OPS/MVS for JES2/JES3 14.0
CA RS 2201 Service List

Service	Description	Type
LU03582	SECURITY OR INTEGRITY PROBLEM	** PRP **
LU03721	EPI ENQ NOT RELEASED WHEN REXX PROGRAM ENDS	PTF
LU03790	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
LU03791	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
LU03792	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
LU03852	ADD A COMMERR CODE TO THE OPSBCPII SERVER OPBCP999E MESSAGE	PTF
LU03884	SECURITY OR INTEGRITY PROBLEM	** PRP **
LU03946	SECURITY OR INTEGRITY PROBLEM	** PRP **
LU04002	SECURITY OR INTEGRITY PROBLEM	** PRP **

The CA RS 2201 service count for this release is 9

FMID	Service	Description	Type
CCLXE00	LU03721	EPI ENQ NOT RELEASED WHEN REXX PROGRAM ENDS	PTF
	LU03790	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
	LU03852	ADD A COMMERR CODE TO THE OPSBCPII SERVER OPBCP999E MESSAGE	PTF
The CA RS 2201 service count for this FMID is 3			

FMID	Service	Description	Type
CCLXE01	LU03582	SECURITY OR INTEGRITY PROBLEM	** PRP **
	LU03791	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
	LU03884	SECURITY OR INTEGRITY PROBLEM	** PRP **
	LU03946	SECURITY OR INTEGRITY PROBLEM	** PRP **
	LU04002	SECURITY OR INTEGRITY PROBLEM	** PRP **

The CA RS 2201 service count for this FMID is 5

FMID	Service	Description	Type
CCLXE03	LU03792	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
The CA RS 2201 service count for this FMID is 1			

Service	Details
LU03582	LU03582 M.C.S. ENTRIES = ++PTF (LU03582) SECURITY OR INTEGRITY PROBLEM PROBLEM DESCRIPTION: Security or Integrity Problem. SYMPTOMS: N/A IMPACT: Security or Integrity Problem. CIRCUMVENTION: N/A PRODUCT(S) AFFECTED: OPS/MVS Version 14.0 Related Problem: OPSMVS 15397 Copyright (C) 2021 CA. All rights reserved. R00156-CLX140-SP0 DESC(SECURITY OR INTEGRITY PROBLEM). ++VER (Z038) FMID (CCLXE01) PRE (LU00044 LU00122 LU00462 LU00633 LU01212 LU02570 LU03791 SO14492 SO14857 SO15022 SO15068 SO15148 SO15200 SO15241 SO15821 SO15877) SUP (BC15146 LT01162 LT03582 ST14979) ++HOLD (LU03582) SYSTEM FMID(CCLXE01) REASON (ACTION) DATE (21348) COMMENT (+----------+ | OPS/MVS Version 14.0 | +----------+ |SEQUENCE | Before Restart | +----------+ |PURPOSE | To enable the use of the new conf.yaml parameter. | +----------+ |USERS | All MTC-A Users | |AFFECTED | | +----------+ |KNOWLEDGE | Knowledge of your site's CCS Messaging Service setup. | |REQUIRED | | +----------+ |ACCESS | Permissions to edit MTC-A conf.yaml file. | |REQUIRED | | +----------+ ********** * STEPS TO PERFORM * ********** A new configuration parameter was added to the hubConfiguration section of the conf.yaml configuration file. This new parameter enables or disables the hostname validation check of the Message Service hub certificate when using one of the TLS connection protocols to connect to the Message Service hub. If using the self-signed certificates generated by the ZMSSSL utility to connect to the Message Service hub, then this parameter must be set to "false".

Service	Details
	Otherwise, if using certificates signed by a Certificate Authority (not self-signed) and using the client trust store to validate the received hub certificate based solely on the signing Certificate Authority certificate chain being present in the trust store, then this parameter should be set to "true". TLS connections using CA-signed certificates must perform hostname validation to prevent potential man-in-the-middle attacks described in CVE-2018-11775.). ++HOLD (LU03582) SYSTEM FMID(CCLXE01) REASON (DOC) DATE (21348) COMMENT (+----------+ | OPS/MVS Version 14.0 | +----------+ ********** * PUBLICATION * ********** See section "Configure the Web Application" in the Using Mainframe Team Center - Automation (MTC-A) topic of the OPS/MVS documentation set at http://techdocs.broadcom.com/opsmvs.). ++HOLD (LU03582) SYSTEM FMID(CCLXE01) REASON (DYNACT) DATE (21348) COMMENT (+----------+ | OPS/MVS Version 14.0 | +----------+----------+ |SEQUENCE | After APPLY | +----------+----------+ |PURPOSE | To deploy a new version of Mainframe Team Center - | | | Automation | +----------+----------+ |USERS | All OPS/MVS MTC-A users | |AFFECTED | | +----------+----------+ |KNOWLEDGE | Basic z/OS systems programming skills and knowledge of | |REQUIRED | your new or existing MTC-A installation and configuration | | | | +----------+----------+ |ACCESS | - Read/write access to the USS directories where your new | |REQUIRED | or existing installation of MTC-A resides | | | - Authority to STOP and START your MTC-A Web Application | +----------+----------+ ********** * STEPS TO PERFORM * ********** Run The MTC-A Configuration Batch Job Sample JCL to execute the configuration script, mtcacfg.sh, is provided in yourHLQ.CCLXCNTL(OPMOIACG). Before executing the batch job, make the following edits: 1. Include a valid job card 2. Set CCLXCLS0 to the fully qualified MVS dataset name of the SMP/E CLIST target library installed by FMID CCLXxr0 OPS/MVS Base. (eg. 'yourHLQ.CCLXCLS0')

