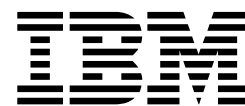


CICS Transaction Server for z/OS
Version 5 Release 2



Upgrading from CICS TS Version 5.1

CICS Transaction Server for z/OS
Version 5 Release 2



Upgrading from CICS TS Version 5.1

Note

Before using this information and the product it supports, read the information in “Notices” on page 167.

This edition applies to the IBM CICS Transaction Server for z/OS Version 5 Release 2 (product number 5655-Y04) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2001, 2016.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Preface	vii	Chapter 8. Changes to the CICS management client interface (CMCI) ..	39
Part 1. Changes to CICS externals ..	1	Chapter 9. Changes to the CICS-supplied transactions	41
Chapter 1. Changes to installation procedures	3	Changes to CSFE	41
Value for the z/OS MEMLIMIT parameter	3	New transaction CFCR	41
Release levels on INQUIRE SYSTEM command.	4	Chapter 10. Changes to global user exits and task-related user exits.	43
Changing start procedures to include the activation module	4	Changes to the DFHUEPAR standard parameter list	44
Chapter 2. Changes to system initialization parameters	5	Changes to global user exits	44
Obsolete system initialization parameters	5	New global user exit points	45
Changed system initialization parameters	5	Changes to task-related user exits	45
New system initialization parameters	6	Chapter 11. Changes to the exit programming interface	47
Chapter 3. Changes to the application programming interface	9	Changes to the exit programming interface (XPI) ..	48
Changed API commands	9	New exit programming interface (XPI) calls	49
New API commands	11	Chapter 12. Changes to user-replaceable programs	51
API commands that have been made threadsafe ..	12	Obsolete user-replaceable programs	51
Chapter 4. Changes to the JCICS application programming interface. ..	13	Changed user-replaceable programs	51
Chapter 5. Changes to resource definitions	15	New user-replaceable programs	54
Obsolete resource definition types and attributes ..	15	Chapter 13. Changes to CICS utilities ..	55
Obsolete CICS-supplied resource definitions	16	Chapter 14. Changes to monitoring ..	57
Changed resource definitions	16	Obsolete monitoring data fields.	57
New resource definitions	17	Changed monitoring data fields	57
New CICS-supplied resource definition groups ..	17	New monitoring data fields	57
DFHFCTRL	17	Monitoring sample program DFH\$MOLS: support for data for earlier CICS releases	57
Changed CICS-supplied resource definition groups	17	Chapter 15. Changes to statistics	59
DFHPGAIP	17	Obsolete statistics types	59
Changes to control tables (macro resource definition)	18	Changed statistics types	59
Chapter 6. Changes to the system programming interface	19	New statistics types	61
Obsolete SPI commands and options	19	Chapter 16. Changes to sample programs	63
Changed SPI commands	20	Chapter 17. Changes to problem determination	65
New SPI commands	30	Chapter 18. Changes to security.	67
SPI commands that have been made threadsafe ..	31	Additions to CICS RACF category 1 transactions ..	69
Chapter 7. Changes to CEMT	33	Changes to command and resource security	69
Obsolete CEMT commands and options	33		
Changed CEMT commands	33		
New CEMT commands	37		

Part 2. Upgrading CICS Transaction Server	71	Making applications and CICS bundles available	106
Chapter 19. Upgrade procedures for all CICS regions	73	Changes to resources defined in CICS bundles ..	107
Redefining and initializing the local and global catalogs	73	Private resources for application versions on platforms.	110
Enabling z/OS conversion services	73	Multi-versioning for applications deployed on platforms.	113
Upgrading the CSD for CICS-supplied and other IBM-supplied resource definitions	74	Application context enhancements	114
Upgrading user-modified CICS-supplied resource definitions.	75	New policy rule types and rule items	115
Upgrading copies of CICS-supplied resource definitions.	76		
DSA size limits	76	Part 3. Changes to CICSplex SM externals	119
CSD compatibility between different CICS releases	77	Chapter 31. Changes to CICSplex SM installation and definition	121
Upgrading CICS Explorer	81	Change to generic alert structures used by CICSplex SM	121
Chapter 20. Upgrading application programs	83	Chapter 32. Changes to CICSplex SM views and resource tables	123
Chapter 21. Upgrading Business Transaction Services (BTS)	85	Changed CICSplex SM views and resource tables	123
Chapter 22. Communicating over IPIC with different levels of CICS	87	New CICSplex SM views and resource tables. ..	123
Chapter 23. Upgrading multiregion operation (MRO)	89	Chapter 33. Programs that connect to a previous release of CICSplex SM ..	125
Chapter 24. Upgrading the Java environment	91	Part 4. Upgrading CICSplex SM	127
Key changes to CICS support for Java applications	91	Chapter 34. Conditions for running CICSplex SM Version 5.2 and earlier releases concurrently	129
Changes to options in JVM profiles	92	Chapter 35. Upgrading CICSplex SM API programs	133
Chapter 25. Upgrading the CICS-WebSphere MQ connection . . .	95	Chapter 36. Upgrading a CMAS. . . .	135
Chapter 26. Upgrading the CICS DB2 connection	97	Chapter 37. Upgrading a Web User Interface server	137
Chapter 27. Upgrading SOAP web services	99	Phased upgrade scenario for Web User Interface servers	139
Chapter 28. Upgrading JSON web services.	101	Upgrading the contents of the Web User Interface server repository (EYUWREP).	140
Upgrading the JSON web services assistant . . .	101	Chapter 38. Upgrading a CICSplex SM managed CICS system (MAS) . . .	141
Chapter 29. Upgrading SAML support	103	Part 5. Changes to CICS messages and codes	143
Chapter 30. Upgrading platforms, applications, policies, and CICS bundles	105		
Requirements for application entry points and operation names	105		

Chapter 39. Deleted messages	145
Chapter 40. Changed messages	147
Chapter 41. New messages	153
Chapter 42. Deletedabend codes	161
Chapter 43. Newabend codes	163
<hr/>	
Part 6. Appendixes	165
Notices	167
Trademarks	169

Bibliography.	171
CICS books for CICS Transaction Server for z/OS	171
CICSplex SM books for CICS Transaction Server	
for z/OS	172
Other CICS publications.	172
Accessibility.	173
Index	175

Preface

This information is about upgrading to CICS® Transaction Server for z/OS®, Version 5 Release 2. This information set provides the relevant information for users who are upgrading from CICS Transaction Server for z/OS, Version 5 Release 1.

If you are upgrading from an older release, select the information set for the release from which you are upgrading. The information sets for older releases include additional information about changes that took place in the intervening releases.

Note: The oldest release for which information about upgrading is provided with CICS Transaction Server for z/OS, Version 5 Release 2 is CICS Transaction Server for z/OS, Version 3 Release 1. If you are upgrading from a release of CICS earlier than this, you are recommended to read the information about upgrading and about changes to functions that was provided in the documentation for any additional intervening releases.

The information about upgrading is designed to tell you about:

- Any changes to the installation process for the product.
- New, changed and obsolete externals of the product, such as commands and messages.
- Tasks that you perform to upgrade from your previous release of the product, to the new release, so that the applications that ran under your previous release can continue to run under the new release at an equivalent level of function. Some tasks apply to all users, and some apply only if your applications use a particular function, such as support for Java™.
- Tasks that you perform if you want to enable new functions that are available in this release, or change your existing system settings or applications to use the new functions.

This information assumes that you are familiar with CICS and CICSplex® System Manager, either as a systems administrator, or as a system or application programmer. You should also have read about the new function in this release of CICS Transaction Server as described in the *CICS Transaction Server for z/OS What's New*.

Notes on terminology

CICS refers to the CICS element of CICS Transaction Server for z/OS.

CICS TS, unless stated otherwise, refers to the release of CICS Transaction Server for z/OS to which you are upgrading.

CICSplex SM refers to the CICSplex System Manager element of CICS Transaction Server for z/OS.

MVS™ is sometimes used for the operating system, the Base Control Program (BCP) element of z/OS.

Part 1. Changes to CICS externals

CICS externals, such as resource definitions and programming interfaces, have changed to support the changes in function for this CICS release. Read these topics to check which changes might affect your system.

Chapter 1. Changes to installation procedures

When you upgrade to CICS Transaction Server for z/OS, Version 5 Release 2, note these changes to the installation process.

You can install this release of CICS Transaction Server using the **SMP/E RECEIVE**, **APPLY**, and **ACCEPT** commands. Use the SMP/E dialogs to complete the SMP/E installation steps. The process meets IBM® Corporate Standards and might be familiar to you if you have installed other z/OS products.

The DFHISTAR process is still available if you prefer this method for installing CICS Transaction Server.

You must install the activation module. For more information, see Installing the CICS TS activation module in Installing.

For information about all the processes for installing CICS Transaction Server, see Installing.

Authorization routines

In z/OS, do not install SVCs or PC routines that return control to their caller in any authorized mode: that is, in supervisor state, system PSW key, or APF-authorized. Such action contravenes the z/OS Statement of Integrity.

If you invoke such services from CICS, you might compromise your system integrity, and IBM Service will not resolve any resulting problems.

Value for the z/OS MEMLIMIT parameter

To provide sufficient 64-bit (above-the-bar) storage for a CICS TS for z/OS, Version 5.2 region, set the value for the z/OS **MEMLIMIT** parameter equal to or greater than 6 GB. The default value in z/OS for **MEMLIMIT** is 2 GB.

CICS requires a **MEMLIMIT** value of 6 GB; any additional use by applications or JVMs should be allowed for with a larger value of **MEMLIMIT**. If you attempt to start a CICS region with a **MEMLIMIT** value that is less than 6 GB, message DFHSM0602 is issued, a system dump with the dump code KERNDUMP is produced, and CICS terminates.

You cannot alter the **MEMLIMIT** value for the CICS region while CICS is running. You can specify a new **MEMLIMIT** value on the next start of the CICS region.

A suitable **MEMLIMIT** value for a CICS region must provide sufficient storage for the facilities that use 64-bit storage that you plan to use. When upgrading, it is recommended that you check your **MEMLIMIT** calculation and take into account any changes in the use of 64-bit storage that may occur. For more information, see Estimating, checking, and setting MEMLIMIT in Improving performance.

This storage is not allocated on initialization; CICS allocates it as the need arises.

Release levels on INQUIRE SYSTEM command

You use the **EXEC CICS INQUIRE SYSTEM CICSTSLEVEL** command to determine the version and release number of CICS. Use the **EXEC CICS INQUIRE SYSTEM OSLEVEL** command to determine the level of z/OS.

To ensure compatibility with previous releases, the CICS base element maintains its own level (identification) number. Each time new function is added to CICS and shipped with the CICS Transaction Server product, the CICS level number is incremented.

The CICS level number in CICS TS 5.2 is 0690. This number is returned in the **RELEASE** parameter of the **INQUIRE SYSTEM** command.

The level number also appears in the alternative decimal form 6.9 in output from offline utilities such as statistics and dump formatters to identify the level of utility being used, and as the suffix in module names such as DFHPD690.

Changing start procedures to include the activation module

If you use a common, release-independent procedure to start CICS regions, you must include the data set for the activation module in the procedure.

The following JCL is an example of how you can add the data set for the activation module:

CICS procedure:

```
//CICSTS PROC REL=52
//CICS      EXEC PGM=DFHSIP,PARM='SI',REGION=0K,TIME=1439
//STEPLIB DD DISP=SHR,DSN=CICS&REL..SDFHAUTH ...
              ... plus other CICS datasets
//              INCLUDE MEMBER=LIC&REL
```

The PROCLIB has the following members for CICS TS for z/OS V5.2 and V5.1:

```
LIC52
//      DD DISP=SHR,DSN=CICS52.SDFHLIC

LIC51
//*      No activation module dataset required
```

Chapter 2. Changes to system initialization parameters

In CICS Transaction Server for z/OS, Version 5 Release 2, new system initialization parameters are available, and you might find that some system initialization parameters that you used previously are now obsolete. Also, the scope, default, or range of possible values for some existing system initialization parameters has changed. You might need to make changes to your system initialization table or your CICS startup JCL because of these changes.

To upgrade with the changes to CICS system initialization parameters described in this section, follow these instructions.

Use the default system initialization table

The unsuffixed default system initialization table (DFHSIT) is supplied in the CICS SDFHAUTH library. You can use the default table to start a CICS region using the default values. CICS loads DFHSIT by default if your JCL does not contain a SIT parameter.

Override defaults using the SYSIN data set

To override default values, specify system initialization parameters in a permanent member of a SYSIN data set. You can vary these during testing by changing the data set member, avoiding the need to reassemble suffixed system initialization tables. Nearly all system initialization parameters entered at run time are used even on a warm start. The main exceptions are the FCT and CSD parameters.

Obsolete system initialization parameters

Remove these obsolete parameters from your system initialization table or from your CICS startup JCL (for example, the SYSIN data set) before upgrading. If you specify any of these parameters, they are rejected and a message is issued.

No system initialization parameters were made obsolete in CICS Transaction Server for z/OS, Version 5 Release 2.

Changed system initialization parameters

For some system initialization parameters, the default is now changed, or the values that you can specify are changed, or the scope of the system initialization parameter is changed. You might need to modify your system initialization table (SIT) or CICS startup JCL because of these changes.

APAR PI28039 update

The default setting for the **ENCRYPTION** system initialization parameter, **ENCRYPTION=STRONG**, no longer allows the use of the SSL version 3.0 security protocol. The minimum security protocol allowed with **ENCRYPTION=STRONG** is now TLS version 1.0.

If you have clients that still require the SSL version 3.0 protocol, you can enable support for that protocol by specifying the system initialization parameter **ENCRYPTION=SSLV3** for the CICS region. SSL 3.0 should only be used for a migration period while clients that still require this protocol are upgraded. Any connections

that require encryption automatically use the TLS protocol, unless the client specifically requires SSL 3.0.

System initialization parameters changed in CICS Transaction Server for z/OS, Version 5 Release 2

ENCRYPTION={ALL|TLS12|STRONG|SSLV3}

Before CICS TS for z/OS, Version 5.2, the **ENCRYPTION** system initialization parameter supported these values: STRONG, ALL, and TLS12FIPS. The value TLS12FIPS is no longer supported. The new value TLS12 is added. To obtain the same result as using the old TLS12FIPS option, use TLS12, and also code the new system initialization parameter **NISTSP800131A=CHECK**.

If your system initialization table contains an invalid value, the default value, STRONG, is used instead. If you specify an override with an invalid value in your CICS JCL, CICS pauses during startup and prompts you to respecify the override. To avoid these occurrences, update any system initialization tables or JCL overrides to specify a valid value.

JVMPROFILEDIR={/usr/lpp/cicsts/cicsts52/JVMProfiles|directory}

From CICS TS for z/OS, Version 5.2, JVM servers can be defined in CICS bundles. For these JVM servers, the JVM profile is packaged in the CICS bundle with the JVMSERVER resource definition. CICS does not load these JVM profiles from the directory that is specified by **JVMPROFILEDIR**. Instead, they are stored in a suitable directory for the CICS bundle, and the location is specified by the CICS bundle.

MXT={250|number}

Before CICS TS for z/OS, Version 5.1, the minimum, default, and maximum values of the **MXT** parameter were 1, 5, and 999. In CICS TS for z/OS, Version 5.1, the minimum, default, and maximum values were changed to 10, 500, and 2000. From CICS TS for z/OS, Version 5.2, the minimum value is 10, the default value is 250, and the maximum value is 2000. These adjustments were made to ensure that CICS regions operate efficiently with the default setting and can process more workload.

New system initialization parameters

The default values for these parameters have minimal impact when you are upgrading from an earlier release of CICS.

New system initialization parameters added in CICS Transaction Server for z/OS, Version 5 Release 2

- The **NISTSP800131A** system initialization parameter specifies whether the CICS region is to check for conformance to the NIST SP800-131A standard.

NISTSP800131A={NOCHECK|CHECK}

NOCHECK

Conformance checking is not required in this CICS region. This is the default value.

CHECK

The CICS region is required to check for conformance with the NIST SP800-131A security standard. If this value is set, CICS issues a message if an actual or potential violation is detected.

This option also causes the CICS SSL environment to use only TLS v 1.2 with FIPS 140-2 standards applied.

The checks that are performed are as follows:

Web services

If the <wsse_handler> tag is specified in a pipeline configuration file, it implies that the pipeline is to be used for web services security. Because not all of the encryption algorithms that can be used for web services security are SP800-131A conformant, installing a pipeline that uses web services means that CICS might be non-conformant. CICS issues message DFHXS1300, which warns of potential nonconformance.

If you receive message DFHXS1300, check whether you are using DFHWSSE as the web services security handler. If you are not using DFHWSSE, inspect your security handler to check which encryption and signing algorithms it uses. If these algorithms are SP800-131A conformant, you can ignore the message. If they are not conformant, consider whether to use conformant algorithms instead. Otherwise, if the CICS region that issues the message must be conformant, consider moving the web service security workload to a different CICS region where conformance is not required.

CICS also checks for certain things that are not conformant to SP800-131A. If any of these situations are found, CICS issues message DFHXS1301:

- An <algorithm> element exists within the <authentication> element of the <wsse_handler> definition in the pipeline configuration file. The only algorithms that can be used are SHA-1 routines, which are not conformant with NIST SP800-131A.
- A <sign_body> element exists in the pipeline configuration file. The only algorithms that can be used are SHA-1 routines, which are not conformant with SP800-131A.
- An <encrypt_body> element in the pipeline configuration file. Of the four algorithms that can be used, three are conformant with SP800-131A but one is not. If the nonconformant algorithm is specified, DFHXS1301 is issued.

If you receive message DFHXS1301, consider not performing the encryption or signing operations in this CICS region. If the nonconformant algorithm is specified in the <encrypt_body> element, consider using a conformant algorithm.

Sockets

If SSL is active, setting **NISTSP800131A=CHECK** forces **ENCRYPTION=TLS12** if it is not already set. If **ENCRYPTION=TLS12** is forced, message DFHSO0144 is issued. Sockets domain initializes the SSL environment with the FIPS option on and the System SSL started task runs in FIPS mode. The effect of this is that SSL allows fewer ciphers to be used on a successful handshake.

To use FIPS with z/OS Version 2 Release 1 or later, ICSF (Integrated Cryptographic Services Facility) must be active on your system. If you have not already done so, apply APAR OA14956 to z/OS.

If SSL is inactive because no **KEYRING** parameter is specified, then setting NISTSP800131A has no effect on sockets domain.

JVM servers

When a JVM server is started, CICS sets the Java properties to make Java NIST SP800-131A conformant.

If you set **NISTSP800131A**=CHECK, you should also set **ENCRYPTION**=TLS12. However, if you do not do so, CICS overrides the value of **ENCRYPTION** to **ENCRYPTION**=TLS12 and issues a warning message.

- The **USSCONFIG** system initialization parameter specifies the name and path of the root directory for CICS Transaction Server configuration files on z/OS UNIX.

USSCONFIG={/var/cicsts/dfhconfig | *directory*}

Specifies the directory in which z/OS UNIX configuration files are stored.
The default value is /var/cicsts/dfhconfig.

Chapter 3. Changes to the application programming interface

CICS Transaction Server for z/OS, Version 5 Release 2 includes some new API commands to support new CICS functions, and some existing commands have changes to options and error conditions.

Program compatibility

CICS provides API compatibility from release to release. However, functional changes to some CICS components can affect some CICS API commands.

Except for the specific cases described in these topics, CICS Transaction Server provides compatibility with future releases, at source and object level, for all CICS application programs that are written to the CICS application programming interface and which run correctly under the previous release.

For information about CICS support for application programming languages, see the *CICS Transaction Server for z/OS What's New*.

Application program mask setting following a handled condition

CICS TS for z/OS, Version 5.2 resolves the problem reported in APAR PM73097. Previously, when CICS handled a condition encountered by an application as requested by an earlier EXEC CICS HANDLE CONDITION command, the application's program mask was set to zero in the PSW. As a consequence, in the event of a subsequent program exception in a PL/I program, such as an overflow, no interrupt occurred. Now, when CICS handles a condition, the application's program mask is correctly restored to the value that it had when the EXEC CICS HANDLE CONDITION command was issued.

Changed API commands

Some API commands are extended with new options or RESP2 values. Also, the usage of certain options on existing API commands has changed. Check the new descriptions to ensure that you are using these options in the best way.

ASSIGN

New options ERRORMSG and ERRORMSGLEN on the **ASSIGN** command return the error message for the CICS task:

ERRORMSG(*data-area*)

Returns the error message up to a maximum of 500 bytes that is currently referenced in the transaction abend control block for the CICS task. Following a failure of a DPL request, the message is that returned from the remote system. For messages shorter than 500 bytes the message is padded with nulls.

If no message is present, the 500 byte area contains nulls.

ERRORMSGLEN(*data-area*)

Returns a halfword binary value representing the length of the message returned for ERRORMSG. If the message referenced in the transaction abend control block exceeds 500 bytes, the message is truncated and the length is set to 500.

If no message is present the length returned is 0.

The new option LINKLEVEL on the **ASSIGN** command returns the program link level:

LINKLEVEL(*data-area*)

Returns a halfword binary value representing the program link level in the local system. The topmost link level is level one and for each EXEC CICS LINK the link level is incremented by one. The link level is not incremented for a language CALL statement. If a program is the target of a DPL request, the link level returned is that within the CICS region it is executing and not the wider distributed transaction. If a program is DPLed to, then link level one will be the CICS mirror program DFHMIRS.

New options APPLICATION, MAJORVERSION, MICROVERSION, MINORVERSION, OPERATION and PLATFORM on the **ASSIGN** command return the current application context associated with the task:

APPLICATION (*data-area*)

Returns the 64 character name of the current application associated with the task. It is part of the application context that is made up of the application name, the platform name, the operation name and the major, minor and micro version number of the application. If there is no application context associated with the task, then blanks are returned.

MAJORVERSION(*data-area*)

Returns the fullword binary value representing the major version of the current application associated with the task, which is part of the application context. If there is no application context associated with the task, then -1 is returned.

MICROVERSION(*data-area*)

Returns the fullword binary value representing the micro version of the current application associated with the task, which is part of the application context. If there is no application context associated with the task, then -1 is returned.

MINORVERSION(*data-area*)

Returns the fullword binary value representing the minor version of the current application associated with the task, which is part of the application context. If there is no application context associated with the task, then -1 is returned.

OPERATION(*data-area*)

Returns the 64 character name of the current operation associated with the task, which is part of the application context. If there is no application context associated with the task, then blanks are returned.

PLATFORM(*data-area*)

Returns the 64 character name of the platform associated with the task, which is part of the application context. If there is no application context associated with the task, then blanks are returned.

For more information see ASSIGN.

DELAY

The **DELAY** command has been enhanced to allow a value to be specified in milliseconds. However, CICS checks for delay expiry every 250 milliseconds, so the actual interval might vary depending on where in the scan cycle your request is made.

MILLISECS(*data-value*)

specifies a fullword binary value in the range 0–999, when HOURS, MINUTES or SECONDS are also specified, or 0-359999999 when MILLISECS is the only option specified.

For more information see DELAY.

FORMATTIME

The new option STRINGZONE on the **FORMATTIME** command specifies in what timezone the DATESTRING value should be returned, UTC or local time.

STRINGZONE(*cvda*)

Specifies the timezone in which the time stamp returned in DATESTRING is to be returned. The CVDA values are as follows:

UTC DATESTRING is to be returned in UTC. This value is the default setting.

LOCAL DATESTRING is to be returned in LOCAL timezone.

For more information see FORMATTIME.

LINK

This command operates in the current application context. If the command is issued by a program that is running under a task for an application deployed on a platform, CICS searches first for the named program in the private program directory for the application. If the named program is not found there, CICS then searches the public program directory.

When this command is used to link to a program that is declared as an application entry point for an application deployed on a platform, the CICS bundle where the application entry point is declared must have a status of AVAILABLE. The link is made to the highest numbered version of the application that is installed, enabled, and available. To link to a specified version of an application deployed on a platform, use the INVOKE APPLICATION command instead of the LINK command.

For more information see LINK.

New API commands

CICS Transaction Server for z/OS, Version 5 Release 2 includes some new API commands that you can use to create application programs that use new CICS functions.

EXEC CICS VERIFY TOKEN

Verify that a Kerberos token is valid, as determined by an external security manager, and optionally allow the caller to extract the RACF user ID that is associated with the principal in the Kerberos token.

EXEC CICS INVOKE APPLICATION

Invoke an application entry point program. **EXEC CICS INVOKE APPLICATION** allows invocation of an application by naming an operation that

corresponds to one of its program entry points, without having to know the name of the application entry point program and regardless of whether the program is public or private.

API commands that have been made threadsafe

These application programming interface commands were not threadsafe when they were first introduced in CICS, but they have now been made threadsafe.

No existing API commands were made threadsafe in this release.

Chapter 4. Changes to the JCICS application programming interface

The JCICS application programming interface has new methods and other new elements to provide Java support for some of the new functions available through the **EXEC CICS** application programming interface.

The methods in the JCICS API do not map exactly to the functions available through the **EXEC CICS** API. For example, the function of a single **EXEC CICS** command might be provided by multiple JCICS methods, or some functions of an **EXEC CICS** command might not be supported by any JCICS method. This topic lists the changes to the JCICS API with the **EXEC CICS** commands that provide the same functions, but the JCICS method and **EXEC CICS** command do not necessarily provide equivalent functions.

A new method in the Task class returns the current application context of the task:

```
com.ibm.cics.server.Task.getApplicationContext()
```

The JCICS API provides an equivalent for the following new API command:

INVOKE APPLICATION

The support is provided by the following new JCICS class:

com.ibm.cics.server.Application

This class is the Java implementation of the **EXEC CICS INVOKE APPLICATION** command.

Chapter 5. Changes to resource definitions

Changes to the resource definitions available in CICS relate to new, changed, or obsolete CICS functions. The changes might involve complete resource definitions or individual attributes. The resource definitions supplied by CICS have corresponding changes, which you can implement by running the UPGRADE function of the CSD utility program (DFHCSDUP).

Resources that can be defined and installed in CICS bundles

The updated BUNDLE resource has additional features to support the use of CICS bundles as part of applications that are deployed on platforms.

You can now create resource definitions in CICS bundles for the following additional CICS RDO resources:

- FILE
- JVMSERVER
- PIPELINE
- TCPIPService
- WEBSERVICE

For the list of all artifacts that you can define and deploy in CICS(r) bundles, including further RDO resources, JSON transforms, web applications, OSGi bundles and events, see [resource.bundle.artifacts](#).

Obsolete resource definition types and attributes

Some resource definition types and some attributes are now obsolete. You must replace obsolete resource definitions, and obsolete attributes as appropriate.

DNSGROUP in TCPIPService resource

The DNSGROUP attribute on TCPIPService resource definitions specified the group name with which CICS registered to Workload Manager, for connection optimization. DNSGROUP is obsolete as part of the removal of support for DNS Connection Optimization. DNSGROUP is supported for CSD compatibility for earlier releases of CICS where it is still valid.

EXPIRYINT in TSMODEL resource

The EXPIRYINT attribute on TSMODEL resource definitions specified the expiry interval for matching temporary storage queues in hours. It has been replaced by the EXPIRYINTMIN attribute, which specifies the expiry interval in minutes. EXPIRYINT is supported for CSD compatibility, and an expiry interval specified using EXPIRYINT is accepted in compatibility mode. New models should use the EXPIRYINTMIN attribute.

GRPCRITICAL in TCPIPService resource

The GRPCRITICAL attribute on TCPIPService resource definitions marked the service as a critical member of the DNS group. GRPCRITICAL is obsolete as part of the removal of support for DNS Connection Optimization. GRPCRITICAL is supported for CSD compatibility for earlier releases of CICS where it is still valid.

Obsolete CICS-supplied resource definitions

Some CICS-supplied resource definition groups are now obsolete, and they have been removed from the CICS-supplied default startup group list, DFHLIST. If you use customized startup group lists, you must remove any obsolete definition groups from them.

No CICS-supplied resource definitions were made obsolete in CICS Transaction Server for z/OS, Version 5 Release 2.

Changed resource definitions

Some existing resource definitions have new attributes added, or have changes to the values or scope of existing attributes. You can use the new attributes to add support for new CICS functions. If you have resource definitions that use the changed attributes, check that the value you are using is still the best for your situation.

If you have existing resource definitions that were created before the new attributes for the resources were available, check those resource definitions after you upgrade to this CICS release, to ensure that the default values are suitable for your situation. In some situations, CICS enforces certain values for options if these are required for compatibility with existing options in your resource definition.

DB2CONN resource definition: changed TCBLIMIT attribute

The CICS-DB2 interface has been enhanced to detect a mismatch between the number of threads defined and the number of TCBs defined. If the sum of the THREADLIMIT value for the pool (specified in the DB2CONN) and the THREADLIMIT values for all the DB2ENTRYs exceeds the TCBLIMIT value in the DB2CONN, then message DFHDB2110 is issued.

IPCONN resource definition: new HA attribute

The new HA attribute specifies whether or not the IPCONN definition can be used to connect to a high-availability cluster. The default setting, NO, means that it cannot be used to connect to a high-availability cluster.

