

Trusted Access Manager for z/OS 1.1
CA RS 2111 Service List

Service	Description	Type
LU02795	SOC4 ABENDS IN TAMRIX02 WHEN IMPLANTED AFTER IBM ZSECURE	PTF
LU02830	RESTRUCTURE SMF LOGSTREAM TO POSITIONALLY FIX THE FIELDS	PTF
LU02977	FIX ABEND 0C4-3B IN TAMRPCST	PTF
LU03086	REPACKAGE UPGRADED CA NIM SM FOR SERVICENOW ORLANDO/PARIS	PTF
The CA RS 2111 service count for this release is 4		

Trusted Access Manager for z/OS
CA RS 2111 Service List for CFH0110

2

FMID	Service	Description	Type
CFH0110	LU02795	SOC4 ABENDS IN TAMRIX02 WHEN IMPLANTED AFTER IBM ZSECURE	PTF
	LU02830	RESTRUCTURE SMF LOGSTREAM TO POSITIONALLY FIX THE FIELDS	PTF
	LU02977	FIX ABEND OC4-3B IN TAMRPCST	PTF
	LU03086	REPACKAGE UPGRADED CA NIM SM FOR SERVICENOW ORLANDO/PARIS	PTF
The CA RS 2111 service count for this FMID is 4			

Service	Details																		
LU02795	<p>LU02795 M.C.S. ENTRIES = ++PTF (LU02795)</p> <p>SOC4 ABENDS IN TAMRIX02 WHEN IMPLANTED AFTER IBM ZSECURE</p> <p>PROBLEM DESCRIPTION:</p> <p>TAMRIX02 may throw a SOC4 abend during RACROUTE VERIFY processing when TAMRIX02 is implanted after the IBM zSecure exits for ICHRIX02.</p> <p>SYMPTOMS:</p> <p>SOC4 abend may occur at exit to TAMRIX02 (around +500 into the module).</p> <p>IMPACT:</p> <p>UserID's and STC's experiencing this will abend and fail to logon.</p> <p>CIRCUMVENTION:</p> <p>Mark TAMR as inactive until this fix is applied and deployed.</p> <p>To do so, issue: /S tamrstc,,,INACT</p> <p>Replacing "tamrstc" with your started task name (TAMRSTC by default).</p> <p>PRODUCT(S) AFFECTED:</p> <p>TRUSTED ACCESS MANAGER FOR Z Release 1.1</p> <p>Related Problem:</p> <p>TAMZ 14795</p> <p>Copyright (C) 2021 CA. All rights reserved. R00040-TAM011-SP1</p> <p>DESC(SOC4 ABENDS IN TAMRIX02 WHEN IMPLANTED AFTER IBM ZSECURE).</p> <p>++VER (Z038)</p> <p>FMID (CFH0110)</p> <p>PRE (LU00584 S008972 S010812 S013783 S014102 S014114 S015557 S015558 S015725 S016059 S016218 S016320)</p> <p>SUP (LT02795)</p> <p>++HOLD (LU02795) SYSTEM FMID(CFH0110)</p> <p>REASON (DYNACT) DATE (21299)</p> <p>COMMENT (</p> <table border="1"> <tr> <td>TRUSTED ACCESS MANAGER FOR Z</td><td>Release 1.1</td></tr> <tr> <td>SEQUENCE</td><td>After Apply</td></tr> <tr> <td>PURPOSE</td><td>To activate maintenance without requiring an IPL.</td></tr> <tr> <td>USERS</td><td>All Users.</td></tr> <tr> <td>AFFECTED</td><td></td></tr> <tr> <td>KNOWLEDGE</td><td>SMP/e</td></tr> <tr> <td>REQUIRED</td><td>Operator Commands</td></tr> <tr> <td>ACCESS</td><td>SMP/e</td></tr> <tr> <td>REQUIRED</td><td>Operator Commands</td></tr> </table> <p>*****</p> <p>* STEPS TO PERFORM *</p> <p>*****</p> <p>1. Apply PTF</p> <p>2. F LLA,REFRESH</p> <p>3. Issue S TAMRSTC,,,REINIT to reimplant TAMRIX02</p> <p>).</p>	TRUSTED ACCESS MANAGER FOR Z	Release 1.1	SEQUENCE	After Apply	PURPOSE	To activate maintenance without requiring an IPL.	USERS	All Users.	AFFECTED		KNOWLEDGE	SMP/e	REQUIRED	Operator Commands	ACCESS	SMP/e	REQUIRED	Operator Commands
TRUSTED ACCESS MANAGER FOR Z	Release 1.1																		
SEQUENCE	After Apply																		
PURPOSE	To activate maintenance without requiring an IPL.																		
USERS	All Users.																		
AFFECTED																			
KNOWLEDGE	SMP/e																		
REQUIRED	Operator Commands																		
ACCESS	SMP/e																		
REQUIRED	Operator Commands																		

