IBM Systems

Debugging Storage Violations in CICS®

Scott McClure (mcclures@us.ibm.com)
November 2015

WebSphere® Support Technical Exchange

ON DEMAND BUSINESS

Agenda

- CICS detected storage violations
- Types of storage violations
- SAAs and Check Zones
- SCEs and SCFs
- Storage violation debug

Storage Violation Types

- CICS detected and reported
  - Reported by DFHSM0102 message
    - DFHSM0102 *applid* A storage violation (code X'*code*') has been detected by module *modname*
- Undetected by CICS
  - Requires different problem determination techniques

CICS Detected Storage Violations

- Initial or duplicate Storage Accounting Area (SAA) of a Terminal Input/Output Area (TIOA) storage element has become corrupted.
- Leading or trailing Check Zone of a user-task storage element has become corrupted.
- Detected at freemain time. Not when the violation actually happened.
  - SAA chains are checked when an individual element is requested to be freed, at least up to the target element.
  - SAA chains are checked during freemain of storage belonging to a TCTTE after the last output has taken place.
  - Check Zones are checked during freemain of a specific user-task storage element.
  - Check Zones chains are checked during freemain of all user-task storage during task termination.

SAAs

- Are eight bytes long
  - First eight bytes of the TIOA are known as the initial (leading) SAA
  - Last eight bytes of the TIOA are known as the duplicate (trailing) SAA
  - First word indicates Storage Class and length
    - First byte represents the Storage Class (x'85' = TIOA storage)
    - Last two bytes represent the length of the TIOA
      - Length includes initial SAA and useable portion of TIOA only
  - Second word is the chain pointer
    - Will point to another TIOA in the chain or to the owning TCTTE +4
- Comparison of the initial and duplicate SAA is done, at freemain time, to detect possible overlay

SAA storage for TIOAs

Storage Address	Offset	Storage			
12FBB310	0000	**85000118**	**12FBB000**	00000000	00000000
12FBB320	0010	00000000	00000000	00000000	00000000
12FBB330	0020	00000000	00000000	00000000	00000000
12FBB340	0030	00000000	00000000	00000000	00000000
12FBB350	0040	00000000	00000000	00000000	00000000
12FBB360	0050	00000000	00000000	00000000	00000000
12FBB370	0060	00000000	00000000	00000000	00000000
		..			
		..			
12FBB3F0	00E0	00000000	00000000	00000000	00000000
12FBB400	00F0	00000000	00000000	00000000	00000000
12FBB410	0100	00000000	00000000	00000000	00000000
12FBB420	0110	00000000	00000000	**85000118**	**12FBB000**

NOTE: The address returned on the GETMAIN request is that of the leading SAA, offset x'0'.

Check Zones

- Are eight bytes long
- First eight bytes are known as the leading check zone
- Last eight bytes are known as the trailing check zone
- Byte 0-3 indicates the task subpool name
  - C00 = CICS above the line storage (ECDSA)
  - M00 = CICS below the line storage (CDSA)
  - U00 = USER above the line storage (EUDSA)
  - B00 = USER below the line storage (UDSA)
- Bytes 4-7 indicates the owning task number
  - For example B0012345 represents user below the line storage for task number 12345
- There are no chain pointers as Storage Manager is aware of all task storage and their lengths via Storage Element Descriptors (SCE) and Free Storage Descriptors (SCF).
- Comparison of the leading and trailing check zone is done, at freemain time, to detect possible overlay

Check Zones

```
CICS24.00005 00046000 CICS storage below 16MB

     0000  D4F0F0F0 F0F0F0F5 00B46EC4 C6C8C5C9  *M0000005..>DFHEI*
     0010  E4E24040 40404040 00000000 00000000  *US        ........*
     0020  00000000 00000000 00000000 00000000  *................*
     0030 -    004F LINES SAME AS ABOVE
     0050  000460D0 00000000 00000000 00000000  *..-}............*
     0060  00000000 00000000 00000000 00000000  *................*
     0070 -    009F LINES SAME AS ABOVE
     00A0  00000000 00000000 00000000 00046050  *..............-&*
     00B0  00046054 00000000 00000000 00000000  *..-............*
     00C0  00656EC4 C6C8C1D7 6DC4C6C8 C5C9C25C  *..>DFHAP_DFHEIB**
     00D0  0000000C 0106080F C3E2E2E8 0000005C  *........CSSY...**
     00E0  00000000 00000000 00000000 00000000  *................*
     00F0  00000000 00000000 00000000 00000000  *................*
     0100  00000040 40404040 40404000 00000000  *...         .....*
     0110  00000000 00000000 00000000 00000000  *................*
     0120 -    045F LINES SAME AS ABOVE
     0460  00000000 00000000 D4F0F0F0 F0F0F0F5  *........M0000005*
```

Output via VERBX DFHPD690 ‘AP’

Note: The address returned on the GETMAIN request is that of the beginning of usable storage , offset x’8’.

SCEs and SCFs

```
SCE.M0000005 11FD0290 Storage Element Descriptor

   0000  11FD3610 11FD3610 00046000 00000470  *.........-.....*
   0010  11F09040 00000000                    *.0. ....       *

SCF.M0000005 11FD0278 Free Storage Descriptor

   0000  11FD3620 11FD3620 00046470 00000B90  *................*
   0010  11F09040 00000000                    *.0. ....       *
```

Third word contains the location of the storage.
Fourth word contains the length of the storage.

Output created via VERBX DFHPD690 ‘SM’

DFHSM0102 Debugging

- Message produced:
  - **DFHSM0102** IYNXH A storage violation (code X'**0F0C**') has been detected by module DFHSMAR.
- From the Messages and Codes manual:
  - Explanation: A storage violation has been detected by module *modname*. The code X'***code***' is the exception trace point ID which uniquely identifies the type of storage violation.