IPCONN resource definition: changed APPLID attribute

The APPLID attribute specifies the application identifier of the remote system, such as a remote CICS region. If the IPCONN definition is used to connect to a high-availability cluster, you must specify a 1 to 8 character value that identifies the cluster.

TCPIPSERVICE resource definition: new SPECIFTCPS attribute

The new SPECIFTCPS attribute names the specific TCPIPSERVICE when you define a generic TCPIPSERVICE as part of a high-availability cluster. Use this parameter with the IPIC protocol, when the IP end point defined by the PORT and HOSTNAME or IPADDRESS attributes is the generic end point of an HA cluster of CICS regions.

TSMODEL resource definition: new EXPIRYINTMIN attribute

Support for expiration of temporary storage queues is extended to include temporary storage queues in shared temporary storage pools. A new attribute, EXPIRYINTMIN, specifies the expiry interval, in minutes, for a temporary storage queue that matches the temporary storage model. EXPIRYINTMIN replaces the EXPIRYINT attribute, which is still accepted for compatibility.

EXPIRYINTMIN specifies the expiry interval in minutes, rather than hours. TSMODEL resource definitions that specify the expiry interval in hours,

using the EXPIRYINT attribute, are accepted. New models should specify the interval in minutes. CICS rounds the minutes value up to a multiple of ten minutes. For more information, see TSMODEL resources in Reference -> System definition.

New resource definitions

You can use the new resource definitions that are available in CICS Transaction Server for z/OS, Version 5 Release 2 to define support for new CICS functions.

No new resource definition types were added in this release.

New CICS-supplied resource definition groups

New groups of CICS-supplied resource definitions are added to your CSD when you run the UPGRADE command.

DFHFCRL

The CICS-supplied group DFHFCRL, introduced in CICS Transaction Server for z/OS, Version 5 Release 2, contains definitions for new file control resources.

Group DFHFCRL is in DFHLIST. It contains a TRANSACTION resource definition for transaction CFCR, which is used by CICS to disable files that are defined in CICS bundles, and a PROGRAM resource definition for the program DFHFCRN which it runs.

Changed CICS-supplied resource definition groups

Changed groups of CICS-supplied resource definitions are added to your CSD when you run the UPGRADE command.

DFHPGAIP

The resource definitions for programs DFHPGADX, DFHPGAHX, DFHPGALX, and DFHPGAOX now specify CONCURRENCY(THREADSAFE).

For more information, see “DFHPGAIP”

DFHPGAIP

In CICS TS 5.2, the definitions for the CICS-supplied default autoinstall program, in the CICS-supplied group DFHPGAIP, changed to specify CONCURRENCY(THREADSAFE) to avoid TCB switching during program autoinstall.

The resource definitions for the following programs now specify CONCURRENCY(THREADSAFE):

- DFHPGADX, Assembler program
- DFHPGAHX, C program
- DFHPGALX, PL/I program
- DFHPGAOX, COBOL program

If you are using the CICS-supplied default program for program autoinstall, examine any code added to the exit to ensure it is threadsafe. If the code is not threadsafe, you must either make changes to make it threadsafe, or change the resource definition to specify CONCURRENCY(QUASIRENT).

For more information about threadsafe programming techniques, see Threadsafe programs in Developing applications.

Changes to control tables (macro resource definition)

When upgrading to CICS Transaction Server for z/OS, Version 5 Release 2, reassemble all CICS control tables using the CICS TS 5.2 macro libraries, even if the macro externals have no changes. You must also reassemble any DFHCNV data conversion tables that you use, because CICS initialization fails if you try to load DFHCNV tables assembled using macros from an earlier release.

DFHMCT monitoring control table

The performance class data fields added for CICS Transaction Server for z/OS, Version 5 Release 2, have corresponding new values, which can be defined on the INCLUDE and EXCLUDE operands of the DFHMCT TYPE=RECORD macro. You can use these values to include or exclude specific fields from performance class monitoring records. Control data recording - DFHMCT TYPE=RECORD in the *CICS Resource Definition Guide* lists all the fields that can now be included or excluded using the macro.

Chapter 6. Changes to the system programming interface

CICS Transaction Server for z/OS, Version 5 Release 2 has some new SPI commands to control new system resources, and some existing commands have new options, or new values for existing options. Some system programming commands, options, or values are now obsolete because they relate to obsolete CICS functions.

Program compatibility

The system programming commands operate on CICS system resources, such as control blocks and tables of resource definitions, and not on user resources, such as data, on which the API operates.

The SPI is also sensitive to the underlying environment in which it is implemented and, as a consequence, compatibility with future releases of CICS cannot be guaranteed.

This section describes the effect on the SPI of the functional changes in CICS, explaining where incompatibilities exist, to enable you to make programming changes where necessary.

Except for the instances given in this section, CICS continues to provide compatibility with future releases, at source and object level, for application programs that use the unaffected SPI commands.

Obsolete SPI commands and options

These system programming interface commands and options are obsolete. Remove these commands and options from your applications, because they represent functions that are no longer available, so the behavior of applications that use these commands changes.

CREATE TCPIP SERVICE

The DNSGROUP and GRPCRITICAL options, which were used in connection with DNS Connection Optimization, are obsolete. DNSGROUP specified the group name with which CICS registered with the z/OS Workload Manager (WLM) for connection optimization. GRPCRITICAL specified whether the TCPIP SERVICE resource was a critical member of the DNS group.

INQUIRE TCPIP SERVICE

The DNSGROUP, DNSSTATUS, and GRPCRITICAL options, which were used in connection with DNS Connection Optimization, are obsolete. DNSGROUP returned the group name with which CICS registered with the z/OS Workload Manager (WLM) for connection optimization. DNSSTATUS returned the Domain Name System (DNS) and Workload Manager (WLM) registration status of the TCPIP SERVICE resource. GRPCRITICAL identified whether the TCPIP SERVICE resource was a critical member of the DNS group.

SET TCPIP SERVICE

The DNSSTATUS option is obsolete. DNSSTATUS was used to specify the

Changed SPI commands

A number of existing system programming interface commands have new options or changes to the values that are available for options.

Inquiring on private resources for applications

A resource that is defined as part of an application installed on a platform is private to that version of that application. For supported resource types, a resource is private if the resource is defined in a CICS bundle that is packaged and installed as part of an application, either as part of the application bundle, or as part of the application binding bundle. A resource that is defined by any other method is publicly available for all tasks, and is known as a public resource.

The following CICS resources are supported as private resources for applications:

- **LIBRARY** resources, which represent one or more data sets, known as dynamic program **LIBRARY** concatenations, from which program load modules can be loaded.
- **POLICY** resources, which represent one or more rules that manage the behavior of user tasks in CICS regions.
- **PROGRAM** resources, which represent an application program. A program that is auto-installed by a task for an application that is deployed on a platform is also private to that version of the application.

You can inquire on or browse private resources using the **EXEC CICS INQUIRE** system programming command for the resource type. By default, CICS searches for the resources that are available to the program where the **EXEC CICS INQUIRE** command is issued. You can also choose to browse private resources for a specified application.

- When you issue an **EXEC CICS INQUIRE** command from a public program, information is returned about the named public resource. If the resource is not available as a public resource, a “not found” response is returned.
- When you issue an **EXEC CICS INQUIRE** command from a program that is running under a task for an application deployed on a platform, information is returned about the named private resource for that application, if it exists. If the application does not have a private resource with that name, information is returned about a public resource with the specified name. If the resource is not available as a private resource for that application or as a public resource, a “not found” response is returned.
- When you use an **EXEC CICS INQUIRE** command in browse mode from a public program, if you do not specify any other input parameters, the set of public resources of the specified type is returned. If the same browse command is issued from a program that is running under a task for an application deployed on a platform, the browse returns a set of resources consisting of any private resources of the specified type for the application, and the public resources of the specified type.
- To browse the private resources for an application, from either a public program or a private program, issue the **EXEC CICS INQUIRE** command with the **START** option and specify as input the application context, consisting of the platform, application, and application version. The browse returns a set of resources

consisting of only the private resources of the specified type for the application. If no application is found with the specified application context, the APPNOTFOUND condition is returned.

For more information about browsing private resources, including examples of browsing resources for a different application from the application where you issue the command, see Browsing resource definitions in Developing system programs.

CREATE IPCONN

A new option HA is added to the **CREATE IPCONN** command.

HA(**{NO|YES}**)

Specifies whether the IPCONN can be used to connect to a high-availability cluster.

NO This is the default value. The IPCONN cannot be used to connect to a high-availability cluster.

YES The IPCONN must connect to a region that is part of a high-availability cluster.

The APPLID option specifies the application identifier of the remote system, such as a remote CICS region. If the IPCONN definition is used to connect to a high-availability cluster, you must specify a 1 to 8 character value that identifies the cluster.

CREATE TCPIP SERVICE

A new option SPECIFTCPS is added to the **CREATE TCPIP SERVICE** command.

SPECIFTCPS

This parameter specifies the 8-character name of the specific TCPIP SERVICE when defining a generic TCPIP SERVICE as part of a high-availability cluster. This parameter is only valid when the protocol is IPIC and the IP end point defined by the PORT and HOSTNAME or IPADDRESS attributes is the generic end point of an HA cluster of CICS regions.

Acceptable characters:

A-Z 0-9 \$ @ #

Unless you are using the CREATE command, any lowercase characters are converted to uppercase.

CREATE TSMODEL

A new option EXPIRYINTMIN is added to the **CREATE TSMODEL** command.

EXPIRYINTMIN(**{0|number}**)

Specifies the expiry interval, in minutes, for a temporary storage queue that matches this model. CICS uses the value rounded up to the nearest multiple of 10 minutes. The interval count begins after each use of the temporary storage queue. If the queue is not used again before the expiry interval is reached, the queue becomes eligible for CICS to delete it automatically.

0 No expiry interval applies to temporary storage queues that match this model, and they are never eligible for automatic deletion. This setting is the default.

number

An expiry interval in minutes, in the range 1 - 900000. After this expiry interval, a temporary storage queue that matches this model becomes eligible for automatic deletion if it has not been used again.

Expiry intervals apply to temporary storage queues in the following locations:

- Main temporary storage in the local CICS region.
- Nonrecoverable auxiliary temporary storage (DFHTEMP data set) associated with the local CICS region.
- Temporary storage queues in shared temporary storage pools (CICS TS 5.2 and higher).

Expiry intervals do not apply to the following types of temporary storage queues, so CICS never deletes them automatically:

- Queues in auxiliary temporary storage that are defined as recoverable.
- Queues in a remote CICS region. To make CICS delete remote temporary storage queues, specify an expiry interval in a suitable TSMODEL resource definition in the region that owns the queues.
- Queues that CICS creates for its own use.

If you change the expiry interval in a TSMODEL resource definition, existing temporary storage queues that match the model are not affected. Those queues continue to use the expiry interval that applied when they were created. If all the TSMODEL resource definitions with a nonzero expiry interval are deleted from a CICS region, CICS stops scanning for expired temporary storage queues.

EXTRACT STATISTICS and COLLECT STATISTICS

When you use the **EXEC CICS EXTRACT STATISTICS** or **EXEC CICS COLLECT STATISTICS** command to request resource statistics for a specific resource of a resource type that is supported as a private resource, the command operates according to the context in which the task is running.

- If the command is issued from a public program, statistics are returned for the named public resource.
- If the command is issued from a program that is part of an application deployed on a platform, so is running with an application context, the private resources for the application are searched first for the named resource. If a private resource is not found, statistics are returned for the named public resource.
- For the **EXEC CICS EXTRACT STATISTICS** command only, you can specify a different application context to be searched for private resources. When you request statistics for a different application, if a private resource is not found for that application, no statistics are returned.

When you use the **EXEC CICS EXTRACT STATISTICS** or **EXEC CICS COLLECT STATISTICS** command to return statistics for a specified program that is declared as an application entry point, only one statistics record is returned. If the command is issued in or for an application context, and the program was defined as a private resource for the application, the DSECT for private resources is used to format the data, even if the program has currently been promoted to a public program in order to make the application entry point available.

The following new options are added to the **EXTRACT STATISTICS** command to specify an application context:

APPLICATION(*data-value*)

Specifies the application name element of the application context. The application name can be up to 64 characters in length.

Specify the application context to return statistics for a private resource that is part of an application deployed on a platform. Statistics for private resources can only be returned as specific, or resource, statistics for a named resource of the JVMPROGRAM, LIBRARY, PROGRAM, or PROGRAMDEF resource types, which are supported as private resources. You must specify a complete application context, including the platform name, application name, and full application version number. If the private resource that you name on the RESID option is not found in the specified application context, no statistics are returned.

You do not need to specify an application context if the command is issued from a program that is part of the relevant application. By default, CICS returns statistics for a private resource from the application where the command is issued, or statistics for a public resource if no private resource can be found.

APPLMAJORVER(*data-value*)

Specifies the application major version element of the application context, in fullword binary form.

APPLMICROVER(*data-value*)

Specifies the application micro version element of the application context, in fullword binary form.

APPLMINORVER(*data-value*)

Specifies the application minor version element of the application context, in fullword binary form.

PLATFORM(*data-value*)

Specifies the platform name element of the application context. The platform name can be up to 64 characters in length.

INQUIRE ASSOCIATION

New attributes ACAPPLNAME, ACMAJORVER, ACMICROVER, ACMINORVER, ACOPERNAME, and ACPLATNAME return the current application context for the application that is associated with the task:

ACAPPLNAME(*data-area*)

Returns, in a 64-character area, the name of the application that is associated with the task. If no application context is associated with the task, this option is blank.

ACMAJORVER(*data-area*)

Returns, in fullword binary form, the major version number of the application associated with the task. If no application context is associated with the task, this option returns 0.

ACMICROVER(*data-area*)

Returns, in fullword binary form, the micro version number of the application associated with the task. If no application context is associated with the task, this option returns 0.

ACMINORVER(*data-area*)

Returns, in fullword binary form, the minor version number of the application associated with the task. If no application context is associated with the task, this option returns 0.

ACOPERNAME(*data-area*)

Returns, in a 64-character area, the name of the application operation that is associated with the task. If no application context is associated with the task, this option is blank.

ACPLATNAME(*data-area*)

Returns, in a 64-character area, the name of the platform that is associated with the task. If no application context is associated with the task, this option is blank.

INQUIRE BUNDLE and INQUIRE BUNDLEPART

The new AVAILSTATUS option on the **INQUIRE BUNDLE** and **INQUIRE BUNDLEPART** commands returns the availability status for the CICS bundle.

AVAILSTATUS(*cvda*)

Returns the status of the BUNDLE resource that represents the CICS bundle:

AVAILABLE

Callers can access all the resources identified in the CICS bundle as application entry points.

UNAVAILABLE

Callers cannot access any of the resources identified in the CICS bundle as application entry points.

SOMEAVAIL

Some application entry points are available and some are unavailable.

NONE

The bundle does not contain any statements of application entry points.

INQUIRE IPCONN

The new HA option on the **INQUIRE IPCONN** command shows whether the IPCONN definition can be used to connect to a high-availability cluster.

HA(*cvda*)

Returns a CVDA value indicating whether the IPCONN can be used to connect to a high-availability cluster. CVDA values are as follows:

NOTREQUIRED

The IPCONN cannot be used to connect to a high-availability cluster.

REQUIRED

The IPCONN must connect to a region that is part of a high-availability cluster.

The APPLID, IPRESOLVED, and PORT options of the **INQUIRE IPCONN** command, when used with HA IPCONN definitions that are acquired, now return the values for the specific region in the high-availability cluster to which the IPCONN connected.

INQUIRE JVMSERVER

The PROFILEDIR option of the **INQUIRE JVMSERVER** command now displays the JVM profile directory for JVM servers that are packaged in CICS bundles.

PROFILEDIR(*data-area*)

Returns a 240-character data value of the directory on z/OS UNIX that contains the JVM profile for the JVM server. For a JVM server that is defined in a local CICS region, which uses a JVM profile stored in the local CICS

region, the value is the directory specified by the JVMPROFILEDIR system initialization parameter in Reference -> System definition system initialization parameter for the CICS region. For a JVM server that is defined in a CICS bundle, which uses a JVM profile packaged in the CICS bundle, the value is the CICS bundle subdirectory where the JVM profile is stored.

INQUIRE LIBRARY

New options are added to the INQUIRE LIBRARY command to specify the application context for browsing private resources.

APPLICATION(*data-area*)

Specifies the application name element of the application context. The application name can be up to 64 characters in length.

To browse private resources for an application deployed on a platform, use the APPLICATION, APPLMAJORVER, APPLMINORVER, APPLMICROVER, and PLATFORM options with the browse command START to specify the platform, application name, and full version number for the application whose resources you want to browse.

APPLMAJORVER(*data-area*)

Specifies the application major version element of the application context, in fullword binary form.

APPLMINORVER(*data-area*)

Specifies the application minor version element of the application context, in fullword binary form.

APPLMICROVER(*data-area*)

Specifies the application micro version element of the application context, in fullword binary form.

PLATFORM(*data-area*)

Specifies the platform name element of the application context. The platform name can be up to 64 characters in length.

INQUIRE PIPELINE

The **INQUIRE PIPELINE** command now includes a MSGFORMAT parameter for determining the message format processed by a pipeline:

MSGFORMAT(*data-area*)

Returns an 8-byte character string that indicates the message format processed by the PIPELINE.

SOAP11

The pipeline processes the SOAP 1.1 message format.

SOAP12

The pipeline processes the SOAP 1.2 message format, and can also process the SOAP 1.1 message format.

JSON

The pipeline processes the JSON message format.

OTHER

The pipeline processes other message formats, such as customer-specified formats.

INQUIRE PROGRAM

A new option RESIDENCY is added to the **INQUIRE PROGRAM** command.

RESIDENCY(*cvda*) (programs only)

Returns a CVDA value that indicates the program's residency attributes. The CVDA values are as follows:

RESIDENT

The program is permanently resident. It is defined as RESIDENT(YES).

NONRESIDENT

The program has been defined as RESIDENT(NO).

New options are added to the **INQUIRE PROGRAM** command to specify the application context for browsing private resources. For the **INQUIRE PROGRAM** command only, the application context is used to specify a different application for browsing private resources, and also to return information for an inquiry on a public PROGRAM resource that is defined as an application entry point. For other resource types that are supported as private resources, the application context is not used to return information.

APPLICATION(*data-area*)

Specifies or returns the application name element of the application context. The application name can be up to 64 characters in length.

To browse private resources for an application deployed on a platform, use the APPLICATION, APPLMAJORVER, APPLMINORVER, APPLMICROVER, and PLATFORM options with the browse command START, to specify the platform, application name, and full version number for the application whose resources you want to browse.

For an inquiry on a public PROGRAM resource, the APPLICATION, APPLMAJORVER, APPLMINORVER, APPLMICROVER, and PLATFORM options return the name, version number, and platform of the application for which the program is defined as an application entry point. The OPERATION option returns the name of the relevant operation in the application. If the program is not defined as an application entry point, APPLICATION returns 64 blanks.

APPLMAJORVER(*data-area*)

Specifies or returns the application major version element of the application context, in fullword binary form. For an inquiry on a public PROGRAM resource, if the program is not defined as an application entry point, APPLMAJORVER returns a value of -1.

APPLMINORVER(*data-area*)

Specifies or returns the application minor version element of the application context, in fullword binary form. For an inquiry on a public PROGRAM resource, if the program is not defined as an application entry point, APPLMINORVER returns a value of -1.

APPLMICROVER(*data-area*)

Specifies or returns the application micro version element of the application context, in fullword binary form. For an inquiry on a public PROGRAM resource, if the program is not defined as an application entry point, APPLMICROVER returns a value of -1.

PLATFORM(*data-area*)

Specifies or returns the platform name element of the application context. The

platform name can be up to 64 characters in length. For an inquiry on a public PROGRAM resource, if the resource is not defined as an application entry point, PLATFORM returns 64 blanks.

INQUIRE SYSTEM

Three new keywords have been added to the **INQUIRE SYSTEM** command. These are MESSAGECASE, MVSSMFID and MVSSYSNAME.

MESSAGECASE(*cvda*)

Returns a CVDA value that shows how the message domains display mixed case messages, as set by the **MSGCASE** system initialization parameter. CVDA values are as follows:

MIXED

All messages displayed by the CICS message domain or the CICSplex SM message domain remain in mixed case.

UPPER

The message domain displays all mixed case messages in uppercase only.

MVSSMFID(*data-area*)

Returns a 4-byte value indicating the MVS system identification. This field is copied from the SMCASID field of the SMCA MVS control block.

MVSSYSNAME(*data-area*)

Returns an 8-byte value indicating the MVS system name. This field is copied from the CVTSNAME field of the MVS CVT control block.

INQUIRE TCPIP SERVICE

New options are added to the **INQUIRE TCPIP SERVICE** command to support access to high-availability clusters of CICS regions over IP interconnectivity (IPIC) connections.

GENERIC TCPS(*data-area*)

Returns the 8-character generic TCPIP SERVICE name that this specific TCP/IP service is associated with when used as part of the configuration within an IPIC high-availability cluster. This information is only present when both TCP/IP services are opened. It is blank when there is no generic TCPIP SERVICE or when this generic TCPIP SERVICE is closed.

SPECIFIC TCPS(*data-area*)

Returns the 8-character specific TCPIP SERVICE name that this generic TCP/IP service uses when receiving a high-availability IPIC connection request.

When the TCP/IP service is in OPEN or CLOSING status, the value returned by the BACKLOG option of the **INQUIRE TCPIP SERVICE** command is now the actual value for the maximum number of queued requests that the local TCP/IP stack permits for this service, taking into account the setting for the SOMAXCONN parameter in the PROFILE.TCPIP data set for the z/OS Communications Server port. When the TCP/IP service is in CLOSED or OPENING status, the value returned by the BACKLOG option is the value defined in the BACKLOG attribute of the TCPIP SERVICE resource definition.

A new value BUNDLE is added for the INSTALLAGENT option of the **INQUIRE TCPIP SERVICE** command, to show that the TCPIP SERVICE resource was installed by a bundle deployment.

INQUIRE UOWLINK

The new PORT option on the **INQUIRE UOWLINK** command returns the port number of the partner system for IPIC connections.

PORT(*data-area*)

For TYPE value IPIC, returns the TCP/IP port number that the partner system was listening on when the connection was acquired. Port is a number in the range 1 to 65535 and will be zero for other TYPE values.

INQUIRE URIMAP

New options are added to the **INQUIRE URIMAP** command to return the details of the application entry point for the URIMAP resource, and of the resulting availability status of the URIMAP resource.

AVAILSTATUS(*cvda*)

Returns the availability status of the URIMAP resource as an application entry point for an application deployed on a platform.

AVAILABLE

The URIMAP resource is declared as an application entry point, and the application entry point controls its availability and is available, so the URIMAP resource is available to callers.

UNAVAILABLE

The URIMAP resource is declared as an application entry point, but the application entry point that controls its availability is unavailable, so the URIMAP resource is not available to callers.

NONE

The URIMAP resource is available to callers. Either the URIMAP resource is not declared as an application entry point, or it is declared as an application entry point but the application entry point is disabled or does not control the availability of the URIMAP resource.

APPLICATION(*data-value*)

Returns a 64-character area containing the application name of the application for which this URIMAP resource is declared as an application entry point. If the URIMAP resource is not defined as an application entry point, APPLICATION returns blanks.

APPLMAJORVER(*data-value*)

Returns the fullword binary form of the major version number of the application for which this URIMAP resource is declared as an application entry point. If the URIMAP resource is not defined as an application entry point, APPLMAJORVER returns -1.

APPLMINORVER(*data-value*)

Returns the fullword binary form of the minor version number of the application for which this URIMAP resource is declared as an application entry point. If the URIMAP resource is not defined as an application entry point, APPLMINORVER returns -1.

APPLMICROVER(*data-value*)

Returns the fullword binary form of the micro version number of the application for which this URIMAP resource is declared as an application entry point. If the URIMAP resource is not defined as an application entry point, APPLMICROVER returns -1.

OPERATION(*data-value*)

Returns a 64-character area containing the operation name of the application for which this URIMAP resource is declared as an application entry point. If the URIMAP resource is not defined as an application entry point, OPERATION returns blanks.

PLATFORM(*data-value*)

Returns a 64-character area containing the platform name of the application for which this URIMAP resource is declared as an application entry point. If the URIMAP resource is not defined as an application entry point, PLATFORM returns blanks.

INQUIRE WEBSERVICE

The STATE option of the **INQUIRE WEBSERVICE** command returns two new states, **DISABLING** and **DISABLED**, which apply only for web services that are packaged in CICS bundles.

DISABLED

This state is only available for WEBSERVICE resources that are defined in a CICS bundle. The web service has completed quiescing and is not accepting new work.

DISABLING

This state is only available for WEBSERVICE resources that are defined in a CICS bundle. The web service is quiescing. It is not accepting new work, but is allowing currently-executing work to complete. When the web service is no longer in use, the state of the WEBSERVICE resource changes to **DISABLED**.

PERFORM STATISTICS RECORD

Continue to use the existing keywords on the **EXEC CICS PERFORM STATISTICS RECORD** system programming command to write statistics for program, program definition, JVM program, or library resource types to the SMF data set. If a resource is a public resource, the existing DSECT is used to map its data, and if a resource is a private resource, the new DSECT is used to map its data.

Programs that are declared as application entry points are identified by a field in the DSECTs for public and private program definitions (PROGRAMDEF statistics keyword) and JVM programs (JVMPROGRAM keyword). When interval statistics, end-of-day statistics, requested statistics, requested reset statistics, or unsolicited statistics are produced for a program definition or JVM program that is declared as an application entry point, two statistics records are written, one mapped by the DSECT for public resources, and one mapped by the DSECT for private resources. For the program statistics that are produced by the loader domain (PROGRAM keyword), application entry points are not identified, and only one private program statistics record is written.

SET BUNDLE

A new option **AVAILSTATUS** on the **SET BUNDLE** command gives or removes access to application entry points that are declared in the CICS bundle. For a CICS bundle that declares application entry points, you must first enable the bundle, then make it available, to give users access to the resources. For a CICS bundle that does not declare application entry points, you only need to enable the bundle.

AVAILSTATUS(*cvda*)

Changes the status of the BUNDLE resource that represents the CICS bundle:

AVAILABLE

CICS gives callers access to the resources identified in the CICS bundle as application entry points, so that they can access all the resources in the CICS bundle.

UNAVAILABLE

CICS removes access to the resources identified in the CICS bundle as application entry points, so callers cannot access any of the private resources in the CICS bundle.

SET FILE

To change the status of a FILE resource that was defined and installed in a CICS bundle, change the status of the CICS bundle or the application with which it is deployed. When you perform the disable action on a CICS bundle that defines a FILE resource, the action completes when the file is no longer in use and any retained locks have been resolved.

If you are experiencing a problem with disabling a CICS bundle that defines a FILE resource, you may issue the **EXEC CICS SET FILE DISABLED** or **EXEC CICS SET FILE CLOSED** command with the **FORCE** option against the dynamically generated resource, if this action is required. Follow the troubleshooting procedure in Diagnosing application errors to diagnose the problem and take suitable action.

SET JVMSERVER

To disable a JVMSERVER resource that is defined in a CICS bundle, you must first disable the CICS bundle or the application with which it is deployed. If the disable process does not complete, because the resource is still in use, you can now use the **SET JVMSERVER PURGE**, **FORCEPURGE**, or **KILL** command on the dynamically generated resource in the CICS region. If you attempt to issue the command before performing the disable action on the CICS bundle, CICS issues error message DFHSJ1203.

SET TCPIPSERVICE

To disable a TCPIPSERVICE resource that is defined in a CICS bundle, you must first disable the CICS bundle or the application with which it is deployed. If the disable process does not complete, because the resource is still in use, you can now use the **SET TCPIPSERVICE IMMCLOSE** command on the dynamically generated resource in the CICS region. If you attempt to issue the command before performing the disable action on the CICS bundle, CICS issues error message DFHSO0140.

New SPI commands

CICS Transaction Server for z/OS, Version 5 Release 2 includes some new SPI commands that you can use to control new system resources or to work in new ways with existing resources.

No new system programming commands were added in CICS Transaction Server for z/OS, Version 5 Release 2.

SPI commands that have been made threadsafe

These system programming interface commands were not threadsafe when they were first introduced in CICS, but they have now been made threadsafe.

DISCARD PROGRAM
DISCARD TRANSACTION
EXTRACT STATISTICS
INQUIRE DISPATCHER
INQUIRE MONITOR
INQUIRE MVSTCB
INQUIRE PROGRAM
INQUIRE STATISTICS
INQUIRE SYSTEM
INQUIRE TRANSACTION
SET DISPATCHER
SET MONITOR
SET PROGRAM
SET STATISTICS
SET SYSTEM
SET TRANSACTION

Chapter 7. Changes to CEMT

The commands available in the CEMT transaction have been modified to reflect changes to resource definitions and new functions.

The CICS transactions accept as few characters of a keyword as needed to identify the keyword uniquely in the request. Minimum abbreviations might change between CICS releases because of the introduction of new commands. If you use automated processes or programs to issue commands for CICS transactions, and you use abbreviations for the keywords, check for any changes to these abbreviations in the new release. In the syntax displays on your screen, the minimum permitted abbreviation is shown in uppercase characters, and the remainder is shown in lowercase.

