Trusted Access Manager for z/OS 1.1
CA RS 2204 Service List

Service	Description	Type
LU03293	TAMR SVC-132 EXIT FIX FOR RACXTRT FRONTEND PROCESSING	PTF
LU03321	MAINTAIN TAMID FOR TAMR ELEVATION EVENTS	PTF
LU03342	TAMR PROVIDE AUDIT RECORDS WHEN TIMEBOX EXPIRES	PTF
LU04998	SECURITY OR INTEGRITY PROBLEM	** PRP **
LU05000	SECURITY OR INTEGRITY PROBLEM	** PRP **
	The CA RS 2204 service count for this release is 5	

FMID	Service	Description	Type
CFH0110	LU03293	TAMR SVC-132 EXIT FIX FOR RACXTRT FRONTEND PROCESSING	PTF
	LU03321	MAINTAIN TAMID FOR TAMR ELEVATION EVENTS	PTF
	LU03342	TAMR PROVIDE AUDIT RECORDS WHEN TIMEBOX EXPIRES	PTF
	LU05000	SECURITY OR INTEGRITY PROBLEM	** PRP **
The CA RS 2204 service count for this FMID is 4			

FMID	Service	Description	Type
CSJV110	LU04998	SECURITY OR INTEGRITY PROBLEM	** PRP **

The CA RS 2204 service count for this FMID is 1

Service	Details
LU03293	LU03293 M.C.S. ENTRIES = ++PTF (LU03293) TAMR SVC-132 EXIT FIX FOR RACXTRT FRONTEND PROCESSING PROBLEM DESCRIPTION: TRUSTED ACCESS MANAGER FOR Z FOR RACF DOES NOT PROPERLY PASS CONTROL TO THE RACF SVC 132(RACXTRT) PROCESSING ROUTINE FROM THE TAMR FRONT END TO SVC 132. SYMPTOMS: ABNORMAL TERMINATION FOLLOWING A SVC 132(RACXTRT) CALL WHEN TRYING TO FREE THE WORKAREA STORAGE THAT WAS SUPPOSED TO BE OBTAINED DURING NORMAL PROCESSING OF THE SUPERVISOR CALL. IMPACT: AN SVC 132 CALL FOR RACXTRT ABENDS WHEN TRUSTED ACCESS MANAGER FOR Z FOR RACF IS ACTIVE. CIRCUMVENTION: PRODUCT(S) AFFECTED: TRUSTED ACCESS MANAGER FOR Z Release 1.1 Related Problem: TAMZ 15155 (C) 2022 Broadcom Inc and/or its subsidiaries; All rights reserved R00047-TAM011 DESC(TAMR SVC-132 EXIT FIX FOR RACXTRT FRONTEND PROCESSING). ++VER (Z038) FMID (CFH0110) PRE (LU00584 LU04112 SO14114 SO16218 SO16320) SUP (LT03293) ++HOLD (LU03293) SYSTEM FMID(CFH0110) REASON (DYNACT) DATE (22075) COMMENT (

```
+----------------------------------------------------------------------+
|     TRUSTED ACCESS MANAGER FOR Z                      Release 1.1     |
+----------+-----------------------------------------------------------+
|SEQUENCE  | After Apply                                               |
+----------+-----------------------------------------------------------+
|PURPOSE   | To implement change without requiring IPL                 |
+----------+-----------------------------------------------------------+
|USERS     | TAMz Users                                                |
|AFFECTED  |                                                           |
+----------+-----------------------------------------------------------+
|KNOWLEDGE | TAMz SMP/e environment                                    |
|REQUIRED  | Operator commands                                         |
+----------+-----------------------------------------------------------+
|ACCESS    | TAMz SMP/e and runtime environments                       |
|REQUIRED  | Operator commands                                         |
+----------+-----------------------------------------------------------+
*************************
* STEPS    TO    PERFORM *
*************************
1.   Deploy PTF to your runtime libraries
2.   F LLA,REFRESH
3.   Restart TAMRSTC with a REINIT; for example, "S TAMRSTC,,,REINIT"
).
```