    System Action:
    An exception entry (X'*code*' in the message) is made in the trace table.
    Use the exception trace point ID, X'code', to investigate the cause of the storage violation. A description of the exception trace point ID, and the data it contains, is in the **CICS Trace Entries** manual.

    A system dump is taken, unless you have specifically suppressed dumps in the dump table.

    CICS continues unless you have specified in the dump table that CICS should terminate.

Storage manager domain trace points

Excerpt from CICS Trace Entries manual

Point ID	Module	Lvl	Type	Data
SM 0F0A	DFHSMAR	Exc	Insufficient storage for SCQs	1 SMAR parameter list
SM 0F0B	DFHSMAR	Exc	Insufficient storage for SMXs	1 SMAR parameter list
SM 0F0C	DFHSMAR	Exc	Storage check failure	1 SMAR parameter list 2 Address of storage element 3 Length of storage element 4 First 512 bytes (max) of storage element 5 Last 512 bytes (max) of storage element 6 Data preceding storage element (1K max) 7 Data following storage element (1K max)

DFHSM0102 Abbreviated Trace

Output via: VERBX DFHPD690 'TR=1'

```
00515 QR    AP 05A8 APRC  ENTRY PERFORM_COMMIT          NO,FORWARD,00000001              =003685=
00515 QR    AP 05A9 APRC  EXIT  PERFORM_COMMIT/OK       NO                               =003686=
00515 QR    RM FA12 RMUO  EXIT  COMMIT_UOW/OK                                            =003687=
00515 QR    KE 0201 KEDD  ENTRY INQUIRE_ANCHOR          0000002C                         =003688=
00515 QR    KE 0202 KEDD  EXIT  INQUIRE_ANCHOR/OK       12075000                         =003689=
00515 QR    DP 0900 DPXM  ENTRY RELEASE_XM_CLIENT                                        =003690=
00515 QR    DP 0901 DPXM  EXIT  RELEASE_XM_CLIENT/OK                                     =003691=
00515 QR    AP 0590 APXM  ENTRY RELEASE_XM_CLIENT       NORMAL                           =003692=
XM    QR    AP 0591 APXM  EXIT  RELEASE_XM_CLIENT/OK                                     =003693=
XM    QR    US 0401 USXM  ENTRY END_TRANSACTION                                          =003694=
XM    QR    XS 0401 XSXM  ENTRY END_TRANSACTION                                          =003695=
XM    QR    XS 0402 XSXM  EXIT  END_TRANSACTION/OK                                       =003696=
XM    QR    US 0402 USXM  EXIT  END_TRANSACTION/OK                                       =003697=
XM    QR    PG 0801 PGXM  ENTRY TERMINATE_TRANSACTION                                    =003698=
XM    QR    PG 0802 PGXM  EXIT  TERMINATE_TRANSACTION/OK                                 =003699=
XM    QR    SM 0F01 SMAR  ENTRY RELEASE_TRANSACTION_STG                                  =003700=
XM    QR    XM 1001 XMIQ  ENTRY SET_TRANSACTION         INCREMENT                        =003701=
XM    QR    XM 1002 XMIQ  EXIT  SET_TRANSACTION/OK                                       =003702=
XM    QR    AP 1700 TFIQ  ENTRY SET_TERMINAL_FACILITY YES                                =003703=
XM    QR    AP 1701 TFIQ  EXIT  SET_TERMINAL_FACILITY/OK                                 =003704=
XM    QR    SM 0F0C SMAR  *EXC* Storage_check_failed_at_address 001007D0
                                                      RELEASE_TRANSACTION_STG          =003705=
XM    QR    ME 0301 MEME  ENTRY SEND_MESSAGE  66,SM0102,11C32D16,00000002,00000008SM     =003706=
XM    QR    KE 0101 KETI  ENTRY INQ_LOCAL_DATETIME_DECIMAL                               =003707=
XM    QR    KE 0102 KETI  EXIT  INQ_LOCAL_DATETIME_DECIMAL/OK                            =003708=
```

DFHSM0102 Full Trace

Output via: VERBX DFHPD690 'TR=2'

```
SM 0F0C SMAR  *EXC* - Storage_check_failed_at_address - 001007D0
                                                    FUNCTION(RELEASE_TRANSACTION_STG)

TASK-XM KE_NUM-0049 TCB-QR /008CCE88 RET-91C40B8E TIME-15:31:20.60 INTERVAL-0.0000011 =003705=

1-00 00280000 000000D1 00000000 00000000  B0000000 00000000 02000100 00000000*.......J.......*
  20 00000000 00000000                                                      *........        *
2-00 001007D0                                                               *...}            *
3-00 000003D0                                                               *...}            *
4-00 C2F0F0F0 F0F5F1F5 00000000 00000000 00000000 00000000 00000000 00000000 *B0000515........*
  20 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
  40 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
  60 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
  80 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
  A0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
  C0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
  E0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 100 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 120 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 140 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 160 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 180 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 1A0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 1C0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 1E0 00000000 00000000                                                      *........        *
```

