SDSF Security – How it works on z/OS 2.5 and what has changed

Rob Scott

Rocket Software

rscott@rs.com

Agenda

- SAF Security Migration
- Security Fundamentals
  - SDSF and SDSFAUX server requirements
  - Connecting to SDSF
- Using SDSF Panels
  - Accessing panels
  - Actions and overtypes
- Advanced Functions
  - Controlling the scope of data
  - Destination operator authority
  - Foreign address space data access
  - Issuing operator commands
- Using SDSF to Understand SDSF Security

SAF Security Migration

Security Migration Implications

- SAF security required starting from z/OS 2.5
    - SDSF Security Migration Guide (SC27-4942)
    - SDSF Operation And Customization (SA23-2274)
- z/OS security planning if currently using non-SAF SDSF security
    - Plan to activate JESSPOOL class
        - Protects JES spool data from both inside and outside SDSF
        - Share session 2665 "JES2 RACF Calls, Control Points and Profiles" (2007)
        - Share session 19490 "Security in JES Best Practices" (2016)
    - Plan to activate OPERCMDS class
        - Protects ability to issue z/OS operator commands from both inside and outside SDSF
    - Activating JESSPOOL and OPERCMDS can be performed in advance of any SDSF security migration
        - Do not underestimate the amount of testing required to implement JESSPOOL successfully
        - Dynamically switching to WARNING mode for JESSPOOL class can aid during the migration effort
            - Check with Broadcom for equivalent functionality for ACF/2 and TSS
        - OPERCMDS and JESSPOOL profiles will affect other software products and z/OS components
            - Automated operations and output archiving products

SDSF Security Migration

- Assess current settings from ISFPARMS and ISFPRMxx
  - ISFPARMS is load module assembled from legacy SDSF macros to define options and security settings. Functionally stabilized for decades.
  - ISFPRMxx is PARMLIB statements read by SDSF server to define options and security settings
  - ISFPARMS can be convered to ISFPRMxx using REXX exec "ISFACP"
  - Review any ISFUSER exit logic and attempt to remove the exit if at all possible

- Understand current SDSF user population
  - Sysprogs, operators and end users
  - Move away from classification by TSO logonproc, terminal name and userid and try to use grouping methods via your ESM instead
    - RACF Groups or equivalent functionality in ACF/2 and TSS

- Security migration utility – "ISFACR"
  - ISPF dialog that takes ISFPRMxx statements and attempts to supply sample RACF commands to define SDSF security profiles
  - Not perfect and will require extensive testing and review
  - Sample JCL provided in SISFJCL to analyze SMF data for SDSF SAF security usage
  - Will require several iterations on test systems to fine tune the new profiles and settings

SDSF Security Migration

- After migration to SAF the following keywords in SDSF GROUP in ISFPRMxx are not required :
  - AUTH   ILPROC
  - CMDAUTH   XLPROC
  - CMDLEV   ITNAME
  - DSPAUTH   XTNAME
  - GPLEN   IUID
  - ISYS   XUID
  - TSOAUTH

- Non-SAF keywords will be parsed but will not affect security decisions
  - Parsed values are still presented to ISFUSER for compatability

- Whole migration process is described in detail in the new "SDSF Security Migration Guide"

Security Fundamentals

SDSF Security SAF Classes

- SAF class SDSF used to protect SDSF resources and product functionality
  - Ability to display certain panels
  - Ability to take actions against objects shown on panels
- SDSF will perform SAF checks for other classes such as JESSPOOL and OPERCMDS
  - SDSF does not own the resources for these classes and the authority check is performed by SDSF to improve the messages and/or displays presented to the user
  - If SAF authority is granted within SDSF code, the request is forwarded to the owning component (eg z/OS BCP or JES2) and they will perform their own SAF checks