Obsolete CEMT commands and options

These CEMT commands and options represent functions that are no longer available, so are no longer displayed in the CEMT transaction.

CEMT INQUIRE TSMODEL, CEMT INQUIRE TSQUEUE, and CEMT INQUIRE TSQNAME

The EXPIRYINT option is obsolete. EXPIRYINT was used to set the expiry interval for temporary storage queues in hours. It has been superseded by the EXPIRYINTMIN option, which sets the expiry interval for temporary storage queues in minutes.

CEMT INQUIRE DISPATCHER

The ACTJVMTCBS option and the MAXJVMTCBS option are obsolete. ACTJVMTCBS was used to inquire on the number of J8 and J9 mode TCBs currently allocated to user tasks. MAXJVMTCBS was used to inquire on the maximum number of J8 and J9 mode TCBs allowed in the JVM pool.

CEMT PERFORM STATISTICS

The BEAN, CORBASERVER, JVMPOOL, JVMPROFILE, and REQUESTMODEL options are obsolete. These options were used to request statistics for enterprise beans, CorbaServer entries, pooled JVMs and their profiles, and request models, which CICS no longer supports.

CEMT SET DISPATCHER

The MAXJVMTCBS option is obsolete. MAXJVMTCBS was used to change the maximum number of J8 and J9 mode open TCBs allowed in the JVM pool, which no longer exists.

Changed CEMT commands

These CEMT commands have new options or new values for options.

Inquiring on private resources for applications

A resource that is defined as part of an application installed on a platform is private to that version of that application. For supported resource types, a resource is private if the resource is defined in a CICS bundle that is packaged and installed as part of an application, either as part of the application bundle, or as part of the application binding bundle. A resource that is defined by any other method is publicly available for all tasks, and is known as a public resource.

The following CICS resources are supported as private resources for applications:

- LIBRARY resources, which represent one or more data sets, known as dynamic program LIBRARY concatenations, from which program load modules can be loaded.
- POLICY resources, which represent one or more rules that manage the behavior of user tasks in CICS regions.
- PROGRAM resources, which represent an application program. A program that is auto-installed by a task for an application that is deployed on a platform is also private to that version of the application.

Private LIBRARY and PROGRAM resources cannot be viewed using the **CEMT INQUIRE LIBRARY** and **CEMT INQUIRE PROGRAM** commands. To inquire on or browse these resources, use the CICS Explorer®, or the **EXEC CICS INQUIRE LIBRARY** and **EXEC CICS INQUIRE PROGRAM** CICS system programming commands.

LIBRARY concatenations and programs that are defined as a dependency or import for an application bundle or an application binding bundle, and LIBRARY concatenations and programs that are defined to CICS using any other method, remain publicly available for all tasks. These LIBRARY concatenations and programs can be viewed using the CEMT commands.

CEMT INQUIRE BUNDLE

The new AVAILSTATUS option for the **CEMT INQUIRE BUNDLE** command returns the availability status for the CICS bundle.

AVAILSTATUS(*value*)

Displays the availability status of the bundle. The possible values are as follows:

AVAILABLE

Callers can access all the resources identified in the CICS bundle as application entry points.

UNAVAILABLE

Callers cannot access any of the resources identified in the CICS bundle as application entry points.

SOMEAVAIL

Some application entry points are available and some are unavailable.

NOTAPPLIC

The bundle does not contain any statements of application entry points.

CEMT INQUIRE JVMSERVER

The PROFILEDIR option for the **CEMT INQUIRE JVMSERVER** command now displays the JVM profile directory for JVM servers that are packaged in CICS bundles.

PROFILEDIR(*directory*)

Displays the directory on z/OS UNIX that contains the JVM profile for the JVM server. For a JVM server that is defined in a local CICS region, which uses a JVM profile stored in the local CICS region, this is the directory specified by the JVMPROFILEDIR system initialization parameter for the CICS region. For a JVM server that is defined in a CICS bundle, which uses a JVM profile packaged in the CICS bundle, this is the CICS bundle subdirectory where the JVM profile is stored.

CEMT INQUIRE PROGRAM

The **CEMT INQUIRE PROGRAM** command has a new option **RESIDENCY**.

RESIDENCY(*value*)

Displays the program's residency attributes:

RESIDENT

The program is permanently resident. It is defined as **RESIDENT**(YES).

NONRESIDENT

The program is defined as **RESIDENT**(NO).

CEMT INQUIRE URIMAP

New options are added to the **CEMT INQUIRE URIMAP** command to return the details of the application entry point for the URIMAP resource, and of the resulting availability status of the URIMAP resource.

AVAILSTATUS(*value*)

Displays the availability status of the URIMAP resource as an application entry point for an application deployed on a platform.

AVAILABLE

The URIMAP resource is declared as an application entry point, and the application entry point controls its availability and is available, so the URIMAP resource is available to callers.

UNAVAILABLE

The URIMAP resource is declared as an application entry point, but the application entry point that controls its availability is unavailable, so the URIMAP resource is not available to callers.

NOTAPPLIC

The URIMAP resource is available to callers. Either the URIMAP resource is not declared as an application entry point, or it is declared as an application entry point but the application entry point is disabled or does not control the availability of the URIMAP resource.

APPLICATION(*data-value*)

Displays the application name of the application for which this URIMAP resource is declared as an application entry point. If the URIMAP resource is not declared as an application entry point, **APPLICATION** displays blanks.

APPLMAJORVER(*data-value*)

Displays the major version number of the application. If the URIMAP resource is declared as an application entry point, the major version number of this application is returned. If the URIMAP resource is not declared as an application entry point, **APPLMAJORVER** returns -1.

APPLMINORVER(*data-value*)

Displays the minor version number of the application. If the URIMAP resource is declared as an application entry point, the minor version number of this application is returned. If the URIMAP resource is not declared as an application entry point, **APPLMINORVER** returns -1.

APPLMICROVER(*data-value*)

Displays the micro version number of the application. If the URIMAP resource is declared as an application entry point, the micro version number of this application is returned. If the URIMAP resource is not declared as an application entry point, **APPLMICROVER** returns -1.

OPERATION(*data-value*)

Displays the operation name of the application for which this URIMAP resource is declared as an application entry point. If the URIMAP resource is not declared as an application entry point, OPERATION displays blanks.

PLATFORM(*data-value*)

Displays the platform name of the application for which this URIMAP resource is declared as an application entry point. If the URIMAP resource is not declared as an application entry point, PLATFORM displays blanks.

CEMT INQUIRE WEBSERVICE

The STATE option of the **CEMT INQUIRE WEBSERVICE** command displays two new states, **DISABLING** and **DISABLED**, which apply only for web services that are packaged in CICS bundles.

DISABLED

This state is only available for WEBSERVICE resources that are defined in a CICS bundle. The web service has completed quiescing and is not accepting new work.

DISABLING

This state is only available for WEBSERVICE resources that are defined in a CICS bundle. The web service is quiescing. It is not accepting new work, but is allowing currently-executing work to complete. When the web service is no longer in use, the state of the WEBSERVICE resource changes to **DISABLED**.

CEMT PERFORM DUMP and CEMT PERFORM SNAP

A new DUMPCODE parameter has been added to the **CEMT PERFORM DUMP** and **CEMT PERFORM SNAP** commands to specify a dump code for the dump request.

DUMPCODE (*data-value*)

Specifies a maximum 8-character dump code for this dump request. The value is a user defined code which can be any character string that does not contain leading or imbedded blank characters. If a dump code is not specified, CICS uses a default dump code of MT0001.

CEMT SET BUNDLE

New **AVAILABLE** and **UNAVAILABLE** options on the **SET BUNDLE** command give or remove access to application entry points that are declared in the CICS bundle. For a CICS bundle that declares application entry points, you must first enable the bundle, then make it available, to give users access to the resources. For a CICS bundle that does not declare application entry points, you only need to enable the bundle.

AVAILABLE

Make one or more BUNDLE resources available. CICS gives callers access to the resources identified in the CICS bundle as application entry points.

UNAVAILABLE

Make one or more BUNDLE resources unavailable. CICS removes access to the resources identified in the CICS bundle as application entry points, so callers cannot access any of the private resources in the CICS bundle.

CEMT SET FILE

To disable a file that is defined in a CICS bundle, you must first disable the CICS bundle or the application with which it is deployed. If you are experiencing a problem with disabling a CICS bundle that defines a FILE resource, you can now issue the **CEMT SET FILE** command with the **FORCECLOSE** option against the dynamically generated resource, if this action is required. Follow the troubleshooting procedure in Diagnosing application errors to diagnose the problem and take suitable action.

CEMT SET JVMSERVER

To disable a JVMSERVER resource that is defined in a CICS bundle, you must first disable the CICS bundle or the application with which it is deployed. If the disable process does not complete, because the resource is still in use, you can now use the **CEMT SET JVMSERVER PURGE**, **FORCEPURGE**, or **KILL** command on the dynamically generated resource in the CICS region.

CEMT SET TCPIPService

To disable a TCPIPService resource that is defined in a CICS bundle, you must first disable the CICS bundle or the application with which it is deployed. If the disable process does not complete, because the resource is still in use, you can now use the **CEMT SET TCPIPService IMMCLOSE** command on the dynamically generated resource in the CICS region.

New CEMT commands

These CEMT commands support new CICS functions.

For detailed information on all the new and changed CEMT transactions and options, see the *CICS Supplied Transactions*.

No new CEMT commands were added in CICS Transaction Server for z/OS, Version 5 Release 2.

Chapter 8. Changes to the CICS management client interface (CMCI)

The CICS management client interface (CMCI) supports additional CICSplex SM and CICS resources, and you can query the resources using external resource names.

No new CICSplex SM resources were added in CICS Transaction Server for z/OS, Version 5 Release 2.

Chapter 9. Changes to the CICS-supplied transactions

Some CICS-supplied transactions are new, or have changed to support new functions.

The CICS transactions accept as few characters of a keyword as needed to identify the keyword uniquely in the request. Minimum abbreviations might change between CICS releases because of the introduction of new commands. If you use automated processes or programs to issue commands for CICS transactions, and you use abbreviations for the keywords, check for any changes to these abbreviations in the new release. In the syntax displays on your screen, the minimum permitted abbreviation is shown in uppercase characters, and the remainder is shown in lowercase.

Changes to CSFE

The CSFE terminal and system test transaction can now be used to check on the status of a previous debug request.

CSFE now allows the status of DEBUG parameters to be queried, so for example to report if the global trap is active, or whether storage violation checking is active.

This transaction is mainly intended to be used by system programmers and IBM field engineers.

New transaction CFCR

CFCR was introduced in CICS Transaction Server for z/OS, Version 5 Release 2. CICS uses this transaction to disable files that are defined in CICS bundles.

CFCR, and the program DFHFERN that it runs, are defined in the new CICS-supplied resource definition group DFHFERN. When you perform the disable action on a CICS bundle that contains a definition for a FILE resource, CICS attaches CFCR to manage the disable process for the file.

CFCR is a RACF® Category 1 transaction.

Chapter 10. Changes to global user exits and task-related user exits

CICS Transaction Server for z/OS, Version 5 Release 2 has changes to some existing global user exit programs and task-related user exit programs. Check your existing global user exit programs against the changes summarized here.

Reassembling global user exit programs

The CICS global user exit programming interface is product-sensitive, and depends on the facilities that are set up in your CICS system. It is advisable to reassemble global user exit programs for each CICS release, because changes to CICS internals might affect structures used by the CICS global user exit programming interface, even if there are no changes to the externals of the programming interface.

For other areas of the XPI, check the changes to externals that are summarized in this section, and modify your global user exit programs to allow for changes to relevant parameters. After you complete your program changes, reassemble the affected global user exit programs against the CICS Transaction Server for z/OS, Version 5 Release 2 libraries.

A global user exit or task-related user exit might be assembled using CICS libraries from one CICS release and make an XPI call on a system that runs a different CICS release. In this situation, whether or not control is successfully transferred from the exit to the correct CICS module to handle that XPI call depends on the combination of CICS releases, and whether the XPI call is a release-sensitive call. For the user exit to succeed, you must also check other factors, for example whether XPI parameters have changed between releases.

If a user exit fails, an error message is issued and the transaction that called the exit might abend.

The following table summarizes the effect of different CICS releases on user exits. Release-sensitive XPI calls are not available in releases before CICS TS 4.1.

Table 1. User exits with different CICS releases

CICS release of the libraries used to assemble the XPI call	Release-sensitive XPI call?	CICS system that the XPI call is made on	Result
CICS TS 5.2, CICS TS 5.1, CICS TS 4.2, or CICS TS 4.1	Yes	All currently supported CICS releases	Control transfers to the correct CICS module for the XPI call
CICS TS 5.2, CICS TS 5.1 or CICS TS 4.2	No	CICS TS 5.2, CICS TS 5.1 or CICS TS 4.2	Control transfers to the correct CICS module for the XPI call
CICS TS 5.2, CICS TS 5.1 or CICS TS 4.2	No	CICS TS 4.1, CICS TS 3.2, and CICS TS 3.1	Unpredictable result

Table 1. User exits with different CICS releases (continued)

CICS release of the libraries used to assemble the XPI call	Release-sensitive XPI call?	CICS system that the XPI call is made on	Result
CICS TS 4.1	No	CICS TS 5.2, CICS TS 5.1, CICS TS 4.2, or CICS TS 4.1	Control transfers to the correct CICS module for the XPI call
CICS TS 4.1	No	CICS TS 3.2 and CICS TS 3.1	Unpredictable result
CICS TS 3.2 or CICS TS 3.1	No	CICS TS 5.2, CICS TS 5.1, CICS TS 4.2, or CICS TS 4.1	Back level XPI call detected, and user exit fails
CICS TS 3.2	No	CICS TS 3.2	Control transfers to the correct CICS module for the XPI call
CICS TS 3.2	No	CICS TS 3.1	Unpredictable result
CICS TS 3.1	No	CICS TS 3.2 or CICS TS 3.1	Control transfers to the correct CICS module for the XPI call

Changes to the DFHUEPAR standard parameter list

DFHUEPAR is a standard parameter list of TCB 2-character codes and symbolic values addressed by the global user exit task indicator field, UEPGIND. TCB modes are represented in DFHUEPAR as both a 2-character code and a symbolic value.

No changes were made to the DFHUEPAR standard parameter list in CICS Transaction Server for z/OS, Version 5 Release 2.

Changes to global user exits

Some existing global user exits have new parameters, new values or return codes, or changes to how the exits are used.

Resource management installation and discard exit: XRSINDI

The new **UEPAPCTXT** and **UEPAPPTK** parameters of the XRSINDI global user exit now supply the application context information for private resources for applications that are deployed on platforms.

UEPAPCTXT

For private resources for applications that are deployed on platforms, this parameter contains the address of a variable-length list, which corresponds to the list in UEPIDNAM, containing the application context information for the resource. The information is listed in the following order:

1. The platform name, padded with spaces to 64 characters.
2. The application name, padded with spaces to 64 characters.
3. The major version number for the application, which is a fullword binary value.
4. The minor version number for the application, which is a fullword binary value.
5. The micro version number for the application, which is a fullword binary value.

CICS supplies a DSECT named **DFHUEACD** which maps this information. For more information about **DFHUEACD**, see UEACD - User exit application context in Data Areas.

UEPAPPTK

Address of a variable-length list, containing an 8-character token representing the application instance to which this resource belongs. For public resources, this address is zero.

New global user exit points

New global user exit points help you customize new or existing CICS functions.

No new global user exit points were added in this release.

Changes to task-related user exits

Task-related user exit programs may be invoked and used in new ways in new CICS releases.

In CICS Transaction Server for z/OS, Version 5 Release 2 there were no changes to task-related user exits.

Chapter 11. Changes to the exit programming interface

CICS Transaction Server for z/OS, Version 5 Release 2 has changes to some existing programming interface. Check your existing global user exit programs against the changes summarized here.

Reassembling global user exit programs

The CICS global user exit programming interface is product-sensitive, and depends on the facilities that are set up in your CICS system. It is advisable to reassemble global user exit programs for each CICS release, because changes to CICS internals might affect structures used by the CICS global user exit programming interface, even if there are no changes to the externals of the programming interface.

For other areas of the XPI, check the changes to externals that are summarized in this section, and modify your global user exit programs to allow for changes to relevant parameters. After you complete your program changes, reassemble the affected global user exit programs against the CICS Transaction Server for z/OS, Version 5 Release 2 libraries.

A global user exit or task-related user exit might be assembled using CICS libraries from one CICS release and make an XPI call on a system that runs a different CICS release. In this situation, whether or not control is successfully transferred from the exit to the correct CICS module to handle that XPI call depends on the combination of CICS releases, and whether the XPI call is a release-sensitive call. For the user exit to succeed, you must also check other factors, for example whether XPI parameters have changed between releases.

If a user exit fails, an error message is issued and the transaction that called the exit might abend.

The following table summarizes the effect of different CICS releases on user exits. Release-sensitive XPI calls are not available in releases before CICS TS 4.1.

Table 2. User exits with different CICS releases

CICS release of the libraries used to assemble the XPI call	Release-sensitive XPI call?	CICS system that the XPI call is made on	Result
CICS TS 5.2, CICS TS 5.1, CICS TS 4.2, or CICS TS 4.1	Yes	All currently supported CICS releases	Control transfers to the correct CICS module for the XPI call
CICS TS 5.2, CICS TS 5.1 or CICS TS 4.2	No	CICS TS 5.2, CICS TS 5.1 or CICS TS 4.2	Control transfers to the correct CICS module for the XPI call
CICS TS 5.2, CICS TS 5.1 or CICS TS 4.2	No	CICS TS 4.1, CICS TS 3.2, and CICS TS 3.1	Unpredictable result

Table 2. User exits with different CICS releases (continued)

CICS release of the libraries used to assemble the XPI call	Release-sensitive XPI call?	CICS system that the XPI call is made on	Result
CICS TS 4.1	No	CICS TS 5.2, CICS TS 5.1, CICS TS 4.2, or CICS TS 4.1	Control transfers to the correct CICS module for the XPI call
CICS TS 4.1	No	CICS TS 3.2 and CICS TS 3.1	Unpredictable result
CICS TS 3.2 or CICS TS 3.1	No	CICS TS 5.2, CICS TS 5.1, CICS TS 4.2, or CICS TS 4.1	Back level XPI call detected, and user exit fails
CICS TS 3.2	No	CICS TS 3.2	Control transfers to the correct CICS module for the XPI call
CICS TS 3.2	No	CICS TS 3.1	Unpredictable result
CICS TS 3.1	No	CICS TS 3.2 or CICS TS 3.1	Control transfers to the correct CICS module for the XPI call

Changes to the exit programming interface (XPI)

Changes to the exit programming interface (XPI) mean that you might need to change global user exit programs that contain XPI calls. Check whether your global user exit programs are affected by these changes to the XPI, and modify your programs accordingly.

Changed INQUIRE_APP_CONTEXT call

The INQ_APP_CONTEXT call now returns the current application context for the most recent application that has been set onto the task.

For details, see The INQUIRE_APP_CONTEXT call in Reference -> System programming reference and Application context in Product overview.

Changed INQUIRE_PROGRAM and START_BROWSE_PROGRAM calls - application context

You can use new options on the INQUIRE_PROGRAM and START_BROWSE_PROGRAM calls to inquire on private programs for applications deployed on platforms. To inquire on private programs for applications deployed on platforms, you must specify the AC_APPLICATION_NAME, AC_MAJOR_VERSION, AC_MINOR_VERSION, AC_MICRO_VERSION, and AC_PLATFORM_NAME fields to provide a complete application context. The SHOW_PROGRAMS option specifies whether to search for private programs only, or both private and public programs.

For details, see The INQUIRE_PROGRAM call in Reference -> System programming reference.

New exit programming interface (XPI) calls

CICS provides XPI calls that you can use in exit programs to retrieve information about functions in CICS.

In CICS Transaction Server for z/OS, Version 5 Release 2 there were no changes to XPI calls.

Chapter 12. Changes to user-replaceable programs

Reassemble all user-replaceable programs, checking whether any changes to the user-replaceable program interface affect your own customized programs.

For each CICS release, you must reassemble all user-replaceable programs, whether or not you make any changes to them. Before reassembling the programs, check whether these changes to the user-replaceable program interface affect your own customized programs, and make any necessary changes.

For example, there might be changes to the parameters passed to the programs or there might be new actions that the programs need to take. To help you to identify any code changes that are required, compare your customized programs with the sample code in the user-replaceable sample programs provided with this CICS release.

See Customizing with user-replaceable programs in the *CICS Customization Guide* for programming information about user-replaceable programs.

Obsolete user-replaceable programs

These user-replaceable programs are no longer used in CICS Transaction Server for z/OS, Version 5 Release 2.

No user-replaceable programs were made obsolete in CICS Transaction Server for z/OS, Version 5 Release 2.

Changed user-replaceable programs

Check whether the changes listed for this release to the user-replaceable program interface affect your own customized programs, and make any necessary changes. For example, the parameters passed to the programs might be changed, or the programs might need to take new actions. To help you to identify any code changes that are required, compare your customized programs with the sample code in the user-replaceable sample programs provided with this CICS release.

DFHDSRP, distributed routing program: DFHDYPDS copybook

There are changes to the copybook DFHDYPDS that defines the communication area for the CICS-supplied sample distributed routing program DFHDSRP.

The following changes were introduced in CICS TS 5.2:

- The following DFHDYPDS tokens are new:

DYRCLOUD
Cloud Routing Data.

DYRPLATFORM
Platform name.

DYRAPPLICATION
Application name.

DYRAPPLVER

Application version.

DYRAPPLMAJOR

Application major version.

DYRAPPLMINOR

Application minor version.

DYRAPPLMICRO

Application micro version.

DYROPERATION

Operation name.

- The DYRVER token is incremented by 1 to indicate that this module is changed for this CICS TS release.

If you use your own routing program, you might have to make adjustments for these changes. Because the length of DFHDYPDS has changed, you must recompile your user-written dynamic routing and distributed routing programs if they check the length of DFHDYPDS as the CICS-supplied samples do.

DFHPGADX, program autoinstall program

In CICS TS 5.2, the definitions for the CICS-supplied default autoinstall program, in the CICS-supplied group DFHPGAIP, changed to specify CONCURRENCY(THREADSAFE) to avoid TCB switching during program autoinstall. The resource definitions for the following programs now specify CONCURRENCY(THREADSAFE):

- DFHPGADX, Assembler program
- DFHPGAHX, C program
- DFHPGALX, PL/I program
- DFHPGAOX, COBOL program

If you are using the CICS-supplied default program for program autoinstall, examine any code added to the exit to ensure it is threadsafe. If the code is not threadsafe, you must either make changes to make it threadsafe, or change the resource definition to specify CONCURRENCY(QUASIRENT).

For more information about threadsafe programming techniques, see Threadsafe programs in Developing applications.

EYU9WRAM, dynamic routing program: EYURWCOM communication area

EYURWCOM is the communication area that is used by the dynamic routing user-replaceable module EYU9WRAM.

The following EYURWCOM tokens were added in CICS TS 5.2:

WCOM_APPL_CONTEXT

Application context.

WCOM_PLATFORM

Requesting platform name.

WCOM_APPLICATION

Requesting application name.

WCOM_APPLVER

Application version.

WCOM_APPLMAJORVER

Application major version.

WCOM_APPLMINORVER

Application minor version.

WCOM_APPLMICROVER

Application micro version.

WCOM_OPERATION

Requesting operation name.

The following EYURWCOM tokens were changed in CICS TS 5.2:

- **WCOM_FILL3** has a new value of **WCOM_VERSION**. In CICS TS 5.2 it is initialized with the character value 01.

If you have customized EYU9WRAM, you might have to make adjustments for these changes.

EYU9XLOP, dynamic routing program: EYURWTRA communication area

EYURWTRA is the communication area for the dynamic routing program EYU9XLOP.

The following EYURWTRA tokens were added in CICS TS 5.2:

WTRA_APPL_CONTEXT

Application context.

WTRA_PLATFORM

Requesting platform name.

WTRA_APPLICATION

Requesting application name.

WTRA_APPLVER

Application version.

WTRA_APPLMAJORVER

Application major version.

WTRA_APPLMINORVER

Application minor version.

WTRA_APPLMICROVER

Application micro version.

WTRA_OPERATION

Requesting operation name.

The following EYURWTRA tokens are changed in CICS TS 5.2:

- **WTRA_FILL1** has a new value of **WTRA_VERSION**.

Note: Existing applications that use this field should have the field initialized to nulls. In CICS TS 5.2 only new fields in the WTRA COMMAREA that are commensurate with the version number are extracted and passed forwards. The

version is in character format, and the version number for the Application Context additions is 01. A new declaration is added to the EYURWTRA member for Version 1:

```
DCL WTRA_VERSION_01 CHAR(2) CONSTANT('01');      /* EYURWTRA Version 1
*/
```

If you want to pass the application contexts through to your own WRAM program, you must initialize the WTRA_APPL_CONTEXT fields with the appropriate values, and must also set:

```
WTRA_VERSION = WTRA_VERSION_01;
```

If you have customized EYU9XLOP, you might have to make adjustments for these changes.

New user-replaceable programs

CICS Transaction Server for z/OS, Version 5 Release 2 includes user-replaceable programs to support new CICS functions.

No new user-replaceable programs were added in CICS Transaction Server for z/OS, Version 5 Release 2.

Chapter 13. Changes to CICS utilities

Changes to CICS utilities in CICS Transaction Server for z/OS, Version 5 Release 2 relate to new, changed, or obsolete CICS functions. The existing utility programs DFHCSDUP, DFHSTUP, and DFH0STAT support new resources. The trace formatting utility program DFHTUxxx and IPCS dump exit routine DFHPDxxx support new resources and are renamed for the release.

DFH0STAT, sample statistics utility program

DFH0STAT, the sample statistics utility program, produces additional statistics reports for any new resource types that are added in each CICS release. Statistics reports relating to any obsolete resource types are no longer produced.

In CICS TS 5.2, no new statistics reports were added.

DFH0STAT does not report any private resources for applications deployed on platforms, and it does not identify programs that are declared as application entry points.

DFHCSDUP, CSD utility program

The CSD utility program supports all the new and changed resource types and attributes. See Chapter 5, “Changes to resource definitions,” on page 15 for details of all the changes to CSD resource definitions that are supported by DFHCSDUP.

If you are sharing the CSD with earlier releases of CICS and want to alter definitions that are used only on earlier releases, you must use the latest DFHCSDUP, even if some attributes are obsolete in the latest releases of CICS. To use the latest DFHCSDUP to update obsolete options on resource definitions, specify the COMPAT option in the **PARM** string to indicate that you want DFHCSDUP to operate in compatibility mode.

DFHPD690, IPCS dump exit routine

The dump formatting utility program is renamed to DFHPD690. When formatting a dump data set always ensure that you use the dump formatting program with the same level number for the release of CICS TS that created the dump data set.

The dump exit routine for formatting CICS system dumps formats the control blocks for the new domains. To select or ignore dump data for any domains, specify the dump component keywords for those domains. The dump component keywords for use with the CICS IPCS dump exit routine are the same as the CETR trace component codes.

DFHSTUP, statistics formatting utility program

The statistics formatting utility program formats additional statistics reports for new and updated resource types. Statistics reports relating to obsolete resource types are no longer produced. See Chapter 15, “Changes to statistics,” on page 59 for information about changes to resource types and new and obsolete keywords on the SELECT TYPE and IGNORE TYPE parameters.

DFHSTUP reports private resources for applications deployed on platforms, and identifies programs that are declared as application entry points.

DFHTU690, trace formatting utility program

The trace formatting utility program is renamed to DFHTU690. When formatting a dump data set always ensure that you use the dump formatting program with the same level number for the release of CICS TS that created the dump data set.

The program formats trace entries written by the new domains and functions. The new identifiers that you can specify to DFHTU690 on the **TYPETR** parameter for these functional areas are the same as the CETR trace component codes.

Chapter 14. Changes to monitoring

Changes to CICS monitoring data might affect user-written and vendor-written utilities that analyze and print CICS SMF 110 monitoring records.

Check your utility programs that process CICS SMF records to ensure that they can still process SMF 110 records correctly. If you have utility programs provided by independent software vendors, you must ensure that they can handle the SMF 110 records correctly. You can identify SMF 110 records from different releases by using the record-version field in the SMF product section.

- The length of a standard performance class monitoring record, as output to SMF, has increased to 3260 bytes. The length does not allow for any user data that you add, or any system-defined data fields that you exclude, by using a monitoring control table (MCT).
- The offsets have changed for a number of the default CICS dictionary entries in the dictionary data sections of CICS monitoring SMF 110 records.

Obsolete monitoring data fields

Some obsolete data fields are no longer available in the CICS monitoring facility. If you have any of these fields specified in a DFHMCT TYPE=RECORD macro, you must remove them.

No performance class data fields were made obsolete in CICS Transaction Server for z/OS, Version 5 Release 2.

Changed monitoring data fields

Existing data fields can change from release to release in the performance class data, identity class data, transaction resource class data, and exception class data produced by CICS monitoring.

No monitoring data fields were changed in CICS Transaction Server for z/OS, Version 5 Release 2.

New monitoring data fields

New data fields are added in the exception class data, identity class data, performance class data, and transaction resource class data produced by CICS monitoring.

