#SHAREorg

SHARE
Technology · Connections · Results

# How to Protect the z/OS Storage Environment from Prying Eyes and Still Get Your Work Done

Chris Taylor
IBM Corporation
ctaylor1@us.ibm.com

March 11, 2014
Session Number 15071

SHARE in Anaheim

# Legal Disclaimer

NOTICES AND DISCLAIMERS



Product information and data has been reviewed for accuracy as of the date of initial publication. Product information and data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements and/or changes in the product(s) and/or programs(s) described herein at any time without notice.

References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Consult your local IBM representative or IBM Business Partner for information about the product and services available in your area.

Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectually property rights, may be used instead. It is the user's responsibility to evaluate and verify the operation of any non-IBM product, program or service.

THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted according to the terms and conditions of the agreements (e.g., IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. IBM is not responsible for the performance or interoperability of any non-IBM products discussed herein.

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

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

# Trademarks

**The following are trademarks of the *International Business Machines Corporation:***

**IBM, DFSMS/MVS, DFSMShsm, DFSMSrmm, DFSMSdss, DFSMSopt, DFSMS Optimizer, z/OS, eServer, zSeries, MVS, FlashCopy®**

The information contained in this presentation is distributed on an 'AS IS' basis without any warranty
either expressed or implied, including, but not limited to, the implied warranties of merchantability or fitness for a particular purpose. The use of this information is a customer responsibility and depends on the customer's ability to evaluate and integrate it into the customer's operational environment.

# Session Abstract

Storage Administrators are asked to perform many different tasks in the storage environment that require access to data. However, your auditors need to be assured that this access is limited to processing data and not creating an exposure to personal and restricted information. z/OS and DFSMS provide resource classes that can be used to protect functions and allow authorization to data for specific purposes. The speaker will discuss how use of functions and data can be controlled for various IBM products, including DFSMSdfp, DFSMShsm, DFSMSdss, DFSMSrmm, IDCAMS and others.

# Agenda

- Storage Administration tasks
- Security access challenges
- SAF & RACF Facility classes
- Product definitions
  - DFSMSdfp/IDCAMS
  - DFSMSdss
  - DFSMShsm
  - DFSMSrmm
  - Other products/components

# Thanks to…..

- Help with preparation of this presentation
  - Marty Hasegawa
- Previous presentations on some of the topics
  - Tony Pearson
  - Ed Baker

A computer lets you make more mistakes faster than any invention in human history - with the possible exceptions of handguns and tequila. — Mitch Ratliff

"Companies spend millions of dollars on firewalls, encryption and secure access devices, and it's money wasted, because none of these measures address the weakest link in the security chain."
*– Kevin Mitnick*

In God we trust. All others, we virus scan.

Computers are like Old Testament Gods; lots of rules and no mercy. – Joseph Campbell

The trouble with quotes on the Internet is that you never know if they are genuine. — Benjamin Franklin

# Storage Administrator Tasks

- Storage Admin 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?

# 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

- “Administrators need to treat data like CARGO, and do not need access to information inside”

# Volume level checking

- Allows defined users to perform maintenance tasks without having access to data set profiles
- DASDVOL class in RACF
- Different function keywords might require different access levels
  - DUMP with DELETE vs DUMP without DELETE
- Used as well with ICKDSF and IDCAMS ALTER
- Does not work with SMS volumes
  - Big Problem!
  - Use OPERATIONS instead

# 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.
  - e.g. ALTER access required but Storage Admin is defined with READ access
- Need is reduced through the use of facility classes

# Security Overview

- 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
  - E.g. 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

# STGADMIN.**

- Profiles for DFSMS functions begin with STGADMIN.**
  - Some vendors also use this format for their checks
- Calls are made using System Authorization Facility (SAF)
  - CA-Top Secret and CA-ACF2 support SAF calls
- Some examples
  - STGADMIN.IDC.**
  - STGADMIN.IGG.**
  - STGADMIN.ADR.**
  - STGADMIN.ARC.**
  - STGADMIN.EDG.**
  - STGADMIN.IGD.**
  - STGADMIN.ICK.**

# ISMF protection

- 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

# ISMF protection

- 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)

- See backup charts for detailed information

# DFSMSdfp facility classes

- Protect various functions in ISMF and operator commands
- Limit access to various catalog-related functions
- Protect ALTER function for changing SMS constructs
- Limit access to certain AMS Services functions
- Protect various SETCACHE commands
- Some classes not checked if running in system key or supervisor state
- Recommendation is to set UACC(None) for STGADMIN.**

- Described in z/OS DFSMSdfp Storage Administration
  - SC23-6860-00 for z/OS DFSMS Version 2 Release 1

# DFSMSdfp facility classes

- STGADMIN.IGD.ACTIVATE.CONFIGURATION
  - Controls ability to activate an SMS configuration
- STGADMIN.IGG.ALTER.SMS
  - Allows Storage Class or Management Class to be ALTER'd
- STGADMIN.IGG.LIBRARY
  - DEFINE, DELETE or ALTER library or volume contents
- STGADMIN.IGWSHCDS.REPAIR
  - Limits access to AMS SHCDS function
- STGADMIN.IGG.ALTER.UNCONVRT
  - Controls ability to convert VSAM from SMS to non-managed

# DFSMSdfp facility classes

- STGADMIN.IDC.DCOLLECT
  - Controls ability to use IDCAMS DCOLLECT command
- STGADMIN.DMO.CONFIG
  - Control access to BUILDIX Rapid Rebuild
- STGADMIN.DPDSRN.***olddsname***
  - Controls access to rename non-SMS data set in use
  - Per the manual,
    - Do not grant access to STGADMIN.DPDSRN.*
    - Severely restrict access to STGADMIN.DPDSRN.***olddsname***
    - Can also be performed using Tivoli Advanced Catalog Management
      - ALTER NONVSAM with NOENQ option

# DFSMSdfp facility classes – ICF catalog maintenance

- STGADMIN.IDC.DIAGNOSE.CATALOG
  - Run DIAGNOSE command against catalogs
- STGADMIN.IGG.DIRCAT
  - Direct request to a specific catalog
- STGADMIN.IGG.DELETE.NOSCRATCH
  - Allows an uncatalog or DELETE NOSCRATCH of SMS data set
- STGADMIN.IGG.DELGDG.FORCE
  - DELETE FORCE for GDG base with existing SMS GDSs
- STGADMIN.IGG.DEFDEL.UALIAS
  - DEFINE/DELETE Alias to catalog without additional authority