SDSF and SDSFAUX Server Requirements

- SDSF server mandatory from z/OS 2.5
  - Security checks performed by SDSF server on behalf of user
  - Unless installing maintenance, there is no need to restart SDSF server after IPL
- SDSFAUX required for data collection and sysplex communication
- Entries required in the STARTED class for each server address space
  - OMVS segment required for SDSFAUX userid
    - If not present, data for z/OS unix resources (eg "FS") panel will be incomplete
- SDSFAUX userid requires
  - READ access to FACILITY class resource MVSADMIN.WLM.POLICY for WLM data
  - READ access to FACILITY class resource ERBSDS.MON2DATA for RMF DA data
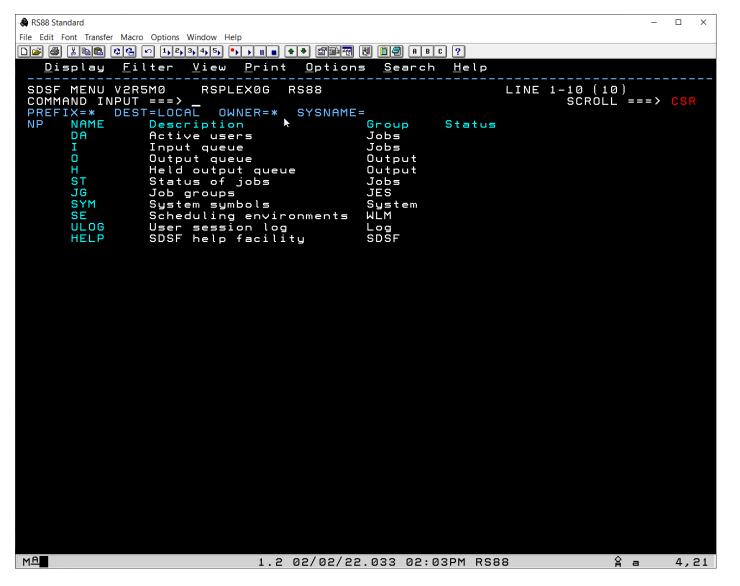
Connecting to SDSF

- Each SDSF user must connect to the SDSF server
  - One connection per task (TCB)
- Ability to connect to SDSF requires
  - READ access to SDSF class profile ISF.CONNECT.*sysname*
- SDSF server attempts to place user into a SDSF group
  - Groups are specified in ISFPRMxx PARMLIB member
  - READ access to SDSF class profile GROUP.*name*.*sysname*
  - User placed into first valid group in the sequence specified in ISFPRMxx
  - If no matching group found the connection will fail
  - SDSF groups dictate options and customizations
    - Examples include "Date Format" and "Cursor position behaviour"
    - No longer used for authorization settings

Using SDSF Panels

Access to SDSF Panels

- Three types of SDSF user in provided ISFPRMxx PARMLIB member
  - Systems programmer
  - Operator
  - General user – for example, a COBOL programmer
- SDSF main panel will normally only show entries that user is authorized to
  - General users have been seeing the same 5 to 8 choices for many years
  - Over 60 other panels for systems programmers and operators
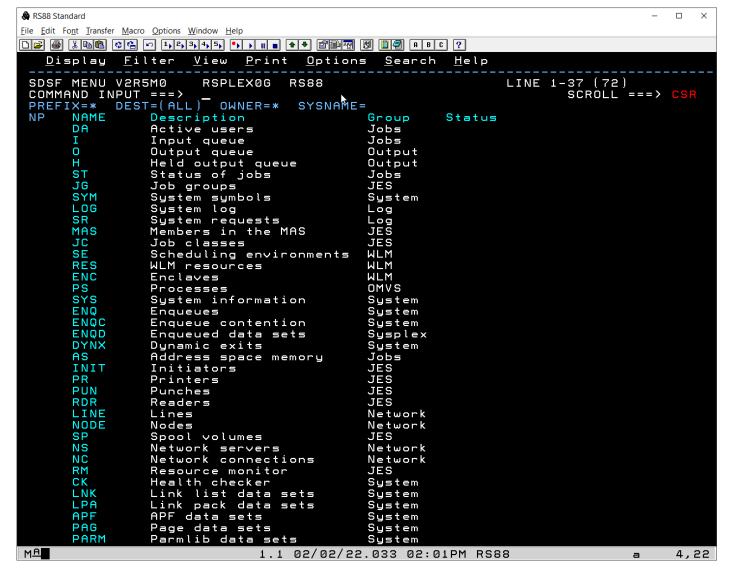 - SET MENU ALL shows entries for unauthorized and not applicable choices

General User

General user panels protected by READ access to SDSF class profile :

ISFCMD.DSP.*name.qualifier*

Think of "DSP" standing for "display"