No monitoring data fields were added in CICS Transaction Server for z/OS, Version 5 Release 2.

Monitoring sample program DFH\$MOLS: support for data for earlier CICS releases

The CICS Transaction Server for z/OS, Version 5 Release 2 release of DFH\$MOLS processes monitoring data for earlier supported CICS releases, but the UNLOAD control statement has additional restrictions.

In CICS Transaction Server for z/OS, Version 5 Release 2, DFH\$MOLS can process SMF 110 monitoring data records for the following supported releases:

- CICS Transaction Server for z/OS, Version 5 Release 2
- CICS Transaction Server for z/OS, Version 5 Release 1
- CICS Transaction Server for z/OS, Version 4 Release 2
- CICS Transaction Server for z/OS, Version 4 Release 1
- CICS Transaction Server for z/OS, Version 3 Release 2
- CICS Transaction Server for z/OS, Version 3 Release 1

However, the UNLOAD control statement (which unloads performance class monitoring data into a fixed length record format) can be used only with monitoring data for CICS Transaction Server for z/OS, Version 3 Release 2 onwards. Any version or release of DFH\$MOLS cannot process monitoring data for a version or release *later* than itself, so you must always use the DFH\$MOLS from the highest version or release available to you.

Chapter 15. Changes to statistics

CICS statistics records contain changes because of new domains or because of enhancements to CICS. Statistics types are added or removed and some statistics types have new or changed fields. You must recompile application programs using the changed DSECTs.

CEMT and EXEC CICS statistics commands

You can retrieve all the new statistics described in this section using the **EXEC CICS EXTRACT STATISTICS** command, the **EXEC CICS PERFORM STATISTICS RECORD** command, and the **CEMT PERFORM STATISTICS** command.

The options on the **EXEC CICS EXTRACT STATISTICS** command, the **EXEC CICS PERFORM STATISTICS RECORD** command, and the **CEMT PERFORM STATISTICS** command for the obsolete resource types described in this section are no longer valid. For details of what happens if you use the obsolete options, see the command documentation.

The list of resources supported by the **EXEC CICS COLLECT STATISTICS** command is now closed. All new resources introduced from CICS Transaction Server for z/OS, Version 3 Release 1 onwards are supported by the **EXEC CICS EXTRACT STATISTICS** command, which operates in the same way.

Obsolete statistics types

CICS no longer provides statistics for these obsolete resource types.

No statistics types were made obsolete in CICS Transaction Server for z/OS, Version 5 Release 2.

Changed statistics types

Changes have been made to the statistics fields for these CICS statistics types. The old DSECTs are not compatible with the new DSECTs, and you must recompile application programs using the changed DSECTs.

Statistics for private resources and application entry points

CICS now produces different SMF statistics records for private resources for applications that are deployed on platforms. A statistics record for a private resource has information about the application for which the resource was defined. The existing DSECTs for program and library resources, which are used to map the data for public resources, have corresponding new DSECTs that are used to map the data for private resources.

Table 3. DSECTs for public and private resources

Resource type	Statistics command keyword	Existing DSECT for public resources	New DSECT for private resources
LIBRARY resource statistics	LIBRARY	DFHLDBDS (STID value 31)	DFHLDYDS (STID value 32)

Table 3. DSECTs for public and private resources (continued)

Resource type	Statistics command keyword	Existing DSECT for public resources	New DSECT for private resources
Program resource statistics	PROGRAM	DFHLDRDS (STID value 25)	DFHLDPPDS (STID value 36)
PROGRAM definition resource statistics	PROGRAMDEF	DFHPGDDS (STID value 120)	DFHPGEDS (STID value 147)
JVM program resource statistics	JVMPROGRAM	DFHPGRDS (STID value 119)	DFHPGPDS (STID value 146)

When you use the **EXEC CICS PERFORM STATISTICS RECORD** command to write resource statistics, use the same resource type keyword whether the resource is public or private. If a resource is a public resource, the public DSECT is used to map its data, and if a resource is a private resource, the private DSECT is used to map its data.

When you use the **EXEC CICS EXTRACT STATISTICS** or **EXEC CICS COLLECT STATISTICS** command to request resource statistics for a specific resource of a resource type that is supported as a private resource, the command operates according to the context in which the task is running.

- If the command is issued from a public program, statistics are returned for the named public resource.
- If the command is issued from a program that is part of an application deployed on a platform, so is running with an application context, the private resources for the application are searched first for the named resource. If a private resource is not found, statistics are returned for the named public resource.
- For the **EXEC CICS EXTRACT STATISTICS** command only, you can specify a different application context to be searched for private resources. When you request statistics for a different application, if a private resource is not found for that application, no statistics are returned.

Programs that are declared as application entry points are identified by a field in the DSECTs for public and private program definitions (PROGRAMDEF statistics keyword) and JVM programs (JVMPROGRAM keyword). When interval statistics, end-of-day statistics, requested statistics, requested reset statistics, or unsolicited statistics are produced for a program definition or JVM program that is declared as an application entry point, two statistics records are written, one mapped by the DSECT for public resources, and one mapped by the DSECT for private resources. For the program statistics that are produced by the loader domain (PROGRAM keyword), application entry points are not identified, and only one private program statistics record is written.

When you use the **EXEC CICS EXTRACT STATISTICS** or **EXEC CICS COLLECT STATISTICS** command to return statistics for a specified program that is declared as an application entry point, only one statistics record is returned. If the command is issued in or for an application context, and the program was defined as a private resource for the application, the DSECT for private resources is used to format the data, even if the program has currently been promoted to a public program in order to make the application entry point available.

The statistics formatting utility program DFHSTUP produces separate reports for private resources. DFHSTUP lists programs that are defined as application entry points twice, in both the report for public program definitions or JVM programs, and the report for private program definitions or JVM programs. The sample statistics utility program, DFH0STAT, does not report any private resources or identify programs that are declared as application entry points.

Other changed statistics types

Table 4. Changed statistics types

Copybook	Functional area
DFHPGDDS	Program statistics
DFHPGRDS	JVM program statistics
DFHPIRDS	Pipeline manager statistics

Changed statistics types might increase the amount of statistics data that is written to the MVS systems management facility (SMF). To avoid any problems caused by multiple CICS regions writing increased interval statistics to the SMF at the same time, you can use the DFH\$STED sample utility program. This program varies the statistics interval occurrence time for each CICS region. For more information, see Stagger end-of-day time sample utility program (DFH\$STED) in Reference -> Utilities.

New statistics types

New CICS statistics types are added because of new domains or because of enhancements to CICS.

Table 5. New statistics types

Copybook	Functional area
DFHLDPDS	Program loader statistics for private programs
DFHLDYDS	LIBRARY resource statistics for private LIBRARY resources
DFHPGEDS	PROGRAM resource definition statistics for private programs
DFHPGPDS	JVM program resource statistics for private Java programs

New values in DFHSTIDS (statistics record identifiers)

The new DSECTs have corresponding values in the common statistics record copybook, DFHSTIDS. The revised list of the statistics record identifiers is shown in CICS statistics data section in the *CICS Customization Guide*.

The new values for CICS Transaction Server for z/OS, Version 5 Release 2 are as follows:

STILDY	32	DFHLDYDS	LIBRARY resources - private
STILDP	36	DFHLDPDS	Private Loader (Resid) id
STIPGP	146	DFHPGPDS	JVM programs - private
STIPGE	147	DFHPGEDS	Program definitions - private

New statistics types might increase the amount of statistics data that is written to the MVS systems management facility (SMF). To avoid any problems caused by multiple CICS regions writing increased interval statistics to the SMF at the same

time, you can use the DFH\$STED sample utility program. This program varies the statistics interval occurrence time for each CICS region. For more information, see Stagger end-of-day time sample utility program (DFH\$STED) in the *CICS Operations and Utilities Guide*.

The statistics formatting utility program, DFHSTUP

The statistics formatting utility program now formats additional statistics reports for the new statistics. You can include or exclude the new statistics reports by using these keywords on the SELECT TYPE and IGNORE TYPE parameters:

- JVMPROGRAM - now reports private as well as public resources
- LIBRARY - now reports private as well as public resources
- PROGRAM - now reports private as well as public resources
- PROGRAMDEF - now reports private as well as public resources

DFHSTUP produces separate reports for private resources for applications that are deployed on platforms. These reports are located after the report for public resources of the same type. DFHSTUP lists programs that are defined as application entry points twice, in both the report for public program definitions or JVM programs, and the report for private program definitions or JVM programs.

Chapter 16. Changes to sample programs

In each CICS release, check for changes to the samples provided to demonstrate the use of different CICS functions. New samples might be provided and existing samples modified or withdrawn. If you have custom programs or other items based on the samples, update them to reflect changes in the samples. Unless otherwise stated, sample programs are supplied in the SDFHSAMP library.

There were no changes to the sample programs in CICS TS 5.2.

Chapter 17. Changes to problem determination

CICS provides information to help you diagnose problems relating to new functions.

Part 5, “Changes to CICS messages and codes,” on page 143 lists messages and abend codes that have been removed, changed, and added for CICS Transaction Server for z/OS, Version 5 Release 2.

There were no other changes to problem determination in CICS Transaction Server for z/OS, Version 5 Release 2.

Chapter 18. Changes to security

When you upgrade to CICS Transaction Server for z/OS, Version 5 Release 2, note these changes to security.

APAR PI28039 update

The default setting for the **ENCRYPTION** system initialization parameter, **ENCRYPTION=STRONG**, no longer allows the use of the SSL version 3.0 security protocol. The minimum security protocol allowed with **ENCRYPTION=STRONG** is now TLS version 1.0.

If you have clients that still require the SSL version 3.0 protocol, you can enable support for that protocol by specifying the system initialization parameter **ENCRYPTION=SSLV3** for the CICS region. SSL 3.0 should only be used for a migration period while clients that still require this protocol are upgraded. Any connections that require encryption automatically use the TLS protocol, unless the client specifically requires SSL 3.0.

Security for CICS bundles

For resources that are dynamically created by CICS bundles, no additional CICS command security checks and resource security checks take place for those resource types, either when the resources are dynamically created at bundle installation time, or when you manipulate the resources by making changes to the CICS bundle. You need authority only to perform the actions on the CICS bundle, or for bundles that are installed with applications and platforms, to perform the actions on the application or platform with which the CICS bundle was deployed. However, CICS command security and resource security for the individual resource types do apply when you inquire on the dynamically created resources, or if you manipulate the dynamically created resources directly.

If you used CICS bundles in earlier CICS releases, check the security permissions that you gave to users for those bundles. Depending on how you set up security for CICS bundles, users with authority to act on individual CICS bundles might now be able to act on new or existing resources that are dynamically created as part of the installation of a bundle. Ensure that the levels of authority for BUNDLE resources are still appropriate.

Permission to make applications and CICS bundles available or unavailable

Operators with UPDATE access for the CLOUD.APPLICATION.*context* security profile now have permission for the new actions to make applications that are deployed on platforms available or unavailable to users, which is required in addition to enabling or disabling them. In releases before CICS TS 5.2, the action of enabling or disabling an application also made it available or unavailable to users, so the new permission is still appropriate for the same operators.

The same situation applies to operators with UPDATE access for a security profile that specifies the BUNDLE resource type and the resource name \$*, as described in

Security for platforms and applications in Administering. These operators can make BUNDLE resources that are created for platforms and applications available and unavailable.

Stand-alone CICS bundles need to be made available or unavailable only if they contain application entry points. Operators with UPDATE access for the security profile for a stand-alone CICS bundle, which specifies the BUNDLE resource type and the name of the BUNDLE resource, can make the resource available or unavailable.

Security for programs declared as application entry points

If you apply security measures to individual PROGRAM resources, for applications that are deployed on platforms, secure the programs that are declared as application entry points, but do not secure other programs in the applications. The security settings that you specify for a program that is part of an application deployed on a platform apply to both public and private programs, and do not take into account the version of the application. Programs that are declared as an application entry point must have a unique PROGRAM resource name in your environment. However, if you secure programs that run at a lower level in the application, programs with the same names might be running in different applications, which can lead to unforeseen consequences. In this situation, a user might have permission to access a program that is declared as an application entry point, but not have permission to access a program that runs at a lower level in the application, because the security settings from another instance of the program name are in effect. Consider the security measures that you apply to a program that is declared as an application entry point program, as applying to the whole application.

Integrated support for SAML

In CICS TS for z/OS, Version 4.2 and CICS TS for z/OS, Version 5.1, support for Security Assertion Markup Language (SAML) was provided in the CICS Transaction Server for z/OS Feature Pack for Security Token Extensions. The functions of that feature pack are now incorporated into CICS itself. You cannot use the feature pack with CICS Version 5.2.

In addition, the following functions are added:

- Support for using a SAML token in a requester application
- Support for adding attributes to a validated SAML token, for use in a requester application
- Support for signing modified SAML tokens
- Support for using the transaction channel for SAML containers to enable verified SAML information to be available to the whole application without the need to restructure the application.
- Support for configuring the clock skew time to allow flexibility in the time validity of SAML tokens

The SAML output containers have been enhanced with additional information extracted from the SAML token.

The SAML IVP has been enhanced to support easier validation of customer defined tokens.

Support for Kerberos

Previously, support for Kerberos tokens was provided remotely by using a web service. You can now validate a Kerberos token with a local external security manager (ESM) by using the CICS API. For more information, see `VERIFY TOKEN`. If your ESM is RACF, support is provided for Kerberos Version 5 and Generic Security Services. For the Kerberos support level of other ESMs, refer to their documentation.

Support is provided for validating Kerberos tokens in inbound web service requests. Optionally, the target application can also be set to run under the user ID associated with the client principal in the Kerberos token. To use Kerberos token validation, set the mode of the `<authentication>` element to the new value `basic-kerberos`. For more information, see The `<authentication>` attribute.

Extended support for cryptographic standards

The enhancements to support NIST SP800-131A compliant cipher suites and certificates, which were supplied in APAR PM97207 for CICS TS for z/OS Version 5.1 are now incorporated into CICS itself. For more information, see `Making your CICS TS system conformant with NIST SP800-131A`.

Additions to CICS RACF category 1 transactions

The list of category 1 transactions has some new CICS internal system transactions. These transactions must be defined to your external security manager, and the CICS region user ID must be authorized to use them, so that CICS can initialize successfully when it is running with security enabled (`SEC=YES`).

For a full list of all the CICS category 1 transactions, see `Category 1 transactions`. Also see the `DFH$CAT1 CLIST`, supplied in the `SDFHSAMP` library.

The new category 1 transactions are as follows:

- `CFCR`
- `CJLR`

Changes to command and resource security

New resource types, their resource identifiers, and associated commands are subject to command security checking and resource security checking.

No new resource types were added in CICS Transaction Server for z/OS, Version 5 Release 2.

Part 2. Upgrading CICS Transaction Server

To upgrade your CICS regions to CICS Transaction Server for z/OS, Version 5 Release 2, carry out the tasks described here. There are some general upgrading tasks which you must always perform. There are also upgrading tasks for some specific functional areas where there is a need for special considerations.

Chapter 19. Upgrade procedures for all CICS regions

Complete these tasks when you upgrade any CICS Transaction Server region to CICS Transaction Server for z/OS, Version 5 Release 2.

Important: Before you upgrade you must install the CICS TS for z/OS V5.2 - activation module or CICS TS for z/OS Value Unit Edition V5.2 - activation module for the version of CICS that you are going to use.

You must also add the SDFHLIC or SDFHVUE library in the STEPLIB of the CICS TS JCL. The SDFHLIC or SDFHVUE library must be APF-authorized. If you use coupling facility data table servers, temporary storage servers, region status servers, or named counter servers, you must also add the SDFHLIC or SDFHVUE library to the STEPLIB of the JCL for each of the servers.

Redefining and initializing the local and global catalogs

When you upgrade to a new CICS release, delete, redefine, and initialize the CICS local catalog and global catalog.

Procedure

1. Delete your existing local catalog and global catalog.
2. Define and initialize new local and global catalogs, following the instructions in the *CICS System Definition Guide*. When you initialize the catalogs, make sure that you use the CICS Transaction Server for z/OS, Version 5 Release 2 versions of the DFHRMUTL and DFHCCUTL utility programs and the sample jobs.
3. When you start the CICS region for the first time after upgrading, make sure that it is an initial start with the START=INITIAL parameter.

Enabling z/OS conversion services

To obtain the benefits of z/OS conversion services for data conversion, perhaps because your system requires support for the conversion of UTF-8 or UTF-16 data to EBCDIC, you must enable the z/OS conversion services and install a conversion image that specifies the conversions that you want CICS to perform.

For the instructions to set up and configure conversions supported through the operating system services, see *z/OS Unicode Services User's Guide and Reference*.

If z/OS conversion services are not enabled, CICS issues a message. If such a message is issued when starting a CICS region that is expected to use the z/OS conversion services, an IPL is necessary to enable these services.

If you do not need the z/OS conversion services, you can suppress that message.

To discover the status of z/OS conversion services after an IPL, use one of the following commands from an MVS console:

- D UNI

This command shows whether z/OS conversion services were enabled.

- D UNI,ALL

This command shows whether z/OS conversion services were enabled and which conversion the system supports.

If you want to enter the command from SDSF, add a / to the beginning of the command.

Upgrading the CSD for CICS-supplied and other IBM-supplied resource definitions

Upgrade the CICS-supplied resource definitions using the UPGRADE function of the CSD utility program DFHCSDUP. If you have resource definitions in your CSD that support other IBM products, such as z/OS, you might need to upgrade these also.

About this task

If you need to share your upgraded CSD with different CICS releases, see “CSD compatibility between different CICS releases” on page 77.

Procedure

1. Run the DFHCSDUP utility program, specifying the UPGRADE command, to upgrade the CICS-supplied definitions in your CSD to the latest CICS TS level. You can create a new CSD using the DFHCSDUP INITIALIZE command. For information about running DFHCSDUP with the UPGRADE command, see the *CICS Operations and Utilities Guide*. To help estimate the space you need in your CSD for definition records, see the *CICS System Definition Guide*.
2. If you have resource definitions in your CSD that support other IBM products, upgrade these as required. For example, if your Language Environment[®] resource definitions are not at the correct z/OS level, you should delete and replace the CSD group containing these. The Language Environment resource definitions are in the SCEESAMP library in member CEECCSD. “Sample job for additional CSD modification” has an example job to delete and replace the CSD group containing these.

Sample job for additional CSD modification

If you need to upgrade the Language Environment resource definitions in your CSD, you can use a job like this.

```

//JOBNAME JOB 1,userid,
//      NOTIFY=userid,CLASS=n,MSGLEVEL=(n,n),MSGCLASS=n
/*JOBPARM SYSAFF=sysid
/* Remove Old Language Environment group
//CSDUP1 EXEC PGM=DFHCSDUP,REGION=2M,PARM='CSD(READWRITE)'
//STEPLIB DD DSN=CICSTS52.CICS.SDFHLOAD,DISP=SHR
//DFHCSD DD DSN=CICSTS52.CICSHURS.DFHCSD,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSABOUT DD SYSOUT=*
//SYSABEND DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSIN DD *
DELETE GROUP(CEE)
/*
/*
//CSDUP2 EXEC PGM=DFHCSDUP,REGION=2M,PARM='CSD(READWRITE)'
//STEPLIB DD DSN=CICSTS52.CICS.SDFHLOAD,DISP=SHR
//DFHCSD DD DSN=CICSTS52.CICSHURS.DFHCSD,DISP=SHR
//SYSPRINT DD SYSOUT=*
//SYSABOUT DD SYSOUT=*
//SYSABEND DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SYSIN DD DSN=SYS1.ZOS113.SCEESAMP(CEECCSD),DISP=SHR
/*
//

```

Figure 1. Upgrading Language Environment resource definitions

Upgrading user-modified CICS-supplied resource definitions

When you run the UPGRADE function of the CSD utility program DFHCSDUP, ensure that you manually upgrade any CICS-supplied definitions that you have modified in earlier releases.

About this task

It is important to upgrade your modified definitions to ensure that they are defined correctly with nondefault values for attributes that are new. If you fail to upgrade modified definitions, CICS assigns default values to any new attributes, and these might be inappropriate for CICS-supplied resource definitions.

Procedure

- If you are not sure whether your CSD contains any modified CICS-supplied definitions, use the DFHCSDUP SCAN command to compare the CICS-supplied resource definitions with any user-modified versions. The DFHCSDUP SCAN command searches for the CICS-supplied version of a specified resource name of a specific resource type and compares it with any other resource definition of the same name and type. DFHCSDUP reports any differences it finds between the CICS-supplied definition and a user-modified version. If you have copied and changed the name of a CICS-supplied definition, the SCAN command enables you to specify the changed name as an alias.
- The safest way to upgrade your definitions is to copy the upgraded CICS-supplied definitions and reapply your modifications. This action is necessary because the UPGRADE command does not operate on your own groups or on CICS groups that you have copied.
- If the CICS region uses CICSplex SM, manually upgrade any of the dynamically created CICSplex SM resource definitions that you modified in your previous

release, using the equivalents in Version 5.2. The dynamically created resource definitions and their attributes are in the following members of the SEYUSAMP sample library:

- EYU\$CDEF contains the default resource definitions for a CMAS.
- EYU\$MDEF contains the default resource definitions for a MAS.
- EYU\$WDEF contains the default resource definitions for a WUI server.

Upgrading copies of CICS-supplied resource definitions

If you have made copies of CICS-supplied resource definitions, you might need to change your copies to match the changes that have been made to the supplied definitions for this release. To help you, member DFH\$CSDU in library SDFHSAMP contains ALTER commands that you can apply using the CSD utility program DFHCSDUP.

Procedure

1. Review your resource definitions to determine if you have copied any CICS-supplied definitions.
2. Review DFH\$CSDU to determine if the changes that it contains should apply to your resource definitions.
3. Make any necessary changes to DFH\$CSDU. It is advisable to make a copy of DFH\$CSDU and apply any changes to the copy.
4. Run DFHCSDUP using your modified version of DFH\$CSDU as input. As supplied, the ALTER commands in DFH\$CSDU specify GROUP(*), which means that DFHCSDUP attempts to change resources in the CICS-supplied groups. This action is not permitted and results in message DFH5151. You can ignore this message.

Example

Program DFHD2EDF is now defined as CONCURRENCY(THREADSAFE). Therefore, DFH\$CSDU contains the following command:

```
ALTER PROGRAM(DFHD2EDF) GROUP(*) CONCURRENCY(THREADSAFE)
```

When you run DFHCSDUP, the attribute is added to the definitions of program DFHD2EDF in all groups. Other attributes not mentioned in DFH\$CSDU are unchanged.

DSA size limits

It is not advisable to set the size of individual dynamic storage areas (DSAs), and usually it is not necessary. However, it is possible to set the size of some DSAs by using the **CDSASZE**, **UDSASZE**, **RDSASZE**, **ECDSASZE**, **EUDSASZE**, **ESDSASZE**, and **ERDSASZE** system initialization parameters.

For example, **CDSASZE** sets the size of the CICS dynamic storage area (CDSA), and **ECDSASZE** specifies the size of the extended CICS dynamic storage area (ECDSA). The default value for these parameters is 0, indicating that the size of the DSA can change dynamically. If you specify a nonzero value, the DSA size is fixed.

If you specify DSA size values that in combination do not allow sufficient space for the remaining DSAs, CICS fails to initialize.

- The limit on the storage available for the DSAs in 24-bit storage (below 16 MB) is specified by the **DSALIM** system initialization parameter. You must allow at least 256K for each DSA in 24-bit storage for which you have not set a size.
- The limit on the storage available for the DSAs in 31-bit storage (above 16 MB but below 2 GB) is specified by the **EDSALIM** system initialization parameter. You must allow at least 1 MB for each DSA in 31-bit storage for which you have not set a size.

You cannot set the size of individual DSAs in 64-bit storage; that is, in the above-the-bar DSA (GDSA).

CSD compatibility between different CICS releases

You can share the CICS system definition data set (CSD) between different CICS releases by using the appropriate compatibility groups.

Most releases of CICS change the CICS-supplied groups of resource definitions that are included in the DFHLIST group list. The old versions of the CICS resource definitions are retained in compatibility groups. If you share the CSD between different CICS releases, these compatibility groups are needed to support earlier releases.

After you upgrade a CSD, if you plan to share the CSD with earlier releases of CICS, include the appropriate DFHCOMP x compatibility groups in your startup group list. Table 6 shows you which DFHCOMP x groups to include for each earlier release.

Do not attempt to share a CSD with a CICS region that is running at a higher release level than the CSD.

You must install the compatibility groups in the correct order, as shown in the table. For example, to run a CICS TS 4.1 region with a CSD that is upgraded to CICS TS 5.2, add the DFHCOMPG compatibility group, followed by the DFHCOMPF compatibility group, followed by the DFHCOMPE compatibility group, to the end of your group list.

Table 6. Required compatibility groups for earlier releases of CICS

	CICS TS 5.2 CSD	CICS TS 5.1 CSD	CICS TS 4.2 CSD	CICS TS 4.1 CSD	CICS TS 3.2 CSD	CICS TS 3.1 CSD
Shared with CICS TS 5.2	None	Do not share	Do not share	Do not share	Do not share	Do not share
Shared with CICS TS 5.1	DFHCOMPG	None	Do not share	Do not share	Do not share	Do not share
Shared with CICS TS 4.2	DFHCOMPG DFHCOMPF	DFHCOMPF	None	Do not share	Do not share	Do not share
Shared with CICS TS 4.1	DFHCOMPG DFHCOMPF DFHCOMPE	DFHCOMPF DFHCOMPE	DFHCOMPE	None	Do not share	Do not share
Shared with CICS TS 3.2	DFHCOMPG DFHCOMPF DFHCOMPE DFHCOMPD	DFHCOMPF DFHCOMPE DFHCOMPD	DFHCOMPE DFHCOMPD	DFHCOMPD	None	Do not share

Table 6. Required compatibility groups for earlier releases of CICS (continued)

	CICS TS 5.2 CSD	CICS TS 5.1 CSD	CICS TS 4.2 CSD	CICS TS 4.1 CSD	CICS TS 3.2 CSD	CICS TS 3.1 CSD
Shared with CICS TS 3.1	DFHCOMPG DFHCOMPF DFHCOMPE DFHCOMPD DFHCOMPC	DFHCOMPF DFHCOMPE DFHCOMPD DFHCOMPC	DFHCOMPE DFHCOMPD DFHCOMPC	DFHCOMPD DFHCOMPC	DFHCOMPC	None

Compatibility group DFHCOMPG

Group DFHCOMPG is required for compatibility with CICS Transaction Server for z/OS, Version 5 Release 1.

Table 7. Contents of compatibility group DFHCOMPG

Resource type	Name
PROGRAM	DFHPGADX DFHPGAHX DFHPGALX DFHPGAOX DFHPIEP

Compatibility group DFHCOMPF

Group DFHCOMPF is required for compatibility with CICS Transaction Server for z/OS, Version 4 Release 2.

Table 8. Contents of compatibility group DFHCOMPF

Resource type	Name
FILE	DFHADEM
MAPSET	DFHADMS
PROFILE	DFHCICSI

Table 8. Contents of compatibility group DFHCOMPF (continued)

Resource type	Name
PROGRAM	DFHADDRM
	DFHADJR
	DFHADWB0
	DFHADWM0
	DFHADWM1
	DFHADWM2
	DFHADWM3
	DFHADWM4
	DFHADWM5
	DFHADWM6
	DFHADWT0
	DFHADWT1
	DFHADWT2
	DFHADWT3
	DFHADWT4
	DFHADWT5
	DFHCHS
	DFHDLLOD
	DFHD2EDF
	DFHEDFX
	DFHEIGDS
	DFHEITAB
	DFHEITBS
	DFHEITSZ
	DFHEJDNX
	DFHEJEP
	DFHEJITL
	DFHIIRS
	DFHJVCVT
	DFHLETRU
	DFHPIVAL
	DFHSJGC
	DFHSJPI
	DFHSMTAB
	DFHXOPUS
	DFJCICS
	DFJCICSB
	DFJCZDTC
	DFJDESN
	DFJIIRP
	DFJIIRQ
	DFJ1ESN
	DFJ1ICS
	DFJ1ICSB
	DFJ1ZDTC

Table 8. Contents of compatibility group DFHCOMPF (continued)

Resource type	Name
TRANSACTION	CBAM
	CDFS
	CEHP
	CEHS
	CEJR
	CEMT
	CEOT
	CESF
	CESL
	CESN
	CEST
	CETR
	CIEP
	CIRP
	CIRR
	CJGC
	CJPI
	CLQ2
	CLR2
	CLS2
	CLS3
	CLS4
	CMPX
	CMSG
	CPMI
	CQPI
	CQPO
	CREA
	CREC
	CRSQ
	CRSR
	CRSY
	CRTE
	CSAC
	CSHR
	CSMI
	CSM1
	CSM2
	CSM3
	CSM5
	CSNC
	CSSF
	CVMI
	CXCU
	CXRT

Compatibility group DFHCOMPE

Group DFHCOMPE is required for compatibility with CICS Transaction Server for z/OS, Version 4 Release 1.

Table 9. Contents of compatibility group DFHCOMPE

Resource type	Name
PROGRAM	DFHMIRS DFHCCNV DFHUCNV DSNTIAC DSNTIA1 DFHEDP DFHDBAT DFHDBUEX DFHPIEP

Compatibility group DFHCOMPD

Group DFHCOMPD is required for compatibility with CICS Transaction Server for z/OS, Version 3 Release 2.

