

What Security Access is Really Required to Perform My Job as Storage Administrator?

Janet Sun

jlsun@pacbell.net

Frank McCune

fmccune@us.ibm.com

Agenda

- Security roles
- SAF & RACF Facility classes
- Typical Storage Administrator tasks
- DFSMShsm task protection
- DFSMSdss task protection
- ISMF function protection
- Catalog & IDCAMS function protection



Let's Get Started!

Stating the Obvious

- Security is (and always should be) a primary concern in any organization
- Ideally only allow enough access for the user to be able to perform their function effectively
- Setup security access in such a way that tweaks do not always require major paperwork
 - Effectively integrate new products or processes without major upheaval
- Nowadays, beware of the internal hacker





A Storage Admin's typical day

- Backup and Recover data sets
- Move data sets from one volume to another
- Full disk volume functions
- Copy data sets to a new name
- Report on data sets and environment
- Resize data sets
- Make changes to SMS constructs

What access does the Storage Admin need to perform these tasks?

The End Goal

- “Administrators need to treat data like CARGO, and should not need to access the information contained in the data set”



Traditional Methods – Data Set Level Access

- Grant **ALTER** access to all data sets in the environment?
 - Allows access to data set contents
 - Requires maintaining a large number of access lists
 - Missing profile access could hinder work
 - Auditors will not probably not like this level of access to all data sets
 - Impractical

Traditional Methods – OPERATIONS Attribute

- Allows access to most storage admin functions
- Also allows access to data sets and DASDVOL
- SETROPTS OPERAUDIT can be used to audit users
- OPERATIONS will allow access as long as no access list counteracts it
 - For example, ALTER access required but Storage Admin is defined with READ access
- Need is reduced through the use of facility classes
- This is what we are trying to avoid

Enter the RACF Facility Class

- Calls are made using System Authorization Facility (SAF)
 - CA-Top Secret and CA-ACF2 support SAF calls
- Security Administrators using other products generally know how to translate rules for their environment
- The examples provided are based on RACF definitions
 - Not every individual profile is described in this presentation
- Assumes Enhanced Generic Naming is in use
 - For example, dataset.**

RACF Facility Class

- Referenced when an action takes place
- Typically used by program products or components
- Commands for Facility Classes

```
SETROPTS RACLIST(FACILITY)
```

```
RDEFINE FACILITY STGADMIN.x.y.z UACC(NONE)
```

```
PERMIT STGADMIN.x.y.z CLASS(FACILITY) USER(userid) ACCESS(read)
```

```
RALTER FACILITY STGADMIN.x.y.z GLOBALAUDIT(SUCCESS)
```

- For most of the STGADMIN.** profiles, READ access is sufficient

- Profiles for DFSMS functions begin with STGADMIN.**
 - Some vendors also use this format for their checks
- Some examples
 - STGADMIN.IDC.**
 - STGADMIN.IGG.**
 - STGADMIN.ADR.**
 - STGADMIN.ARC.**
 - STGADMIN.EDG.**
 - STGADMIN.IGD.**
 - STGADMIN.ICK.**



DFSMShsm

- DFSMSHsm previously provided rudimentary authorization using the AUTH command
 - Either Storage Admin or End-user
- SAF interface introduced for z/OS DFSMS V1R5
- Allowed more control for user access
- Storage Administrators
 - STGADMIN.ARC.command
- Storage End Users defined differently
 - STGADMIN.ARC.ENDUSER.*
- Described in DFSMSHsm Implementation and Customization Guide

DFSMSHsm Profiles

STGADMIN.**	System level storage administrator command protection. Generic profile provides default access if other DFSMSHsm profiles are not defined
STGADMIN.ARC.**	DFSMSHsm command protection, generic profile for all DFSMSHsm commands
STGADMIN.ARC.command	DFSMSHsm authorized command protection, discrete profile for specific DFSMSHsm authorized command
STGADMIN.ARC.ENDUSER.**	DFSMSHsm end user command protection
STGADMIN.ARC.ENDUSER.h_command	DFSMSHsm end user command protection, discrete profile protects specific DFSMSHsm end user command
STGADMIN.ARC.ENDUSER.h_command.parameter	Discrete profile protects specific DFSMSHsm end user command with specific parameter