Service	Details
LU03321	LU03321 M.C.S. ENTRIES = ++PTF (LU03321) MAINTAIN TAMID FOR TAMR ELEVATION EVENTS ENHANCEMENT DESCRIPTION: Trusted Access Manager for RACF for z now gives the user the ability to create a comprehensive Elevation report that ties all the events during an Elevation period together. Each Elevation is associated with a unique TAMID, which is deleted at the time of Deelevation. The TAMID is included in the LOGSTR of the RACF events. PRODUCT(S) AFFECTED: TRUSTED ACCESS MANAGER FOR Z Release 1.1 Related Problem: TAMZ 14288 (C) 2022 Broadcom Inc and/or its subsidiaries; All rights reserved R00049-TAM011 DESC(MAINTAIN TAMID FOR TAMR ELEVATION EVENTS). ++VER (Z038) FMID (CFH0110) PRE (LU00584 LU04112 SO08972 SO10581 SO12359 SO14114 SO15058 SO15557 SO15558 SO15725 SO16059 SO16218 SO16320) SUP (AC13107 AS12359 AS14114 LT02557 LT02571 LT02795 LT02830 LT02831 LT02832 LT03293 LT03313 LT03321 LU02795 LU02830 LU03293 LU03313 SO10812 SO13553 SO13783 SO14064 SO14102 SO15020 SO15516 ST10812 ST13553 ST13783 ST14064 ST14102 ST15020 ST15516) ++HOLD (LU03321) SYSTEM FMID(CFH0110) REASON (DDDEF) DATE (22075) COMMENT (

```
+----------------------------------------------------------------------+
|      TRUSTED ACCESS MANAGER FOR Z                  Release 1.1       |
+----------+-----------------------------------------------------------+
|SEQUENCE  | Before Apply                                             |
+----------+-----------------------------------------------------------+
|PURPOSE   | To update DDDEF's required for new modules added by PTF   |
+----------+-----------------------------------------------------------+
|USERS     | Installer                                                 |
|AFFECTED  |                                                           |
+----------+-----------------------------------------------------------+
|KNOWLEDGE | SMP/e                                                     |
|REQUIRED  | JCL                                                       |
+----------+-----------------------------------------------------------+
|ACCESS    | Update access to SMP/e CSI                                |
|REQUIRED  |                                                           |
+----------+-----------------------------------------------------------+
*************************
* STEPS    TO    PERFORM *
*************************
1. Run this job to determine if the new DDDEF is already present
in your CSI:
//STEP1     EXEC PGM=GIMSMP,REGION=4M
//SMPCSI    DD   DISP=SHR,DSN=cai.your.CSI   <-- Provide your CSI
//SMPCNTL   DD   *
```

Service	Details

	``
	SET BDY(CAIT0) /* <-- Provide name of target zone */ .
	LIST DDDEF(SCEELKED).
	/*
	If the job ends with a return code of zero then the DDDEF
	is already defined. You do not need to take any action.
	If the job ends with a return code of four or higher then continue
	with the next step.
	2. Run this job to add the SCEELKED DDDEF:
	//STEP2 EXEC PGM=GIMSMP,REGION=4M
	//SMPCSI DD DISP=SHR,DSN=cai.your.CSI <-- Provide your CSI
	//SMPCNTL DD *
	SET BDY(CAIT0) /* <-- Provide name of target zone */ .
	ADD DDDEF(SCEELKED)
	SHR DA(CEE.SCEELKED) /* <-- Verify dataset name */ .
	/*
	The job should end with a return code of zero.
	).
	++HOLD (LU03321) SYSTEM FMID(CFH0110)
	REASON (DYNACT) DATE (22075)
	COMMENT (
	+---+
	| TRUSTED ACCESS MANAGER FOR Z Release 1.1 |
	+----------+--+
	|SEQUENCE
		After Apply |
		+----------+--+
		|PURPOSE
			To activate maintenance without requiring an IPL. |
			+----------+--+
			|USERS
				All TAMz users.

AFFECTED		 +----------+--+ 	KNOWLEDGE	SMP/e
REQUIRED	Operator commands
	TAMR commands	 +----------+--+ 	ACCESS	SMP/e
REQUIRED	Operator commands
	TAMR commands
	Read access to TAM.DISPLAY.ALLUSERS in the CATAM class | +----------+--+ ************************* * STEPS TO PERFORM * ************************* 1. Apply PTF 2. F LLA REFRESH 3. Logoff all actively elevated users. Do not log them back on until the next step is completed. 4. Issue TAMR DEELEVATE(userid) CLASS(classname) for all active elevations. Issue TAMR LIST ACTIVE for a list of active elevations. 5. Issue S TAMRSTC,,,REINIT to reimplant TAMRPC00). ```

