY
5 profiles in class GROUP
```

- If you select the option to convert via batch job, the JCL is displayed so you can tailor before submitting it. For example:

```
//SYS001  JOB (1),'SDSF CONVERSION',CLASS=A,
//             MSGCLASS=H,MSGLEVEL=(1,1),NOTIFY=SYS001
//*
//*  Part 1 of the ISFPARMS to security profile conversion
//*
//TMP     EXEC PGM=IKJEFT01,REGION=0M
//SYSTSPRT DD SYSOUT=*
//*
//DDSAVE   DD DSN=SYS001.SDSF.PROFILES,DISP=SHR
//ISFPARMS DD DSN=SYS001.PARMI.SDSF,DISP=SHR
//*
//SYSTSIN  DD *
  EXEC 'ISF.SISFEXEC(ISFDC42M)' 'ISF ISF JES2 JES3'
//
```

Results

Once the conversion process is complete, the profile description data set SYS001.SDSF.PROFILES (specified in step1) will be populated with the results of the conversion. Note that the same will happen if you run it as a batch job.

Step 3: Review profile descriptions

After the RACF profile descriptions have been created, review the profile descriptions as created to ensure they are suitable for your system.

Procedure

1. On the **SDSF Security Conversion** panel, select option 3.

   A set of instructions that need to be followed is displayed, as in the following example:

```
/* ---------------------------------------------- */
/* RACF SDSF CONVERSION OUTPUT OF PART ONE        */
/* ---------------------------------------------- */
/* Generated by SYS001 18 Oct 2020 16:15:44       */
/* ---------------------------------------------- */
```

```
/*                                                */
/* Instructions:                                  */
/*                                                */
/* - Find all entries 'CHANGE' and change them    */
/*   into a sensible value for your organization. */
/*                                                */
/* - Put MVS.*, JES2.*, and JES3.* profiles in    */
/*   warning mode.                                */
/*                                                */
/* - If you find an asterisk as membername of a   */
/*   group profile, then this means that all RACF */
/*   users are connected to that group.           */
/*                                                */
/*   Thus, when this group is mentioned in the    */
/*   access list of a profile, the UACC of that   */
/*   profile should be set to the appropriate     */
/*   access level.                                */
/* ---------------------------------------------- */
```

The generated profile descriptions are ordered by RACF class and are made of statements as shown in the following example:

```
Class= SDSF
ISFCMD.DSP.ACTIVE.JES2
SDSF_COMMANDS
ISF
NONE
NOWARNING
ALL
MEMBERS
ACCESS LIST
ISFSPROG READ
ISFOPER READ
ISFUSER READ
CONDITIONAL ACCESS LIST
```

A description of these statements is contained in the Table 11 on page 29:

Table 11. Explanation of profile statements

Statement	**Description**
Class= SDSF	RACF class
ISFCMD.DSP.ACTIVE.JES2	RACF profile
SDSF_COMMANDS	Descriptive text
ISF	Owner
NONE	UACC
NOWARNING	WARNING | NOWARNING mode
ALL	Audit settings
MEMBERS	Heading for members
	Entry for group class or for general resource grouping class. In the example, there are no members.
ACCESS LIST	Heading for Access Control List (ACL)
ISFSPROG READ ISFOPER READ ISFUSER READ	Entries in the ACL with USERID|GROUP and access level
CONDITIONAL ACCESS LIST	Heading for conditional access list
	Entries in the conditional ACL. In the example, there are no entries in the conditional ACL.

2. The access list information for some profile descriptions contain the word "CHANGE" instead of a user ID or group name. These instances of "CHANGE" need to be changed to a correct user ID or group name.

   The bold text shows one example in the list:

```
Class= JESSPOOL
*.*.$JESNEWS.*.D*.JESNEWS
JESNEWS
ISF
READ
NOWARNING
ALL
MEMBERS
ACCESS LIST
CHANGE ALTER
CONDITIONAL ACCESS LIST
```

   You can change these strings now, while reviewing the profile descriptions, or change them later when you are reviewing and updating the RACF commands (step 5 of the migration process).

Step 4: Convert descriptions to RACF commands

This step converts the statements in the profile description data set into RACF commands.

About this task

None of the generated RACF commands are automatically executed. You must review and modify these commands (see “Step 5: Review RACF commands” on page 31) and decide when to execute the commands.

It is important to note that this is a one-to-one conversion from ISFPARMS security to RACF, When the RACF profiles are created, there might be more profiles created than you need. You should analyze the generated RACF profiles and combine them where practical.

Procedure

1. On the **SDSF Security Conversion** panel, select option 4.
2. The **RACF Command Generation** panel is displayed:

```
          RACF Command Generation

Select foreground or batch.
1   1.  Foreground
    2.  Batch

Select the RACF class to convert.
Select "All" to convert all classes.
1   1.  SDSF
    2.  GSDSF
    3.  JESSPOOL
    4.  OPERCMDS
    5.  WRITER
    6.  XFACILIT
    7.  All
```

3. Select option 1 to do the conversion in the foreground or option 2 to do the conversion in as a batch job. In addition, enter the number for the RACF class that you wish to convert. It is recommended that you select option 7 to convert all RACF classes.

   Selecting option 1 to process in the foreground automatically starts the conversion process and issues reporting messages as in the following example:

```
    EXEC NAME = ISFDC43M

    DESCRIPTIVE NAME = Conversion Processing Part 2

    PROPRIETARY STATEMENT =
```

```
      LICENSED MATERIALS - PROPERTY OF IBM

      5650-ZOS

      Copyright IBM CORP. 1997, 2019.
      Copyright Rocket Software, Inc. 2015, 2019.

      STATUS = HQX77C0

Conversion Part 2 Running.....
***
```

If you select the option to convert via batch job, the JCL is displayed so you can tailor before submitting it. For example:

```
//SYS001   JOB (1),'SDSF CONVERSION',CLASS=A,
//             MSGCLASS=H,MSGLEVEL=(1,1),NOTIFY=SYS001
//*
//*  Part 2 of the ISFPARMS to security profile conversion
//*
//TMP     EXEC PGM=IKJEFT01,REGION=0M
//SYSTSPRT DD SYSOUT=*
//*
//DDSAVE   DD DSN=SYS001.SDSF.PROFILES,DISP=SHR
//DDOUT    DD DSN=SYS001.SDSF.RACF,DISP=SHR
//*
//SYSTSIN  DD *
  EXEC 'ISF.SISFEXEC(ISFDC43M)' 'ALL ISF'
//
```

Results

The generated RACF commands are stored in the data set that is specified in step 1 (in this example, SYS001.SDSF.RACF).

Step 5: Review RACF commands

The last step of the ISFACR migration utility allows you to review the generated RACF commands.

Before you begin

The RACF commands must be reviewed and modified as appropriate before submitting them. You can delay execution of the RACF commands until later, when all of your requirements are met (such as change request and approvals).

Procedure

- Review the RACF commands and modify them as appropriate for your system.

  The following example shows a snapshot of the RACF commands that might be generated:

```
  CONTROL MAIN NOFLUSH

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

 /* Remove profile(s) in class GROUP */
 /*REMOVE  IBMUSER GROUP(ISF)*/
 /*DELGROUP  ISF*/

 /* Remove profiles in class JESSPOOL */
 RDEL JESSPOOL **

 /* Remove profiles in class GSDSF */
 /* Remove profiles in class SDSF */
 RDEL SDSF ISFNODE.*.JES3
 RDEL SDSF ISFNS.*.JES3
 RDEL SDSF **

 /* Remove profiles in class WRITER */
 /* Remove profile(s) in class GLOBAL */
 /* Remove profiles in class OPERCMDS */
```

```
RDEL OPERCMDS MVS.CANCEL.STC.CCITCPGW.CCITCPGW
/*PERMIT  MVS.DISPLAY.JOB CLASS(OPERCMDS) ID( #SYSPROG) DELETE*/
```

When reviewing the generated RACF commands, note the following and address if needed.

ACL entries marked with the word CHANGE (e.g. CHANGE READ)
These entries must be reviewed and modified. The word "CHANGE" needs to be replaced by a valid RACF user ID or a group.

Commented out RACF commands
Certain RACF commands are commented out by default during the security migration (RDELETE, REMOVE, CLASSACT). Review these commands and remove the comments if appropriate.

RACF commands with inappropriate scope
Some RACF commands may have an asterisk (*) to define the scope. If this is not correct, replace it with the correct entries of scope.

Generic Owner facility
The ISFACR migration utility assumes that a Generic Owner facility is to be used. This has a great impact on the ownership of RACF profiles, in particular on JESSPOOL profiles. Remove the associated RACF command if you do not plan to use Generic Owner.

RACF classes need to be defined as GENERIC
Ensure all the required RACF classes are defined as GENERIC.

&RACUID entry in the GLOBAL profile
&RACUID will be treated as a variable. You must change the single ampersand (&) to two ampersands (&&) before running the RACF commands.

For more information on RACF commands, see *Security Server RACF Command Language Reference*.

Related reference

"ISFPARMS vs RACF profiles" on page 47
The table in this topic cross-references the ISFPARMS parameters that have an equivalent RACF class/profile.

"RACF classes and profiles that protect SDSF" on page 59
The table that follows provides a list of SDSF functions and the RACF classes and profiles required to protect them.

"RACF profiles that protect JES2 commands" on page 79
RACF class OPERCMDS can be used to protect JES2 operator commands.

"RACF profiles that protect MVS commands" on page 85
RACF class OPERCMDS can be used to protect MVS operator commands.

Activating the RACF classes

As part of SDSF security migration from ISFPARMS into RACF, you must ensure the required RACF classes are active in your mainframe system.

Procedure

- Review the RACF commands generated in "Step 4: Convert descriptions to RACF commands" on page 30. These are generated at the end of the RACF commands list and are commented out. For example:

```
/*SETROPTS CLASSACT(SDSF WRITER JESSPOOL OPERCMDS)*/
```

Step 4 also generates other RACF commands affecting the required RACF classes:

```
/*SETROPTS RACLIST(SDSF OPERCMDS)*/
/*SETROPTS NORACLIST(WRITER JESSPOOL)*/
/*SETROPTS LOGOPTIONS(ALWAYS(SDSF WRITER OPERCMDS))*/
/*SETROPTS LOGOPTIONS(FAILURES(JESSPOOL))*/
/*SETROPTS GENERICOWNER*/
/*SETROPTS REFRESH RACLIST(SDSF OPERCMDS)*/
```

Ensure that your RACF environment meets these requirements. If it does not, uncomment the required RACF commands and include them as part of your SDSF security migration process.

The RACF command SETR0PTS LIST can be used to asses the required changes to the RACF classes in scope. For more information on the required RACF classes, see "RACF classes that protect SDSF" on page 3.

For more information on RACF commands, see *Security Server RACF Command Language Reference*.

Cleaning up ISFPRMxx

The active ISFPRMxx member no longer requires the statements to control SDSF security, which means that they can be removed after you implement the SDSF security migration.

Procedure

1. Review and remove the statements that control SDSF security in the ISFPRMxx member.

   For example, with the default ISFPRM00 (see Appendix G, "Default member ISFPRM00," on page 91), and for the three groups in scope (ISFSPROG, ISFOPER, and ISFUSER), the end result would be as shown in the following tables:

Table 12. ISFSPROG group

ISFPRMxx Before Migration	ISFPRMxx After Migration
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)	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)

Table 13. ISFOPER group

ISFPRMxx Before Migration	ISFPRMxx After Migration
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)	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)

Table 14. ISFUSER group

ISFPRMxx Before Migration	ISFPRMxx After Migration
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)	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)

2. Once the ISFPRMxx cleanup is complete, dynamically update the system by using the `MODIFY MVS` command.

```
/F server_name,REFRESH,<MEMBER=xx>,<TEST>
```

Examples:

- Refresh the current ISFPRMxx member (as defined in started task SDSF):

```
/F SDSF,REFRESH
```

- Same as previous but checks the statement's syntax instead of activating them:

```
/F SDSF,REFRESH,TEST
```

- Activate ISFPRMxx member 01:

```
/F SDSF,REFRESH,M=01
```

- Same as previous but checks the statement's syntax instead of activating them:

```
/F SDSF,REFRESH,M=01,TEST
```

3. Exit SDSF and restart it.

Chapter 6. Testing the RACF implementation before migration

Building a testing plan

So far, you have analyzed your current position, planned your migration, and used the ISFACR security migration utility to help build the required RACF commands. You should now build an inventory and a testing plan of what needs to be tested.

To help create a test plan, you should prepare to answer the following questions:

Table 15. RACF considerations for your test plan

Question	Your answer
Which RACF groups are impacted?	
Which RACF user IDs are impacted?	
What access should each of the groups and user IDs have?	

You can then build a matrix to define your testing plan, as shown in the following table.

Table 16. Sample test plan to record access results for RACF profiles after migration

Group	RACF Class	RACF Profile	Access	Result
ISFSPROG	SDSF	ISFCMD.DSP.ACTIVE.JES2	READ	
ISFSPROG	SDSF	ISFCMD.DSP.ACTIVE.JES3	READ	
ISFSPROG	SDSF	ISFCMD.DSP.HELD.JES2	READ	
ISFSPROG	SDSF	ISFCMD.DSP.HELD.JES3	READ	
ISFSPROG	SDSF	ISFCMD.DSP.INPUT.JES2	READ	
ISFSPROG	SDSF	ISFCMD.DSP.INPUT.JES3	READ	
ISFSPROG	SDSF	ISFCMD.DSP.HELD.JES2	READ	
ISFSPROG	SDSF	ISFCMD.DSP.HELD.JES3	READ	
ISFSPROG	SDSF	ISFCMD.DSP.INPUT.JES2	READ	
ISFSPROG	SDSF	ISFCMD.DSP.INPUT.JES3	READ	
ISFSPROG	OPERCMDS	JES2.CANCEL.STC	UPDATE	
ISFSPROG	OPERCMDS	JES2.CANCEL.TCP	UPDATE	
ISFSPROG	OPERCMDS	JES2.CANCEL.TSU	UPDATE	
ISFOPER	SDSF	ISFCMD.DSP.ACTIVE.JES2	READ	
ISFOPER	SDSF	ISFCMD.DSP.ACTIVE.JES3	READ	
ISFOPER	SDSF	ISFCMD.DSP.HELD.JES2	READ	
ISFOPER	SDSF	ISFCMD.DSP.HELD.JES3	READ	

You can do the same to associate user IDs with RACF groups.

Table 17. Sample test plan to record access results for user IDS after migration

Group	User ID	Results
ISFSPROG	TSGAT	
ISFOPER	TSGAT	
ISFOPER	TSGTS	
ISFOPER	TSGCH	
ISFOPER	TSGATA	
ISFOPER	TSGMK	

Using the SDSF security trace function

SDSF provides a security trace function that can be used to validate SDSF security with RACF (it also works for ISFPARMS). The security trace function reacts to a user's actions within SDSF. For example, if a user issues a command or overtypes a column value in SDSF, the SDSF security trace issues messages indicating the associated RACF resource.

For migration, you can use the SET SECTRACE command to control how the SDSF security trace function works.T The command and its variants are as follows:

```
SET SECTRACE ON
```

Sends the trace messages to the ULOG. This also activates SDSFAUX SECTRACE.

```
SET SECTRACE OFF
```

Ends security tracing.

```
SET SECTRACE WTP
```

Sends the trace messages as write-to-programmer messages.

```
SET SECTRACE ?
```

Displays the current SET SECTRACE setting.

You can obtain more information about SET SECTRACE by entering the SEARCH command in SDSF, and then search for "SET SECTRACE".

Examples

To check the current SET SECTRACE setting, in SDSF, enter the SET SECTRACE ? command. In this example, the security trace is off:

```
               Set Security Trace

 Select an option to control security trace.

 3   1.  Send messages to the user log
     2.  Issue write-to-programmer messages
     3.  Turn security trace off
```

The example below is the security trace results of entering SET SECTRACE ON in SDSF ULOG:

```
ISF045W Unable to open table library ISFTABL, number of saved commands may be limited.
ISF050I USER=SYS001 GROUP=ISFSPROG PROC=RSMPROC TERMINAL=A05TCP20
ISF031I CONSOLE SYS001 ACTIVATED
```

```
ISF050I USER=SYS001 GROUP=ISFSPROG PROC=RSMPROC TERMINAL=A05TCP20
ISF051I SAF Access allowed SAFRC=0 ACCESS=READ CLASS=SDSF RESOURCE=ISFCMD.DSP.ACTIVE.JES2
ISF051I SAF Access allowed SAFRC=0 ACCESS=READ CLASS=SDSF RESOURCE=ISFCMD.DSP.ACTIVE.JES2
ISF059I SAF Access allowed SAFRC=(0,0,0) ACCESS=READ CLASS=SDSF RESOURCE=ISFCMD. DSP.ACTIVE.JES2
ISF059I SAF Access allowed SAFRC=(0,0,0) ACCESS=READ CLASS=SDSF RESOURCE=ISFCMD. DSP.ACTIVE.JES2
ISF051I SAF Access allowed SAFRC=0 ACCESS=READ CLASS=SDSF RESOURCE=ISFCMD.ODSP.ULOG.JES2
```

Using SMF data

You can also rely on SMF data to analyze how SDSF security is used with RACF after migration. You can use the RACF SMF data unload utility IRRADU00 and DFSORT ICETOOL to produce a useful report.

Before you begin

You must ensure that the RACF profiles defined to the classes in scope have audit settings set to ALL(READ) and that the SMF data is available for analysis. See "RACF classes that protect SDSF" on page 3 for list of RACF classes.

For more information on SMF, see *MVS™ System Management Facility (SMF)*.

Using RACF SMF data unload utility IRRADU00, you can produce a report in two stages. This procedure provides the code required to extract SMF data related to RACF class SDSF.

Procedure

1. Use the SMF data dump data set to translate to auditable data using IRRADU00:

```
//SMFDUMP EXEC PGM=IFASMFDP,REGION=0M
//SYSPRINT DD SYSOUT=A
//ADUPRINT DD SYSOUT=A
//OUTDD DD DISP=SHR,DSN=TSGRF.SMF.RACF.IRRADU00
//SMFDATA DD DISP=SHR,DSN=SMF.RSMP.DAILY.D181020
//SMFOUT DD DUMMY
//SYSIN DD *
     INDD(SMFDATA,OPTIONS(DUMP))
     OUTDD(SMFOUT,TYPE(30,80:83))
     ABEND(NORETRY)
     USER2(IRRADU00)
     USER3(IRRADU86)
/*
```

   Note: If you get the following error messages, you might want to check the SMFDLEXIT or SMFDPEXIT statement with USER2 and USER3 option in your SMFPRMxx parmlib member.

