



CONSULTING

RACF and Storage Administration

June 2024





RSH Consulting, Inc. is an IT security professional services firm established in 1992 and dedicated to helping clients strengthen their IBM z/OS mainframe access controls by fully exploiting all the capabilities and latest innovations in RACF. RSH's services include RACF security reviews and audits, initial implementation of new controls, enhancement and remediation of existing controls, and training.

- www.rshconsulting.com
- 617-969-9050
- www.linkedin.com/company/rsh-consulting-inc.



Robert S. Hansel is Lead RACF Specialist and founder of RSH Consulting, Inc. He began working with RACF in 1986 and has been a RACF administrator, manager, auditor, instructor, developer, and consultant. Mr. Hansel is especially skilled at redesigning and refining large-scale implementations of RACF using role-based access control concepts. He is a leading expert in securing z/OS Unix using RACF. Mr. Hansel has created elaborate automated tools to assist clients with RACF administration, database merging, identity management, and quality assurance.

- 617-969-8211
- R.Hansel@rshconsulting.com
- www.linkedin.com/in/roberthansel



■ Tasks and Functions

- Manage System Managed Storage (SMS) configuration, constructs, and Automatic Class Selection (ACS) routines
- Copy and move data between devices and systems
- Backup (dump) and restore data
- Manage space - compress, defrag, and release
- Migrate, recall, catalog, and delete (scratch) data
- Merge, move, and fix catalogs
- Manage DASD devices
- Manage Removal Media (tape)

■ Tools - DFSMS/MVS

- DFSMSdfp Data Facility Product (IDCAMS utility - Access Method Services)
- DFSMSdss Data Set Services (ADRDSSU utility)
- DFSMShsm Hierarchical Storage Manager
- DFSMSrmm Removal Media Manager
- DFSMSopt SMS Optimizer (obsolete?)
- ICKDSF Device Support Facilities
- ISMF Interactive Storage Management Facility

RACF, DFSMS, and z/OS are Trademarks of the International Business Machines Corporation



- RACF Authorities
 - Dataset Profiles
 - OPERATIONS Authority
 - Catalog Profiles
 - DASDVOL Profiles
 - FACILITY Storage Admin Profiles
 - ISMF Program Authorization
 - DFSMSHsm Authorities

- Storage Admin authorities can and should be used to replace OPERATIONS authority in most cases

- RACF can be used to govern SMS data management
 - STORCLAS and MGMTCLAS classes and profiles
 - DFP segments on user, group, and dataset profiles



OPERATIONS Authority



- Grants ALTER level access to resources whose classes have been defined with OPER=YES or OPERATIONS(YES) in the Class Descriptor Table

- RACF predefined z/OS classes with OPER=YES

DATASET	TAPEVOL	DASDVOL/GDASDVOL	
PSFMPL	NETCMDS	NETSPAN	RODMMGR

- Scope of authority

- SYSTEM / USER-Attribute

ALU userid attribute

```
USER=JSMITH1  NAME=JOHN SMITH          OWNER=SECGRP1  CREATED=01.067
DEFAULT-GROUP=USRGRPA  PASSDATE=00.351  PASS-INTERVAL= 30
ATTRIBUTES=OPERATIONS
```

Authority applies across entire RACF system

- GROUP / CONNECT-Attribute

CO userid GROUP(groupid) attribute

```
GROUP=DASDMGT  AUTH=USE  CONNECT-OWNER=RJONES2  CONNECT-DATE=92.181
CONNECTS=      00  UACC=NONE  LAST-CONNECT=UNKNOWN
CONNECT ATTRIBUTES=OPERATIONS
```

Authority limited by Scope-of-Groups



- OPERATIONS authority ...
 - Applies to both SMS and non-SMS managed data
 - Grants ALTER access to datasets unless restricted (see below)
 - Allows creation of group datasets and profiles (implicit group CREATE authority)
 - Allows defining or renaming RACF-indicated datasets and discrete profiles
 - Allows deleting orphaned temporary datasets when TEMPDSN is active

- Can be restricted by ...
 - Permitting an OPERATIONS user's USERID or one of its connect groups to a profile's Standard Access List limits the user's access to the level permitted (e.g., READ)
 - Connecting the USERID of an OPERATIONS user to the Group matching a dataset HLQ (e.g., SYS1) with AUTHORITY(USE) ...
 - ❖ Prevents the creation of new datasets under that HLQ using OPERATIONS authority
 - ❖ Prevents the creation of group dataset profiles under that HLQ
 - ❖ Interesting functionality, but may not be of any practical use

OPERATIONS Authority



- OPERATIONS authority use may be needed on an occasional basis
 - Changing a dataset's SMS storage or management class requires ALTER access to the dataset or catalog
 - Defining or renaming a RACF-indicated dataset
 - ❖ Alternative - find and turn off all orphaned RACF-indicated bits (bit is ON but no discrete profile) by creating then deleting a discrete profile [VOLUME - may be required]
 ADDSD '*dataset-name*' **NOSET** [VOLUME(*vol-ser*)]
 DELDSD '*dataset-name*' [VOLUME(*vol-ser*)]
 - Deleting orphaned temporary datasets when TEMPDSN is active



■ Best Practices

- Specify OPER=NO / OPERATIONS(NO) for installation-defined classes
 - ❖ Classes originally defined to ICHRRCDE often have OPER=YES because this is the ICHERCDE macro default and 3rd party product class definition instructions failed to specify OPER=NO
 - ❖ Subsequent ICHRRCDE conversions to CDT class profiles often retained OPERATIONS(YES)
- Assign OPERATIONS only to alternate "emergency" IDs for storage administrators
 - ❖ Vault OPERATIONS IDs if feasible
- Be wary of SURROGAT profiles allowing use of IDs with OPERATIONS
- Create an OPERATIONS access blocking group (e.g., XOPERACC), connect all OPERATIONS users to this group, and minimally permit access to ...
 - ❖ DASDVOL profiles - NONE
 - ❖ DATASET profiles protecting Catalogs - READ or UPDATE
 - ❖ DATASET profiles protecting RACF databases, including backups - NONE
- Consider using blocking group to restrict access to other sensitive datasets (e.g., APF libraries, PHI/PII application datasets)
- Block OPERATIONS users use of ADDSD with PROGRAM profiles or RACF command exit
- Monitor OPERATIONS use by activating SETROPTS OPERAUDIT
- Implement Storage Admin authorities as an alternative

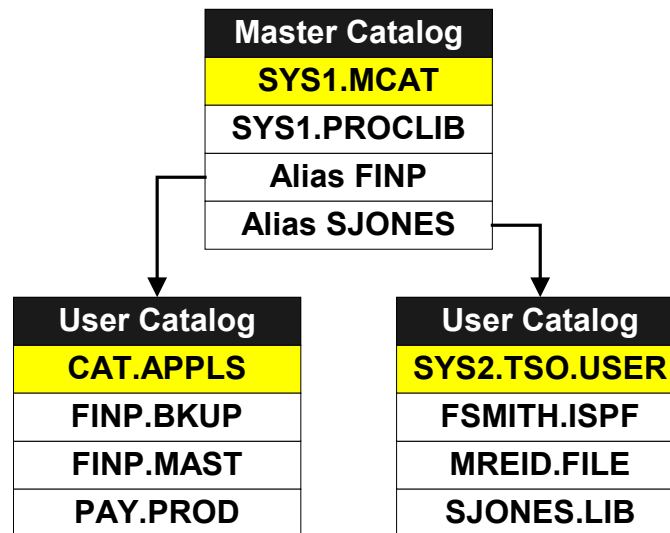


- Barriers to best practice implementation
 - Politics | Inertia | Inconvenience | FUD (Fear, Uncertainty, and Doubt)
 - Standard Operating Procedures - may require ALTER access to any/all files
 - ❖ Technical Assistance - help any user or application team with dataset problems
 - ❖ Dataset Allocation - team pre-allocates all production files
 - ❖ Production Fixes - rerun production job with ID that sidesteps RACF dataset violations
 - ❖ Problem Resolution ("Firecall") - fix any production problem
 - Consider use of Group-OPERATIONS for application fire-call IDs

Catalog Authorization



- A catalog is a dataset that contains information about other datasets and provides users with the ability to locate a dataset by name without knowing where the dataset resides
- Typical catalog structure and entries
 - Master catalog
 - ❖ SYS1 datasets
 - ❖ Key system datasets - referenced in IPL (e.g., RACF databases, PARMLIBs)
 - ❖ User catalogs
 - ❖ Aliases (dataset prefixes with pointers to user catalogs)
 - User catalogs
 - ❖ Application datasets
 - ❖ User datasets
- To find a dataset, the Master catalog is searched first, and then the User catalog pointed to by the alias