- “***STGADMIN.ARC.***** can be used to protect all DFSMShsm authorized commands
 - User or group requires ACCESS(**READ**) to issue command
 - ACCESS(**NONE**) means that user or group can't issue command
- ***STGADMIN.ARC.command*** or ***STGADMIN.ARC.command.parameter*** can be used to restrict the use of any authorized command

- ***STGADMIN.ARC.ENDUSER.***** can be used to protect all DFSMSHsm end user commands
 - User or group requires ACCESS(**READ**) to issue command
 - ACCESS(**NONE**) means that user or group can't issue command
- ***STGADMIN.ARC.ENDUSER.h_command*** or ***STGADMIN.ARC.ENDUSER.h_command.parameter*** can be used to restrict the use of any end user command
- The use of end user commands will also require RACF authorization to data sets for:
 - HDELETE, HMIGRATE, HRECALL, HRECOVER, HBDELETE, HLIST, or HQUERY

Migration of Data Sets by Storage Admin

- Migration of data sets from volume
- Requires **READ** access to profile STGADMIN.ARC.MIGRATE
 - Does not check data set level access
- Can be performed by
 - Volume (single-threaded)
 - HSEND MIGRATE VOLUME(SMS001)
 - Can also be used for transition processing only (z/OS V2R2)
 - Data set name (single-threaded)
 - HSEND MIGRATE DATASETNAME(XXX.YYY.ZZZ)
 - Must be fully qualified
 - XXX.** not allowed

Migration of Data Sets by Storage Admin

- Storage group name (multiple tasks)
 - MIGRATE STORAGEGROUP(sgname)
 - MIGRATIONONLY (do not process for class transition)
 - TRANSITIONONLY does not migrate data sets
- Example
 - HSEND MIGRATE STORAGEGROUP(SGLRG,SGSML) MIGRATIONONLY
 - Volumes will be processed up to number of migrationtasks
 - No transition processing will take place

Recall of HSM Migrated Data Sets

- Recall data sets from Migration Level 1 or 2
 - HSEND RECALL xxx.yyy.zzz
 - Requires **READ** access to STGADMIN.ARC.RECALL
- Recall of data sets using HRECALL
 - HRECALL XXX.YYY.ZZZ
 - Requires **READ** access to STGADMIN.ARC.ENDUSER.HRECALL
 - Requires **EXECUTE** access to data set profile

Backing Up Volumes or Storage Groups

- Requires **READ** access to STGADMIN.ARC.BACKVOL
- Backup Volumes
 - HSEND BACKVOL VOLUMES(VOL001,VOL002) INCREMENTAL
 - Backup changed data sets on a volume
 - INCREMENTAL is the default value
- Backup Storage Group
 - HSEND BACKVOL STORAGEGROUP(SG001) TOTAL
 - Backup up all data sets on volumes in the storage group

Recover of Data Sets From HSM Backup

- Recover data sets from backup with original name
 - HSEND RECOVER xxx.yyy.zzz
 - Requires **READ** access to STGADMIN.ARC.RECOVER
- Recover data sets from backup using a NEWNAME
 - HSEND RECOVER XXX.YYY.ZZZ + NEWNAME(AAA.BBB.CCC)
 - Requires **READ** access to STGADMIN.ARC.RECOVER.NEWNAME

Recover of Data Sets Using NEWNAME

- Some sites restrict access to HRECOVER for their users
 - They would like to review recovery of backups when requested by applications
 - Especially when using NEWNAME
- Also restrict use of HBDELETE
 - Ensure that needed data set backup copies are not deleted
- In both cases access would be **NONE** for general users
 - STGADMIN.ARC.ENDUSER.HRECOVER
 - STGADMIN.ARC.ENDUSER.HBDELETE



DFSMdss

DFSMSdss for Storage Administrators

- DFSMSdss allows for Storage Administrators to process data (“CARGO”) without individual data set checking
- RACF Facility Class must be active
- Facility Class Profiles must be defined
 - STGADMIN.ADR.STGADMIN.** command
- Userid must have **READ** access to profile
 - Generally, end users should not need access to ADMIN
- Userid must specify ADMIN keyword on batch job

```
COPY DATASET(INCLUDE(MYDATSET)) -  
  LOGINDDNAME(DASD1) OUTDDNAME(DASD2)  
DELETE CATALOG ADMIN
```