```
IFA840I USER EXIT IRRADU00 NOT REGISTERED WITH SYSTEM
IFA840I USER EXIT IRRADU86 NOT REGISTERED WITH SYSTEM
```

2. Produce the final report on RACF class SDSF using the translated auditable data using DFSORT ICETOOL.

```
//SMFRPTR EXEC PGM=ICETOOL
//IRRSMF DD DISP=SHR,DSN=TSGRF.SMF.RACF.IRRADU00
//TEMPSMF DD DSN=&&TEMPS,SPACE=(CYL,(200,100)),UNIT=SYSDA
//REPORT DD DISP=SHR,DSN=TSGRF.SMF.REPORT
//TOOLMSG DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//DFSMSG DD SYSOUT=*
//TOOLIN DD *
  COPY FROM(IRRSMF) TO(TEMPSMF) USING(SMFI)
  DISPLAY FROM(TEMPSMF) LIST(REPORT) -
    TITLE('SDSF RACF RECORDS') DATE TIME PAGE -
    BLANK -
    ON(63,8,CH) HEADER('USERID') -
    ON(72,8,CH) HEADER('GROUP') -
    ON(5,8,CH) HEADER('EVENT') -
    ON(14,8,CH) HEADER('RESULT') -
    ON(23,8,CH) HEADER('TIME') -
    ON(32,10,CH) HEADER('DATE') -
    ON(43,4,CH) HEADER('SYSTEM') -
    ON(184,8,CH) HEADER('JOBNAME') -
    ON(578,8,CH) HEADER('CLASS') -
```

```
    ON(286,36,CH) HEADER('RESOURCE') -
    ON(605,20,CH) HEADER('PROFILE')
/*
//SMFICNTL DD *
  SORT FIELDS=(32,10,CH,A,23,8,CH,A)
  INCLUDE COND=(5,8,CH,EQ,C'ACCESS',AND,
                578,8,CH,EQ,C'SDSF')
  OPTION VLSHRT
/*
//
```

The following is a snapshot of the generated report:

```
1SDSF RACF RECORDS 10/24/20 14:52:51 - 1 -
USERID GROUP EVENT RESULT TIME DATE SYSTEM JOBNAME CLASS RESOURCE PROFILE
-------- -------- -------- -------- -------- ---------- ---------- ------ -------- --------
------------------------------------ --------------------
TSGDB #RSM ACCESS SUCCESS 12:50:14 2020-10-18 RSMP TSGDB SDSF ISF.CONNECT.RSMP **
TSGDB #RSM ACCESS SUCCESS 12:50:17 2020-10-18 RSMP TSGDB SDSF ISFCMD.FILTER.PREFIX **
TSGDB #RSM ACCESS SUCCESS 12:50:18 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.STATUS.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:50:18 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.STATUS.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:53:33 2020-10-18 RSMP TSGDB SDSF ISFCMD.FILTER.PREFIX **
TSGDB #RSM ACCESS SUCCESS 12:53:35 2020-10-18 RSMP TSGDB SDSF ISFCMD.FILTER.PREFIX **
TSGDB #RSM ACCESS SUCCESS 12:53:39 2020-10-18 RSMP TSGDB SDSF ISFCMD.FILTER.OWNER **
TSGDB #RSM ACCESS SUCCESS 12:53:39 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.STATUS.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:53:39 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.STATUS.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:55:39 2020-10-18 RSMP TSGDB SDSF ISFCMD.FILTER.OWNER **
TSGDB #RSM ACCESS SUCCESS 12:55:41 2020-10-18 RSMP TSGDB SDSF ISFCMD.FILTER.PREFIX **
TSGDB #RSM ACCESS SUCCESS 12:55:42 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.STATUS.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:55:42 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.STATUS.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:55:42 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.STATUS.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:59:48 2020-10-18 RSMP TSGDB SDSF ISF.CONNECT.RSMP **
TSGDB #RSM ACCESS SUCCESS 12:59:48 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.ACTIVE.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:59:48 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.ACTIVE.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:59:49 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.ACTIVE.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:59:49 2020-10-18 RSMP TSGDB SDSF ISF.CONNECT.RSMP **
TSGDB #RSM ACCESS SUCCESS 12:59:49 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.ACTIVE.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:59:49 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.ACTIVE.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:59:49 2020-10-18 RSMP TSGDB SDSF ISF.CONNECT.RSMP **
TSGDB #RSM ACCESS SUCCESS 12:59:49 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.ACTIVE.JES2 **
TSGDB #RSM ACCESS SUCCESS 12:59:49 2020-10-18 RSMP TSGDB SDSF ISFCMD.DSP.ACTIVE.JES2 **
TSGDB #RSM ACCESS SUCCESS 13:02:36 2020-10-18 RSMP TSGDB SDSF ISFCMD.FILTER.PREFIX **
```

What to do next

For more information on IRRADU00, see *z/OS Security Server RACF Auditor's Guide*.

For details about the format and content of the records created, see *Security Server RACF Macros and Interfaces*.

Using IBM zSecure Access Monitor

If you are running IBM zSecure Access Monitor, you can take advantage of this facility to help analyze SDSF security with RACF.

You can do this either via ISPF panels with menu option AM (RACF Access Monitor) or using the CARLa reporting language.

The following example shows CARLa code for RACF class SDSF:

```
newlist type=access nodetailinherit required,
  st="Access monitor records for Classes like SDSF"
 define tot_count("Occurrence",10,udec$abbr) sum(access_count_big)
 define avg_reclen avg(record_length)
 define first_tod_sum("First occurrence") min(last_tod)
 define last_tod_sum("Last occurrence") max(last_tod)
 select ,class=SDSF rectype=(auth,fast,def)
sortlist / " "(8) class,
    resource(84,wrap) " " access_count last_tod,
/ " "(17) class access_proftype(9),
          access_profile(80,wrap),
/ " "(17) "Intent=" ! intent(11),
          "Allowed=" ! access_allowed,
          "Result=" ! access_result(0),,
```

```
/
summary userid userid:name,
  "       ",
* intent(9),
  rectype,
  req_status_access(6,hb),
  access_result(5,"AccRC",dec),
* class(8) complex(8) system(6),
  ! " "(12) ! tot_count(10) last_tod_sum
```

A snapshot of the generated report follows:

```
Access monitor records for Classes like SDSF

 Userid   Name                          Intent    Type   RetAll AccRC Class    Complex  Syst             Occurrence Last occurrence
 BATCH01  BATCH PROCESSING                                                                                      102 20Aug2020 01:16
                                        READ      Auth             0                                          90 20Aug2020 01:16
                                                                      SDSF     TESTPLEX RSMP                    90 20Aug2020 01:16

          SDSF     GROUP.ISFOPER.SDSF                                                                          12 20Aug2020 01:16
                   SDSF     GENERIC   **
                   Intent=READ        Allowed=ALTER   Result=0


          SDSF     ISFAUTH.DEST..DATASET.JESMSGLG                                                               3 20Aug2020 01:16
                   SDSF     GENERIC   **
                   Intent=READ        Allowed=ALTER   Result=0


          SDSF     ISFAUTH.DEST..DATASET.JESYSMSG                                                               3 20Aug2020 01:16
                   SDSF     GENERIC   **
                   Intent=READ        Allowed=ALTER   Result=0


          SDSF     ISFCMD.DSP.STATUS.JES2                                                                      12 20Aug2020 01:16
                   SDSF     GENERIC   **
                   Intent=READ        Allowed=ALTER   Result=0


          SDSF     ISFCMD.FILTER.OWNER                                                                         12 20Aug2020 01:16
                   SDSF     GENERIC   **
                   Intent=READ        Allowed=ALTER   Result=0
```

Chapter 7. Implementation

After you have performed the analysis, documentation, and planning steps, and have run the ISFACR migration utility to produce the RACF commands, you can now perform the SDSF security migration.

It is highly recommended that you first test your SDSF security migration on a test mainframe system, followed by a quality assurance mainframe system, before finally implementing it on a production mainframe system.

Also, you should ensure that you have raised a change request and got the appropriate approval before making any changes to your mainframe systems.

Summary of steps for implementation

The following checklist can be used to help you implement the SDSF security migration RACF commands:

Table 18. Step summary for implementing RACF security

Task	**Check when complete**
Change request raised and approved	
Logged on to the correct system	
Test plan in place	
RACF commands ready for implementation	
Implement RACF commands	
Required RACF classes are active	
Implemented RACF profiles in place	
Required RACF classes refreshed	
SDSF class RACLISTed, if required	
Clean ISFPRMxx	
Start test	
Record test results	

Chapter 8. Reporting requirements

At the end of the SDSF security migration, you might want to create a report that shows the status of the RACF classes affected by the migration.

There are several ways you can do this; two are covered in these topics.

Using RACF commands

The RACF SEARCH command can be used against each of the affected RACF classes to establish which profiles they have.

The following SEARCH command can determine all profiles in all classes:

```
SEARCH CLASS(JESSPOOL) NOMASK
SEARCH CLASS(LOGSTRM) NOMASK
SEARCH CLASS(OPERCMDS) NOMASK
SEARCH CLASS(SDSF) NOMASK
SEARCH CLASS(WRITER) NOMASK
SEARCH CLASS(XFACILIT) NOMASK
```

Each individual profile can be checked by issuing the RACF RLIST command. For example:

```
RLIST SDSF GROUP.ISFSPROG.** GENERIC ALL
```

Alternatively, you can use the RACF CLIST facility to produce a report in batch, as follows:

```
//STEP01 EXEC PGM=IKJEFT01,REGION=25M
//SYSTSPRT DD DISP=SHR,
// DSN=TSGRF.SDSF.REPORTS(MIGCLASS)
//SYSOUT DD SYSOUT=*
//SYSTSIN DD *
SR CLASS(JESSPOOL) NOMASK CLIST('RLIST SDSF ' ' GEN ALL')
SR CLASS(LOGSTRM) NOMASK CLIST('RLIST SDSF ' ' GEN ALL')
SR CLASS(OPERCMDS) NOMASK CLIST('RLIST SDSF ' ' GEN ALL')
SR CLASS(SDSF) NOMASK CLIST('RLIST SDSF ' ' GEN ALL')
SR CLASS(WRITER) NOMASK CLIST('RLIST SDSF ' ' GEN ALL')
SR CLASS(XFACILIT) NOMASK CLIST('RLIST SDSF ' ' GEN ALL')
//STEP02 EXEC PGM=IKJEFT01,REGION=25M
//SYSTSPRT DD DISP=SHR,
// DSN=TSGRF.SDSF.REPORTS(MIGPROF)
//SYSOUT DD SYSOUT=*
//SYSTSIN DD DISP=SHR,DSN=TSGRF.EXEC.RACF.CLIST
/*
```

A few notes about the batch job:

- For the SYSTSPRT DD, on both STEP01 and STEP02, the data set defined can be the same. It must be allocated as a partitioned data set with record format of FB and record length of 80.
- For the SYSTSIN DD on STEP02, *tsouserid*.EXEC.RACF.CLIST is the default name used by RACF when issuing commands with the CLIST parameter. The system allocates this data set as sequential with record format of VB and record length of 255.

When run, this batch job produces two members in data set TSGRF.SDSF.REPORTS:

- The MIGCLASS member stores the result of the RACF SEARCH (SR) command. This will then be used as input for the RLIST command.
- The MIGPROF member stores the result of the RACF RLIST command.

Using IBM zSecure

An alternative to producing RACF reports is using IBM zSecure, which offers a simpler way to generate reports and allows you to have control over what is reported (such as the RACF fields to be included).

You can use IBM zSecure ISPF panels, or use CARLa, zSecure's reporting language.

An example of the CARLa code that could be used to produce the report follows:

```
NEWLIST ESM=RACF TITLE="SDSF SECURITY - RACF CLASSES AND PROFILES"
SELECT C=JESSPOOL S=BASE
SORTLIST COMPLEX CLASS(5) KEY(32) PROFTYPE(1,"T") OWNER WARNING(1),
UACC ACL(SORT) INSTDATA(0,WRAP) /

NEWLIST ESM=RACF
SELECT C=LOGSTRM S=BASE
SORTLIST COMPLEX CLASS(5) KEY(32) PROFTYPE(1,"T") OWNER WARNING(1),
UACC ACL(SORT) INSTDATA(0,WRAP) /

NEWLIST ESM=RACF
SELECT C=OPERCMDS S=BASE
SORTLIST COMPLEX CLASS KEY(37) PROFTYPE(1,"T") OWNER WARNING(1),,
UACC ACL(SORT) INSTDATA(0,WRAP) /

NEWLIST ESM=RACF
SELECT C=SDSF S=BASE
SORTLIST COMPLEX CLASS KEY(37) PROFTYPE(1,"T") OWNER WARNING(1),,
UACC ACL(SORT) INSTDATA(0,WRAP) /

NEWLIST ESM=RACF
SELECT C=WRITER S=BASE
SORTLIST COMPLEX CLASS KEY(37) PROFTYPE(1,"T") OWNER WARNING(1),,
UACC ACL(SORT) INSTDATA(0,WRAP) /