Includes active jobs and JES input and output queues

Sysprog/Operator Users

Systems programmer and operator panels protected by READ access to SDSF class profile :

ISFCMD.ODSP.name.qualifier

Think of "ODSP" standing for "operator display"

Includes more powerful displays and functions

General users can be easily denied access to advanced displays by having no access to ISFCMD.ODSP.*.*

Actions Typed in "NP"

- NP column is where row actions are entered ("*iNPut*")
- Access checked against resource that protects the row
  - READ access for display style actions
  - Higher access (UPDATE, CONTROL or ALTER) for change or delete style actions
  - When action just displays another SDSF panel, then row object access is not required
- JESSPOOL class profile used for active jobs and output
  - Rows on ST, DA, H, I and O
- Other IBM classes used if applicable
  - For example, XFACILIT for CK rows (HealthCheck)
- SDSF class profile used for other panel objects when generating operator commands
  - ISF*xxxxx.qualifier_1.qualifier_2…qualifier_n*
  - xxxxx = short name for panel object, e.g. "APF" for entries on APF panel
  - Qualifiers depend on panel, e.g. the dataset name on APF
- OPERCMDS profile checked when action generates z/OS operator command
  - Checked after successful access to profile covering row object
- SDSF manuals contain tables of resources checked

Action Typed in "NP" – Example 1

```
SDSF HELD OUTPUT DISPLAY ALL CLASSES LINES 418,875      LINE 1-41 (41)
COMMAND INPUT ===>                                        SCROLL ===> CSR
NP      JOBNAME  JobID      Owner       Prty C Max-RC      REC-Cnt  PAGE-Cnt Dest
p       BOWLING  JOB01234 BARNEY        128 H ABEND S522     3,989            LOCAL
        BAMBAM   JOB01235 BETTY         144 F ABEND S522        52            LOCAL
```

- User FRED types "H" to display the held output queue for the JES subsystem "JES2"
- User "FRED" then issues "P" against JES jobid JOB01234 "BOWLING" on node "BEDROCK". The job is owned by user "BARNEY".
  - "P" action requires ALTER access as "delete" style request.
  - Row is protected by JESSPOOL profile
  - OPERCMDS profile checked as "P" generates operator command
  - Sequence of SAF checks :
    - READ access for SDSF profile ISFCMD.DSP.HELD.JES2
    - ALTER access for JESSPOOL profile BEDROCK.BARNEY.BOWLING.JOB01234.qualifiers
    - UPDATE access for OPERCMDS profile JES2.CANCEL.BATOUT
      - BATOUT means "batch job output" in JESSPOOL profile name

Action Typed in "NP" – Example 2

```
SDSF NETWORK ACTIVITY   WILMA        WILMA                      LINE 39-51 (51)
COMMAND INPUT ===>                                              SCROLL ===> CSR
NP    JOBNAME   Status     IPAddr                  Port InBufSz OutBufSz EXCP-Cnt
      GPMSERMS  LISTEN     ::0                     31350       0        0        0
      SSHD3     ESTABLSH   10.117.222.101          35762   65536    65536    82498
      SSHD3     ESTABLSH   10.117.222.101          45510   65536    65536   827123
dn    TN3270    ESTABLSH   ::FFFF:10.5.82.199      52365   65536    65536      465
```

- User FRED types "NA" on system WILMA to show the network activity and then types "DN" beside the row for TN3270 to display the connections.
  - "DN" action requires READ as a "display" style request
  - Row is protected by SDSF class profile ISFNETACT.*qualifiers*
  - OPERCMDS profile checked as "DN" generated operator command
  - Sequence of SAF checks
    - READ access for SDSF profile ISFCMD.ODSP.NETACT.WILMA
    - READ access for SDSF profile ISFNETACT.TN3270
    - READ access for OPERCMDS profile MVS.DISPLAY.TCPIP

Action Typed in "NP" – Example 3

```
SDSF HEALTH CHECKS   WILMA                            LINE 3-59 (169)
COMMAND INPUT ===>                                        SCROLL ===>
NP    NAME                          CheckOwner       State
      ALLOC_SPEC_WAIT_POLICY        IBMALLOC         ACTIVE(ENABLED)
      ALLOC_TIOT_SIZE               IBMALLOC         ACTIVE(ENABLED)
ds    ASM_LOCAL_SLOT_USAGE          IBMASM           ACTIVE(ENABLED)
      ASM_PAGE_ADD                  IBMASM           ACTIVE(ENABLED)
```