DFHSM0102 Full Trace

```
5-00 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
  20 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
  40 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  *................*
 160 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 180 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 1A0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 1C0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 03BC00C8 *............ .H*
 1E0 00C8200C 02C00008                                                     *.H . .  . .     *
6-00 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
  20 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
  40 00000000 00000000 00000000 0010005C 00000000 500C10DC 0008211C 001007C4 *.......*....&..D*
  60 001004F0 12BF5838 000C1028 12BF4F70 12446F0F 12447F0E 12448F0D 12449F0C *...0..|.?."....*
  80 00100B94 1244BF0A 001000D0 008B8000 00100488 00000000 C2F0F0F0 F0F5F1F5 *.m.}.h.B0000515*
  A0 C2F0F0F0 F0F5F1F5 0008034E 00000000 00000000 00000000 00000000 0010005C *B0000515.+....**
     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  *................*
 360 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 380 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 3A0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 3C0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 3E0 00000000 00000000 00000000 00000000 00000000 03BC0000 C2F0F0F0 F0F5F1F5 *.......B0000515*
7-00 00008C00 12080000 08000020 600602F0 00280000 00000000 00000000 00000000 *..{..... ......*
  20 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  *................*
 100 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 120 00000000 00000000 00000000 00000000 00000000 00000000 C2F0F0F0 F0F0F4F3 *.......B0000043*
 140 C2F0F0F0 F0F0F4F3 000802E0 00000000 00100478 00100488 00000000 00100488 *B0000043..\.h.h*
     . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .  *................*
 3A0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 3C0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 3E0 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
```

Storage Manager View

SCA.B0000515 31471458 Subpool Control Area

```
 0000 C2F0F0F0 F0F5F1F5 314713A4 11FD3B60 08010200 00000000 00000000 00000000 *B0000515.u..-..*
 0020 00000000 00000000 00000000 00000000 00000004 00000000 00000002 00000000 *................*
 0040 00000000 00000000 00000000 00000000 11FD0BF0 11FD0C98 00100470 00000000 *.....0..q......*
 0060 11F9B368 11F9B308 7FFFFFFF 7FFFFFFF 00000000 11DF4470 314714D0 314714D0 *.9..9."..".}.}*
 0080 00000000 00000000 FFFFFFF0 00100201 01020000 00000000 00001000 00000840 *............0.. *
 00A0 00000000 00001000 11FEB228 00000000 00000000                             *...........    *
```

SCE.B0000515 11FD0BF0 Storage Element Descriptor

```
   0000  11FD0C98 314714A8 001007D0 000003D0  11FD1A88 00000000                 *..q..y..}...   *
```

SCE.B0000515 11FD0C98 Storage Element Descriptor

```
   0000  314714A8 11FD0BF0 00100000 00000470  11FD1A88 00000000                 *..y...0..h.... *
```

SCF.B0000515 11F9B368 Free Storage Descriptor

```
   0000  11F9B308 314714B8 00100470 00000360  11FD1A88 00000000                 *.9....-..h...  *
```

SCF.B0000515 11F9B308 Free Storage Descriptor

```
   0000  314714B8 11F9B368 00100BA0 00000460  11FD1A88 00000000                 *...9...-...h.. *
```

Output via: VERBX DFHPD690 ‘SM’

Storage Browse

```
00100470  C2F0F0F0  F0F5F1F5  0008034E  00000000   | B0000515...+....|
00100480  00000000  00000000  00000000  0010005C   | ............... *|
00100490  00000000  500C10DC  00000000  001007C4   | ....&..........D|
001004A0  001004F0  12BF5838  000C1028  12BF4F70   | ...0..........|.|
001004B0  12446F0F  12447F0E  12448F0D  12449F0C   | ..?..."........|
001004C0  00100B94  1244BF0A  001000D0  008B8000   | ...m.......}....|
001004D0  00000000  00000000  00000000  00100488   | ...............h|
001004E0  008B8000  001000D0  00000000  00000000   | .......}........|
001004F0  800C184C  001005F8  801007C4  00000000   | ...<...8...D....|
00100500.:1005EF. LENGTH(X'F0')--All bytes contain X'00'             |
001005F0  00000000  00000000  001007D8  00000000   | ............Q....|
00100600.:1007BF. LENGTH(X'01C0')--All bytes contain X'00'           |
001007C0  00000000  03BC0000  C2F0F0F0  F0F5F1F5   | ........B0000515|
001007D0  C2F0F0F0  F0F5F1F5  00000000  00000000   | B0000515........|
001007E0.:100B8F. LENGTH(X'03B0')--All bytes contain X'00'           |
00100B90  00000000  03BC00C8  00C8200C  02C00008   | ........ H.H. ..|
00100BA0  00008C00  12080000  08000020  400602F0   | ..{.............|
00100BB0  00280000  00000000  00000000  00000000   | . ..............|
00100BC0.:100CCF. LENGTH(X'0110')--All bytes contain X'00'           |
00100CD0  00000000  00000000  C2F0F0F0  F0F0F4F3   | ........B0000043|
```

00100470 = Free storage x’360’ long (SCF)
001007D0 = Allocated storage x’3D0’ long (SCE)
00100BA0 = Free storage x’460’ long (SCF)

DFHSM0102 Full Trace

```
AP 00E1 EIP ENTRY GETMAIN            REQ(0004) FIELD-A(00100488 ...h) FIELD-B(08000C02 ....)

TASK-00515 KE_NUM-0049 TCB-QR/008CCE88 RET-500C10B0 TIME-15:31:20 INTERVAL-0.00000104 =003633=

SM 0C01 SMMG  ENTRY - FUNCTION(GETMAIN) GET_LENGTH(3BC) SUSPEND(YES) STORAGE_CLASS(USER24) CALLER(EXEC)

TASK-00515 KE_NUM-0049 TCB-QR/008CCE88 RET-928B1AAC TIME-15:31:20 INTERVAL-0.00000212 =003634=
 1-00 00800000 00000011 00000000 00000000 B6580000 00000000 02BF014E 1244FFA8 *............+.*
   20 00100478 0000034E 000003BC 00000360 1244FFA8 01441201 11FD1A88 0005B680 *....+...-..h..*
   40 0005BB74 12BF60A0 11DF4F30 00000000 000001E0 11E2FD70 0000003C 11E2FDAC *...-..\.S...S.*
   60 000001E0 0010003C 00000000 00400000 BE9ACE34 7DF9F27E 00C2E7C8 003C00EF *.\.. 92=.BXH..*

                        . . . . . .

SM 0C02 SMMG  EXIT  - FUNCTION(GETMAIN) RESPONSE(OK) ADDRESS(001007D8)

TASK-00515 KE_NUM-0049 TCB-QR/008CCE88 RET-928B1AAC TIME-15:31:20 INTERVAL-0.00000104 =003636=
```