NEWLIST ESM=RACF
SELECT C=XFACILIT S=BASE
SORTLIST COMPLEX CLASS KEY(37) PROFTYPE(1,"T") OWNER WARNING(1),,
UACC ACL(SORT) INSTDATA(0,WRAP) /
```

Appendix A. ISFPARMS vs RACF profiles

The table in this topic cross-references the ISFPARMS parameters that have an equivalent RACF class/ profile.

Table 19. RACF class and profile equivalents to ISFPARMS

ISFPARM	RACF Class	Access	RACF Profile	Description
AUTH=ABEND	SDSF	READ	ISFCMD.MAINT.ABEND	Authority to issue the ABEND command.
AUTH=ACTION	SDSF	READ	ISFCMD.FILTER.ACTION	Authority to issue the ACTION command.
AUTH=ALL	SDSF	READ	ISFCMD.**	Authority to issue any SDSF command.
AUTH=ALLOPER	SDSF	READ	ISFCMD.DSP.* ISFCMD.ODSP.* ISFCMD.FILTER.ACTION ISFCMD.FILTER.DEST ISFCMD.FILTER.FINDLIM ISFCMD.FILTER.OWNER ISFCMD.FILTER.PREFIX ISFCMD.FILTER.RSYS ISFCMD.FILTER.SYSID ISFCMD.FILTER.SYSNAME	Authority to issue any SDSF operator command.
AUTH=ALLUSER	SDSF	READ	ISFCMD.DSP.*	Authority to issue any SDSF end user command.
AUTH=APF	SDSF	READ	ISFCMD.ODSP.APF.system	Authority to issue the APF command.
AUTH=AS	SDSF	READ	ISFCMD.ODSP.AS.system	Authority to issue the AS command.
AUTH=CFC	SDSF	READ	ISFCMD.ODSP.COUPLE.system	Authority to issue the CFC command.
AUTH=CFS	SDSF	READ	ISFCMD.ODSP.CFSTRUCT.system	Authority to issue the CFS command.
AUTH=CK	SDSF	READ	ISFCMD.ODSP.HCHECKER.system	Authority to issue the CK command.
AUTH=CSR	SDSF	READ	ISFCMD.ODSP.CSR.system	Authority to issue the CSR command.
AUTH=DA	SDSF	READ	ISFCMD.DSP.ACTIVE.jesx	Authority to issue the DA command.
AUTH=DEST	SDSF	READ	ISFCMD.FILTER.DEST	Authority to issue the DEST command.

Table 19. RACF class and profile equivalents to ISFPARMS (continued)

ISFPARM	RACF Class	Access	RACF Profile	Description
AUTH=DEST	SDSF	READ	ISFOPER.ANYDEST.jesx	Equivalent to DEST for the AUTH parameter, with no DEST parameter. Users authorized to the DEST command and to this resource can issue the DEST command using any destination name.
AUTH=DEST	SDSF	READ	ISFAUTH.DEST.destname	Equivalent to DEST for the AUTH parameter, with a DEST parameter. In the SAF resource, destname is a destination name specified through the DEST parameter.
AUTH=DEV	SDSF	READ	ISFCMD.ODSP.DEVACT.system	Authority to issue the DEV command.
AUTH=DYNX	SDSF	READ	ISFCMD.ODSP.DYNX.system	Authority to issue the DYNX command.
AUTH=EMCS	SDSF	READ	ISFCMD.ODSP.EMCS.system	Authority to issue the EMCS command.
AUTH=ENC	SDSF	READ	ISFCMD.ODSP.ENCLAVE.system	Authority to issue the ENC command.
AUTH=ENQ	SDSF	READ	ISFCMD.ODSP.ENQUEUE.system	Authority to issue the ENQ command.
AUTH=FINDLIM	SDSF	READ	ISFCMD.FILTER.FINDLIM	Authority to issue the FINDLIM command.
AUTH=FS	SDSF	READ	ISFCMD.ODSP.FILESYS.system	Authority to issue the FS command.
AUTH=GT	SDSF	READ	ISFCMD.ODSP.TRACKER.system	Authority to issue the GT command.
AUTH=H	SDSF	READ	ISFCMD.DSP.HELD.jesx	Authority to issue the H command.
AUTH=I	SDSF	READ	ISFCMD.DSP.INPUT.jesx	Authority to issue the I command.
AUTH=INIT	SDSF	READ	ISFCMD.ODSP.INITIATOR.jesx	Authority to issue the INIT command.
AUTH=INPUT	SDSF	READ	ISFCMD.FILTER.INPUT	Authority to issue the INPUT command.
AUTH=JC	SDSF	READ	ISFCMD.ODSP.JOBCLASS.jesx	Authority to issue the JC command.
AUTH=JES	SDSF	READ	ISFCMD.ODSP.JES.system	Authority to issue the JES command.

Table 19. RACF class and profile equivalents to ISFPARMS (continued)

ISFPARM	RACF Class	Access	RACF Profile	Description
AUTH=JRI	SDSF	READ	ISFCMD.ODSP.JESINFO.jesx	Authority to issue the JRI command.
AUTH=JRJ	SDSF	READ	ISFCMD.ODSP.JESINFO.jesx	Authority to issue the JRJ command.
AUTH=JG	SDSF	READ	ISFCMD.DSP.GROUP.jesx	Authority to issue the JG command.
AUTH=JO	SDSF	READ	ISFCMD.ODSP.JOB0.jesx	Authority to issue the JO command.
AUTH=LI	SDSF	READ	ISFCMD.ODSP.LINE.jesx	Authority to issue the LI command.
AUTH=LNK	SDSF	READ	ISFCMD.ODSP.LNK.system	Authority to issue the LNK command.
AUTH=LOG	SDSF	READ	ISFCMD.ODSP.SYSLOG.jesx	Authority to issue the LOG command.
AUTH=LPA	SDSF	READ	ISFCMD.ODSP.LPA.system	Authority to issue the LPA command.
AUTH=LPD	SDSF	READ	ISFCMD.ODSP.LPD.system	Authority to issue the LPD command.
AUTH=MAS	SDSF	READ	ISFCMD.ODSP.MAS.jesx	Authority to issue the MAS command.
AUTH=NA	SDSF	READ	ISFCMD.ODSP.NETACT.system	Authority to issue the NA command.
AUTH=NC	SDSF	READ	ISFCMD.ODSP.NC.jesx	Authority to issue the NC command.
AUTH=NO	SDSF	READ	ISFCMD.ODSP.NODE.jesx	Authority to issue the NO command.
AUTH=NS	SDSF	READ	ISFCMD.ODSP.NS.jesx	Authority to issue the NS command.
AUTH=O	SDSF	READ	ISFCMD.DSP.OUTPUT.jesx	Authority to issue the O command.
AUTH=OMVS	SDSF	READ	ISFCMD.ODSP.OMVS.system	Authority to issue the OMVS command.
AUTH=PAG	SDSF	READ	ISFCMD.ODSP.PAGE.system	Authority to issue the PAG command.
AUTH=PARM	SDSF	READ	ISFCMD.ODSP.PARMLIB.system	Authority to issue the PARM command.
AUTH=PR	SDSF	READ	ISFCMD.ODSP.PRINTER.jesx	Authority to issue the PR command.
AUTH=PREF	SDSF	READ	ISFCMD.FILTER.PREFIX	Authority to issue the PREFIX command.
AUTH=PROC	SDSF	READ	ISFCMD.ODSP.PROCLIB.jesx	Authority to issue the PROC command.

Table 19. RACF class and profile equivalents to ISFPARMS (continued)

ISFPARM	RACF Class	Access	RACF Profile	Description
AUTH=PS	SDSF	READ	ISFCMD.ODSP.PROCESS.system	Authority to issue the PS command.
AUTH=PUN	SDSF	READ	ISFCMD.ODSP.PUNCH.jesx	Authority to issue the PUN command.
AUTH=RDR	SDSF	READ	ISFCMD.ODSP.READER.jesx	Authority to issue the RDR command.
AUTH=RES	SDSF	READ	ISFCMD.ODSP.RESOURCE.system	Authority to issue the RES command.
AUTH=REPC	SDSF	READ	ISFCMD.ODSP.REPC.system	Authority to issue the REPC command.
AUTH=RGRP	SDSF	READ	ISFCMD.ODSP.RGRP.system	Authority to issue the RGRP command.
AUTH=RM	SDSF	READ	ISFCMD.ODSP.RESMON.jesx	Authority to issue the RM command.
AUTH=RMA	SDSF	READ	ISFCMD.ODSP.RMA.system	Authority to issue the RMA command.
AUTH=RSYS	SDSF	READ	ISFCMD.FILTER.RSYS	Authority to issue the RSYS command.
AUTH=SE	SDSF	READ	ISFCMD.DSP.SCHENV.system	Authority to issue the SE command.
AUTH=SMSG	SDSF	READ	ISFCMD.ODSP.STORGRP.system	Authority to issue the SMSG command.
AUTH=SMSV	SDSF	READ	ISFCMD.ODSP.SMSVOL.system	Authority to issue the SMSV command.
AUTH=SO	SDSF	READ	ISFCMD.ODSP.SO.jesx	Authority to issue the SO command.
AUTH=SP	SDSF	READ	ISFCMD.ODSP.SPOOL.jesx	Authority to issue the SP command.
AUTH=SR	SDSF	READ	ISFCMD.ODSP.SR.system	Authority to issue the SR command.
AUTH=SRVC	SDSF	READ	ISFCMD.ODSP.SRVC.system	Authority to issue the SRVC command.
AUTH=SSI	SDSF	READ	ISFCMD.ODSP.SUBSYS.system	Authority to issue the SSI command.
AUTH=ST	SDSF	READ	ISFCMD.DSP.STATUS.jesx	Authority to issue the ST command.
AUTH=SYS	SDSF	READ	ISFCMD.ODSP.SYSTEM.system	Authority to issue the SYS command.
AUTH=SYSID	SDSF	READ	ISFCMD.FILTER.SYSID	Authority to issue the SYSID command.
AUTH=SYSNAME	SDSF	READ	ISFCMD.FILTER.SYSNAME	Authority to issue the SYSNAME command.

Table 19. RACF class and profile equivalents to ISFPARMS (continued)

ISFPARM	RACF Class	Access	RACF Profile	Description
AUTH=TRACE	SDSF	READ	ISFCMD.MAINT.TRACE	Authority to issue the TRACE command.
AUTH=ULOG	SDSF	READ	ISFCMD.ODSP.ULOG.jesx	Authority to issue the ULOG command.
AUTH=VMAP	SDSF	READ	ISFCMD.ODSP.VIRTSTOR.system	Authority to issue the VMAP command.
AUTH=WKLD	SDSF	READ	ISFCMD.ODSP.WKLD.system	Authority to issue the WKLD command.
AUTH=WLM	SDSF	READ	ISFCMD.ODSP.WLM.system	Authority to issue the WLM command.
AUTH=XCFM	SDSF	READ	ISFCMD.ODSP.CFMEMBER.system	Authority to issue the XCFM command.
CMDAUTH=DEST	SDSF	READ	ISFOPER.DEST.jesx	SDSF does further checking for authority to jobs and output based on destination (destination operator authority).
CMDAUTH=DEST	SDSF	ALTER	ISFAUTH.DEST.destname	Used with the above ISFOPER.DEST.jesx resource, is equivalent to DEST for CMDAUTH with a DEST parameter, when destname is a destination name specified through the DEST parameter.
CMDAUTH=DEST	WRITER	ALTER	jesx.LOCAL.devicename jesx.RJE.devicename	Authority to specific LOCAL or RJE printers or punches based on devicename.
CMDAUTH=DISPLAY	JESSPOOL	READ	node.userid.jobname.jobid node.userid.jobname.jobid.GROUP.ogroupid	Authority to issue D and L action characters for any job or output group to which they have READ access.
CMDAUTH=GROUP	JESSPOOL	ALTER	node.userid.jobname.jobid node.userid.jobname.jobid.GROUP.ogroupid	Equivalent to GROUP for CMDAUTH, when jobname is the group prefix. (With structured TSO user IDs, you can specify user ID instead of jobname.)
CMDAUTH=INIT	SDSF	CONTROL	ISFINIT.I(xx).jesx	Equivalent to INIT for CMDAUTH, when xx is the initiator identifier.
CMDAUTH=NOTIFY	No direct SAF equivalent.			
CMDAUTH=MSG	Logging of user access to resources is controlled by RACF.			

Table 19. RACF class and profile equivalents to ISFPARMS (continued)

ISFPARM	RACF Class	Access	RACF Profile	Description
CMDAUTH=USERID	JESSPOOL	ALTER	node.userid.jobname.jobid node.userid.jobname.jobid.GROUP.ogroupid	Equivalent to USERID for CMDAUTH, when userid is the name of the job the user is trying to access. (Even when no profiles are defined in the JESSPOOL class, users are authorized to output that they own.)
CMDAUTH=ALL	SDSF	READ	ISFOPER.SYSTEM	Authority to issue the SDSF / command.
CMDAUTH=ALL	SDSF	READ	ISFOPER.DEST.jesx	SDSF does further checking for authority to jobs and output based on destination.
CMDAUTH=ALL	SDSF	ALTER	ISFAUTH.DEST.destname	Used with the above ISFOPER.DEST.jesx resource, is equivalent ALL for CMDAUTH, with no DEST parameter. Use generic profiles to give authority to all jobs and output.
CMDAUTH=ALL	WRITER	ALTER	jesx.LOCAL.devicename jesx.RJE.devicename	Use generic profiles to give authority to all printers and punches.
CMDAUTH=ALL	SDSF	ALTER	ISFINIT.I(xx).jesx	Use generic profiles to give authority to all initiators.

Table 19. RACF class and profile equivalents to ISFPARMS (continued)

ISFPARM	RACF Class	Access	RACF Profile	Description
CMDLEV	SDSF	UPDATE	ISFATTR.JOB.field ISFATTR.OUTPUT.field ISFATTR.OUTDESC.field ISFATTR.CHECK.field ISFATTR.ENCLAVE.field ISFATTR.JOBCL.field IISFATTR.LINE.field ISFATTR.MEMBER.field ISFATTR.NETOPTS.field ISFATTR.NODE.field ISFATTR.OFFLOAD.field SFATTR.PROPTS.field ISFATTR.RDR.field ISFATTR.RESMON.field ISFATTR.RESOURCE.field ISFATTR.SPOOL.field ISFATTR.MODIFY.field ISFATTR.SELECT.field	Authorizes use of overtypeable fields.
CMDLEV	OPERCMDS		Depends on the generated MVS or JES2 command.	
DEST	SDSF	ALTER	ISFAUTH.DEST.destname	Equivalent to DEST for the CMDAUTH parameter, with a DEST parameter. In the SAF resource, destname is a destination name specified through the DEST parameter.
DEST	SDSF	READ	ISFAUTH.DEST.destname. Ddsid.dsname	Equivalent to DEST for the DSPAUTH parameter, with a DEST parameter. In the SAF resource, destname is a destination name specified through the DEST parameter.
DSPAUTH=ADEST	SDSF	READ	ISFOPER.DEST.jesx	SDSF does further checking for authority to jobs and output based on destination.

Table 19. RACF class and profile equivalents to ISFPARMS (continued)

ISFPARM	RACF Class	Access	RACF Profile	Description
DSPAUTH=ADEST	SDSF	READ	ISFAUTH.DEST.destname. DATASET.dsname	Equivalent to ADEST for the DSPAUTH parameter, with a DEST parameter. In the SAF resource, destname is a destination name specified through the DEST parameter.
DSPAUTH=ALL	SDSF	READ	ISFOPER.DEST.jesx	SDSF does further checking for authority to jobs and output based on destination.
DSPAUTH=ALL	SDSF	READ	ISFAUTH.DEST.destname	Equivalent to ALL for the DSPAUTH parameter, with a DEST parameter. In the SAF resource, destname is a destination name specified through the DEST parameter.
DSPAUTH=AMDEST	SDSF	READ	ISFOPER.DEST.jesx	SDSF does further checking for authority to jobs and output based on destination.
DSPAUTH=AMDEST	SDSF	READ	ISFAUTH.DEST.destname. DATASET.JESMSGLG ISFAUTH.DEST.destname. DATASET.JESJCL ISFAUTH.DEST.destname. DATASET.JESYSMSG	Equivalent to AMDEST for the DSPAUTH parameter, with a DEST Parameter, when JESMSGLG, JESJCL, JESYSMSG are data set names of JES2 message data sets and destname is a destination name specified through the DEST parameter.
DSPAUTH=AMSG	JESSPOOL	READ	node.userid.jobname.jobid. Ddsid.JESMSGLG node.userid.jobname.jobid. Ddsid.JESJCL node.userid.jobname.jobid. Ddsid.JESYSMSG	Equivalent to AMSG for the DSPAUTH parameter, when JESMSGLG, JESJCL, JESYSMSG are data set names of JES2 message data sets. (You can define generic profiles for the above AMDEST resources to obtain equivalent function.)

Table 19. RACF class and profile equivalents to ISFPARMS (continued)

ISFPARM	RACF Class	Access	RACF Profile	Description
DSPAUTH=GROUP	JESSPOOL	READ	node.userid.jobname.jobid. Ddsid.dsname	Equivalent to GROUP for the DSPAUTH parameter, when jobname is the group prefix. (With structured TSO user IDs, you can specify user ID instead of jobname.)
DSPAUTH=GRPMSG	JESSPOOL	READ	node.userid.jobname.jobid. Ddsid.JESMSGLG node.userid.jobname.jobid. Ddsid.JESJCL node.userid.jobname.jobid. Ddsid.JESYSMSG	Equivalent to GRPMSG for the DSPAUTH parameter, when JESMSGLG, JESJCL, JESYSMSG are data set names of JES2 message data sets and jobname is the group prefix.
DSPAUTH=NOTIFY	No direct SAF equivalent.			
DSPAUTH=USERID	JESSPOOL	READ	node.userid.jobname.jobid. Ddsid.dsname	Equivalent to USERID for the DSPAUTH parameter, when userid is the name of the job the user is trying to access. (Even when no profiles are defined in the JESSPOOL class, users are authorized to output that they own.)
ICMD	JESSPOOL	ALTER	node.userid.jobname.jobid node.userid.jobname.jobid. GROUP.ogroupid	Equivalent to the ICMD parameter, when jobname is a job name specified by the associated ISFNTBL macro or NTBL statement.
IDEST	SDSF	READ	ISFOPER.ANYDEST.jesx	If users do not have an IDEST parameter with initial destinations specified, they must have READ access to this resource, or no jobs can appear on the panels.
IDEST	SDSF	READ	ISFAUTH.DEST.destname	SDSF initialization function. Users must be authorized to the destnames that correspond to the initial destination values specified by their IDEST parameter. If not, no jobs can appear on the panels.

Table 19. RACF class and profile equivalents to ISFPARMS (continued)

ISFPARM	RACF Class	Access	RACF Profile	Description
IDSP	JESSPOOL	READ	node.userid.jobname.jobid. Ddsid.dsname	Equivalent to the IDSP parameter, when jobname is a job name specified by the associated ISFNTBL macro or NTBL statement.
IDSPD	JESSPOOL	READ	node.userid.jobname.jobid. Ddsid.JESMSGLG node.userid.jobname.jobid. Ddsid.JESJCL node.userid.jobname.jobid. Ddsid.JESYSMSG	Equivalent to the IDSPD parameter, when JESMSGLG, JESJCL, JESYSMSG are data set names of JES message data sets.
ISTATUS	Includes jobs on the SDSF panels based on job name. Work around by using a table build exit point.			
XCMD	JESSPOOL	NONE	node.userid.jobname.jobid node.userid.jobname.jobid. GROUP.ogroupid	Equivalent to the XCMD parameter, when jobname is a job name specified by the associated ISFNTBL macro or NTBL statement and the access is NONE.
XDSP	JESSPOOL	NONE	node.userid.jobname.jobid. Ddsid.dsname	Equivalent to the XDSP parameter, when jobname is a job name specified by the associated ISFNTBL macro or NTBL statement and the access is NONE.
XDSPD	JESSPOOL	NONE	node.userid.jobname.jobid. Ddsid.dsname	Equivalent to the XDSPD parameter, when jobname is a job name specified by the associated ISFNTBL macro or NTBL statement and the access is NONE.
XDSPD	JESSPOOL	READ	node.userid.jobname.jobid. Ddsid.JESMSGLG node.userid.jobname.jobid. Ddsid.JESJCL node.userid.jobname.jobid. Ddsid.JESYSMSG	User must then be authorized to the message data sets for the job.
XSTATUS	Excludes jobs on the SDSF panels based on job name. Work around by using a table build exit point.			

Appendix B. ISFPARMS parameters not applicable to SAF

Some ISFPARMS are not applicable to SAF.

The following lists the ISFPARMS that are not applicable to SAF:

- A
- ACTION
- ACTIONBAR
- APPC
- AUPDT
- B
- BROWSE
- C
- CONFIRM
- CPUFMT
- CTITLE
- CURSOR
- D
- DADFLT
- DATE
- DATESEP
- DISPLAY
- E
- EMCAUTH
- EMCSREQ
- G
- GPLEN
- GPREF
- I
- ILOGCOL
- INPUT
- ISYS (see note below)
- L
- LANG
- LOG/LOGOPT
- O
- OWNER (see note below)
- P
- PREFIX (see note below)
- R
- RSYS

- S
- SYSID
- U
