

OPS/MVS for JES2/JES3 13.5
CA RS 2201 Service List

1

Service	Description	Type
LU03241	ADD A COMMERR CODE TO THE OPSBCPII SERVER OPBCP999E MESSAGE	PTF
LU03396	SECURITY OR INTEGRITY PROBLEM	** PRP **
LU03738	EPI ENQ NOT RELEASED WHEN REXX PROGRAM ENDS	PTF
LU03793	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
LU03794	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
LU03795	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
LU03883	SECURITY OR INTEGRITY PROBLEM	** PRP **
LU03941	SECURITY OR INTEGRITY PROBLEM	** PRP **
LU03970	SECURITY OR INTEGRITY PROBLEM	** PRP **
LU04003	SECURITY OR INTEGRITY PROBLEM	** PRP **
The CA RS 2201 service count for this release is 10		

OPS/MVS for JES2/JES3
CA RS 2201 Service List for CCLXD50

2

FMID	Service	Description	Type
CCLXD50	LU03241	ADD A COMMERR CODE TO THE OPSBCPII SERVER OPBCP999E MESSAGE	PTF
	LU03738	EPI ENQ NOT RELEASED WHEN REXX PROGRAM ENDS	PTF
	LU03793	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
The CA RS 2201 service count for this FMID is 3			

OPS/MVS for JES2/JES3
CA RS 2201 Service List for CCLXD51

3

FMID	Service	Description	Type
CCLXD51	LU03396	SECURITY OR INTEGRITY PROBLEM	** PRP **
	LU03794	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
	LU03883	SECURITY OR INTEGRITY PROBLEM	** PRP **
	LU03941	SECURITY OR INTEGRITY PROBLEM	** PRP **
	LU03970	SECURITY OR INTEGRITY PROBLEM	** PRP **
	LU04003	SECURITY OR INTEGRITY PROBLEM	** PRP **
The CA RS 2201 service count for this FMID is 6			

OPS/MVS for JES2/JES3
CA RS 2201 Service List for CCLXD53

FMID	Service	Description	Type
CCLXD53	LU03795	ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE	PTF
The CA RS 2201 service count for this FMID is 1			

Service	Details
LU03241	LU03241 M.C.S. ENTRIES = ++PTF (LU03241) 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. R00362-CLX135-SP1 DESC(ADD A COMMERR CODE TO THE OPSBCPII SERVER OPBCP999E MESSAGE). ++VER (Z038) FMID (CCLXD50) PRE (LU02826 LU03793 S010262 S011203 S011260 S011445 S011812 S013347) SUP (LT03241) ++HOLD (LU03241) SYSTEM FMID(CCLXD50) REASON (ACTION) DATE (21344) COMMENT (<pre> +-----+ CA OPS/MVS Base Release 13.5 +-----+-----+ SEQUENCE Before using the OPSBCPII Server. +-----+-----+ PURPOSE To receive OPBCP999E WTO's with additional error related error status. +-----+-----+ 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.) </pre>

Service	Details		
LU03396	LU03396 M.C.S. ENTRIES = ++PTF (LU03396) 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 15257 Copyright (C) 2021 CA. All rights reserved. R00367-CLX135-SP1 DESC (SECURITY OR INTEGRITY PROBLEM). ++VER (Z038) FMID (CCLXD51) PRE (LU03794 S000236 S000873 S001943 S003775 S004412 S005192 S005737 S005996 S006920 S008475 S008614 S011188 S011438 S011596 S015023 S015149) SUP (CC14441 LT03396 S003595 S005593 S005638 S005908 S007182 S007596 S008367 ST00658 ST00866 ST00869 ST00873 ST01648 ST01941 ST01943 ST03595 ST03775 ST04412 ST04897 ST05192 ST05208 ST05504 ST05593 ST05638 ST05908 ST07182 ST07539 ST07596 ST07696 ST07803 ST08367 ST08398 ST08682 ST09209 ST10447 ST11184 ST13800 ST13876 ST13877 ST13886 ST15147) ++HOLD (LU03396) SYSTEM FMID (CCLXD51) REASON (ACTION) DATE (21348) COMMENT (<table> <tr> <td>OPS/MVS</td><td>Release 13.5</td></tr> </table> 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	OPS/MVS	Release 13.5
OPS/MVS	Release 13.5		