- User FRED types "CK" on system WILMA to show the HealthChecks and then types "DS" against the ASM_LOCAL_SLOT_USAGE check to display its status
  - "DS" action requires READ as a "display" style request
  - Row is protected by XFACILIT class profile HZS.qualifiers
  - OPERCMDS profile checked as "DS" generates operator command
  - Sequence of SAF checks
    - READ access for SDSF profile ISFCMD.ODSP.HCHECKER.WILMA
    - READ access for XFACILIT profile HZS.WILMA.IBMASM.ASM_LOCAL_SLOT_USAGE.QUERY
    - UPDATE access for OPERCMDS profile MVS.MODIFY.STC.HZSPROC.HZSPROC

Overtype value on panel

- Overtype columns protected by SDSF class profile
  - ISFATTR.*type*.*column*
  - *Type* describes the panel row object
  - *Column* is the internal column name (not the title)
    - See "COLH" display for panel to see list of internal column names
  - UPDATE access required
- SAF check performed when column becomes first becomes visible in the display
  - All of the column (both left and right bounds) must be visible on the screen
  - If access allowed, the screen attributes for the column are changed to allow input
  - If access denied, the screen attributes for the column are left as output only
- If valid overtype value is detected, security processing matches the sequence described for "NP" actions

Advanced Functions

Controlling the Scope of Data Displayed

- PREFIX command
  - Allows filtering by jobname using masking characters
    - Applies to active jobs and JES queue displays
  - Only user with authority to PREFIX can change the default specified in the SDSF group they are assigned to
  - READ access to SDSF class profile ISFCMD.FILTER.PREFIX

- OWNER command
  - Allows filtering by job owner using masking characters
    - Applies to active jobs and JES queue displays
  - Only user with authority to OWNER can change the default specified in the SDSF group they are assigned to
  - READ access to SDSF class profile ISFCMD.FILTER.OWNER

Controlling the Scope of Data Displayed

- DEST command
  - Allows filtering by destination using masking characters
    - Applies to JES queue displays
  - Only user with authority to DEST can change the default specified in the SDSF group they are assigned to
  - READ access to SDSF class profile ISFCMD.FILTER.DEST
- Careful specification of PREFIX, OWNER and DEST can safeguard general users from seeing or manipulating jobs outside of their normal responsibilities
  - SET DISPLAY ON causes values to be shown above the column titles

Cross-System Data Access

- SYSNAME command
  - Allows the user to access data from one or more systems in the sysplex
  - Masking characters can be used against the z/OS system name (CVTSNAME)
  - Causes SDSF to send a message from the local SDSFAUX server to other SDSFAUX address spaces in the sysplex
  - Responses are collected from all responding systems and presented locally to the user
  - READ access to SDSF class profile ISFCMD.FILTER.SYSNAME
  - If SYSNAME authority denied, then data gathering request is confined to the local system

Destination Operator Authority

- Sometimes impractical to permit operators to every JESSPOOL class profile so that they can view or manage output
- SDSF provides ability to define users with authority based on the destination for output rather than owner, jobname etc
  - SDSF uses term "destination operator"
- To be a destination operator, the userid must have
  - READ access to SDSF class profile ISFOPER.DEST.*jesname*
  - ALTER access to SDSF class profile ISFAUTH.DEST.*destname* for full management
    - READ access for just browse authority to output
- Destination operator authority functions
  - SDSF populates the BTOKRCID (network receiver userid) in the JES browse token
  - SAF authority check by JES for JESSPOOL uses RECVR keyword on RACROUTE

Foreign Address Space Data Access

- Some SDSF commands require cross-memory access to other address spaces that are not necessarily under SDSF (or user) control
    - Defines the term "foreign address space"
    - Data is typically gathered by scheduling SRB into foreign ASID
- Ability to gather foreign address space data protected by SDSF class profiles
    - ISFJOB.*type.owner.jobname.sysname*
    - READ access required
    - If no owner assigned to address space then SDSF uses value "++++++++"
        - Typically system address spaces started early in IPL process, eg "RASP" and "PCAUTH"
    - Type values
        - DDNAME   JDD action
        - MODULE   JC action
        - TASK   JT action
        - STORAGE   JM, JMO and MEM