- UPCTAB
- V
- VALTAB
- VIO

Note: ISYS, OWNER, and PREFIX can be specified only to declare default values for the user. The user will be restricted by these specifications if they do not have SAF authority to the associated commands that can change them from within the product.

Appendix C. RACF classes and profiles that protect SDSF

The table that follows provides a list of SDSF functions and the RACF classes and profiles required to protect them.

Table 20. RACF classes and profiles that protect SDSF functions

RACF Class	RACF Profile	What it protects
JESSPOOL	nodeid.+MASTER+.SYSLOG.SYSTEM.sysname	Access to the JES logical log, for displaying the SYSLOG.
JESSPOOL	nodeid.userid.groupname.groupid	Job groups.
JESSPOOL	nodeid.userid.jobname.jobid	Jobs.
JESSPOOL	nodeid.userid.jobname.jobid.Ddsid.dsname	SYSIN/SYSOUT data sets.
JESSPOOL	nodeid.userid.jobname.jobid.EVENTLOG.SMFSTEP nodeid.userid.jobname.jobid.EVENTLOG.STEPDATA	JES data sets used for job steps.
JESSPOOL	nodeid.userid.jobname.jobid.GROUP.ogroupid	Output groups.
LOGSTRM	HZS.sysname.checkowner.checkname.function	Log stream for check history (CKH panel).
LOGSTRM	SYSPLEX.OPERLOG	Log stream used for OPERLOG.
OPERCMDS	jesname.command[.qualifier] MVS.command[.qualifier]	MVS and JES generated commands.
OPERCMDS	server-name.MODIFY.DEBUG	DEBUG parameter of MODIFY.
OPERCMDS	server-name.MODIFY.DISPLAY	DISPLAY parameter of MODIFY.
OPERCMDS	server-name.MODIFY.FOLDMSG	FOLDMSG parameter of MODIFY.
OPERCMDS	server-name.MODIFY.LOGCLASS	LOGCLASS parameter of MODIFY.
OPERCMDS	server-name.MODIFY.REFRESH	REFRESH parameter of MODIFY.
OPERCMDS	server-name.MODIFY.START	START parameter of MODIFY.
OPERCMDS	server-name.MODIFY.STOP	STOP parameter of MODIFY.
OPERCMDS	server-name.MODIFY.TRACE	TRACE parameter of MODIFY.
OPERCMDS	server-name.MODIFY.TRCLASS	TRCLASS parameter of MODIFY.
SDSF	GROUP.group-name.server-name	Membership in groups defined in ISFPARMS.
SDSF	ISF.CONNECTsystem	To connect to the SDSF server, the user must have READ access.
SDSF	ISFAPF.datasetname	APF data sets.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFAPPL.device-name.jesx ISFSOCK.device-name.jesx ISFLINEdevice-name.jesx	Network connections.
SDSF	ISFATTR.CHECK.CATEGORY	Panel CK – overtypeable field CATEGORY.
SDSF	ISFATTR.CHECK.DEBUG	Panel CK – overtypeable field DEBUG.
SDSF	ISFATTR.CHECK.EINTERVAL	Panel CK – overtypeable field EINTERVAL.
SDSF	ISFATTR.CHECK.INTERVAL	Panel CK – overtypeable field INTERVAL.
SDSF	ISFATTR.CHECK.PARM	Panel CK – overtypeable field PARAMETERS.
SDSF	ISFATTR.CHECK.SEVERITY	Panel CK – overtypeable field SEVERITY.
SDSF	ISFATTR.CHECK.USERDATE	Panel CK – overtypeable field USERDATE.
SDSF	ISFATTR.CHECK.VERBOSE	Panel CK – overtypeable field VERBOSE.
SDSF	ISFATTR.CHECK.WTOTYPE	Panel CK – overtypeable field WTOTYPE.
SDSF	ISFATTR.CKPT.OPVERIFY	Panel CKPT – overtypeable field OPVERIFY.
SDSF	ISFATTR.EMCS.AUTH	Panel EMCS – overtypeable field AUTH.
SDSF	ISFATTR.EMCS.INTIDS	Panel EMCS – overtypeable field INITDS.
SDSF	ISFATTR.EMCS.MSCOPE	Panel EMCS – overtypeable field MSCOPE.
SDSF	ISFATTR.EMCS.ROUTCDE	Panel EMCS – overtypeable field ROUTCODE.
SDSF	ISFATTR.EMCS.UNKNIDS	Panel EMCS – overtypeable field UNKNIDS.
SDSF	ISFATTR.ENCLAVE.SRVCLASS	Panel ENC – overtypeable field SRVCLASS.
SDSF	ISFATTR.INIT.ALLOC	Panel INIT – overtypeable field ALLOC.
SDSF	ISFATTR.INIT.BARRIER	Panel INIT – overtypeable field BARRIER.
SDSF	ISFATTR.INIT.DEFCNT	Panel INIT – overtypeable field DEFCOUNT.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.INIT.GROUP	Panel INIT – overtypeable field GROUP.
SDSF	ISFATTR.INIT.MODE	Panel INIT – overtypeable field MODE.
SDSF	ISFATTR.INIT.UNALLOC	Panel INIT – overtypeable field UNALLOC.
SDSF	ISFATTR.JOB.CLASS	Panels I, ST – overtypeable field C.
SDSF	ISFATTR.JOB.EXECNODE	Panels I, ST – overtypeable field EXECNODE.
SDSF	ISFATTR.JOB.PGN	Panel DA – overtypeable field PGN.
SDSF	ISFATTR.JOB.PRTDEST	Panels I, ST – overtypeable field PRTDEST.
SDSF	ISFATTR.JOB.PRTY	Panels I, ST – overtypeable field PRTY.
SDSF	ISFATTR.JOB.QUIESCE	Panel DA – overtypeable field QUIESCE.
SDSF	ISFATTR.JOB.SCHENV	Panels I, ST – overtypeable field SCHEDULING-ENV.
SDSF	ISFATTR.JOB.SRVCLASS	Panel DA – overtypeable field SRVCLASS.
SDSF	ISFATTR.JOB.SRVCLS	Panels I, ST – overtypeable field SRVCLASS.
SDSF	ISFATTR.JOB.SYSAFF	Panels I, ST – overtypeable field SAFF.
SDSF	ISFATTR.JOBCL.ACCT	Panel JC – overtypeable field ACCT.
SDSF	ISFATTR.JOBCL.ACTIVE	Panel JC – overtypeable field ACTIVE.
SDSF	ISFATTR.JOBCL.AUTH	Panel JC – overtypeable field AUTH.
SDSF	ISFATTR.JOBCL.BLP	Panel JC – overtypeable field BLP.
SDSF	ISFATTR.JOBCL.COMMAND	Panel JC – overtypeable field COMMAND.
SDSF	ISFATTR.JOBCL.CONDPURG	Panel JC – overtypeable field CPR.
SDSF	ISFATTR.JOBCL.COPY	Panel JC – overtypeable field CPY.
SDSF	ISFATTR.JOBCL.GDGBIAS	Panel JC – overtypeable field GDGBIAS.
SDSF	ISFATTR.JOBCL.GROUP	Panel JC – overtypeable field GROUP.
SDSF	ISFATTR.JOBCL.HOLD	Panel JC – overtypeable field HOLD.
SDSF	ISFATTR.JOBCL.IEFUJP	Panel JC – overtypeable field UJP.
SDSF	ISFATTR.JOBCL.IEFUSO	Panel JC – overtypeable field USO.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.JOBCL.JCLIM	Panel JC – overtypeable field JCLIM.
SDSF	ISFATTR.JOBCL.JESLOG	Panel JC – overtypeable field JESLOG.
SDSF	ISFATTR.JOBCL.JLOG	Panel JC – overtypeable field LOG.
SDSF	ISFATTR.JOBCL.JOBRC	Panel JC – overtypeable field JOBRC.
SDSF	ISFATTR.JOBCL.JOURNAL	Panel JC – overtypeable field JRNL.
SDSF	ISFATTR.JOBCL.MODE	Panel JC – overtypeable field MODE.
SDSF	ISFATTR.JOBCL.MSGCLASS	Panel JC – overtypeable field MC.
SDSF	ISFATTR.JOBCL.MSGLEVEL	Panel JC – overtypeable field MSGLV.
SDSF	ISFATTR.JOBCL.ODISP	Panel JC – overtypeable field ODISP.
SDSF	ISFATTR.JOBCL.OUTPUT	Panel JC – overtypeable field OUT.
SDSF	ISFATTR.JOBCL.PARTNAME	Panel JC – overtypeable field PARTNAME.
SDSF	ISFATTR.JOBCL.PGMRNAME	Panel JC – overtypeable field PGNM.
SDSF	ISFATTR.JOBCL.PGN	Panel JC – overtypeable field PGN.
SDSF	ISFATTR.JOBCL.PROCLIB	Panel JC – overtypeable field PL.
SDSF	ISFATTR.JOBCL.PROMORATE	Panel JC – overtypeable field PROMORT.
SDSF	ISFATTR.JOBCL.QHELD	Panel JC – overtypeable field QHLD.
SDSF	ISFATTR.JOBCL.REGION	Panel JC – overtypeable field REGION.
SDSF	ISFATTR.JOBCL.RESTART	Panel JC – overtypeable field RST.
SDSF	ISFATTR.JOBCL.SCAN	Panel JC – overtypeable field SCN.
SDSF	ISFATTR.JOBCL.SCHENV	Panel JC – overtypeable field SCHEDULING-ENV.
SDSF	ISFATTR.JOBCL.SDEPTH	Panel JC – overtypeable field SDEPTH.
SDSF	ISFATTR.JOBCL.SWA	Panel JC – overtypeable field SWA.
SDSF	ISFATTR.JOBCL.SYSSYM	Panel JC – overtypeable field SYSSYM.
SDSF	ISFATTR.JOBCL.TDEPTH	Panel JC – overtypeable field TDEPTH.
SDSF	ISFATTR.JOBCL.TIME	Panel JC – overtypeable field MAX-TIME.
SDSF	ISFATTR.JOBCL.TYPE26	Panel JC – overtypeable field TP26.
SDSF	ISFATTR.JOBCL.TYPE6	Panel JC – overtypeable field TP6.
SDSF	ISFATTR.JOBCL.XBM	Panel JC – overtypeable field XBM.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.JOBGROUP.SCHENV	Panel JG – overtypeable field SCHEDULING-ENV.
SDSF	ISFATTR.JOBGROUP.SYSAFF	Panel JG – overtypeable field SAFF.
SDSF	ISFATTR.LINE.APPLID	Panel LI – overtypeable field APPLID.
SDSF	ISFATTR.LINE.AUTODISC	Panel LI – overtypeable field ADISC.
SDSF	ISFATTR.LINE.CODE	Panel LI – overtypeable field CODE.
SDSF	ISFATTR.LINE.COMPRESS	Panel LI – overtypeable field COMP.
SDSF	ISFATTR.LINE.DUPLEX	Panel LI – overtypeable field DUPLEX.
SDSF	ISFATTR.LINE.INTERFACE	Panel LI – overtypeable field INTF.
SDSF	ISFATTR.LINE.JRNUM	Panel LI – overtypeable field JRNUM.
SDSF	ISFATTR.LINE.JTNUM	Panel LI – overtypeable field JTNUM.
SDSF	ISFATTR.LINE.LINECCHR	Panel LI – overtypeable field LINECCHR.
SDSF	ISFATTR.LINE.LOG	Panel LI – overtypeable field LOG.
SDSF	ISFATTR.LINE.NODE	Panel LI – overtypeable field NODE.
SDSF	ISFATTR.LINE.PASSWORD	Panel LI – overtypeable field PASSWORD.
SDSF	ISFATTR.LINE.REST	Panels LI, NC – overtypeable field REST.
SDSF	ISFATTR.LINE.SPEED	Panel LI – overtypeable field SPEED.
SDSF	ISFATTR.LINE.SRNUM	Panel LI – overtypeable field SRNUM.
SDSF	ISFATTR.LINE.STNUM	Panel LI – overtypeable field STNUM.
SDSF	ISFATTR.LINE.TRANSPARENCY	Panel LI – overtypeable field TRANSP.
SDSF	ISFATTR.LOGON.PASSWORD	Panel NS – overtypeable field PASSWORD.
SDSF	ISFATTR.MEMBER.CKPTHOLD	Panel MAS – overtypeable field CKPTHOLD.
SDSF	ISFATTR.MEMBER.DORMANCY	Panel MAS – overtypeable field DORMANCY.
SDSF	ISFATTR.MEMBER.SELMNAME	Panel JP – overtypeable field SELECTMODENAME.
SDSF	ISFATTR.MEMBER.SPARTN	Panel JP – overtypeable field PARTNAME.
SDSF	ISFATTR.MEMBER.SYNCTOL	Panel MAS – overtypeable field SYNCTOL.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.MODIFY.BURST	Panel SO – overtypeable field MBURST.
SDSF	ISFATTR.MODIFY.CLASS	Panel SO – overtypeable field MCLASS.
SDSF	ISFATTR.MODIFY.DEST	Panel SO – overtypeable field MDEST.
SDSF	ISFATTR.MODIFY.FCB	Panel SO – overtypeable field MFCB.
SDSF	ISFATTR.MODIFY.FLASH	Panel SO – overtypeable field MFLH.
SDSF	ISFATTR.MODIFY.FORMS	Panel SO – overtypeable field MFORMS.
SDSF	ISFATTR.MODIFY.HOLD	Panel SO – overtypeable field MHOLD.
SDSF	ISFATTR.MODIFY.ODISP	Panel SO – overtypeable field MODSP.
SDSF	ISFATTR.MODIFY.PRMODE	Panel SO – overtypeable field MPRMODE.
SDSF	ISFATTR.MODIFY.SYSAFF	Panel SO – overtypeable field MSAFF.
SDSF	ISFATTR.MODIFY.UCS	Panel SO – overtypeable field MUCS.
SDSF	ISFATTR.MODIFY.WRITER	Panel SO – overtypeable field MWRITER.
SDSF	ISFATTR.NETOPTS.APPL	Panel NS – overtypeable field APPL.
SDSF	ISFATTR.NETOPTS.CONNECT	Panels LI, NC, NO – overtypeable field CONNECT.
SDSF	ISFATTR.NETOPTS.CTIME	Panels LI, NC, NO – overtypeable field CONN-INT.
SDSF	ISFATTR.NETOPTS.IPNAME	Panels NC, NS – overtypeable field IPNAME.
SDSF	ISFATTR.NETOPTS.LINE	Panel NC – overtypeable field LINE.
SDSF	ISFATTR.NETOPTS.LOG	Panel NS – overtypeable field LOG.
SDSF	ISFATTR.NETOPTS.LOGON	Panel NC – overtypeable field LOGON.
SDSF	ISFATTR.NETOPTS.NETSRV	Panel NC – overtypeable field NETSRV.
SDSF	ISFATTR.NETOPTS.NETSRV	Panel NC – overtypeable field SRVNAME.
SDSF	ISFATTR.NETOPTS.NODE	Panel NC – overtypeable field ANODE.
SDSF	ISFATTR.NETOPTS.NSECURE	Panel NS – overtypeable field NSECURE.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.NETOPTS.PORT	Panels NC, NS – overtypeable field PORT.
SDSF	ISFATTR.NETOPTS.SECURE	Panels NC, NO, NS – overtypeable field SECURE.
SDSF	ISFATTR.NETOPTS.SOCKET	Panel NS – overtypeable field SOCKET.
SDSF	ISFATTR.NETOPTS.STACK	Panel NS – overtypeable field STACK.
SDSF	ISFATTR.NODE.AUTHORITY	Panel NO – overtypeable field AUTHORITY.
SDSF	ISFATTR.NODE.COMPACT	Panel NC – overtypeable field COMPACT.
SDSF	ISFATTR.NODE.COMPACT	Panel NO – overtypeable field CP.
SDSF	ISFATTR.NODE.DIRECT	Panel NO – overtypeable field DIRECT.
SDSF	ISFATTR.NODE.ENDNODE	Panel NO – overtypeable field END.
SDSF	ISFATTR.NODE.HOLD	Panel NO – overtypeable field HOLD.
SDSF	ISFATTR.NODE.JRNUM	Panel NO – overtypeable field JRNUM.
SDSF	ISFATTR.NODE.JTNUM	Panel NO – overtypeable field JTNUM.
SDSF	ISFATTR.NODE.LINE	Panels NC, NO – overtypeable field LINE.
SDSF	ISFATTR.NODE.LOGMODE	Panels NC, NO – overtypeable field LOGMODE.
SDSF	ISFATTR.NODE.LOGON	Panel NO – overtypeable field LOGON.
SDSF	ISFATTR.NODE.MAXRETR	Panel NO – overtypeable field MAXRETRIES.
SDSF	ISFATTR.NODE.NETHOLD	Panel NO – overtypeable field NHOLD.
SDSF	ISFATTR.NODE.NETSRV	Panel NO – overtypeable field NETSRV.
SDSF	ISFATTR.NODE.NODENAME	Panel NO – overtypeable field NODENAME.
SDSF	ISFATTR.NODE.PARTNAM	Panel NO – overtypeable field PARTNAME.
SDSF	ISFATTR.NODE.PATH	Panel NO – overtypeable field PATH.
SDSF	ISFATTR.NODE.PATHMGR	Panel NO – overtypeable field PMG.
SDSF	ISFATTR.NODE.PENCRYPT	Panel NO – overtypeable field PEN.
SDSF	ISFATTR.NODE.PRIVATE	Panel NO – overtypeable field PRV.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.NODE.PRTDEF	Panel NO – overtypeable field PRTDEF.
SDSF	ISFATTR.NODE.PRTTSO	Panel NO – overtypeable field PRTTSO.
SDSF	ISFATTR.NODE.PRTXWTR	Panel NO – overtypeable field PRTXWTR.
SDSF	ISFATTR.NODE.PTYPE	Panel NO – overtypeable field PTYPE.
SDSF	ISFATTR.NODE.PUNDEF	Panel NO – overtypeable field PUNDEF.
SDSF	ISFATTR.NODE.PWCNTL	Panel NO – overtypeable field PWCNTL.
SDSF	ISFATTR.NODE.RECEIVE	Panel NO – overtypeable field RECV.
SDSF	ISFATTR.NODE.REST	Panel NO – overtypeable field REST.
SDSF	ISFATTR.NODE.SENDP	Panel NO – overtypeable field SENDP.
SDSF	ISFATTR.NODE.SENTREST	Panel NO – overtypeable field SENTRS.
SDSF	ISFATTR.NODE.SRNUM	Panel NO – overtypeable field SRNUM.
SDSF	ISFATTR.NODE.SSIGNON	Panel NO – overtypeable field SSIGNON.
SDSF	ISFATTR.NODE.STNUM	Panel NO – overtypeable field STNUM.
SDSF	ISFATTR.NODE.SUBNET	Panel NO – overtypeable field SUBNET.
SDSF	ISFATTR.NODE.TRACE	Panel NO – overtypeable field TR.
SDSF	ISFATTR.NODE.TRANSMIT	Panel NO – overtypeable field TRANS.
SDSF	ISFATTR.NODE.VERIFYP	Panel NO – overtypeable field VERIFYP.
SDSF	ISFATTR.NODE.VFYPATH	Panel NO – overtypeable field VFYPATH.
SDSF	ISFATTR.OFFLOAD.ARCHIVE	Panel SO – overtypeable field ARCHIVE.
SDSF	ISFATTR.OFFLOAD.CRTIME	Panel SO – overtypeable field CRTIME.
SDSF	ISFATTR.OFFLOAD.DATASET	Panel SO – overtypeable field DSNAME.
SDSF	ISFATTR.OFFLOAD.LABEL	Panel SO – overtypeable field LABEL.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.OFFLOAD.NOTIFY	Panel SO – overtypeable field NOTIFY.
SDSF	ISFATTR.OFFLOAD.PROTECT	Panel SO – overtypeable field PROT.
SDSF	ISFATTR.OFFLOAD.RETENT	Panel SO – overtypeable field RTPD.
SDSF	ISFATTR.OFFLOAD.VALIDATE	Panel SO – overtypeable field VALIDATE.
SDSF	ISFATTR.OFFLOAD.VOLS	Panel SO – overtypeable field VOLS.
SDSF	ISFATTR.OMVS.VALUE	Panel OMVS – overtypeable field NUMVALUE.
SDSF	ISFATTR.OUTDESC.ADDRESS	Panels JDS, OD – overtypeable field ADDRESS.
SDSF	ISFATTR.OUTDESC.AFPPARMS	Panels JDS, OD – overtypeable field AFPPARMS.
SDSF	ISFATTR.OUTDESC.BLDG	Panels JDS, OD – overtypeable field BUILDING.
SDSF	ISFATTR.OUTDESC.COLORMAP	Panels JDS, OD – overtypeable field COLORMAP.
SDSF	ISFATTR.OUTDESC.COMSETUP	Panels JDS, OD – overtypeable field COMSETUP.
SDSF	ISFATTR.OUTDESC.DEPT	Panels JDS, OD – overtypeable field DEPARTMENT.
SDSF	ISFATTR.OUTDESC.FORMDEF	Panels JDS,, OD – overtypeable field FORMDEF.
SDSF	ISFATTR.OUTDESC.FORMLEN	Panels JDS OD – overtypeable field FORMLEN.
SDSF	ISFATTR.OUTDESC.INTRAY	Panel JDS – overtypeable field ITY.
SDSF	ISFATTR.OUTDESC.INTRAY	Panel OD – overtypeable field INTRAY.
SDSF	ISFATTR.OUTDESC.IPDEST	Panel OD – overtypeable field IP DESTINATION.
SDSF	ISFATTR.OUTDESC.NAME	Panels JDS, OD – overtypeable field NAME.
SDSF	ISFATTR.OUTDESC.NOTIFY	Panels JDS, OD – overtypeable field NOTIFY.
SDSF	ISFATTR.OUTDESC.OCOPYCNT	Panels JDS, OD – overtypeable field OCOPYCNT.
SDSF	ISFATTR.OUTDESC.OFFSETXB	Panels JDS, OD – overtypeable field OFFSETXB.
SDSF	ISFATTR.OUTDESC.OFFSETXF	Panels JDS, OD – overtypeable field OFFSETXF.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.OUTDESC.OFFSETYB	Panels JDS, OD – overtypeable field OFFSETYB.
SDSF	ISFATTR.OUTDESC.OFFSETYF	Panels JDS, OD – overtypeable field OFFSETYF.
SDSF	ISFATTR.OUTDESC.OUTBIN	Panel JDS – overtypeable field OUTBIN.
SDSF	ISFATTR.OUTDESC.OUTBIN	Panel OD – overtypeable field OUTBIN.
SDSF	ISFATTR.OUTDESC.OVERLAYB	Panels JDS, OD – overtypeable field OVERLAYB.
SDSF	ISFATTR.OUTDESC.OVERLAYF	Panels JDS, OD – overtypeable field OVERLAYF.
SDSF	ISFATTR.OUTDESC.PAGEDEF	Panels JDS, OD – overtypeable field PAGEDEF.
SDSF	ISFATTR.OUTDESC.PORTNO	Panel JDS – overtypeable field PORT.
SDSF	ISFATTR.OUTDESC.PORTNO	Panel OD – overtypeable field PORTNO.
SDSF	ISFATTR.OUTDESC.PRINTO	Panel OD – overtypeable field PRTOPTNS.
SDSF	ISFATTR.OUTDESC.PRINTQ	Panel OD – overtypeable field PRTQUEUE.
SDSF	ISFATTR.OUTDESC.RETAINF	Panel OD – overtypeable field RETAINF.
SDSF	ISFATTR.OUTDESC.RETAINS	Panel OD – overtypeable field RETAINS.
SDSF	ISFATTR.OUTDESC.RETRYL	Panel OD – overtypeable field RETRYL.
SDSF	ISFATTR.OUTDESC.RETRYT	Panel OD – overtypeable field RETRYT.
SDSF	ISFATTR.OUTDESC.ROOM	Panels JDS, OD – overtypeable field ROOM.
SDSF	ISFATTR.OUTDESC.TITLE	Panels JDS, OD – overtypeable field TITLE.
SDSF	ISFATTR.OUTDESC.USERDATA	Panel JDS – overtypeable field USERDATA1.
SDSF	ISFATTR.OUTDESC.USERDATA	Panel OD – overtypeable field USERDATA.
SDSF	ISFATTR.OUTDESC.USERLIB	Panels JDS, OD – overtypeable field USERLIB.