Service	Details
	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.). ++HOLD (LU03396) SYSTEM FMID(CCLXD51) REASON (DOC) DATE (21348) COMMENT (<pre> +-----+ OPS/MVS Release 13.5 +-----+ ***** * PUBLICATION * ***** See section "Configure the Web Application" in the CA OPS/MVS documentation set at http://techdocs.broadcom.com/opsmvs). ++HOLD (LU03396) SYSTEM FMID(CCLXD51) REASON (DYNACT) DATE (21348) COMMENT (<pre> +-----+ CA OPS/MVS Web Components Release 13.5 +-----+ 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 </pre> </pre>

Service	Details
	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 <pre>). 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)) . </pre>

Service	Details		
LU03738	LU03738 M.C.S. ENTRIES = ++PTF (LU03738) 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. R00368-CLX135-SP1 DESC(EPI ENQ NOT RELEASED WHEN REXX PROGRAM ENDS) . ++VER (Z038) FMID (CCLXD50) PRE (LU01174 LU03793 S000476 S004411 S005680 S006939 S009364 S010241 S010450 S010726 S011144 S013481) SUP (AS00476 LT00830 LT03738 LU00830 S001297 S001752 S005727 S012101 S012676 ST01297 ST01752 ST05727 ST12101 ST12676) ++HOLD (LU03738) SYSTEM FMID(CCLXD50) REASON (DYNACT) DATE (21344) COMMENT (<table border="1"> <tr> <td>OPS/MVS</td><td>Release 13.5</td></tr> </table> 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 SMPDOUT to identify the specific load modules that are updated.	OPS/MVS	Release 13.5
OPS/MVS	Release 13.5		

Service	Details
	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). 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
LU03793	LU03793 M.C.S. ENTRIES = ++PTF (LU03793) 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. R00370-CLX135-SP1 DESC(ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE). ++VER (Z038) FMID (CCLXD50) SUP (LT03793) ++IF FMID(CCLXD51) REQ(LU03794) . ++IF FMID(CCLXD53) REQ(LU03795) . ++HOLD (LU03793) SYSTEM FMID(CCLXD50) 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
LU03794	LU03794 M.C.S. ENTRIES = ++PTF (LU03794) 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. R00370-CLX135-SP1 DESC(ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE). ++VER (Z038) FMID (CCLXD51) SUP (LT03794) ++IF FMID(CCLXD53) REQ(LU03795) . ++IF FMID(CCLXD50) REQ(LU03793) .

Service	Details
LU03795	LU03795 M.C.S. ENTRIES = ++PTF (LU03795) 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. R00370-CLX135-SP1 DESC(ENABLE SYSVIEW PRODUCT PTF ANALYSIS FEATURE). ++VER (Z038) FMID (CCLXD53) SUP (LT03795) ++IF FMID(CCLXD51) REQ(LU03794) . ++IF FMID(CCLXD50) REQ(LU03793) .