# DFSMSdfp facility classes – VVDS Maintenance

- STGADMIN.IDC.DIAGNOSE.VVDS
  - DIAGNOSE command against a VVDS
- STGADMIN.IGG.DEFNVSAM.NOBCS
  - Define or alter NVR without affecting BCS entry
- STGADMIN.IGG.DELNVR.NOBCSCHK
  - Delete NVR without checking the BCS entry
- STGADMIN.IGG.DLVVRNVR.NOCAT
  - Delete VVR or NVR without an associated catalog

# DFSMSdfp Generic examples

```
zSecure Admin+Audit for RACF General resource overview
Command ===> _____________________________________________ Scroll===> CSR
Class FACILITY, like STGADMIN.I*.**              4 Mar 2014 14:51
   Class    Profile key                            T UACC     Owner    S/F W
__ FACILITY STGADMIN.IDC.DIAGNOSE.CATALOG            NONE     SYS1      R
__ FACILITY STGADMIN.IDC.DIAGNOSE.VVDS               NONE     SYS1      R
__ FACILITY STGADMIN.IDC.*                         G NONE     IBMUSER   R
__ FACILITY STGADMIN.IDC.**                        G NONE     SYS1      R
__ FACILITY STGADMIN.IGD.*                         G NONE     IBMUSER   R
__ FACILITY STGADMIN.IGG.DELETE.NOSCRTCH             NONE     SYS1      R
__ FACILITY STGADMIN.IGG.LIBRARY                     NONE     SYS1      R
__ FACILITY STGADMIN.IGG.*                         G NONE     IBMUSER   R
****************************** Bottom of Data ********************************
```

# 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
- 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 for Storage Administrators

- DFSMSdss commands can be invoked from ISMF panels
- Protect in a similar way to other DFSMSdfp ISMF functions
  - RACF program checking and module names
- Load library default name is SYS1.DGTLLIB
- See backup slides for list of modules and profile tables

- Definitions can be found in DFSMSdss Storage Administration
  - SC23-6868-00 in z/OS DFSMS V2 R1

# DFSMSdss for Regular Users

- Other DFSMSdss functions can be protected using RACF
- RACF Facility class needs to be active
- Profiles defined as STGADMIN.ADR.**
- Allows protection of DFSMSdss functions and certain keywords

# DFSMSdss for Regular Users

- DUMP function
  - Additional keyword protection for
    - Concurrent copy
      - *STGADMIN.ADR.DUMP.CNCURRNT*
    - INCAT processing
      - *STGADMIN.ADR.DUMP.INCAT*
    - NEWNAMEUNCONDITIONAL
      - *STGADMIN.ADR.DUMP.NEWNAME*
    - Process SYS1 data sets
      - *STGADMIN.ADR.DUMP.PROCESS.SYS*
    - Dump without serialization
      - *STGADMIN.ADR.DUMP.TOLERATE.ENQF*

# DFSMSdss for Regular Users

- COPY function
  - Additional keyword protection for
    - Bypass ACS routines
      - *STGADMIN.ADR.COPY.BYPASSACS*
    - Concurrent copy
      - *STGADMIN.ADR.COPY.CNCURRNT*
    - FCCGFREEZE (Source volume part of FC Consistency Grp)
      - *STGADMIN.ADR.COPY.FCFREEZE*
    - FCFASTREVERSERESTORE
      - *STGADMIN.ADR.COPY.FCFRR*
    - FCSETGTOK
      - *STGADMIN.ADR.COPY.FCSETGT*

# DFSMSdss for Regular Users

- COPY function (cont)
  - Additional keyword protection for
    - FCTOPPRCPRIMARY
      - *STGADMIN.ADR.COPY.FCTOPPRCP*
    - Flashcopy with COPY
      - *STGADMIN.ADR.COPY.FLASHCPY*
    - INCAT with COPY
      - *STGADMIN.ADR.COPY.INCAT*
    - COPY SYS1 data sets
      - *STGADMIN.ADR.COPY.PROCESS.SYS*
    - Bypass serialization
      - *STGADMIN.ADR.COPY.TOLERATE.ENQF*

# DFSMSdss for Regular Users

- RESTORE Function
  - Additional keyword protection for
    - Bypass ACS routines
      - *STGADMIN.ADR.RESTORE.BYPASSACS*
    - Delete catalog entry
      - *STGADMIN.ADR.RESTORE.DELCATE*
    - IMPORT with RESTORE
      - *STGADMIN.ADR.RESTORE.IMPORT*
    - Bypass serialization
      - *STGADMIN.ADR.RESTORE.TOLERATE.ENQF*

# DFSMSdss for Regular Users

- DEFRAG Function
  - Additional keyword protection for
    - Base Defrag function
      - *STGADMIN.ADR.DEFRAG*
    - Flashcopy to Primary PPRC
      - *STGADMIN.ADR.DEFRAG.FCTOPPRCP*
    - Flashcopy use with Defrag
      - *STGADMIN.ADR.DEFRAG.FLASHCPY*

# DFSMSdss for Regular Users

- CONSOLIDATE Function
  - Base Consolidate function
    - *STGADMIN.ADR.CONSOLID*
  - Flashcopy use with Consolidate
    - *STGADMIN.ADR.CONSOLID.FLASHCPY*
- RELEASE Function
  - INCAT with Release
    - *STGADMIN.ADR.RELEASE.INCAT*
  - Release SYS1 data sets
    - *STGADMIN.ADR.RELEASE.PROCESS.SYS*
- Other functions
  - Convert volume to SMS
    - *STGADMIN.ADR.CONVERTV*

# DFSMSdss generic example

```
zSecure Admin+Audit for RACF General resource overview
Command ===> _____________________________________________ Scroll===> CSR
Class FACILITY, like STGADMIN.adr.**            4 Mar 2014 14:55
   Class    Profile key                          T UACC     Owner    S/F W
__ FACILITY STGADMIN.ADR.CONSOLID                  NONE     SYS1      R _
__ FACILITY STGADMIN.ADR.DEFRAG                    NONE     SYS1      R _
__ FACILITY STGADMIN.ADR.DUMP.**                 G NONE     SYS1      R _
__ FACILITY STGADMIN.ADR.*                       G NONE     IBMUSER   R _
****************************** Bottom of Data ********************************
```