SDSF	ISFATTR.OUTPUT.BURST	Panel H, O – overtypeable field BURST.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.OUTPUT.BURST	Panels JDS, J0 – overtypeable field BURST.
SDSF	ISFATTR.OUTPUT.CHARS	Panels JDS, J0 – overtypeable field CHARS.
SDSF	ISFATTR.OUTPUT.CLASS	Panels H, O, JDS, J0 – overtypeable field C.
SDSF	ISFATTR.OUTPUT.COPYCNT	Panels JDS, J0 – overtypeable field CC.
SDSF	ISFATTR.OUTPUT.COPYMOD	Panel JDS – overtypeable field CPYMOD.
SDSF	ISFATTR.OUTPUT.DEST	Panel H – overtypeable field DEST.
SDSF	ISFATTR.OUTPUT.DEST	Panels H, O, JDS, J0 – overtypeable field DEST.
SDSF	ISFATTR.OUTPUT.FCB	Panels H, O – overtypeable field FCB.
SDSF	ISFATTR.OUTPUT.FCB	Panels JDS, J0 – overtypeable field FCB.
SDSF	ISFATTR.OUTPUT.FLASH	Panels H, O – overtypeable field FLASH.
SDSF	ISFATTR.OUTPUT.FLASH	Panels JDS, J0 – overtypeable field FLASH.
SDSF	ISFATTR.OUTPUT.FORMS	Panels H, O, JDS, J0 – overtypeable field FORMS.
SDSF	ISFATTR.OUTPUT.ODISP	Panels H, JDS, O – overtypeable field ODISP.
SDSF	ISFATTR.OUTPUT.PRMODE	Panels H, O, JDS, J0 – overtypeable field PRMODE.
SDSF	ISFATTR.OUTPUT.PRTY	Panels H, O – overtypeable field PRTY.
SDSF	ISFATTR.OUTPUT.UCS	Panels H, O, JDS, J0 – overtypeable field UCS.
SDSF	ISFATTR.OUTPUT.WRITER	Panels H, O, JDS, J0 – overtypeable field WTR.
SDSF	ISFATTR.PROPTS.ASIS	Panel PR – overtypeable field ASIS.
SDSF	ISFATTR.PROPTS.BPAGE	Panels PR, PUN – overtypeable field B.
SDSF	ISFATTR.PROPTS.CB	Panel PR – overtypeable field CB.
SDSF	ISFATTR.PROPTS.CCTL	Panels PR, PUN – overtypeable field CCTL.
SDSF	ISFATTR.PROPTS.CHAR	Panel PR – overtypeable field CHAR1-4.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.PROPTS.CKPTLINE	Panels PR, PUN – overtypeable field CKPTLINE.
SDSF	ISFATTR.PROPTS.CKPTMODE	Panel PR – overtypeable field CKPTMODE.
SDSF	ISFATTR.PROPTS.CKPTPAGE	Panels PR, PUN – overtypeable field CKPTPAGE.
SDSF	ISFATTR.PROPTS.CKPTSEC	Panel PR – overtypeable field CKPTSEC.
SDSF	ISFATTR.PROPTS.CMPCT	Panels PR, PUN – overtypeable field CMPCT.
SDSF	ISFATTR.PROPTS.COMPACT	Panels PR, PUN – overtypeable field COMPACT.
SDSF	ISFATTR.PROPTS.COMPRESS	Panels PR, PUN – overtypeable field COMP.
SDSF	ISFATTR.PROPTS.COPIES	Panels PR, PUN – overtypeable field COPIES.
SDSF	ISFATTR.PROPTS.COPYMARK	Panel PR – overtypeable field COPYMARK.
SDSF	ISFATTR.PROPTS.COPYMOD	Panels J0, PR – overtypeable field CPYMOD.
SDSF	ISFATTR.PROPTS.CTRACE	Panels LI, NC, NS – overtypeable field CTR.
SDSF	ISFATTR.PROPTS.DEVFCB	Panel PR – overtypeable field DFCB.
SDSF	ISFATTR.PROPTS.DGRPY	Panels PR, PUN – overtypeable field DGRPY.
SDSF	ISFATTR.PROPTS.DYN	Panels PR, PUN – overtypeable field DYN.
SDSF	ISFATTR.PROPTS.FLUSH	Panel PUN – overtypeable field FLS.
SDSF	ISFATTR.PROPTS.FSATRACE	Panel PR – overtypeable field FSATRACE.
SDSF	ISFATTR.PROPTS.FSSNAME	Panel PR – overtypeable field FSSNAME.
SDSF	ISFATTR.PROPTS.HONORTRC	Panel PR – overtypeable field HONORTRC.
SDSF	ISFATTR.PROPTS.JTRACE	Panels LI, NC, NS – overtypeable field JTR.
SDSF	ISFATTR.PROPTS.LRECL	Panel PUN – overtypeable field LRECL.
SDSF	ISFATTR.PROPTS.MARK	Panel PR – overtypeable field M.
SDSF	ISFATTR.PROPTS.MODE	Panel PR – overtypeable field MODE.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.PROPTS.NEWPAGE	Panel PR – overtypeable field NEWPAGE.
SDSF	ISFATTR.PROPTS.NPRO	Panel PR – overtypeable field NPRO.
SDSF	ISFATTR.PROPTS.OPACTLOG	Panels PR, PUN – overtypeable field OPLOG.
SDSF	ISFATTR.PROPTS.PAUSE	Panels PR, PUN – overtypeable field PAU.
SDSF	ISFATTR.PROPTS.PDEFAULT	Panel PR – overtypeable field PDEFAULT.
SDSF	ISFATTR.PROPTS.PRESELCT	Panel PR – overtypeable field PSEL.
SDSF	ISFATTR.PROPTS.RESTART	Panel LI – overtypeable field RESTART.
SDSF	ISFATTR.PROPTS.RTIME	Panels LI, NS – overtypeable field REST-INT.
SDSF	ISFATTR.PROPTS.SELECT	Panels PR, PUN – overtypeable field SELECT.
SDSF	ISFATTR.PROPTS.SEP	Panels PR, PUN – overtypeable field SEP.
SDSF	ISFATTR.PROPTS.SEPCHARS	Panels PR, PUN – overtypeable field SEPCHAR.
SDSF	ISFATTR.PROPTS.SEPDS	Panels PR, PUN, RDR – overtypeable field SEPDS.
SDSF	ISFATTR.PROPTS.SETUP	Panels PR, PUN – overtypeable field SETUP.
SDSF	ISFATTR.PROPTS.SPACE	Panel PR – overtypeable field K.
SDSF	ISFATTR.PROPTS.SUSPEND	Panel PUN – overtypeable field SUS.
SDSF	ISFATTR.PROPTS.TRACE	Panels LI, NC, NS, PR, PUN – overtypeable field TR.
SDSF	ISFATTR.PROPTS.TRANS	Panel PR – overtypeable field TRANS.
SDSF	ISFATTR.PROPTS.TRKCELL	Panel PR – overtypeable field TRKCELL.
SDSF	ISFATTR.PROPTS.UCSVERFY	Panel PR – overtypeable field UCSV.
SDSF	ISFATTR.PROPTS.UNIT	Panels LI, PR, PUN, SO – overtypeable field UNIT.
SDSF	ISFATTR.PROPTS.VTRACE	Panels LI, NC, NS – overtypeable field VTR.
SDSF	ISFATTR.PROPTS.WS	Panels LI, PR, PUN, SO – overtypeable field WORK-SELECTION.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.RDR.AUTHORITY	Panel RDR – overtypeable field AUTHORITY.
SDSF	ISFATTR.RDR.CLASS	Panel RDR – overtypeable field C.
SDSF	ISFATTR.RDR.HOLD	Panel RDR – overtypeable field HOLD.
SDSF	ISFATTR.RDR.MCLASS	Panel RDR – overtypeable field MC.
SDSF	ISFATTR.RDR.PRIOINC	Panel RDR – overtypeable field PI.
SDSF	ISFATTR.RDR.PRIOLIM	Panel RDR – overtypeable field PL.
SDSF	ISFATTR.RDR.PRTDEST	Panel RDR – overtypeable field PRTDEST.
SDSF	ISFATTR.RDR.PUNDEST	Panel RDR – overtypeable field PUNDEST.
SDSF	ISFATTR.RDR.SYSAFF	Panel RDR – overtypeable field SAFF1.
SDSF	ISFATTR.RDR.TRACE	Panel RDR – overtypeable field TR.
SDSF	ISFATTR.RDR.UNIT	Panel RDR – overtypeable field UNIT.
SDSF	ISFATTR.RDR.XEQDEST	Panel RDR – overtypeable field XEQDEST.
SDSF	ISFATTR.RESMON.LIMIT	Panel RM – overtypeable field LIM.
SDSF	ISFATTR.RESMON.WARNPCT	Panel RM – overtypeable field WARN%.
SDSF	ISFATTR.RESOURCE.system	Panel RES – overtypeable field System.
SDSF	ISFATTR.SELECT.BURST	Panels PR, SO – overtypeable field SBURST.
SDSF	ISFATTR.SELECT.CLASS	Panels PR, PUN – overtypeable field SCLASS.
SDSF	ISFATTR.SELECT.CLASS	Panel SO – overtypeable field SCLASS, SCLASS1-8.
SDSF	ISFATTR.SELECT.DEST	Panels PR, PUN, SO – overtypeable field SDEST1.
SDSF	ISFATTR.SELECT.DISP	Panel SO – overtypeable field SDISP.
SDSF	ISFATTR.SELECT.FCB	Panels PR, SO – overtypeable field SFCB.
SDSF	ISFATTR.SELECT.FLASH	Panels PR, SO – overtypeable field SFLH.
SDSF	ISFATTR.SELECT.FORMS	Panels PR, PUN, SO – overtypeable field SFORMS.
SDSF	ISFATTR.SELECT.HOLD	Panel SO – overtypeable field SHOLD.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.SELECT.JOBCLASS	Panel INIT – overtypeable field CLASSES, CLASS1-8.
SDSF	ISFATTR.SELECT.JOBNAME	Panels PR, PUN, SO – overtypeable field SJOBNAME.
SDSF	ISFATTR.SELECT.LIM	Panels LI, NC, PR, PUN, SO – overtypeable field LINE-LIMIT.
SDSF	ISFATTR.SELECT.LIM	Panels PR, PUN – overtypeable field LINE-LIM-HI.
SDSF	ISFATTR.SELECT.LIM	Panels PR, PUN – overtypeable field LINE-LIM-LO.
SDSF	ISFATTR.SELECT.ODISP	Panels NC, SO – overtypeable field LINE- SODSP.
SDSF	ISFATTR.SELECT.OUTDISP	Panel LI – overtypeable field LINE-SODSP.
SDSF	ISFATTR.SELECT.OWNER	Panels PR, PUN, SO – overtypeable field SOWNER.
SDSF	ISFATTR.SELECT.PLIM	Panels LI, NC, PR, SO – overtypeable field PAGE-LIMIT.
SDSF	ISFATTR.SELECT.PLIM	Panel PR – overtypeable field PAGE-LIM-HI.
SDSF	ISFATTR.SELECT.PLIM	Panel PR – overtypeable field PAGE-LIM-LOW.
SDSF	ISFATTR.SELECT.PRMODE	Panels PR, PUN, RDR – overtypeable field SPRMODE1.
SDSF	ISFATTR.SELECT.PRMODE	Panel SO – overtypeable field SPRMODE1.
SDSF	ISFATTR.SELECT.RANGE	Panel PR – overtypeable field SRANGE.
SDSF	ISFATTR.SELECT.RANGE	Panels PUN, SO – overtypeable field SRANGE.
SDSF	ISFATTR.SELECT.SCHENV	Panel SO – overtypeable field SSCHEDULING-ENV.
SDSF	ISFATTR.SELECT.SRVCLS	Panel SO – overtypeable field SSRVCLASS.
SDSF	ISFATTR.SELECT.SYSAFF	Panel SO – overtypeable field SSAFF.
SDSF	ISFATTR.SELECT.UCS	Panels PR, SO – overtypeable field SUCS.
SDSF	ISFATTR.SELECT.VOL	Panel PR – overtypeable field SVOL1.
SDSF	ISFATTR.SELECT.VOL	Panels PUN, SO – overtypeable field SVOL.
SDSF	ISFATTR.SELECT.WRITER	Panels PR, PUN, SO – overtypeable field SWRITER.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFATTR.SPOOL.MINPCT	Panel SP – overtypeable field MINPCT.
SDSF	ISFATTR.SPOOL.OVFNAME	Panel SP – overtypeable field OVERFNAM.
SDSF	ISFATTR.SPOOL.PARTNAME	Panel SP – overtypeable field PARTNAME.
SDSF	ISFATTR.SPOOL.RESERVED	Panel SP – overtypeable field RES.
SDSF	ISFATTR.SPOOL.SYSAFF	Panel SP – overtypeable field SAFF.
SDSF	ISFAUTH.DEST.destname	Operator destinations for command objects and destination names for the DEST command.
SDSF	ISFAUTH.DEST.destname.DATASET.dsname ISFAUTH.DEST.DATASET.dsname	Operator destination to browse objects.
SDSF	ISFCFC.connectionname	CFC connections.
SDSF	ISFCFS.structurename	CFS structures.
SDSF	ISFCMD.DSP.ACTIVE.jesx	DA panel command.
SDSF	ISFCMD.DSP.HELD.jesx	H panel command.
SDSF	ISFCMD.DSP.INPUT.jesx	I panel command.
SDSF	ISFCMD.DSP.JGROUP.jesx	JG panel command.
SDSF	ISFCMD.DSP.OUTPUT.jesx	O panel command.
SDSF	ISFCMD.DSP.SCHENV.system	SE panel command.
SDSF	ISFCMD.DSP.STATUS.jesx	ST panel command.
SDSF	ISFCMD.DSP.SYMBOL.system	SYM panel command.
SDSF	ISFCMD.FILTER.ACTION	ACTION command.
SDSF	ISFCMD.FILTER.DEST	DEST command.
SDSF	ISFCMD.FILTER.FINDLIM	FINDLIM command.
SDSF	ISFCMD.FILTER.INPUT	INPUT command.
SDSF	ISFCMD.FILTER.OWNER	OWNER command.
SDSF	ISFCMD.FILTER.PREFIX	PREFIX command.
SDSF	ISFCMD.FILTER.RSYS	RSYS command.
SDSF	ISFCMD.FILTER.SYSID	SYSID command.
SDSF	ISFCMD.FILTER.SYSNAME	SYSNAME command.
SDSF	ISFCMD.MAINT.ABEND	ABEND command.
SDSF	ISFCMD.MAINT.DIAG	DIAG panel command.
SDSF	ISFCMD.MAINT.TRACE	TRACE command.
SDSF	ISFCMD.ODSP.APF.system	APF panel command.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFCMD.ODSP.AS.system	AS panel command.
SDSF	ISFCMD.ODSP.CDE.system	JC action character.
SDSF	ISFCMD.ODSP.CFMEMBER.system	XCFM panel command.
SDSF	ISFCMD.ODSP.CFSTRUCT.system	CFS panel command.
SDSF	ISFCMD.ODSP.COUPLE.system	CFC panel command.
SDSF	ISFCMD.ODSP.CSR.system	CSR panel command.
SDSF	ISFCMD.ODSP.DEVACT.system	DEV panel command.
SDSF	ISFCMD.ODSP.DEVICE.system	JD action character.
SDSF	ISFCMD.ODSP.DEVICE.system	JDD action character on DA, AS, I, ST, INIT, and NS Panels.
SDSF	ISFCMD.ODSP.DYNX.system	DYNX panel command.
SDSF	ISFCMD.ODSP.EMCS.system	EMCS panel command.
SDSF	ISFCMD.ODSP.ENCLAVE.system	ENC panel command.
SDSF	ISFCMD.ODSP.ENQUEUE.system	ENQ panel command.
SDSF	ISFCMD.ODSP.FILESYS.system	FS panel command.
SDSF	ISFCMD.ODSP.HCHECKER.system	CK panel command.
SDSF	ISFCMD.ODSP.INITIATOR.jesx	INIT panel command.
SDSF	ISFCMD.ODSP.JES.system	JES panel command.
SDSF	ISFCMD.ODSP.JESCKPT.jesname	JC action character (CKPT panel).
SDSF	ISFCMD.ODSP.JOB0.jesx	J0 panel command.
SDSF	ISFCMD.ODSP.JOBCLASS.jesx	JC panel command.
SDSF	ISFCMD.ODSP.LINE.jesx	LI panel command.
SDSF	ISFCMD.ODSP.LNK.system	LNK panel command.
SDSF	ISFCMD.ODSP.LPA.system	LPA panel command.
SDSF	ISFCMD.ODSP.LPD.system	LPD panel command.
SDSF	ISFCMD.ODSP.MAS.jesx	MAS panel command.
SDSF	ISFCMD.ODSP.NC.jesx	NC panel command.
SDSF	ISFCMD.ODSP.NETACT.system	NA panel command.
SDSF	ISFCMD.ODSP.NODE.jesx	NO panel command.
SDSF	ISFCMD.ODSP.NS.jesx	NS panel command.
SDSF	ISFCMD.ODSP.OMVS.system	OMVS panel command.
SDSF	ISFCMD.ODSP.PAGE.system	PAGE panel command.
SDSF	ISFCMD.ODSP.PARMLIB.system	PARM panel command.
SDSF	ISFCMD.ODSP.PRINTER.jesx	PR panel command.
SDSF	ISFCMD.ODSP.PROCESS.system	PS panel command.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFCMD.ODSP.PROCLIB.jesx	PROC panel command.
SDSF	ISFCMD.ODSP.PUNCH.jesx	PUN panel command.
SDSF	ISFCMD.ODSP.READER.jesx	RDR panel command.
SDSF	ISFCMD.ODSP.REPC.system	REPC panel command.
SDSF	ISFCMD.ODSP.RESMON.jesx	RM panel command.
SDSF	ISFCMD.ODSP.RESMON.jesx	RMA panel command.
SDSF	ISFCMD.ODSP.RESOURCE.system	RES panel command.
SDSF	ISFCMD.ODSP.RGRP.system	RGRP panel command.
SDSF	ISFCMD.ODSP.SMSVOL.system	SMSV panel command.
SDSF	ISFCMD.ODSP.SO.jesx	SO panel command.
SDSF	ISFCMD.ODSP.SPOOL.jesx	SP panel command.
SDSF	ISFCMD.ODSP.SR.system	SR panel command.
SDSF	ISFCMD.ODSP.SRVC.system	SRVC panel command.
SDSF	ISFCMD.ODSP.STORAGE.system	JM action character.
SDSF	ISFCMD.ODSP.STORAGE.system	JMO action character.
SDSF	ISFCMD.ODSP.STORGRP.system	SMSG panel command.
SDSF	ISFCMD.ODSP.SYSLOG.jesx	LOG panel command.
SDSF	ISFCMD.ODSP.SYSTEM.system	SYS panel command.
SDSF	ISFCMD.ODSP.TCB.system	JT action character.
SDSF	ISFCMD.ODSP.TRACKER.system	GT panel command.
SDSF	ISFCMD.ODSP.ULOG.jesx	ULOG panel command.
SDSF	ISFCMD.ODSP.VIRTSTOR.system	VMAP panel command.
SDSF	ISFCMD.ODSP.WKLD.system	WKLD panel command.
SDSF	ISFCMD.ODSP.WLM.system	WLM panel command.
SDSF	ISFCMD.OPT.JESNAME	JESNAME parameter on SDSF command.
SDSF	ISFDEV.volser	DEV device activity.
SDSF	ISFDISP.DELAY.owner.jobname	JY action character on the DA panel.
SDSF	ISFDYNX.exitname	DYNX data sets.
SDSF	ISFEMCS.consolename	Extended console.
SDSF	ISFENC.subsys-type.subsys-name	Enclaves.
SDSF	ISFENQ.majorname.sysname	Enqueues.
SDSF	ISFFS.filesystemname	FS file systems.
SDSF	ISFGT.eventowner	GT generic tracking events.
SDSF	ISFINIT.I(xx).jesx	Initiators.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFJDD.CF.sysname	Coupling facility on the JD panel.
SDSF	ISFJDD.IP.sysname	TCP/IP server on the JD panel.
SDSF	ISFJES.subsysname	JES subsystems.
SDSF	ISFJOB.DDNAME.owner.jobname.system	JD action character on the AS, DA, I, INIT, NS and ST panels.
SDSF	ISFJOB.DDNAME.owner.jobname.system	JDD action character on the DA, AS, I, ST, INIT, and NS panels.
SDSF	ISFJOB.STORAGE.owner.jobname.system	JM action character on the AS, DA, I, INIT, NS and ST panels.
SDSF	ISFJOB.STORAGE.owner.jobname.system	JMO action character on the DA and AS panels.
SDSF	ISFJOB.TASK.owner.jobname.system	JT action character.
SDSF	ISFJOBCL.class.jesx	Job class members.
SDSF	ISFJOBCL.class.jesx	Job classes.
SDSF	ISFJRI.resourcenamejesx	JES subsystems.
SDSF	ISFJRJ.jobnamejobid	JES subsystems.
SDSF	ISFLINE.device-name.jesx	Lines.
SDSF	ISFLNK.datasetname	LnkLst data sets.
SDSF	ISFLPA.datasetname	LPA data sets.
SDSF	ISFNETACT.jobname	NA network activity.
SDSF	ISFNODE.node-name.jesx	Nodes.
SDSF	ISFNS.device-name.jesx	Network servers.
SDSF	ISFOMVS.optionname	OMVS options.
SDSF	ISFOPER.ANYDEST.jesx	All destinations for the DEST command.
SDSF	ISFOPER.DEST.jesx	Operator authority.
SDSF	ISFOPER.SYSTEM	Command line commands.
SDSF	ISFPAG.datasetname	Page data sets.
SDSF	ISFPARM.datasetname	Parmlib data sets.
SDSF	ISFPLIB.proc-name	PROC data sets.
SDSF	ISFPROC.owner.jobname	z/OS UNIX processes.
SDSF	ISFRDR.device-name.jesx	Readers.
SDSF	ISFRES.resource.system	WLM resources.
SDSF	ISFRM.resource.jesx	JES resources.
SDSF	ISFRMA.type.jesx	RMA monitor alerts.
SDSF	ISFSE.sched-env.system	Scheduling environments.

Table 20. RACF classes and profiles that protect SDSF functions (continued)		
RACF Class	**RACF Profile**	**What it protects**
SDSF	ISFSMSVOL.filesystemname	SMS storage volumes.
SDSF	ISFSO.device-name.jesx	Offloaders.
SDSF	ISFSP.volser.jesx	Spool volumes.
SDSF	ISFSR.ACTION.system.jobname	C action character.
SDSF	ISFSR.msg-type.system.jobname	System requests, where message-type is ACTION or REPLY.
SDSF	ISFSR.REPLY.system.jobname	AI, R action characters.
SDSF	ISFSTORGRP.storagegroupname	SMSG storage groups.
SDSF	ISFSUBSYS.subsysname	SSI subsystems.
SDSF	ISFSYM.symbolname.sysname	System symbols.
SDSF	ISFSYS.sysplexname.systemname	Systems.
SDSF	ISFXCFM.membername	XCF Groups and Members.
SDSF	SERVER.NOPARM	Fall-back to ISFPARMS in assembler format.
WRITER	jesx.LOCAL.devicename	Local printers and punches, including those on other systems.
WRITER	jesx.RJE.devicename	RJE devices.
XFACILIT	HZS.sysname.checkowner.checkname.action	IBM Health Checker for z/OS.

Appendix D. RACF profiles that protect JES2 commands

RACF class OPERCMDS can be used to protect JES2 operator commands.

RACF class OPERCMDS can be used to protect JES2 operator commands. The following table provides a list of the RACF profiles required and the security risk associated with each JES2 command.

Table 21. RACF profiles and JES2 commands

JES2 Command	Resource Name	Generic Profile	Access Required[1]	Security Risk
$A A	JES2.MODIFYRELEASE.JOB	JES2.MODIFYRELEASE.**	Update	Medium
$A J	JES2.MODIFYRELEASE.BAT	JES2.MODIFYRELEASE.**	Update	Medium
$A 'jobname'	JES2.MODIFYRELEASE.JOB	JES2.MODIFYRELEASE.**	Update	Medium