Service	Details
	3. Set CCLSHFSM to the USS mount point of the zFS installed by FMID CLXxr1 OPS/MVS OPSLOG WebView and Web Features. 4. Set TOMCATCONF to the USS path of your deployed Tomcat server's "context" directory. Typically: <catalina_base>/conf/Catalina/localhost 5. Set MTCADEPLOY to the USS path where you wish to deploy the MTCA Web App. A new directory called '/mtca' will be created on this path and will contain the mtcaApp.war as well as '/conf' and '/log' sub-directories. The configuration script creates the MTC-A directory structure at your chosen deployment location and defines the context for MTC-A to your Tomcat installation. If a previous MTC-A installation exists, your current configuration is saved as 'MTCADEPLOY/mtca/conf/config.yaml.YY_MM_DD_hh_mm_ss'. Your configuration is then automatically merged and upgraded to the version supplied within this PTF. Verify the STDOUT of the configuration batch job for messages indicating the addition of fields to the 'conf.yaml' that must be set specifically for your site before MTC-A is restarted. If your '/mtca' directory is on path 'a/b/c/mtca' supply path '/a/b/c' as your value for the deploy location). BINARY LINK('../conf.yaml') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../mtcacfg.sh') PARM(PATHMODE(0,7,5,5)) . BINARY LINK('../mtcaApp.war') PARM(PATHMODE(0,7,5,5)) .

Service	Details
LU03721	LU03721 M.C.S. ENTRIES = ++PTF (LU03721) EPI ENQ NOT RELEASED WHEN REXX PROGRAM ENDS PROBLEM DESCRIPTION: The End Of Task exit that runs the EPI cleanup code was not called when a REXX running in an OSF server ended. SYMPTOMS: EPI ENQ failures due to a previous ENQ on the terminal. IMPACT: REXX code using ADDRESS EPI ENQ commands may fail. CIRCUMVENTION: Add DEQ logic to the REXX code. PRODUCT(S) AFFECTED: OPS/MVS Release 13.5 OPS/MVS Version 14.0 Related Problem: OPSMVS 15483 Copyright (C) 2021 CA. All rights reserved. R00157-CLX140-SP0 DESC(EPI ENQ NOT RELEASED WHEN REXX PROGRAM ENDS). ++VER (Z038) FMID (CCLXE00) PRE (LU00913 LU03790) SUP (LT00679 LT03721 LU00679) ++HOLD (LU03721) SYSTEM FMID(CCLXE00) REASON (DYNACT) DATE (21344) COMMENT (+----------+ | OPS/MVS Version 14.0 | +----------+----------+ |SEQUENCE | After APPLY | +----------+----------+ |PURPOSE | To activate load modules updated by this PTF | +----------+----------+ |USERS | All OPS/MVS users | |AFFECTED | | +----------+----------+ |KNOWLEDGE | Basic z/OS systems programming skills | |REQUIRED | | +----------+----------+ |ACCESS | - Access to OPS/MVS SMP/E Target loadlib CCLXLOAD and any | |REQUIRED | deployed copies | | | - Authority to issue MVS system commands | | | - Authority to stop and start OPS/MVS | +----------+----------+ ********** * STEPS TO PERFORM * ********** 1. APPLY of this PTF updates SMP/E Target loadlib CCLXLOAD. Refer to GIM23903I messages in the SMPOUT to identify the specific load modules that are updated. 2. Copy the updated load modules from SMP/E Target loadlib CCLXLOAD to any other deployed copies, such as a loadlib in the OPSMAIN STEPLIB or the system link list (LNKLIST).

Service	Details
	3. If the system library lookaside (LLA) program is managing any updated loadlib, you must refresh LLA by using MVS system command "F LLA,REFRESH" or some equivalent method. 4. If the system link pack area (LPA) contains any updated load module, you must refresh LPA by using MVS system command "SETPROG LPA" or some equivalent method. * Note that load module OPSAEX is commonly placed in LPA. 5. Stop and re-start OPS/MVS by using MVS system commands "P OPSS" and "S OPSS" or some equivalent method. * For possible alternatives to restarting OPS/MVS, see the topic "RELOAD Modules and RESTART Components" in the user documentation at https://techdocs.broadcom.com/opsmvs 6. TSO users must exit and re-enter OPSVIEW to activate any changes. Depending on how OPSVIEW is accessed, this may require a TSO logoff and logon.).