# DFSMShsm – Setup steps

- Create userid for DFSMShsm started task
  - Create separate or use same userid if using ABARS
- Associate userid with started task
  - STARTED Class in security system
  - ICHRIN03 table in RACF
- If using DFSMSdss in Cross-memory mode, started tasks can be defined generically
  - RACF example:

```
SETR GENERIC(STARTED)
RDEFINE STARTED ARC*.* STDATA(USER(DFHSM))
SETR RACLIST(STARTED) REFRESH
```

# DFSMShsm – z/OS UNIX Systems Services (USS)

- Backup of zFS or HFS data sets mounted by z/OS UNIX Systems Services
- Needed to quiesce or unquiesce a file system
- 2 methods
  - UPDATE authority to UNIXPRIV SUPERUSER.FILESYS.QUIESCE
  - Defined as a SUPERUSER with OMVS segment and group id(GID)
    - UID(0) HOME('/')

# DFSMShsm for Storage Administrators

- DFSMShsm previously provided rudimentary authorization using 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

| Profile | Function |
|---|---|
| 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 |

# RACF Authorized Commands

- ***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

# RACF Storage Admin command profiles

```
zSecure Admin+Audit for RACF General resource overview
Command ===> _____________________________________________ Scroll===> CSR
Class FACILITY, like stgadmin.arc.*              4 Mar 2014 08:44
   Class    Profile key                              T UACC     Owner    S/F W
__ FACILITY STGADMIN.ARC.BACKVOL                      NONE     SYS1      R  _
__ FACILITY STGADMIN.ARC.DELVOL                       NONE     SYS1      R  _
__ FACILITY STGADMIN.ARC.EXPIREBV                     NONE     SYS1      R  _
__ FACILITY STGADMIN.ARC.**                         G NONE     SYS1      R  _
****************************** Bottom of Data ********************************
```

# RACF End-user commands

- ***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

# RACF End-user command profiles

```
zSecure Admin+Audit for RACF General resource overview
Command ===> _____________________________________________ Scroll===> CSR
Class FACILITY, like stgadmin.arc.enduser.**    4 Mar 2014 08:46
   Class    Profile key                                T UACC    Owner    S/F W
__ FACILITY STGADMIN.ARC.ENDUSER.HBACKDS.RETAINDAYS      NONE    SYS1      R
__ FACILITY STGADMIN.ARC.ENDUSER.HBACKDS.**            G NONE    SYS1      R
__ FACILITY STGADMIN.ARC.ENDUSER.HDELETE                 NONE    SYS1      R
__ FACILITY STGADMIN.ARC.ENDUSER.HRECALL                 NONE    SYS1      R
__ FACILITY STGADMIN.ARC.ENDUSER.HRECOVER                NONE    SYS1      R
__ FACILITY STGADMIN.ARC.ENDUSER.**                    G NONE    SYS1      R
****************************** Bottom of Data ********************************
```

# Data Set Access in DFSMShsm

- HRECALL
  - EXECUTE access to data set being recalled
- HMIGRATE
  - UPDATE access to data set(s) being migrated
- HBACKDS
  - UPDATE access to data set being backed up
- HRECOVER
  - ALTER access, if NEWNAME not being used
  - If NEWNAME is used, READ access to original data set and ALTER access to the new name data set
- HDELETE
  - ALTER access to data set
- HBDELETE
  - ALTER access to data set

# ARCCATGP

- Normally, UNCATALOG, RECATALOG or DELETE NOSCRATCH will cause recall of migrated data set
- MIGRAT catalog entry may point to non-existent MCDS entry
- Connect storage admin userids to group ARCCATGP
- LOGON to system specifying this group
- Following jobcard could also be used

```
//JOBNAME JOB (accounting information),'USERNAME',
//USER=userid,GROUP=ARCCATGP,PASSWORD=password,
// EXEC PGM=….
```

# ARCCATGP Group definition

```
zSecure Admin+Audit for RACF GROUP ARCCATGP Overview
Command ===> _____________________________________________ Scroll===> CSR
like ARCCATGP                                  4 Mar 2014 08:52

_ Identification                                                  SYS1
_ RACF group name                ARCCATGP
_ Superior group                 SYS1
_ Owner                          SYS1
  Installation data              ____________________________________________

  User/Grp Auth     R SOA AG Uacc     Revokedt     Resumedt     Name
_ IBMUSER  USE      _ ___ __ NONE     ____________ ____________
_ LHANNA   USE      _ ___ __ NONE     ____________ ____________ LOUIS
_ P390     USE      _ ___ __ NONE     ____________ ____________ CHRIS


  Safeguards                                 Statistics
  Terminal use authorization     No          Creation date                 21May09
  Universal access authority     NONE        Universal group               No
  Data set model profile name    ____________________________________________
```

# Logon with group ARCCATGP

```
------------------------------- TSO/E LOGON -----------------------------------

   Enter LOGON parameters below:                RACF LOGON parameters:

   Userid    ===> P390

   Password  ===>                               New Password ===>

   Procedure ===> CTPROCAN                      Group Ident  ===> arccatgp

   Acct Nmbr ===> ACCT#

   Size      ===> 2096128

   Perform   ===>

   Command   ===> ispf

   Enter an 'S' before each option desired below:
           -Nomail         -Nonotice       S -Reconnect        -OIDcard

PF1/PF13 ==> Help    PF3/PF15 ==> Logoff    PA1 ==> Attention    PA2 ==> Reshow
You may request specific help information by entering a '?' in any entry field
```

# DFSMSrmm – Setup steps

- Create userid for DFSMSrmm started task
- Associate userid with started task
  - STARTED Class in security system
  - ICHRIN03 table in RACF
- Various DDs require different levels of data set level access
  - EG. Activity, EDGPDOX/Y, Journal, Master, Parmlib
  - Refer to Step 9 in DFSMSrmm Implementation and Customization Guide

# Protecting DFSMSrmm functions

- Generally, users creating tape data sets are the owners and have access to the data
  - COMMANDAUTH parm in EDGRMMxx
- RMM resources are protected by STGADMIN facility class
  - STGADMIN.EDG.**
    - Examples
      - *STGADMIN.EDG.MASTER*
      - *STGADMIN.EDG.RELEASE*
      - *STGADMIN.EDG.INIT*
      - *STGADMIN.EDG.LISTCONTROL*