Table 10. Contents of compatibility group DFHCOMPD

Resource type	Name
TDQUEUE	CPLD CPLI
PROGRAM	DFHPIVAL DFHSJJML IXMI33DA IXMI33D1 IXMI33IN IXMI33UC IXM4C56
TRANSACTION	CJMJ

Compatibility group DFHCOMPC

Group DFHCOMPC is required for compatibility with CICS Transaction Server for z/OS, Version 3 Release 1.

Table 11. Contents of compatibility group DFHCOMPC

Resource type	Name
PROGRAM	IXM4C53

Upgrading CICS Explorer

You must upgrade the CICS Explorer to Version 5.2 before you can connect to CICS regions at CICS TS Version 5.2. When you upgrade CICS Explorer you can use it to work with CICS TS 5.2 regions, and also with other CICS TS regions that are not yet upgraded.

For CICS Explorer Version 5.1.1 and later, you can use the facilities that the Eclipse platform provides to update your CICS Explorer, or other software, or add new software plug-ins, such as CICS Tools.

The update site for the CICS Explorer is already coded in the product. The site address is displayed on the Installed Software page in the Software Updates window. If you choose not to use the composite update site, you must specify the

address of your preferred update site, which can be either on your local workstation or a remote location. You can add multiple update sites, each containing one or more software downloads.

For CICS Explorer versions earlier than Version 5.1.1, you must install a new copy of CICS Explorer. You cannot upgrade in the way described earlier because earlier versions of CICS Explorer use a different version of Eclipse than CICS Explorer Version 5.1.1. Before you install the new copy of CICS Explorer, it is advisable to back up your CICS Explorer workspace so that you can restore the workspace to a previous version, if required.

For more information about upgrading CICS Explorer, see Updating and installing software in the CICS Explorer product documentation.

 Taking a backup of the CICS Explorer workspace in Installing

Chapter 20. Upgrading application programs

CICS translator support for pre-Language Environment compilers is withdrawn. Runtime support is provided for existing application programs that were developed using these compilers, except for OS/VS COBOL and OO COBOL programs, which do not have runtime support.

Withdrawal of support for pre-Language Environment compilers

CICS translator support is withdrawn for the following compilers:

- OS/VS COBOL (5740-CB1, 5740-LM1, and 5734-CB4)
- VS COBOL II (5668-958 and 5688-023)
- OS PL/I Version 1 (5734-PL1)
- OS PL/I Version 2 (5668-910 and 5668-909)
- SAA AD/Cycle C/370™ (5688-216)

For details of the compilers that are supported by CICS, see High-level language support in What's new.

The following JCL procedures that were supplied in earlier releases for translating, compiling, and link-editing using the unsupported compilers are also withdrawn:

COBOL

The DFHEITVL, DFHEXTVL, DFHEBTVL, DFHEITCL, and DFHEXTCL procedures.

PL/I The DFHEITPL, DFHEXTPL, and DFHEBTPL procedures.

C The DFHEITDL and DFHEXTDL procedures.

CICS now supplies the following procedures only, for use with compilers that conform to Language Environment:

Language	CICS-online	EXCI	Integrated translator
C	DFHYITDL	DFHYXTDL	DFHZITDL (without XPLINK) DFHZITFL (with XPLINK)
C++	DFHYITEL	DFHYXTEL	DFHZITEL (without XPLINK) DFHZITGL (with XPLINK)
COBOL	DFHYITVL	DFHYXTVL	DFHZITCL
PL/I	DFHYITPL	DFHYXTPL	DFHZITPL

The following CICS translator options, which all relate to the unsupported compilers, are obsolete:

- ANSI85
- LANGLVL
- FE

The CICS translators ignore these translator options and issue a return code 4 warning message.

Runtime support for programs developed using pre-Language Environment compilers

Although application program development support for obsolete compilers is withdrawn, CICS usually continues to provide runtime support for your existing application programs that were developed using these old compilers. However, to apply maintenance to these application programs, use one of the supported compilers that conforms to Language Environment.

Applications compiled and linked with pre-Language Environment compilers usually run successfully using the runtime support provided by Language Environment. These applications do not usually need to be recompiled or re-link-edited. If required, adjust Language Environment runtime options to allow these applications to run correctly. For more information, see the z/OS Language Environment Run-Time Application Migration Guide and the migration information for the language in use. Because pre-Language Environment compilers are not Language Environment-conforming, programs compiled by these compilers cannot take advantage of all Language Environment facilities in a CICS region.

Runtime libraries provided by Language Environment replace the runtime libraries that were provided with older compilers such as VS COBOL II, OS PL/I, and C/370. The runtime libraries provided with pre-Language Environment compilers are not supported. Language libraries, other than the Language Environment libraries, must not be present in your CICS startup JCL.

Withdrawal of runtime support for OO COBOL

In this CICS release, you cannot use COBOL class definitions and methods (object-oriented COBOL). This restriction includes both Java classes and COBOL classes.

Modules using OO features and compiled in earlier CICS releases with the OOCOBOL translator option cannot run in this CICS release. The OOCOBOL translator option was used for the older SOM-based (System Object Manager-based) OO COBOL, and runtime support for this form of OO COBOL was withdrawn in z/OS V1.2. The newer Java-based OO COBOL, which is used in Enterprise COBOL, is not supported by the CICS translator.

Chapter 21. Upgrading Business Transaction Services (BTS)

When you upgrade your BTS environment to CICS Transaction Server for z/OS, Version 5 Release 2, you might need to migrate the DFHLRQ data set. Be aware that even if you are not explicitly making use of BTS services in your applications, it is possible that they are being exploited by vendor code or IBM-supplied products executing within your CICS environment.

Migrating the DFHLRQ data set

The local request queue data set stores pending BTS requests, such as timer requests, or requests to run activities. It is recoverable and is used to ensure that, if CICS fails, no pending requests are lost.

Requests that CICS can execute immediately, such as requests to run activities, are stored on the data set only briefly. Requests that CICS cannot execute immediately, such as timer or unserviceable requests, might be stored for longer periods. When CICS has processed a request, the request is deleted from the data set.

If you have outstanding BTS activities for BTS processes in CICS, you must migrate the contents of your DFHLRQ data set as part of the upgrade. You can use a utility such as IDCAMS COPY to update the CICS TS for z/OS, Version 5.2 DFHLRQ data set with the contents of the DFHLRQ data set from your previous CICS release.

Be aware that even if you are not explicitly making use of BTS services in your applications, it is possible that they are being exploited by vendor code or IBM-supplied products executing within your CICS environment.

Repository data sets

When a process is not executing under the control of the CICS business transaction services domain, its state and the states of its constituent activities are preserved by being written to a VSAM data set known as a repository.

To use BTS, you must define at least one BTS repository data set to MVS. You may decide to define more than one, assigning a different set of process-types to each. One reason for doing this might be storage efficiency, for example, if some of your process-types tend to produce longer records than others.

If you operate BTS in a sysplex, several CICS regions may share access to one or more repository data sets. This sharing enables requests for the processes and activities stored on the data sets to be routed across the participating regions. As you upgrade your CICS releases, you may therefore still share older versions of repository data sets. The expectation is that you define and use different repository data sets whenever you want to assign different sets of process-types, rather than because a CICS upgrade has occurred.

Chapter 22. Communicating over IPIC with different levels of CICS

If both an APPC or MRO connection and an IPIC connection exist between two CICS regions, and both have the same name, the IPIC connection takes precedence. However, if your terminal-owning region (TOR) and application-owning region (AOR) are in CICS systems that are using different levels of CICS, the rules can differ.

An APPC or MRO connection is defined using the CONNECTION resource. An IPIC connection is defined using the IPCONN resource.

If both CONNECTION resources and IPCONN resources are active in a CICS region, CICS searches for an IPIC connection first, so that when resources with the same name exist, the preference for an IPCONN resource can be maintained. However, if an IPCONN resource is not available, CICS attempts to route over an APPC or MRO connection using a CONNECTION resource. If the request fails, a SYSID error is returned to the application that scheduled the request. For more information about how IPIC overrides default connections, see *Changes to resource definitions*.

Table 12 and Table 13 on page 88 show how the resources are used depending on the level of CICS installed at the communicating regions, the availability of resources, and the intercommunication method that is being used.

Table 12. Selection behavior for IPCONN and CONNECTION resources with TOR and AOR communications

Version of CICS in TOR or routing region	Status of IPCONN resource	CICS TS 3.2 AOR			CICS TS 4.1 AOR			CICS TS 4.2, 5.1, or 5.2 AOR		
		DPL	Asynchronous processing and transaction routing	Enhanced Routing	DPL	Asynchronous processing and transaction routing	Enhanced Routing	DPL	Asynchronous processing and transaction routing	Enhanced Routing
CICS TS 3.2	Acquired	IPIC connection	APPC or MRO connection	APPC or MRO connection	IPIC connection	APPC or MRO connection	APPC or MRO connection	IPIC connection	APPC or MRO connection	APPC or MRO connection
	Released	Request rejected	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection
CICS TS 4.1	Acquired	IPIC connection	APPC or MRO connection	APPC or MRO connection	IPIC connection	IPIC connection	APPC or MRO connection	IPIC connection	IPIC connection	APPC or MRO connection
	Released	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection
CICS TS 4.2, 5.1, or 5.2	Acquired	IPIC connection	APPC or MRO connection	APPC or MRO connection	IPIC connection	IPIC connection	APPC or MRO connection	IPIC connection	IPIC connection	IPIC connection
	Released	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection

Table 13. Selection behavior for IPCONN and CONNECTION resources with AOR and ROR communications

Version of CICS in the AOR	Status of IPCONN resource	CICS TS 3.2 or 4.1 ROR				CICS TS 4.2, 5.1, or 5.2 ROR			
		File control	Transient data	Temporary storage	DL/I	File control	Transient data	Temporary storage	DL/I
CICS TS 3.2	Acquired	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection
	Released	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection
CICS TS 4.1	Acquired	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection
	Released	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection
CICS TS 4.2, 5.1, or 5.2	Acquired	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	IPIC connection	IPIC connection	IPIC connection	APPC or MRO connection
	Released	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection	APPC or MRO connection

Chapter 23. Upgrading multiregion operation (MRO)

To upgrade CICS multiregion operation (MRO) support, install the latest DFHIRP and DFHCSVC modules in the MVS link pack area (LPA) and carry out tests.

About this task

For MRO, the interregion communication program DFHIRP is installed in the link pack area (LPA). The CICS TS for z/OS, Version 5.2 DFHIRP module is compatible with earlier releases, and works with all releases of CICS. However, the CICS TS for z/OS, Version 5.2 version of DFHIRP, required for multiple XCF group support, can be used only on z/OS Version 1.7 or later.

DFHIRP can be used only from the LPA. Therefore in an MVS image you can have only one version of the module named DFHIRP, which must be at the *highest* release level of the CICS regions that run in that MVS image.

In a Parallel Sysplex®, where MRO communication between MVS images is through XCF/MRO, the DFHIRP programs installed in the different MVS images can be at different release levels. However, the DFHIRP in an MVS image must still be installed from the *highest* release of CICS running in that MVS image. For example, a CICS TS 3.2 DFHIRP can communicate with a CICS TS for z/OS, Version 5.2 DFHIRP across XCF/MRO, but the CICS regions running in the MVS with the CICS TS 3.2 DFHIRP cannot be later than CICS TS 3.2.

These steps are a guide to the upgrading process for MRO, to install the latest DFHIRP and DFHCSVC modules in the MVS link pack area (LPA). For information about how to perform some of these steps, such as installing the SVC or IRP modules in the LPA, see *Installing CICS modules in the MVS link pack area* in the *CICS Transaction Server for z/OS Installation Guide*. These steps assume that RACF is your external security manager (ESM).

Procedure

1. Install the CICS SVC routine, DFHCSVC, in the LPA, and specify a new CICS SVC number for this routine in the MVS SVC Parm table. If the new DFHCSVC must coexist with an older version, rename one of them so that both versions can be installed in the LPA. However, coexistence is not recommended or necessary: DFHCSVC is compatible with earlier releases and the latest CICS TS version supports all the earlier releases of CICS.
2. Test the new SVC on stand-alone CICS regions, without using any MRO. You can do this running the CICS IVP, DFHIVPOL.
3. Install the CICS interregion communication program, DFHIRP, in a suitable LPA library. If you have a strategy whereby all users of DFHIRP on the z/OS image being upgraded can be quiesced, then you can use the dynamic LPA function to replace DFHIRP. Otherwise you must IPL MVS with the **CLPA** option. Failing to shut down all users of DFHIRP during the upgrade process can cause incompatibility between control blocks resulting in abends.

To dynamically update DFHIRP perform the following steps:

- a. Quiesce all users of DFHIRP. For example, WebSphere® EXCI, CTG EXCI, all CICS regions including any CMASs must either be shutdown or logged off from MRO/XM, and finally all other work using EXCI must be shut down.

Important: The process described here does not include upgrading CICSplex SM to the CICS TS 5.2 level. For more information, see Chapter 36, “Upgrading a CMAS,” on page 135.

- b. Update LPA modules DFHCVSC, DFHDSPEX, DFHUMPX, DFHIRP, DFHSSEN and DFHSVC99 using the dynamic LPA facility specifying the **ADD** verb.
- c. Run the CICS TS 5.2 supplied utility DFHCSVCU to update the z/OS SVC table as documented in Running the DFHCSVCJ job.
- d. Restart MRO by either setting IRC connected in all executing CICS regions or restarting the CICS regions.
- e. As dynamic changes are discarded by an IPL, you must schedule an IPL for a convenient time to ensure that all dynamically applied changes have been correctly applied to the z/OS system libraries.

Important: If you do not follow these steps an IPL is required to shut everything down and use the new DFHIRP module.

4. Test your production MRO CICS regions, under your existing release of CICS, but using the new SVC number and the new DFHIRP. For this test, run without any logon or bind-time security checking: that is, do not define any RACF FACILITY class profiles.
5. Define the required DFHAPPL.applid profiles in the RACF FACILITY general resource class. When the profiles are ready for all the MRO regions, test the production regions again with the new SVC and DFHIRP, this time using the FACILITY class profiles for logon and bind-time security checking.
6. If the production MRO regions successfully log on to the new IRP with the new SVC, and bind-time security checking works successfully, use the new DFHIRP and SVC for the production regions.
7. With the production regions running successfully under the CICS SVC and IRP, you can initialize and test some CICS Transaction Server regions using MRO. These test regions can coexist in the same MVS image as the production regions, all using the same SVC and IRP.

Chapter 24. Upgrading the Java environment

When you upgrade to a new CICS release, you might require changes to your JVM profiles and to other aspects of your Java environment. You might also require changes to your Java applications.

Earlier versions of Java

Java programs that ran under CICS Transaction Server for z/OS, Version 3 and CICS Transaction Server for z/OS, Version 4 can also run under CICS Transaction Server for z/OS, Version 5.

When you upgrade from one version of Java to another, check for compatibility issues between the Java APIs, and compatibility issues specific to the IBM SDK for z/OS. You can find this information at Java Standard Edition Products on z/OS.

To avoid potential problems with deprecated APIs, develop all new Java programs for CICS Transaction Server for z/OS, Version 5 Release 2 using an application development environment that supports the same version of Java as the environment used by CICS. You can run code compiled with an older version of Java in a new runtime environment, if the environment does not use APIs that are removed in the newer version of Java or CICS. For further details refer to the **Target Platform** setting when using the CICS Explorer SDK.

JVM profiles

If you already have JVM profiles that you set up in a previous CICS release, upgrade these profiles. Settings that are suitable for use in JVM profiles can change from one CICS release to another, so check the CICS documentation for any significant changes. You must also compare your existing JVM profiles to the latest samples supplied with CICS. Changes to the JVM profile options are described in “Changes to options in JVM profiles” on page 92. A list of suitable options for this release is in JVM profiles: options and samples in Deploying. Use the new samples supplied with CICS Transaction Server for z/OS, Version 5 Release 2 to help you create new profiles, rather than upgrading your existing files.

Copy your JVM profiles to a new location on z/OS UNIX to use with the new CICS release then apply the required upgrades. Do not try to use JVM profiles with more than one CICS release at the same time, because the settings are not compatible.

Ensure that the JVM profiles that you want to use are in the z/OS UNIX directory that is specified by the **JVMPROFILEDIR** system initialization parameter.

Key changes to CICS support for Java applications

Check for changes that can affect your Java environment when you upgrade to CICS Transaction Server for z/OS, Version 5 Release 2.

Be aware of the following significant changes that can affect your Java environment when you upgrade to CICS Transaction Server for z/OS, Version 5 Release 2:

- CICS uses the IBM 64-bit SDK for z/OS, Java Technology Edition, Version 7 or Version 7 Release 1.
- The supported Axis2 version is changed to Axis2 V1.6.2 and its prerequisite software.
- The Liberty Angel process must be started if you use the CICS Liberty security feature.
- Only one Liberty JVM server can be run per region with the CICS Liberty security feature enabled.
- You can no longer use OSGi bundles in a Liberty JVM server. A CICS bundle containing OSGi bundles resources will no longer deploy to a Liberty JVM server, and a Liberty JVM server will not enable if it has the OSGI_BUNDLES option in its JVM profile. OSGi bundles can only be deployed to a Liberty JVM server as part of an enterprise bundle archive (EBA), or as library bundles using the bundle repository of Liberty. You therefore cannot specify the DB2 .jar files in OSGi bundles. Instead, specify the <cicsts_jdbcDriver> element in the server.xml file.

Changes to options in JVM profiles

When you upgrade to a new release of CICS TS, there are normally some changes to the options available in JVM profiles and to their possible or suggested settings.

The JVM server supports a variety of Java workloads. The following sample JVM profiles are supplied with CICS TS for z/OS, Version 5.2:

- DFHJVMAX.jvmprofile is a JVM profile that specifies the options for initializing the JVM server to support SOAP processing by Axis2 applications. Axis2 is an open source web services engine from the Apache foundation that supports a number of the web service specifications and provides a programming model to create Java applications that can run in Axis2.
- DFHJVMST.jvmprofile is a JVM profile that allows the JVM server to be configured for a Security Token Service.
- DFHOSGI.jvmprofile is a JVM profile that specifies the options for initializing the JVM server for Java applications that comply with the OSGi specification.
- DFHWLP.jvmprofile is a JVM profile to run workloads for the Liberty profile, a lightweight application server that can support JSP and servlet applications for developing modern web interfaces for CICS. Liberty profile servers must use a file encoding of ISO-8859-1 or UTF-8. The supplied sample profile DFHWLP is configured to use ISO-8859-1.

JVM profiles must have a file extension of .jvmprofile. The JVM server fails to enable if this extension is not present. The sample JVM profiles that are shipped with CICS TS for z/OS, Version 5.2 have this file extension.

When you upgrade to a new release of CICS TS, there are normally some changes to the options available in JVM profiles and to their possible or suggested settings. A good practice is to use the sample JVM profiles that are shipped with the new release, and reapply the customization that you made to those JVM profiles in previous releases. Using the latest JVM profiles ensures that you do not miss important updates to the options and their settings.

The obsolete, changed, and new options in JVM profiles are summarized here. For more details about the options, see JVM profiles: options and samples in *Deploying*.

Table 14. New options in JVM profiles

Option	Status	CICS and Java launcher action	Notes
JNDI_REGISTRATION	For CICS sample profiles	Accepted	Specifies that the JNDI registration JAR files are automatically added to the JVM runtime environment.
SECURITY_TOKEN_SERVICE	For CICS sample profiles	Accepted	Controls whether the JVM server can use security tokens. This option must be set to YES for a JVM server to use security tokens. If this configuration option is set to NO, the JVM server is initialized as an OSGi JVM server and Security Token Service support is disabled for that JVM server. SECURITY_TOKEN_SERVICE=YES is not compatible with JAVA_PIPELINE=YES, which configures the JVM to support Axis2.
WSDL_VALIDATOR	For CICS sample profiles	Accepted	Enables validation for SOAP requests and responses against their definition and schema.

Table 15. Changed and obsolete options in JVM profiles

Option	Status	CICS and Java launcher action	Replace with	Notes
OSGI_BUNDLES	Not supported in Liberty JVM server	Liberty JVM server does not enable with this option	n/a	Deploy OSGi bundles in a Liberty JVM server as part of an enterprise bundle archive (EBA) or as library bundles.

Changes to JVM profile symbols

&CONFIGROOT;

When you use this symbol in a JVM profile, the absolute path of the directory where the JVM profile is located is substituted at run time.

For information about the other supported JVM profile symbols, see JVM profiles: options and samples in Deploying.

Chapter 25. Upgrading the CICS-WebSphere MQ connection

If you use the CICS-WebSphere MQ adapter, bridge, trigger monitor, or API crossing exit to connect CICS to WebSphere MQ, check your configuration and make any necessary changes.

When you upgrade to a new version or release of WebSphere MQ, ensure that you specify the new versions of the WebSphere MQ libraries in the STEPLIB and DFHRPL concatenations in your CICS procedure, replacing the previous versions of these libraries. The libraries are *thlqual.SCSQAUTH*, *thlqual.SCSQCICS*, and *thlqual.SCSQLOAD*, where *thlqual* is the high-level qualifier for the WebSphere MQ libraries. The SCSQAUTH library is included in both concatenations, but the SCSQLOAD library and the optional SCSQCICS library are included in the DFHRPL concatenation only. Include the WebSphere MQ libraries after the CICS libraries to ensure that the correct code is used.

Support for WebSphere MQ Version 7 API calls

New or changed CICS applications that use the new API calls in WebSphere MQ Version 7 must be link-edited with the WebSphere MQ API stub modules that are shipped with CICS.

The new API calls are MQBUFMH, MQCB, MQCTL, MQCRTMH, MQDLTMH, MQDLTMP, MQINQMP, MQMHBUF, MQSETMP, MQSTAT, MQSUB, and MQSUBRQ. These Version 7 API calls are only supported in CICS when you use the stubs shipped with CICS, not the stubs shipped with WebSphere MQ. New and existing CICS applications that do not use the Version 7 API calls can use the stubs shipped with CICS or WebSphere MQ.

If you use the new Version 7 API calls MQCB and MQCTL for asynchronous message consumption by CICS applications, you must code your program using information given in the CICS documentation, in addition to the WebSphere MQ programming documentation. The requirements for asynchronous message consumption in a CICS environment are listed in Asynchronous message consumption and callback routines.

Chapter 26. Upgrading the CICS DB2 connection

This information enables you to plan and carry out installation or upgrade procedures in the CICS DB2[®] environment.

CICS provides an attachment facility (the CICS DB2 adapter) that works with all supported releases of DB2. The CICS DB2 attachment facility is shipped with CICS Transaction Server and you must use this version of the attachment facility to connect a CICS region to DB2. Always use the correct attachment facility for the release of CICS under which a region is running.

Chapter 27. Upgrading SOAP web services

If you have used SOAP web services in earlier CICS releases, be aware of the following changes when you upgrade to CICS Transaction Server for z/OS, Version 5 Release 2.

- WEBSERVICE resources can now be defined and packaged in CICS bundles. The resource is dynamically installed in the CICS region when you install the BUNDLE resource. You can import a web service binding file and a WSDL document or WSDL archive file to be packaged with the resource definition, and for a service provider you can include a PROGRAM definition in the bundle. You can also use an existing WEBSERVICE definition in a CICS bundle to generate related URIMAP resources and alias transactions.

Data mapping

SOAP web services are enhanced to provide additional data mapping.

CICS now provides data mapping to support COBOL OCCURS DEPENDING ON and OCCURS INDEXED BY clauses.

- The OCCURS DEPENDING ON clause is supported at a mapping level of 4.0 or higher. Complex OCCURS DEPENDING ON is not supported. This limitation means that OCCURS DEPENDING ON is only supported for the last field of a structure.
- The OCCURS INDEXED BY clause is supported at any mapping level.

CICS now provides support for transforming application data encoded in UTF-16 at a mapping level of 4.0 or higher.

- You can enable this behavior by using language-specific data types for UTF-16 when you use the DFHLS2JS, DFHLS2SC, or DFHLS2WS assistants.
- You can enable this behavior by setting CCSID=1200 when you use the DFHJS2LS, DFHSC2LS, or DFHWS2LS assistants.

Chapter 28. Upgrading JSON web services

If you used JSON web services in earlier releases, be aware of the following changes when you upgrade to CICS Transaction Server for z/OS, Version 5 Release 2.

In previous releases support for JSON web services was provided by CICS TS Feature Pack for Mobile Extensions. In CICS TS 5.2 this function is incorporated into CICS, therefore there is no longer a requirement to install the feature pack.

JSON web services are enhanced to provide additional data mapping.

CICS now provides data mapping to support COBOL OCCURS DEPENDING ON and OCCURS INDEXED BY clauses.

- The OCCURS DEPENDING ON clause is supported at a mapping level of 4.0 or higher. Complex OCCURS DEPENDING ON is not supported. This limitation means that OCCURS DEPENDING ON is only supported for the last field of a structure.
- The OCCURS INDEXED BY clause is supported at any mapping level.

CICS now provides support for transforming application data encoded in UTF-16 at a mapping level of 4.0 or higher.

- You can enable this behavior by using language-specific data types for UTF-16 when you use the DFHLS2JS, DFHLS2SC, or DFHLS2WS assistants.
- You can enable this behavior by setting CCSID=1200 when you use the DFHJS2LS, DFHSC2LS, or DFHWS2LS assistants.

Upgrading the JSON web services assistant

In previous releases, the JSON assistant batch jobs DFHJS2LS and DFHLS2JS were provided as part of CICS TS Feature Pack for Mobile Extensions. These functions are now incorporated into CICS TS, so you must change any JCL that calls the assistant.

Procedure

1. Change the JCL procedure library where DFHJS2LS or DFHLS2JS are located. In CICS TS 5.2, these batch jobs are in the HLQ.XDFHINST library.
2. Review the values of the symbolic parameters **JAVADIR**, **PATHPREF**, and **USSDIR**. In CICS TS 5.2, you might not need to specify them at all, as the DFHJS2LS and DFHLS2JS procedures are customized by DFHISTAR. For more information about these parameters, see DFHJS2LS: JSON schema to high-level language conversion for request-response services and DFHLS2JS: High-level language to JSON schema conversion for request-response services.

Chapter 29. Upgrading SAML support

If you used Security Assertion Markup Language (SAML) support in earlier CICS releases, follow this procedure to upgrade to CICS Transaction Server for z/OS, Version 5 Release 2.

About this task

In previous releases, support for SAML was provided by CICS TS Feature Pack for Security Extensions V1.0. In CICS TS 5.2, this function is incorporated into CICS and the feature pack is not supported.

Procedure

1. Copy your STS configuration file to a new location on z/OS UNIX to use with the new CICS release.
2. Upgrade your `java.policy` file.

- a. If you are using a user `java.policy` file, copy it to a new location on z/OS UNIX to use with the new CICS release.

- b. Update the following rule to refer to the new CICS root directory.

```
:// All permissions granted to CICS codesource protection domain
grant codeBase "file://USSHOME/-" {
  permission java.security.AllPermission;
};
```

where *USSHOME* is the name and path of the root directory for CICS Transaction Server files on z/OS® UNIX.

- c. Remove the rule that applies to the feature pack files:

```
grant codeBase "file:fp_dir-" { permission java.security.AllPermission;
};
```

where *fp_dir* is the Feature Pack installation directory.

3. Upgrade your JVM profile by following the general instructions for upgrading JVM profiles, which are given in Chapter 24, "Upgrading the Java environment," on page 91. Perform the following additional steps:
 - a. Delete the `CLASSPATH_SUFFIX` line from your JVM server profile.
 - b. If you are using a user `java.policy` file, update the `java.security.policy` property to refer to the new location of this file.
4. When no CICS instances are using it, uninstall the feature pack.

Chapter 30. Upgrading platforms, applications, policies, and CICS bundles

If you have used platforms, applications, policies, and CICS bundles in CICS in earlier releases, be aware of the following changes when you upgrade to CICS Transaction Server for z/OS, Version 5 Release 2.

Requirements for application entry points and operation names

In CICS regions from CICS TS 5.2, applications that are deployed on platforms must have application entry points declared for all the resources that are an access point to the application. Application entry points are now used to control users' access to different versions of an application that is deployed on a platform. An application that defines a PROGRAM resource cannot be made available to callers in CICS TS 5.2 regions unless it declares an application entry point for that resource.

The resource for an application entry point does not have to be defined in the same CICS bundle as the application entry point. CICS adds the application operation to the specified resource when the application is installed. For PROGRAM resources that are declared as application entry points, the application entry point controls users' access to the program regardless of the location of the PROGRAM resource. However, for URIMAP resources that are declared as application entry points, the application entry point only controls access to the URIMAP resource if it is declared in the same CICS bundle where the URIMAP resource is defined.

You can declare an application entry point for a resource that is not defined in any CICS bundle, but already exists in the CICS regions where the bundle will be deployed. You can also declare an application entry point for a PROGRAM resource that can be autoinstalled in the CICS regions where the bundle will be deployed. When you install an application, if the resource targeted by an application entry point is not present and cannot be autoinstalled, the CICS bundle containing the declaration of the application entry point does not install and is marked with a warning.