Service	Details
LU03790	LU03790 M.C.S. ENTRIES = ++PTF (LU03790) ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE PROBLEM DESCRIPTION: This PTF will enable you to use a feature in SYSVIEW called Product PTF Analysis. This PTF delivers an element that contains metadata for all published PTFs for OPS/MVS. Any subsequent PTF published after this PTF will contain its own PTF tracking element metadata. What is Product PTF Analysis? Product PTF Analysis combines PTF tracking elements from your run-time XML library with maintenance data found in your product SMP/E installation CSI library. Product PTF Analysis provides the ability to: * Determine the PTFs and APARs currently applied. * View detailed descriptions of published PTFs. * Using the Cross System component, you are able to compare the PTFs applied on each LPAR. * Detailed SYSMOD information can be viewed from the SMP/E CSI data set used during installation and maintenance. Product PTF Analysis shows this information for all Broadcom Mainframe products that have the necessary XML data available. Please note that not every product will update XML data for all prior and new fixes at the same time. Consult each product's documentation for more information. How can I view Product PTF Analysis? SYSVIEW 16.0 Feature PTF LU03153 added a Product PTF Analysis feature that performs an analysis of product SMP/E CSIs and PTF tracking metadata. A PTFS command was added to SYSVIEW 16.0 with PTF LU03153 that performs the analysis. For more information, see the "New Features" page on the SYSVIEW Tech Docs Portal here: https://techdocs.broadcom.com/sysview PRODUCT(S) AFFECTED: OPS/MVS Release 13.5 OPS/MVS Version 14.0 Related Problem: OPSMVS 15499 Copyright (C) 2021 CA. All rights reserved. R00159-CLX140-SP0 DESC(ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE). ++VER (Z038) FMID (CCLXE00) SUP (LT03790) ++IF FMID(CCLXE01) REQ(LU03791) . ++IF FMID(CCLXE03) REQ(LU03792) . ++HOLD (LU03790) SYSTEM FMID(CCLXE00) REASON (DDDEF) DATE (21341) COMMENT (+----------+ | OPS/MVS Release 13.5 | +----------+----------+ |SEQUENCE | Before Apply | +----------+----------+ |PURPOSE | To make room for new PRODXML elements | +----------+----------

Service	Details
	|USERS | All users | |AFFECTED | | +----------+----------+ |KNOWLEDGE | Basic z/OS system programming skills. | |REQUIRED | | +----------+----------+ |ACCESS | Authority to expand yourHLQ.CCLXXML dataset | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** This PTF will add many elements to yourHLQ.CCLXXML. If this dataset is a PDS the PTF may fail during the SMP/E APPLY step. To avoid this, expand yourHLQ.CCLXXML to accomodate for the new elements.).

Service	Details
LU03791	LU03791 M.C.S. ENTRIES = ++PTF (LU03791) ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE PROBLEM DESCRIPTION: This PTF will enable you to use a feature in SYSVIEW called Product PTF Analysis. This PTF delivers an element that contains metadata for all published PTFs for OPS/MVS. Any subsequent PTF published after this PTF will contain its own PTF tracking element metadata. What is Product PTF Analysis? Product PTF Analysis combines PTF tracking elements from your run-time XML library with maintenance data found in your product SMP/E installation CSI library. Product PTF Analysis provides the ability to: * Determine the PTFs and APARs currently applied. * View detailed descriptions of published PTFs. * Using the Cross System component, you are able to compare the PTFs applied on each LPAR. * Detailed SYSMOD information can be viewed from the SMP/E CSI data set used during installation and maintenance. Product PTF Analysis shows this information for all Broadcom Mainframe products that have the necessary XML data available. Please note that not every product will update XML data for all prior and new fixes at the same time. Consult each product's documentation for more information. How can I view Product PTF Analysis? SYSVIEW 16.0 Feature PTF LU03153 added a Product PTF Analysis feature that performs an analysis of product SMP/E CSIs and PTF tracking metadata. A PTFS command was added to SYSVIEW 16.0 with PTF LU03153 that performs the analysis. For more information, see the "New Features" page on the SYSVIEW Tech Docs Portal here: https://techdocs.broadcom.com/sysview PRODUCT(S) AFFECTED: OPS/MVS Release 13.5 OPS/MVS Version 14.0 Related Problem: OPSMVS 15499 Copyright (C) 2021 CA. All rights reserved. R00159-CLX140-SP0 DESC(ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE). ++VER (Z038) FMID (CCLXE01) SUP (LT03791) ++IF FMID(CCLXE03) REQ(LU03792) . ++IF FMID(CCLXE00) REQ(LU03790) .