Catalog Authorization



S E L E C T E D	D A T A	S E T S	R E P O R T		
DATA SET NAME	VOLUME SERIAL	SELECTION CRITERION	RACF INDICATED	RACF PROTECTION	UACC
CA7.PROD.LOADLIB	DBD023	APF	NO	YES	READ
CATLG.MSTR	SYSCAT	MASTER CATALOG	NO	YES	READ
CATLG.USERA	SYSCAT	USER CATALOG	NO	YES	UPDATE
CICS.TEST.R33.LIB	TSTA02	APF	N.F.	YES	UPDATE
FDR.LOADLIB	SYS033	APF	YES	YES	READ
		LNKLST - APF			
PAY.PROD.LOADLIB	APP770	LNKLST - APF	NO	NO	
SYS1.IMAGELIB	SYS034	SYSTEM	NO	YES	READ
SYS1.PARMLIB	SYSRS1	SYSTEM	NO	YES	UPDATE
SYS1.RACF.V19.PRIM	SYS011	RACF PRIMARY	NO	YES	READ
TMS.LINKLIB	ALT222	APF	NO	YES	UPDATE
UCC7.PROD.LOADLIB	D11456	APF	N.M.	NO	

N.F. - Not Found
 N.C. - Not Cataloged
 N.M. - VOLSER Not Mounted

LD DA('CATALOG.USER001') GEN AUTH
 INFORMATION FOR DATASET CATALOG.USER*.** (G)

LEVEL	OWNER	UNIVERSAL ACCESS	WARNING	ERASE
00	TECHSPT1	NONE	YES	NO

ID	ACCESS
*	UPDATE
FOREIGNU	READ
CATMGT	ALTER
APPLDEV	ALTER
TMSCLEAN	ALTER

< Questionable permission

Catalog Authorization



- READ access to the catalog is required to locate a dataset via the catalog

- UPDATE access to the catalog is required to add or change an entry when creating, cataloging, and uncataloging a dataset, provided the user also has ALTER access to the target dataset
 - UPDATE access to a User catalog is not required to add an entry when creating an SMS-managed dataset

- ALTER access to a dataset ...
 - Allows deleting the dataset and removing its entry from the catalog without requiring access to the catalog
 - Allows renaming of the dataset and changing its entry in the catalog without requiring access to the catalog; however, the user must also have either ALTER access or group CREATE authority to the new dsname

Catalog Authorization



- ALTER access to the catalog allows the following actions:
 - Uncatalog any non-SMS-managed dataset without ALTER access to the dataset
 - Delete any SMS-managed dataset or VSAM file without ALTER access to the dataset
 - ❖ Can prohibit deletion with XFACILIT STGADMIN.IGG.DELAUDIT.catalogname profile
 - Change certain dataset catalog entry attributes without ALTER access to the dataset itself (e.g., SMS management and storage classes)
 - Perform catalog administration functions not governed by STGADMIN profiles
 - Open the catalog as a dataset (must also have APF-authorization)

- Catalogs can be locked for copy and recovery processing
 - READ access to FACILITY class resource IGG.CATLOCK, in combination with ALTER access to the catalog, allows locking and unlocking of the catalog
 - READ access to IGG.CATLOCK allows use of a locked catalog

- OPERCMDS MVS.MODIFY.STC.CATALOG.CATALOG.SECURE
 - READ allows MODIFY CATALOG subcommands for reporting type functions
 - UPDATE allows MODIFY CATALOG subcommands for all other functions (e.g., CLOSE)

Catalog Authorization - Alias Administration



- If RACF Administration or an identity Management (IDM) product maintains catalog aliases for TSO users, permit either ...
 - READ access to FACILITY STGADMIN.IGG.DEFDEL.UALIAS
 - ❖ Allows creation and deletion of aliases
 - Deletion not limited to aliases for users
 - Deletion not prevented if there are cataloged datasets
 - ALTER access to the Master Catalog
 - ❖ Allows creation and deletion of aliases
 - Deletion not limited to aliases for users
 - Deletion not prevented if there are cataloged datasets
 - ❖ Allows other actions associated with catalog ALTER access
 - UPDATE access to the Master Catalog to create aliases
 - ❖ Allows creation of aliases
 - ❖ Allows cataloging datasets in the Master Catalog if permitted ALTER access to the datasets
 - ❖ Alias deletion is handled by Catalog Administrators
 - ALTER access to the User Catalog containing the TSO user dataset entries
 - ❖ Allows deletion of aliases related to that catalog
 - Deletion not limited to aliases for users
 - Deletion not prevented if there are cataloged datasets
 - ❖ Allows other actions associated with catalog ALTER access
 - Can prohibit dataset deletion with XFACILIT STGADMIN.IGG.DELAUDIT.catalogname profile

Catalog Authorization - Residual Data Cleanup



- If RACF Administration is responsible for residual TSO user data cleanup ...
 - Add AUDIT(ALL) to TSO user dataset profiles to monitor access activity before deletion
 - To delete datasets, permit either ...
 - ❖ ALTER access to the dataset profiles protecting the TSO user data
 - ❖ ALTER access to the User Catalog containing the TSO user dataset entries
 - ❖ READ access to XFACILIT profile STGADMIN.IGG.DELAUDIT.catalogname for the User Catalog containing the TSO user dataset entries
 - Generates SMF 80 records logging deletions if the profile has AUDIT(ALL(READ))
 - The latter two options should only be considered when TSO user datasets are cataloged in their own separate User Catalog apart from other datasets

Catalog Authorization



- Common / Best Practices
 - Set UACC READ for Master Catalog
 - Set UACC UPDATE for User Catalogs (unless DSNAMES themselves are sensitive)
 - Add UACC equivalent entries in the Global Access Table
 - Permit UACC equivalent access to RESTRICTED users
 - Permit ALTER to Catalog Administrators
 - Permit UPDATE to the Master Catalog only to users and processes creating aliases and datasets cataloged in the Master Catalog
 - (Optional) Permit ALTER to User Catalogs containing TSO user dataset entries to facilitate data disposal
 - Permit ALTER to dataset cleanup processes (e.g., tape catalog maintenance routine)
 - Permit UACC or ID(*) equivalent access to an OPERATIONS authority blocking group
 - Do **not** put WARNING on profiles protecting catalogs



- Controls who can manage and manipulate data on an entire DASD volume via certain software facilities
 - DFSMSdss ADRDSSU utility
 - ❖ 'Physical' functions for all volumes (e.g., DUMP FULL)
 - ❖ 'Logical' functions for non-SMS-managed volumes
 - DFSMSdfp DADSM Scratch Macro (non-SMS-managed volumes)
 - ICKDSF utility
 - AMASPZAP utility VTOC Update

- General Resource
 - Classes - DASDVOL / GDASDVOL
 - Resource - *DASD_ volume-serial_ number* (e.g., SYS011)

DASDVOL Profiles



DASDVOL Authority	ICKDSF Command / Function	ADRDSU Command / Function	DADSM	AMASPZAP
ALTER	BUILDIX	COPY to target - Volume / Track	Scratch	
	INIT	COPY DELETE from source - Dataset		
	INSPECT	DUMP DELETE		
	REFORMAT EXTINDEX	RESTORE to target - Volume / Track		
	REFORMAT EXTVTOC	SPACEREL to source		
	REFORMAT NEWVTOC			
	REFORMAT REFVTOC			
UPDATE	REFORMAT IPLDD	BUILDSA to target		VTOC Update
		COMPRESS - Dataset		
		CONSOLIDATE to source - Dataset		
		COPY to target - Dataset		
		COPY DELETE to target - Dataset		
		DEFRAG - Dataset		
		RELEASE - Dataset		
		RESTORE to target - Dataset		
READ		COPY from source - Volume / Track / Dataset		
		DUMP		
		PRINT - Tracks / Dataset		
		RESTORE from source - Dataset		

DASDVOL Profiles - Use by Other Products



- DITTO and File Manager
 - Control use of DITTO's and File Manager's functions to manipulate DASD datasets with full disk volume processing
 - Only applicable if product is running APF-authorized
 - FACILITY *prefix*.DISK.FULLPACK (prefix = DITTO or FILEM)
 - ❖ READ - Read and update access to entire contents of specific volsers
 - To read, requires READ to associated DASDVOL profile
 - To update, requires ALTER to associated DASDVOL profile
 - ❖ UPDATE - Read access to entire contents of all volsers, update to specific ones
 - To update, requires ALTER to associated DASDVOL profile
 - ❖ ALTER - Read and update access to all volsers (no DASDVOL access required)
 - If DASDVOL is active, permission is required; if inactive, all access is allowed
 - Best Practices
 - ❖ Define *prefix*.DISK.FULLPACK as a discrete profile with UACC(NONE) AUDIT(ALL(READ))
 - ❖ Avoid granting access of ALTER to *prefix*.DISK.FULLPACK
 - ❖ If any access is granted to *prefix*.DISK.FULLPACK, activate DASDSVOL and define a catch-all ** profile with UACC(NONE)