# Protecting DFSMSrmm functions

- STGADMIN.EDG.MASTER covers access to a number of different RMM functions
- Individual definitions override STGADMIN.EDG.MASTER
  - Some examples
    - LIST
    - LISTCONTROL
    - CHANGEVOLUME
- DFSMSrmm Primer Redbook provides some recommendations
  - Currently available as draft version
  - http://www.redbooks.ibm.com/redpieces/pdfs/sg245983.pdf

# Allowing DFSMShsm access to DFSMSrmm resources

- Allow access to DFSMSrmm scratch tape pool
  - Grant access to the following resources
    - STGADMIN.EDG.MASTER (READ)
    - STGADMIN.EDG.RELEASE(READ)
    - STGADMIN.EDG.OWNER.hsmid (UPDATE)
- If using DFSMShsm-managed tape pools
    - STGADMIN.EDG.MASTER (UPDATE)
    - STGADMIN.EDG.OWNER.hsmid (UPDATE)
- For ABARS
    - STGADMIN.EDG.MASTER (READ)
    - STGADMIN.EDG.RELEASE(READ)
    - STGADMIN.EDG.OWNER.abarsid (UPDATE)

# DEVSUPxx support

- Allows security checking using standard data set profiles
  - No need to define separate tape data set profiles
  - Full 44 character data set name supplied during security call
- DEVSUPxx member in SYS1.PARMLIB
  - TAPEAUTHDSN=YES
- TAPEVOL and TAPEDSN no longer required
- As of z/OS V2R1, DFSMSrmm no longer checks DATASET class with DSTYPE=T
  - RACROUTE now correctly issued as with DASD data sets
  - Used if TAPEAUTHDSN=YES in DEVSUPxx
- For more information, see session 3088 from Share in San Diego, 2007

# Other Components - ICKDSF

- Protected by STGADMIN.ICK.**

| ICKDSF Command | FACILITY Class Profile Name |
|---|---|
| ANALYZE | STGADMIN.ICK.ANALYZE |
| BUILDIX | STGADMIN.ICK.BUILDIX |
| CONTROL | STGADMIN.ICK.CONTROL |
| CPVOLUME | STGADMIN.ICK.CPVOLUME |
| FLASHCOPY | STGADMIN.ICK.FLASHCPY |
| INIT | STGADMIN.ICK.INIT |
| INSPECT | STGADMIN.ICK.INSPECT |
| INSTALL | STGADMIN.ICK.INSTALL |
| IODELAY | STGADMIN.ICK.IODELAY |
| PPRCOPY | STGADMIN.ICK.PPRCOPY |
| REFORMAT | STGADMIN.ICK.REFORMAT |
| REVAL | STGADMIN.ICK.REVAL |
| TRKFMT | STGADMIN.ICK.TRKFMT |

# Others – Advanced Catalog Management

- IBM Tivoli Advanced Catalog Management functions can also be protected
- IBMTIVOLI.ACM.** generic profile
- Some subfunctions check during JCL generation using ISPF dialog
  - ZAP function
- Most functions are checked during batch execution
- Pre-checking is also performed against STGADMIN.IGG when needed
  - Prevents security failure after critical action has taken place
    - i.e. catalog deletion

# Questions?

# Backup slides

# ISMF Application protection

| Application | Module Name |
|---|---|
| Profile | DGTFPF00 |
| Data set | DGTFDS00 |
| DASD Volume | DGTFVA00 |
| Mountable Optical Volume | DGTFOVCD |
| Mountable Tape Volume | DGTFTVCD |
| Management class | DGTFMCCD |
| Data class | DGTFDCCD |
| Storage class | DGTFSCCD |
| Storage group | DGTFSGDR |
| Automatic class selection | DGTFFLAD |
| Control data set | DGTFSACD |
| Aggregate Group | DGTFAGCD |
| Optical Library Configuration | DGTFLCCD |
| Optical Drive Configuration | DGTFRCCD |
| Tape Library Configuration | DGTFLMCD |
| Data Collection | DGTFADAD |
| Report Generation | DGTHMD30 |
| List | DGTFJLCD |
| Copy Pool | DGTFCPCD |

# ISMF Functions protection

| Function | Module Name |
|---|---|
| User mode | DGTFPF05 |
| Logging and abend control | DGTFPF02 |
| ISMF job statement information | DGTFPF03 |
| DFSMSdss execute statement information | DGTFPF04 |
| ICKDSF execute statement information | DGTFPF20 |
| Data set print execute statement information | DGTFPF21 |
| IDCAMS execute statement information | DGTFPF22 |
| | |
| Data Class DEFINE | DGTFDCDA |
| Data Class ALTER | DGTFDCAA |
| Data Class DISPLAY | DGTFDCDI |
| Data Class LIST | DGTFDCLD |
| | |
| Storage Class DEFINE | DGTFSCDA |
| Storage Class ALTER | DGTFSCAA |
| Storage Class DISPLAY | DGTFSCDI |
| Storage Class LIST | DGTFSCLD |

# ISMF Functions protection

| Function | Module Name |
|---|---|
| Management Class DEFINE | DGTFMCDA |
| Management Class ALTER | DGTFMCAA |
| Management Class DISPLAY | DGTFMCDI |
| Management Class LIST | DGTFMCLD |
| | |
| Storage Group DEFINE | DGTFSGFR |
| Storage Group ALTER | DGTFSGAR |
| Storage Group LIST | DGTFSGLD |
| Storage Group VOLUME | DGTFSGVR |
| | |
| Aggregate Group DEFINE | DGTFAGDA |
| Aggregate Group ALTER | DGTFAGAA |
| Aggregate Group DIQPLAY | DGTFAGDI |
| Aggregate Group LIST | DGTFAGLD |