Service	Details
LU03792	LU03792 M.C.S. ENTRIES = ++PTF (LU03792) ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE PROBLEM DESCRIPTION: This PTF will enable you to use a feature in SYSVIEW called Product PTF Analysis. This PTF delivers an element that contains metadata for all published PTFs for OPS/MVS. Any subsequent PTF published after this PTF will contain its own PTF tracking element metadata. What is Product PTF Analysis? Product PTF Analysis combines PTF tracking elements from your run-time XML library with maintenance data found in your product SMP/E installation CSI library. Product PTF Analysis provides the ability to: * Determine the PTFs and APARs currently applied. * View detailed descriptions of published PTFs. * Using the Cross System component, you are able to compare the PTFs applied on each LPAR. * Detailed SYSMOD information can be viewed from the SMP/E CSI data set used during installation and maintenance. Product PTF Analysis shows this information for all Broadcom Mainframe products that have the necessary XML data available. Please note that not every product will update XML data for all prior and new fixes at the same time. Consult each product's documentation for more information. How can I view Product PTF Analysis? SYSVIEW 16.0 Feature PTF LU03153 added a Product PTF Analysis feature that performs an analysis of product SMP/E CSIs and PTF tracking metadata. A PTFS command was added to SYSVIEW 16.0 with PTF LU03153 that performs the analysis. For more information, see the "New Features" page on the SYSVIEW Tech Docs Portal here: https://techdocs.broadcom.com/sysview PRODUCT(S) AFFECTED: OPS/MVS Release 13.5 OPS/MVS Version 14.0 Related Problem: OPSMVS 15499 Copyright (C) 2021 CA. All rights reserved. R00159-CLX140-SP0 DESC(ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE). ++VER (Z038) FMID (CCLXE03) SUP (LT03792) ++IF FMID(CCLXE01) REQ(LU03791) . ++IF FMID(CCLXE00) REQ(LU03790) .

Service	Details
LU03852	LU03852 M.C.S. ENTRIES = ++PTF (LU03852) ADD A COMMERR CODE TO THE OPSBCPII SERVER OPBCP999E MESSAGE ENHANCEMENT DESCRIPTION: When ADDRESS HWS commands fail after invoking the GETATTR, SETATTR or SENDCMD command, an OPBCP999E WTO will be issued that includes the COMMERR code if one is returned by BCPII in the request DIAGAREA. PRODUCT(S) AFFECTED: CA OPS/MVS Base Release 13.5 CA OPS/MVS Base Version 14.0 Related Problem: OPSMVS 15119 Copyright (C) 2021 CA. All rights reserved. R00161-CLX140-SP0 DESC(ADD A COMMERR CODE TO THE OPSBCPII SERVER OPBCP999E MESSAGE). ++VER (Z038) FMID (CCLXE00) PRE (LU02514 LU03049 LU03137 LU03790) SUP (LT01080 LT03852 LU01080) ++HOLD (LU03852) SYSTEM FMID(CCLXE00) REASON (ACTION) DATE (21344) COMMENT (+----------+----------+ | OPS/MVS Version 14.0 | +----------+----------+ |SEQUENCE | Before using the OPSBCPII Server. | +----------+----------+ |PURPOSE | To issue a WTO indicating an error has occurred which | | | includes return and reason codes. | +----------+----------+ |USERS | All users of the OPSBCPII Server. | |AFFECTED | | +----------+----------+ |KNOWLEDGE | Basic z/OS system programming skills. | |REQUIRED | | +----------+----------+ |ACCESS | Authority to stop and start the OPS/MVS. | |REQUIRED | | +----------+----------+ | | | +----------+----------+ ********** * STEPS TO PERFORM * ********** 1. After applying the PTF restart OPSBCPII Server by issuing the following command: "F OPSx RESTART(HWS)" where OPSx is the OPS/MVS subsystem id.).

Service	Details
LU03884	LU03884 M.C.S. ENTRIES = ++PTF (LU03884) SECURITY OR INTEGRITY PROBLEM PROBLEM DESCRIPTION: Security or Integrity Problem. SYMPTOMS: N/A IMPACT: Security or Integrity Problem. CIRCUMVENTION: N/A PRODUCT(S) AFFECTED: OPS/MVS Release 13.5 OPS/MVS Version 14.0 Related Problem: OPSMVS 15595 Copyright (C) 2021 CA. All rights reserved. R00162-CLX140-SP0 DESC(SECURITY OR INTEGRITY PROBLEM). ++VER (Z038) FMID (CCLXE01) PRE (LU00633 LU03791 SO15821) SUP (CC15146 LT03165 LT03884 LU03165) ++HOLD (LU03884) SYSTEM FMID(CCLXE01) REASON (ACTION) DATE (21350) COMMENT (+----------+ | CA OPS/MVS Web Components Release 14.0 | +----------+----------+ |SEQUENCE |After Apply | +----------+----------+ |PURPOSE |To activate the fix | +----------+----------+ |USERS |User's of the OPS/MVS Web Services | |AFFECTED | | +----------+----------+ |KNOWLEDGE |Web servers and USS directories | |REQUIRED | | +----------+----------+ |ACCESS |USS directories for Tomcat Web Server | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** 1. Update your OPS/MVS Web Services host server by copying the opsmvs.war file from the installation HFS to your runtime web server. See the following documentation for detailed instructions on how to deploy the new module. - Install and Configure CA OPS/MVS RESTful Web Services on Tomcat 2. Stop and restart your OPS/MVS web server STC so it recognizes and uses the newly updated opsmvs.war file.).