Service	Details
LU03342	LU03342 M.C.S. ENTRIES = ++PTF (LU03342) TAMR PROVIDE AUDIT RECORDS WHEN TIMEBOX EXPIRES ENHANCEMENT DESCRIPTION: Trusted Access Manager for RACF for z will now allow TAMz for RACF DEELEVATE events to be logged to the SMF, Journal, ENF71, OPS/MVS, CSV and JSON reports when an elevation expires due to timeout. PRODUCT(S) AFFECTED: TRUSTED ACCESS MANAGER FOR Z Release 1.1 Related Problem: TAMZ 14757 (C) 2022 Broadcom Inc and/or its subsidiaries; All rights reserved R00050-TAM011

```
DESC(TAMR PROVIDE AUDIT RECORDS WHEN TIMEBOX EXPIRES).
++VER (Z038)
FMID (CFH0110)
PRE ( LU00584 LU04112 SO08972 SO10581 SO12359 SO14114
SO15058 SO15557 SO15558 SO15725 SO16059 SO16218
SO16320  )
SUP ( AC13107 AS12359 AS14114 LT02557 LT02571 LT02795
LT02830 LT02831 LT02832 LT02977 LT03156 LT03293
LT03313 LT03321 LT03342 LU02795 LU02830 LU02977
LU03293 LU03313 LU03321 SO10812 SO13553 SO13783
SO14064 SO14102 SO15020 SO15516 ST10812 ST13553
ST13783 ST14064 ST14102 ST15020 ST15516  )
++HOLD (LU03342) SYSTEM FMID(CFH0110)
REASON (IPL    )   DATE (22076)
COMMENT (
+-------------------------------------------------------------------+
|      TRUSTED ACCESS MANAGER FOR Z                  Release 1.1     |
+----------+--------------------------------------------------------+
|SEQUENCE  | After Apply                                            |
+----------+--------------------------------------------------------+
|PURPOSE   | To implement changes                                   |
+----------+--------------------------------------------------------+
|USERS     | TAMz Users and Admins                                  |
|AFFECTED  |                                                        |
+----------+--------------------------------------------------------+
|KNOWLEDGE | TAMz SMP/e Environment                                 |
|REQUIRED  | Operator Commands                                      |
|          | IPL Process                                            |
+----------+--------------------------------------------------------+
|ACCESS    | TAMz SMP/e Environment                                 |
|REQUIRED  | Operator Commands                                      |
|          | IPL Process                                            |
+----------+--------------------------------------------------------+
*************************
* STEPS    TO    PERFORM *
*************************
1.  Apply and deploy PTF to your TAMz runtime libraries.
2.  *REQUIRED* IPL the system.  This fix makes changes to stubs
that will need to be re-implanted.
3.  start TAMRSTC by issuing the start command for TAMRSTC.
```

Service	Details
	For example: /S TAMRSTC This will restart TAMRSTC and re-implant updated modules. NOTE: After this enhancement, TAMRSTC will be a persistent task. To mark TAMz for RACF inactive, use "/P TAMRSTC", the INACT parameter has been deprecated. (e.g. "/S TAMRSTC,,,INACT") In order to issue a REINIT, first stop the persistant task then issue the start with REINIT (e.g. "/P TAMRSTC" "/S TAMRSTC,,,REINIT")).

For example: /S TAMRSTC

This will restart TAMRSTC and re-implant updated modules.

NOTE: After this enhancement, TAMRSTC will be a persistent task.

To mark TAMz for RACF inactive, use "/P TAMRSTC", the

Service	Details

LU04998	LU04998 M.C.S. ENTRIES = ++PTF (LU04998)
	
	SECURITY OR INTEGRITY PROBLEM
	PROBLEM DESCRIPTION:
	Security or Integrity Problem.
	For more details access Security Advisories using the following URL:
	support.broadcom.com/security-advisory/security-advisories-list.html
	Broadcom recommends that you subscribe to notifications for Security
	Advisories for the associated products that you support in your
	organization. Please use the following URL to register for proactive
	notifications: https://support.broadcom.com/user/notifications.html
	SYMPTOMS:
	N/A
	IMPACT:
	Security or Integrity Problem.
	CIRCUMVENTION:
	N/A
	PRODUCT(S) AFFECTED:
	MF Security JVM Release 1.1
	MF Security JVM Release 1.1
	Related Problem:
	SJV 16386
	(C) 2022 Broadcom Inc and/or its subsidiaries; All rights reserved
	R00020-SJV011
	
	DESC(SECURITY OR INTEGRITY PROBLEM).
	++VER (Z038)
	FMID (CSJV110)
	PRE (LU04129 SO07610 SO10051 SO10217 SO11254 SO12468)
	SUP (AC04995 LT04998 ST06110)
	++HOLD (LU04998) SYSTEM FMID(CSJV110)
	REASON (DYNACT) DATE (22066)
	COMMENT (
	<pre>+---+
	| MF Security JVM Release 1.1 |
	+----------+--+
	|SEQUENCE | After Apply |
	+----------+--+
	|PURPOSE | Implement Sec/Int Mitigation |
	+----------+--+
	|USERS | TAMZ SMP/e environment |
	|AFFECTED | Operator Commands |
	+----------+--+
	|KNOWLEDGE | TAMZ SMP/e environment |
	|REQUIRED | Operator Commands |
	+----------+--+
	|ACCESS | TAMZ SMP/e environment |
	|REQUIRED | Operator Commands |
	+----------+--+</pre>**************************
	* STEPS TO PERFORM *
	**************************
	1. Deploy new sjvv1.jar to your deployment libraries
	For example: /u/user/sjvm

Service	Details
	2. Restart SJVM Started Task
	For example: /P SJVSTC
	/S SJVSTC
	).
	LINK('../sjvv1.jar')
	PARM(PATHMODE(0,7,0,0)) .