Service	Details																		
LU03883	LU03883 M.C.S. ENTRIES = ++PTF (LU03883) 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. R00372-CLX135-SP1 DESC (SECURITY OR INTEGRITY PROBLEM). ++VER (Z038) FMID (CCLXD51) PRE (LU03794 S000236 S005737 S005996 S006380 S007231 S011488 S012373) SUP (DC14441 LT03166 LT03883 LU03166 S004296 ST04296 TR99948) ++HOLD (LU03883) SYSTEM FMID(CCLXD51) REASON (ACTION) DATE (21350) COMMENT (<table border="1"> <tr> <td>CA OPS/MVS Web Components</td><td>Release 13.5</td></tr> <tr> <td>SEQUENCE</td><td>After Apply</td></tr> <tr> <td>PURPOSE</td><td>To activate the fix</td></tr> <tr> <td>USERS</td><td>User's of the OPS/MVS Web Services</td></tr> <tr> <td>AFFECTED</td><td></td></tr> <tr> <td>KNOWLEDGE</td><td>Web servers and USS directories</td></tr> <tr> <td>REQUIRED</td><td></td></tr> <tr> <td>ACCESS</td><td>USS directories for Tomcat Web Server</td></tr> <tr> <td>REQUIRED</td><td></td></tr> </table> ***** * 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	CA OPS/MVS Web Components	Release 13.5	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	
CA OPS/MVS Web Components	Release 13.5																		
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																			

Service	Details
	and uses the newly updated opsmvs.war file.). 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('../listks.sh') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../makeks.sh') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../opwebsvc.prop') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../OPWShhttp.rex') PARM(PATHMODE(0,7,5,5)) . BINARY LINK('../opsmvs.war') PARM(PATHMODE(0,7,5,5)) .

Service	Details		
LU03941	LU03941 M.C.S. ENTRIES = ++PTF (LU03941) 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. R00373-CLX135-SP1 DESC (SECURITY OR INTEGRITY PROBLEM). ++VER (Z038) FMID (CCLXD51) PRE (LU03794 S000236 S000873 S001943 S003775 S004412 S005192 S005737 S005996 S006920 S008475 S008614 S011188 S011438 S011596 S015023 S015149) SUP (AL03396 CC14441 LT03396 LT03941 LU03396 S003595 S005593 S005638 S005908 S007182 S007596 S008367 ST00658 ST00866 ST00869 ST00873 ST01648 ST01941 ST01943 ST03595 ST03775 ST04412 ST04897 ST05192 ST05208 ST05504 ST05593 ST05638 ST05908 ST07182 ST07539 ST07596 ST07696 ST07803 ST08367 ST08398 ST08682 ST09209 ST10447 ST11184 ST13800 ST13876 ST13877 ST13886 ST15147) ++HOLD (LU03941) SYSTEM FMID(CCLXD51) REASON (ACTION) DATE (21351) COMMENT (<table> <tr> <td>OPS/MVS Web Components</td><td>Release 13.5</td></tr> </table> 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	OPS/MVS Web Components	Release 13.5
OPS/MVS Web Components	Release 13.5		

Service	Details
	<pre> 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. 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 (LU03941) SYSTEM FMID(CCLXD51) REASON (DOC) DATE (21351) COMMENT (+-----+-----+ OPS/MVS Release 13.5 +-----+-----+ ***** * PUBLICATION * ***** See section "Configure the Web Application" in the OPS/MVS documentation set at http://techdocs.broadcom.com/opsmvs.). ++HOLD (LU03941) SYSTEM FMID(CCLXD51) REASON (DYNACT) DATE (21351) COMMENT (+-----+-----+ OPS/MVS Release 13.5 +-----+-----+ 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 </pre>

Service	Details
	<pre> - 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)) . </pre>