Trace can be used to discover what program issued the getmain for the storage. To find the getmain, search for the address Storage Manager knows +x'8'. This will find the trace entry showing the exit of DFHSMMG. Back up in trace to find the EIP ENTRY GETMAIN trace entry. The RET value will point to the program that issued the getmain.

Loader Domain

```
PGM NAME ENTRY PT  CSECT    LOAD PT. REL. PTF LVL. LAST COMPILED  COPY NO. USERS  LOCN  TYP


 IBMRSAP  800ABA20 -noheda- 000ABA20                                 1       1    RDSA  RPL
 READUPDT 000C1000 DFHYA640 000C1000 640                            1       0    SDSA  RPL
 DFHSIP   11C554B8 DFHCICS  11C00000 0640 HCI6400   I  02/03 08.21  1       0    ERGN  ANY
                   DFHKEDCL 11C00200 640  UK04769   06/23/05 12.51
                   -noheda- 11C007F8
                   DFHKEDRT 11C00800 640  HCI6400   03/02/05 06.28
                   -noheda- 11C00DF8
                   DFHKESCL 11C00E00 640  HCI6400   03/02/05 06.28
                   -noheda- 11C013F8
                   DFHKESRT 11C01400 640  HCI6400   03/02/05 06.28
                   -noheda- 11C019F8
                   DFHKETA  11C01A00 640  HCI6400   03/02/05 06.29
                   DFHKETI  11C02220 640  HCI6400   03/02/05 06.29
                   DFHKETIX 11C03870 640  HCI6400   03/02/05 06.29
                   DFHDDDI  11C04388 640  HCI6400   03/02/05 05.59
                   DFHDDLO  11C07618 640  HCI6400   03/02/05 05.59
                   DFHDDBR  11C07F20 640  HCI6400   03/02/05 05.59
                   DFHDSAT  11C09680 640  INUCPUT   02/22/06 19.34
                   DFHDSSR  11C0E9D0 640  INUCPUT   02/22/06 19.34
```

Output via: VERBX DFHPD690 ‘LD=1’

Storage Browse of READUPDT Program

```
000C1000  C4C6C8E8  C1F6F4F0  58F0021C  58F0F0D0  | DFHYA640.0...00} |
000C1010  58F0F014  58F0F00C  58FF000C  07FF5CC6  | .00..00.......*F |
000C1020  C9D3D3C9  D55C0000  47F0F028  23D9C5C1  | ILLIN*...00..REA |
000C1030  C4E4D7C4  E34DE45D  40F0F461  F0F461F1  | DUPDT(U) 04/04/1 |
000C1040  F540F1F6  4BF2F940  C5E2C1F6  F9F04040  | 5 16.29 ESA690   |
000C1050  90ECD00C  183F4510  3036033E  000058F0  | ..}.............0 |
000C1060  37C805EF  50D01004  18F1BF1F  D0184780  | .H..&}...1..}... |
000C1070  3050D207  F05C1000  18DF58B0  D05CD201  | .&K.0*......}*K. |
```

Note: To calculate a proper offset into the module, you must account for the length of the Exec Interface stub. The entry point is offset x'28' because this is the branch instruction that will branch to the STM instruction (offset x'50') upon entry to the module.

Findings

- Task 515 was terminating when storage violation was determined
- AP 0F0C trace entry indicates:
  - Violated storage is located at address 001007D0
  - Violated storage is x'3D0' bytes long
  - Trailing Check Zone is overlaid with value of **00C8200C 02C00008**
    - Violation was at least 8 bytes long
    - Unable to determine if violation affected more storage as the following storage was never allocated
- Program READUPDT getmained the storage in question
- Program READUPDT most likely wrote past his allocated storage
  - When / Where / Why ?

Storage Violation Trap (CSFE)

- Built in storage violation trap
- Runs each time an old style AP trace entry is written (has old style Field A and Field B)
  - Ensure level 1 trace is turned on for all components and level 1-2 for the EI component
    - Ensure Monitoring package is not suppressing EI trace entries
- Checks all storage areas on the transaction storage chain for the currently running task
- Produces a DFHSM0103 dump and turns itself off when a violation is detected
  - Will catch the violation within a window much closer to when the violation actually occurs
  - If window is still too large, consider adding additional user trace points to the application using EXEC CICS ENTER TRACENUM commands
- Turned ON/OFF via:
  - SIT parameter CHKSTSK
    - CHKSTSK=CURRENT
    - CHKSTSK=NONE
  - Manually as a transaction
    - CSFE DEBUG,CHKSTSK=CURRENT
    - CSFE DEBUG,CHKSTSK=NONE

DFHSM0103 Debugging

- Message produced:
  - **DFHSM0103** IYNXH A storage violation (*code* X'**0932**') has been detected by the storage violation trap. Trap is now inactive.
- From the Messages and Codes manual:
  - Explanation: A storage violation has been detected by the storage violation trap, which may be enabled via the CHKSTSK or the CHKSTRM system initialization parameters or via the CSFE transaction. The code X'***code***' is the exception trace point ID which uniquely identifies the type of storage violation detected.

