CA Trusted Access Manager for z/OS 1.1
CA RS 2010 Service List

Service	Description	Type
SO11254	TCP/IP ACTIVE ALWAYS REQUIRED FOR START	PTF
SO12468	FALLBACK PROCESSING FOR TAMZ	PTF
SO13553	FIX STORAGE OVERLAY RESULTING IN 30XCLASS LIMIT IN TAMZ RACF	** PRP **
SO13783	FIX S0C4 IN TAMRPC00	PTF
SO14064	FIX TAMRDQ48 SD78-04 ABEND	PTF
SO14102	TAMRCX01 ENHANCEMENT FOR REQUEST=VERIFY,ENVIRON=CREATE,APPL=	PTF
SO14114	ADD SUPPORT FOR ELEVATE TO GAIN RACF PRIVILEGES	PTF

The CA RS 2010 service count for this release is 7

CA Trusted Access Manager for z/OS
CA RS 2010 Service List for CFH0110

FMID	Service	Description	Type
CFH0110	SO13553	FIX STORAGE OVERLAY RESULTING IN 30XCLASS LIMIT IN TAMZ RACF	** PRP **
	SO13783	FIX S0C4 IN TAMRPC00	PTF
	SO14064	FIX TAMRDQ48 SD78-04 ABEND	PTF
	SO14102	TAMRCX01 ENHANCEMENT FOR REQUEST=VERIFY,ENVIRON=CREATE,APPL=	PTF
	SO14114	ADD SUPPORT FOR ELEVATE TO GAIN RACF PRIVILEGES	PTF

The CA RS 2010 service count for this FMID is 5

CA Trusted Access Manager for z/OS
CA RS 2010 Service List for CSJV110

FMID	Service	Description	Type
CSJV110	SO11254	TCP/IP ACTIVE ALWAYS REQUIRED FOR START	PTF
	SO12468	FALLBACK PROCESSING FOR TAMZ	PTF

The CA RS 2010 service count for this FMID is 2

Service	Details
SO11254	SO11254 M.C.S. ENTRIES = ++PTF (SO11254) TCP/IP ACTIVE ALWAYS REQUIRED FOR START PROBLEM DESCRIPTION: When the SJV STC starts, it checks to see if TCP/IP is active. If it is not, initialization fails. SYMPTOMS: Message: SJV0520E TCPIP is not active - ending IMPACT: SJV STC will not start unless TCP/IP is active CIRCUMVENTION: None PRODUCT(S) AFFECTED: MF Security JVM Release 1.1 Related Problem: SJV 16 Copyright (C) 2020 CA. All rights reserved. R00014-SJV011-SP1 DESC(TCP/IP ACTIVE ALWAYS REQUIRED FOR START). ++VER (Z038) FMID (CSJV110) PRE (SO06988 SO07610 SO10051 SO10217) SUP (SO09874 ST06110 ST09874 ST11254) ++HOLD (SO11254) SYSTEM FMID(CSJV110) REASON (DYNACT) DATE (20268) COMMENT (+---+ | MF Security JVM Release 1.1 | +----------+--+ |SEQUENCE | After Apply | +----------+--+ |PURPOSE | Enable new code | +----------+--+ |USERS | All users | |AFFECTED | | +----------+--+ |KNOWLEDGE | z/OS Console | |REQUIRED | | +----------+--+ |ACCESS | z/OS Console | |REQUIRED | | +----------+--+ ************************** * STEPS TO PERFORM * ************************** 1. LLA Refresh (if applicable) 2. Start SJV STC). LINK('../sjvv1.jar') PARM(PATHMODE(0,7,0,0)) .