DFSMSdss for Storage Administrators

- ADMIN functions protected using profiles
 - Compress
 - Consolidate
 - Copy
 - Defrag
 - Dump
 - Print
 - Release
 - Restore

DFSMSdss COPY Command

- Use ADMIN option to perform copy
- Needs **READ** access to STGADMIN.ADR.STGADMIN.COPY to perform basic copy
 - Needs additional profile access if DELETE or RENAME are used
 - **READ** access to
 - STGADMIN.ADR.STGADMIN.COPY.DELETE
 - STGADMIN.ADR.STGADMIN.COPY.RENAME
- Access check for individual data sets is not performed

```
//PROC      EXEC  PGM=ADRDSSU,REGION=4096K,TIME=10
//SYSPRINT DD   SYSOUT=*
//SYSIN      DD   *
COPY        -
ADMIN        -
DATASET (INCLUDE (P390.XMIT.**)) -
RENAMEU (P390.XMIT.** ,P390.TEST.** ) -
OUTDYNAM (SMS001)
```

DFSMSdss COPY Command

- If running **without** ADMIN option
- No check is performed on STGADMIN profiles for basic copy functions
 - Needs **READ** access to input data sets
 - Needs **ALTER** access to output/renamed data sets

```
//PROC      EXEC  PGM=ADRDSSU,REGION=4096K,TIME=10
//SYSPRINT DD   SYSOUT=*
//SYSIN      DD   *
COPY        -
DATASET (INCLUDE (P390.XMIT.**)) -
RENAMEU (P390.XMIT.** , P390.TEST.** ) -
OUTDYNAM (SMS001)
/*
```

DFSMSdss CONSOLIDATE command

- Use ADMIN option to perform extent reduction
- Needs **READ** access to STGADMIN.ADR.STGADMIN.CONSolid to perform extent reduction without checking access to data sets

```
//SMS009 EXEC   PGM=ADRDSSU,REGION=5M
//SYSPRINT  DD   SYSOUT=*
//INVOL1    DD   VOL=SER=SMS009,UNIT=3390,DISP=SHR
//SYSIN     DD   *
      CONSOLIDATE -
          PHYSINDDNAME (INVOL1) -
          ADMINISTRATOR -
          WAIT (2,2)
/*
```

DFSMSdss CONSOLIDATE command

- If performed **without** ADMIN function
- Needs **READ** access to STGADMIN.ADR.CONSOLID and will then check for **READ** access to data sets

```
//SMS009 EXEC   PGM=ADRDSSU,REGION=5M
//SYSPRINT  DD   SYSOUT=*
//INVOL1    DD   VOL=SER=SMS009,UNIT=3390,DISP=SHR
//SYSIN      DD   *
      CONSOLIDATE -
          PHYSINDDNAME (INVOL1) -
          WAIT (2,2)
/*
```



ISMF

- Can be used to protect:
 - All or some of ISMF applications
 - ISMF commands
 - ISMF line commands
- Uses RACF program control
 - RACF program task must be active
- Access is controlled via access to module name

- Default load library data set names
 - SYS1.DGTLLIB for DFSMSdfp/ISMF
 - SYS1.DGTLLIB for DFSMSdss/ISMF
 - SYS1.DFQLLIB for DFSMSHsm
- RDEFINE PROGRAM `mod-name OWNER(ownerid) + UACC(NONE)`
`ADDMEM(' load.dsn/volser/NOPADCHK)`
- Make sure that PROGRAM CONTROL WHEN(PROGRAM) is active

ISMF Disabling User Mode Changes

- RDEFINE PROGRAM **DGTFPF05** OWNER(**xxxx**) UACC(NONE) + ADDMEM('SYS1.DGTLLIB'/NOPADCHK)
- SETROPTS WHEN(PROGRAM) REFRESH
- Violation

```
CSV025I PROGRAM CONTROLLED MODULE DGTFPF05 NOT ACCESSED, USER UNAUTHORIZED  
CSV025I PROGRAM CONTROLLED MODULE DGTFPF05 NOT ACCESSED, USER UNAUTHORIZED  
***
```