    System Action: CICS disables the storage violation trap. An exception entry (X'*code*' in the message) is made in the trace table. A system dump is taken, unless you have specifically suppressed dumps in the dump table.

    CICS continues unless you have specified in the dump table that CICS should terminate.

Storage manager domain trace points

Point ID	Module	Lvl	Type	Data
SM 0932	DFHSMCK	Exc	Storage zone check failed	1 SMCK parameter list 2 Subpool name 3 Address of storage 4 First 128 bytes of storage element 5 Last 16 bytes of storage element

DFHSM0103 Abbreviated Trace

```
00108 QR AP 1940 APLI  ENTRY START PROGRAM        READUPDT,CEDF,FULLAPI,EXEC,NO,12FB9140 =004694=
00108 QR SM 0C01 SMMG  ENTRY GETMAIN              34E,YES,00,TASK24                      =004695=
00108 QR SM 0C02 SMMG  EXIT  GETMAIN/OK           00100478                               =004696=
00108 QR AP 00E1 EIP   ENTRY GETMAIN                        0004,00100488 ...h,08000C02  =004697=
00108 QR SM 0901 SMCK  ENTRY CHECK_STORAGE        CURRENT_TASK,NO                        =004698=
00108 QR SM 0902 SMCK  EXIT  CHECK_STORAGE/OK                                            =004699=
00108 QR AP E160 EXEC  ENTRY GETMAIN              AT X'001005F8',956 AT X'801007C4',ASM  =004700=
00108 QR SM 0C01 SMMG  ENTRY GETMAIN              3BC,YES,USER24,EXEC                    =004701=
00108 QR SM 0C02 SMMG  EXIT  GETMAIN/OK           001007D8                               =004702=
00108 QR AP E161 EXEC  EXIT  GETMAIN              X'001007D8' AT X'001005F8',956 AT      =004703=
00108 QR AP 00E1 EIP   EXIT  GETMAIN              OK      00F4,00000000 ..,00000C02      =004704=
00108 QR SM 0901 SMCK  ENTRY CHECK_STORAGE        CURRENT_TASK,NO                        =004705=
00108 QR SM 0902 SMCK  EXIT  CHECK_STORAGE/OK                                            =004706=
00108 QR AP 00E1 EIP   ENTRY SUSPEND                       0004,00100488 ...h,08001208 ..  =004707=
00108 QR SM 0901 SMCK  ENTRY CHECK_STORAGE        CURRENT_TASK,NO                        =004708=
00108 QR XM 1001 XMIQ  ENTRY SET_TRANSACTION      INCREMENT,1200A030 , 0000108C          =004709=
00108 QR XM 1002 XMIQ  EXIT  SET_TRANSACTION/OK                                          =004710=
00108 QR AP 1700 TFIQ  ENTRY SET_TERMINAL_FACILITY 12C4C4D0,YES                          =004711=
00108 QR AP 1701 TFIQ  EXIT  SET_TERMINAL_FACILITY/OK                                    =004712=
00108 QR SM 0932 SMCK  *EXC* Zone check failed    CHECK_STORAGE,CURRENT_TASK,NO          =004713=
```

Output via: VERBX DFHPD690 ‘TR=1’

DFHSM0103 Full Trace

```
AP 1940 APLI  ENTRY - FUNCTION(START PROGRAM) PROGRAM(READUPDT) CEDF_STATUS(CEDF)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-9229C972 TIME-17:19:29 INTERVAL-0.0000046  =004694=

SM 0C01 SMMG  ENTRY - FUNCTION(GETMAIN) GET_LENGTH(34E) SUSPEND(YES) INITIAL_IMAGE(00)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80085E44 TIME-17:19:29 INTERVAL-0.0000065  =004695=

SM 0C02 SMMG  EXIT  - FUNCTION(GETMAIN) RESPONSE(OK) ADDRESS(00100478)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80085E44 TIME-17:19:29 INTERVAL-0.0000016  =004696=

AP 00E1 EIP ENTRY GETMAIN      REQ(0004) FIELD-A(00100488 ...h) FIELD-B(08000C02 ....)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-500C10B0 TIME-17:19:29 INTERVAL-0.0000020  =004697=

SM 0901 SMCK  ENTRY - FUNCTION(CHECK STORAGE) TASK_STORAGE(CURRENT_TASK) TP_STORAGE(NO)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80083BB6 TIME-17:19:29 INTERVAL-0.0000014  =004698=

SM 0902 SMCK  EXIT  - FUNCTION(CHECK STORAGE) RESPONSE(OK)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80083BB6 TIME-17:19:29 INTERVAL-0.0000013  =004699=

AP E160 EXEC ENTRY GETMAIN SET( AT X'001005F8') LENGTH(956 AT X'801007C4') ASM
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-8008245C TIME-17:19:29 INTERVAL-0.0000044  =004700=

SM 0C01 SMMG  ENTRY - FUNCTION(GETMAIN) GET_LENGTH(3BC) SUSPEND(YES) STORAGE_CLASS(USER24)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-928B4CBC TIME-17:19:29 INTERVAL-0.0000052  =004701=
```

Output via: VERBX DFHPD690 ‘TR=2’