<table>
<tr><th>Service</th><th>Details</th></tr>
<tr><td>SO12468</td><td>

```
SO12468   M.C.S. ENTRIES  = ++PTF (SO12468)

FALLBACK PROCESSING FOR TAMZ
ENHANCEMENT DESCRIPTION:
This enhancement enables Trusted Access Manager for z/OS (TAMz)
users to implement a fallback procedure in the event that the
Service Desk Ticket Validation is unable to be performed.  Users who
are given the FALLBACK permit for TAMz for a CLASS can get access
to the CLASS even when ticket validation cannot be performed; for
example, when the Service Desk is offline for maintenance.
PRODUCT(S) AFFECTED:
MF Security JVM                                              Release 1.1
Trusted Access Manager for z/OS                              Release 1.1
Related Problem:
SJV    19
Copyright (C) 2020 CA. All rights reserved. R00016-SJV011-SP1

DESC(FALLBACK PROCESSING FOR TAMZ).
++VER (Z038)
FMID (CSJV110)
PRE ( SO10217 SO11254 )
SUP ( SO07610 SO10051 ST06110 ST07610 ST10051 ST12346
ST12468  )
++HOLD (SO12468) SYSTEM FMID(CSJV110)
REASON (DYNACT )   DATE (20268)
COMMENT (
+----------------------------------------------------------------------+
|     MF Security JVM                                 Release 1.1      |
+----------+-----------------------------------------------------------+
|SEQUENCE  | After Apply                                               |
+----------+-----------------------------------------------------------+
|PURPOSE   | Applay feature for Fallback Resource Check on TAMz        |
+----------+-----------------------------------------------------------+
|USERS     | TAMz Users                                                |
|AFFECTED  |                                                           |
+----------+-----------------------------------------------------------+
|KNOWLEDGE | SMP/e                                                     |
|REQUIRED  | Operator commands                                         |
|          | TAMz install/config DD's                                  |
|          | TAMz install/config OMVS directories                      |
+----------+-----------------------------------------------------------+
|ACCESS    | SMP/e                                                     |
|REQUIRED  | Operator commands                                         |
|          | TAMz install/config DD's                                  |
|          | TAMz install/config OMVS directories                      |
+----------+-----------------------------------------------------------+
**************************
* STEPS    TO    PERFORM *
**************************
1. Stop SJVSTC
2. Make sure new copy of SJVJAR and SJVFBCK are in the correct USS
directory:
- SJVJAR (sjvv1.jar) should replace the old version of sjvv1.jar
- SJVFBCK (SJVM-Fallback.jar) should be placed in the same directory
```

</td></tr>
</table>

Service	Details
	as sjvv1.jar - If you alread have an ENV for SJV be sure to copy: CLASSPATH=$CLASSPATH:"${SJV_HOME}"/SJVM-Fallback.jar into it just before the CLASSPATH variable is exported. Otherwise use the provided SJVENV 3. Restart SJVSTC). LINK('../SJVM-Fallback.jar') PARM(PATHMODE(0,7,0,0)) . LINK('../sjvv1.jar') PARM(PATHMODE(0,7,0,0)) .

<table>
<tr><th>Service</th><th>Details</th></tr>
<tr><td>SO13553</td><td>SO13553   M.C.S. ENTRIES = ++PTF (SO13553)

FIX STORAGE OVERLAY RESULTING IN 30XCLASS LIMIT IN TAMZ RACF
PROBLEM DESCRIPTION:
After SO12359 is applied, an internal storage overlay has occurred
which results in an upper limit of 31 Trusted Access Manager for Z
CLASSes in the internal tables.
SYMPTOMS:
After issuing RACF ADDGROUP and TAMR REFRESH commands to harden
newly defined Trusted Access Manager for Z CLASSes into the internal
tables, TAMR LIST TAM output will only properly show the first 31
CLASSes; beyond that, behavior is unpredictable. Some may show,
some may not, even though a "RACF LISTGROUP TAMRCLSS" could
indicate more than 31 subgroups attached to it.
IMPACT:
Trusted Access Manager for Z implementations are effectively limited
to a 31-CLASS upper limit. Any CLASSes after the 31st may or may
not get hardened into the internal tables for use with ELEVATEs.
CIRCUMVENTION:
To ensure all CLASSes are hardened and available for use, stick to a
30-CLASS upper limit until this PTF is applied.
PRODUCT(S) AFFECTED:
TRUSTED ACCESS MANAGER FOR Z   Release 1.1
Related Problem:
TAMZ   17
Copyright (C) 2020 CA. All rights reserved. R00013-TAM011-SP1