CICS bundles that are installed as part of platform bundles, or added to a running platform, must not contain declarations of application entry points in the bundle manifest. Application entry points are not supported for CICS bundles installed directly on platforms, and CICS does not enable the application entry points in this situation, although the CICS bundle and its resources are installed. Standalone CICS bundles that are installed directly in CICS regions can contain declarations of application entry points to enable scoping of region level policies.

Application entry points only control users' access to the resources that are specified in the application entry points. If an application includes any public resources that are not named as application entry points, when the application is installed and enabled, these resources can be accessed by other applications installed on the platform or in the CICS region regardless of the availability status of the application. Private resources for an application version cannot be accessed by other applications.

Each application entry point names an operation. For example, you could declare application entry points for create, read, update, or delete operations in the application. In CICS regions from CICS TS 5.2, an operation name must now be unique within an application. An application cannot be made available to callers in CICS TS 5.2 regions if it contains duplicate operation names. Operation names are case sensitive, so you may use operation names that are differentiated only by case, such as “browse” and “Browse”.

Making applications and CICS bundles available

A new availability status has been introduced for applications that are deployed on platforms, so that you can install and verify installation of an application version before making the application version available to users of the platform.

Applications that are deployed on platforms therefore now require an additional step to make them available for users in CICS regions from CICS TS 5.2. After installing and enabling the application, you must perform the **Make Available** action in the CICS Explorer to make the application available to users.

You can make an installed application version available or unavailable in the Cloud Explorer view, or in the online application editor for installed applications. Making an application available makes the application entry points, and therefore the resources for the application, available to callers. For more details, see “Multi-versioning for applications deployed on platforms” on page 113.

Standalone CICS bundles must also be made available in CICS regions from CICS TS 5.2 if they contain application entry points. After installing and enabling the CICS bundle, you can perform the **Make Available** action in the CICS Explorer, or use the new AVAILSTATUS option on the **EXEC CICS SET BUNDLE** command to set the status of the CICS bundle to AVAILABLE.

Before you disable or discard an application that is deployed on a platform in CICS regions from CICS TS 5.2, you must perform the **Make Unavailable** action in the CICS Explorer. Before you disable or discard a standalone CICS bundle that contains application entry points, you must perform the **Make Unavailable** action in the CICS Explorer, or use the AVAILSTATUS option on the **EXEC CICS SET BUNDLE** command to set the status of the CICS bundle to UNAVAILABLE.

If your platform includes any CICS regions that are still at CICS TS 5.1, the **Make Available** and **Make Unavailable** actions are not required or supported for applications or standalone CICS bundles installed in those CICS regions. In CICS TS 5.1 regions, applications or standalone CICS bundles are assumed to be available when they have been enabled using the **Enable** action, and unavailable when they have been disabled using the **Disable** action, as was the case for all applications in CICS TS 5.1.

The availability status of an application version is not applied at the start of a CICS region that is defined as part of a platform, and it is not recovered during a restart of a CICS region. The CICS bundles for all application versions are in an unavailable state in a started or restarted CICS region. Use the Cloud Explorer view in the CICS Explorer to make the appropriate version of the application available.

CICS bundles that are deployed with platform bundles, or added to a platform, do not require the **Make Available** and **Make Unavailable** actions, because these actions are performed on the application entry points for applications.

Changes to resources defined in CICS bundles

You can now create resource definitions in CICS bundles for the additional CICS resource types FILE, JVMSERVER, PIPELINE, TCPIPService, and WEBSERVICE. You can issue commands to change the status of dynamically generated JVMSERVER and TCPIPService resources. A URIMAP resource defined in a CICS bundle can be specified as an application entry point to control access to the service that it provides.

You use new wizards in the CICS Explorer to define FILE, JVMSERVER, PIPELINE, TCPIPService, and WEBSERVICE resources in CICS bundles.

When you define resources in CICS bundles, they can be packaged, deployed, and managed as part of applications on a platform. You can also deploy the CICS bundles at the level of the platform, to provide services to all the applications on the platform, or you can install them as standalone CICS bundles in CICS regions that are not part of a platform.

The full list of CICS resource types for which you can create resource definitions in CICS bundles is as follows:

- FILE
- JVMSERVER
- LIBRARY
- PIPELINE
- PROGRAM
- TCPIPService
- TRANSACTION
- URIMAP
- WEBSERVICE

For the list of all artifacts that you can define and deploy in CICS bundles, including OSGi bundles and events, see *Artifacts that can be deployed in bundles* in *Administering*.

Some characteristics of CICS resources change because they are defined in a CICS bundle and dynamically created as part of a bundle deployment.

FILE resources

The following file types are supported for definition in CICS bundles:

- VSAM files (including files that refer to CICS-maintained, user-maintained, and coupling facility data tables, as well as files that refer to VSAM data sets)
- Remote VSAM files
- Remote BDAM files

The initial status of a FILE resource that is dynamically created from a CICS bundle is derived from the initial status of the CICS bundle that defines the resource. As a result, it is not possible to define a FILE resource with a STATUS of UNENABLED to inhibit the implicit opening of files by applications.

The PASSWORD attribute is not supported for dynamically created FILE resources.

JVMSERVER resources

For JVM servers that are packaged in CICS bundles, the JVM profiles are packaged with the resource definitions in the CICS bundles. You can therefore install the JVM server in any CICS region without needing to set up a JVM profile in the local JVM profile directory for the CICS region.

When creating a JVM server, you can create the JVM profile using sample templates for an OSGi JVM server, an Axis2 JVM server, or a Liberty JVM server, or import an existing JVM profile to the CICS bundle from elsewhere in the workspace or from the local file system.

The set of acceptable characters in the JVM profile name is more restricted when the JVMSERVER resource is defined in a CICS bundle. For details, see JVMSERVER attributes.

A JVM server that is defined in a CICS bundle must be installed and enabled before you install OSGi bundles or other application artifacts for Java applications that run in it. It is good practice to deploy a CICS bundle containing the definition for a JVMSERVER resource as part of a platform bundle, and to then deploy the CICS bundles containing OSGi bundles or other Java application artifacts as part of applications that are deployed on the platform. This architecture ensures that when the resources are first installed in a CICS region or if the CICS region is restarted, the JVM server and the Java application resources are installed and enabled in the correct order.

PIPELINE resources

For pipelines that are packaged in CICS bundles, the pipeline configuration files are also packaged with the resource definitions in the CICS bundles. You can create a pipeline configuration file using one of the CICS-supplied sample pipeline configuration files, or import an existing pipeline configuration file from the local file system.

If a PIPELINE resource is packaged in a CICS bundle, it should be deployed as part of a platform for hosting WEBSERVICE resources that are defined using CICS bundles. PIPELINE resources that are defined in CICS bundles can only be used with WEBSERVICE resources that are defined in CICS bundles or created dynamically by a pipeline scan. WEBSERVICE resources defined using the CICS CSD or BAS are not compatible with PIPELINE resources that are defined in CICS bundles.

A PIPELINE resource that is packaged in a CICS bundle must be installed and enabled before you install the WEBSERVICE resources that require it. It is good practice to deploy a CICS bundle containing the definition for a PIPELINE resource as part of a platform bundle, and to then deploy the CICS bundles containing WEBSERVICE resources as part of applications that are deployed on the platform. This architecture ensures that when the resources are first installed in a CICS region or if the CICS region is restarted, the PIPELINE resource and the WEBSERVICE resources are installed and enabled in the correct order.

A PIPELINE resource that is defined in a CICS bundle can specify a WSDIR attribute, but this is discouraged. The SHELF attribute is not used for PIPELINE resources that are defined in CICS bundles.

WEBSERVICE resources

For web services that are packaged in CICS bundles, you can import a web service binding file and a WSDL document or WSDL archive file to be packaged in the bundle along with the resource definition. To support the web service, you can use a WEBSERVICE definition packaged in a CICS bundle to generate a URIMAP definition in a separate bundle. You can also create an alias transaction for the URI map, and an optional URIMAP definition for WSDL discovery.

Web services that are packaged in CICS bundles have additional states of **DISABLING** and **DISABLED**, which do not apply to web services created using other methods. When disabling is in progress for a CICS bundle, WEBSERVICE resources defined in the bundle enter **DISABLING** state. Work that is currently executing is allowed to complete, but the web service does not accept new work. When the web service is no longer in use, the WEBSERVICE resource enters **DISABLED** state. Requests to a web service in **DISABLING** or **DISABLED** state are rejected and a SOAP fault, “Web service is not in service”, is sent. If CICS is the web service requester, the **INVOKE SERVICE** command returns a **RESP** code of **INVREQ** and a **RESP2** value of 8.

If the CICS bundle is enabled again, the WEBSERVICE resource returns to **INSERVICE** state. Otherwise, the WEBSERVICE resource can be discarded by discarding the CICS bundle. You can inquire on the state of a WEBSERVICE resource using the **EXEC CICS** or **CEMT INQUIRE WEBSERVICE** command, the CICSplex SM web user interface, or the CICS Explorer, but you cannot set it manually.

Direct access to bundle resources

You can now issue commands to change the status of certain CICS resources that are defined in a CICS bundle and dynamically generated in the CICS region. With this function, in a situation that requires immediate removal of a resource, you can force completion of the disable process when the resources are still in use.

With the default disable process, **FILE**, **JVMSEVER**, and **TCPIP SERVICE** resources are not disabled until all the current tasks have finished using them. When these resources are defined in a CICS bundle, you must first disable the CICS bundle or the application with which it is deployed. If the disable process does not complete, because the resource is still in use, you can now take the following actions:

- For a **JVMSEVER** resource, if you want to disable the JVM server immediately and purge the tasks that are running in it, you can use the **SET JVMSEVER PURGE**, **FORCEPURGE**, or **KILL** command on the dynamically generated resource in the CICS region. You can also perform this action in CICS Explorer.
- For a **TCPIP SERVICE** resource, if you want to disable the service immediately and close all the connections, you can use the **SET TCPIP SERVICE IMMCLOSE** command on the dynamically generated resource in the CICS region. You can also perform this action in CICS Explorer.
- If you are experiencing a problem with disabling a CICS bundle that defines a **FILE** resource, you may issue the **EXEC CICS SET FILE DISABLED** or **EXEC CICS SET FILE CLOSED** command with the **FORCE** option, or the **CEMT SET FILE FORCECLOSE** command, against the dynamically generated resource, if this action is required. CICS also issues message **DFHFC6043** when you have attempted to disable a file defined in a CICS bundle, but the file is still in use, or there is a retained lock on the file.

Follow the troubleshooting procedure in Diagnosing application errors to diagnose the problem and take suitable action.

The **EXEC CICS SET BUNDLE** command also has a new option **AVAILSTATUS** to make available or unavailable an individual CICS bundle that contains application entry points. This action is normally performed using the CICS Explorer at the level of the application that packages the CICS bundle, but you can use the command to operate directly on the individual CICS bundle.

URIMAP resources as application entry points

When you define a URIMAP resource in a CICS bundle, you can use an application entry point declaration to control users' access to the service provided by the URIMAP resource. For this function, declare the application entry point and define the URIMAP resource in the same CICS bundle. In this case, when you install and enable the application, the service provided by the URIMAP resource is not yet available to callers. When you choose to provide the service to users, you make the CICS bundle containing the application entry point and the URIMAP resource available using the CICS Explorer. This action makes the application entry point, and therefore the service provided by the URIMAP resource, available to callers.

If you do not want the application entry point to control access to the service provided by the URIMAP resource, declare the application entry point and define the URIMAP resource in different CICS bundles. You can also declare as an application entry point a URIMAP resource that is defined outside the application and declared as a dependency, or import, for the application. In either of these cases, the service becomes available to users as soon as you install and enable the URIMAP resource.

Private resources for application versions on platforms

When you define certain CICS resources in CICS bundles as part of an application installed on a platform, the resources are private to that version of that application. You can therefore install more than one resource of those types with the same name, at the same time.

This facility avoids resource name clashes between applications that were developed independently, but used the same resource names. The requirement for unique resource names for the supported CICS resources can be removed by managing the resources as part of applications deployed on a platform. You can use this process to assist with server consolidation.

For supported resource types, a CICS resource is private if the resource is defined in a CICS bundle that is packaged and installed as part of an application, either as part of the application bundle, or as part of the application binding. When you create a CICS resource in this way, the resource is not available to any other application or version installed on the platform, and it is not available to other applications in the CICS region. It can only be used by the version of the application where the resource is defined. These resources are known as private resources.

The following CICS resources are supported as private resources for applications:

- **LIBRARY** resources, which represent one or more data sets, known as dynamic program **LIBRARY** concatenations, from which program load modules can be loaded.

- POLICY resources, which represent one or more rules that manage the behavior of user tasks in CICS regions.
- PROGRAM resources, which represent an application program. A program that is auto-installed by a task for an application that is deployed on a platform is also private to that version of the application.

CICS resources of other resource types that are defined as part of applications, and CICS resources that are defined by any other methods, are publicly available for all tasks. These resources are known as public resources. In applications that have only a single version, private resources that are declared as application entry points become public resources when the application entry point is made available. For multi-versioned applications, if the application is the highest available version, a program that is declared as an application entry point is public. The programs that are declared as application entry points for the other versions of the same application are private.

If you do not want a resource of the supported resource types to be private, do not package the resource definition as part of an application. Instead, define the CICS resource using a standalone CICS bundle, a CICS bundle that is installed at the level of a platform, the CICS CSD, or the CICSplex SM data repository. If an application requires the CICS resource to be available in the CICS region, add the resource as a dependency for the application or the application binding, in an `<import>` element of the bundle manifest.

Policies, which are not a CICS resource, have the same support as private resources when they are defined in a CICS bundle that is deployed as part of an application. You can therefore use policies with the same name in different applications and application versions.

Managing private resources in CICS bundles

When you make changes to an application, you use the CICS Explorer to modify the relevant elements of the application that are packaged in CICS bundles, apply a new version number to those CICS bundles to identify the change, and then reversion and reinstall the application. You leave any unmodified CICS bundles at the same version number as before, because CICS manages the process of multiple installations of CICS bundles with the same ID and version number.

Reinstallation of unmodified CICS bundles is only available for CICS bundles that are installed as part of an application deployed on a platform. Standalone CICS bundles cannot be reinstalled if they are already installed with the same ID and version, or in the case of CICS bundles created in releases before CICS TS 5.1, installed with no ID and version. However, the same CICS bundle can be installed in CICS regions as a standalone CICS bundle, and also installed and reinstalled as part of one or more applications deployed on a platform.

Special CICS messages are issued when actions such as installing and discarding are performed on private resources. The messages provide the same information as for the corresponding actions on public resources of that type, but they also state the platform, application, and application version to which the private resource applies, so that you can audit or troubleshoot the actions in the relevant context.

To view the private resources for each installed version of an application, use the CICS Explorer. In the online application editor, you can view the private resources and the application entry points for the application by resource type, and filter them by CICS region or by CICS bundle to help locate particular resources. You

can also view the DD names that z/OS has generated for the LIBRARY concatenation of data sets for private LIBRARY resources.

You can inquire on or browse private resources using the **EXEC CICS INQUIRE** system programming command for the resource type. By default, CICS searches for the resources that are available to the program where the **EXEC CICS INQUIRE** command is issued. You can also choose to browse private resources for a specified application.

To support private resources in CICSplex SM's real-time analysis (RTA) function, you must specify the application context parameters PLATFORM, APPLICATION, APPLMAJORVER, APPLMINORVER and APPLMICROVER in the evaluation definition (EVALDEF) for the resource. For instructions to create and maintain real-time analysis definitions using user-defined CICSplex SM WUI views and resource objects, see Real-time analysis.

CICS produces separate statistics records for private resources. A statistics record for a private resource has information about the application for which the resource was defined. The statistics DSECTs and DFHSTUP reports for public program and library resources have corresponding DSECTs and DFHSTUP reports for private resources. Programs that are declared as application entry points are identified and reported in both the public and private statistics, because, while the entry point is publicly accessible, it is also part of the application.

Private LIBRARY resources in CICS bundles

LIBRARY resources represent one or more data sets, known as dynamic program LIBRARY concatenations, from which program load modules can be loaded. The LIBRARY resource is supported as a private resource for an application version. Each version of an application should include at least one private LIBRARY resource representing the version-specific data sets containing the load modules for the application.

If any of the private LIBRARY concatenations for an application are disabled, because the CICS bundle that defines the relevant LIBRARY resource is disabled, CICS does not search any other private LIBRARY concatenations, or any public LIBRARY concatenations that are defined for the whole CICS region. All subsequent program loads by the application therefore fail until the CICS bundle that defines the LIBRARY resource is enabled.

For a private LIBRARY resource that is defined in a CICS bundle that is packaged and installed as part of an application bundle or application binding bundle, the name of the LIBRARY resource is not used as the DD name for the LIBRARY concatenation of data sets. Instead, CICS requests a unique DD name for the LIBRARY concatenation of data sets when the application is installed on the platform. The resource name can therefore be the same as LIBRARY names used elsewhere in the installation, or by different versions of the application. CICS issues message DFHLD0518 to state the DD name that z/OS has generated for the LIBRARY concatenation. You can also view the data set names for an installed application in the CICS Explorer.

Private PROGRAM resources in CICS bundles

A PROGRAM resource represents a program load module that is stored in the program library. The PROGRAM resource is supported as a private resource for an

application version. A program that is auto-installed by a task for an application that is deployed on a platform is also private to that version of the application.

Only one copy of each version of each program is loaded in CICS storage. Before loading a private program, CICS checks whether that version of the program has already been loaded from the same data set (PDS or PDSE) with a matching PROGRAM resource definition. If so, CICS uses the existing copy. The following rules therefore apply when you are reusing PROGRAM resource names:

- Multiple applications that are intended to share the same program loaded from the same PDS or PDSE must use the same attributes in the PROGRAM resource definition.
- If multiple applications use the same name for different program resources, each application must load the programs from a different data set (PDS or PDSE).

If you specify **RELOAD=YES** in the PROGRAM resource definition for a private program, its behavior for program loading changes to be the same as for a public program. A program control link, load, or XCTL request brings a fresh copy of the program into storage. RELOAD(YES) programs cannot be reused, and they cannot be shared by multiple applications. Each of the program copies must be removed from storage explicitly, using a storage control FREEMAIN request, when it is no longer required and before the transaction terminates.

If a program that is required by an application is not found in the private program directory for the application, CICS searches the public program directory.

Programs that are declared as an application entry point must have a unique PROGRAM resource name in your environment. To enable these programs to be called from outside the application, they must be public resources. When you make an application available that contains an application entry point for a private PROGRAM resource, the PROGRAM resource that is named as the application entry point changes from a private resource to a public resource. Only one instance of a public resource with a particular name can exist in a CICS region. The PROGRAM resource therefore cannot have the same name as a public program that is installed in the CICS region, or the same name as a public program that is defined as an application entry point by a different installed application. However, multiple versions of the same PROGRAM resource defined as an application entry point can be installed for multiple versions of the same application, because CICS manages the promotion of PROGRAM resources to public status for the versions of an application.

Multi-versioning for applications deployed on platforms

You can now install and manage multiple versions of an application at the same time on the same platform instance. New versions of an application can be deployed to the platform without the need to disable or remove the previous version. When you have installed and enabled a version of an application, you take an additional step to make it available to users.

Applications deployed on platforms that use the CICS resources that are supported as private resources, in combination with other resources designed for applications and with imported resources, are eligible for multi-versioning. The following resources are supported as part of multi-versioned applications:

- PROGRAM resources defined in CICS bundles that are part of the application
- LIBRARY resources defined in CICS bundles that are part of the application
- Policies

- Statements of application entry points
- Any resource that is defined as a dependency, or import, for the application

For more details about the CICS resources that are supported as private resources, see Private resources for application versions in Configuring.

Other resources may be involved with multi-versioned applications if you manage the resources appropriately to avoid resource name clashes between different versions of the application. For example, a URIMAP resource that is part of an application can be renamed when packaging and installing a new version of the application. Or an application can be architected so that a resource not supported for multi-versioning is managed outside the application, but declared as a dependency, or import, for the application. For resources that are, or could be, used by different applications, such as JVMSERVER resources, deploy and manage the resource at the level of the platform, where it can be used by any version of any application deployed on the platform.

Applications that are eligible for multi-versioning benefit from more sophisticated management capabilities:

- You can install multiple versions of the application, at the same time, on the same platform instance.
- New versions of an application can be deployed to the platform and phased in without the need to remove the previous versions.
- You can install and verify installation of an application version before making the application version available to users of the platform.
- Users can be moved over to a new version of the application without a break in service, and quickly moved back to another version if necessary.
- Programs that are not aware of multi-versioning automatically link to the highest version of the application that you have made available on the platform.
- Programs can exploit multi-versioning by invoking any available version of the application using the INVOKE APPLICATION command.

You control users' access to the resources in a multi-versioned application by declaring application entry points. PROGRAM and URIMAP resources can be declared as application entry points, which can be set as available or unavailable to users. With application entry points, you can install the application and its resources in the CICS regions in the platform, then enable them to verify the installation. When you choose to provide the service to users, you make the application entry points, and therefore the resources that they control for the application, available to callers.

You can use the CICS Cloud perspective in the CICS Explorer to view, update, and remove all the versions of an application that are deployed on a platform. You can open an installed application version in the online application editor to view more details about it, including the private resources and application entry points for the application. You can make available or unavailable, enable or disable, and install or discard an installed application version in the Cloud Explorer view, and you can also modify its state in the online application editor for installed applications.

Application context enhancements

You can now use the application context of the current application set onto the task instead of the initial application context of the first application set onto the task.

A task may pass through one or more applications as it executes. Each task can have up to two application contexts associated with it at any time:

- The **initial** application context of a task is used for monitoring and measuring how much resource an application or a particular application operation is using across CICS regions and multiple tasks. The initial application context can be used when applying a policy to tasks that are part of an application, to define threshold conditions to manage the behavior of the tasks. The initial application context can be inherited from an invoking task, or set when the task first passes through an application entry point.
- The **current** application context of a task is used for loading private libraries and WLM user exits. The current application context can be queried using XPI, SPI, and API calls. The current application context changes each time the task passes through an application entry point.

The initial or current application context can be used with the transaction tracking capability in the CICS Explorer to quickly identify and diagnose application-related problems. Both the initial and the current application contexts are propagated from task to task.

The behaviour when a CICS TRANSACTION names an initial program that is an entry point, is changed from CICS TS 5.1. When issuing EXEC CICS START TRANSACTION, where the initial program named on the started transaction is an entry point, the application context is not passed from the issuing task to the newly started task.

The TASK base table and the HTASK base tables contain the initial application context values, the TASKASSC base table contains the current application context values.

The behavior of the EXEC CICS INQUIRE ASSOCIATION, EXEC CICS ASSIGN, and XPI - INQUIRE_APP_CONTEXT commands are changed to refer to the current application context. You can also use the new JCICS Task.getApplicationContext() method to return the current application context.

For more information, see Application context in Product overview.

New policy rule types and rule items

Some new policy rule types and rule items are available to help you manage the run time behavior of your CICS applications and platforms.

New policy rule types

The following new policy rule types are now available to take an automatic action if a specified threshold is exceeded:

Table 16. New policy rule types

New policy rule type	Policy rule items
Start request Used to define a threshold for the number of EXEC CICS START requests issued by a user task.	START command The START command rule item allows a user to define a threshold for the number of EXEC CICS START requests issued by a user task.

Table 16. New policy rule types (continued)

New policy rule type	Policy rule items
Syncpoint request Used to define a threshold for the number of EXEC CICS SYNCPOINT and SYNCPOINT ROLLBACK requests issued by a user task.	SYNCPOINT command The SYNCPOINT command rule item allows a user to define a threshold for the number of EXEC CICS SYNCPOINT and SYNCPOINT ROLLBACK requests issued by a user task.
TD Queue request Used to define a threshold for the number of EXEC CICS READQ and WRITEQ TD requests issued by a user task.	READQ TD command The READQ TD command rule item allows a user to define a threshold for the number of EXEC CICS READQ TD requests issued by a user task to either intrapartition or extrapartition transient data queues. WRITEQ TD command The WRITEQ TD command rule item allows a user to define a threshold for the number of EXEC CICS WRITEQ TD requests issued by a user task to either intrapartition or extrapartition transient data queues.
TS Queue bytes Used to define a threshold for the amount of data written to temporary storage by EXEC CICS WRITEQ TS requests issued by a user task.	WRITEQ TS command The WRITEQ TS command rule item allows a user to define a threshold for the total amount of data that is written to both auxiliary and main temporary storage queues by a user task. WRITEQ TS auxiliary command The WRITEQ TS auxiliary command rule item allows a user to define a threshold for the total amount of data that is written to auxiliary temporary storage queues by a user task. WRITEQ TS main command The WRITEQ TS main command rule item allows a user to define a threshold for the total amount of data that is written to main temporary storage queues by a user task.

Table 16. New policy rule types (continued)

New policy rule type	Policy rule items
TS Queue request Used to define a threshold for the number of EXEC CICS READQ and WRITEQ TS requests issued by a user task.	READQ TS command The READQ TS command rule item allows a user to define a threshold for the number of EXEC CICS READQ TS requests issued by a user task to both auxiliary and main temporary storage queues. WRITEQ TS command The WRITEQ TS command rule item allows a user to define a threshold for the number of EXEC CICS WRITEQ TS requests issued by a user task to both auxiliary and main temporary storage queues. WRITEQ TS auxiliary command The WRITEQ TS auxiliary command rule item allows a user to define a threshold for the number of WRITEQ TS requests issued by a user task to auxiliary temporary storage queues. WRITEQ TS main command The WRITEQ TS main command rule item allows a user to define a threshold for the number of WRITEQ TS requests issued by a user task to main temporary storage queues.

New policy rule items for existing policy rule types

The following new policy rule items are available for existing policy rule types:

Table 17. New policy rule items

Policy rule type	New policy rule items
Time	Elapsed limit Used to define a threshold for a user task's elapsed time.

For more information about policies, see Policies in Product overview.

Part 3. Changes to CICSplex SM externals

CICSplex SM views and functions have changed to support the changes in function for this release of CICS and CICSplex SM. Check which changes might affect your system.

Chapter 31. Changes to CICSplex SM installation and definition

Changes to CICSplex SM installation, initialization parameters, resource definition, or setup are summarized here.

Change to generic alert structures used by CICSplex SM

When you upgrade to a new version of CICS TS, there is a change to SNA generic alerts and resolutions as they are used by CICSplex SM.

“Product Set ID” (X'10') MS common subvector is a “Product ID” (X'11') common subvector that identifies the product as IBM Software (X'04'). It contains a “Product Number” (X'08') Product ID subfield that identifies the product number. In CICS Transaction Server for z/OS, Version 5, this product number has changed to 5655Y04.

The previous product numbers were as follows, depending on the version of CICS TS from which you are upgrading:

- In CICS Transaction Server for z/OS, Version 2, the product number was 5695081.
- In CICS Transaction Server for z/OS, Version 3, the product number was 5655M15.
- In CICS Transaction Server for z/OS, Version 4, the product number was 5655S97.

Chapter 32. Changes to CICSplex SM views and resource tables

These changes affect CICSplex SM views, resource tables, and Business Application Services definition objects.

Changed CICSplex SM views and resource tables

A number of changed CICSplex SM views and resource tables now support new or changed CICS resource types and functions.

Changed CICSplex SM views

Table 18. Changed CICSplex SM views

Changed CICS resource type or function	Corresponding CICSplex SM views that have changed
WEBSERVICE resources in CICS bundles	1. CICS operations views > TCP/IP service operations views > Web services

Changed CICSplex SM resource tables

Review the following resource tables for possible effects on any RTA evaluation definitions (EVALDEF) or CICSplex SM API programs that you are using:

- APACTV
- APPLCTN
- BUNDLE
- BUNDPART
- LIBDSN
- LIBRARY
- MGMPART
- PIPELINE
- PROGRAM
- RTAACTV
- URIMAP
- WEBSERV

New CICSplex SM views and resource tables

New CICSplex SM views and resource tables support CICS resource types and functions.

New views and resource tables by functional area

Table 19. New CICSplex SM views and resource tables

Resource type or function	CICSplex SM views	CICSplex SM resource tables
Installed analysis definitions associated with an analysis point specification	Real Time Analysis (RTA) views > Installed analysis definitions associated with an analysis point specification	APACTV
Real Time Analysis (RTA) installed analysis and status definitions	Real Time Analysis (RTA) views > Real Time Analysis (RTA) installed analysis and status definitions	RTAACTV

Chapter 33. Programs that connect to a previous release of CICSplex SM

CICSplex SM API programs that use the CONNECT verb specifying a VERSION keyword for a previous release of CICSplex SM can experience significant increases in both CPU consumption by the CMAS address space and data space storage use by the Environment Services System Services (ESSS) address space.

API programs that specify a CRITERIA string to limit the size of a result set on a GET or PERFORM OBJECT request, or use the SPECIFY FILTER verb, can experience the increase in CMAS CPU and ESSS storage. Batch job run times might also increase.