DASDVOL Profiles - Use by Other Products



- FDR - backup/restore authorization by DASD volume
 - Requires option ALLCALL be set to YES to enable security checking
 - If a DASD volume is not protected by a DASDVOL profile, a user with READ access to the FDR volume backup can restore the volume

- ISMF - RAUTH - Remote access codes to a 3990 Control Unit
 - ALTER authority required to volume request is made against

- EMC - TimeFinder/Clone Mainframe Snap Facility - clone DASD volumes
 - READ authority is required to the volume being copied
 - ALTER authority is required to the volume being restored

- IBM - Device Manager (DEVMAN)
 - ALTER authority is required to perform certain functions
 - READ access to FACILITY STGADMIN.ICK.REFORMAT and STGADMIN.ICK.INIT



- Considerations
 - DASDVOL access authority supersedes dataset access authority
 - UPDATE access allows VTOC changes using AMASPZAP (e.g., reset RACF-indicated bit)
 - ❖ Overrides requirement for console operator authorization
 - With ICKDSF INIT, INSPECT, and TRKFMT, dataset access authority is checked if the volume is not defined to DASDVOL
 - DASDVOL profiles work in combination with FACILITY STGADMIN.ICK profiles; STGADMIN.ICK profiles govern the use of ICKDSF functions and DASDVOL limits the VOLSERS where these functions can be performed
 - OPERATIONS authority grants ALTER level access
 - In some cases, DASDVOL access is needlessly checked when ADRDSSU Administrator authority is permitted (vote for RFE 102423 to eliminate such checks)

- DASDVOL profiles do not ...
 - Restrict who can allocate data on a DASD device
 - Grant access through other utilities or facilities (e.g., TSO)
 - Allow define or rename of RACF-indicated datasets
 - Log unsuccessful access attempts (dataset logging is applied)
 - Grant access to migrated datasets (dataset access is required)



■ Common / Best Practices

- Define a catch-all profile ** to cover all volumes
- Restrict access to storage administration staff and processes (e.g., backup and restore jobs)
- Block OPERATIONS authority with access-excluding group permit of NONE
- RACLIST the DASDVOL class, especially if using GDASDVOL grouping class
- Do **not** put WARNING on DASDVOL profiles

■ Recommended profiles for comprehensive protection:

```
RDEF DASDVOL ** UACC(NONE)
```

```
PERMIT ** CLASS(DASDVOL) ID(stgadmin-group) ACCESS(ALTER)
```

```
PERMIT ** CLASS(DASDVOL) ID(devman-stc) ACCESS(ALTER)
```

```
PERMIT ** CLASS(DASDVOL) ID(operations-users) ACCESS(NONE)
```

```
[optional] PERMIT ** CLASS(DASDVOL) ID(backup-user) ACCESS(READ)
```

```
[optional] PERMIT ** CLASS(DASDVOL) ID(dr-restore-user) ACCESS(ALTER)
```

FACILITY Storage Admin Profiles



- Controls who can manage catalogs and data using DFSMS/MVS utilities and services
- General Resource
 - Class - FACILITY
 - Access level - READ - Perform Function (RMM uses various access levels)
 - Resources - STGADMIN.*service*(.STGADMIN | ENDUSER).*function/command*[.parm]
 - ❖ STGADMIN.ADR.STGADMIN.*function*[.parm] DSS - ADMINISTRATOR
 - ❖ STGADMIN.ADR.*command*[.parm] DSS
 - ❖ STGADMIN.ANT.*component.function* Data Mover
 - ❖ STGADMIN.ARC.ABACKUP[.parm] ABARS
 - ❖ STGADMIN.ARC.ARECOVER[.parm] ABARS
 - ❖ STGADMIN.ARC.ENDUSER.*command*[.parm] HSM - End-User
 - ❖ STGADMIN.ARC.*command*[.parm] HSM
 - ❖ STGADMIN.EDG.*function* RMM
 - ❖ STGADMIN.HMT.*function* StorWatch HSM Monitor
 - ❖ STGADMIN.ICK.*command* ICKDSF
 - ❖ STGADMIN.IDC.*command*[.parm] IDCAMS
 - ❖ STGADMIN.IGG.*function* IDCAMS - SMS-managed entries

FACILITY Storage Admin Profiles



■ General Resource (Continued)

• Resources - STGADMIN.*service*(.STGADMIN | ENDUSER).*function/command*[.*parm*]

- ❖ STGADMIN.DFSMSOPT.*function* SMS Monitor/Tuner
- ❖ STGADMIN.DPDSRN.*currentdsname* IDCAMS
- ❖ STGADMIN.DMO.CONFIG SMS
- ❖ STGADMIN.IFG.READVTOC.*volser* DFP
- ❖ STGADMIN.IGD.ACTIVATE.CONFIGURATION SMS
- ❖ STGADMIN.IGWSHCDS.REPAIR IDCAMS
- ❖ STGADMIN.SMS.ALLOW.DATASET.ENCRYPT DFP
- ❖ STGADMIN.SMS.FAIL.INVALID.DSNTYPE.ENC DFP
- ❖ STGADMIN.DMS.STGADMIN[.*function*] CA-DISK

■ Other related resources

- IGG.CATLOCK IGG - ICF Catalogs
- IHJ.CHKPT.*volser* Create checkpoints on shared DASD

FACILITY Storage Admin Profiles



- ADRDSSU utility ADMINISTRATOR keyword
 - Protected by STGADMIN.ADR.STGADMIN prefixed profiles
 - Supersedes dataset authority - allows operations without requiring dataset access permissions
 - Does not allow define or rename of RACF-indicated dataset

```
RLIST FACILITY STGADMIN.ADR.STGADMIN.RESTORE.RENAME AUTH
CLASS      NAME
-----
FACILITY   STGADMIN.ADR.STGADMIN.* (G)

LEVEL      OWNER          UNIVERSAL ACCESS    YOUR ACCESS    WARNING
-----
  00      TECH$RES              NONE                NONE            NO

INSTALLATION DATA
-----
STOR ADMIN FUNCTIONS - ADMIN KEYWORD RES - READ=USE

USER       ACCESS      ACCESS COUNT
-----
DASDMGT    READ
TECHSPT    READ
COMPOPRS   UPDATE      < Questionable permission
```

FACILITY Storage Admin Profiles



- Profiles where UACC / ID(*) other than NONE is recommended
 - STGADMIN.ARC.ENDUSER.** READ ⁽¹⁾
 - STGADMIN.EDG.LABEL.volser UPDATE
 - STGADMIN.EDG.LISTCONTROL CONTROL
 - STGADMIN.EDG.MASTER READ
 - STGADMIN.EDG.NOLABEL.volser UPDATE
 - STGADMIN.EDG.RELEASE READ
 - STGADMIN.EDG.VRS READ

(1) Use of H-prefixed HSM commands (e.g., HRECALL) usually requires access permission to the target dataset (see upcoming slide)

FACILITY Storage Admin Profiles



- When not defined to RACF, many functions can be executed by any user
 - Cannot use ADRDSSU ADMINISTRATOR keyword if no profile

- Common / Best Practices
 - Restrict access to storage administration staff and processes
 - Define profiles out to second node (service) (e.g., STGADMIN.ADR)
 - Define a catch-all STGADMIN.** with UACC(NONE) and no permits
 - Limit access to STGADMIN.DPDSRN.*oldname* (use requires operator approval)
 - Optionally permit select users access to resources for tolerating enqueues
 - Strictly control authority to use ADMINISTRATOR keyword
 - Do **not** put WARNING on STGADMIN profiles

ISMF - End User (EU) Mode



Panel Help

ISMF PRIMARY OPTION MENU - z/OS DFSMS V2 R5

Enter Selection or Command ==>

Select one of the following options and press Enter:

- | | | |
|---|-------------------------|--|
| 0 | ISMF Profile | - Change ISMF User Profile |
| 1 | Data Set | - Perform Functions Against Data Sets |
| 2 | Volume | - Perform Functions Against Volumes |
| 3 | Management Class | - Specify Data Set Backup and Migration Criteria |
| 4 | Data Class | - Specify Data Set Allocation Parameters |
| 5 | Storage Class | - Specify Data Set Performance and Availability |
| 9 | Aggregate Group | - Specify Data Set Recovery Parameters |
| L | List | - Perform Functions Against Saved ISMF Lists |
| R | Removable Media Manager | - Perform Functions Against Removable Media |
| X | Exit | - Terminate ISMF |