DESC(FIX STORAGE OVERLAY RESULTING IN 30XCLASS LIMIT IN TAMZ RACF).
++VER (Z038)
FMID (CFH0110)
PRE (SO12359)
SUP (AS12359 ST13553)
++HOLD (SO13553) SYSTEM FMID(CFH0110)
REASON (DYNACT)   DATE (20258)
COMMENT (
+---+
| TRUSTED ACCESS MANAGER FOR Z   Release 1.1 |
+----------+--+
|SEQUENCE | After Apply |
+----------+--+
|PURPOSE | To implement solution without needing an IPL. |
+----------+--+
|USERS | All Trusted Access Manager for Z Users. |
AFFECTED		 +----------+--+ 	KNOWLEDGE	SMP/e
REQUIRED	Operator Commands
	Trusted Access Manager for Z REFRESH command.	 +----------+--+ 	ACCESS	SMP/e
REQUIRED	Operator Commands
	Trusted Access Manager for Z REFRESH command.	 +----------+--+ **************************</td></tr>
</table>

Service	Details
	* STEPS TO PERFORM * ************************** 1. Apply PTF 2. Issue LLA REFRESH 3. ***REQUIRED*** Restart TAMRSTC with REINIT: "s TAMRSTC,,,REINIT" NOTE: This fix adjusts PC Routine "TAMRPC00" that is implanted during the startup of TAMRSTC. This PC Routine is not reimplanted unless a REINIT occurs, or this is the first start of TAMRSTC since an IPL. Failure to issue a REINIT will cause TAMR REFRESH to return to the original 31-CLASS limit when issued.).

Service	Details
SO13783	SO13783 M.C.S. ENTRIES = ++PTF (SO13783) FIX S0C4 IN TAMRPC00 PROBLEM DESCRIPTION: TAMRPC00 S0C4 at +17DC when in cross-memory mode during SMF and CIEM functions for Trusted Access Manager for z/OS events. SYMPTOMS: Internal recovery routines will capture the failing events, and mark the Trusted Access Manager for z/OS product as INACTIVE, preventing any further TAMR commands from being issued, records being cut, etc. Since these appear around logging events and that it only takes 3 of them to mark the product INACTIVE, this can happen in quick succession. So, even when TAMRSTC is restarted to reactivate the product, it can return to an INACTIVE state relatively quickly. IMPACT: Depending on the level of logging the product is attempting to perform when active, it can reenter INACTIVE state quickly after restarts and become effectively inoperable. CIRCUMVENTION: N/A PRODUCT(S) AFFECTED: TRUSTED ACCESS MANAGER FOR Z Release 1.1 Related Problem: TAMZ 18 Copyright (C) 2020 CA. All rights reserved. R00014-TAM011-SP1 DESC(FIX S0C4 IN TAMRPC00). ++VER (Z038) FMID (CFH0110) PRE (SO08972 SO10812 SO12359) SUP (ST13783) ++HOLD (SO13783) SYSTEM FMID(CFH0110) REASON (DYNACT) DATE (20258) 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 | +----------+--+ |ACCESS | TAMz SMP/e Environment | |REQUIRED | Operator commands | +----------+--+ ************************** * STEPS TO PERFORM * ************************** 1. Apply PTF

Service	Details
	2. LLA REFRESH 3. Issue a REINIT of TAMRSTC to reimplant the PC routine (TAMRPC00) and exits TAMRDQ48 and TAMRIX02.).