DFHSM0103 Full Trace (cont.…)

```
SM 0C02 SMMG  EXIT  - FUNCTION(GETMAIN) RESPONSE(OK) ADDRESS(001007D8)
 TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-928B4CBC TIME-17:19:29 INTERVAL-0.00000082 =004702=

AP E161 EXEC EXIT GETMAIN SET(X'001007D8' AT X'001005F8') LENGTH(956 AT X'801007C4') RESP(0)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80083A5C TIME-17:19:29 INTERVAL-0.0000023  =004703=

AP 00E1 EIP EXIT GETMAIN OK     REQ(00F4) FIELD-A(00000000 ....) FIELD-B(00000C02 ....)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-500C10B0 TIME-17:19:29 INTERVAL-0.00000067 =004704=

SM 0901 SMCK  ENTRY - FUNCTION(CHECK STORAGE) TASK_STORAGE(CURRENT_TASK) TP_STORAGE(NO)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80083BB6 TIME-17:19:29 INTERVAL-0.00000035 =004705=

SM 0902 SMCK  EXIT  - FUNCTION(CHECK STORAGE) RESPONSE(OK)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80083BB6 TIME-17:19:29 INTERVAL-0.00000075 =004706=

AP 00E1 EIP ENTRY SUSPEND     REQ(0004) FIELD-A(00100488 ...h) FIELD-B(08001208 ....)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-500C10DA TIME-17:19:29 INTERVAL-0.00000073 =004707=

SM 0901 SMCK  ENTRY - FUNCTION(CHECK STORAGE) TASK_STORAGE(CURRENT_TASK) TP_STORAGE(NO)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80083BB6 TIME-17:19:29 INTERVAL-0.00000035 =004708=
```

DFHSM0103 Full Trace (cont…)

```
XM 1001 XMIQ  ENTRY - FUNCTION(SET_TRANSACTION) STORAGE_VIOLATIONS(INCREMENT)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-91CECD68 TIME-17:19:29 INTERVAL-0.0000016  =004709=

XM 1002 XMIQ  EXIT  - FUNCTION(SET_TRANSACTION) RESPONSE(OK)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-91CECD68 TIME-17:19:29 INTERVAL-0.0000011  =004710=

AP 1700 TFIQ  ENTRY - FUNCTION(SET_TERMINAL_FACILITY) TERMINAL_TOKEN(12C4C4D0)
                                                      COUNT_STORAGE_VIOLATION(YES)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-91CECDE6 TIME-17:19:29 INTERVAL-0.0000019  =004711=

AP 1701 TFIQ  EXIT  - FUNCTION(SET_TERMINAL_FACILITY) RESPONSE(OK)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-91CECDE6 TIME-17:19:29 INTERVAL-0.0000019  =004712=

SM 0932 SMCK *EXC* -Zone_check_failed-FUNCTION(CHECK_STORAGE) TASK_STORAGE(CURRENT_TASK) TP_STOR

  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80083BB6 TIME-17:19:29 INTERVAL-0.00000034 =004713=
   1-00 00200000 00000010 00000000 00000000 BC000000 00000000 01000100 0201C621 *.............F*
   2-00 C2F0F0F0 F0F1F0F8                                                     *B0000108       *
   3-00 001007D0                                                              *...}           *
   4-00 C2F0F0F0 F0F1F0F8 00000000 00000000 00000000 00000000 00000000 00000000 *B0000108......*
     20 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *............*
     40 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *............*
     60 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *............*
   5-00 00000000 03BC00C8 00C8200C 02C00008                                   *. H.H . . .    *
```

NOTE: The SM 0932 trace point does not offer the length of the violated storage.
Storage Manager must be used to determine the length.

Storage Manger

```
SCA.B0000108 314529F8 Subpool Control Area

00 C2F0F0F0 F0F1F0F8 31452944 31452AAC 08010200 00000000 00000000 00000000 *B0000108.........*
20 00000000 00000000 00000000 00000000 00000003 00000000 00000000 00000000 *.................*
40 00000000 00000000 00000000 00000000 11FD1D58 11FD1A70 00000000 00000000 *.................*
60 11FD1B90 11FD1B90 7FFFFFFF 7FFFFFFF 00000000 11DF4470 31452A70 31452A70 *........"...".....*
80 00000000 00000000 FFFFFFF0 00100201 01020000 00000000 00001000 00000BA0 *............0.....*
A0 00000000 00001000 11FF225C 00000000 00000000                           *...........*    *

SCE.B0000108 11FD1D58 Storage Element Descriptor

 0000  11FD1518 31452A48 001007D0 000003D0  11FD2160 00000000                *.....}...}...-  *

SCE.B0000108 11FD1518 Storage Element Descriptor

 0000  11FD1A70 11FD1D58 00100470 00000360  11FD2160 00000000                *.....-...-.     *

SCE.B0000108 11FD1A70 Storage Element Descriptor

 0000  31452A48 11FD1518 00100000 00000470  11FD2160 00000000                *........-.      *

SCF.B0000108 11FD1B90 Free Storage Descriptor

 0000  31452A58 31452A58 00100BA0 00000460  11FD2160 00000000                *...-...-....    *
```

Output via: VERBX DFHPD690 ‘SM

Storage Browse

```
001007D0   C2F0F0F0   F0F1F0F8   00000000   00000000   | B0000108........ |
001007E0.:100B8F. LENGTH(X'03B0')--All bytes contain X'00'
00100B90   00000000   03BC00C8   00C8200C   02C00008   *. . . . . H.H . . *

00100BA0   00008C00   12080000   08000020   400602F0   | ..{............. |
00100BB0   00280000   00000000   00000000   00000000   | . ............... |
00100BC0.:100FFF. LENGTH(X'0440')--All bytes contain X'00'
00101000   C2F0F0F0   F0F0F5F8   00B46EC4   C6C8C5C9   | B0000058..>DFHEI |
```

001007D0 addresses the violated storage (trailing check zone is overlaid)
00100BA0 addresses an SCF