$A JOBQ	JES2.MODIFYRELEASE.JST	JES2.MODIFYRELEASE.**	Update	Medium
$A Q	JES2.MODIFYRELEASE.JOB	JES2.MODIFYRELEASE.**	Update	Medium
$A S	JES2.MODIFYRELEASE.STC	JES2.MODIFYRELEASE.**	Update	Medium
$A T	JES2.MODIFYRELEASE.TSU	JES2.MODIFYRELEASE.**	Update	Medium
$ADD APPL	JES2.ADD.APPL	JES2.ADD.**	Control	High
$ADD CONNECT	JES2.ADD.CONNECT	JES2.ADD.**	Control	High
$ADD DESTID	JES2.ADD.DESTID	JES2.ADD.**	Control	High
$ADD FSS	JES2.ADD.FSS	JES2.ADD.**	Control	High
$ADD RMT	JES2.ADD.RMT	JES2.ADD.**	Control	High
$B device	JES2.BACKSP.DEV	JES2.BACKSP.**	Update	Medium
$C A[2]	JES2.CANCEL.AUTOCMD	JES2.CANCEL.**	See note 1	Medium
$C device	JES2.CANCEL.DEV	JES2.CANCEL.**	Update	Medium
$C J	JES2.CANCEL.BAT	JES2.CANCEL.BAT.**	Update	Medium
$C 'jobname'	JES2.CANCEL.JOB	JES2.CANCEL.**	Update	Medium
$C JOBQ	JES2.CANCEL.JST	JES2.CANCEL.**	Update	Medium
$C Lx.yy	JES2.CANCEL.DEV	JES2.CANCEL.**	Update	Medium
$C S	JES2.CANCEL.STC	JES2.CANCEL.**	Update	Medium
$C T	JES2.CANCEL.TSU	JES2.CANCEL..TSU.**	Update	Low
$D A	JES2.DISPLAY.JOB	JES2.DISPLAY.**	Read	Low
$D ACTRMT	JES2.DISPLAY.ACTRMT	JES2.DISPLAY.**	Read	Low
$D F	JES2.DISPLAY.QUE	JES2.DISPLAY.**	Read	Low
$D I	JES2.DISPLAY.INITIATOR	JES2.DISPLAY.**	Read	Low
$D init stmt	JES2.DISPLAY.initstmt	JES2.DISPLAY.**	Read	Low
$D J	JES2.DISPLAY.BAT	JES2.DISPLAY.**	Read	Low

Table 21. RACF profiles and JES2 commands (continued)

JES2 Command	Resource Name	Generic Profile	Access Required[1]	Security Risk
$D 'jobname'	JES2.DISPLAY.JOB	JES2.DISPLAY.**	Read	Low
$D JOBQ	JES2.DISPLAY.JST	JES2.DISPLAY.**	Read	Low
$D M	JES2.SEND.MESSAGE	JES2.SEND.**	Read	Low
$D N	JES2.DISPLAY.JOB	JES2.DISPLAY.**	Read	Low
$D PCE	JES2.DISPLAY.PCE	JES2.DISPLAY.**	Read	Low
$D PRT	JES2.DISPLAY.DEV	JES2.DISPLAY.**	Read	Low
$D Q	JES2.DISPLAY.JOB	JES2.DISPLAY.**	Read	Low
$D REBLD	JES2.DISPLAY.REBLD	JES2.DISPLAY.**	Read	Low
$D S	JES2.DISPLAY.STC	JES2.DISPLAY.**	Read	Low
$D SPOOL	JES2.DISPLAY.SPOOL	JES2.DISPLAY.**	Read	Low
$D T	JES2.DISPLAY.TSU	JES2.DISPLAY.**	Read	Low
$D TRACE	JES2.DISPLAY.TRACE	JES2.DISPLAY.**	Read	Low
$D U	JES2.DISPLAY.DEV	JES2.DISPLAY.**	Read	Low
$DEL CONNECT	JES2.DEL.CONNECT	JES2.DEL.**	Control	High
$DEL DESTID	JES2.DEL.DESTID	JES2.DEL.**	Control	High
$E CKPTLOCK,HELDBY=	JES2.RESTART.SYS	JES2.RESTART.**	Control	High
$E device	JES2.RESTART.DEV	JES2.RESTART.**	Update	Medium
$E J	JES2.RESTART.BAT	JES2.RESTART.**	Control	High
$E 'jobname'	JES2.RESTART.BAT	JES2.RESTART.**	Control	High
$E LINE(x)	JES2.RESTART.LINE	JES2.RESTART.**	Control	High
$E LOGON(x)	JES2.RESTART.LOGON	JES2.RESTART.**	Control	High
$E Lx.YYY	JES2.RESTART.DEV	JES2.RESTART.**	Update	Medium
$E MEMBER( )	JES2.RESTART.SYS	JES2.RESTART.**	Control	High
$F device	JES2.FORWARD.DEV	JES2.FORWARD.**	Update	Medium
$G A	JES2.GMODIFYRELEASE.JOB	JES2.G*.**	Update	Medium
$G C	JES2.GCANCEL.JOB	JES2.G*.**	Update	Medium
$G D	JES2.GDISPLAY.JOB	JES2.G*.**	Read	Low
$G H	JES2.GMODIFYHOLD.JOB	JES2.G*.**	Update	Medium
$G R	JES2.GROUTE.JOBOUT	JES2.G*.**	Update	Medium
$H A	JES2.MODIFYHOLD.JOB	JES2.MODIFYHOLD.**	Update	Medium
$H J	JES2.MODIFYHOLD.BAT	JES2.MODIFYHOLD.**	Update	Medium
$H 'jobname'	JES2.MODIFYHOLD.JOB	JES2.MODIFYHOLD.**	Update	Medium

Table 21. RACF profiles and JES2 commands (continued)

JES2 Command	Resource Name	Generic Profile	Access Required[1]	Security Risk
$H JOBQ	JES2.MODIFYHOLD.JST	JES2.MODIFYHOLD.**	Update	Medium
$H Q	JES2.MODIFYHOLD.JOB	JES2.MODIFYHOLD.**	Update	Medium
$H S	JES2.MODIFYHOLD.STC	JES2.MODIFYHOLD.**	Update	Medium
$H T	JES2.MODIFYHOLD.TSU	JES2.MODIFYHOLD.**	Update	Medium
$I device	JES2.INTERRUPT.DEV	JES2.INTERRUPT.**	Update	Medium
$L J	JES2.DISPLAY.BATOUT	JES2.DISPLAY.**	Read	Low
$L 'jobname'	JES2.DISPLAY.JOBOUT	JES2.DISPLAY.**	Read	Low
$L JOBQ	JES2.DISPLAY.JSTOUT	JES2.DISPLAY.**	Read	Low
$L S	JES2.DISPLAY.STCOUT	JES2.DISPLAY.**	Read	Low
$L T	JES2.DISPLAY.TSUOUT	JES2.DISPLAY.**	Read	Low
$M	JES2.MSEND.CMD	JES2.MSEND.**	Read	Low
$N	JES2.NSEND.CMD	JES2.NSEND.**	Read	Low
$N device	JES2.REPEAT.DEV	JES2.REPEAT.**	Update	Medium
$O J	JES2.RELEASE.BATOUT	JES2.RELEASE.**	Update	Medium
$O 'jobname'	JES2.RELEASE.JOBOUT	JES2.RELEASE.**	Update	Medium
$O JOBQ	JES2.RELEASE.JSTOUT	JES2.RELEASE.**	Update	Medium
$O Q	JES2.RELEASE.JOBOUT	JES2.RELEASE.**	Update	Medium
$O S	JES2.RELEASE.STCOUT	JES2.RELEASE.**	Update	Medium
$O T	JES2.RELEASE.TSUOUT	JES2.RELEASE.**	Update	Medium
$P	JES2.STOP.SYS	JES2.STOP.**	Control	High
$P device	JES2.STOP.DEV	JES2.STOP.**	Update	Medium
$P I	JES2.STOP.INITIATOR	JES2.STOP.**	Control	High
$P J	JES2.STOP.BAT	JES2.STOP.**	Update	Medium
$P JES2	JES2.STOP.SYS	JES2.STOP.**	Control	High
$P 'jobname'	JES2.STOP.JOB	JES2.STOP.**	Update	Medium
$P JOBQ	JES2.STOP.JST	JES2.STOP.**	Update	Medium
$P LINE(x)	JES2.STOP.LINE	JES2.STOP.**	Control	High
$P LOGON(x)	JES2.STOP.LOGON	JES2.STOP.**	Control	High
$P Lx.yyy	JES2.STOP.DEV	JES2.STOP.**	Update	Medium
$P Q	JES2.STOP.JOBOUT	JES2.STOP.**	Update	Medium
$P RMT(x)	JES2.STOP.RMT	JES2.STOP.**	Control	High
$P S	JES2.STOP.STC	JES2.STOP.**	Update	Medium
$P SPOOL	JES2.STOP.SPOOL	JES2.STOP.**	Control	High
$P T	JES2.STOP.TSU	JES2.STOP.**	Update	Medium

Table 21. RACF profiles and JES2 commands (continued)

JES2 Command	Resource Name	Generic Profile	Access Required[1]	Security Risk
$P TRACE(x)	JES2.STOP.TRACE	JES2.STOP.**	Control	High
$R ALL	JES2.ROUTE.JOBOUT	JES2.ROUTE.**	Update	Medium
$R PRT	JES2.ROUTE.JOBOUT	JES2.ROUTE.**	Update	Medium
$R PUN	JES2.ROUTE.JOBOUT	JES2.ROUTE.**	Update	Medium
$R XEQ	JES2.ROUTE.JOBOUT	JES2.ROUTE.**	Update	Medium
$S	JES2.START.SYS	JES2.START.**	Control	High
$S A	JES2.START.AUTOCMD	JES2.START.**	Control	High
$S device	JES2.START.DEV	JES2.START.**	Update	Medium
$S I	JES2.START.INITIATOR	JES2.START.**	Control	High
$S LINE(x)	JES2.START.LINE	JES2.START.**	Control	High
$S LOGON(x)	JES2.START.LOGON	JES2.START.**	Control	High
$S Lx.yyy	JES2.START.DEV	JES2.START.**	Update	Medium
$S N	JES2.START.NET	JES2.START.**	Control	High
$S RMT(x)	JES2.START.RMT	JES2.START.**	Control	High
$S SPOOL	JES2.START.SPOOL	JES2.START.**	Control	High
$S TRACE(x)	JES2.START.TRACE	JES2.START.**	Control	High
$T A*,**	JES2.MODIFY.AUTOCMD	JES2.MODIFY.**	See note 1	High
$T ALL	JES2.MODIFY.SYS	JES2.MODIFY.**	Control	High
$T device	JES2.MODIFY.DEV	JES2.MODIFY.**	Update	Medium
$T I	JES2.MODIFY.INITIATOR	JES2.MODIFY.**	Control	High
$T init stmt	JES2.MODIFY.init stmt	JES2.MODIFY.**	Control	High
$T J	JES2.MODIFY.BAT	JES2.MODIFY.**	Update	Medium
$T 'jobname'	JES2.MODIFY.JOB	JES2.MODIFY.**	Update	Medium
$T JOBQ	JES2.MODIFY.JST	JES2.MODIFY.**	Update	Medium
$T LINE	JES2.MODIFY.LINE	JES2.MODIFY.**	Control	High
$T LOGON	JES2.MODIFY.LOGON	JES2.MODIFY.**	Control	High
$T MEMBER(x)	JES2.MODIFY.SYS	JES2.MODIFY.**	Control	High
$T NODE	JES2.MODIFY.NODE	JES2.MODIFY.**	Control	High
$T NUM	JES2.MODIFY.NUM	JES2.MODIFY.**	Control	High
$T O J	JES2.MODIFY.BATOUT	JES2.MODIFY.BATOUT.**	Update	Medium
$T O 'jobname'	JES2.MODIFY.JOBOUT	JES2.MODIFY.**	Update	Medium
$T O JOBQ	JES2.MODIFY.JSTOUT	JES2.MODIFY.**	Update	Medium
$T O S	JES2.MODIFY.STCOUT	JES2.MODIFY.**	Update	Medium
$T O T	JES2.MODIFY.TSUOUT	JES2.MODIFY.TSUOUT.**	Update	Low

Table 21. RACF profiles and JES2 commands (continued)

JES2 Command	Resource Name	Generic Profile	Access Required[1]	Security Risk
$T OFFLOADx	JES2.MODIFY.OFFLOAD	JES2.MODIFY.**	Control	High
$T OFFx.yy	JES2.MODIFY.OFF	JES2.MODIFY.**	Control	High
$T RMT	JES2.MODIFY.RMT	JES2.MODIFY.**	Control	High
$T S	JES2.MODIFY.STC	JES2.MODIFY.**	Update	Medium
$T SSI	JES2.MODIFY.SSI	JES2.MODIFY.**	Control	High
$T T	JES2.MODIFY.TSU	JES2.MODIFY.**	Update	Medium
$VS[3]	JES2.VS	JES2.VS.**	Control	High
$Z A	JES2.HALT.AUTOCMD	JES2.HALT.**	Control	High
$Z device	JES2.HALT.DEV	JES2.HALT.**	Update	Medium
$Z I	JES2.HALT.INITIATOR	JES2.HALT.**	Control	High
$Z SPOOL	JES2.HALT.SPOOL	JES2.HALT.**	Control	High
JES2.UNKNOWN	JES2.UNKNOWN	JES2.UNKNOWN.**	Read	
	All JES2 Commands	JES2.**	Control	

Notes:

1. The command can be issued with different authorities, based on what the command affects and who is issuing the command.
2. When changing or canceling automatic commands, if the user ID issuing the command is not the same as the original user ID, the issuing user ID must have control authority.
3. The $VS command syntax is: $VS,'MVS *command*'. The user ID issuing this command must also have authority to issue the MVS command. For example, a user that issues $VS,'C *jobname*' must have authority to both the JES2 $VS and the MVS CANCEL commands.

Appendix E. RACF profiles that protect MVS commands

RACF class OPERCMDS can be used to protect MVS operator commands.

The following table provides a list of the RACF profiles required and the security risk associated with each MVS command. The assigned risk factor only provides guidance for granting user access to the resource; your installation's requirements might vary.

Table 22. RACF profiles and MVS commands

MVS Command	Resource Name	Generic Profile	Access Required	Risk
<catchall profile>		MVS.**	Control	High
CANCEL jobname	MVS.CANCEL.ATX.jobname	MVS.CANCEL.**	Update	Medium
CANCEL jobname	MVS.CANCEL.JOB.jobname	MVS.CANCEL.**	Update	Medium
CANCEL jobname.id or CANCEL.id	MVS.CANCEL.STC.mbrname.id	MVS.CANCEL.**	Update	Medium
CANCEL U=userid	MVS.CANCEL.TSU.userid	MVS.CANCEL.**	Update	Medium
CONTROL C	MVS.CONTROL.C	MVS.CONTROL.**	Read	Medium
DEVSERV	MVS.DEVSERV	MVS.DEVSERV.**	Read	Medium
D A	MVS.DISPLAY.JOB	MVS.DISPLAY.**	Read	Low
D ALLOC	MVS.DISPLAY.ALLOC	MVS.DISPLAY.**	Read	Low
D AUTOR	MVS.DISPLAY.AUTOR	MVS.DISPLAY.**	Read	Low
D ASM	MVS.DISPLAY.ASM	MVS.DISPLAY.**	Read	Low
D CEE	MVS.DISPLAY.CEE	MVS.DISPLAY.**	Read	Low
D CONSOLES	MVS.DISPLAY.CONSOLES	MVS.DISPLAY.**	Read	Low
D DEVSUP	MVS.DISPLAY.DEVSUP	MVS.DISPLAY.**	Read	Low
D DIAG	MVS.DISPLAY.DIAG	MVS.DISPLAY.**	Read	Low
D DUMP	MVS.DISPLAY.DUMP	MVS.DISPLAY.**	Read	Low
D EMCS	MVS.DISPLAY.EMCS	MVS.DISPLAY.**	Read	Low
D FXE	MVS.DISPLAY.FXE	MVS.DISPLAY.**	Read	Low
D GRS	MVS.DISPLAY.GRS	MVS.DISPLAY.**	Read	Low
D GTZ	MVS.DISPLAY.GTZ	MVS.DISPLAY.**	Read	Low
D ICSF	MVS.DISPLAY.ICSF	MVS.DISPLAY.**	Read	Low
D IEFOPZ	MVS.DISPLAY.IEFPOZ	MVS.DISPLAY.**	Read	Low
D IKJTSO	MVS.DISPLAY.IKJTSO	MVS.DISPLAY.**	Read	Low
D IOS	MVS.DISPLAY.IOS	MVS.DISPLAY.**	Read	Low
D IPLINFO	MVS.DISPLAY.IPLINFO	MVS.DISPLAY.**	Read	Low
D IQP	MVS.DISPLAY.IQP	MVS.DISPLAY.**	Read	Low

Table 22. RACF profiles and MVS commands (continued)

MVS Command	Resource Name	Generic Profile	Access Required	Risk
D IZU	MVS.DISPLAY.IZU	MVS.DISPLAY.**	Read	Low
D JOBS	MVS.DISPLAY.JOB	MVS.DISPLAY.**	Read	Low
D LLA	MVS.DISPLAY.LLA	MVS.DISPLAY.**	Read	Low
D LOGGER	MVS.DISPLAY.LOGGER	MVS.DISPLAY.**	Read	Low
D LOGREC	MVS.DISPLAY.LOGREC	MVS.DISPLAY.**	Read	Low
D M	MVS.DISPLAY.M	MVS.DISPLAY.**	Read	Low
D MPF	MVS.DISPLAY.MPF	MVS.DISPLAY.**	Read	Low
D OMVS	MVS.DISPLAY.OMVS	MVS.DISPLAY.**	Read	Low
D OPDATA	MVS.DISPLAY.OPDATA	MVS.DISPLAY.**	Read	Low
D PARMLIB	MVS.DISPLAY.PARMLIB	MVS.DISPLAY.**	Read	Low
D PCIE	MVS.DISPLAY.PCIE	MVS.DISPLAY.**	Read	Low
D PPT	MVS.DISPLAY.PPT	MVS.DISPLAY.**	Read	Low
D PROD	MVS.DISPLAY.PROD	MVS.DISPLAY.**	Read	Low
D PROG	MVS.DISPLAY.PROG	MVS.DISPLAY.**	Read	Low
D R	MVS.DISPLAY.R	MVS.DISPLAY.**	Read	Low
D SLIP	MVS.DISPLAY.SLIP	MVS.DISPLAY.**	Read	Low
D SMF	MVS.DISPLAY.SMF	MVS.DISPLAY.**	Read	Low
D SMFLIM	MVS.DISPLAY.SMFLIM	MVS.DISPLAY.**	Read	Low
D SMS	MVS.DISPLAY.SMS	MVS.DISPLAY.**	Read	Low
D SSI	MVS.DISPLAY.SSI	MVS.DISPLAY.**	Read	Low
D SYMBOLS	MVS.DISPLAY.SYMBOLS	MVS.DISPLAY.**	Read	Low
D TCPIP	MVS.DISPLAY.TCPIP	MVS.DISPLAY.**	Read	Low
D TIMEDATE	MVS.DISPLAY.TIMEDATE	MVS.DISPLAY.**	Read	Low
D TRACE	MVS.DISPLAY.TRACE	MVS.DISPLAY.**	Read	Low
D U	MVS.DISPLAY.U	MVS.DISPLAY.**	Read	Low
D UNI	MVS.DISPLAY.UNI	MVS.DISPLAY.**	Read	Low
D VIRSTOR	MVS.DISPLAY.VIRSTOR	MVS.DISPLAY.**	Read	Low
D WLM	MVS.DISPLAY.WLM	MVS.DISPLAY.**	Read	Low
D XCF	MVS.DISPLAY.XCF	MVS.DISPLAY.**	Read	Low
FORCE jobname	MVS.FORCE.JOB.jobname	MVS.FORCE*.**	Control	High
FORCE jobname.id or FORCE id	MVS.FORCE.STC.mbrname.id	MVS.FORCE*.**	Control	High
FORCE jobname	MVS.FORCE.STC.mbrname.jobname	MVS.FORCE*.**	Control	High

Table 22. RACF profiles and MVS commands (continued)

MVS Command	Resource Name	Generic Profile	Access Required	Risk
FORCE U=userid	MVS.FORCE.TSU.userid	MVS.FORCE*.**	Control	High
FORCE jobname,ARM	MVS.FORCEARM.JOB.jobname	MVS.FORCE*.**	Control	High
FORCE [jobname.]identifier, ARM	MVS.FORCEARM.STC.mbrname.id	MVS.FORCE*.**	Control	High
FORCE U=userid,ARM	MVS.FORCEARM.TSU.userid	MVS.FORCE*.**	Control	High
Console activation	MVS.MCSOPER.consolid	MVS.MCSOPER.**	Read	Low
F jobname	MVS.MODIFY.JOB.jobname	MVS.MODIFY.**	Update	Medium
F jobname | jobname.id | id	MVS.MODIFY.STC.mbrname.id	MVS.MODIFY.**	Update	Medium
F jobname	MVS.MODIFY.STC.mbrname. jobname	MVS.MODIFY.**	Update	Medium
REPLY	MVS.REPLY	MVS.REPLY.**	Read	Medium
RESET	MVS.RESET	MVS.RESET.**	Update	Medium
RESET CN	MVS.RESET.CN	MVS.RESET.**	Control	High
ROUTE system	MVS.ROUTE.CMD.system	MVS.ROUTE.**	Read	Medium
ROUTE *ALL	MVS.ROUTE.CMD.ALLSYSTEMS	MVS.ROUTE.**	Read	Medium
ROUTE *OTHER	MVS.ROUTE.CMD.OTHERSYSTEMS	MVS.ROUTE.**	Read	Medium
ROUTE sysgrpname	MVS.ROUTE.CMD.sysgrpname	MVS.ROUTE.**	Read	Medium
ROUTE (sysl,...,sysN)	MVS.ROUTE.CMD.sysl	MVS.ROUTE.**	Read	Medium
ROUTE (group1,...,groupN)	MVS.ROUTE.CMD.group1	MVS.ROUTE.**	Read	Medium
SET PROG	MVS.SET.PROG	MVS.SET*.**	Update	Medium
SETAUTOR	MVS.SETAUTOR	MVS.SET*.**	Update	Medium
SETCON	MVS.SETCON	MVS.SET*.**	Update	Medium
SETOMVS	MVS.SETOMVS	MVS.SET*.**	Update	Medium
SETSSI ADD	MVS.SETSSI.ADD.subname	MVS.SET*.**	Control	High
SETSSI ACTIVATE	MVS.SETSSI.ACTIVATE.subname	MVS.SET*.**	Control	High
SETSSI DEACTIVATE	MVS.SETSSI.DEACTIVATE.subnam e	MVS.SET*.**	Control	High
STOP jobname	MVS.STOP.JOB.jobname	MVS.STOP.**	Update	Medium
STOP jobname.id	MVS.STOP.STC.mbrname.id	MVS.STOP.**	Update	Medium
STOP id	MVS.STOP.STC.mbrname.id	MVS.STOP.**	Update	Medium
VARY CN	MVS.VARY.CN	MVS.VARY.**	Update	Medium

Table 22. RACF profiles and MVS commands (continued)

MVS Command	Resource Name	Generic Profile	Access Required	Risk
VARY CN,ACTIVATE	MVS.VARY.CN	MVS.VARY.**	Read	Medium
VARY CN,AUTH	MVS.VARYAUTH.CN	MVS.VARY.**	Control	High
VARY CN,DEACTIVATE	MVS.VARY.CN	MVS.VARY.**	Update	Medium
VARY OFFLINE	MVS.VARY.DEV	MVS.VARY.**	Update	Medium
VARY OFFLINE,FORCE	MVS.VARYFORCE.DEV	MVS.VARY.**	Control	High
VARY ONLINE	MVS.VARY.DEV	MVS.VARY.**	Update	Medium
VARY SMS	MVS.VARY.SMS	MVS.VARY.**	Update	Medium
VARY XCF	MVS.VARY.XCF	MVS.VARY.**	Control	High

Appendix F. ISFPARMS security migration to RACF checklist

Refer to the following checklist to help completed the migration process for SDSF security from ISFPARMS to RACF

Table 23. Security migration checklist

Task	Section	Check
Preparation		
Document current status	Chapter 3, “Analyzing your current SDSF environment,” on page 11	
User ID access requirements	“User ID access requirements” on page 17	
Setup migration utility ISFACR	“Setting up the security migration utility ISFACR” on page 20	
Migration tasks		
Establish RACF group tree structure	“Architecting a RACF group structure” on page 23	
Define ISFACR parameters	“Establishing ISFACR parameters” on page 21	
Migrate ISFPARMS to RACF security	“Using the ISFACR security migration utility” on page 24	
Define profile	“Step 1: Define the profile” on page 26	
Convert ISFPARMS to profile descriptions	“Step 2: Convert ISFPARMS to profile descriptions” on page 27	
Review profile descriptions	“Step 3: Review profile descriptions” on page 28	
Convert descriptions to RACF commands	“Step 4: Convert descriptions to RACF commands” on page 30	
Review RACF commands	“Step 5: Review RACF commands” on page 31	
Activate RACF classes	“Activating the RACF classes” on page 32	
Testing Plan		
Build a testing plan	“Building a testing plan” on page 37	
Implementation		
Implementation steps	Chapter 7, “Implementation,” on page 43	
Test implementation	Chapter 6, “Testing the RACF implementation before migration,” on page 37	

Appendix G. Default member ISFPRM00

The default IBM provided ISFPRM00 member has been used throughout this technical manual as the ISFPARMS member used for the SDSF security migration to RACF. This member can be found in ISF.SISFJCL(ISFPRM00) in your mainframe system. A copy is also presented here.