<table>
<tr><th>Service</th><th>Details</th></tr>
<tr><td>SO14064</td><td>SO14064   M.C.S. ENTRIES = ++PTF (SO14064)

FIX TAMRDQ48 SD78-04 ABEND
PROBLEM DESCRIPTION:
TAMRDQ48 abends with SD78-04 when trying to release storage in
LSQA, when no TCB is present.
SYMPTOMS:
TAMRDQ48 throws an SD78-04 abend and takes a dump. After 3 dumps,
TAMR is marked inactive until another "S TAMRSTC" is issued.
IMPACT:
TAMRDQ48 throws an SD78-04 abend and takes a dump. After 3 dumps,
TAMR is marked inactive until another "S TAMRSTC" is issued.
CIRCUMVENTION:
N/A
PRODUCT(S) AFFECTED:
TRUSTED ACCESS MANAGER FOR Z   Release 1.1
Related Problem:
TAMZ   20
Copyright (C) 2020 CA. All rights reserved. R00018-TAM011-SP1

DESC(FIX TAMRDQ48 SD78-04 ABEND).
++VER (Z038)
FMID (CFH0110)
PRE (SO08972 SO10812 SO13783)
SUP (ST14064)
++HOLD (SO14064) SYSTEM FMID(CFH0110)
REASON (DYNACT)   DATE (20258)
COMMENT (
+--+
| TRUSTED ACCESS MANAGER FOR Z   Release 1.1 |
+----------+---+
|SEQUENCE | After Apply |
+----------+---+
|PURPOSE | To activate fix without an IPL. |
+----------+---+
|USERS | All TAMz Users. |
|AFFECTED | |
+----------+---+
|KNOWLEDGE | TAMz SMP/e |
|REQUIRED | Operator commands |
+----------+---+
|ACCESS | TAMz SMP/e |
|REQUIRED | Operator commands |
+----------+---+
****
* STEPS   TO   PERFORM *
****
1. After apply, issue LLA REFRESH
2. Restart TAMRSTC with a REINIT (e.g. "S TAMRSTC,,,REINIT"), to
re-implant modified modules: TAMRBCG0 and TAMRDQ48.
).</td></tr>
</table>

CA Trusted Access Manager for z/OS 1.1
CA RS 2010 - PTF SO14102 Details

Service	Details
SO14102	SO14102 M.C.S. ENTRIES = ++PTF (SO14102) TAMRCX01 ENHANCEMENT FOR REQUEST=VERIFY,ENVIRON=CREATE,APPL= ENHANCEMENT DESCRIPTION: Added support for RACROUTE REQUEST=VERIFY,ENVIRON=CREATE,APPL= PRODUCT(S) AFFECTED: TRUSTED ACCESS MANAGER FOR Z Release 1.1 Related Problem: TAMZ 21 Copyright (C) 2020 CA. All rights reserved. R00019-TAM011-SP1 DESC(TAMRCX01 ENHANCEMENT FOR REQUEST=VERIFY,ENVIRON=CREATE,APPL=). ++VER (Z038) FMID (CFH0110) PRE (SO08972 SO10812 SO13783) SUP (ST14102) ++HOLD (SO14102) SYSTEM FMID(CFH0110) REASON (ENH) DATE (20258) COMMENT (+--+ | TRUSTED ACCESS MANAGER FOR Z Release 1.1 | +-----------+--+ |SEQUENCE | After Apply | +-----------+--+ |PURPOSE | To implement enhancement without requiring an IPL | | | | +-----------+--+ |USERS | All TAMz users | |AFFECTED | | +-----------+--+ |KNOWLEDGE | TAMz SMP/e | |REQUIRED | Operator commands | +-----------+--+ |ACCESS | TAMz SMP/e | |REQUIRED | Operator commands | +-----------+--+ ************************** * STEPS TO PERFORM * ************************** 1. Apply and deploy this PTF 2. Issue LLA REFRESH 3. Restart TAMRSTC with a REINIT to re-implant TAMRCX01 and TAMRIX02 exits).