F1=Help F2=Split F3=End F4=Return F7=Up F8=Down F9=Swap

F10=Left F11=Right F12=Cursor

ISMF - Storage Administrator (SA) Mode



Panel Help

ISMF PRIMARY OPTION MENU - z/OS DFSMS V2 R5

Selection or Command ==>

More: +

0	ISMF Profile	- Specify ISMF User Profile
1	Data Set	- Perform Functions Against Data Sets
2	Volume	- Perform Functions Against Volumes
3	Management Class	- Specify Data Set Backup and Migration Criteria
4	Data Class	- Specify Data Set Allocation Parameters
5	Storage Class	- Specify Data Set Performance and Availability
6	Storage Group	- Specify Volume Names and Free Space Thresholds
7	Automatic Class Selection	- Specify ACS Routines and Test Criteria
8	Control Data Set	- Specify System Names and Default Criteria
9	Aggregate Group	- Specify Data Set Recovery Parameters
10	Library Management	- Specify Library and Drive Configurations
11	Enhanced ACS Management	- Perform Enhanced Test/Configuration Management
C	Data Collection	- Process Data Collection Function
G	Report Generation	- Create Storage Management Reports
L	List	- Perform Functions Against Saved ISMF Lists
P	Copy Pool	- Specify Pool Storage Groups for Copies

F1=Help F2=Split F3=End F4=Return F7=Up F8=Down F9=Swap

F10=Left F11=Right F12=Cursor

ISMF Program Authorization



- ISMF provides ISPF panels and programs for interactively invoking DFSMS functions
 - ISMF programs include applications (i.e., panels), functions, and line commands
 - ISMF programs do not check FACILITY STGADMIN profiles
 - ISMF programs do not run APF-authorized or circumvent RACF dataset protection so users still require access to the datasets they attempt to act upon

- To control the use of ISMF, either ...
 - Restrict access to ISMF libraries to just the storage administrators
 - Limit access to individual ISMF programs

- User must be in ‘Storage Administrator Mode’ to perform high level management functions
 - Program DGTFPF05 changes the mode in the user’s ISPF options dataset
 - Some installations choose to only protect program DGTFPF05
 - Simply protecting DGTFPF05 is not fool-proof; a knowledgeable user could manipulate option in own ISPF dataset

ISMF Program Authorization



- Options / Best Practices (Note: Installation library names may vary)
 - Protect ISMF program libraries - guard against copying
 - ADDSO 'SYS1.DGTLLIB' GEN UACC(NONE) DATA('ISMF DFSMS/DFP and DFSMS/DSS')
 - ADDSO 'SYS1.DFQLLIB' GEN UACC(NONE) DATA('ISMF DFSMS/HSM')
 - If use of ISMF is to be restricted to storage administrators ...
 - ❖ Permit storage administrators at least READ access to ISMF libraries
 - ❖ Do not put libraries in LINKLST
 - If use of ISMF is to be allowed to all users, PROGRAM protect ISMF programs
 - RDEF PROGRAM DGTxxxxx UACC(NONE) ADDMEM('SYS1.DGTLLIB'//NOPADCHK)
 - RDEF PROGRAM ACBFUTOn UACC(NONE) ADDMEM('SYS1.DGTLLIB'//NOPADCHK)
 - RDEF PROGRAM DFQFxxxx UACC(NONE) ADDMEM('SYS1.DFQLLIB'//NOPADCHK)
 - ❖ Implementation options, either ...
 - Define individual 'controlled' programs with UACC of NONE and access granted only to storage administrators, and leave all other programs open to anyone's use
 - Define individual programs all users are to be allowed to use with default access of READ and define catch-all profiles DGT*, ACBFUT*, and DFQF* to cover all other programs with UACC of NONE and access granted only to storage administrators
 - ❖ Put ISMF libraries in LINKLST to allow user execution

DFSMSHsm Considerations



- When the FACILITY class is active, DFSMSHsm command authority relies strictly on explicit permission to the profile covering each STGADMIN.ARC. resource - **RC=4 No profile -> No access**
- 'H'-prefixed ENDUSER commands require access permissions to the target datasets, at least ...
 - EXECUTE HRECALL
 - READ HRECOVER with NEWNAME to source dataset
 - UPDATE HBACKDS, HMIGRATE
 - ALTER HBDELETE, HDELETE, HRECOVER
- Administrator commands (e.g., RECALL) bypass dataset checking
 - Administrator commands are invoked from TSO via the HSEDCMD command
 - No RACF checking is performed for commands entered via the console
- If using RRSF to propagate commands, IBM recommends giving the DFSMSHsm Started Task ID on all recipient systems either ...
 - SPECIAL and OPERATIONS
 - TRUSTED
- If using DFSMSHsm to backup Unix HFS and zFS datasets, give its ID either ...
 - UPDATE access to UNIXPRIV resource SUPERUSER.FILESYS.QUIESCE (preferred)
 - UID(0)



- Aggregate Backup And Recovery Support (ABARS)
 - Comprehensive Authorization
 - ❖ All aggregates - bypass all dataset access authorization
 - ❖ STGADMIN.ARC.ABACKUP
 - ❖ STGADMIN.ARC.ARECOVER
 - Restricted Authorization
 - ❖ Specific aggregates - ABACKUP also requires at least READ access to all datasets
 - ❖ STGADMIN.ARC.ABACKUP.aggregate
 - ❖ STGADMIN.ARC.ARECOVER.aggregate
 - ❖ STGADMIN.ARC.ARECOVER.aggregate.REPLACE
 - ❖ STGADMIN.ARC.ARECOVER.aggregate.RENTGT

- Access checking
 - First checks authorization to restricted 'aggregate' resource
 - If disallowed, checks authorization to comprehensive resource
 - To enable use of comprehensive authority, disallow access to restricted 'aggregate' resources
 - ❑ STGADMIN.ARC.ABACKUP.* UACC(NONE)
 - ❑ STGADMIN.ARC.ABACKUP UACC(NONE) -&- PERMIT ID(backup-id) ACC(READ)

DFSMShsm Considerations



- Group ARCCATGP
 - Permits catalog operations on migrated datasets while bypassing automatic recall
 - User must be connected to and logged on with this group
 - ❖ Batch JCL - `//jobname JOB ...,GROUP=ARCCATGP`
 - To avoid dataset recall during deletion, DELETE command must be the first command for the dataset
 - Best practice - define ARCCATGP and connect catalog administrators
- User OPER
 - ABACKUP and ARECOVER commands entered via the console and executed by HSM are run with user OPER
 - Permit to STGADMIN.ARC.ABACKUP and/or ...ARECOVER profiles
 - Best practices
 - ❖ Define user OPER to RACF to reserve it
 - ❖ Make it PROTECTED and RESTRICTED
 - ❖ REVOKE if not needed
 - ❖ Do not use for other purposes
 - Can be set to a different ID with the PATCH command

Console Operator Actions



- Console Operator approval is required for certain functions
 - Required for updates to the following unless permitted by DASDVOL or ADRDSSU ADMINISTRATOR:
 - ❖ Volume Table of Contents (VTOC)
 - ❖ VTOC Index Dataset
 - ❖ VSAM Volume Dataset (VVDS)
 - ❖ Checkpoint / Restart Dataset
 - Operator only prompted once for first dataset encountered for one of the above types in processing a single command
 - Required to use ICKDSF to initialize (INIT) a volume with PURGE (delete all data)
 - Required to activate SMS configuration if FACILITY class resource STGADMIN.IGD.ACTIVATE.CONFIGURATION not protected by a RACF profile
 - Required along with access to STGADMIN.DPDSRN.*currentdsname* to rename a non-SMS dataset whose name is allocated to another address space or in the scope of the SYSDSN enqueue - may not be the same dataset, but the name matches so it is considered it to be in use



- SMS data management and revoked USERID failures
 - When moving or restoring data, SMS attempts to validate the STORCLAS and MGMTCLAS for the USERID
 - ❖ SMS option - PARMLIB(IGDSMSxx) - ACSDEFAULTS(YES | NO) - YES activates RACF SMS interface
 - ❖ Check only occurs when STORCLAS or MGMTCLAS are active
 - Attempts to perform RACROUTE REQUEST=VERIFYX and fails due to revoked ID
 - Options
 - ❖ SMS option - PARMLIB(IGDSMSxx) - USE_RESOWNER=(YES | NO) - NO uses authority of initiating user (e.g., storage administrator) rather than the dataset owner
 - ❖ ADRDSSU can be set to ignore revoked IDs using ADRPATCH Serviceability Aid flags