Service	Details																		
LU03970	LU03970 M.C.S. ENTRIES = ++PTF (LU03970) 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 15671 Copyright (C) 2021 CA. All rights reserved. R00374-CLX135-SP1 DESC (SECURITY OR INTEGRITY PROBLEM). ++VER (Z038) FMID (CCLXD51) PRE (LU03794 S006167) SUP (AS06167 LT03970) ++HOLD (LU03970) SYSTEM FMID(CCLXD51) REASON (ACTION) DATE (21351) COMMENT (<table border="1"> <tr> <td>OPS/MVS</td><td>Release 13.5</td></tr> </table> ----- <table border="1"> <tr> <td>SEQUENCE</td><td>After Apply</td></tr> </table> ----- <table border="1"> <tr> <td>PURPOSE</td><td>To redeploy NIM SM</td></tr> </table> ----- <table border="1"> <tr> <td>USERS</td><td>Users of NIM SM</td></tr> </table> ----- <table border="1"> <tr> <td>AFFECTED</td><td></td></tr> </table> ----- <table border="1"> <tr> <td>KNOWLEDGE</td><td>Basic z/OS programming skills</td></tr> </table> ----- <table border="1"> <tr> <td>REQUIRED</td><td></td></tr> </table> ----- <table border="1"> <tr> <td>ACCESS</td><td>Authority to access NIM-SM installation directories</td></tr> </table> ----- <table border="1"> <tr> <td>REQUIRED</td><td></td></tr> </table> ----- ***** * STEPS TO PERFORM * ***** 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).	OPS/MVS	Release 13.5	SEQUENCE	After Apply	PURPOSE	To redeploy NIM SM	USERS	Users of NIM SM	AFFECTED		KNOWLEDGE	Basic z/OS programming skills	REQUIRED		ACCESS	Authority to access NIM-SM installation directories	REQUIRED	
OPS/MVS	Release 13.5																		
SEQUENCE	After Apply																		
PURPOSE	To redeploy NIM SM																		
USERS	Users of NIM SM																		
AFFECTED																			
KNOWLEDGE	Basic z/OS programming skills																		
REQUIRED																			
ACCESS	Authority to access NIM-SM installation directories																		
REQUIRED																			

Service	Details
	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). BINARY LINK('.. /ca-nim-sm.war') PARM(PATHMODE(0,7,5,5)) .

Service	Details	
LU04003	M.C.S. ENTRIES = ++PTF (LU04003) 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. R00375-CLX135-SP1 DESC(SECURITY OR INTEGRITY PROBLEM). ++VER (Z038) FMID (CCLXD51) PRE (LU03166 LU03396 LU03794 LU03883 LU03941 LU03970 S000236 S000873 S001943 S003775 S004412 S005192 S005737 S006167 S006380 S006920 S007231 S008475 S008614 S011188 S011438 S011488 S011596 S012373 S015023 S015149) SUP (AL03970 BL03883 BL03941 LT04003 S003595 S004296 S005593 S005638 S005908 S005996 S007182 S007596 S008367 ST00658 ST00866 ST00869 ST00873 ST01648 ST01941 ST01943 ST03595 ST03775 ST04296 ST04412 ST04897 ST05192 ST05208 ST05504 ST05593 ST05638 ST05908 ST05996 ST07182 ST07539 ST07596 ST07696 ST07803 ST08367 ST08398 ST08682 ST09209 ST10447 ST11184 ST13800 ST13876 ST13877 ST13886 ST15147 TR99948) ++HOLD (LU04003) SYSTEM FMID(CCLXD51) REASON (ACTION) DATE (21355) COMMENT (+-----+ OPS/MVS Release 13.5 +-----+ SEQUENCE After apply +-----+ PURPOSE To activate the fix +-----+ USERS All MTC-A, NIM SM, OPS/MVS Web Services users AFFECTED +-----+	

Service	Details
	<pre> KNOWLEDGE Basic z/OS programming skills REQUIRED +-----+-----+ ACCESS MTC-A, NIM SM, and Web Services installation access REQUIRED +-----+-----+ ***** * STEPS TO PERFORM * ***** 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 (LU04003) SYSTEM FMID(CCLXD51) REASON (DOC) DATE (21355) COMMENT (+-----+-----+ OPS/MVS Release 13.5 +-----+-----+ ***** * PUBLICATION * </pre>

Service	Details
	<pre>***** See section "Configure the Web Application" in the OPS/MVS documentation set at http://techdocs.broadcom.com/opsmvs.). ++HOLD (LU04003) SYSTEM FMID(CCLXD51) REASON (DYNACT) DATE (21355) COMMENT (+-----+ OPS/MVS Release 13.5 +-----+-----+ 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'</pre>