Service	Details
	TEXT LINK('../opwebsvc.config') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../opwscfg.sh') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../opwebsvc.env') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../opwebsvc.prop') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../OPWShttp.rex') PARM(PATHMODE(0,7,5,5)) . BINARY LINK('../opsmvs.war') PARM(PATHMODE(0,7,5,5)) .

Service	Details
LU03946	LU03946 M.C.S. ENTRIES = ++PTF (LU03946) 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: OPS/MVS Release 13.5 OPS/MVS Version 14.0 Related Problem: OPSMVS 15632 Copyright (C) 2021 CA. All rights reserved. R00163-CLX140-SP0 DESC(SECURITY OR INTEGRITY PROBLEM). ++VER (Z038) FMID (CCLXE01) PRE (LU00044 LU00122 LU00462 LU00633 LU01212 LU02570 LU03582 LU03791 SO14492 SO14857 SO15022 SO15068 SO15148 SO15200 SO15241 SO15821 SO15877) SUP (BL03582 LT01162 LT03946 ST14979) ++HOLD (LU03946) SYSTEM FMID(CCLXE01) REASON (ACTION) DATE (21351) COMMENT (+----------+ | OPS/MVS Version 14.0 | +----------+----------+ |SEQUENCE | Before Restart | +----------+----------+ |PURPOSE | To enable the use of the new conf.yaml parameter | +----------+----------+ |USERS | All MTC-A Users and/or SM users | |AFFECTED | | +----------+----------+ |KNOWLEDGE | Knowledge of your site's CCS Messaging Service setup | |REQUIRED | | +----------+----------+ |ACCESS | Permissions to edit MTC-A conf.yaml file | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * ********** FOR MTC-A

Service	Details

	A new configuration parameter was added to the hubConfiguration section
	of the conf.yaml configuration file. This new parameter enables or
	disables the hostname validation check of the Message Service hub
	certificate when using one of the TLS connection protocols to connect
	to the Message Service hub.
	If using the self-signed certificates generated by the ZMSSSL utility
	to connect to the Message Service hub, then this parameter must be
	set to false.
	Otherwise, if using certificates signed by a Certificate Authority (not
	self-signed) and using the client trust store to validate the received
	hub certificate based solely on the signing Certificate Authority
	certificate chain being present in the trust store, then this parameter
	should be set to true. TLS connections using CA-signed certificates
	must perform hostname validation to prevent potential man-in-the-middle
	attacks described in CVE-2018-11775.
	FOR NIM SM

	To redeploy your instance of NIM SM with the war file in this PTF, you
	will need to locate ca-nim-sm.war under your USS path name defined by
	SMP/E DDDEF CCLXHFSM (i.e. /opsmvs/directory/CCLXHFS).
	Place this war file in your target NIM SM USS directory and restart.
	For more information about deploying CA NIM SM, see CA Normalized
	Integration Management for Service Management at
	http://techdocs.broadcom.com
	).
	++HOLD (LU03946) SYSTEM FMID(CCLXE01)
	REASON (DOC) DATE (21351)
	COMMENT (
	+----------+
	| OPS/MVS Version 14.0 |
	+----------+
	**********
	* PUBLICATION *
	**********
	See section "Configure the Web Application" in the OPS/MVS
	documentation set at http://techdocs.broadcom.com/opsmvs.
	).
	++HOLD (LU03946) SYSTEM FMID(CCLXE01)
	REASON (DYNACT) DATE (21351)
	COMMENT (
	+----------+
	| OPS/MVS Version 14.0 |
	+----------+----------+
	|SEQUENCE | After APPLY |
	+----------+----------+
	|PURPOSE | To deploy a new version of Mainframe Team Center - |
	| | Automation |
	+----------+----------+
	|USERS | All OPS/MVS MTC-A users |
	|AFFECTED | |
	+----------+----------+
	|KNOWLEDGE | Basic z/OS systems programming skills and knowledge of |
	|REQUIRED | your new or existing MTC-A installation and configuration |