Common Findings - Storage Administration



- Excessive access authority granted to related profiles, especially to those governing the use of the ADMINISTRATOR keyword
- WARNING used on storage admin profiles
- OPERATIONS authority used instead of storage administrator authority profiles
 - Storage administrator authorities are not defined
 - Storage administrator authorities are defined and permitted, but not used
- OPERATIONS authority users access to catalog, DASDVOL, and RACF database profiles is not blocked
- Users are assigned OPERATIONS authority to their primary ID as opposed to an alternate ID
- Installation-defined classes allow OPERATIONS authority use
- ISMF programs not protected

Storage Administration References



- z/OS DFSMS Access Method Services Commands
- z/OS DFSMS Advanced Copy Services
- z/OS DFSMS Implementing System-Managed Storage
- z/OS DFSMS Managing Catalogs
- z/OS DFSMS OAM Planning, Installation, and Storage Administration Guide for Tape Libraries
- z/OS DFSMS Software Support for IBM System Storage TS1140, TS1130, and TS1120 Tape Drives (3592)
- z/OS DFSMS Using Data Sets
- z/OS DFSMS Using the New Functions
- z/OS DFSMSdfp Advanced Services
- z/OS DFSMSdfp Storage Administration
- z/OS DFSMShsm Implementation and Customization Guide
- z/OS DFSMShsm Storage Administration
- z/OS DFSMSrmm Diagnosis Guide
- z/OS DFSMSrmm Implementation and Customization Guide
- z/OS DFSMSrmm Managing and Using Removable Media
- z/OS DFSMStvs Administration Guide
- ICKDSF User's Guide and Reference

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

RACF Storage Administration Resources

FACILITY PROFILE	STORAGE ADMIN COMPONENT & COMMAND	NOTES
IGG.CATLOCK	IDCAMS Lock catalogs and access locked catalogs	
IHJ.CHKPT.volser	DFSMS Define checkpoints on shared DASD	
STGADMIN.ADR.CGCREATE	DFSMSdss CGCREATE	
STGADMIN.ADR.CLOUD.FORCE	DFSMSdss FORCE with CLOUDUTILS	
STGADMIN.ADR.CLOUDUTILS	DFSMSdss CLOUDUTILS	
STGADMIN.ADR.CLOUDUTILS.DELETE	DFSMSdss DELETE with CLOUDUTILS	
STGADMIN.ADR.CONOLID	DFSMSdss CONSOLIDATE	
STGADMIN.ADR.CONOLID.FLASHCPY	DFSMSdss FlashCopy with CONSOLIDATE	
STGADMIN.ADR.CONVERTV	DFSMSdss CONVERTV	
STGADMIN.ADR.COPY.BYPASSACS	DFSMSdss BYPASSACS with COPY	
STGADMIN.ADR.COPY.CNCRUNT	DFSMSdss CONCURRENT with COPY	
STGADMIN.ADR.COPY.FCFREEZE	DFSMSdss FCCGFREEZE with COPY	
STGADMIN.ADR.COPY.FCFRR	DFSMSdss FCFASTREVERSERESTORE with COPY	
STGADMIN.ADR.COPY.FCSETGT	DFSMSdss FCSETGTOK	
STGADMIN.ADR.COPY.FCTOPPRCP	DFSMSdss FCTOPPRCPPRIMARY with COPY	
STGADMIN.ADR.COPY.FCTOXRCP	DFSMSdss - FCTOXRCPPRIMARY with COPY	
STGADMIN.ADR.COPY.FLASHCPY	DFSMSdss FlashCopy with COPY	
STGADMIN.ADR.COPY.INCAT	DFSMSdss INCAT with COPY	
STGADMIN.ADR.COPY.PROCESS.SYS	DFSMSdss PROCESS with COPY for SYS1 datasets	
STGADMIN.ADR.COPY.TOLERATE.ENQF	DFSMSdss TOLERATE(ENQF) with COPY	
STGADMIN.ADR.DEFRAG	DFSMSdss DEFRAG	
STGADMIN.ADR.DEFRAG.FCTOPPRCP	DFSMSdss FCTOPPRCPPRIMARY with DEFRAG	
STGADMIN.ADR.DEFRAG.FLASHCPY	DFSMSdss FlashCopy with DEFRAG	
STGADMIN.ADR.DUMP.CLOUD	DFSMSdss CLOUD with DUMP	
STGADMIN.ADR.DUMP.CNCRUNT	DFSMSdss CONCURRENT with DUMP	
STGADMIN.ADR.DUMP.INCAT	DFSMSdss INCAT with DUMP	
STGADMIN.ADR.DUMP.PROCESS.SYS	DFSMSdss PROCESS with DUMP for SYS1 datasets	
STGADMIN.ADR.DUMP.RESET	DFSMSdss RESET with DUMP	
STGADMIN.ADR.DUMP.TOLERATE.ENQF	DFSMSdss TOLERATE(ENQF) with DUMP	
STGADMIN.ADR.DUMP.TOLERATE.WRITERS	DFSMSdss TOLERATE(WRITERS) with DUMP	
STGADMIN.ADR.DUMP.ZCOMPRESS	DFSMSdss ZCOMPRESS with DUMP	
STGADMIN.ADR.DUMP.ZCOMPRESS	DFSMSdss ZCOMPRESS with DUMP	
STGADMIN.ADR.PATCH	DFSMS SET PATCH for ADDRSSU	
STGADMIN.ADR.PRINT	DFSMSdss PRINT	
STGADMIN.ADR.PRINT	DFSMSdss PRINT	
STGADMIN.ADR.PRINT.TRACKS	DFSMSdss PRINT with TRACKS	
STGADMIN.ADR.PRINT.TRACKS	DFSMSdss PRINT with TRACKS	
STGADMIN.ADR.RELEASE.INCAT	DFSMSdss INCAT with RELEASE	
STGADMIN.ADR.RELEASE.PROCESS.SYS	DFSMSdss PROCESS with RELEASE for SYS1 datasets	
STGADMIN.ADR.RESTORE.BYPASSACS	DFSMSdss BYPASSACS with RESTORE	
STGADMIN.ADR.RESTORE.CLOUD	DFSMSdss CLOUD with RESTORE	
STGADMIN.ADR.RESTORE.DELCATE	DFSMSdss DELETCATALOGENTRY with RESTORE	
STGADMIN.ADR.RESTORE.IMPORT	DFSMSdss IMPORT with RESTORE	
STGADMIN.ADR.RESTORE.RESET.YES	DFSMSdss RESET(YES) with RESTORE	
STGADMIN.ADR.RESTORE.TOLERATE.ENQF	DFSMSdss TOLERATE(ENQF) with RESTORE	
STGADMIN.ADR.SPACEREL	DFSMSdss SPACEREL	
STGADMIN.ADR.STGADMIN.BUILDSA	DFDSS BUILDSA command with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.COMPRESS	DFSMSdss COMPRESS with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.CONOLID	DFSMSdss CONSOLIDATE with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.COPY	DFSMSdss COPY with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.COPY.DELETE	DFSMSdss COPY DELETE with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.COPY.RENAME	DFSMSdss COPY RENAME with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.DEFRAG	DFSMSdss DEFRAG with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.DUMP	DFSMSdss DUMP with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.DUMP.DELETE	DFSMSdss DUMP DELETE with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.PRINT	DFSMSdss PRINT with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.RELEASE	DFSMSdss RELEASE with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.RESTORE	DFSMSdss RESTORE with ADMINISTRATOR	
STGADMIN.ADR.STGADMIN.RESTORE.RENAME	DFSMSdss RESTORE RENAME with ADMINISTRATOR	
STGADMIN.ALLOW.SMS.PDSE.COMPACT	DFSMS Allow compression of PDSEs	
STGADMIN.ANT.ESFC.COMMANDS	DFSMSdss Enterprise Storage Server FlashCopy commands	
STGADMIN.ANT.ESFC.CQUERY	DFSMSdss Enterprise Storage Server FlashCopy Query	
STGADMIN.ANT.ESS.OBJSTORE	DFSMSdss Use OBJSTORE ILK on the ANTRQST API	
STGADMIN.ANT.ESS.QHA	DFSMSdss QHA Requests	
STGADMIN.ANT.ESS.STATESAVE	DFSMSdss STATESAVE Requests	
STGADMIN.ANT.PPRC.COMMANDS	DFSMSdss Advanced Copy PPRC commands	
STGADMIN.ANT.PPRC.CQUERY	DFSMSdss Advanced Copy PPRC PQUERY requests	
STGADMIN.ANT.PPRC.FENCE	DFSMSdss Advanced Copy PPRC FENCE requests	
STGADMIN.ANT.SNAPSHOT.COMMANDS	DFDMSdss Advanced Copy SNAPSHOT Commands	
STGADMIN.ANT.SNAPSHOT.SQUERY	DFSMSdss Advanced Copy SNAPSHOT Query	
STGADMIN.ANT.XRC.COMMANDS	DFSMSdss Advanced Copy XRC commands	
STGADMIN.ANT.XRC.XQUERY	DFSMSdss Advanced Copy XRC Query	
STGADMIN.ARC.ABACKUP	DFSMSshm ABACKUP command	
STGADMIN.ARC.ABACKUP.agname	DFSMSshm ABACKUP command	
STGADMIN.ARC.ADDVOL	DFSMSshm ADDVOL command	
STGADMIN.ARC.ALTERDS	DFSMSshm ALTERDS command	
STGADMIN.ARC.ALTERPRI	DFSMSshm Prioritize Queued Requests	
STGADMIN.ARC.ARECOVER	DFSMSshm ARECOVER command	
STGADMIN.ARC.ARECOVER.agname	DFSMSshm ARECOVER command	
STGADMIN.ARC.ARECOVER.agname.RENTGT	DFSMSshm ARECOVER command	