- Using module name DGTFMD01 disables access to ISMF



Catalog & IDCAMS

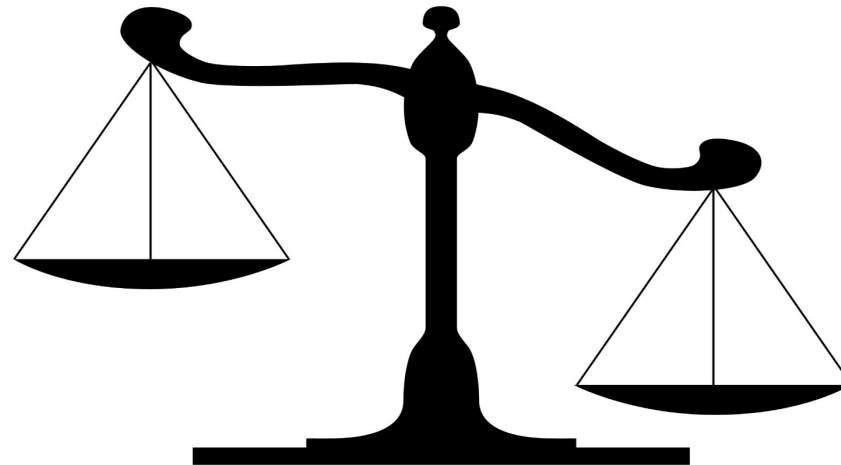
The Catalog Administrator

- Catalog Administrators need to:
 - Perform Backup and Recovery of Catalogs
 - Maintain Catalogs
 - Reorg
 - Split
 - Diagnostics
 - Interact with the Catalog Environment
 - Modify Commands



The Catalog Administrator

- In an SMS environment, the catalog is part of a data set's identity
- All SMS managed data must be cataloged
- Authority to the Catalog assumes authority to the data set and vice versa in cases
- *The administrator needs a high level of authority to do his/her job... the administrator does not need access to everyone's data*



IGG.CATLOCK protects the ability to LOCK / SUSPEND and UNLOCK / RESUME a user catalog. This is vital for any catalog maintenance activity

User's with READ authority to this FACILITY class are also allowed to access the catalog while LOCKed or SUSPENDed

```
SETROPTS CLASSACT(FACILITY)
RDEFINE FACILITY IGG.CATLOCK UACC(NONE)
PERMIT IGG.CATLOCK CLASS(FACILITY) ID(USER1) ACCESS(READ)
```

'User2' is unable to even LISTCAT the LOCKed catalog without IGG.CATLOCK authority

```
CPD: 0 HR 00 MIN 00.00 SEC SRB: 0 HR 00 MIN 00.00 SEC
IDCAMS SYSTEM SERVICES TIME: 15

LISTCAT ENT(FRANK2.SHARECAT) CAT(FRANK2.SHARECAT) ALL
IDCAMS SYSTEM SERVICES TIME: 15

LISTING FROM CATALOG -- FRANK2.SHARECAT

IDC3014I CATALOG ERROR
IDC3009I ** VSAM CATALOG RETURN CODE IS 186 - REASON CODE IS IGGOCLFT-0
IDC1566I ** FRANK2.SHARECAT NOT LISTED
IDCAMS SYSTEM SERVICES TIME: 15
```

Storage Administrator Profiles

- Catalog Storage Administrator profiles follow the naming convention of STGADMIN.IGG.**
- Intended for SMS managed data sets
- Generally, these facility classes are **Restrictive** – restricting the functionality to only those with authority to them
- A few facility classes are **Permissive** – allowing those with authority special abilities

Alter STGADMIN Profiles

STGADMIN.IGG.ALTER.SMS

Protects ability to ALTER a data set's Management or Storage Class

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
ALTER will succeed pending User is otherwise authorized	Unauthorized Users receive a 190-16	Allows admins to ALTER mgmtclas and storclass attributes

```
      ALTER  SHRRAC2,SAMSO,CLUSTE2 MANAGEMENTCLASS(FRANK  )          00070078
IDC2054I INVALID AUTHORIZATION TO EXECUTE FUNCTION
IDC3009I ** VSAM CATALOG RETURN CODE IS 190 - REASON CODE IS IGG0CLFT-16
IDC0532I **ENTRY SHRRAC2,SAMSO,CLUSTE2 NOT ALTERED
IDC0001I FUNCTION COMPLETED, HIGHEST CONDITION CODE WAS 8
```