Service	Details

	<pre>| | |
	+----------+--+
	|ACCESS | - Read/write access to the USS directories where your new |
	|REQUIRED | or existing installation of MTC-A resides |
	| | - Authority to STOP and START your MTC-A Web Application |
	+----------+--+
	**************************
	* STEPS TO PERFORM *
	**************************
	Run The MTC-A Configuration Batch Job
	Sample JCL to execute the configuration script, mtcacfg.sh, is provided
	in yourHLQ.CCLXCNTL(OPMOIACG). Before executing the batch job, make the
	following edits:
	1. Include a valid job card
	2. Set CCLXCLS0 to the fully qualified MVS dataset
	name of the SMP/E CLIST target library installed by FMID
	CCLXxr0 OPS/MVS Base. (eg. 'yourHLQ.CCLXCLS0')
	3. Set CCLSHFSM to the USS mount point of the zFS installed
	by FMID CLXxr1 OPS/MVS OPSLOG WebView and Web Features.
	4. Set TOMCATCONF to the USS path of your deployed Tomcat
	server's "context" directory. Typically:
	<catalina_base>/conf/Catalina/localhost
	5. Set MTCADEPLOY to the USS path where you wish to deploy
	the MTCA Web App. A new directory called '/mtca' will be
	created on this path and will contain the mtcaApp.war as
	well as '/conf' and '/log' sub-directories.
	The configuration script creates the MTC-A directory structure at your
	chosen deployment location and defines the context for MTC-A to your
	Tomcat installation.
	If a previous MTC-A installation exists, your current configuration
	is saved as 'MTCADEPLOY/mtca/conf/config.yaml.YY_MM_DD_hh_mm_ss'. Your
	configuration is then automatically merged and upgraded to the version
	supplied within this PTF. Verify the STDOUT of the configuration batch
	job for messages indicating the addition of fields to the 'conf.yaml'
	that must be set specifically for your site before MTC-A is restarted.
	If your '/mtca' directory is on path 'a/b/c/mtca' supply path '/a/b/c'
	as your value for the deploy location
	).
	BINARY
	LINK('../conf.yaml')
	PARM(PATHMODE(0,7,5,5)) .
	TEXT
	LINK('../mtcacfg.sh')
	PARM(PATHMODE(0,7,5,5)) .
	BINARY
	LINK('../mtcaApp.war')
	PARM(PATHMODE(0,7,5,5)) .
	BINARY
	LINK('../ca-nim-sm.war')
	PARM(PATHMODE(0,7,5,5)) .</pre>

Service	Details
LU04002	LU04002 M.C.S. ENTRIES = ++PTF (LU04002) 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: OPS/MVS Release 13.5 OPS/MVS Version 14.0 Related Problem: OPSMVS 15687 Copyright (C) 2021 CA. All rights reserved. R00165-CLX140-SP0 DESC(SECURITY OR INTEGRITY PROBLEM). ++VER (Z038) FMID (CCLXE01) PRE (LU00044 LU00122 LU00462 LU00633 LU01212 LU02570 LU03165 LU03582 LU03791 LU03884 LU03946 SO14492 SO14857 SO15022 SO15068 SO15148 SO15200 SO15241 SO15821 SO15877) SUP (AL03884 AL03946 LT01162 LT04002 ST14979) ++HOLD (LU04002) SYSTEM FMID(CCLXE01) REASON (ACTION) DATE (21355) COMMENT (+----------+ | OPS/MVS Version 14.0 | +----------+----------+ |SEQUENCE | After apply | +----------+----------+ |PURPOSE | To activate the fix | +----------+----------+ |USERS | All MTC-A, NIM SM, OPS/MVS Web Services users | |AFFECTED | | +----------+----------+ |KNOWLEDGE | Basic z/OS programming skills | |REQUIRED | | +----------+----------+ |ACCESS | MTC-A, NIM SM, and Web Services installation access | |REQUIRED | | +----------+----------+ ********** * STEPS TO PERFORM * **********

Service	Details
	FOR MTC-A --------- A new configuration parameter was added to the hubConfiguration section of the conf.yaml configuration file. This new parameter enables or disables the hostname validation check of the Message Service hub certificate when using one of the TLS connection protocols to connect to the Message Service hub. If using the self-signed certificates generated by the ZMSSSL utility to connect to the Message Service hub, then this parameter must be set to false. Otherwise, if using certificates signed by a Certificate Authority (not self-signed) and using the client trust store to validate the received hub certificate based solely on the signing Certificate Authority certificate chain being present in the trust store, then this parameter should be set to true. TLS connections using CA-signed certificates must perform hostname validation to prevent potential man-in-the-middle attacks. FOR NIM SM ---------- To redeploy your instance of NIM SM with the war file in this PTF, you will need to locate ca-nim-sm.war under your USS path name defined by SMP/E DDDEF CCLXHFSM (i.e. /opsmvs/directory/CCLXHFS). Place this war file in your target NIM SM USS directory and restart. For more information about deploying CA NIM SM, see CA Normalized Integration Management for Service Management at http://techdocs.broadcom.com FOR WEB SERVICES ---------------- 1. Update your OPS/MVS Web Services host server by copying the opsmvs.war file from the installation HFS to your runtime web server. See the following documentation for detailed instructions on how to deploy the new module. - Install and Configure CA OPS/MVS RESTful Web Services on Tomcat 2. Stop and restart your OPS/MVS web server STC so it recognizes and uses the newly updated opsmvs.war file.). ++HOLD (LU04002) SYSTEM FMID(CCLXE01) REASON (DOC) DATE (21355) COMMENT (+--+ | OPS/MVS Version 14.0 | +--+ ************************** * PUBLICATION * ************************** See section "Configure the Web Application" in the OPS/MVS documentation set at http://techdocs.broadcom.com/opsmvs.). ++HOLD (LU04002) SYSTEM FMID(CCLXE01) REASON (DYNACT) DATE (21355) COMMENT (+--+ | OPS/MVS Version 14.0 |