Service	Details	
	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)) . 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('../listks.sh') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../makeks.sh') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../opwebsvc.prop') PARM(PATHMODE(0,7,5,5)) . TEXT LINK('../OPWShhttp.rex') PARM(PATHMODE(0,7,5,5)) . BINARY LINK('../opsmvs.war') PARM(PATHMODE(0,7,5,5)) .	
MCS	LU03241	STARTS ON PAGE 0002
MCS	LU03396	STARTS ON PAGE 0003
MCS	LU03738	STARTS ON PAGE 0006
MCS	LU03793	STARTS ON PAGE 0008
MCS	LU03794	STARTS ON PAGE 0015
MCS	LU03795	STARTS ON PAGE 0017
MCS	LU03883	STARTS ON PAGE 0018
MCS	LU03941	STARTS ON PAGE 0020
MCS	LU03970	STARTS ON PAGE 0023
MCS	LU04003	STARTS ON PAGE 0025

OPS/MVS for JES2/JES3 13.5
CA RS 2201 Product/Component Listing

26

Product Family	Product	Release
Systems Management	CA OPS/MVS BASE	13.05.00
The CA RS 2201 Product/Component Count for this release is 1		

CA RS Level	Service	FMID
CAR2201	LU04003	CCLXD51
	LU03970	CCLXD51
	LU03941	CCLXD51
	LU03883	CCLXD51
	LU03795	CCLXD53
	LU03794	CCLXD51
	LU03793	CCLXD50
	LU03738	CCLXD50
	LU03396	CCLXD51
	LU03241	CCLXD50
	LU03388	CCLXD50
	LU03374	CCLXD51
CAR2112	LU03319	CCLXD50
	LU03048	CCLXD53
	LU03304	CCLXD50
	LU03176	CCLXD50
CAR2111	LU03166	CCLXD51
	LU03100	CCLXD50
	LU03098	CCLXD50
	LU03071	CCLXD50
	LU02946	CCLXD50
	LU02826	CCLXD50
	LU02686	CCLXD50
	LU02563	CCLXD50
CAR2109	LU02546	CCLXD50
	LU02483	CCLXD50
	LU02288	CCLXD50
	LU02156	CCLXD50
	LU02088	CCLXD50
	LU02210	CCLXD50
	LU02081	CCLXD50
CAR2108	LU02043	CCLXD50
	LU02019	CCLXD50
	LU01397	CCLXD50
	LU01174	CCLXD50
CAR2106	LU01075	CCLXD50
	LU01114	CCLXD50
	LU00996	CCLXD50
CAR2105	LU00878	CCLXD50
	LU00830	CCLXD50
	LU00629	CCLXD50
	LU00675	CCLXD50
	LU00608	CCLXD50
CAR2104	LU00495	CCLXD50
	LU00461	CCLXD50
	LU00408	CCLXD50
	LU00347	CCLXD50
	LU00347	CCLXD50

CA RS Level	Service	FMID
CAR2102	LU00079	CCLXD50
	LU00073	CCLXD50
	LU00068	CCLXD50
	LU00064	CCLXD50
	LU00062	CCLXD50
	LU00043	CCLXD50
	LU00038	CCLXD50
CAR2101	S015923	CCLXD50
	S015904	CCLXD50
	LU00026	CCLXD50
CAR2012	S015707	CCLXD50
	S015685	CCLXD50
	S015657	CCLXD50
	S015612	CCLXD50
	S015580	CCLXD50
	S015562	CCLXD50
	S015547	CCLXD50
	S015523	CCLXD50
	S015471	CCLXD50
	S015181	CCLXD50
	S015141	CCLXD50
CAR2011	S015423	CCLXD50
	S015253	CCLXD50
	S015164	CCLXD50
	S015149	CCLXD51
	S015066	CCLXD50
	S015023	CCLXD51
	S014910	CCLXD50
CAR2010	S015017	CCLXD50
	S014997	CCLXD50
	S014972	CCLXD50
	S014933	CCLXD50
	S014645	CCLXD50
	S014390	CCLXD50
CAR2009	S014532	CCLXD50
	S014418	CCLXD51
	S014302	CCLXD50
	S014192	CCLXD50
	S012679	CCLXD50
CAR2008	S014096	CCLXD50
	S013923	CCLXD50
	S013046	CCLXD50
CAR2007	S013791	CCLXD50
	S013681	CCLXD50
	S013680	CCLXD50
	S013643	CCLXD50
	S013638	CCLXD50