STGADMIN.IGG.ALTER.UNCONVRT

Protects ability to make an SMS-managed data set unmanaged via DSS CONVERTV

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
Users authorized to DSS CONVERTV can unconvert SMS->NonSMS	Unauthorized Users running CONVERTV NONSMS will fail for SMS volumes containing VSAM data	Allows admins to run DSS CONVERTV NONSMS

Delete & Define STGADMIN Profiles

STGADMIN.IGG.DEFDEL.UALIAS

Protects ability to DEFINE and DELETE User Catalog Aliases in the master catalog
– Permissive facility class

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
UACC(Update) to the master catalog required to define user catalog aliases	Requires UPDATE authority to master catalog to define aliases	allows admin to bypass need for UPDATE authority to master catalog

STGADMIN.IGG.DIRCAT

Protects ability to bypass Standard Order of Search via CATALOG() parameter

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
Directed catalog requests succeed	Unauthorized users will receive 190-2 for certain catalog functions	Admins can use CATALOG() parm to delete/define/alter entries outside of Standard Order of Search

```
DELETE SHRRAC2.SAMSO.CLUSTE2 CLUSTER -  
CATALOG(SYS1.MVSRES9.MASTCAT)  
IDC2054I INVALID AUTHORIZATION TO EXECUTE FUNCTION  
IDC3009I ** VSAM CATALOG RETURN CODE IS 190 - REASON CODE IS IGGOCLFT-2  
IDC0551I ** ENTRY SHRRAC2.SAMSO.CLUSTE2 NOT DELETED  
IDC0001I FUNCTION COMPLETED, HIGHEST CONDITION CODE WAS 8
```

Delete & Define STGADMIN Profiles

STGADMIN.IGG.DELNVR.NOBCSCHK

Bypasses BCS name checking when executing DELETE – **Permissive** facility class

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
DELETE NONVSAM will 50-88 if NVR catalog name does not match the entry's catalog	DELETE NONVSAM will 50-88 if NVR catalog name does not match the entry's catalog	DELETE NONVSAM will succeed in spite of NVR catalog name reference

```
DELETE SHRRAC.SAMSO.NONVSAM NONVSAM
IDC0550I ENTRY (A) SHRRAC.SAMSO.NONVSAM DELETED
IDC3014I CATALOG ERROR
IDC3009I ** VSAM CATALOG RETURN CODE IS 50 - REASON CODE IS IGG0CLF0-88
IDC0551I ** ENTRY SHRRAC.SAMSO.NONVSAM NOT DELETED
```

STGADMIN.IGG.DLVVRNVR.NOCAT

Protects the ability to DELETE an NVR or VVR without an associated BCS

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
DELETE NVR succeeds whether or not catalog is connected	DELETE NVR will fail if data set's catalog is not connected	DELETE NVR succeeds whether or not catalog is connected

Protecting Catalog Commands

- MVS.MODIFY.STC.CATALOG.CATALOG.SECURE in the OPERCMDS class protects the ability to issue Catalog Modify commands
- Unauthorized issuers receive IEC395I

```
14,58,00          QJMSF100 PRY1          INACTIVE - CLASS=AD  
00- 14,58,33          IEC395I USER IS NOT AUTHORIZED TO PERFORM MODIFY  
- CATALOG COMMAND: F CATALOG,OPEN  
IEEC10T,00-0000500,000000-0500,000-00000000
```

- **READ** allows users to perform reporting modify commands
 - Example: F CATALOG,OPEN; F CATALOG,REPORT,PERFORMANCE
- **UPDATE** allows users to manipulate the Catalog Address Space
 - Example: F CATALOG,CLOSE(catname); F CATALOG,ALIASLEVEL(#)
- RDEFINE OPERCMDS MVS.MODIFY.STC.CATALOG.CATALOG.SECURE UACC (NONE)
- PERMIT MVS.MODIFY.STC.CATALOG.CATALOG.SECURE CLASS (OPERCMDs) +
- ID (USER1) ACCESS (READ)