You are not required to recompile your CICSplex SM API programs when you upgrade to the new release. However, if you do not recompile affected programs, the CMAS has to convert the records from the current release format to the level specified on the VERSION keyword on the CONNECT verb. This transformation process is highly intensive for CPU and storage when the result set is very large, for example, 300,000 to 500,000 records. The increases are observed in most cases when a criteria string is used to filter the result set; for example, specifying a criteria for the PROGRAM object using the NAME key for a specific or generic program. In this case, CICSplex SM has to retrieve all program objects and return them to the CMAS where the API is connected, transform the records to the version of the API, and then apply the filtering.

If you recompile your programs to specify the VERSION keyword to match the current release of CICSplex SM, this conversion does not take place, and storage and CPU consumption do not increase significantly.

Part 4. Upgrading CICSplex SM

To upgrade CICSplex SM to the CICS Transaction Server for z/OS, Version 5 Release 2 level, carry out the tasks described here. Also check the important information here about the compatibility of CICSplex SM with previous releases of CICS Transaction Server.

Make sure that you complete all your upgrades to CICS TS for z/OS, Version 5.2 CICSplex SM, including your CMAS, all MASs that are connected to it, and all MASs that act as Web User Interface servers for it, before you restart CICSplex SM.

Several skeleton postinstallation members are distributed with CICSplex SM. You must generate these postinstallation members for use during the upgrade. For information about generating the postinstallation members, see CICS Transaction Server for z/OS Installation Guide.

So that you can revert to the previous release of CICSplex SM if you encounter problems during the upgrade to CICS TS for z/OS, Version 5.2 CICSplex SM, take backup copies of the previous release components such as JCL, CLISTs, CICS tables, CMAS data repositories, and WUI repositories before you start the upgrade process.

Chapter 34. Conditions for running CICSplex SM Version 5.2 and earlier releases concurrently

You can run CICSplex SM Version 5.2 and earlier releases concurrently, but you must take account of a number of conditions for compatibility.

The CICSplex SM releases referred to in this information are the CICSplex SM element of CICS Transaction Server for z/OS releases. They are not available as separate products. For example, CICSplex SM Version 5.2 is the CICSplex SM element of CICS Transaction Server for z/OS, Version 5 Release 2.

You can run CICSplex SM Version 5.2, Version 5.1, Version 4.2, Version 4.1, Version 3.2, and Version 3.1 at the same time, with interconnected CMASs at different levels. The ability to do this allows gradual upgrading of the environment to Version 5.2. However, in CICS TS for z/OS, Version 5.2, a CICSplex SM CMAS will run only in a CICS system at Version 5.2.

CICS systems (MASs) running the following supported CICS releases can be connected to CICSplex SM Version 5.2:

- CICS TS for z/OS, Version 5.2
- CICS TS for z/OS, Version 5.1
- CICS TS for z/OS, Version 4.2
- CICS TS for z/OS, Version 4.1
- CICS TS for z/OS, Version 3.2
- CICS TS for z/OS, Version 3.1

To be connected to CICSplex SM Version 5.2, CICS systems must use the CICSplex SM Version 5.2 MAS agent, so they must have the CICSplex SM Version 5.2 libraries in their CICS JCL. For a CICS system running CICS TS for z/OS, Version 3.1, you must also apply the compatibility APAR PK17360 to the CICS system.

If you have difficulty running CICSplex SM with CICS TS for z/OS, Version 3.2 because of a recursive 0c4 protection exception in module DFHMSMR, apply PTF UK43094 for apar PK77484 and restart the system.

If you have any CICS systems at the release levels listed here that are connected to an earlier release of CICSplex SM, you are recommended to migrate them to the current release of CICSplex SM to take full advantage of the enhanced management services.

If you want to manage CICS systems at an earlier release level than those listed here, connect them to a CMAS running at an earlier release level that supported those systems. This CMAS can be connected to your CICSplex SM Version 5.2 CMAS, so that the older CICS systems are indirectly connected to the Version 5.2 CMAS.

The following conditions apply to environments in which CICSplex SM Version 5.2 and earlier releases of CICSplex SM are running concurrently:

- For a CMAS and a MAS (including those MASs that act as Web User Interface servers) to communicate, they must be running at the same release of CICSplex SM.

- A CMAS running at Version 5.2 can be connected to a CMAS running at Version 5.2, Version 5.1, Version 4.2, Version 4.1, Version 3.2, or Version 3.1.
- In a CICSplex that consists of CMASs at the Version 5.2 level and at one or more earlier levels, the maintenance point CMAS must be at the Version 5.2 level. So, when a CICSplex contains CMASs at more than one level, the first CMAS upgraded to Version 5.2 must be the maintenance point.
- If you are using the API or Web User Interface to manage MASs connected to a CMAS at an earlier release, you must ensure that the MASs are managed indirectly from the Version 5.2 CMAS:
 - All WUI servers must connect to the Version 5.2 CMAS.
 - All API programs must run in such a way that they are connected to the Version 5.2 CMAS. This requirement applies only if the API program accesses new fields or later-level CICS systems. If the API program connects to an earlier-level CMAS, any resource tables that contain new or updated fields for the new release are not returned to the API program connected to the earlier release level CMAS.
- You cannot view all resources of a CICS TS for z/OS, Version 5.2 region using a CMAS running at an earlier release.
- A WUI server at an earlier release that is connected to a CMAS at an earlier release can retrieve data from a MAS connected to a Version 5.2 CMAS if the CMAS participates in the management of the CICSplex. However, the WUI server cannot retrieve data about resource types that were not available in the earlier release.
- If you want to create any of the following CICSplex SM objects, you must create them using a WUI server that is running at the same CICSplex SM release level as the maintenance point CMAS:
 - CPLEXDEF (CICSplex definition)
 - CMTCMDEF (CMAS to CMAS link definition)
 - CSYSGRP (system group definition)
 - PERIODEF (time period definition)
 - MONSPEC (monitor specification)
 - MONGROUP (monitor group)
 - MONDEF (monitor definition)
 - RTAGROUP (RTA group)
 - RTADEF (RTA definition)
 - WLMSPEC (WLM specification)
 - WLMGROUP (WLM group)
 - WLMDEF (WLM definition)
 - TRANGRP (transaction group)

If you use the API or the BATCHREP batched repository-update facility to create these objects, CICSplex SM and the maintenance point CMAS release level must, again, be at the same release level.

- If you are using workload management, to use the unit of work (UOW) affinities introduced in CICS TS for z/OS, Version 4.2, the CMAS that owns the workload must be at the Version 4.2 level or later.

Workload function is controlled by the CMAS that owns a workload. The workload owner is assigned to the CMAS that manages the first started TOR that causes the workload to be initialized. If the workload is not shown as ACTIVE, the first started TOR associated with the workload will cause its associated CMAS to be the workload owner. If the workload owning CMAS is

not at the Version 4.2 level or later, any UOW affinity definitions cannot be honored, which means that affinities will not be correctly created and obeyed, and will be denied to any other CMASs that subsequently join the workload, even if those CMASs are at the Version 4.2 level or later.

To ensure that UOW affinities can be exploited by a workload, ensure that the existing workload is cloned to a new name, and that any required UOW affinity definitions are applied to the new name. You must then ensure that the first TOR that is started for the new name is at the Version 4.2 level or later. This will cause UOW affinities to be honoured by any other region joining the workload name that is at the Version 4.2 level or later. If any regions that are at earlier release levels join the workload, they are not able to use the UOW affinity function, and must continue to make routing decisions on the basis of the standard workload routing algorithms.

If you believe that your defined UOW affinities are not being implemented, use the **System ID of workload owner** hyperlink in any of the WUI workload runtime views to determine the CICSplex SM version of the workload owning CMAS. If the CPSM version of CMAS attribute is not at least at the 0420 level, the workload is not capable of exploiting any defined UOW affinities.

Chapter 35. Upgrading CICSplex SM API programs

CICSplex SM API programs that were written to run in a MAS at a previous release can be run in a Version 5.2 MAS.

You can either continue to access the data provided by the previous release or access the new data available from Version 5.2. For information about using API programs with different releases of CICSplex SM, see the *CICSplex System Manager Application Programming Guide*.

New EYUDA values

The following new EYUDA general values are added for the CICSplex SM API:

- AVAILABLE (778)
- UNAVAILABLE (779)
- SOMEAVAIL (780)

Chapter 36. Upgrading a CMAS

You must upgrade your CICSplex SM CMAS to Version 5.2 at the same time as you upgrade the CICS system on which it runs. A CICSplex SM CMAS runs only in a CICS system of the same release level. During startup, the CMAS checks the CICS release level and stops with message EYUXL0142 if the release does not match.

Before you begin

In a CICSplex that consists of CMASs at the Version 5.2 level and at one or more earlier levels, the maintenance point CMAS must be at the Version 5.2 level. So, when a CICSplex contains CMASs at more than one level, the first CMAS upgraded to Version 5.2 must be the maintenance point.

Before you upgrade a CMAS, check that the maintenance point CMAS for the CICSplex has been upgraded in every CICSplex where the CMAS is a member. Remove the CMAS from any CICSplex where the maintenance point CMAS is still at an earlier level. If the CMAS is started in a CICSplex that has a maintenance point CMAS at an earlier level, message EYUCP0012E is issued. In an environment with multiple interconnecting CICSplexes, this message and message EYUTS0012E can be issued repeatedly.

Note: When you upgrade a CMAS that is not a maintenance point CMAS, all of the CICSplex records are removed from its data repository. It cannot connect to its MASs, or join MASs connected to other CMASs, until it reconnects to its maintenance point, at which point its data repository is resynchronized for the CICSplex. Both the maintenance point and non-maintenance point issue EYULOG messages EYUCP0203I and EYUCP0204I. The data repository synchronize is not complete until both CMASs issue both messages. Depending upon the number of records in the CICSplex, the maintenance point usually takes longer than the non-maintenance point, and so the time between the two messages on the non-maintenance point is short, while the time between the two messages on the maintenance point is longer.

Procedure

1. If the CMAS is running, stop it and upgrade the CICS modules to Version 5.2. For more information about dynamically updating DFHIRP, see Chapter 23, "Upgrading multiregion operation (MRO)," on page 89.
2. In the z/OS image that contains the CMAS, verify that the IEASYSxx member of the SYS1.PARMLIB library that you use for z/OS initialization includes the **MAXCAD** and **NSYSLX** parameters, with an appropriate value. the *CICS Transaction Server for z/OS Installation Guide* explains what values are suitable. If you are running both a previous release and Version 5.2 of CICSplex SM, an Environment Services System Services (ESSS) space is started for each release, so you might need to modify the **NSYSLX** value.
3. Authorize the Version 5.2 libraries by adding them to the list of APF-authorized libraries in the appropriate PROGxx or IEAAPFxx member in SYS1.PARMLIB. See in the *CICS Transaction Server for z/OS Installation Guide*.
4. Update the MVS linklist with the Version 5.2 modules that are required for CICS and CICSplex SM. See the *CICS Transaction Server for z/OS Installation Guide*.

5. Upgrade the CSD file with the Version 5.2 group of resource definitions and CICS startup group list. See “Upgrading the CSD for CICS-supplied and other IBM-supplied resource definitions” on page 74. You do not need to carry out an additional upgrade using a release-dependent set of definitions for CICSplex SM.
6. If you modified the default resource definitions for your earlier release, supplied by CICSplex SM in the EYU\$CDEF sample (which contains definitions for a CMAS), manually upgrade your modified resource definitions using the equivalents in the EYU\$CDEF sample for Version 5.2. The safest way is to copy the upgraded default resource definitions and reapply your modifications. It is important to upgrade your modified definitions to ensure that they are defined correctly with nondefault values for attributes that are new. If you fail to upgrade modified definitions, CICS assigns default values to any new attributes. The default values might be inappropriate for your requirements.
7. Edit the JCL used to start the CMAS, changing the previous release of CICSplex SM library names to the Version 5.2 names. If you have BBACTDEF, BBVDEF, or BBIPARM DD statements in the JCL, delete them. For information about the CMAS startup JCL, see the *CICS Transaction Server for z/OS Installation Guide*.
8. Use the EYU9XDUT utility to upgrade the data repository (EYUDREP data set) for the CMAS to Version 5.2. For information about how to upgrade the data repository, see the *CICS Transaction Server for z/OS Installation Guide*. The conversion utility copies the contents of the existing data repository to a newly allocated data repository. The existing data repository is not modified.

Note: After upgrading the data repository for the CMAS, the next time the CMAS is started it must point to the upgraded EYUDREP data set. If it does not, data repository updates might be lost. This loss can lead to incorrect results, which can include other CMASs isolating themselves when they connect to this CMAS. If after upgrading you choose to roll back to the version you upgraded from, use the EYU9XDUT utility to downgrade the upgraded data repository for the CMAS. Failure to do this could result in CMASs becoming isolated.

9. Delete, redefine, and initialize the CICS local catalog and global catalog using the DFHCCUTL and the DFHRMUTL utility programs.
10. Verify the CICSplex SM system parameters referenced by the EYUPARM DD statement. If the CASNAME system parameter is present, delete it. For information about these parameters, see the *CICS Transaction Server for z/OS Installation Guide*.
11. Verify that the CICS system initialization parameter GRPLIST references the CICS supplied default startup group list, DFHLIST, and any CSD groups containing resource definitions that were modified.
12. Verify that the maintenance point CMAS for the CICSplex is running in every CICSplex where the CMAS is a member, then perform a cold start of the upgraded CMAS. Allow the upgraded CMAS to perform repository synchronization with the other CMASs in the network. EYULOG messages EYUCP0203I and EYUCP0204I are issued when repository synchronization begins and completes. After repository synchronization is complete, you can proceed to upgrade the MAS regions that are connected to the CMAS.

Chapter 37. Upgrading a Web User Interface server

A Web User Interface server and the CMAS to which it connects must be at the highest level of CICSplex SM and CICS in the CICSplex. They must be at the same level as the maintenance point CMAS. Web User Interface servers that have not yet been upgraded to the same level as the maintenance point CMAS can be used, but they might return unreliable results until you upgrade them.

About this task

A Web User Interface server can connect only to a CMAS at the same release level. Before you upgrade a Web User Interface server, you must upgrade the CMAS to which it connects. If the CMAS to which the Web User Interface server connects is not the maintenance point CMAS, you must also upgrade the maintenance point CMAS before you start the Web User Interface server and the CMAS to which it connects. Upgrade the Web User Interface server to Version 5.2 before you start any other MASs, so that it is ready to manage the upgraded MASs.

A CICS system that acts as a Web User Interface server is a local MAS. However, when you upgrade a Web User Interface server, you must upgrade both the CICSplex SM MAS agent and the CICS region to Version 5.2. In other MASs you may upgrade only the CICSplex SM MAS agent, and you are not required to upgrade the CICS region.

Procedure

1. Increase the size of the DFHTEMP data set, which is used in the COVC import process. The standard CICS sample has only a primary allocation, but include a secondary allocation for RECORDS, as shown in the following statements:

```
//DEFTS    JOB accounting info,name
//AUXTEMP  EXEC PGM=IDCAMS
//SYSPRINT DD  SYSOUT=A
//SYSIN    DD  *
           DEFINE CLUSTER(NAME(CICSTS52.CICS.CNTL.CICSqualifier.DFHTEMP)-
                           RECORDSIZE(4089,4089)           -
                           RECORDS(200 200)                 -
                           NONINDEXED                         -
                           CONTROLINTERVALSIZE(4096)         -
                           SHAREOPTIONS(2 3)                 -
                           VOLUMES(volid))                   -
                           DATA(NAME(CICSTS52.CICS.CNTL.CICSqualifier.DFHTEMP.DATA) -
                           UNIQUE)
/*
```

2. With your Web User Interface server still running at your current release, use the export function of the COVC transaction to export your existing view set and menu definitions from the Web User Interface server repository (EYUWREP) to an extrapartition transient data queue. It is not necessary for the Web User Interface server to be connected to a CMAS. For information about exporting definitions, see the *CICSplex System Manager Web User Interface Guide*. You will use this information when you upgrade the contents of the Web User Interface server repository in a later process.
3. Authorize the Version 5.2 CICS and CICSplex SM libraries. See the *CICS Transaction Server for z/OS Installation Guide*.

4. If you use the link pack area (LPA), decide when you will replace the previous release modules in the LPA with the Version 5.2 modules. Every CICSplex SM module installed in the LPA can be used only by the release of CICSplex SM to which it relates.
 - a. If you put the Version 5.2 modules in the LPA immediately, change your previous release MASs to use the previous release modules from the STEPLIB and DFHRPL concatenations, instead of the LPA.
 - b. If you put the Version 5.2 modules in the LPA at the end of the upgrade process, make sure your upgraded MASs are using the Version 5.2 modules from the STEPLIB and DFHRPL concatenations instead of the LPA, then change them to use the LPA when you replace the modules.

For more information, see the *CICS Transaction Server for z/OS Installation Guide*.

5. Upgrade the CSD file with the Version 5.2 group of resource definitions and CICS startup group list. For information about upgrading the CSD, see “Upgrading the CSD for CICS-supplied and other IBM-supplied resource definitions” on page 74. You do not need to carry out an additional upgrade using a release-dependent set of definitions for CICSplex SM.
6. If you made any modifications to the dynamically created resource definitions for your earlier release that were supplied by CICSplex SM in the EYU\$WDEF sample, manually upgrade your modified resource definitions using the equivalents in the EYU\$WDEF sample for Version 5.2. The safest way to do this is to copy the Version 5.2 resource definitions and reapply your modifications. It is important to upgrade your modified definitions to ensure that they are defined correctly with nondefault values for attributes that are new. If you fail to upgrade modified definitions, CICS assigns default values to any new attributes, and these might be inappropriate for CICS-supplied resource definitions.
7. Edit the JCL used to start the Web User Interface server, changing library names for the previous release of CICSplex System Manager to the Version 5.2 names. For information about the MAS startup JCL, see the *CICS Transaction Server for z/OS Installation Guide*.
8. Verify that the CICS system initialization parameter **EDSALIM** is specified for the CICS region, and set it to a value of 800 MB. 800 MB is the default EDSALIM value for a CICS region in Version 5.1 and later. This value may be tuned by the user in a similar manner to tuning CICS storage in a CMAS. System initialization parameters can be specified before startup in the following locations:
 - In the system initialization table specified in the DFHSITxx load module whose suffix (xx) is specified as a SIT= system initialization parameter.
 - In the PARM parameter of the EXEC PGM=DFHSIP statement.
 - In the SYSIN data set defined in the startup job stream.
9. Verify that the CICS system initialization parameter **CPSMCONN=WUI** is specified for the CICS region. This system initialization parameter initializes the CICS region as a Web User Interface server and dynamically creates the required resource definitions for CICSplex SM.
10. Verify that the CICS system initialization parameter **GRPLIST** references the CICS-supplied default startup group list, DFHLIST, any CSD groups containing resource definitions that you have modified, and the lists of definitions for your own applications.

11. Ensure that you have deleted, redefined, and initialized the CICS local catalog and global catalog using the DFHCCUTL and the DFHRMUTL utility programs.
12. If you use MAS history recording, define new history data sets using the EYUJHIST sample job. If you prefer to upgrade your existing history data sets, you can also do this using the EYUJHIST sample job by following the upgrading instructions, supplied as comments, in the sample. The EYUJHIST sample is supplied uncustomized in the TDFHINST library, and customized by DFHISTAR in the XDFHINST library. Remember to edit the MAS startup JCL to include the history data sets.
13. Upgrade the contents of the Web User Interface server repository (EYUWREP). During this process you will start the Web User Interface server at Version 5.2. See “Upgrading the contents of the Web User Interface server repository (EYUWREP)” on page 140.

Phased upgrade scenario for Web User Interface servers

If you have CICSplex SM Web User Interface servers connected to CMASs other than the maintenance point CMAS, which have many other MASs connected to them, you might not want to upgrade the other MASs at the same time as the CMAS. In that case, consider using this phased upgrade path.

About this task

Assuming you are running the latest CICSplex SM maintenance levels, you can upgrade one LPAR at a time.

Procedure

1. Define a new Version 5.2 CMAS on the same z/OS image as the Web User Interface server.
2. Define CMAS to CMAS links between the new Version 5.2 CMAS and the maintenance point CMAS in the CICSplex where the Web User Interface server CMAS is connected.
3. Upgrade the maintenance point CMAS in the CICSplex to Version 5.2.
4. Assign the new Version 5.2 CMAS to the CICSplex.
5. Upgrade the Web User Interface server to Version 5.2 and, when you restart it, connect it to the Version 5.2 CMAS. If the Web User Interface server is configured to connect specifically to the original CMAS, you must change the configuration to connect to the Version 5.2 CMAS.
6. Upgrade the remaining MASs to Version 5.2 when required, and connect them to the Version 5.2 CMAS as you restart them. If the MASes are configured to connect specifically to the original CMAS, you must change their configuration to connect to the Version 5.2 CMAS.
7. When you have moved all the MASs to the Version 5.2 CMAS, you can remove the original CMAS from the CICSplex, and delete CMAS to CMAS links between the original CMAS and the other CMASes in the CICSplex.

Upgrading the contents of the Web User Interface server repository (EYUWREP)

With each release of CICS, internal Web User Interface repository record versions might be incremented to enable the new features in view definitions. For this reason, if your existing Web User Interface repository contains customized view sets or menus, you must upgrade your view set and menu definitions.

Before you begin

At the start of your upgrade of the Web User Interface server, when your Web User Interface server is still running at your current release, use the export function of the COVC transaction to export your existing view set and menu definitions from the Web User Interface server repository to an extrapartition transient data queue. This step is included in the upgrade instructions Chapter 37, “Upgrading a Web User Interface server,” on page 137.

About this task

When you upgrade the Web User Interface server repository to CICS TS for z/OS, Version 5.2, you can import a view set and menu definitions from a previous release into your new Web User Interface server repository.

You do not need to make any changes to existing customized views and menus, but you can consider modifying or creating view sets to take into account the new attributes and resources.

Procedure

1. Create a new Web User Interface server repository using the JCL described in the *CICS Transaction Server for z/OS Installation Guide*.
2. Start the CICS TS for z/OS, Version 5.2 Web User Interface server using the new Web User Interface server repository.
3. Use COVC to import the view set and menu definitions from your previous release from the extrapartition transient data queue to which you exported them. For information about the import function of the COVC transaction, see the *CICSplex System Manager Web User Interface Guide*. This import is necessary for each type of resource (VIEW, MENU, USER, USERGRP, and so on) that you had previously customized.
4. Use COVC to import the new starter set definitions. Specify the **OVERWRITE** option on the **Import option** field of the COVC panel to ensure that none of the new starter set views are accidentally overwritten by views from a previous release. For information about using COVC, see the *CICSplex System Manager Web User Interface Guide*.

What to do next

You can also export view set and menu definitions from a CICS TS for z/OS, Version 5.2 Web User Interface server and import them into a server repository of a previous release. However, any new attributes or resources that are new in this release are not accessible in previous releases. You can remove these attributes and view sets using the View Editor. For information about the View Editor, see the *CICSplex System Manager Web User Interface Guide*.

Chapter 38. Upgrading a CICSplex SM managed CICS system (MAS)

When you upgrade a CICSplex SM MAS to CICSplex SM Version 5.2, you might choose to upgrade only the CICSplex SM MAS agent. You are not required to upgrade the CICS region to Version 5.2 at the same time.

Before you begin

Before you upgrade a CICSplex SM MAS to CICSplex SM Version 5.2, you must upgrade the CICSplex SM CMAS to which it connects, following the instructions in Chapter 36, “Upgrading a CMAS,” on page 135. You must also upgrade the Web User Interface server for the CICSplex, following the instructions in Chapter 37, “Upgrading a Web User Interface server,” on page 137.

About this task

These steps explain how to upgrade the CICSplex SM MAS agent in a CICS region to Version 5.2. For details of supported combinations of CICSplex SM and CICS releases, see Chapter 34, “Conditions for running CICSplex SM Version 5.2 and earlier releases concurrently,” on page 129.

Procedure

1. If you use the link pack area (LPA), decide when you will replace the previous release modules in the LPA with the Version 5.2 modules. Every CICSplex SM module installed in the LPA can be used only by the release of CICSplex SM to which it relates.
 - a. If you put the Version 5.2 modules in the LPA immediately, change your previous release MASs to use the previous release modules from the STEPLIB and DFHRPL concatenations, instead of the LPA.
 - b. If you put the Version 5.2 modules in the LPA at the end of the upgrade process, make sure your upgraded MASs are using the Version 5.2 modules from the STEPLIB and DFHRPL concatenations instead of the LPA, then change them to use the LPA when you replace the modules.

For more information, see the *CICS Transaction Server for z/OS Installation Guide*.

2. If you made any modifications to the default resource definitions for your earlier release that were supplied by CICSplex SM in the EYU\$MDEF sample (which contains definitions for a MAS), or the EYU\$WDEF sample (which contains definitions for a WUI), manually upgrade your modified resource definitions using the equivalents in the EYU\$MDEF or EYU\$WDEF sample for Version 5.2. The safest way to do this is to copy the upgraded default resource definitions and reapply your modifications. It is important to upgrade your modified definitions to ensure that they are defined correctly with nondefault values for attributes that are new. If you fail to upgrade modified definitions, CICS assigns default values to any new attributes, and these might be inappropriate for CICS-supplied resource definitions.
3. In the JCL that is used to start the MAS, replace the previous release SEYUAUTH library name in the STEPLIB concatenation, and the previous release SEYULOAD library name in the DFHRPL concatenation, with the Version 5.2 SEYUAUTH and SEYULOAD library names. The Version 5.2 SEYUAUTH library must be authorized for APF, which you did when you

upgraded the CMAS, but the SEYULOAD library must not be authorized. For information about the MAS startup JCL, see the *CICS Transaction Server for z/OS Installation Guide*.

4. Verify that the CICS system initialization parameter **EDSALIM** is specified for the CICS region, and set it to a value of 800 MB. 800 MB is the default EDSALIM value for a CICS region in Version 5.2. System initialization parameters can be specified before startup in the following locations:
 - In the system initialization table specified in the DFHSITxx load module whose suffix (xx) is specified as a SIT= system initialization parameter.
 - In the PARM parameter of the EXEC PGM=DFHSIP statement.
 - In the SYSIN data set defined in the startup job stream.
5. Verify that the CICS system initialization parameter **CPSMCONN=LMA5** is specified for the CICS region. This system initialization parameter initializes the CICS region as a MAS and dynamically creates the required resource definitions for CICSplex SM. If you made any modifications to the dynamically created resource definitions in your previous release, you must manually upgrade these using the equivalents in the EYU\$MDEF sample for Version 5.2.
6. If you use MAS history recording, define new history data sets using the EYUJHIST sample job. If you prefer to upgrade your existing history data sets, you can also do this using the EYUJHIST sample job by following the upgrading instructions, supplied as comments, in the sample. The EYUJHIST sample is supplied uncustomized in the TDFHINST library, and customized by DFHISTAR in the XDFHINST library. Remember to edit the MAS startup JCL to include the history data sets.
7. Optional: If you also want to upgrade the CICS region to Version 5.2 at this time, follow the instructions in Chapter 19, “Upgrade procedures for all CICS regions,” on page 73. You must upgrade the CSD for CICS as instructed, but you do not need to carry out any additional upgrade to your CSD to obtain the resource definitions for CICSplex SM, because all CICSplex SM resources are defined and installed dynamically.

Results

When you have completed this task, you can carry out a cold start of the MAS.

Part 5. Changes to CICS messages and codes

This section lists messages and abend codes that have been removed, changed, and added for CICS Transaction Server for z/OS, Version 5 Release 2.

The DFHCMACD file is not updated by PTFs that are applied to CICS. For the latest message updates, see the descriptions in CICS messages in Reference -> Diagnostics. The CMAC transaction uses the DFHCMACD file to provide online descriptions of the CICS messages and codes.

Chapter 39. Deleted messages

These messages are deleted for CICS Transaction Server for z/OS, Version 5 Release 2. Where a range of message numbers is specified, all the message numbers in that range were previously issued and have now been deleted.

Messages deleted in CICS Transaction Server for z/OS, Version 5 Release 2

- DFHSJ0902
- DFHCZ0357 to DFHCZ0362

Chapter 40. Changed messages

These messages are changed for CICS Transaction Server for z/OS, Version 5 Release 2.