```
/*********************************************************************/
/*                                                                   */
/*              Sample SDSF Initialization Statements                */
/*                                                                   */
/*                                                                   */
/*  Proprietary Statement =                                          */
/*                                                                   */
/*    Licensed Materials - Property of IBM                           */
/*    5650-ZOS                                                       */
/*    Copyright IBM Corp. 1981, 2019.                                */
/*    Copyright Rocket Software, Inc. 2015, 2019.                    */
/*                                                                   */
/*    Status = HQX77C0                                               */
/*                                                                   */
/*  EXTERNAL CLASSIFICATION = OTHER                                  */
/*  END OF EXTERNAL CLASSIFICATION:                                  */
/*                                                                   */
/*                                                                   */
/*  This is a sample SDSF parameter definition.  It is equivalent    */
/*  to the macros supplied in ISFPARMS.                              */
/*                                                                   */
/*  To use this member, copy it to SYS1.PARMLIB or a dataset         */
/*  concatenated to it and edit the member as appropriate.           */
/*  Alternatively, you can modify the SDSF server JCL to point       */
/*  to a data set that contains the member.                          */
/*                                                                   */
/*  Note that, even with conditional processing, if you want         */
/*  to use a common member with different levels of SDSF, you        */
/*  must ensure that the member does not include support (such       */
/*  as new keywords or values) that was introduced in a              */
/*  higher level of SDSF.                                            */
/*                                                                   */
/*  The SDSF server must be started for the member to be used.       */
/*  If the SDSF server is not active, the macros in ISFPARMS         */
/*  are used instead.                                                */
/*                                                                   */
/*  The following are general syntax rules for coding the SDSF       */
/*  initialization statements.  Refer to the SDSF Operation and      */
/*  Customization manual for more details.                           */
/*                                                                   */
/*    - Statements are free form, and can appear in any column 1-71. */
/*      An optional sequence number may be coded in columns 73-80,   */
/*      but it is not used by SDSF.                                  */
/*                                                                   */
/*    - A statement can span any number of lines.  Use a trailing    */
/*      comma to indicate that a statement is continued.             */
/*                                                                   */
/*    - Comments can be coded at any point a blank is allowed using  */
/*      the slash-asterisk notation.  Blank lines can be inserted    */
/*      at any point to improve readability.                         */
/*                                                                   */
/*    - All values are translated to upper case.  Enclose the value  */
/*      in quotes if it contains special characters or contains      */
/*      mixed case.                                                  */
/*                                                                   */
/*    - Statements may appear in any order, except that the FLDENT   */
/*      must follow an FLD, and the NTBLENT must follow an NTBL.     */
/*      SERVER statements must follow a SERVERGROUP.                 */
/*                                                                   */
/*    - A keyword value of blanks may be specified by coding one     */
/*      or more blanks enclosed in quotes for the value.             */
/*                                                                   */
/*********************************************************************/