Trusted Access Manager for z/OS 1.1
CA RS 2111 - PTF LU02830 Details

Service	Details																		
LU02830	<p>LU02830 M.C.S. ENTRIES = ++PTF (LU02830)</p> <p>RESTRUCTURE SMF LOGSTREAM TO POSITIONALLY FIX THE FIELDS</p> <p>PROBLEM DESCRIPTION:</p> <p>Trusted Access Manager for Z for RACF logs the ELEVATE and DEELEVATE command in the SMF Logstream exactly as entered, suppressing the CRED value. This causes the Logstream to display user credentials in case the CRED field is not entered properly or the credentials are entered outside the CRED field.</p> <p>SYMPTOMS:</p> <p>Credentials are displayed in the SMF logstream for TAMR Commands in case of an invalid keyword entered, for example CRAD instead of CRED. Credentials are displayed in the SMF logstream for TAMR Commands if IKJPARS fails to identify the contents of the CRED field.</p> <p>IMPACT:</p> <p>Trusted Access Manager for RACF for z fails to suppress the credentials entered in case of step-up authentication.</p> <p>CIRCUMVENTION:</p> <p>PRODUCT(S) AFFECTED:</p> <p>TRUSTED ACCESS MANAGER FOR Z Release 1.1</p> <p>Related Problem:</p> <p>TAMZ 14634</p> <p>Copyright (C) 2021 CA. All rights reserved. R00041-TAM011-SP1</p> <p>DESC (RESTRUCTURE SMF LOGSTREAM TO POSITIONALLY FIX THE FIELDS).</p> <p>++VER (Z038)</p> <p>FMID (CFH0110)</p> <p>PRE (LU00584 S008972 S012359 S014114 S015020 S015058 S015558 S015725 S016059 S016218 S016320)</p> <p>SUP (LT02557 LT02830)</p> <p>++HOLD (LU02830) SYSTEM FMID(CFH0110)</p> <p>REASON (DYNACT) DATE (21299)</p> <p>COMMENT (</p> <table border="1"> <tr> <td>TRUSTED ACCESS MANAGER FOR Z</td><td>Release 1.1</td></tr> <tr> <td>SEQUENCE</td><td>After Apply</td></tr> <tr> <td>PURPOSE</td><td>To activate maintenance without requiring an IPL.</td></tr> <tr> <td>USERS</td><td>All TAMz users.</td></tr> <tr> <td>AFFECTED</td><td></td></tr> <tr> <td>KNOWLEDGE</td><td>SMP/e</td></tr> <tr> <td>REQUIRED</td><td>Operator commands</td></tr> <tr> <td>ACCESS</td><td>SMP/e</td></tr> <tr> <td>REQUIRED</td><td>Operator commands</td></tr> </table> <p>*****</p> <p>* STEPS TO PERFORM *</p> <p>*****</p> <p>1. Apply PTF</p>	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	SMP/e	REQUIRED	Operator commands
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	SMP/e																		
REQUIRED	Operator commands																		

Service	Details
	2. F LLA REFRESH) .

