TUTORIAL: PROTECTING DATASETS IN RACF

Stuart Henderson
the Henderson Group
Bethesda, MD
(301) 229-7187
www.stuhenderson.com

1

AGENDA

I. INTRODUCTION

II. DISK DATASETS

III. TAPE DATASETS

IV. SUMMARY AND CALL TO ACTION

2

I. INTRODUCTION

- We All Know How to Protect Datasets
- But Sometimes It's Nice to Take a Systematic Review of What We Have, Taking Note of Special Issues for Disk and for Tape

3

I. INTRODUCTION

- Today We'll Briefly Mention Some Things to Keep in Mind
- Then We'll Cover Some Specifics for Disk and Tape
- Then We'll Wrap Up with Some Recommendations to Consider

4

I. INTRODUCTION

SOME THINGS TO KEEP IN MIND

- Always-Call and PROTECTALL
- PROTECTALL and SPECIAL
- Naming Standards
- Protection by DSNAME or by VOLSER

5

I. INTRODUCTION

SOME THINGS TO KEEP IN MIND

- HLQ=Userid
- PRIVILEGED, TRUSTED
- NOPASS in PPT

6

I. INTRODUCTION

SOME THINGS TO KEEP IN MIND

- Clumsy RACF GLOBAL Rules (for example, SYS1.*/READ)
- OPERATIONS attribute in RACF

7

I. INTRODUCTION

SOME THINGS TO KEEP IN MIND

- SETR GENERIC(REFRESH)
- CATDSNS (on SETR)
- DSNS (on LD)

8

I. INTRODUCTION

SOME THINGS TO KEEP IN MIND

Access by Shared Hardware:

- Imagine Two CPUs with a Common, Shared DASD Device
- It Has a Sensitive Dataset, Perhaps the Accounts Payable File of Checks to Be Written

9

I. INTRODUCTION

SOME THINGS TO KEEP IN MIND

Access by Shared Hardware:

- Each CPU has a Different RACF Database, with Different Rules for This Dataset
- If the Auditors Only Look at One of the RACF Databases.

10

I. INTRODUCTION

SOME THINGS TO KEEP IN MIND

Access by Shared Hardware:

- **Imagine the Same Risk with a SYSPLEX Mirroring Databases, Each Protected by Dataset Rules in a Different RACF Database**

11

II. Disk Datasets

- **Discretes Ignored Unless the Bit is On**
- **ALTER Access to a Catalog Lets You Delete Any Dataset Catalogued in It**

12

II. Disk Datasets

- **Utilities like DFDSS, IOF, FDR (but not AMASPZAP, note to auditors please)**
- **Use of DASDVOL Resource Class**

13

II. Disk Datasets

- **Residual Data and EOS**
- **How the Hardware Improvement Works**
- **Who Should Decide? Who Should Implement? Who Should Be Consulted?**

14

III. Tape Datasets

Three Places to Set TAPEDSN:

- **SETR TAPEDSN**
- **DEVSUPxx Member in Parmlib**
- **TMS (Tape Management Software)**

Why Not With SETR TAPEDSN?

15

III. Tape Datasets

Some Well-Known TMS:

- **CA1**
- **TLMS**
- **ZEKE**
- **ZARA**
- **RMM**
- **Control-T**

16

III. Tape Datasets

- **The "17-character dsname" weakness**
- **The "2 files on a tape" weakness**
- **Residual data (after the retention period is up)**

17

III. Tape Datasets

- **980000 and Other TMS Functions**
- **Bypass Label Processing**

18

The First Two Records on a Tape Are Called Labels:

VOL1 123456	

Unique VOLSER Number That Identifies THIS Tape

19

The First Two Records on a Tape Are Called Labels:

VOL1 123456	HDR1 OLL.FILE.G0014.V00

//DD1 DD DSN=PROD.PAYROLL.FILE.G0014V00,…

DSNAME GOES INTO HDR1 LABEL

20

OPEN Makes Two Checks for SL Tapes

VOL1 123456	HDR1 OLL.FILE.G0014.V00

```
//DD1 DD DSN=PROD.PAYROLL.FILE.G0014V00,…
```

1. Compare DSNAME in Label Against DD Card
2. Call SAF with RACHECK

21

But If the Rogue STU Wants to Read It:

VOL1 123456	HDR1 OLL.FILE.G0014.V00

```
//DD1 DD DSN=PROD.PAYROLL.FILE.G0014V00,…

//DD2 DD DSN=STU.XX.OLL.FILE.G0014V00,…
```

1. Compare DSNAME in Label Against DD Card
2. Call SAF with RACHECK

22

But If the Rogue STU Wants to Read It:

VOL1 123456	HDR1 OLL.FILE.G0014.V00

```
//DD1 DD DSN=PROD.PAYROLL.FILE.G0014V00,…

//DD2 DD DSN=STU.XX.OLL.FILE.G0014V00,…
```

1. Compare DSNAME in Label Against DD Card
2. Call SAF with RACHECK

23

But If the Rogue STU Wants to Read It:

VOL1 123456	HDR1 OLL.FILE.G0014.V00

```
//DD1 DD DSN=PROD.PAYROLL.F  E.G0014V00,…

//DD2 DD DSN=STU.XX.OLL.FILE.G0014V00,…
```

1. Compare DSNAME in Label Against DD Card
2. Call SAF with RACHECK

24

IV. Summary and Call to Action

- **Many Items to Consider Beyond PROTECTALL and ADDSD**
- **If We Don't Stop to Consider, It's Easy to Think We're Protecting Everything Properly, and Still Be Missing Important Coverage.**

25

IV. Summary and Call to Action

Life Is Easier When Protection Is:

- **Automatic**
- **Comprehensive**
- **Simple Enough to Explain on a Cocktail Napkin**

26

IV. Summary and Call to Action

Rules of Thumb for Dataset Rules:

- **More Than 4 Permissions Per Dataset Rule Probably Not Needed**
- **Most Permissions Should Be to Groups, Not to Userids**
- **More Than 4 Dataset Rules Per Production Application Probably Not Needed**

27

Some Recommendations

- **RACF control over BLP**
- **Tape management software and pooling**
- **Encryption (hardware and software, DB2)**
- **Tape Drive Encryption**

28

Some Recommendations

- Only Send Out Brand New Tapes
- Restrict granting of OPERATIONS
- Parmlib Member DEVSUPxx Fields Named TAPEAUTHxx

29

Make RACF Userids Be Restricted

- ALU userid RESTRICTED
- Doesn't Permit Access By:
  - UACC
  - ID(*)
  - GLOBAL rules
  - USS ACLs (Access Control Lists)
- Does Permit By:
  - WARNING
  - UNIX File Security Bits (Note Exception with UNIXPRIV Rule RESTRICTED.FILESYS.ACCESS)

30

IV. Summary and Call to Action

Thanks for Your Kind Attention

31