Perform REPRO MERGECAT Without ALTER Authority to Data Sets

STGADMIN.IGG.DEFINE.RECAT

Removes requirement for ALTER to data set to perform REPRO MERGECAT

– **Permissive** facility class

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
REPRO MERGECAT requires ALTER authority to data sets being moved from catalog A->B because of internal recatalog function	If admin does not have ACC(ALTER) to data sets within the catalog being REPRO'd, mergecat fails	REPRO MERGECAT succeeds with only ACC(ALTER) authority to the source and target catalogs. Admin must also have ACC(READ) to STGADMIN.IGG.DELETE.NOSCRTH

DELETE Non-VSAM Data Sets Flagged as Rename-in-Progress

During the rename process, catalog uses a 'rename-in-progress' flag to ensure entries are not accidentally deleted or accessed during the rename process itself. In rare occasions, the rename can be interrupted leaving this flag on indefinitely

- IDC3009I 90-54 during DELETE
- IDC3009I 100-10 during Generic Locate

DELETE Non-VSAM data sets flagged as Rename-in-Progress

During the rename process, catalog uses a 'rename-in-progress' flag to ensure entries are not accidentally deleted or accessed during the rename process itself. In rare occasions, the rename can be interrupted leaving this flag on indefinitely

- IDC3009I 90-54 during DELETE
- IDC3009I 100-10 during Generic Locate

STGADMIN.IGG.DELETE.RENAME

Bypasses Rename-in-Progress checking – **Permissive** facility class

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
DELETE of data sets with Rename-in-Progress indicator fail with 90-54	DELETE of data sets with Rename-in-Progress indicator fail with 90-54	Data sets successfully deleted

VSAM OPEN Security Changes

Prior to z/OS 3.2, applications running in supervisor state or key 0 could access VSAM data sets on behalf of users even if the user was not explicitly permitted to them. In z/OS 3.2, this will not be allowed unless the applications opens the VSAM data set with **ACBBYPSS** or **JSCBPASS** **explicitly set** or alternatively if the user has authority to **STGADMIN.IGG.AUTO.BYPASS.ALLOW**

- **STGADMIN.IGG.AUTO.BYPASS.LOG** can be used in 3.1 and lower releases to identify what applications have been allowing access via SMF 80 records, that will no longer be supported in 3.2. The goal is to identify these applications and make necessary changes in their Open routines. Otherwise, facilitate users with **STGADMIN.IGG.AUTO.BYPASS.ALLOW** or provide those users with necessary authority to the VSAM data
- <https://www.ibm.com/docs/en/zos/3.2.0?topic=racf-protection-vsam-data-sets>

Questions



z/OS DFSMS Managing Catalogs "[Protecting Catalogs](#)"

z/OS DFSMS Access Method Services Commands "[Security Authorization Levels](#)"

[z/OS Security Server RACF Command Language Reference](#)

What Security Access is Really Required to Perform My Job as Storage Administrator?

Janet Sun

jlsun@pacbell.net

Frank McCune

fmccune@us.ibm.com

BACKUP

HRECOVER of data sets using HSM backup

HRECOVER can also be used to recover backup data sets

HRECOVER 'XXX.YYY.ZZZ'

Requires **READ** access to STGADMIN.ARC.ENDUSER.HRECOVER

Requires **ALTER** access to data set XXX.YYY.ZZZ

HRECOVER to a different data set name

HRECOVER 'XXX.YYY.ZZZ' NEWNAME('AAA.BBB.CCC')

Requires **READ** access to STGADMIN.ARC.ENDUSER.HRECOVER

Requires **READ** access to data set XXX.YYY.ZZZ

Requires **ALTER** access to data set AAA.BBB.CCC

Backing up data sets using HBACKDS

Requires **READ** access to STGADMIN.ARC.ENDUSER.HBACKDS

Requires **UPDATE** access to data set

Backup data sets

HBACKDS 'XXX.**' NOWAIT

Backup data sets beginning with HLQ XXX and do not wait for completion

Backup with RETAINDDAYS

HBACKDS 'XXX.YYY.ZZZ' RETAINDDAYS(60)