Service	Details
SO14114	SO14114 M.C.S. ENTRIES = ++PTF (SO14114) The following items are included in this solution: 1. ADD SUPPORT FOR ELEVATE TO GAIN RACF PRIVILEGES 2. ADD SVC 132 EXIT ROUTINE TO TAMR == ADD SUPPORT FOR ELEVATE TO GAIN RACF PRIVILEGES ENHANCEMENT DESCRIPTION: Trusted Access Manager for Z will now allow users to provide the following RACF USER ATTRIBUTES with an ELEVATE: SPECIAL, AUDITOR, ROAUDIT, and OPERATIONS. Users can now define TAMz Classes which will associate one or more of these 4 Attributes with a user when they elevate to the class. PRODUCT(S) AFFECTED: TRUSTED ACCESS MANAGER FOR Z Release 1.1 Related Problem: TAMZ 16 == ADD SVC 132 EXIT ROUTINE TO TAMR PROBLEM DESCRIPTION: 1. On De-elevation from a Trusted Access Manager for Z CLASS, the elevated access is retained on invocation of RACTRT or ICHEINTY by the user.e user. 2. Trusted Access Manager for Z for RACF SMF records appear to be 1 byte off in Logstream SYMPTOMS: 1. After an elevation is timed out and the user is DE-ELEVATED from a Trusted Access Manager for Z class, accesses or actions are still allowed by the elevation if RACXTRT or ICHEINTY is invoked. 2. When the user generates a TAMRSMF report, the logstream elements added by Trusted Access Manager for Z are displayed 1 byte to the right of the expected positions. IMPACT: 1. Trusted Access Manager for Z fails to revoke elevated access. 2. Trusted Access Manager for Z doesn't display the SMF records in the correc layout. CIRCUMVENTION: PRODUCT(S) AFFECTED: Trusted Access Manager for Z Version 1.1 Related Problem: TAMZ 19 Copyright (C) 2020 CA. All rights reserved. R00020-TAM011-SP1 DESC(ADD SUPPORT FOR ELEVATE TO GAIN RACF PRIVILEGES). ++VER (Z038) FMID (CFH0110) PRE (SO08972 SO10581 SO12359) SUP (AC13107 SO10812 SO13783 SO14064 SO14102 ST10812 ST13783 ST13852 ST13894 ST14064 ST14102 ST14114) ++HOLD (SO14114) SYSTEM FMID(CFH0110) REASON (ENH) DATE (20273) COMMENT (+---+ | TRUSTED ACCESS MANAGER FOR Z Release 1.1 | +----------+--+

Service	Details

```
|SEQUENCE  | After Apply                                                  |
+----------+--------------------------------------------------------------+
|PURPOSE   | To implement the TAMz for RACF Privilege Enhancement         |
+----------+--------------------------------------------------------------+
|USERS     | All TAMz Users.                                              |
|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 enhancement creates new Exit
stubs and updates some existing ones.  Changes to existing
exit stubs require an IPL to get refreshed.
3.  *REQUIRED* Update the TAMRSPGR CSDATA definitions.  In order
to define the new RACF USER Attributes into TAMz CLASSes, rerun
the the TAMRSPGR job to delete and redefine the TAMz supergroups
in RACF.
4.  After IPL completes and you have re-run TAMRSPGR to define the
new CSDATA fields, restart TAMRSTC to implant the exits and the
PC routines.
5.  Once startup completes, add any TAMz CLASSes with RACF USER
ATTRIBUTEs as needed.  For a brief overview, see the New
Feature description "Support for New Class Privileges for CA
Trusted Access Manager for Z for IBM RACF" in Techdocs.  For
specifics on the class changes, see "Add Class Groups" in the
"Using with IBM RACF" sections.
).
```

CA Trusted Access Manager for z/OS 1.1
CA RS 2010 Product/Component Listing

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

The CA RS 2010 Product/Component Count for this release is 2

CA RS Level	Service	FMID
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