z/OS 3.2 IBM Education Assistant

Solution Name: RACF Support for Tape Data Set Encryption and Granularity

Solution Element: RACF

July 2025

© 2025 IBM Corporation

Agenda

- Trademarks
- Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Upgrade & Coexistence Considerations
- Installation & Configuration
- Summary
- Appendix

© 2025 IBM Corporation

Trademarks

- See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks.
- Additional Trademarks:
  - None

© 2025 IBM Corporation

Objectives

- As DFSMS provides tape data set encryption, provide a way for customers to request or bypass encryption for tape data sets covered by a RACF profile
- Extend this policy control to PDSE and sequential (basic and large format) data sets, for which DFSMS already provides encryption support

- The overall goal is to avoid application outage when the application uses EXCP to access data, thus bypassing the access methods, and breaking when accessing encrypted data

- The ability to include and exclude various data set types is accomplished with a new ENCRYPTTYPES keyword in the DFP segment of the RACF DATASET profile

© 2025 IBM Corporation

Overview

- Who (Audience)
  - Security Administrators
- What (Solution)
  - The ability to specify policy for encryption of various data set types covered by a singe RACF DATASET profile
- Wow (Benefit / Value, Need Addressed)
  - Accommodation of applications that do not support encryption/decryption of data in data sets

© 2025 IBM Corporation

Usage & Invocation

- A new field in the DFP segment of the DATASET profile specifies encryption policy for tape, PDSE, and sequential basic and large format data sets covered by the profile
  - No change to current support of extended format data sets
- This policy is not bound to the encryption key label in the DFP DATAKEY field
  - That is, the key can be sourced elsewhere, like today
- For each type, you can choose to
  - **IN**clude the type for encryption
  - **EX**clude the type from encryption
  - Defer to SMS for the decision (the default). SMS checks a FACILITY profile for system-wide default policy.

© 2025 IBM Corporation

Usage & Invocation … ADDSD and ALTDSD

```
[ DFP(
      [RESOWNER(userid or group-name) | NORESOWNER]
      [DATAKEY(CKDS key label) | NODATAKEY]
      [ENCRYPTTYPES(
          [ALL |
          [INTAPE | EXTAPE | NOTAPE]
          [INPDSE | EXPDSE | NOPDSE]    ← NOxxxx values undocumented for ADDSD, but 'work'
          [INSEQ  | EXSEQ  | NOSEQ ]
          ]
                  ) | NOENCRYPTTYPES]
    ) | NODFP ]
```

- ALL is mutually exclusive with EXxxxx and NOxxxx
- NOxxxx, INxxxx, and Exxxxx are mutually exclusive for the same type
- Authorized by system SPECIAL, or UPDATE access to FIELD class resource DATASET.DFP.ENCTYPES

© 2025 IBM Corporation

Usage & Invocation … LISTDSD

- Requires SPECIAL, AUDITOR, ROAUDIT, or READ access to FIELD class resource DATASET.DFP.ENCTYPES

```
INFORMATION FOR DATASET BRUCE.* (G)

DFP INFORMATION
---------------
RESOWNER= NONE
DATAKEY= MYKEY
DATA SET TYPES ENCRYPTED= INTAPE EXSEQ

INFORMATION FOR DATASET BRUCE.* (G)

DFP INFORMATION
---------------
RESOWNER= NONE
DATAKEY= MYKEY
DATA SET TYPES ENCRYPTED= ALL INTAPE INPDSE INSEQ
```

© 2025 IBM Corporation

Usage & Invocation … R_admin (IRRSEQ00)

- R_admin (IRRSEQ00) callable service
  - On DATASET-extract, the field is treated as a repeat group of character values
  - Possible values are INTAPE|EXTAPE, INPDSE|EXPDSE, INSEQ|EXSEQ
    - No NOxxxx values are emitted. NOxxxx is implied when neither INxxxx nor EXxxxx is emitted
    - “ALL” is never emitted

Field name	Flag byte values	ADDSD/ALTDSD keyword reference	Allowed on add requests	Allowed on alter requests	Returned on extract requests
ENCTYPES (list ENCTYPEN)	‘Y’	ENCRYPTTYPES(xx)	Yes	Yes	Yes
	‘N’	NOENCRYPTTYPES	No	Yes	

© 2025 IBM Corporation

Usage & Invocation … IRRDBU00

- DFP record type 0410 is extended
- Values are treated as a series of YES/NO fields for each type
- Blanks for a given type implies NOxxxx
- Space is reserved for 13 more possible types
  - The database field is 4 bytes, requiring two bits (IN and EX) per type