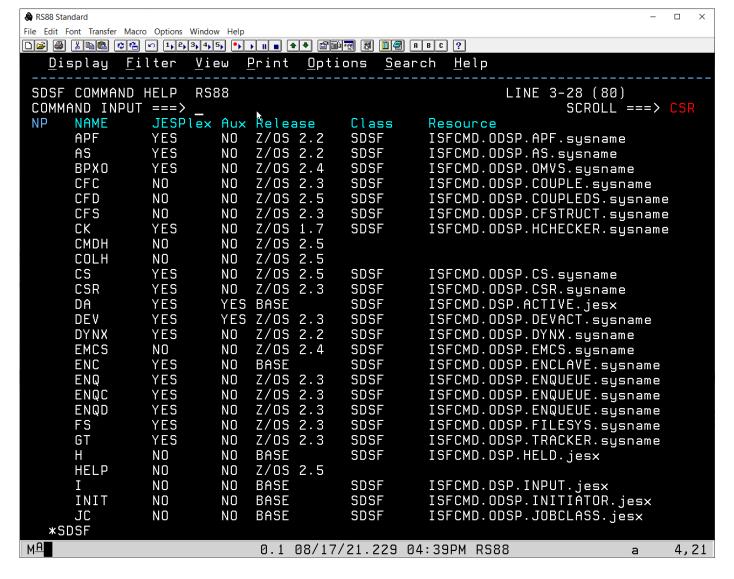# Issuing operator commands

- Freeform operator commands using "/"
  - Or ISFSLASH function in REXX

- READ access to SDSF class profile
  - ISFOPER.SYSTEM
  - Only restricts user from issuing operator commands in SDSF
    - Other authorized programs can issue operator commands outside of SDSF

- Command text passed directly to z/OS to process
  - No attempt made by SDSF to parse the freeform text and internally issue OPERCMDS authority checks
    - Includes any saved operator commands in SDSF profile or command groups
  - z/OS BCP will issue SAF OPERCMDS check on the command passed to it

Handling "No Decision" Situations

- SAF authority check return code
  - RC=0   User access is permitted to the profile covering the resource
  - RC=4   No decision can be made
  - RC=8   User access is denied to the profile covering the resource
- No decision circumstances
  - Class is not active
  - Class is active but not RACLISTed (applies to certain classes only)
  - Class is active (and RACLISTed if applicable) but no matching profile found
    - No "catch-all" profile "**" defined with site-defined UACC value
- ISFPRMxx CONNECT statement keyword AUXSAF(FAILRC4/NOFAILRC4)
  - FAILRC4   Convert RC=4 from SAF into RC=8 (Default)
  - NOFAILRC4   Convert RC=4 from SAF into RC=0
- Applies to all profiles checked by SDSF, not just SDSF class profiles
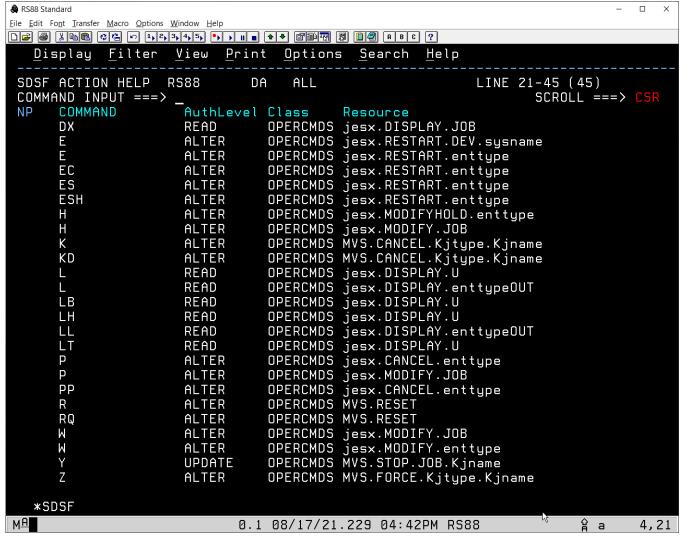
Using SDSF to understand SDSF Security