Service	Details		
LU02977	<p>LU02977 M.C.S. ENTRIES = ++PTF (LU02977)</p> <p>FIX ABEND 0C4-3B IN TAMRPCST</p> <p>PROBLEM DESCRIPTION:</p> <p>Some callers of the TAMz for RACF PC Routine may be 64-bit, and as such, the high halves of the incoming registers may have data in them. This can cause TAMRPCST to abend with an 0C4-3B during an MVCL that occurs very early in the routine.</p> <p>SYMPTOMS:</p> <p>Abend 0C4-3B occurs in TAMRPCST, and desired TAMz function will not be performed.</p> <p>IMPACT:</p> <p>TAMz functionality will be affected, as the PC routine drives many features within the product.</p> <p>CIRCUMVENTION:</p> <p>N/A</p> <p>PRODUCT(S) AFFECTED:</p> <p>TRUSTED ACCESS MANAGER FOR Z Release 1.1</p> <p>Related Problem:</p> <p>TAMZ 14934</p> <p>Copyright (C) 2021 CA. All rights reserved. R00044-TAM011-SP1</p> <p>DESC(FIX ABEND 0C4-3B IN TAMRPCST).</p> <p>++VER (Z038)</p> <p>FMID (CFH0110)</p> <p>PRE (S008972 S014114 S015557 S015558 S015725 S016059 S016218 S016320)</p> <p>SUP (LT02977)</p> <p>++HOLD (LU02977) SYSTEM FMID(CFH0110)</p> <p>REASON (IPL) DATE (21300)</p> <p>COMMENT (</p> <table border="1"> <tr> <td>TRUSTED ACCESS MANAGER FOR Z</td><td>Release 1.1</td></tr> </table> <p> SEQUENCE After Apply</p> <p> PURPOSE To implement the fix</p> <p> USERS All TAMz users</p> <p> AFFECTED </p> <p> KNOWLEDGE TAMz SMP/e environment</p> <p> REQUIRED Operator commands</p> <p> IPL process</p> <p> ACCESS TAMz SMP/e environment</p> <p> REQUIRED Operator commands</p> <p> IPL process</p> <p>*****</p> <p>* STEPS TO PERFORM *</p> <p>*****</p> <p>1. Apply and deploy PTF to your TAMz runtime libraries.</p> <p>2. *REQUIRED* IPL the system. This fix makes changes to stubs</p>	TRUSTED ACCESS MANAGER FOR Z	Release 1.1
TRUSTED ACCESS MANAGER FOR Z	Release 1.1		

Service	Details
	that will need to be re-implanted. 3. Start the TAMR STC, for example, '/S TAMRSTC').

Trusted Access Manager for z/OS 1.1
CA RS 2111 - PTF LU03086 Details

8

Service	Details		
LU03086	<p>LU03086 M.C.S. ENTRIES = ++PTF (LU03086)</p> <p>REPACKAGE UPGRADED CA NIM SM FOR SERVICENOW ORLANDO/PARIS</p> <p>PROBLEM DESCRIPTION:</p> <p>Prior to this PTF, ServiceNow ORLANDO and PARIS versions could not be reached by CA NIM SM contained inside the TAMSTC proc.</p> <p>SYMPTOMS:</p> <p>CA NIM SM SOAP calls into ServiceNow always return HTTP 200 with empty results.</p> <p>IMPACT:</p> <p>Ticket validation with ServiceNow ORLANDO and PARIS instances cannot be performed. Prior versions of ServiceNow are supported.</p> <p>TAMz CLASSES which do not require a ticket are unaffected.</p> <p>Ticket Validation with other Service Desks are unaffected.</p> <p>CIRCUMVENTION:</p> <p>N/A for ServiceNow ORLANDO and PARIS.</p> <p>PRODUCT(S) AFFECTED:</p> <p>TRUSTED ACCESS MANAGER FOR Z Release 1.1</p> <p>Related Problem:</p> <p>TAMZ 14260</p> <p>Copyright (C) 2021 CA. All rights reserved. R00045-TAM011-SP1</p> <p>DESC(REPACKAGE UPGRADED CA NIM SM FOR SERVICENOW ORLANDO/PARIS).</p> <p>++VER (Z038)</p> <p>FMID (CFH0110)</p> <p>PRE (S012359)</p> <p>SUP (LT03086 S007607 S011137 S012878 ST07607 ST11137 ST12878)</p> <p>++HOLD (LU03086) SYSTEM FMID(CFH0110)</p> <p>REASON (DYNACT) DATE (21300)</p> <p>COMMENT (</p> <table border="1"> <tr> <td>TRUSTED ACCESS MANAGER FOR Z</td><td>Release 1.1</td></tr> </table> <p>SEQUENCE After Apply</p> <p>PURPOSE To implement PTF without requiring an IPL.</p> <p>USERS All TAMz users.</p> <p>AFFECTED </p> <p>KNOWLEDGE TAMz SMP/e environment</p> <p>REQUIRED Operator commands</p> <p>ACCESS TAMz SMP/e environment</p> <p>REQUIRED Operator commands</p> <p>*****</p> <p>* STEPS TO PERFORM *</p> <p>*****</p> <p>1. After applying the PTF, open your NIM UI and copy out all configuration and customization details for your service desk(s). Having a copy of this information will make later steps easier to complete.</p>	TRUSTED ACCESS MANAGER FOR Z	Release 1.1
TRUSTED ACCESS MANAGER FOR Z	Release 1.1		