Backup up data sets and retain for at least 60 days

Requires **READ** access to STGADMIN.ARC.ENDUSER.BACKUP.RETAINDDAYS

Migration of data sets by Storage Admin

HMIGRATE 'PROD.*.PAYROLL.**' ML2 NOWAIT

Can be used to migrate data set name using masks

Write to Migration Level 2

Must have **READ** access to facility class
STGADMIN.ARC.ENDUSER.HMIGRATE

```
ARC1710E USER ADCDA NOT AUTHORIZED FOR RESOURCE STGADMIN.ARC.ENDUSER.HMIGRATE
ARC1001I P390.AAMTEST.ALLOCPT MIGRATE FAILED, RC=0004, REAS=1710
ARC1604I COMMAND NOT AUTHORIZED FOR USER
ARC1007I MIGRATE REQUEST 00000122 SENT TO DFSMSHSM
***
```

Must also have **UPDATE** access to data set profile

```
ARC1001I P390.AAMTEST.ALLOCPT MIGRATE FAILED, RC=0039, REAS=0008
ARC1239I ERROR PROCESSING RACF PROTECTED DATA SET, MIGRATION TERMINATED
ARC1007I MIGRATE REQUEST 00000123 SENT TO DFSMSHSM
***
```



Catalog functions and their required authority

Protecting Sequential Files

	Authority to the Dataset	AND / OR	Authority to the Catalog	Notes
DEFINE Non-SMS	ALTER	AND	UPDATE	
DEFINE SMS	ALTER		(none)	*If cataloging to Master cat, requires update to Master
DELETE Non-SMS	ALTER		(none)	
DELETE SMS	ALTER	OR	ALTER	
ALTER	ALTER	OR	ALTER	*NEWNAME requires ALTER to the Dataset Name

Protecting VSAM Clusters

	Authority to the Dataset	AND / OR	Authority to the Catalog	Notes
DEFINE KSDS Non-SMS	ALTER	AND	UPDATE	
DEFINE KSDS SMS	ALTER		(none)	
DEFINE KSDS RECATALOG	ALTER	AND	UPDATE	Used during REPRO MERGECAT. With STGADMIN.IGG.DEFINE.RECAT authority, no authority to the data set is require
DELETE KSDS Non-SMS	ALTER	OR	ALTER	* differs from non-vsam
DELETE KSDS SMS	ALTER	OR	ALTER	
ALTER KSDS SMS	ALTER	OR	ALTER	* NEWNAME requires ALTER to the New Dataset name

*Authority is tested against the Cluster name

Protecting GDGs

	Authority to the Dataset	AND / OR	Authority to the Catalog	Notes
DEFINE GDG	ALTER	AND	UPDATE	
DELETE GDG	ALTER	OR	ALTER	
DEFINE GDS Non-SMS	ALTER	AND	UPDATE	Similar to seq file
DEFINE GDS SMS	ALTER		(none)	Similar to seq file
DELETE GDS Non-SMS	ALTER		(none)	Similar to seq file
DELETE GDS SMS	ALTER	OR	ALTER	Similar to seq file

*Authority is tested against the GDG base name

Protecting User Catalogs

	Authority to User Catalog	AND / OR	Authority to the Master Catalog	Notes
DEFINE Usercatalog	ALTER	AND	UPDATE	
DELETE Usercatalog	ALTER		(none)	
ALTER Usercatalog	ALTER	OR	ALTER	Newname inapplicable
DEFINE Alias	(none)		UPDATE	
DELETE Alias	ALTER	OR	ALTER	
Import Connect	ALTER	AND	UPDATE	
Export Disconnect	ALTER		(none)	



More Catalog Facility classes

Delete & Define STGADMIN Profiles

STGADMIN.IGG.DEFNVSAM.NOBCS

Allows non-IDCAMS authorized services to define NVRs with no BCS entry

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
Applications issuing SVC26 can directly define NVRs	Prevents authorized services from defining just NVRs	Allows authorized services to define just NVRs

STGADMIN.IGG.DEFNVSAM.NONVR

Allows non-IDCAMS authorized services to define BCS entries with no NVR

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
Applications issuing SVC26 can directly define BCS entries	Prevents authorized services from defining just BCS entries	Allows authorized services to define just BCS entries