RACF Storage Administration Resources

FACILITY PROFILE	STORAGE ADMIN COMPONENT & COMMAND	NOTES
STGADMIN.ARC.ARECOVER.agname.REPLACE	DFSMSHsm ARECOVER command	
STGADMIN.ARC.AUDIT	DFSMSHsm AUDIT command	
STGADMIN.ARC.AUTH	DFSMSHsm AUTH command	
STGADMIN.ARC.BACKDS	DFSMSHsm BACKDS command	
STGADMIN.ARC.BACKDS.DELETE	DFSMSHsm BACKDS command	
STGADMIN.ARC.BACKDS.NEWNAME	DFSMSHsm BACKDS command	
STGADMIN.ARC.BACKDS.RETAINDAYS	DFSMSHsm BACKDS command	
STGADMIN.ARC.BACKVOL	DFSMSHsm BACKVOL command	
STGADMIN.ARC.BDELETE	DFSMSHsm BDELETE command	
STGADMIN.ARC.CANCEL	DFSMSHsm CANCEL command	
STGADMIN.ARC.DEFINE	DFSMSHsm DEFINE command	
STGADMIN.ARC.DELETE	DFSMSHsm DELETE command	
STGADMIN.ARC.DELVOL	DFSMSHsm DELVOL command	
STGADMIN.ARC.DISPLAY	DFSMSHsm DISPLAY command	
STGADMIN.ARC.ENDUSER.HALTERDS	DFSMSHsm HALTERDS command	
STGADMIN.ARC.ENDUSER.HBACKDS	DFSMSHsm HBACKDS command	
STGADMIN.ARC.ENDUSER.HBACKDS.NEWNAME	DFSMSHsm HBACKDS command	
STGADMIN.ARC.ENDUSER.HBACKDS.RETAINDAYS	DFSMSHsm HBACKDS command	
STGADMIN.ARC.ENDUSER.HBACKDS.TARGET	DFSMSHsm HBACKDS command	
STGADMIN.ARC.ENDUSER.HBDELETE	DFSMSHsm HBDELETE command	
STGADMIN.ARC.ENDUSER.HCANCEL	DFSMSHsm HCANCEL command	
STGADMIN.ARC.ENDUSER.HDELETE	DFSMSHsm HDELETE command	
STGADMIN.ARC.ENDUSER.HLIST	DFSMSHsm HLIST command	
STGADMIN.ARC.ENDUSER.HMIGRATE	DFSMSHsm HMIGRATE command	
STGADMIN.ARC.ENDUSER.HMIGRATE.CLOUD	DFSMSHsm HMIGRATE command with CLOUD	
STGADMIN.ARC.ENDUSER.HQUERY	DFSMSHsm HQUERY command	
STGADMIN.ARC.ENDUSER.HRECALL	DFSMSHsm HRECALL command	
STGADMIN.ARC.ENDUSER.HRECOVER	DFSMSHsm HRECOVER command	
STGADMIN.ARC.EXPIREBV	DFSMSHsm EXPIREBV command	
STGADMIN.ARC.FB.cpname	DFSMSHsm FRBACKUP command	
STGADMIN.ARC.FD.cpname	DFSMSHsm FRDELETE command	
STGADMIN.ARC.FIXCDS	DFSMSHsm FIXCDS command	
STGADMIN.ARC.FIXCDS.DISPLAY	DFSMSHsm FIXCDS command DISPLAY keyword	
STGADMIN.ARC.FR.cpname	DFSMSHsm FRRECOV command	
STGADMIN.ARC.FR.NEWNAME	DFSMSHsm FRRECOV command	
STGADMIN.ARC.FREEVOL	DFSMSHsm FREEVOL command	
STGADMIN.ARC.HOLD	DFSMSHsm HOLD command	
STGADMIN.ARC.LC.cpname	DFSMSHsm LIST with COPYPOOL	5
STGADMIN.ARC.LIST	DFSMSHsm LIST command	
STGADMIN.ARC.LOG	DFSMSHsm LOG command	
STGADMIN.ARC.MIGRATE	DFSMSHsm MIGRATE command	
STGADMIN.ARC.PATCH	DFSMSHsm PATCH command	
STGADMIN.ARC.QUERY	DFSMSHsm QUERY command	
STGADMIN.ARC.RECALL	DFSMSHsm RECALL command	
STGADMIN.ARC.RECOVER	DFSMSHsm RECOVER command	
STGADMIN.ARC.RECOVER.NEWNAME	DFSMSHsm RECOVER command with NEWNAME	
STGADMIN.ARC.RECYCLE	DFSMSHsm RECYCLE command	
STGADMIN.ARC.RELEASE	DFSMSHsm RELEASE command	
STGADMIN.ARC.REPORT	DFSMSHsm REPORT command	
STGADMIN.ARC.SETMIG	DFSMSHsm SETMIG command	
STGADMIN.ARC.SETSYS	DFSMSHsm SETSYS command	
STGADMIN.ARC.STOP	DFSMSHsm STOP command	
STGADMIN.ARC.SWAPLOG	DFSMSHsm SWAPLOG command	
STGADMIN.ARC.TAPECOPY	DFSMSHsm TAPECOPY command	
STGADMIN.ARC.TAPEREP	DFSMSHsm TAPEREP command	
STGADMIN.ARC.TRAP	DFSMSHsm TRAP command	
STGADMIN.ARC.UPDATEC	DFSMSHsm UPDATEC command	
STGADMIN.ARC.UPDTCDS	DFSMSHsm UPDTCDS command	
STGADMIN.DMO.CONFIG	DFSMSopt BUILDIX command for Rapid Index Rebuild	
STGADMIN.DMS.STGADMIN	CA-Disk Storage Administration	
STGADMIN.DMS.STGADMIN.\$AUTORES	CA-DISK Storage Administration Command \$AUTORES	
STGADMIN.DMS.STGADMIN.ARCHDUMP	CA-DISK Storage Administration Command ARCHDUMP	
STGADMIN.DMS.STGADMIN.ARCHIVE	CA-DISK Storage Administration Command ARCHIVE	
STGADMIN.DMS.STGADMIN.ARCHIVE.NEWHLQ	CA-DISK Storage Administration Command ARCHIVE.NEWHLQ	
STGADMIN.DMS.STGADMIN.ARCHIVE.NEWNAME	CA-DISK Storage Administration Command ARCHIVE.NEWNAME	
STGADMIN.DMS.STGADMIN.BACKUP	CA-DISK Storage Administration Command BACKUP	
STGADMIN.DMS.STGADMIN.BACKUP.NEWHLQ	CA-DISK Storage Administration Command BACKUP.NEWHLQ	
STGADMIN.DMS.STGADMIN.BACKUP.NEWNAME	CA-DISK Storage Administration Command BACKUP.NEWNAME	
STGADMIN.DMS.STGADMIN.BACKUPCC	CA-DISK Storage Administration Command BACKUPCC	
STGADMIN.DMS.STGADMIN.BILLING	CA-DISK Storage Administration Command BILLING	
STGADMIN.DMS.STGADMIN.COMPRESS	CA-DISK Storage Administration Command COMPRESS	
STGADMIN.DMS.STGADMIN.COPY	CA-DISK Storage Administration Command COPY	
STGADMIN.DMS.STGADMIN.COPY.NEWNAME	CA-DISK Storage Administration Command COPY.NEWNAME	
STGADMIN.DMS.STGADMIN.DBACKUP	CA-DISK Storage Administration Command DBACKUP	
STGADMIN.DMS.STGADMIN.DEL3435	CA-DISK Storage Administration Command DEL3435	
STGADMIN.DMS.STGADMIN.DELETE	CA-DISK Storage Administration Command DELETE	
STGADMIN.DMS.STGADMIN.DERASE	CA-DISK Storage Administration Command DERASE	
STGADMIN.DMS.STGADMIN.DISPOSEA	CA-DISK Storage Administration Command DISPOSEA	
STGADMIN.DMS.STGADMIN.DISPOSER	CA-DISK Storage Administration Command DISPOSER	
STGADMIN.DMS.STGADMIN.DRESTORE	CA-DISK Storage Administration Command DRESTORE	