Service	Details

```
+----------+-------------------------------------------------------------+
|SEQUENCE  | After APPLY                                                 |
+----------+-------------------------------------------------------------+
|PURPOSE   | To deploy a new version of Mainframe Team Center -          |
|          | Automation                                                  |
+----------+-------------------------------------------------------------+
|USERS     | All OPS/MVS MTC-A users                                     |
|AFFECTED  |                                                             |
+----------+-------------------------------------------------------------+
|KNOWLEDGE | Basic z/OS systems programming skills and knowledge of      |
|REQUIRED  | your new or existing MTC-A installation and configuration   |
|          |                                                             |
+----------+-------------------------------------------------------------+
|ACCESS    | - Read/write access to the USS directories where your new   |
|REQUIRED  |   or existing installation of MTC-A resides                 |
|          | - Authority to STOP and START your MTC-A Web Application    |
+----------+-------------------------------------------------------------+
**************************
* STEPS    TO    PERFORM *
**************************
Run The MTC-A Configuration Batch Job
Sample JCL to execute the configuration script, mtcacfg.sh, is provided
in yourHLQ.CCLXCNTL(OPMOIACG). Before executing the batch job, make the
following edits:
1. Include a valid job card
2. Set CCLXCLS0 to the fully qualified MVS dataset
name of the SMP/E CLIST target library installed by FMID
CCLXxr0 OPS/MVS Base. (eg. 'yourHLQ.CCLXCLS0')
3. Set CCLSHFSM to the USS mount point of the zFS installed
by FMID CLXxr1 OPS/MVS OPSLOG WebView and Web Features.
4. Set TOMCATCONF to the USS path of your deployed Tomcat
server's "context" directory. Typically:
<catalina_base>/conf/Catalina/localhost
5. Set MTCADEPLOY to the USS path where you wish to deploy
the MTCA Web App. A new directory called '/mtca' will be
created on this path and will contain the mtcaApp.war as
well as '/conf' and '/log' sub-directories.
The configuration script creates the MTC-A directory structure at your
chosen deployment location and defines the context for MTC-A to your
Tomcat installation.
If a previous MTC-A installation exists, your current configuration
is saved as 'MTCADEPLOY/mtca/conf/config.yaml.YY_MM_DD_hh_mm_ss'. Your
configuration is then automatically merged and upgraded to the version
supplied within this PTF. Verify the STDOUT of the configuration batch
job for messages indicating the addition of fields to the 'conf.yaml'
that must be set specifically for your site before MTC-A is restarted.
If your '/mtca' directory is on path 'a/b/c/mtca' supply path '/a/b/c'
as your value for the deploy location
).
BINARY
LINK('../conf.yaml')
PARM(PATHMODE(0,7,5,5)) .
TEXT
LINK('../mtcacfg.sh')
```

Service	Details
	PARM(PATHMODE(0,7,5,5)) .
	BINARY
	LINK('../mtcaApp.war')
	PARM(PATHMODE(0,7,5,5)) .
	BINARY
	LINK('../ca-nim-sm.war')
	PARM(PATHMODE(0,7,5,5)) .
	TEXT
	LINK('../opwebsvc.config')
	PARM(PATHMODE(0,7,5,5)) .
	TEXT
	LINK('../opwscfg.sh')
	PARM(PATHMODE(0,7,5,5)) .
	TEXT
	LINK('../opwebsvc.env')
	PARM(PATHMODE(0,7,5,5)) .
	TEXT
	LINK('../opwebsvc.prop')
	PARM(PATHMODE(0,7,5,5)) .
	TEXT
	LINK('../OPWShttp.rex')
	PARM(PATHMODE(0,7,5,5)) .
	BINARY
	LINK('../opsmvs.war')
	PARM(PATHMODE(0,7,5,5)) .
	MCS LU03582 STARTS ON PAGE 0002
	MCS LU03721 STARTS ON PAGE 0005
	MCS LU03790 STARTS ON PAGE 0006
	MCS LU03791 STARTS ON PAGE 0010
	MCS LU03792 STARTS ON PAGE 0012
	MCS LU03852 STARTS ON PAGE 0013
	MCS LU03884 STARTS ON PAGE 0014
	MCS LU03946 STARTS ON PAGE 0016
	MCS LU04002 STARTS ON PAGE 0020