CA RS Level	Service	FMID
	S013481	CCLXD50
	S013470	CCLXD50
	S013447	CCLXD50
	S013422	CCLXD50
CAR2006	S013347	CCLXD50
	S013070	CCLXD50
	S012245	CCLXD50
CAR2005	S012733	CCLXD50
	S012722	CCLXD50
	S012676	CCLXD50
	S012673	CCLXD50
	S012658	CCLXD50
	S012630	CCLXD50
	S012622	CCLXD50
	S012418	CCLXD50
CAR2004	S012591	CCLXD50
	S012414	CCLXD50
	S012403	CCLXD50
	S012373	CCLXD51
CAR2003	S012139	CCLXD50
	S012138	CCLXD50
	S012101	CCLXD50
	S012096	CCLXD50
	S012060	CCLXD50
	S012013	CCLXD50
	S011954	CCLXD50
	S011953	CCLXD50
	S011878	CCLXD50
	S011877	CCLXD51
	S011812	CCLXD50
CAR2002	S011652	CCLXD50
	S011596	CCLXD51
	S011591	CCLXD50
	S011514	CCLXD50
	S011508	CCLXD50
	S011488	CCLXD51
	S011487	CCLXD50
	S011445	CCLXD50
	S011438	CCLXD51
	S011437	CCLXD50
	S011434	CCLXD50
	S011428	CCLXD50
	S011347	CCLXD50
	S011214	CCLXD50
	S006491	CCLXD50
CAR2001	S011260	CCLXD50
	S011241	CCLXD50

CA RS Level	Service	FMID
	S011213	CCLXD50
	S011203	CCLXD50
	S011188	CCLXD51
	S011144	CCLXD50
	S011125	CCLXD50
	S011100	CCLXD50
	S011092	CCLXD50
	S010733	CCLXD51
CAR1912	S010914	CCLXD50
	S010765	CCLXD50
	S010764	CCLXD50
	S010726	CCLXD50
	S010719	CCLXD50
	S010672	CCLXD50
	S010613	CCLXD50
	S010552	CCLXD50
CAR1911	S010490	CCLXD50
	S010476	CCLXD50
	S010453	CCLXD50
	S010450	CCLXD50
	S010413	CCLXD50
	S010402	CCLXD50
	S010384	CCLXD50
	S010262	CCLXD50
CAR1910	S010241	CCLXD50
	S010050	CCLXD50
	S010024	CCLXD50
	S009878	CCLXD50
	S009794	CCLXD50
	S009449	CCLXD50
	S008614	CCLXD51
	S008478	CCLXD50
CAR1909	S009846	CCLXD50
	S009840	CCLXD50
	S009667	CCLXD50
	S009544	CCLXD50
	S009387	CCLXD50
	S009094	CCLXD50
CAR1908	S009364	CCLXD50
	S009193	CCLXD50
	S009160	CCLXD50
	S009115	CCLXD50
CAR1907	S009020	CCLXD50
	S009000	CCLXD50
	S008999	CCLXD50
	S008872	CCLXD50
	S008831	CCLXD50