Service	Details												
	<p>2. Once copied, deploy the new tam-microservice.war and ca-nim-sm.war files from your installation TAMz USS directory to your runtime TAMz USS directory. For example, /u/users/tamstc.</p> <p>3. After deploying the 2 .war files, you can either update your TAMENV file to include the following line within the TAMSTC SSL OPTIONS block:</p> <pre>IJO="\$IJO -Dcom.ibm.jsse2.overrideDefaultTLS=true"</pre> <p>--OR--</p> <p>Create a backup copy of your current TAMENV, deploy the new TAMENV, and update the variables as necessary using the values from your old TAMENV file.</p> <p>4. Once the TAMENV file is updated and the 2x .war files are deployed, restart the TAMSTC to pick up the new files.</p> <p>5. Once TAMSTC has started (look for the TAM00100 message in the joblog), open your NIM UI, and reset your configurations and customizations details using what you copied in Step 1.</p> <p>).</p> <pre>BINARY LINK('../ca-nim-sm.war') PARM(PATHMODE(0,7,5,5)) . BINARY LINK('../tam-microservice.war') PARM(PATHMODE(0,7,5,5)) .</pre> <table><tr><td>MCS</td><td>LU02795</td><td>STARTS ON PAGE 0002</td></tr><tr><td>MCS</td><td>LU02830</td><td>STARTS ON PAGE 0003</td></tr><tr><td>MCS</td><td>LU02977</td><td>STARTS ON PAGE 0004</td></tr><tr><td>MCS</td><td>LU03086</td><td>STARTS ON PAGE 0006</td></tr></table>	MCS	LU02795	STARTS ON PAGE 0002	MCS	LU02830	STARTS ON PAGE 0003	MCS	LU02977	STARTS ON PAGE 0004	MCS	LU03086	STARTS ON PAGE 0006
MCS	LU02795	STARTS ON PAGE 0002											
MCS	LU02830	STARTS ON PAGE 0003											
MCS	LU02977	STARTS ON PAGE 0004											
MCS	LU03086	STARTS ON PAGE 0006											

Trusted Access Manager for z/OS 1.1
CA RS 2111 Product/Component Listing

10

Product Family	Product	Release
Security	MF SECURITY JVM	01.01.00
	TRUSTED ACCESS MANAGER FOR Z	01.01.00
The CA RS 2111 Product/Component Count for this release is 2		

CA RS Level	Service	FMID
CAR2111	LU03086	CFH0110
	LU02977	CFH0110
	LU02830	CFH0110
	LU02795	CFH0110
CAR2108	S016320	CFH0110
	LU00584	CFH0110
CAR2107	S016218	CFH0110
CAR2104	S016059	CFH0110
	S015725	CFH0110
	S015558	CFH0110
	S015557	CFH0110
	LU00206	CFH0110
CAR2012	S015516	CFH0110
	S015058	CFH0110
	S015020	CFH0110
CAR2010	S014114	CFH0110
	S014102	CFH0110
	S014064	CFH0110
	S013783	CFH0110
	S013553	CFH0110
	S012468	CSJV110
	S011254	CSJV110
CAR2006	S012878	CFH0110
	S012359	CFH0110
	S010812	CFH0110
CAR2001	S011137	CFH0110
	S010220	CFH0110
	S010217	CSJV110
	S010051	CSJV110
CAR1911	S010581	CFH0110
	S007548	CFH0110
CAR1910	S009874	CSJV110
	S008972	CFH0110
CAR1908	S007549	CSJV110
	S006988	CSJV110
CAR1907	S007610	CSJV110
	S007607	CFH0110