# ISMF Functions protection

| Function | Module Name |
|---|---|
| Optical Library Configuration DEFINE | DGTFLCDE |
| Optical Library Configuration ALTER | DGTFLCAL |
| Optical Library Configuration DISPLAY | DGTFLCDI |
| Optical Library Configuration LIST | DGTFLCLD |
| | |
| Optical Drive Configuration DEFINE | DGTFRCDE |
| Optical Drive Configuration ALTER | DGTFRCAL |
| Optical Drive Configuration DISPLAY | DGTFRCDI |
| Optical Drive Configuration LIST | DGTFRCLD |
| | |
| Tape Library Configuration DEFINE | DGTFLMDE |
| Tape Library Configuration ALTER | DGTFLMAL |
| Tape Library Configuration DISPLAY | DGTFLMDI |
| Tape Library Configuration LIST | DGTFLMLD |
| | |
| Copy Pool Define | DGTFCPDA |
| Copy Pool Alter | DGTFCPAA |
| Copy Pool Display | DGTFCPDI |
| Copy Pool List | DGTFCPLD |

# ISMF Line Operator protection

| Line Operator | Aggregate Group List | Data Class | Data Set List | Optical Drive List |
|---|---|---|---|---|
| ALTER | DGTFALH1 | DGTFALD1 | DGTFAL01 | DGTFALR1 |
| ANALYZE | - | - | - | - |
| BROWSE | - | - | DGTFBR01 | - |
| CLIST | - | - | DGTFCL01 | - |
| COMPRESS | - | - | DGTFCM01 | - |
| CONDENSE | - | - | DFQFCND1 | - |
| CONVERTV | - | - | - | - |
| COPY | DGTFCAH1 | DGTFCAD1 | DGTFCY01 | DGTFCAR1 |
| DEFRAG | - | - | - | - |
| DELETE | DGTFDNH1 | DGTFDND1 | DGTFDL01 | DGTFDNR1 |
| DISPLAY | DGTFDIH1 | DGTFDID1 | - | DGTFDIR1 |
| DUMP | - | - | DGTFDP01 | - |
| EDIT | - | - | DGTFED01 | - |
| EJECT | - | - | - | - |
| ERASE | DGTFDNH1 | DGTFDND1 | DGTFDL01 | DGTFDNR1 |
| HALTERDS | - | - | DFQFHA01 | - |
| HBACKDS | - | - | DFQFHB01 | - |
| HBDELETE | - | - | DFQFHBD1 | - |
| HDELETE | - | - | DFQFHD01 | - |
| HIDE | DGTFHI01 | DGTFHI01 | DGTFHI01 | DGTFHI01 |
| HMIGRATE | - | - | DFQFHM01 | - |
| HRECALL | - | - | DFQFHRL1 | - |
| HRECOVER | - | - | DFQFHRC1 | - |
| INIT | - | - | - | - |
| INSPECT | - | - | - | - |
| LIST | - | - | - | - |
| LISTSYS | - | - | - | - |
| LISTVOL | - | - | - | - |
| MESSAGE | DGTFMS00 | DGTFMS00 | DGTFMS00 | DGTFMS00 |
| RAUTH | - | - | - | - |
| RECOVER | - | - | - | - |
| RELEASE | - | - | DGTFRL01 | - |
| RESTORE | - | - | DGTFRT01 | - |
| REFORMAT | - | - | - | - |
| SECURITY | DGTFSRD1 | - | DGTFSRD1 | - |
| SETCACHE | - | - | - | - |
| STATUS | - | - | - | - |
| TSO Commands and CLIST | DGTFUS01 | DGTFUS01 | DGTFUS01 | DGTFUS01 |

# ISMF Line Operator protection

| Line Operator | Optical Library List | List | Management Class | Mountable Optical Volume List | Copy Pool |
|---|---|---|---|---|---|
| ALTER | DGTFALL1 | - | DGTFALM1 | - | DGTFALP1 |
| AUDIT | DGTFAUL1 | - | - | DGTFAU01 | - |
| ANALYZE | - | - | - | - | - |
| BROWSE | - | - | - | - | - |
| CLIST | - | - | - | DGTFCL01 | - |
| COMPRESS | - | - | - | - | - |
| CONDENSE | - | - | - | - | - |
| CONVERTV | - | - | - | - | - |
| COPY | DGTFCAL1 | - | DGTFCAM1 | - | DGTFCAP1 |
| DEFRAG | - | - | - | - | - |
| DELETE | DGTFDNL1 | DGTFEL01 | DGTFDNM1 | - | DGTFDNP1 |
| DISPLAY | DGTFDIL1 | - | DGTFDIM1 | - | DGTFDIP1 |
| DUMP | - | - | - | - | - |
| EDIT | - | - | - | - | - |
| EJECT | - | - | - | DGTFEF01 | - |
| ERASE | DGTFDNL1 | DGTFEL01 | DGTFDNM1 | - | - |
| HALTERDS | - | - | - | - | - |
| HBACKDS | - | - | - | - | - |
| HBDELETE | - | - | - | - | - |
| HDELETE | - | - | - | - | - |
| HIDE | DGTFHI01 | DGTFHI01 | DGTFHI01 | DGTFHI01 | DGTFHI01 |
| HMIGRATE | - | - | - | - | - |
| HRECALL | - | - | - | - | - |
| HRECOVER | - | - | - | - | - |
| INIT | - | - | - | - | - |
| INSPECT | - | - | - | - | - |
| LIST | - | DGTFLL01 | - | - | - |
| LISTSYS | - | - | - | - | - |
| LISTVOL | DGTFLVL1 | - | - | - | - |
| MESSAGE | DGTFMS00 | DGTFMS00 | DGTFMS00 | DGTFMS00 | DGTFMS00 |
| RAUTH | - | - | - | - | - |
| RECOVER | - | - | - | DGTFRC01 | - |
| RELEASE | - | - | - | - | - |
| REMAP | DGTFRML1 | - | - | - | - |
| RESTORE | - | - | - | - | - |
| REFORMAT | - | - | - | - | - |
| SECURITY | - | - | DGTFSRD1 | - | - |
| SETCACHE | - | - | - | - | - |
| STATUS | - | - | - | - | - |
| TSO Commands and CLIST | DGTFUS01 | DGTFUS01 | DGTFUS01 | DGTFUS01 | DGTFUS01 |