    /*************************************************/
    /* WHEN Statement - Provide Conditional Processing */
    /*************************************************/

 WHEN                        /* Reset any prior WHEN conditions      */
```

```
 /*****************************************************************/
 /* Note: The following statements are commented out to show the    */
 /*       syntax.  The statements are only needed when the sysplex  */
 /*       support is to be used.                                    */
/*                                                                 */
 /*       Refer to the Operation and Customization Guide for the    */
 /*       complete set of options that may be specified.            */
 /*****************************************************************/

    /*********************************************************/
    /* SERVERGROUP, SERVER, and COMM - Define Communications */
    /*********************************************************/

 /* SERVERGROUP */               /* Defines a group of SDSF servers */

 /*****************************************************************/
 /*   Each SERVER statement defines an SDSF server in the sysplex.   */
 /*   The server in turn relates to a specific JES2 member for which */
 /*   data is to be gathered.  Repeat the SERVER and COMM statements */
 /*   as many times as necessary to define all the JES2 members for  */
 /*   which data is to be shown.                                     */
 /*                                                                  */
 /*   Note: All servers must be in the same sysplex and all JES2     */
/*   members must be in the same MAS.                               */
 /*****************************************************************/


 /*   SERVER NAME(sdsf-servername),    /* Names the SDSF server      */
 /*          SYSNAME(system-name),     /* System name for server     */
 /*          JESNAME(jes2-subsystem-name),  /* JES2 procedure name   */
 /*          MEMBER(jes2-member-name), /* JES2 member name           */
 /*          COMM(comm-statement-name) /* Related COMM statement     */

 /*   COMM NAME(statement-name),    /* Defines communications parms  */
 /*        QMGR(qmgr-name)             /* QMgr name for connections  */
 /*        CLUSTER(clustername),       /* Cluster name for queues    */
 /*        QREPLACE(YES),              /* Replace prior queue defs   */
 /*        QDELETE(NO),                /* Do not delete queues       */
 /*        QDEFINE(YES)                /* Define required queues     */


    /*******************************/
    /* CONNECT - Connection Options */
    /*******************************/
 CONNECT DEFAULT(COND),/* Default server if not already assigned    */
                     /* DEFAULT(NO) to not assign server as default */
                       /* DEFAULT(YES) to unconditionally assign    */
                       /*   server as default                       */
         XCFSRVNM(SAME)  /* Use server name as XCF appl name       */

    /*****************************************/
    /* OPTIONS Statement - Global SDSF Options */
    /*****************************************/

 OPTIONS DCHAR('?'),         /* Command query character             */
   DSI(NO),                  /* Bypass ENQ for dynamic allocation   */
   FINDLIM(5000),            /* Maximum lines to search for FIND    */
   LINECNT(55),              /* Print lines per page                */
   LOGLIM(0),                /* OPERLOG search limit in hours       */
   MENUS(ISF.SISFPLIB),      /* Panels dataset name for TSO         */
   SCHARS('*%'),             /* Generic and placeholder characters  */
   SCRSIZE(1920),            /* Maximum screen size                 */
   SYSOUT(A),                /* Default print sysout class          */
   TIMEOUT(5),               /* Communications timeout in seconds   */
   TRACE(C000),              /* Default trace mask                  */
   TRCLASS(A),               /* Default trace sysout class          */
   UNALLOC(NO)               /* Do not free dynalloc data sets      */



    /*************************************/
    /* GROUP ISFSPROG - System Programmers */
    /*************************************/

 GROUP NAME(ISFSPROG),       /* Group name                          */
   TSOAUTH(JCL,OPER,ACCT),   /* User must have JCL, OPER, ACCT      */
   ACTION(ALL),              /* All route codes displayed           */
   ACTIONBAR(YES),           /* Display the action bar on panels    */
   APPC(ON),                 /* Include APPC sysout                 */
   AUPDT(2),                 /* Minimum auto update interval        */
```

```
  AUTH(ALL),               /* All authorized functions            */
  BROWSE(NONE),            /* Browse default action character     */
  CMDAUTH(ALL),            /* Commands allowed for all jobs       */
  CMDLEV(7),               /* Authorized command level            */
  CONFIRM(ON),             /* Enable cancel confirmation          */
  CPUFMT(LONG),            /* Long format CPU utilization on DA   */
  CTITLE(ASIS),            /* Allow mixed case column titles      */
  CURSOR(ON),              /* Leave cursor on last row processed  */
/*CUSTOM(SPRGPROP),*/      /* Uncomment for custom properties     */
  DADFLT(IN,OUT,TRANS,STC,TSU,JOB), /* Default rows shown on DA    */
  DATE(MMDDYYYY),          /* Default date format                 */
  DATESEP('/'),            /* Default datesep format              */
  DFIELD2(DAFLD2),         /* Sample alternate field list for DA  */
  DISPLAY(OFF),            /* Do not display current values       */
  DSPAUTH(ALL),            /* Browse allowed for all jobs         */
  EMCSAUTH(MASTER),        /* Activate EMCS cons with master auth */
  EMCSREQ(NO),             /* EMCS console not required           */
  GPLEN(2),                /* Group prefix length                 */
  ILOGCOL(1),              /* Initial display column in log       */
  INPUT(OFF),              /* Initial value for INPUT command     */
  ISYS(LOCAL),             /* Initial system default              */
  LOG(OPERACT),            /* Default log option                  */
  OWNER(NONE),             /* Default owner                       */
  RSYS(NONE),              /* Initial system default for wtors    */
  UPCTAB(TRTAB2),          /* Upper case translate table name     */
  VALTAB(TRTAB),           /* Valid character translate table     */
  VIO(SYSALLDA)            /* Unit name for page mode output      */


   /*****************************/
   /* GROUP ISFOPER - Operators */
   /*****************************/
GROUP NAME(ISFOPER),       /* Group name                          */
  TSOAUTH(JCL,OPER),       /* User must have JCL and OPER         */
  ACTION(ALL),             /* All route codes displayed           */
  ACTIONBAR(YES),          /* Display action bar on panels        */
  APPC(ON),                /* Include APPC sysout                 */
  AUPDT(2),                /* Minimum auto update interval        */
  AUTH(ALLOPER),           /* All operator authorized functions   */
  BROWSE(NONE),            /* Browse default action character     */
  CMDAUTH(ALL),            /* Commands allowed for all jobs       */
  CMDLEV(7),               /* Authorized command level            */
  CONFIRM(ON),             /* Enable cancel confirmation          */
  CPUFMT(LONG),            /* Long format CPU utilization on DA   */
  CTITLE(ASIS),            /* Allow mixed case column titles      */
  CURSOR(ON),              /* Leave cursor on last row processed  */
/*CUSTOM(OPERPROP),*/      /* Uncomment for custom properties     */
  DADFLT(IN,OUT,TRANS,STC,TSU,JOB), /* Default rows shown on DA    */
  DATE(MMDDYYYY),          /* Default date format                 */
  DATESEP('/'),            /* Default datesep format              */
  DISPLAY(OFF),            /* Do not display current values       */
  DSPAUTH(USERID,NOTIFY,AMSG), /* Browse authority                    */
  EMCSAUTH(MASTER),        /* Activate EMCS cons with master auth */
  EMCSREQ(NO),             /* EMCS console not required           */
  GPLEN(2),                /* Group prefix length                 */
  ILOGCOL(1),              /* Initial display column in log       */
  ISYS(LOCAL),             /* Initial system default              */
  LOG(OPERACT),            /* Default log option                  */
  OWNER(NONE),             /* Default owner                       */
  RSYS(NONE),              /* Initial system default for wtors    */
  UPCTAB(TRTAB2),          /* Upper case translate table name     */
  VALTAB(TRTAB),           /* Valid character translate table     */
  VIO(SYSALLDA)            /* Unit name for page mode output      */


   /*********************************/
   /* GROUP ISFUSER - General Users */
   /*********************************/
GROUP NAME(ISFUSER),       /* Group name                          */
  TSOAUTH(JCL),            /* User must have JCL                  */
  ACTION(11,12,USER),      /* Default route codes in log          */
  ACTIONBAR(YES),          /* Display action bar on panels        */
  APPC(ON),                /* Include APPC sysout                 */
  AUPDT(10),               /* Default auto update interval        */
  AUTH(ALLUSER),           /* All user authorized functions       */
  BROWSE(NONE),            /* Browse default action character     */
  CMDAUTH(USERID,NOTIFY),  /* Command authority                   */
  CMDLEV(2),               /* Command level                       */
  CONFIRM(ON),             /* Enable cancel confirmation          */
  CPUFMT(LONG),            /* Long format CPU utilization on DA   */
  CTITLE(ASIS),            /* Allow mixed case column titles      */
/*CUSTOM(USERPROP),*/      /* Uncomment for custom properties     */
```

```
  CURSOR(ON),               /* Leave cursor on last row processed  */
  DADFLT(IN,OUT,TRANS,STC,TSU,JOB), /* Default rows on DA          */
  DATE(MMDDYYYY),           /* Default date format                 */
  DATESEP('/'),             /* Default datesep format              */
  DISPLAY(OFF),             /* Do not display current values       */
  DSPAUTH(USERID,NOTIFY),   /* Browse authority                    */
  EMCSAUTH(MASTER),         /* Activate EMCS cons with master auth */
  EMCSREQ(NO),              /* EMCS console not required           */
  ILOGCOL(1),               /* Initial display column in log       */
  LOG(OPERACT),             /* Default log option                  */
  OWNER(USERID),            /* Default owner                       */
  PREFIX(USERID),           /* Default prefix                      */
  UPCTAB(TRTAB2),           /* Upper case translate table name     */
  VALTAB(TRTAB),            /* Valid character translate table     */
  VIO(SYSALLDA)             /* Unit name for page mode output      */


   /*******************/
   /* Sample NTBL list */
   /*******************/
NTBL NAME(SLIST)
  NTBLENT STRING($S),OFFSET(1)
  NTBLENT STRING(P),OFFSET(7)
  NTBLENT STRING(PAY),OFFSET(3)


   /*******************************/
   /* Define default SDSF Codepage */
   /*******************************/
TRTAB CODPAG(SDSF) VALTAB(TRTAB) UPCTAB(TRTAB2)


   /*********************************************/
   /* Sample alternate field list for DA display */
   /*********************************************/
FLD NAME(DAFLD2) TYPE(DA)  /* Name referenced by GROUP statement */

  FLDENT COLUMN(STEPN),TITLE('StepName'),WIDTH(D)
  FLDENT COLUMN(PROCS),TITLE('ProcStep'),WIDTH(D)
  FLDENT COLUMN(JOBID),TITLE('JobID'),WIDTH(D)
  FLDENT COLUMN(OWNERID),TITLE('Owner'),WIDTH(D)
  FLDENT COLUMN(JCLASS),TITLE('C'),WIDTH(D)
  FLDENT COLUMN(ASID),TITLE('ASID'),WIDTH(D)
  FLDENT COLUMN(ASIDX),TITLE('ASIDX'),WIDTH(D)
  FLDENT COLUMN(EXCP),TITLE(' EXCP-Cnt'),WIDTH(D)
  FLDENT COLUMN(CPU),TITLE('  CPU-Time'),WIDTH(D)
  FLDENT COLUMN(REAL),TITLE('Real'),WIDTH(D)
  FLDENT COLUMN(PAGING),TITLE('Paging'),WIDTH(D)
  FLDENT COLUMN(EXCPRT),TITLE('   SIO'),WIDTH(D)
  FLDENT COLUMN(CPUPR),TITLE('  CPU%'),WIDTH(D)
  FLDENT COLUMN(DP),TITLE('DP'),WIDTH(D)
  FLDENT COLUMN(POS),TITLE('Pos'),WIDTH(D)
  FLDENT COLUMN(SWAPR),TITLE('SR'),WIDTH(D)
  FLDENT COLUMN(PGN),TITLE('PGN'),WIDTH(D)
  FLDENT COLUMN(DOMAIN),TITLE('DmN'),WIDTH(D)
  FLDENT COLUMN(STATUS),TITLE('Status'),WIDTH(D)
  FLDENT COLUMN(WORKLOAD),TITLE('Workload'),WIDTH(D)
  FLDENT COLUMN(SRVCLASS),TITLE('SrvClass'),WIDTH(D)
  FLDENT COLUMN(PERIOD),TITLE('SP'),WIDTH(D)
  FLDENT COLUMN(RESGROUP),TITLE('ResGroup'),WIDTH(D)
  FLDENT COLUMN(SERVER),TITLE('Server'),WIDTH(D)
  FLDENT COLUMN(QUIESCE),TITLE('Quiesce'),WIDTH(D)
  FLDENT COLUMN(SYSNAME),TITLE('SysName'),WIDTH(D)
  FLDENT COLUMN(SPAGING),TITLE('SPag'),WIDTH(D)
  FLDENT COLUMN(SCPU),TITLE('SCPU%'),WIDTH(D)
  FLDENT COLUMN(ECPU),TITLE(' ECPU-Time'),WIDTH(D)
  FLDENT COLUMN(ECPUPR),TITLE(' ECPU%'),WIDTH(D)
  FLDENT COLUMN(CPUCRIT),TITLE('CPUCrit'),WIDTH(D)
  FLDENT COLUMN(STORCRIT),TITLE('StorCrit'),WIDTH(D)
  FLDENT COLUMN(RPTCLASS),TITLE('RptClass'),WIDTH(D)
  FLDENT COLUMN(MEMLIMIT),TITLE('MemLimit'),WIDTH(D)
  FLDENT COLUMN(TRANACT),TITLE('Tran-Act'),WIDTH(D)
  FLDENT COLUMN(TRANRES),TITLE('Tran-Res'),WIDTH(D)
  FLDENT COLUMN(SPIN),TITLE('Spin'),WIDTH(D)
  FLDENT COLUMN(SECLABEL),TITLE('SecLabel'),WIDTH(D)
  FLDENT COLUMN(GCPTIME),TITLE('GCP-Time'),WIDTH(D)
  FLDENT COLUMN(ZAAPTIME),TITLE('zAAP-Time'),WIDTH(D)
  FLDENT COLUMN(ZAAPCPTM),TITLE('zACP-Time'),WIDTH(D)
  FLDENT COLUMN(GCPUSE),TITLE('GCP-Use%'),WIDTH(D)
  FLDENT COLUMN(ZAAPUSE),TITLE('zAAP-Use%'),WIDTH(D)
  FLDENT COLUMN(SZAAP),TITLE('SzAAP%'),WIDTH(D)
  FLDENT COLUMN(SZIIP),TITLE('SzIIP%'),WIDTH(D)
```

```
   FLDENT COLUMN(PROMOTED),TITLE('Promoted'),WIDTH(D)
   FLDENT COLUMN(ZIIPTIME),TITLE('zIIP-Time'),WIDTH(D)
   FLDENT COLUMN(ZIIPCPTM),TITLE('zICP-Time'),WIDTH(D)
   FLDENT COLUMN(ZIIPNTIM),TITLE('zIIP-NTime'),WIDTH(D)
   FLDENT COLUMN(ZIIPUSE),TITLE('zIIP-Use%'),WIDTH(D)
   FLDENT COLUMN(SLCPU),TITLE('SLCPU%'),WIDTH(D)
   FLDENT COLUMN(JTYPE),TITLE('Type'),WIDTH(D)
   FLDENT COLUMN(ZAAPNTIM),TITLE('zAAP-NTime'),WIDTH(D)
   FLDENT COLUMN(IOPRIOGRP),TITLE('IOPrioGrp'),WIDTH(D)
   FLDENT COLUMN(JOBCORR),TITLE('JobCorrelator'),WIDTH(D)
   FLDENT COLUMN(TRESGROUP),TITLE('TenantResGroup'),WIDTH(D)
   FLDENT COLUMN(ESRB),TITLE('ESRB-Time'),WIDTH(D)
   FLDENT COLUMN(CPULIMIT),TITLE('CPU-Limit'),WIDTH(D)
   FLDENT COLUMN(REUS),TITLE('Reus'),WIDTH(D)
   FLDENT COLUMN(SYSLEVEL),TITLE('SysLevel'),WIDTH(D)
   FLDENT COLUMN(ISFEND)

     /*********************/
     /* Custom Properties */
     /*********************/

 /* The custom properties are defined using a PROPLIST statement */
 /* which is referenced by the CUSTOM keyword on the GROUP.  For */
 /* each PROPLIST, define the PROPERTY statements for the custom */
 /* properties that are required.  See the SDSF Operation and    */
 /* Customization manual for the complete list of properties     */
/* that may be specified.                                       */

 /* PROPLIST NAME(SPRGPROP)          Group ISFSPROG properties */
   /* PROPERTY NAME(property-name),VALUE(TRUE or FALSE) */

 /* PROPLIST NAME(OPERPROP)          Group ISFOPER properties  */
   /* PROPERTY NAME(property-name),VALUE(TRUE or FALSE) */

 /* PROPLIST NAME(USERPROP)          Group ISFUSER properties  */
   /* PROPERTY NAME(property-name),VALUE(TRUE or FALSE) */
```

Appendix H. Accessibility

Accessible publications for this product are offered through IBM Documentation (www.ibm.com/docs/en/zos).

If you experience difficulty with the accessibility of any z/OS information, send a detailed message to the Contact the z/OS team web page (www.ibm.com/systems/campaignmail/z/zos/contact_z) or use the following mailing address.

IBM Corporation
Attention: MHVRCFS Reader Comments
Department H6MA, Building 707
2455 South Road
Poughkeepsie, NY 12601-5400
United States

Notices

This information was developed for products and services that are offered in the USA or elsewhere.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

This information could include missing, incorrect, or broken hyperlinks. Hyperlinks are maintained in only the HTML plug-in output for IBM Documentation. Use of hyperlinks in other output formats of this information is at your own risk.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Site Counsel
2455 South Road

Poughkeepsie, NY 12601-5400
USA

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or

reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user, or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's name, email address, phone number, or other personally identifiable information for purposes of enhanced user usability and single sign-on configuration. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at ibm.com®/privacy and IBM's Online Privacy Statement at ibm.com/privacy/details in the section entitled "Cookies, Web Beacons and Other Technologies," and the "IBM Software Products and Software-as-a-Service Privacy Statement" at ibm.com/software/info/product-privacy.

Policy for unsupported hardware

Various z/OS elements, such as DFSMSdfp, JES2, JES3, and MVS, contain code that supports specific hardware servers or devices. In some cases, this device-related element support remains in the product even after the hardware devices pass their announced End of Service date. z/OS may continue to service element code; however, it will not provide service related to unsupported hardware devices. Software problems related to these devices will not be accepted for service, and current service activity will cease if a problem is determined to be associated with out-of-support devices. In such cases, fixes will not be issued.

Minimum supported hardware

The minimum supported hardware for z/OS releases identified in z/OS announcements can subsequently change when service for particular servers or devices is withdrawn. Likewise, the levels of other software products supported on a particular release of z/OS are subject to the service support lifecycle of those

products. Therefore, z/OS and its product publications (for example, panels, samples, messages, and product documentation) can include references to hardware and software that is no longer supported.

- For information about software support lifecycle, see: IBM Lifecycle Support for z/OS (www.ibm.com/software/support/systemsz/lifecycle)
- For information about currently-supported IBM hardware, contact your IBM representative.

Index

Product Number: 5650-ZOS

SC27-4942-50