* OAM, HSM, and vendor applications may need authority to these profiles

Delete & Define STGADMIN Profiles

STGADMIN.IGG.DELGDG.FORCE

Protects ability to use DELETE GDG FORCE command which also also deletes active GDSs

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
Users can use DELETE GDG FORCE	Prevents users from mistakenly deleting all active GDSs when deleting GDG with 190-12	Admins can delete the GDG and all active GDSs

```
DELETE SHRRAC,SAMSO,GDG    GDG FORCE
IDC2054I INVALID AUTHORIZATION TO EXECUTE FUNCTION
IDC3009I ** VSAM CATALOG RETURN CODE IS 190 - REASON CODE IS IGGOCLFT-12
IDC0551I ** ENTRY SHRRAC,SAMSO,GDG NOT DELETED
IDC0001I FUNCTION COMPLETED, HIGHEST CONDITION CODE WAS 8
```

STGADMIN.IGG.DELGDG.RECOVERY

Protects ability to use DELETE GDG RECOVERY command which also uncatalogs active GDSs

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
Users can use DELETE GDG RECOVERY	Prevents users from mistakenly deleting GDG with 190-20	Admins can delete the GDG

```
DELETE SHRRAC,SAMSO,GDG    GDG RECOVERY
IDC2054I INVALID AUTHORIZATION TO EXECUTE FUNCTION
IDC3009I ** VSAM CATALOG RETURN CODE IS 190 - REASON CODE IS IGGOCLFT-20
IDC0551I ** ENTRY SHRRAC,SAMSO,GDG NOT DELETED
IDC0001I FUNCTION COMPLETED, HIGHEST CONDITION CODE WAS 8
```

Delete & Define STGADMIN Profiles

STGADMIN.IGG.DELETE.NOSCRATCH Protects the ability to uncatalog data sets

If Not Defined..	If Defined & ACC(NONE).. ACC(READ)
DELETE NOSCRATCH succeeds for Non-VSAM and VSAM	DELETE NOSCRATCH prevented sms data sets with 190-10

```
DELETE SHRRAC,SAMSO,NONVSAM2 NOSCRATCH
IDC2054I INVALID AUTHORIZATION TO EXECUTE FUNCTION
IDC3009I ** VSAM CATALOG RETURN CODE IS 190 - REASON CODE IS IGGOCLFT-10
IDC0551I ** ENTRY SHRRAC,SAMSO,NONVSAM2 NOT DELETED
IDC0001I FUNCTION COMPLETED, HIGHEST CONDITION CODE WAS 8
```

Volcat (TCDB) STGADMIN Profiles

STGADMIN.IGG.LIBRARY

Protects ability to CREATE, DELETE or ALTER tape library and tape volume entries

If Not Defined..	If Defined & ACC(NONE)..	ACC(READ)
Actions towards tape volume catalogs succeed	Attempts to CREATE, DELETE, or ALTER volcat entries will fail with 190-18	Actions towards tape volume catalogs will succeed

```
CREATE VOLUMEENTRY - 00
  (NAME (VDA2883) - 00
    LIBRARYNAME (ATLIB02) - 00
    LOCATION (LIBRARY) - 00
    USEATTRIBUTE (SCRATCH) - 00
    MEDIATYPE (MEDIA7) - 00
    RECORDING (EFMT1)) 00
IDC11902I STORAGEGROUP SET TO DEFAULT OF *SCRATCH*
IDC2054I INVALID AUTHORIZATION TO EXECUTE FUNCTION
IDC3009I ** VSAM CATALOG RETURN CODE IS 190 - REASON CODE IS IGGOCLFT-18
IDC3003I FUNCTION TERMINATED. CONDITION CODE IS 12
```

Access method services provide users access to catalog entries for tape libraries and tape volumes, allowing them to create, alter, list and delete entries residing in the TCDB. However, access method services is used mainly as a recovery tool to repair damaged catalogs and should be used with caution whenever you create, alter, and delete TCDB entries. Incorrect use of this recovery tool can cause database (host, library manager, and tape management) conflicts. For example, IDCAMS ALTER can be used to change the use attribute of a volume in the TCDB but it does not change the library manager's inventory

- z/OS DFSMS OAM Planning, Installation, and Storage Administration Guide for Tape Libraries