# ISMF Line Operator protection

| Line Operator | Storage Class | Storage Group | Volume | Tape Library | Mountable Tape Volume |
|---|---|---|---|---|---|
| ALTER | DGTFALS1 | DGTFALG1 | - | DGTFALY1 | DGTFAL11 |
| ANALYZE | - | DGTFAZ01 | DGTFAZ01 | - | - |
| AUDIT | - | - | - | DGTFAUL1 | DGTFAU04 |
| BROWSE | - | - | - | - | - |
| BUILDX | - | - | DGTFBX01 | - | - |
| CLIST | - | - | DGTFCL01 | DGTFCL01 | DGTFCL01 |
| COMPRESS | - | - | DGTFCS01 | - | - |
| CONDENSE | - | - | - | - | - |
| CONSOLID | - | - | DGTFCI01 | - | - |
| CONTROL | - | - | DGTFCT01 | - | - |
| CONVERTV | - | - | DGTFCN01 | - | - |
| COPY | DGTFCAS1 | DGTFCAG1 | DGTFCV01 | DGTFCAY1 | - |
| DEFRAG | - | - | DGTFDF01 | - | - |
| DELETE | DGTFDNS1 | DGTFDNG1 | - | DGTFDNY1 | - |
| DISPLAY | DGTFDIS1 | - | - | DGTFDIY1 | - |
| DUMP | - | - | DGTFDM01 | - | - |
| EDIT | - | - | - | - | - |
| EJECT | - | - | - | - | DGTFEJ01 |
| ERASE | DGTFDNS1 | DGTFDNG1 | - | - | - |
| HALTERDS | - | - | - | - | - |
| HBACKDS | - | - | - | - | - |
| HBDELETE | - | - | - | - | - |
| HDELETE | - | - | - | - | - |
| HIDE | DGTFHI01 | DGTFHI01 | DGTFHI01 | DGTFHI01 | DGTFHI01 |
| HMIGRATE | - | - | - | - | - |
| HRECALL | - | - | - | - | - |
| HRECOVER | - | - | - | - | - |
| INIT | - | - | DGTFIN01 | - | - |
| INSPECT | - | - | DGTFIV01 | - | - |
| INSTALL | - | - | DGTFIL01 | - | - |
| LIST | - | - | DGTFIV01 | - | - |
| LISTSYS | - | DGTFLIC1 | - | - | - |
| LISTVOL | - | DGTFLVC1 | - | DGTFLVL1 | - |
| MESSAGE | DGTFMS00 | DGTFMS00 | DGTFMS00 | DGTFMS00 | DGTFMS00 |
| RAUTH | - | - | DGTFRA01 | - | - |
| RECOVER | - | - | - | - | - |
| REFORMAT | - | - | DGTFRF01 | - | - |
| RELEASE | - | - | DGTFRV01 | - | - |
| RESTORE | - | - | DGTFRO01 | - | - |
| REVAL | - | - | DGTFRB01 | - | - |
| SECURITY | DGTFSRD1 | - | - | DGTFSRD1 | - |
| SETCACHE | - | - | DGTFCB01 | - | - |
| STATUS | - | - | - | - | |
| TSO Commands and CLIST | DGTFUS01 | DGTFUS01 | DGTFUS01 | - | - |

# ISMF Line Operator protection

| Command | Module Name | CLIST |
|---|---|---|
| ACTIVATE | DGTFACAT | - |
| AUDIT | DGTFAU02 | - |
| BOTTOM | DGTFDO01 | - |
| CLEAR | DGTFCR01 | - |
| COMPRESS | DGTFCP01 | - |
| COPY | DGTFCO01 | - |
| DOWN | DGTFDO01 | - |
| DSUTIL | - | DSUTIL |
| DUMP | DGTFDU01 | - |
| ERTB | DGTFER02 | - |
| FILTER | DGTFFI01 | - |
| FILTER CLEAR | DGTFFI01 | - |
| FIND | DGTFFN01 | - |
| FOLD | DGTFFU01 | - |
| LEFT | DGTFLE01 | - |
| LIBRARY | - | LIBRARY |
| LISTPRT | DGTFPR01 | - |
| MIGRATE | - | MIGRATE |
| PROFILE | DGTFPF01 | - |
| QRETRIEV (DS) | ACBUTO3 | - |
| QRETRIEV (DVOL) | ACBUTO4 | - |
| QSAVE (DS) | ACBUTO6 | - |
| QSAVE (DVOL) | ACBUTO7 | - |
| RECALL | - | RECALL |
| RECOVER | DGTFRC01 | - |
| RELEASE | DGTFRE01 | - |
| RESHOW | DGTFRW01 | - |
| RESTORE | DGTFRR00 | - |
| RIGHT | DGTFRI01 | - |
| SAVE | DGTFSLDS | - |
| SORT | DGTFSO01 | - |
| TOP | DGTFUP01 | - |
| UP | DGTFUP01 | - |
| VALIDATE | DGTFVLVA | - |
| VIEW | DGTFVW01 | - |

# DFSMSdss functions and Profile names

Table 1. RACF FACILITY Class Profile Names for DFSMSdss Keywords

| Keyword or Function | Profile Name |
|---|---|
| BYPASSACS with COPY | STGADMIN.ADR.COPY.BYPASSACS |
| BYPASSACS with RESTORE | STGADMIN.ADR.RESTORE.BYPASSACS |
| CGCREATED | STGADMIN.ADR.CGCREATE |
| CONCURRENT with COPY | STGADMIN.ADR.COPY.CNCURRNT |
| CONCURRENT with DUMP | STGADMIN.ADR.DUMP.CNCURRNT |
| CONSOLIDATE | STGADMIN.ADR.CONSOLID |
| CONVERTV | STGADMIN.ADR.CONVERTV |
| DEFRAG | STGADMIN.ADR.DEFRAG |
| DELETECATALOGENTRY with RESTORE | STGADMIN.ADR.RESTORE.DELCATE |
| FCCGFREEZE with COPY | STGADMIN.ADR.COPY.FCFREEZE |
| FCFASTREVERSERESTORE with COPY | STGADMIN.ADR.COPY.FCFRR |
| FCSETGTOK with COPY | STGADMIN.ADR.COPY.FCSETGT |
| FCTOPPRCPRIMARY with COPY | STGADMIN.ADR.COPY.FCTOPPRCP |
| FCTOPPRCPRIMARY with DEFRAG | STGADMIN.ADR.DEFRAG.FCTOPPRCP |
| FlashCopy® with CONSOLIDATE | STGADMIN.ADR.CONSOLID.FLASHCPY |
| FlashCopy with COPY | STGADMIN.ADR.COPY.FLASHCPY |
| FlashCopy with DEFRAG | STGADMIN.ADR.DEFRAG.FLASHCPY |
| IMPORT with RESTORE | STGADMIN.ADR.RESTORE.IMPORT |
| INCAT(catname) with COPY | STGADMIN.ADR.COPY.INCAT |
| INCAT(catname) with DUMP | STGADMIN.ADR.DUMP.INCAT |
| INCAT(catname) with RELEASE | STGADMIN.ADR.RELEASE.INCAT |
| NEWNAMEUNCONDITIONAL with DUMP | STGADMIN.ADR.DUMP.NEWNAME |
| PROCESS(SYS1) with COPY | STGADMIN.ADR.COPY.PROCESS.SYS |
| PROCESS(SYS1) with DUMP | STGADMIN.ADR.DUMP.PROCESS.SYS |
| PROCESS(SYS1) with RELEASE | STGADMIN.ADR.RELEASE.PROCESS.SYS |
| RESET with DUMP | STGADMIN.ADR.DUMP.RESET |
| RESET(YES) with RESTORE | STGADMIN.ADR.RESTORE.RESET.YES |
| TOLERATE(ENQF) with COPY | STGADMIN.ADR.COPY.TOLERATE.ENQF |
| TOLERATE(ENQF) with DUMP | STGADMIN.ADR.DUMP.TOLERATE.ENQF |
| TOLERATE(ENQF) with RESTORE | STGADMIN.ADR.RESTORE.TOLERATE.ENQF |