Service	Details
LU05000	LU05000 M.C.S. ENTRIES = ++PTF (LU05000) SECURITY OR INTEGRITY PROBLEM PROBLEM DESCRIPTION: Security or Integrity Problem. For more details access Security Advisories using the following URL: support.broadcom.com/security-advisory/security-advisories-list.html Broadcom recommends that you subscribe to notifications for Security Advisories for the associated products that you support in your organization. Please use the following URL to register for proactive notifications: https://support.broadcom.com/user/notifications.html SYMPTOMS: N/A IMPACT: Security or Integrity Problem. CIRCUMVENTION: N/A PRODUCT(S) AFFECTED: TRUSTED ACCESS MANAGER FOR Z Release 1.1 Related Problem: TAMZ 16383 (C) 2022 Broadcom Inc and/or its subsidiaries; All rights reserved R00056-TAM011 DESC(SECURITY OR INTEGRITY PROBLEM). ++VER (Z038) FMID (CFH0110) PRE (LU03086 LU03940 LU04005 LU04112) SUP (CC13107 LT05000) ++HOLD (LU05000) SYSTEM FMID(CFH0110) REASON (DYNACT) DATE (22066) COMMENT (+---+ | TRUSTED ACCESS MANAGER FOR Z Release 1.1 | +----------+--+ |SEQUENCE | After Apply | +----------+--+ |PURPOSE | Implement Sec/Int Mitigation | +----------+--+ |USERS | All TAMz Users | |AFFECTED | | +----------+--+ |KNOWLEDGE | TAMZ SMP/e environment | |REQUIRED | Operator Commands | +----------+--+ |ACCESS | TAMZ SMP/e environment | |REQUIRED | Operator Commands | +----------+--+ ************************** * STEPS TO PERFORM * ************************** 1. Deploy new sjvv1.jar to your deployment libraries For example: /u/user/sjvm 2. Restart SJVM Started Task

Service	Details
	For example: /P SJVSTC
	/S SJVSTC
	).
	BINARY
	LINK('../tam-microservice.war')
	PARM(PATHMODE(0,7,5,5)) .
	MCS LU03293 STARTS ON PAGE 0002
	MCS LU03321 STARTS ON PAGE 0003
	MCS LU03342 STARTS ON PAGE 0007
	MCS LU04998 STARTS ON PAGE 0011
	MCS LU05000 STARTS ON PAGE 0012

Service	Details
	For example: /P SJVSTC
	/S SJVSTC
	).
	BINARY

Product Family	Product	Release
Security	MF SECURITY JVM	01.01.00
	TRUSTED ACCESS MANAGER FOR Z	01.01.00

The CA RS 2204 Product/Component Count for this release is 2

CA RS Level	Service	FMID
CAR2204	LU05000	CFH0110
	LU04998	CSJV110
	LU03342	CFH0110
	LU03321	CFH0110
	LU03293	CFH0110
CAR2202	LU04129	CSJV110
	LU04112	CFH0110
	LU03313	CFH0110
CAR2201	LU04005	CFH0110
	LU03940	CFH0110
CAR2111	LU03086	CFH0110
	LU02977	CFH0110
	LU02830	CFH0110
	LU02795	CFH0110
CAR2108	SO16320	CFH0110
	LU00584	CFH0110
CAR2107	SO16218	CFH0110
CAR2104	SO16059	CFH0110
	SO15725	CFH0110
	SO15558	CFH0110
	SO15557	CFH0110
	LU00206	CFH0110
CAR2012	SO15516	CFH0110
	SO15058	CFH0110
	SO15020	CFH0110
CAR2010	SO14114	CFH0110
	SO14102	CFH0110
	SO14064	CFH0110
	SO13783	CFH0110
	SO13553	CFH0110
	SO12468	CSJV110
	SO11254	CSJV110
CAR2006	SO12878	CFH0110
	SO12359	CFH0110
	SO10812	CFH0110
CAR2001	SO11137	CFH0110
	SO10220	CFH0110
	SO10217	CSJV110
	SO10051	CSJV110
CAR1911	SO10581	CFH0110
	SO07548	CFH0110
CAR1910	SO09874	CSJV110
	SO08972	CFH0110
CAR1908	SO07549	CSJV110
	SO06988	CSJV110
CAR1907	SO07610	CSJV110
	SO07607	CFH0110