Violation Caught

```
AP 00E1 EIP EXIT GETMAIN OK      REQ(00F4) FIELD-A(00000000 ....) FIELD-B(00000C02 ....)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-500C10B0 TIME-17:19:29 INTERVAL-0.00000067 =004704=

SM 0901 SMCK  ENTRY - FUNCTION(CHECK STORAGE) TASK_STORAGE(CURRENT_TASK) TP_STORAGE(NO)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80083BB6 TIME-17:19:29 INTERVAL-0.00000035 =004705=

SM 0902 SMCK  EXIT  - FUNCTION(CHECK STORAGE) RESPONSE(OK)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80083BB6 TIME-17:19:29 INTERVAL-0.00000075 =004706=

AP 00E1 EIP ENTRY SUSPEND      REQ(0004) FIELD-A(00100488 ...h) FIELD-B(08001208 ....)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-500C10DA TIME-17:19:29 INTERVAL-0.00000073 =004707=

SM 0901 SMCK  ENTRY - FUNCTION(CHECK STORAGE) TASK_STORAGE(CURRENT_TASK) TP_STORAGE(NO)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-80083BB6 TIME-17:19:29 INTERVAL-0.00000035 =004708=

XM 1001 XMIQ  ENTRY - FUNCTION(SET_TRANSACTION) STORAGE_VIOLATIONS(INCREMENT)
  TASK-00108 KE_NUM-0048 TCB-QR/008CCE88 RET-91CECD68 TIME-17:19:29 INTERVAL-0.0000016  =004709=
```

The window, of the violation being detected, is between the exit of the getmain request and the entry to the suspend request. The code running between this window is responsible for the violation. Make note of the two RET addresses for calculation of offset into responsible program.

Loader Domain

PROGRAM STORAGE MAP

PGM NAME	ENTRY PT	CSECT	LOAD PT.	REL.	PTF LVL.	LAST COMPILED	COPY NO.	USERS	LOCN	TYP
IBMRSAP	800ABA20	-noheda-	000ABA20				1	1	RDSA	RPL
READUPDT	**000C1000**	**DFHYA640**	**000C1000**	640			1	0	SDSA	RPL
DFHSIP	11C554B8	DFHCICS	11C00000	0640	HCI6400	I 02/03 08.21	1	0	ERGN	ANY
		DFHKEDCL	11C00200	640	UK04769	06/23/05 12.51				
		-noheda-	11C007F8							
		DFHKEDRT	11C00800	640	HCI6400	03/02/05 06.28				
		-noheda-	11C00DF8							
		DFHKESCL	11C00E00	640	HCI6400	03/02/05 06.28				
		-noheda-	11C013F8							
		DFHKESRT	11C01400	640	HCI6400	03/02/05 06.28				
		-noheda-	11C019F8							
		DFHKETA	11C01A00	640	HCI6400	03/02/05 06.29				
		DFHKETI	11C02220	640	HCI6400	03/02/05 06.29				
		DFHKETIX	11C03870	640	HCI6400	03/02/05 06.29				
		DFHDDDI	11C04388	640	HCI6400	03/02/05 05.59				
		DFHDDLO	11C07618	640	HCI6400	03/02/05 05.59				
		DFHDDBR	11C07F20	640	HCI6400	03/02/05 05.59				
		DFHDSAT	11C09680	640	INUCPUT	02/22/06 19.34				
		DFHDSSR	11C0E9D0	640	INUCPUT	02/22/06 19.34				

Output via: VERBX DFHPD690 ‘LD=1

READUPDT Program

```
00005E D201 3058 321A 00058 0021A   930          MVC  MOVELEN,=X'0020'
000064 D201 3056 3214 00056 00214   931          MVC  GETLEN,=X'03BC'
                                    932 *        EXEC CICS GETMAIN LENGTH(GETLEN) SET(4)
                                    933          DFHECALL =X'0C02C0000800008C00',(PTR4__RF,4)
                                    935+*************************************************
00006A                              936+         DS    0H
00006A 4110 D068            00068   937+         LA    1,DFHEIPL
00006E 41E0 321B            0021B   938+         LA    14,=X'0C02C0000800008C00'
000072 41F0 D170            00170   939+         LA    15,DFHEITP1
000076 4100 3056            00056   940+         LA    0,GETLEN
00007A 90E0 1000            00000   941+         STM   14,0,0(1)
00007E 9680 1008      00008         942+         OI    8(1),X'80'          LAST ARGUMENT
000082 58F0 31F4            001F4   943+         L     15,=V(DFHEI1)
000086 0DEF                         944+         BASR  14,15               INVOKE EXEC INTERFACE
000088 5840 D170            00170   945+         L     4,DFHEITP1
                                    946+*************************************************
00008C 4144 03BC            003BC   947          LA   R4,X'3BC'(4)
000090 5850 3058            00058   948          L    R5,MOVELEN
000094 41A3 0214            00214   949          LA   R10,X'214'(3)
000098 1FBB                         950          SLR  R11,R11
00009A 0E4A                         951          MVCL R4,10
                                    952 *        EXEC CICS SUSPEND
                                    953          DFHECALL =X'120800000800002040'
                                    955+*************************************************
00009C                              956+         DS    0H
00009C 4110 D068            00068   957+         LA    1,DFHEIPL
0000A0 41E0 3224            00224   958+         LA    14,=X'120800000800002040'
0000A4 50E0 1000            00000   959+         ST    14,0(,1)
0000A8 9680 1000      00000         960+         OI    0(1),X'80'          LAST ARGUMENT
0000AC 58F0 31F4            001F4   961+         L     15,=V(DFHEI1)
0000B0 0DEF                         962+         BASR  14,15               INVOKE EXEC INTERFACE
```