# DFSMShsm functions and Profile names

Table 1. RACF FACILITY Class Profiles for DFSMShsm Storage Administrator Commands

| Command name | RACF FACILITY class resource name |
|---|---|
| ABACKUP | STGADMIN.ARC.ABACKUP<br>STGADMIN.ARC.ABACKUP.*agname* |
| ARECOVER | STGADMIN.ARC.ARECOVER<br>STGADMIN.ARC.ARECOVER.*agname*<br>STGADMIN.ARC.ARECOVER.*agname*.REPLACE |
| ADDVOL | STGADMIN.ARC.ADDVOL |
| ALTERDS | STGADMIN.ARC.ALTERDS |
| ALTERPRI | STGADMIN.ARC.ALTERPRI |
| AUDIT | STGADMIN.ARC.AUDIT |
| AUTH | STGADMIN.ARC.AUTH |
| BACKDS | STGADMIN.ARC.BACKDS<br>STGADMIN.ARC.BACKDS.NEWNAME<br>STGADMIN.ARC.BACKDS.RETAINDAYS |
| BACKVOL | STGADMIN.ARC.BACKVOL |
| BDELETE | STGADMIN.ARC.BDELETE |
| CANCEL | STGADMIN.ARC.CANCEL |
| DEFINE | STGADMIN.ARC.DEFINE |
| DELETE | STGADMIN.ARC.DELETE |
| DELVOL | STGADMIN.ARC.DELVOL |
| DISPLAY | STGADMIN.ARC.DISPLAY |
| EXPIREBV | STGADMIN.ARC.EXPIREBV |
| FIXCDS | STGADMIN.ARC.FIXCDS |
| FREEVOL | STGADMIN.ARC.FREEVOL |
| FRBACKUP | STGADMIN.ARC.FB.*cpname* |
| FRDELETE | STGADMIN.ARC.FD.*cpname* |
| FRRECOV | STGADMIN.ARC.FR.*cpname*<br>STGADMIN.ARC.FR.NEWNAME |
| HOLD | STGADMIN.ARC.HOLD |
| LIST | STGADMIN.ARC.LIST 2 Exception:<br>STGADMIN.ARC.LC.*cpname*, when<br>COPYPOOL(*cpname*) keyword is specified . |
| LOG | STGADMIN.ARC.LOG |
| MIGRATE | STGADMIN.ARC.MIGRATE |
| PATCH | STGADMIN.ARC.PATCH |
| QUERY | STGADMIN.ARC.QUERY |
| RECALL | STGADMIN.ARC.RECALL |
| RECOVER | STGADMIN.ARC.RECOVER<br>STGADMIN.ARC.RECOVER.NEWNAME |
| RECYCLE | STGADMIN.ARC.RECYCLE |
| RELEASE | STGADMIN.ARC.RELEASE |
| REPORT | STGADMIN.ARC.REPORT |
| SETMIG | STGADMIN.ARC.SETMIG |
| SETSYS | STGADMIN.ARC.SETSYS |
| STOP | STGADMIN.ARC.STOP |
| SWAPLOG | STGADMIN.ARC.SWAPLOG |
| TAPECOPY | STGADMIN.ARC.TAPECOPY |
| TAPEREPL | STGADMIN.ARC.TAPEREPL |
| TRAP | STGADMIN.ARC.TRAP |
| UPDATEC | STGADMIN.ARC.UPDATEC |

# DFSMShsm User Functions and Profile names

| Command name | RACF FACILITY class resource name |
|---|---|
| HALTERDS | STGADMIN.ARC.ENDUSER.HALTERDS |
| HBACKDS | STGADMIN.ARC.ENDUSER.HBACKDS<br>STGADMIN.ARC.ENDUSER.HBACKDS.NEWNAME<br>STGADMIN.ARC.ENDUSER.HBACKDS.RETAINDAYS<br>STGADMIN.ARC.ENDUSER.HBACKDS.TARGET |
| HBDELETE | STGADMIN.ARC.ENDUSER.HBDELETE |
| HCANCEL | STGADMIN.ARC.ENDUSER.HCANCEL |
| HDELETE | STGADMIN.ARC.ENDUSER.HDELETE |
| HLIST | STGADMIN.ARC.ENDUSER.HLIST |
| HMIGRATE | STGADMIN.ARC.ENDUSER.HMIGRATE |
| HQUERY | STGADMIN.ARC.ENDUSER.HQUERY |
| HRECALL | STGADMIN.ARC.ENDUSER.HRECALL |
| HRECOVER | STGADMIN.ARC.ENDUSER.HRECOVER |