RACF Storage Administration Resources

FACILITY PROFILE	STORAGE ADMIN COMPONENT & COMMAND	NOTES
STGADMIN.DMS.STGADMIN.DRESTORE.\$AUTORES	CA-DISK Storage Administration Command DRESTORE.\$AUTORES	
STGADMIN.DMS.STGADMIN.DRESTORE.DNAME	CA-DISK Storage Administration Command DRESTORE.DNAME	
STGADMIN.DMS.STGADMIN.DRESTORE.INAME	CA-DISK Storage Administration Command DRESTORE.INAME	
STGADMIN.DMS.STGADMIN.DRESTORE.NEWNAME	CA-DISK Storage Administration Command DRESTORE.NEWNAME	
STGADMIN.DMS.STGADMIN.DSETMAP	CA-DISK Storage Administration Command DSETMAP	
STGADMIN.DMS.STGADMIN.EXPIRE	CA-DISK Storage Administration Command EXPIRE	
STGADMIN.DMS.STGADMIN.ISPF.ADSINDX	CA-DISK Storage Administration Command ISPF.ADSINDX	
STGADMIN.DMS.STGADMIN.ISPF.AQUEUED	CA-DISK Storage Administration Command ISPF.AQUEUED	
STGADMIN.DMS.STGADMIN.ISPF.CDSINDX	CA-DISK Storage Administration Command ISPF.CDSINDX	
STGADMIN.DMS.STGADMIN.ISPF.DDSINDX	CA-DISK Storage Administration Command ISPF.DDSINDX	
STGADMIN.DMS.STGADMIN.ISPF.DQUEUED	CA-DISK Storage Administration Command ISPF.DQUEUED	
STGADMIN.DMS.STGADMIN.ISPF.LDSINDX	CA-DISK Storage Administration Command ISPF.LDSINDX	
STGADMIN.DMS.STGADMIN.ISPF.LQUEUED	CA-DISK Storage Administration Command ISPF.LQUEUED	
STGADMIN.DMS.STGADMIN.IXCATLG	CA-DISK Storage Administration Command IXCATLG	
STGADMIN.DMS.STGADMIN.IXMAINT	CA-DISK Storage Administration Command IXMAINT	
STGADMIN.DMS.STGADMIN.IXUPDATE	CA-DISK Storage Administration Command IXUPDATE	
STGADMIN.DMS.STGADMIN.LOADLIB	CA-DISK Storage Administration Command LOADLIB	
STGADMIN.DMS.STGADMIN.MIGRATE	CA-DISK Storage Administration Command MIGRATE	
STGADMIN.DMS.STGADMIN.MOVE	CA-DISK Storage Administration Command MOVE	
STGADMIN.DMS.STGADMIN.RECOVER	CA-DISK Storage Administration Command RECOVER	
STGADMIN.DMS.STGADMIN.RECOVER.NEWHLQ	CA-DISK Storage Administration Command RECOVER.NEWHLQ	
STGADMIN.DMS.STGADMIN.RELEASE	CA-DISK Storage Administration Command RELEASE	
STGADMIN.DMS.STGADMIN.REPARCH	CA-DISK Storage Administration Command REPARCH	
STGADMIN.DMS.STGADMIN.REPORT	CA-DISK Storage Administration Command REPORT	
STGADMIN.DMS.STGADMIN.REPTAPE	CA-DISK Storage Administration Command REPTAPE	
STGADMIN.DMS.STGADMIN.RESTORE	CA-DISK Storage Administration Command RESTORE	
STGADMIN.DMS.STGADMIN.RESTORE.\$AUTORES	CA-DISK Storage Administration Command RESTORE.\$AUTORES	
STGADMIN.DMS.STGADMIN.RESTORE.DNAME	CA-DISK Storage Administration Command RESTORE.DNAME	
STGADMIN.DMS.STGADMIN.RESTORE.INAME	CA-DISK Storage Administration Command RESTORE.INAME	
STGADMIN.DMS.STGADMIN.RESTORE.NEWNAME	CA-DISK Storage Administration Command RESTORE.NEWNAME	
STGADMIN.DMS.STGADMIN.SEQMIG	CA-DISK Storage Administration Command SEQMIG	
STGADMIN.DMS.STGADMIN.VBACKUP	CA-DISK Storage Administration Command VBACKUP	
STGADMIN.DMS.STGADMIN.VRECOVER	CA-DISK Storage Administration Command VRECOVER	
STGADMIN.DMS.STGADMIN.VREPORT	CA-DISK Storage Administration Command VREPORT	
STGADMIN.DMS.STGADMIN.XCOPY	CA-DISK Storage Administration Command XCOPY	
STGADMIN.DPDSRN.currentdsname	IDCAMS rename non-SMS while in use	
STGADMIN.EDG.ACTIONS.action	DFSMSrmm Setting of Release Actions	
STGADMIN.EDG.AV.status.volser	DFSMSrmm Setting of Volume Status	
STGADMIN.EDG.CD.COPYFROM.dsname	DFSMSrmm Copy dataset attributed from one dataset to another	1
STGADMIN.EDG.CD.VX	DFSMSrmm Override VRSEL processing for a dataset	1
STGADMIN.EDG.CMOVE.ALL.ALL	DFSMSrmm Confirm global with subcommand CV CMOVE (ALL,ALL)	
STGADMIN.EDG.CMOVE.location.destination	DFSMSrmm Confirmation of moves and ejects.	
STGADMIN.EDG.CRLSE.action	DFSMSrmm Confirmation of Release Actions	
STGADMIN.EDG.CV.HOLD.volser	DFSMSrmm setting volume HOLD attribte	2
STGADMIN.EDG.CV.NOHOLD.volser	DFSMSrmm removing volume HOLD attribte	2
STGADMIN.EDG.CV.RM	DFSMSrmm Update volume retention attributes	2
STGADMIN.EDG.DV.SCRATCH.volser	DFSMSrmm Deletion of Scratch Volumes	
STGADMIN.EDG.EDGUPDT.UPDATE	DFSMSrmm EDGUPDT utility UPDATE function	
STGADMIN.EDG.FORCE	DFSMSrmm adding or deleting datasets	
STGADMIN.EDG.HOUSEKEEP	DFSMSrmm inventory management	
STGADMIN.EDG.HOUSEKEEP.RPTEXT	DFSMSrmm inventory management extract	
STGADMIN.EDG.IGNORE.TAPE.NORMM.volser	DFSMSrmm volume serial	
STGADMIN.EDG.IGNORE.TAPE.RMM.volser	DFSMSrmm volume serial	
STGADMIN.EDG.IGNORE.TAPE.volser	DFSMSrmm volume serial	
STGADMIN.EDG.INERS.WRONGLABEL	DFSMSrmm wrong label processing	
STGADMIN.EDG.INIT	DFSMSrmm Setting of INIT Action	
STGADMIN.EDG.LABEL.volser	DFSMSrmm tape labels	
STGADMIN.EDG.LIST	DFSMSrmm LIST command	
STGADMIN.EDG.LISTCONTROL	DFSMSrmm LISTCONTROL command	
STGADMIN.EDG.MASTER	DFSMSrmm control dataset access	
STGADMIN.EDG.MOVES.location.destination	DFSMSrmm Initiation of Moves and Ejects	
STGADMIN.EDG.NOLABEL.volser	DFSMSrmm unlabeled tapes	
STGADMIN.EDG.OPERATOR	DFSMSrmm initialize and erase	
STGADMIN.EDG.OWNER.userid	DFSMSrmm owned resources	
STGADMIN.EDG.RELEASE	DFSMSrmm DELETEVOLUME command	
STGADMIN.EDG.RESET.SSI	DFSMSrmm RESET facility	
STGADMIN.EDG.VRS	DFSMSrmm vital records	
STGADMIN.ICK.ANALYZE	ICKDSF ANALYZE command	
STGADMIN.ICK.BUILDIX	ICKDSF BUILDIX command	
STGADMIN.ICK.CONTROL	ICKDSF CONTROL command	
STGADMIN.ICK.CPVOLUME	ICKDSF CPVOLUME command	
STGADMIN.ICK.FLASHCPY	ICKDSF FLASHCOPY command	
STGADMIN.ICK.INIT	ICKDSF INIT command	
STGADMIN.ICK.INSPECT	ICKDSF INSPECT command	
STGADMIN.ICK.INSTALL	ICKDSF INSTALL command	
STGADMIN.ICK.IODELAY	ICKDSF IODELAY command	
STGADMIN.ICK.PPRCOPY	ICKDSF PPRCOPY command	
STGADMIN.ICK.REFORMAT	ICKDSF REFORMAT command	
STGADMIN.ICK.REVAL	ICKDSF REVAL command	
STGADMIN.ICK.TRKFMT	ICKDSF TRKFMT command	