CA RS Level	Service	FMID
	S008829	CCLXD50
	S008714	CCLXD50
	S008712	CCLXD50
	S008651	CCLXD50
	S008640	CCLXD50
	S008475	CCLXD51
	S008474	CCLXD50
CAR1906	S008647	CCLXD50
	S008645	CCLXD50
	S008583	CCLXD50
	S008572	CCLXD50
	S008535	CCLXD50
	S008471	CCLXD50
	S008386	CCLXD50
	S008367	CCLXD51
	S008357	CCLXD50
	S008339	CCLXD50
	S008299	CCLXD50
	S008241	CCLXD50
	S008166	CCLXD53
	S006836	CCLXD50
CAR1905	S008113	CCLXD50
CAR1904	S007801	CCLXD50
	S007732	CCLXD50
	S007650	CCLXD50
	S007596	CCLXD51
	S007510	CCLXD50
CAR1903	S007406	CCLXD50
	S007289	CCLXD50
	S007231	CCLXD51
	S007197	CCLXD50
CAR1902	S007182	CCLXD51
	S007131	CCLXD50
	S006990	CCLXD50
	S006965	CCLXD50
	S006962	CCLXD50
	S006939	CCLXD50
	S006933	CCLXD50
	S006920	CCLXD51
	S006788	CCLXD50
CAR1901	S006555	CCLXD50
	S006527	CCLXD50
	S006526	CCLXD50
	S006167	CCLXD51
	S006166	CCLXD50
CAR1812	S006502	CCLXD50
	S006380	CCLXD51

CA RS Level	Service	FMID
	S006379	CCLXD50
	S006345	CCLXD50
	S006257	CCLXD50
	S006212	CCLXD50
	S006109	CCLXD50
	S005996	CCLXD51
CAR1811	S006105	CCLXD50
	S006042	CCLXD50
	S005965	CCLXD50
	S005934	CCLXD50
	S005908	CCLXD51
	S005737	CCLXD51
	S005727	CCLXD50
	S005704	CCLXD50
	S005690	CCLXD50
CAR1810	S005680	CCLXD50
	S005674	CCLXD50
	S005661	CCLXD50
	S005638	CCLXD51
	S005619	CCLXD50
	S005593	CCLXD51
	S005592	CCLXD50
	S005541	CCLXD50
	S005320	CCLXD50
	S005285	CCLXD50
	S005275	CCLXD50
CAR1809	S005192	CCLXD51
	S005191	CCLXD50
	S005047	CCLXD50
	S005042	CCLXD50
	S004989	CCLXD50
	S004944	CCLXD50
	S004928	CCLXD50
	S004900	CCLXD50
	S004898	CCLXD50
	S004808	CCLXD50
	S004772	CCLXD50
	S004680	CCLXD50
	S004634	CCLXD50
CAR1808	S004649	CCLXD50
	S004626	CCLXD50
	S004490	CCLXD50
	S004412	CCLXD51
	S004411	CCLXD50
	S004296	CCLXD51
CAR1807	S003933	CCLXD50
	S003910	CCLXD50

CA RS Level	Service	FMID
	S003905	CCLXD50
	S003594	CCLXD50
	S001859	CCLXD50
CAR1806	S003775	CCLXD51
	S003731	CCLXD50
	S003595	CCLXD51
	S001956	CCLXD50
	S001943	CCLXD51
	S001874	CCLXD50
	S001813	CCLXD50
	S001752	CCLXD50
CAR1805	S001580	CCLXD50
	S001320	CCLXD50
	S001297	CCLXD50
	S001270	CCLXD50
	S001221	CCLXD50
CAR1804	S001097	CCLXD50
	S001092	CCLXD50
	S001061	CCLXD50
	S000908	CCLXD50
	S000873	CCLXD51
	S000597	CCLXD50
CAR1803	S000632	CCLXD50
	S000630	CCLXD50
	S000572	CCLXD50
	S000562	CCLXD50
	S000476	CCLXD50
	S000444	CCLXD50
	S000393	CCLXD50
	S000371	CCLXD50
	S000247	CCLXD50
	S000245	CCLXD50
	S000239	CCLXD50
	S000236	CCLXD51
	S000235	CCLXD50