IBM Education Assistance for z/OS V2R2

Item: SMF VTOC Audit Log
Element/Component: DFSMSdfp

Material current as of May 2015

Agenda

- Trademarks
- Presentation Objectives
- Overview
- Usage & Invocation
- Interactions & Dependencies
- Migration & Coexistence Considerations
- Installation
- Presentation Summary
- Appendix

Presentation Objectives

- New SMF Record 42 subtype 27 – VTOC Audit Log

Overview

- Problem Statement
  - Vendor-built channel program updated a DSCB with stale extent info. Wrong extent was freed when data set was scratched.
- Solution
  - New SMF Record 42 subtype 27 for DASD VTOC Operations
  - Captures updates to the VTOC for IBM and Vendor-built channel programs
- Benefit / Value
  - Provides an audit log for VTOC updates
  - Helps diagnose problems when VTOC is compromised

Usage & Invocation

- Writes to the VTOC are detected by EXCP
  - CKD and ECKD channel programs
  - DADSM/CVAF
  - DSS Defrag/Consolidate, Copy/Restore/Dump
  - Vendor channel programs
  - XDAP macro instruction
    - Adds support for IOB Extension block
  - SuperZAP (AMASPZAP service)
- Not all VTOC updates are logged:
  - System Resident volume
  - Temporary DASD data sets
  - I/O to an offline volume
  - Updates to DSCB FMT 1,5, and 7; 2nd DSCB written in chnl pgm

VTOC DSCB Update – SMF 42 subtype 27

- Record contents
  - Date / Time
  - System ID, Job Name, Job number, Step name, Prod name
  - User Security Token (mapped by ICHRUTKN)
  - Activity (from IOBEUSER in IOB Extension)
    - Dxxx: DFSMS Actvitity
    - DCVF: CVAFDIR
    - DCRE, DREN: Dataset create and rename
    - DEXT, DPAR: Dataset extend and partial release
    - DDEL: Dataset scratch (read prior to actual erase)
    - DFRG, DCON: DFSMSdss defrag and consolidate
    - DDMP, DRST: DFSMSdss dump and restore
    - IOBE: IOBE not provided
    - USER: IOBEUSER not specified
  - Volume Serial, Device ID (UCB Channel number)
  - Seek and Search ID (CCCC HHHH R)
  - Caller's PSW following EXCP SVC
  - Device is Reserved flag
  - DSCB Key and Data field (140 bytes)

VTOC SMF 42 subtype 27 Examples

- DADSM Create Data Set
  - Activity = DCRE
  - Chnl Pgm = 472903 06030347 0D
  - Caller's Address following SVC EXCP = 841015AC
  - User Token = 50012206 0001C000 ...

```
5E2A004D DF3D0114 352FF3F0 F9F0E2D4   E240001B 00020000 00000034 00280001   *;..(......3090SMS ..............*
0000005C 009C0001 000000F8 008C0001   C8C4E9F2 F2F2F040 E961D6E2 40C4C6E2   *...*.......8....HDZ2220 Z/OS DFS*
D4E20100 00000000 00000000 00000000   00000000 00000000 C9C2D4E4 E2C5D940   *MS.....................IBMUSER *
E3E2E4F0 F0F0F1F7 E2D1D7C1 C3C3D5E3   E2D1D7C1 C3C3D5E3 C9D5C5F9 C5F80F45   *TSU00017SJPACCNTSJPACCNTINE9E8..*
C4C3D9C5 80000000 00040001 00040001   06472903 06030347 0D000000 00000000   *DCRE............................*
841015AC 50012206 0001C000 00000000   00000000 00000000 00000000 00000000   *....&.....{....................*
00000000 00000000 00000000 00000000   00000000 D3D6C3C1 D3C3F0F1 00000000   *....................LOCALC01....*
00000000 C9C2D4E4 E2C5D940 E2E8E2F1   40404040 C9C2D4E4 E2C5D94B E2D4C6E5   *....IBMUSER SYS1    IBMUSER.SMFV*
E3D6C34B C4F1F2F1 F8404040 40404040   40404040 40404040 40404040 40404040   *TOC.D1218                       *
F1C9D5C5 F9C5F800 01720160 00000001   0000C9C2 D4D6E2E5 E2F24040 40404000   *1INE9E8....-......IBMOSVS2     .*
00000080 00504000 90000050 00500000   00005000 00140000 00E5A200 00010000   *.....& ....&.&....&......V......*
00000100 00000100 00000000 00000000   00000000 00000000 00000000 00000000   *................................*
```

VTOC SMF 42 subtype 27 Examples

- VTOC Writer Not Identified
  - Job Id JOB00024
  - Step Name ZAP
  - Activity = IOBE (IOBE not provided)
  - Chnl Pgm = 310D
  - Caller's Address following SVC EXCP = 00014C3C

```
5E2A004E FB460114 352FF3F0 F9F0E2D4   E240001B 00020000 00000034 00280001   *;..+......3090SMS ..............*
0000005C 009C0001 000000F8 008C0001   C8C4E9F2 F2F2F040 E961D6E2 40C4C6E2   *...*.......8....HDZ2220 Z/OS DFS*
D4E20100 00000000 00000000 00000000   00000000 00000000 D6C1F2F9 F0F6F8C2   *MS.....................OA29068B*
D1D6C2F0 F0F0F2F4 E9C1D740 40404040   00000000 00000000 C9D5C5F9 C5F80F45   *JOB00024ZAP     ........INE9E8..*
C9D6C2C5 80000000 00040001 00040001   06310D00 00000000 00000000 00000000   *IOBE............................*
00014C3C 5001000C 4003C000 00000000   00000000 E2D1D7D3 F4F0F940 5CC2E8D7   *..<.&... .{.........SJPL409 *BYP*
C1E2E25C E2D1D7D3 F4F0F940 00000000   00000000 D9C4D9F1 40404040 00000000   *ASS*SJPL409 ........RDR1    ....*
00000000 4E4E4E4E 4E4E4E4E 40404040   40404040 D6C1F2F9 F0F6F8C2 4BC3D6D4   *....++++++++        OA29068B.COM*
D7D9C5E2 E2404040 40404040 40404040   40404040 40404040 40404040 40404040   *PRESS                           *
F1C9D5C5 F9C5F800 02720160 00000001   0000C9C2 D4D6E2E5 E2F24040 40404072   *1INE9E8....-......IBMOSVS2     .*
01600000 00004000 80000050 00500000   0082C000 00030040 08CE4200 00810000   *.-.... ....&.&....{.... ........*
A2000000 AB000E00 00000000 00000000   00000000 00000000 00000000 00000000   *................................*
```

Interactions & Dependencies

- Software Dependencies
  - None
- Hardware Dependencies
  - None
- Exploiters
  - No changes required.
  - Set IOB Extension field IOBEUSER to identify writes to the VTOC
  - ICN in December 2014

Installation

- PARMLIB member SMFPRMXX keyword NOTYPE is used to identify Record Subtypes that should not be recorded.
  - Specify NOTYPE(42(27)) to disable VTOC Audit logging

Appendix

- Communications to other z/OS platform and/or vendors
  - IGWSMF macro (SMF record 42 subtype 27 added)

- Publication Changes: distributed in V2R2
  - *Introduction and Release Guide* GA32-0887
  - *z/OS MVS System Management Facilities (SMF)* SA22-7630
  - *z/OS DFSMSdfp Advanced Services Document* SC23-6861
    - XDAP