RACF Storage Administration Resources

FACILITY PROFILE	STORAGE ADMIN COMPONENT & COMMAND	NOTES
STGADMIN.IDC.BINDDATA	IDCAMS BINDDATA command	
STGADMIN.IDC.DCOLLECT	IDCAMS DCOLLECT command	
STGADMIN.IDC.DCOLLECT. <i>exitname</i>	IDCAMS DCOLLECT command - invoke exit	
STGADMIN.IDC.DIAGNOSE.CATALOG	IDCAMS DIAGNOSE command against catalogs	
STGADMIN.IDC.DIAGNOSE.VVDS	IDCAMS DIAGNOSE command against VVDS	
STGADMIN.IDC.EXAMINE.DATASET	IDCAMS EXAMINE command	
STGADMIN.IDC.LISTDATA	IDCAMS LISTDATA command	
STGADMIN.IDC.LISTDATA.ACCESSCODE	IDCAMS LISTDATA ACCESSCODE command	
STGADMIN.IDC.SETCACHE	IDCAMS SETCACHE command	
STGADMIN.IDC.SETCACHE.DISCARDPINNED	IDCAMS SETCACHE DISCARDPINNED command	
STGADMIN.IDC.SETCACHE.PENDINGOFF	IDCAMS SETCACHE PENDINGOFF command	
STGADMIN.IDC.SETCACHE.REINITIALIZE	IDCAMS SETCACHE REINITIALIZE command	
STGADMIN.IDC.SETCACHE.SUBSYSTEM	IDCAMS SETCACHE SUBSYSTEM command	
STGADMIN.IFG.READVTOC.volser	DFSMSdftp access to VTOC or VTOC index when MLSNAMES active	
STGADMIN.IGD.ACTIVATE.CONFIGURATION	DFSMS activate SMS configuration	
STGADMIN.IGG.ALTER.SMS	DFSMSdftp alter storage and management class	6
STGADMIN.IGG.ALTER.UNCONVRT	DFSMSdftp make VSAM dataset unmanaged	
STGADMIN.IGG.CATALOG.SECURITY.BOTH	DFSMSdftp Requires ALTER to VSAM Cluster if defining a path or alt index	
STGADMIN.IGG.CATALOG.SECURITY.CHANGE	DFSMSdftp Define alt name, path, or alt index without ALTER dataset access	
STGADMIN.IGG.DEFDEL.UALIAS	DFSMSdftp delete alias	3,4
STGADMIN.IGG.DEFDEL.RECAT	DFSMSdftp define recatalog datasets being merged to target catalog	3,4,7
STGADMIN.IGG.DEFNVSAM.NOBCS	DFSMSdftp define nonvsam with no BCS entry	3
STGADMIN.IGG.DEFNVSAM.NONVR	DFSMSdftp define nonvsam with no VVDS entry	3
STGADMIN.IGG.DELAUDIT.catalogname	DFSMSdftp Allow deleting of datasets cataloged in specified catalogname	8
STGADMIN.IGG.DELETE.NOSCRATCH	DFSMSdftp uncatalog but no scratch	3
STGADMIN.IGG.DELETE.RENAME	DFSMSdftp delete datasets flagged as rename in process	4
STGADMIN.IGG.DELGDG.FORCE	DFSMSdftp DELETE FORCE on gdg	3
STGADMIN.IGG.DELGDG.RECOVERY	IDCAMS delete GDG catalog entries	3
STGADMIN.IGG.DELNVR.NOBCSCHK	DFSMSdftp delete nonvsam NVR with no BCS check	3,4
STGADMIN.IGG.DIRCAT	DFSMSdftp direct request to specific catalog	3
STGADMIN.IGG.DLVVRNVR.NOCAT	DFSMSdftp delete VVR or NVR with no catalog	
STGADMIN.IGG.LIBRARY	DFSMSdftp manage volume entries in tape library	3
STGADMIN.IGWSHCDS.REPAIR	IDCAMS SHCDS functions (READ=List functions; UPDATE=Repair functions)	
STGADMIN.SMS.ALLOW.DATASET.ENCRYPT	DFSMS Allows use of Prevasive Encryption to encrypt dataset	
STGADMIN.SMS.ALLOW.DATASET.SEQ.ENCRYPT	DFSMS Allow encryption for basis and large format data sets	
STGADMIN.SMS.ALLOW.PDSE.ENCRYPT	DFSMS Allow encryption for PDSEs	
STGADMIN.SMS.DADSM.UNMAP.PREFER	DFSMS DADSM UNMAP prevents access to delete dataset residual data	
STGADMIN.SMS.DISPLAY.ZHYPERLINK	DFSMS Allow use of D SMS,DSNAME,ZHL command	
STGADMIN.SMS.FAIL.INVALID.DSNTYPE.ENC	DFSMS Allows creation of unencrypted dataset if encryption fails	
STGADMIN.SMS.VARY.ZHYPERLINK	DFSMS Allow use of V SMS,DSNAME,ZHLWRITE=,ZHLREAD= command	
Obsolete - No Longer Used:		
STGADMIN.IGG.ALTBCS	DFSMSdftp alter BCS catalog attributes (Obsolete as of z/OS 1.9)	
STGADMIN.ARC.FRBACKUP	DFSMSshm FRBACKUP command (Obsolete as of z/OS 1.8)	
STGADMIN.ARC.FRBACKUP.cpname	DFSMSshm FRBACKUP command (Obsolete as of z/OS 1.8)	
STGADMIN.ARC.FRDELETE	DFSMSshm FRDELETE command (Obsolete as of z/OS 1.8)	
STGADMIN.ARC.FRDELETE.cpname	DFSMSshm FRDELETE command (Obsolete as of z/OS 1.8)	
STGADMIN.ARC.FRRECOV	DFSMSshm FRRECOV command (Obsolete as of z/OS 1.8)	
STGADMIN.ARC.FRRECOV.cpname	DFSMSshm FRRECOV command (Obsolete as of z/OS 1.8)	
Invalid Resource Name - Manuals to be updated:		
STGADMIN.ADR.DUMP.NEWNAME	DFSMSdss NEWNAMEUNCONDITIONAL with DUMP	
STGADMIN.ADR.DUMP.NEWNAMEU	DFSMSdss NEWNAMEUNCONDITIONAL with DUMP	
Related Products Believed to be Obsolete and No Longer Offered:		
STGADMIN.DFSMSOPT.CANCEL	DFSMSopt HSM Monitor/Tuner CANCEL command	
STGADMIN.DFSMSOPT.GFTMONTR	DFSMSopt HSM Monitor/Tuner application access	
STGADMIN.DFSMSOPT.PROFILE	DFSMSopt updates to HSM Monitor/Tuner profile	
STGADMIN.DFSMSOPT.SWAPLOG	DFSMSopt swap HSM Monitor/Tuner logs	
STGADMIN.HMT.CANCEL	DFSMSshm StorWatch HSM Monitor CANCEL command	
STGADMIN.HMT.GFTMONTR	DFSMSshm StorWatch HSM Monitor application access	
STGADMIN.HMT.PROFILE	DFSMSshm Change and Store a StorWatch HSM Monitor	
STGADMIN.HMT.SWAPLOG	DFSMSshm Swap StorWatch HSM Monitor logs	
NOTES:		
1 - To protect this resource, a Generic profile must minimally start with 'STGADMIN.EDG.CD'		
2 - To protect this resource, a Generic profile must minimally start with 'STGADMIN.EDG.Cv'		
3 - Not checked if caller is using a system key or running in supervisor state		
4 - Checked with RACROUTE option LOG=NONE		
5 - For LIST COPYPOOL, checked when a copypool name is specified; otherwise, STGADMIN.ARC.LIST is checked		
6 - Requires ALTER access to dataset whose storage or management class is to be changed		
7 - Requires ALTER to source/target catalog for REPRO MERGECAT; requires UPDATE to target catalog for DEFINE RECATALOG		
8 - Class XFACILIT		