Product Family	Product	Release
Systems Management	CA OPS/MVS BASE	14.00.00

The CA RS 2201 Product/Component Count for this release is 1

CA RS Level	Service	FMID
CAR2201	LU04002	CCLXE01
	LU03946	CCLXE01
	LU03884	CCLXE01
	LU03852	CCLXE00
	LU03792	CCLXE03
	LU03791	CCLXE01
	LU03790	CCLXE00
	LU03721	CCLXE00
	LU03582	CCLXE01
CAR2112	LU03548	CCLXE00
	LU03512	CCLXE03
	LU03481	CCLXE00
	LU03418	CCLXE00
	LU03387	CCLXE00
	LU03373	CCLXE01
	LU03334	CCLXE00
	LU03258	CCLXE00
CAR2111	LU03303	CCLXE00
	LU03179	CCLXE00
	LU03165	CCLXE01
	LU03149	CCLXE00
	LU03137	CCLXE00
	LU03119	CCLXE00
	LU03099	CCLXE00
	LU03084	CCLXE00
	LU03082	CCLXE00
	LU03072	CCLXE00
	LU03049	CCLXE00
	LU03011	CCLXE00
CAR2110	LU02790	CCLXE00
	LU02570	CCLXE01
	LU02514	CCLXE00
	LU02484	CCLXE00
	LU02253	CCLXE01
	LU02252	CCLXE00
CAR2109	LU02562	CCLXE00
	LU02545	CCLXE00
	LU02521	CCLXE00
	LU02515	CCLXE00
	LU02478	CCLXE00
	LU02417	CCLXE00
	LU02313	CCLXE00
	LU02285	CCLXE00
	LU02105	CCLXE00
CAR2108	LU02209	CCLXE00
	LU02161	CCLXE00
	LU02080	CCLXE00

CA RS Level	Service	FMID
	LU02046	CCLXE00
	LU02021	CCLXE00
	LU01967	CCLXE00
CAR2107	LU01929	CCLXE00
	LU01862	CCLXE00
	LU01797	CCLXE00
	LU01655	CCLXE00
	LU01630	CCLXE00
	LU01562	CCLXE01
	LU01212	CCLXE01
	LU01211	CCLXE00
	LU01140	CCLXE01
CAR2106	LU01398	CCLXE00
	LU01310	CCLXE00
	LU01080	CCLXE00
	LU00913	CCLXE00
CAR2105	LU01117	CCLXE00
	LU01116	CCLXE00
	LU00998	CCLXE00
	LU00876	CCLXE00
	LU00741	CCLXE00
	LU00717	CCLXE00
	LU00679	CCLXE00
CAR2104	LU00716	CCLXE01
	LU00715	CCLXE00
	LU00677	CCLXE00
	LU00634	CCLXE00
	LU00633	CCLXE01
	LU00632	CCLXE00
	LU00610	CCLXE00
	LU00496	CCLXE00
	LU00477	CCLXE00
	LU00462	CCLXE01
	LU00442	CCLXE00
	LU00407	CCLXE00
	LU00361	CCLXE00
	LU00235	CCLXE00
CAR2103	LU00278	CCLXE00
	LU00210	CCLXE00
	LU00188	CCLXE00
	LU00122	CCLXE01
	LU00121	CCLXE00
CAR2102	SO15877	CCLXE01
	SO15876	CCLXE00
	LU00117	CCLXE00
	LU00113	CCLXE00
	LU00078	CCLXE00

CA RS Level	Service	FMID
	LU00077	CCLXE00
	LU00074	CCLXE00
	LU00067	CCLXE00
	LU00063	CCLXE00
	LU00060	CCLXE00
	LU00058	CCLXE00
	LU00057	CCLXE00
	LU00044	CCLXE01
	LU00040	CCLXE00
CAR2101	SO15920	CCLXE00
	SO15902	CCLXE00
	SO15821	CCLXE01
	SO15820	CCLXE00
	SO15729	CCLXE00
	LU00028	CCLXE00
	LU00025	CCLXE00
CAR2012	SO15758	CCLXE00
	SO15662	CCLXE00
	SO15610	CCLXE00
	SO15578	CCLXE00
	SO15569	CCLXE00
	SO15565	CCLXE00
	SO15526	CCLXE00
	SO15515	CCLXE00
	SO15505	CCLXE00
	SO15502	CCLXE00
	SO15497	CCLXE00
CAR2011	SO15373	CCLXE00
	SO15324	CCLXE00
	SO15241	CCLXE01
	SO15200	CCLXE01
	SO15151	CCLXE00
	SO15148	CCLXE01
	SO15069	CCLXE00
	SO15068	CCLXE01
	SO15067	CCLXE00
	SO14750	CCLXE00
CAR2010	SO15022	CCLXE01
	SO15018	CCLXE00
	SO14993	CCLXE00
	SO14932	CCLXE00
	SO14903	CCLXE00
	SO14875	CCLXE00
	SO14871	CCLXE00
	SO14857	CCLXE01
	SO14824	CCLXE00
	SO14801	CCLXE00

CA RS Level	Service	FMID
	SO14646	CCLXE00
	SO14644	CCLXE00
	SO14609	CCLXE00
CAR2009	SO14537	CCLXE00
	SO14492	CCLXE01
	SO14477	CCLXE00
	SO14434	CCLXE01
	SO14412	CCLXE00