READUPDT Program

```
000214 03BC                1158          =X'03BC'
000216 00C8                1159          =Y(L'REC)
000218 00C8                1160          =Y(L'RECB)
00021A 20                  1161          =X'20'
00021B 0C02C0000800008C00  1162          =X'0C02C0000800008C00'
000224 1208000008000020 40 1163          =X'1208000008000020 40'
00022D 0602F000280000 8000 1164          =X'0602F0002800008000'
000236 0602F0000800008400  1165          =X'0602F0000800008400'
00023F 1004801008000420 80 1166          =X'1004801008000420 80'
000248 0606E0000800004000  1167          =X'0606E0000800004000'
000251 1812000008 00C20000 1168          =X'1812000008 00C20000 08400 4000021'
000260 0E0800000800001000  1169          =X'0E0800000800001000'
```

Storage Browse

```
001007D0   C2F0F0F0   F0F1F0F8   00000000   00000000   | B0000108........ |
001007E0.:100B8F. LENGTH(X'03B0')--All bytes contain X'00'
00100B90   00000000   03BC00C8   00C8200C   02C00008   | ...H.H..  ..... |
00100BA0   00008C00   12080000   08000020   400602F0   | ..{........0.... |
00100BB0   00280000   00000000   00000000   00000000   | . ............. |
00100BC0.:100FFF. LENGTH(X'0440')--All bytes contain X'00'
00101000   C2F0F0F0   F0F0F5F8   00B46EC4   C6C8C5C9   | B0000058..>DFHEI |
```

We now know the violation actually started at location 00100B94 and carried on into the following (free) piece of storage located at 00100BA0.

AP Domain within DFHSM0103 Dump

```
USER24.00108 001007D0 USER storage below 16MB

 000 C2F0F0F0 F0F1F0F8 00000000 00000000 00000000 00000000 00000000 00000000 *B0000108.........*
 020 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00000000 *................*
 040  -  03BF LINES SAME AS ABOVE
 3C0 00000000 03BC00C8 00C8200C 02C00008                                   *..H.H . . . .   *

 ** DFHPD0125  Storage violation detected at 001007D0. Trailing SAA is invalid.


 USER24.00108 00100470 USER storage below 16MB

 000 C2F0F0F0 F0F1F0F8 0008034E 00000000 00000000 00000000 00000000 0010005C *B0000108...+.....*
 020 00000000 500C10C6 00000000 001007C4 001004F0 12BEF838 000C1028 12BEEF70 *...&..F...D..0.8.*
```

Note: The AP domain is useful within a DFHSM0103 dump because the violation was caught during normal execution of the application and not at task termination time.

Output via: VERBX DFHPD690 ‘AP’

Findings / Solution

- Findings
  - Program READUPDT was responsible for the violation
  - Violation was caught between an EXEC CICS Getmain command issued at offset x'86' and an EXEC CICS SUSPEND command issued at offset x'B0'
  - Inspection of program READUPDT:
    - Shows register 4 originally pointed to the getmained storage but was incremented by x'3BC' just prior to a MVCL instruction to move x'20' bytes. This move instruction was the cause of the violation.
- Possible Solutions
  - If you truly want to move data into this getmained storage:
    - Adjust the increment of register 4 to a value that falls within the getmained storage, allowing for x'20' bytes to be moved.
  - If the move was not meant to be:
    - Remove the code associated with the move

Additional Product Resources

- Engage with the community, share expertise & get answers on dW Answers
  https://developer.ibm.com/answers/index.html
- Follow IBM_CICS support on Twitter to see the latest updates
  http://www.ibm.com/support/docview.wss?uid=swg21384915
- Find CICS documentation in the IBM Knowledge Center
  https://developer.ibm.com/answers/questions/170485/finding-cics-product-documentation-in-ibm-knowledg.html
- Find software & hardware requirements in CICS Detailed System Requirements
  http://www.ibm.com/support/docview.wss?uid=swg27006382
- Learn from replays of CICS & CICS Tools Webcasts
  http://www.ibm.com/support/docview.wss?uid=swg27007244
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically
  http://www.ibm.com/software/websphere/support/d2w.html

References

- CICS Messages and Codes (GC34-7283-00) Version 5 Release 2
- CICS Problem Determination Guide (GC34-7287-00) Version 5 Release 2
- CICS Supplied Transactions (SC34-7292-00) Version 5 Release 2
- CICS System Definition Guide (SC34-7293-00) Version 5 Release 2
- CICS Trace Entries (SC34-7295-00) Version 5 Release 2

Connect with us!

1. **Get notified on upcoming webcasts**
   Send an e-mail to wsehelp@us.ibm.com with subject line “wste subscribe” to get a list of mailing lists and to subscribe
2. **Tell us what you want to learn**
   Send us suggestions for future topics or improvements about our webcasts to wsehelp@us.ibm.com

Questions and Answers

Additional WebSphere Product Resources

- Learn about upcoming WebSphere Support Technical Exchange webcasts, and access previously recorded presentations at: http://www.ibm.com/software/websphere/support/supp_tech.html
- Discover the latest trends in WebSphere Technology and implementation, participate in technically-focused briefings, webcasts and podcasts at: http://www.ibm.com/developerworks/websphere/community/
- Join the Global WebSphere Community: http://www.websphereusergroup.org
- Access key product show-me demos and tutorials by visiting IBM Education Assistant: http://www.ibm.com/software/info/education/assistant
- View a webcast replay with step-by-step instructions for using the Service Request (SR) tool for submitting problems electronically: http://www.ibm.com/software/websphere/support/d2w.html
- Sign up to receive weekly technical My Notifications emails: http://www.ibm.com/software/support/einfo.html