# DFSMSrmm functions and Profile names

| able 1. Resources you protect with RACF profiles | |
|---|---|
| Define the Profile | To Control the |
| STGADMIN.EDG.ACTIONS.action[1] | Setting of the release action. |
| STGADMIN.EDG.AV.status.volser[2] | Adding of volumes. |
| STGADMIN.EDG.CD.COPYFROM.dsname[4] | Use of CHANGEDATASET COPYFROM subcommand to copy the data set attributes from one data set dsname to another data set. |
| STGADMIN.EDG.CD.VX[4] | Overriding of DFSMSrmm VRSEL processing for a data set. |
| STGADMIN.EDG.CMOVE.location.destination | Confirmation of moves and ejects. |
| STGADMIN.EDG.CRLSE.action[1] | Confirmation of the release action. |
| STGADMIN.EDG.CV.[HOLD\|NOHOLD].volser[3] | Setting and resetting the volume HOLD attribute |
| STGADMIN.EDG.CV.RM[3] | Use of the RMM CHANGEVOLUME RETENTIONMETHOD subcommand to update the retention method for a volume. Use of the RMM CHANGEVOLUME RETAINBY subcommand to update the retain by attribute of a volume managed by the EXPDT retention method. |
| STGADMIN.EDG.DV.SCRATCH.volser | Deleting of scratch volumes. |
| STGADMIN.EDG.FORCE | Changing of information recorded by DFSMSrmm during O/C/EOV processing. Adding or deleting data sets on volumes or to use the DELETEVOLUME command. |
| STGADMIN.EDG.EDGUPDT.UPDATE | Use of the EDGUPDT utility UPDATE function. |
| STGADMIN.EDG.HOUSEKEEP | Use of DFSMSrmm inventory management functions. |
| STGADMIN.EDG.HOUSEKEEP.RPTEXT | Use of DFSMSrmm inventory management extract function |

# DFSMSrmm functions and Profile names

| | |
|---|---|
| STGADMIN.EDG.IGNORE.TAPE.volser | Use of volume serial numbers that are not defined to DFSMSrmm and use of duplicate volume serial numbers to allow a volume to be ignored. If you are authorized to ignore use of a tape volume, DFSMSrmm also overrides the SAF authorization for you to access data on the tape when the data is not defined to RACF and when the user is not authorized to the data. **Recommendation:** Do not assign an access level to the STGADMIN.EDG.IGNORE.TAPE.volser resource to any specific user group. When a tape volume that must be ignored by DFSMSrmm is identified, grant the user or user group the needed access level. Once the volume is no longer needed, delete the resource. |
| STGADMIN.EDG.IGNORE.TAPE.RMM.volser | Use of duplicate volume serial numbers and to allow a volume to be ignored. If you are authorized to ignore use of a tape volume, DFSMSrmm also overrides the SAF authorization for you to access data on the tape when the data is not defined to RACF and when the user is not authorized to the data. **Recommendation:** Specify UACC(NONE) to the STGADMIN.EDG.IGNORE.TAPE.RMM.volser resource. Grant a user or user group the needed access level only when access is needed. When the volume is no longer needed, delete the resource. |
| STGADMIN.EDG.IGNORE.TAPE.NORMM.volser | Use of volume serial numbers that are not defined to DFSMSrmm to allow a volume to be ignored. If you are authorized to ignore use of a tape volume, DFSMSrmm also overrides the SAF authorization for you to access data on the tape when the data is not defined to RACF and when the user is not authorized to the data.Recommendation: Specify UACC(NONE) to the STGADMIN.EDG.IGNORE.TAPE.NORMM.volser resource. Grant the needed access level to a user or user group only when access is needed. When the volume is no longer needed, delete the resource. |

# DFSMSrmm functions and Profile names

| | |
|---|---|
| STGADMIN.EDG.INIT | Setting of the INIT action. |
| STGADMIN.EDG.LABEL.volser | Creation of standard tape labels. The variable volser can be specified as a specific volume serial number or a generic volume serial number. For example, A12345 is a specific volume serial number and AB* is a generic volume serial number. If you use generic profiles you can use these functions in a subset of your volumes. If the volume serial numbers and rack numbers match, you can control relabeling at the pool level. For example you could have a pool using rack number prefix AB*. If you want to create an AL tape and your installation has an SL scratch pool, you need ALTER access to STGADMIN.EDG.LABEL.volser. The volser can be specified as the pool prefix of the scratch pool. If you want to switch to an AL tape from either an SL or NL tape that has already been assigned to you, UPDATE access to STGADMIN.EDG.LABEL.volser is required. |
| STGADMIN.EDG.LIST | List and search DFSMSrmm resources. |
| STGADMIN.EDG.LISTCONTROL | Use of the RMM LISTCONTROL subcommand to display DFSMSrmm control data set control record information and EDGRMMxx parmlib settings. |

# DFSMSrmm functions and Profile names

| | |
|---|---|
| STGADMIN.EDG.MASTER | Access to information in the DFSMSrmm control data set. Assign the control data set a universal access of NONE so that DFSMSrmm grants access to various functions through STGADMIN.EDG.MASTER. |
| STGADMIN.EDG.MOVES.location.destination | Initiation of moves and ejects. |
| STGADMIN.EDG.NOLABEL.volser | Creation of tapes without labels. |
| STGADMIN.EDG.OPERATOR | Use of the initialize, erase, and scan functions. |
| STGADMIN.EDG.OWNER.userid | Access to owned resources. DFSMSrmm checks this entity only if the command issuer is not the owner of the resource and does not have CONTROL access to STGADMIN.EDG.MASTER. Use of the RMM CHANGEVOLUME subcommand to update information based on the owner. Using STGADMIN.EDG.OWNER.userid, individual owners can permit other users to access owned volumes. An owner can be a group or department as well as an individual. Define owner resources only for those owners who will allow their volumes to be managed by another user. |
| STGADMIN.EDG.RELEASE | Use of the RMM DELETEVOLUME RELEASE subcommand to process any release actions specified for a volume. |
| STGADMIN.EDG.RESET.SSI | Use of the RESET facility for removing DFSMSrmm from the system. You can use the facility without defining this resource when you have no security product installed. |
| STGADMIN.EDG.VRS | Use of the RMM LISTVRS and SEARCHVRS subcommands to obtain information about vital record specifications. Use of the RMM ADDVRS and DELETEVRS subcommands to define or remove vital record specifications. |
| STGADMIN.EDG.INERS.WRONGLABEL | Processing for volumes mounted with the wrong label. |

#SHAREorg

SHARE
Technology · Connections · Results

# How to Protect the z/OS Storage Environment from Prying Eyes and Still Get Your Work Done

Chris Taylor
IBM Corporation
ctaylor1@us.ibm.com

March 11, 2014
Session Number 15071

SHARE in Anaheim