© 2025 IBM Corporation

Usage & Invocation … messages

- Existing, unchanged message indicates mutually exclusive operands entered

```
IRR52128I Mutually exclusive operands are specified for
keyword ENCRYPTTYPES. Processing terminated.
```

© 2025 IBM Corporation

Usage & Invocation … RACF database templates

- The version string is updated to
  - **OA66305** 00000285.00000050 on 2.5 and 3.1
  - **HRF77F0** 00000285.00000050 on 3.2
- All 3.2 template updates are rolled back
- When extracting the 4-byte field using RACROUTE REQUEST=EXTRACT or ICHEINTY LOCATE, the field is formatted as follows.

```
DFP      001 00 00 00000000 00 DFP - START OF SEGMENT FIELDS
RESOWNER 002 00 00 00000008 FF DFP - RESOURCE OWNER
DATAKEY  003 00 00 00000000 00 DFP - CKDS label of default key
ENCTYPES 004 00 00 00000004 00 DFP - Types of data set encrypted
$*                               Byte 1:
$*                                X'80' - INTAPE
$*                                X'40' - INPDSE
$*                                X'20' - INSEQ
$*                                X'08' - EXTAPE
$*                                X'04' - EXPDSE
$*                                X'02' - EXSEQ
```

© 2025 IBM Corporation

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - DFSMS

© 2025 IBM Corporation

Upgrade & Coexistence Considerations

- To exploit this solution, all systems in the Plex must be at the new z/OS level: No
- List any toleration/coexistence APARs/PTFs:
  - zSecure support for new DFP field
    - HRF77D0
      - ++IF FMID(HCKR250) THEN REQ(UJ96644). zSecure Admin and Audit
      - ++IF FMID(HC4R250) THEN REQ(UJ96650). zSecure Admin and Audit
      - ++IF FMID(JC4R250) THEN REQ(UJ96649). zSecure Command Verifier
      - ++IF FMID(HCKR310) THEN REQ(UJ96643).
      - ++IF FMID(HC4R310) THEN REQ(UJ96646).
      - ++IF FMID(JC4R310) THEN REQ(UJ96645)
    - HRF77E0
      - ++IF FMID(HCKR310) THEN REQ(UJ96643).
      - ++IF FMID(HC4R310) THEN REQ(UJ96646).
      - ++IF FMID(JC4R310) THEN REQ(UJ96645).
      - ++IF FMID(HCKR250) THEN REQ(UJ96644).
      - ++IF FMID(HC4R250) THEN REQ(UJ96650).
      - ++IF FMID(JC4R250) THEN REQ(UJ96649)
- List anything that doesn't work the same anymore: Nothing

© 2025 IBM Corporation

Installation & Configuration

- List anything that a client needs to be aware of during installation and include **examples** where appropriate - clients appreciate these:
  - Are any APARs or PTFs needed for enablement?
    - When sharing the RACF database with a 2.5/3.1 system, have OA66305 applied on 2.5/3.1
  - What jobs need to be run?
    - RACF templates should be updated by running IRRMIN00 with PARM=UPDATE after IPL
    - RACF Dynamic Parse initialization (IRRDPI00 UPDATE) is executed as part of your IPL automation
  - What hardware configuration is required? None
  - What PARMLIB statements or members are needed? None
  - Are any other system programmer procedures required? None
  - Are there any planning considerations? None
  - Are any special web deliverables needed? None
  - Does installation change any system defaults? None

© 2025 IBM Corporation

Summary

- DFSMS is providing tape data set encryption
- Some applications may not support encrypted data sets
- Granularity is required at the data set level to specify the data set types that should be encrypted, for data sets covered by the RACF profile
- In the absence of RACF policy, DFSMS checks a FACILITY profile to determine if tape encryption is to be done at a system-wide level

- The same level of granularity is also desired for previously supported (for encryption) types PDSE and Sequential
  - So, we added it as well
- Policy can be established using ADDSD/ALTDSD and R_admin (IRRSEQ00)
- Policy can be retrieved by LISTDSD, RACROUTE REQUEST=EXTRACT, R_admin (IRRSEQ00), and the Database Unload utility (IRRDBU00)

© 2025 IBM Corporation

Appendix

- Publications
  - z/OS Security Server RACF Callable Services
    - R_Admin
  - z/OS Security Server RACF Command Language Reference
    - ADDSD, ALTDSD, LISTDSD
  - z/OS Security Server RACF Macros and Interfaces
    - RACF database templates, DB Unload table
  - z/OS Security Server RACF Security Administrator's Guide
    - FIELD level access table

© 2025 IBM Corporation