CMDH (Command Help)

List of primary SDSF commands and include any covering resource profile and class

Note that basic user interface commands are not protected by SAF
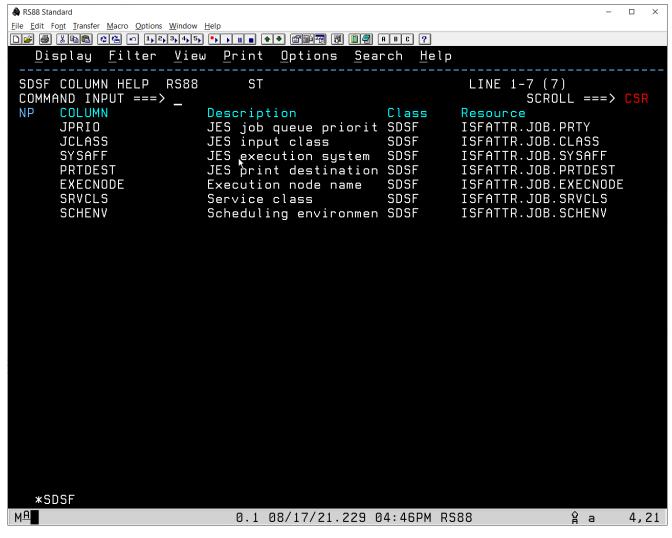
ACTH (Action Help)

Shows all actions for one or more panels

Auth level required shown along with the resource profile name and class

Lowercase values in resource name indicate variable replacements (inserts)

COLH (Column Help)
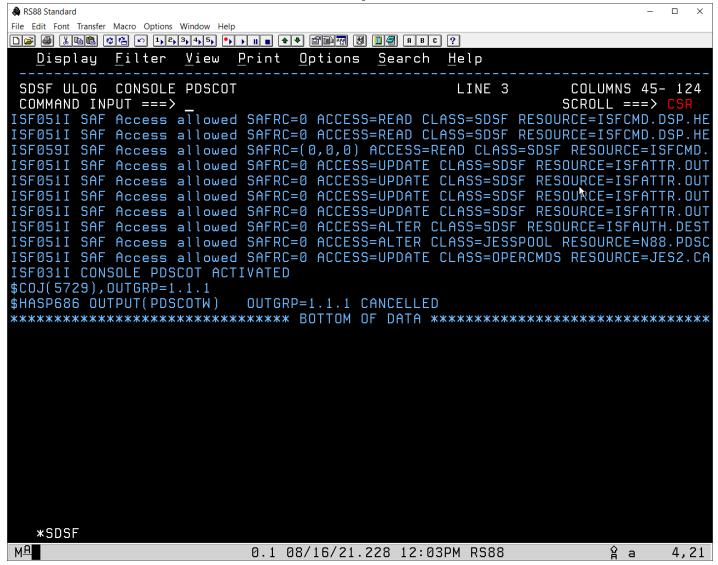

Shows column attributes for one or more panels

Overtype columns show resource name and class

Note that internal column name is used in the resource name and not the title

Security Trace

- Independent of normal SDSF trace
- Can be used to see all SAF checks issued by SDSF for current user
- Trace output sent to ULOG by default
- Issued via SET command
  - SET SECTRACE ON
  - SET SECTRACE OFF
  - SET SECTRACE WTP
    - Issue "write to programmer" style WTOs instead of ULOG
    - Useful for tracing SDSF initialization security calls
- Messages issued
  - ISF051I
  - ISF059I
- Alternate special DD names
  - ISFSECTR   Equivalent to "SET SECTRACE ON"
  - ISFSECTW   Equivalent to "SET SECTRACE WTP"

SECTRACE Output

HealthCheck - SDSF_CLASS_SDSF_ACTIVE

- Verifies if SDSF class is active
- Produces report on SDSF resources and how the security decision is derived
  - SAFRC
    - Covering profile found and SAF return code will be used
  - FAILRC4
    - No covering profile found and access will be denied due to AUXSAF(FAILRC4) in ISFPRMxx
  - NOFAILRC4
    - No covering profile found and access will be allowed due to AUXSAF(NOFAILRC4) in ISFPRMxx
- Note that no security check is performed by this healthcheck, it only reports the method that will be used.

HealthCheck Output