Table 20. Messages changed in CICS Transaction Server for z/OS, Version 5 Release 2

Message number	Message text
DFHAM4952	<i>applid</i> The installation of standalone CICS bundle <i>resourcename</i> failed because its ID and version are a duplicate of a standalone CICS bundle that already exists.
DFHAP1903	<i>date time applid</i> CICS failed to write SPI audit message DFHAP1900.
DFHCA4952	<i>applid</i> The installation of standalone CICS bundle <i>resourcename</i> failed because its ID and version are a duplicate of a standalone CICS bundle that already exists.
DFHLD0503W	<i>date time applid termid tranid</i> Install of LIBRARY <i>libname</i> has failed to complete successfully, for reason: {library not found. dynamic allocation of data set failed. concatenation of data sets failed. open of library concatenation failed. close of library concatenation failed. deconcatenation of data sets failed. de-allocation of data set failed. mvs abend condition. incompatible bundle set. library not disabled. insufficient storage. library lock error. library chain error. catalog write failed. catalog_delete failed. unknown.} Enablement status is Disabled.
DFHLD0513W	<i>date time applid termid tranid</i> Discard of LIBRARY <i>libname</i> has failed for reason: {library not found. dynamic allocation of data set failed. concatenation of data sets failed. open of library concatenation failed. close of library concatenation failed. deconcatenation of data sets failed. de-allocation of data set failed. mvs abend condition. incompatible bundle set. library not disabled. insufficient storage. library lock error. library chain error. catalog write failed. catalog_delete failed. unknown.}
DFHLD0525W	<i>date time applid termid tranid</i> Attempt to set attributes or status of LIBRARY <i>libname</i> has failed for reason: {library not found. dynamic allocation of data set failed. concatenation of data sets failed. open of library concatenation failed. close of library concatenation failed. deconcatenation of data sets failed. de-allocation of data set failed. mvs abend condition. incompatible bundle set. library not disabled. insufficient storage. library lock error. library chain error. catalog write failed. catalog_delete failed. unknown.}
DFHLD0850	<i>date time applid</i> BUNDLE <i>bundlename</i> has successfully installed LIBRARY <i>library</i> as {Enabled Disabled}.
DFHMP2006	<i>date time applid</i> The CICS managed platform domain failed to create the policy <i>policyname</i> in BUNDLE resource <i>bundle</i> because the rule <i>rulename</i> { has an invalid rule type has an invalid condition name for rule type has an invalid item name has an invalid operator value has an invalid storage unit has an invalid count unit has an invalid time unit has an invalid abend code has an invalid EP adapter name has an invalid EP adapter set name has a missing XML element}: 'error_data'.
DFHPA1909	<i>applid</i> DATA <i>data</i> IS INVALID FOR KEYWORD <i>keyword</i> . RESPECIFY KEYWORD AND DATA OR BYPASS BY TYPING '.END'.
DFHPG0304	<i>date time applid</i> BUNDLE <i>bundlename</i> has made the PROGRAM <i>programname</i> available as an entry point for operation <i>operationname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> , on platform <i>platformname</i> .
DFHPG0305	<i>date time applid</i> BUNDLE <i>bundlename</i> has made the PROGRAM <i>programname</i> unavailable as an entry point for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> , on platform <i>platformname</i> .

Table 20. Messages changed in CICS Transaction Server for z/OS, Version 5 Release 2 (continued)

Message number	Message text
DFHPG0306	<i>date time applid BUNDLE bundlename unable to enable PROGRAM programname as an entry point for operation operationname as {the PROGRAM does not exist. the PROGRAM failed to autoinstall. an internal error occurred. the PROGRAM name is invalid. the named PROGRAM is remote. the named resource is a MAPSET. the named resource is a PARTITIONSET. the PROGRAM has the same name as an existing public program.}</i>
DFHPI0516	<i>date time applid tranid A request to the SAML security token service on JVM server jvmserver has failed because {of an invalid token. of a container error. a required input container is missing. the JVM server is not enabled. the JVM server cannot be found. the DFHSAML-FUNCTION container is not DATATYPE(CHAR). the DFHSAML-TOKEN container is not found. the DFHSAML-TOKEN container is not DATATYPE(CHAR). the DFHSAML-JVM container is not DATATYPE(CHAR). the DFHSAML-FILTER container is not DATATYPE(CHAR). the DFHSAML-SIGNED container is not DATATYPE(CHAR). of an error in parsing the token. the DFHSAML-FILTER container has invalid data. the DFHSAML-FUNCTION container has invalid data. the DFHSAML-SIGNED container has invalid data. the DFHSAML-OUTTOKEN container is not found. the certificate in the token has expired. the token is no longer valid. the certificate in the token is not trusted the DFHSAML-RESPONSE container cannot be found. of an internal error.}</i>
DFHPI0914	<i>date time applid userid WEBSERVICE WebService is UNUSABLE because: {the WSBind file was not found CICS is not authorized to read the WSBind file there is insufficient storage to load the WSBind file the zFS read for the WSBind file failed writing the WSBind file to the shelf failed the PIPELINE is incompatible with this WEBSERVICE the CPIR resolution transaction could not be attached the direction of the PIPELINE can't be determined the WSBind file is corrupt the WSBind file has an invalid version number the WSBind file has an out of date version number the WSBind file product number was not recognized the PIPELINE is not a SOAP PIPELINE the PIPELINE does not support SOAP version 1.2 the PIPELINE is not configured for SOAP version 1.1 the WSBind file is incompatible with the LOCALCCSID it is incompatible with a Bundle defined PIPELINE} .</i>
DFHPI1007	<i>DATE TIME APPLID TRANNUM {XML JSON} to data transformation failed because of incorrect input ({XML_FORMAT_ERROR UNEXPECTED_CONTENT HEADER_FORMAT_ERROR UNDEFINED_ELEMENT UNDEFINED_NAME_SPACE ARRAY_OVERFLOW NAME_TOO_LONG PREFIX_TOO_LONG NAME_SPACE_TOO_LONG UNEXPECTED_XOP_INCLUDE XOP_INCLUDE_ERROR DUPLICATE_CHOICE MISSING_XSI_TYPE UNKNOWN_XSI_TYPE MISSING_ATTRIBUTE MIXED_CONTENT MISSING_EQUALS_ATTR MISSING_CLOSE_TAG_CHAR MISSING_QUOTE_OR_APOSTROPHE MISSING_END_QUOTE DUPLICATE_ATTRIBUTE MISMATCHED_TAGS UNSUPPORTED_ENTITY INVALID_UNICODE_DATA} error_qualifier) for {WEBSERVICE XMLTRANSFORM BUNDLE EVENTBINDING SCACOMPOSITE JVMSERVER pipeline handler program EPADAPTER OSGIBUNDLE PROGRAM POLICY EPADAPTERSET APPLDEF TRANSACTION URIMAP PLATDEF LIBRARY WARBUNDLE EBABUNDLE TCPIPSERVICE JVMSERVER FILE PIPELINE JSONTRANSFRM TYPE UNKNOWN} resource_name.</i>
DFHPI1008	<i>DATE TIME APPLID TRANID TRANNUM {XML JSON} generation failed because of incorrect input ({ARRAY_CONTAINER_TOO_SMALL DATA_STRUCTURE_TOO_SMALL ARRAY_TOO_LARGE ARRAY_TOO_SMALL CONTAINER_NOT_FOUND CONTAINER_NOT_BIT CONTAINER_NOT_CHAR BAD_CHOICE_ENUM LENGTH_TOO_LONG LITTLE_ENDIAN_BOM INVALID_UNICODE_DATA} error_qualifier) for {WEBSERVICE XMLTRANSFORM BUNDLE EVENTBINDING SCACOMPOSITE JVMSERVER pipeline handler program EPADAPTER OSGIBUNDLE PROGRAM POLICY EPADAPTERSET APPLDEF TRANSACTION URIMAP PLATDEF LIBRARY WARBUNDLE EBABUNDLE TCPIPSERVICE JVMSERVER FILE PIPELINE JSONTRANSFRM TYPE UNKNOWN} resource_name.</i>

Table 20. Messages changed in CICS Transaction Server for z/OS, Version 5 Release 2 (continued)

Message number	Message text
DFHPI1009	DATE TIME APPLID TRANNUM {XML JSON} to data transformation failed. A conversion error ({UNKNOWN_CONVERSION INPUT_TOO_LONG OUTPUT_OVERFLOW NEGATIVE_UNSIGNED NO_FRACTION_DIGITS FRACTION_TOO_LONG INVALID_CHARACTER ODD_HEX_DIGITS INVALID_BASE64 NOT_PURE_DBCS INVALID_FIELD_SIZE EXPONENT_OVERFLOW EXPONENT_UNDERFLOW ABSTIME_INVALID}) occurred when converting field <i>fieldname</i> for {WEBSERVICE XMLTRANSFORM BUNDLE EVENTBINDING SCACOMPOSITE JVMSERVER pipeline handler program EPADAPTER OSGIBUNDLE PROGRAM POLICY EPADAPTERSET APPLDEF TRANSACTION URIMAP PLATDEF LIBRARY WarBUNDLE EBABUNDLE TCPIPService JVMSERVER FILE PIPELINE JSONTRANSFORM TYPE UNKNOWN} <i>resource_name</i> .
DFHPI1010	DATE TIME APPLID TRANNUM {XML JSON} generation failed. A conversion error ({UNKNOWN_CONVERSION NEGATIVE_UNSIGNED INVALID_CHARACTER INVALID_PACKED_DEC INVALID_ZONED_DEC INCOMPLETE_DBCS ODD_DBCS_BYTES INVALID_FIELD_SIZE EXPONENT_OVERFLOW EXPONENT_UNDERFLOW ABSTIME_INVALID}) occurred when converting field <i>fieldname</i> for {WEBSERVICE XMLTRANSFORM BUNDLE EVENTBINDING SCACOMPOSITE JVMSERVER pipeline handler program EPADAPTER OSGIBUNDLE PROGRAM POLICY EPADAPTERSET APPLDEF TRANSACTION URIMAP PLATDEF LIBRARY WarBUNDLE EBABUNDLE TCPIPService JVMSERVER FILE PIPELINE JSONTRANSFORM TYPE UNKNOWN} <i>resource_name</i> .
DFHRL0115 W	<i>date time applid tranid</i> The attempt to {enable disable discard} the BUNDLE <i>bundle_name</i> failed because one or more of its defined resources are {in an ENABLED in an UNUSABLE not in a DISABLED} state.
DFHRL0128 I	<i>date time applid userid</i> The CICS resource lifecycle manager has started to create BUNDLE <i>bundle_name</i> with bundle ID <i>bundle_id</i> and version <i>bundle_major_ver.bundle_minor_ver.bundle_micro_ver</i> for application <i>application_id</i> version <i>appl_major_ver.appl_minor_ver.appl_micro_ver</i> on platform <i>platform_id</i> .
DFHSJ0914 E	<i>date time applid userid</i> JVMSERVER <i>jvmserver</i> is installed as DISABLED because {the JVM server was not found. CICS is not authorized to read the JVM profile. the CJSR transaction could not be attached. there is insufficient storage available. the activate mode failed. the add of the TP tcb failed. the change mode to the TP tcb failed. the Language Environment Enclave was not created. there was a runtime options failure. there was a failure updating the JVMProfile table. there were insufficient threads available.the CJSR transaction could not be attached. the CJSR ThreadJoiner class could not be created.}
DFHSJ1105	<i>date time applid bundletype</i> BUNDLE <i>resname</i> from BUNDLE <i>bundlename</i> has been installed as {Enabled Disabled}.
DFHWP0800	<i>date time applid</i> BUNDLE <i>bundlename</i> has successfully installed URIMAP <i>urimdef</i> as {Enabled Disabled}.
DFHXM0600	<i>date time applid</i> BUNDLE <i>bundlename</i> has successfully installed TRANSACTION <i>trandef</i> as {Enabled Disabled}.
EYUWI0020	<i>date time applid</i> WLM Routing initiated for workload(<i>ins#1</i>) in Routing Region(<i>ins#2</i>), CICSplex(<i>ins#3</i>).
EYUWI0021	<i>date time applid</i> WLM Routing initialization failed for workload(<i>workload</i>) in Routing Region(<i>region</i>), CICSplex(<i>plexname</i>).
EYUWI0080	<i>date time applid</i> WLM Workload { <i>query</i> <i>analysis</i> } process for workload(<i>workload</i>), CICSplex(<i>plexname</i>) has been started {- directed to CMAS (- initiated by CMAS (} <i>cmasname</i>).
EYUWI0081	<i>date time applid</i> WLM Workload { <i>analysis</i> <i>build</i> } process for workload(<i>workload</i>) , CICSplex(<i>plexname</i>) has been completed {- initiated by CMAS (} <i>cmasname</i>).

Table 20. Messages changed in CICS Transaction Server for z/OS, Version 5 Release 2 (continued)

Message number	Message text
EYUWI0082	<i>date time applid</i> WLM Workload { <i>query</i> <i>analysis</i> } process failed for workload(<i>workload</i>), CICSplex(<i>plexname</i>) {- directed to CMAS (- initiated by CMAS (} <i>cmasname</i>).
EYUWI0083	<i>date time applid</i> WLM Query Workload has encountered an unknown { <i>object</i> <i>command</i> } for workload(<i>workload</i>), CICSplex(<i>plexname</i>) during workload build process - { <i>object</i> <i>command</i> } (<i>nn</i>) ignored.
EYUWI0084	<i>date time applid</i> WLM Query Workload was unable to locate object(<i>nn</i>), key(<i>type</i>), workload(<i>workload</i>), CICSplex(<i>plexname</i>), update ignored.
EYUWI0085	<i>date time applid</i> WLM Query Workload has detected a workload synchronization failure for workload(<i>workload</i>), CICSplex(<i>plexname</i>).
EYUWI0090	<i>date time applid</i> CMAS <i>ins#1</i> is unavailable for workload(<i>ins#2</i>), CICSplex(<i>ins#3</i>).
EYUWM0400	<i>date time applid</i> Workload { <i>Specification</i> <i>Group</i> <i>Definition</i> } (<i>name</i>) has been successfully installed for CICSplex(<i>plexname</i>), workload(<i>workload</i>) {- initiated by CMAS (} <i>cmasname</i>).
EYUWM0401	<i>date time applid</i> Workload { <i>Specification</i> <i>Group</i> <i>Definition</i> } (<i>name</i>) failed to install for CICSplex(<i>plexname</i>), workload(<i>workload</i>) {- initiated by CMAS (- initiated by join of router (} <i>objectname</i>).
EYUWM0402	<i>date time applid</i> Workload { <i>Specification</i> <i>Definition</i> <i>Transaction Group</i> } (<i>name</i>) { <i>is not defined</i> <i>has no transaction links</i> <i>has an invalid scope specification</i> } for CICSplex(<i>plexname</i>), workload(<i>workload</i>).
EYUWM0420	<i>date time applid</i> Routing region (<i>sysname</i>) for CICSplex(<i>plexname</i>) has been joined to workload(<i>name</i>).
EYUWM0421	<i>date time applid</i> Routing region (<i>sysname</i>) for CICSplex(<i>plexname</i>) has been removed from workload(<i>name</i>).
EYUWM0422	<i>date time applid</i> Routing region (<i>sysname</i>) for CICSplex(<i>plexname</i>) already active in workload(<i>name</i>).
EYUWM0424	<i>date time applid</i> Target region (<i>sysname</i>) for CICSplex (<i>plexname</i>) has been activated in workload (<i>name</i>).
EYUWM0425	<i>date time applid</i> Target region (<i>sysname</i>) for CICSplex (<i>plexname</i>) has been terminated in workload (<i>name</i>).
EYUWM0426	<i>date time applid</i> { <i>Definition</i> <i>Transaction Group</i> <i>Transaction</i> } (<i>name</i>) already installed in workload(<i>name</i>) for CICSplex(<i>plexname</i>) - parameter ignored.
EYUWM0427	<i>date time applid</i> Parameters have been ignored during the installation of Workload { <i>Group</i> <i>Definition</i> } (<i>name</i>) for CICSplex(<i>plexname</i>), workload(<i>workload</i>) {- initiated by CMAS (} <i>cmasname</i>).
EYUWM0428	<i>date time applid</i> WLMDEF (<i>defname1</i>) already installed in workload(<i>workloadname</i>) as (<i>defname2</i>) for CICSplex(<i>plexname</i>) - parameter ignored.
EYUWM0429	<i>date time applid</i> WLMDEFs (<i>defname1</i>) and (<i>defname2</i>) in workload(<i>workloadid</i>) for CICSplex(<i>plexname</i>) contain conflicting parameters. WLMDEF(<i>defname3</i>) is ignored.
EYUWM0430	<i>date time applid</i> Workload(<i>workloadid</i>) for CICSplex(<i>plexname</i>) transition to type: <i>sysname</i> at <i>sysplex</i> reason.
EYUWM0431	<i>date time applid</i> AOR (<i>name</i>) has failed activation for workload(<i>workloadid</i>), CICSplex(<i>plexname</i>) because it has the same APPLID(<i>applid</i>) as previously activated AOR(<i>name2</i>).
EYUWM0432	<i>date time applid</i> WLMDEF (<i>defname</i>) in workload(<i>workloadid</i>) cannot be processed for CICSplex(<i>plexname</i>) due to a CICS BTS Processtype specification.
EYUWM0433	<i>date time applid</i> TRANGRP (<i>trangrpname</i>) in workload(<i>workloadname</i>) cannot be processed for CICSplex(<i>plexname</i>) due to a CICS BTS Affinity specification.
EYUWM0503	<i>date time applid</i> Routing region (<i>name</i>), CICSplex(<i>plexname</i>) is running in Sysplex Optimized WLM state for workload(<i>workload</i>).

Table 20. Messages changed in CICS Transaction Server for z/OS, Version 5 Release 2 (continued)

Message number	Message text
EYUWM0504	<i>date time applid</i> Routing region (<i>name</i>), CICSplex(<i>plexname</i>) is not running in Sysplex Optimized WLM state for workload(<i>workload</i>).
EYUWM0505	<i>date time applid</i> Target region (<i>name</i>), CICSplex(<i>plexname</i>) is running in Sysplex Optimized WLM state.
EYUWM0506	<i>date time applid</i> Target region (<i>name</i>), CICSplex(<i>plexname</i>) is not running in Sysplex Optimized WLM state.
EYUWM0507	<i>date time applid</i> Routing region (<i>name</i>), CICSplex(<i>plexname</i>) optimization termination in workload(<i>workload</i>) reason: ({ <i>RS server failure</i> <i>Optimization disabled</i> <i>RSPoolID changed</i> }).
EYUWM0508	<i>date time applid</i> Target region (<i>name</i>), CICSplex(<i>plexname</i>) optimization termination reason: ({ <i>RS server failure</i> <i>Optimization disabled</i> <i>RSPoolID changed</i> <i>Link to DFHRSFDL failed</i> }).

Chapter 41. New messages

These messages are new for CICS Transaction Server for z/OS, Version 5 Release 2.

Table 21. New messages in CICS Transaction Server for z/OS, Version 5 Release 2

Message number	Message text
DFHFC0600	<i>date time applid</i> BUNDLE <i>bundlename</i> has successfully installed FILE <i>filename</i> as {Enabled Disabled}.
DFHFC6042	<i>datetime applid</i> Attempt to discard file <i>filename</i> failed.
DFHFC6043	<i>datetime applid</i> Attempt to disable bundle <i>bundlename</i> failed because file <i>filename</i> has retained locks or is in use.
DFHKE0007	<i>applid</i> Licence module DFHSIVT not found.
DFHLD0508I	<i>date time applid termid tranid</i> LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> is being installed with status {Enabled Disabled}.
DFHLD0509I	<i>date time applid termid tranid</i> Install of LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> has completed successfully. Enablement status is {Enabled Disabled}.
DFHLD0510I	<i>date time applid</i> Details for LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> , ranking: <i>ranking</i> , enablement status: {Enabled Disabled}.
DFHLD0514W	<i>date time applid termid tranid</i> Install of LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> , has failed to complete successfully, for reason: {library not found. dynamic allocation of data set failed. concatenation of data sets failed. open of library concatenation failed. close of library concatenation failed. deconcatenation of data sets failed. de-allocation of data set failed. mvsabend condition. incompatible bundle set. library not disabled. insufficient storage. library lock error. library chain error. catalog write failed. catalog_delete failed. unknown.} Enablement status is Disabled.
DFHLD0515E	<i>date time applid termid tranid</i> Install of LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> , has failed because a LIBRARY of that name is already installed.
DFHLD0516I	<i>date time applid termid tranid</i> LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> has been successfully discarded.
DFHLD0517W	<i>date time applid termid tranid</i> Discard of LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> has failed for reason: {library not found. dynamic allocation of data set failed. concatenation of data sets failed. open of library concatenation failed. close of library concatenation failed. deconcatenation of data sets failed. de-allocation of data set failed. mvsabend condition. incompatible bundle set. library not disabled. insufficient storage. library lock error. library chain error. catalog write failed. catalog_delete failed. unknown.}
DFHLD0518I	<i>date time applid termid tranid</i> LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> has been assigned a DD name of <i>ddname</i> .
DFHLD0526I	<i>date time applid termid tranid</i> LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> has been enabled.
DFHLD0527I	<i>date time applid termid tranid</i> LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> has been disabled.

Table 21. New messages in CICS Transaction Server for z/OS, Version 5 Release 2 (continued)

Message number	Message text
DFHLD0528W	<i>date time applid termid tranid</i> Attempt to set attributes or status of LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> has failed for reason: {library not found. dynamic allocation of data set failed. concatenation of data sets failed. open of library concatenation failed. close of library concatenation failed. deconcatenation of data sets failed. de-allocation of data set failed. mvs abend condition. incompatible bundle set. library not disabled. insufficient storage. library lock error. library chain error. catalog write failed. catalog_delete failed. unknown.}
DFHLD0557I	<i>date time applid</i> Current LIBRARY search order for platform <i>platformname</i> , application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> follows.
DFHLD0558I	<i>date time applid</i> Current LIBRARY search order for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> is empty.
DFHLD0733	<i>applid</i> Install of LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> encountered an error. The LIBRARY is installed but disabled.
DFHLD0734	<i>applid</i> Install of LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> encountered an error. The LIBRARY is installed as disabled.
DFHLD0735	<i>applid</i> Attempt to install or enable LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> will be delayed because data set <i>dsname</i> is being recalled.
DFHLD0736	<i>applid</i> Attempt to enable LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> encountered an error. The LIBRARY is disabled.
DFHLD0737	<i>applid</i> Disable processing for LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> encountered an error.
DFHLD0738	<i>applid</i> Dynamic allocation of data set <i>dsname</i> for LIBRARY <i>libname</i> for application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> failed. DYNALOC return codes: X'rrrr', X'cccc', X'dddd'.
DFHLD0739	<i>applid</i> Dynamic concatenation of data sets for LIBRARY <i>libname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> failed. DYNALOC return codes: X'rrrr', X'cccc', X'dddd'.
DFHLD0740	APPLID Open of DD for LIBRARY <i>libname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> failed.
DFHLD0741	<i>applid</i> Dynamic unallocation of data set <i>dsname</i> for LIBRARY <i>libname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> failed. DYNALOC return codes: X'cccc', X'rrrr', X'dddd'.
DFHLD0742	<i>applid</i> Dynamic deconcatenation of data sets for LIBRARY <i>libname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> failed. DYNALOC return codes: X'rrrr', X'cccc', X'dddd'.
DFHLD0743	<i>applid</i> Close of DD for LIBRARY <i>libname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> failed.
DFHLD0744	APPLID An MVS ABEND occurred during {Getmain of LIBRARY control area Dynamic allocation Dynamic concatenation Open Close Dynamic deconcatenation Dynamic unallocation Freemain of LIBRARY control area} for LIBRARY <i>libname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> .
DFHLD0745	APPLID Data set <i>dsname</i> could not be allocated for LIBRARY <i>libname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> because CICS could not determine that the data set is valid for a dynamic LIBRARY. Reason: {LOCATE error. LOCATE macro OBTAIN error. OBTAIN macro not enough working storage. Loader SVC CICS internal error. Loader SVC } return code: X'rc'

Table 21. New messages in CICS Transaction Server for z/OS, Version 5 Release 2 (continued)

Message number	Message text
DFHLD0746	<i>APPLID</i> Data set <i>dsname</i> could not be allocated for LIBRARY <i>libname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> on platform <i>platformname</i> because it is not valid for a dynamic LIBRARY. Reason: { <i>not DASD volume</i> <i>not partitioned organization</i> <i>record format is not set to unspecified</i> }.
DFHMP1007	<i>date time applid</i> Policy <i>polycyname</i> from BUNDLE resource <i>bundle</i> successfully enabled.
DFHMP1008	<i>date time applid</i> Policy <i>polycyname</i> from BUNDLE resource <i>bundle</i> successfully disabled.
DFHMP2013	<i>date time applid</i> The CICS managed platform domain failed to create the policy scope for operation <i>operation</i> defined in BUNDLE resource <i>bundle</i> because the policy name <i>polycyname</i> is invalid. The BUNDLE resources was installed with a scope of platform(<i>platformname</i>), application(<i>applicationname</i>), and version(<i>majorversion.minorversion.microversion</i>).
DFHMQ0793	Check for associated messages to determine if the WebSphere MQ message was reprocessed or moved to another queue. Previous messages may explain why the remote system was unable to commit.
DFHPG0111	<i>date time applid terminal userid tranid</i> Resource definition for <i>progrname</i> in application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> has been added.
DFHPG0112	<i>date time applid terminal userid tranid</i> Resource definition for <i>progrname</i> in application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> has been deleted.
DFHPG0113	<i>date time applid terminal userid tranid</i> An application entry point for operation <i>operationname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> , on platform <i>platformname</i> has been set disabled and unavailable because PROGRAM <i>programname</i> has been replaced.
DFHPG0221	<i>date time applid terminal userid tranid</i> Program autoinstall exit <i>urmname</i> indicated that program <i>progrname</i> in application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> should not be installed.
DFHPG0224	<i>date time applid terminal userid tranid</i> Autoinstall for program <i>progrname</i> in application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> failed. Program autoinstall model <i>modelname</i> is not defined.
DFHPG0226	<i>date time applid terminal userid tranid</i> Autoinstall for program <i>progrname</i> in application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> failed. Programs starting with “DFH” cannot be defined as remote programs.
DFHPG0227	<i>date time applid terminal userid tranid</i> Autoinstall for program <i>progrname</i> in application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> failed. The program name is not valid.
DFHPG0228	<i>date time applid terminal userid tranid</i> Autoinstall for program <i>progrname</i> in application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> failed.
DFHPG0229	<i>date time applid terminal userid tranid</i> Resource definition for <i>progrname</i> in application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> has been autoinstalled using model <i>modelname</i> .
DFHPG0230	<i>date time applid terminal userid tranid</i> Resource definition for <i>progrname</i> in application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> has been system autoinstalled.
DFHPG0231	<i>date time applid terminal userid tranid</i> Autoinstall for program <i>progrname</i> in application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> of platform <i>platformname</i> failed. Program autoinstall model <i>modelname</i> is disabled.

Table 21. New messages in CICS Transaction Server for z/OS, Version 5 Release 2 (continued)

Message number	Message text
DFHPG0308	<i>date time applid</i> BUNDLE <i>bundlename</i> has associated an application entry point for operation <i>operationname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> , on platform <i>platformname</i> with PROGRAM <i>programname</i>
DFHPG0309	<i>date time applid</i> BUNDLE <i>bundlename</i> has disassociated an application entry point for operation <i>operationname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> , on platform <i>platformname</i> with PROGRAM <i>programname</i> .
DFHPG0310	<i>date time applid</i> BUNDLE <i>bundlename</i> unable to make available PROGRAM <i>programname</i> as an application entry point for operation <i>operationname</i> of application <i>applicationname</i> , version <i>majorversion.minorversion.microversion</i> , on platform <i>platformname</i> as {the PROGRAM name is invalid. the PROGRAM does not exist. the PROGRAM has the same name as an existing public PROGRAM. the operation is not unique within the application. an internal error occurred.}
DFHPG0311	<i>date time applid</i> BUNDLE <i>bundlename</i> has made the PROGRAM <i>programname</i> available as an entry point for operation <i>operationname</i>
DFHPG0312	<i>date time applid</i> BUNDLE <i>bundlename</i> has associated an application entry point for operation <i>operationname</i> with PROGRAM <i>programname</i>
DFHPG0500	<i>date time applid</i> The public version of the application entry point program <i>programname</i> for operation <i>operationname</i> of application <i>applicationname</i> on platform <i>platformname</i> is version <i>majorversion.minorversion.microversion</i> .
DFHPG0501	<i>date time applid</i> The public version of the application entry point program <i>programname</i> for operation <i>operationname</i> of application <i>applicationname</i> on platform <i>platformname</i> has changed from version <i>majorversion.minorversion.microversion</i> to version <i>majorversion.minorversion.microversion</i> .
DFHPG0502	<i>date time applid</i> All versions of the application entry point program <i>programname</i> for operation <i>operationname</i> of application <i>applicationname</i> on platform <i>platformname</i> are now unavailable.
DFHPI0200	<i>date time applid</i> BUNDLE <i>bundlename</i> has successfully installed PIPELINE <i>pipeline</i> in the {Disabled state. Enabling process initiated Disabled state}.
DFHPI0201	<i>date time applid</i> BUNDLE <i>bundlename</i> has failed to install PIPELINE <i>pipeline</i> because {the definition is invalid of an installation failure an internal error occurred}.
DFHPI0202	<i>date time applid</i> PIPELINE name was not specified or is too long in BUNDLE <i>bundlename</i> .
DFHPI0203	CONFIGFILE <i>path</i> in PIPELINE <i>pipelinename</i> is too long in BUNDLE <i>bundlename</i> .
DFHPI0204	<i>date time applid userid</i> PIPELINE <i>pipeline</i> is now ENABLED and is ready for use.
DFHPI0220	<i>date time applid</i> BUNDLE <i>bundlename</i> has successfully installed WEBSERVICE <i>webservice</i> in the {Disabled state. Enabling process initiated Disabled state}.
DFHPI0221	<i>date time applid</i> BUNDLE <i>bundlename</i> has failed to install WEBSERVICE <i>webservice</i> because {the definition is invalid of an installation failure an internal error occurred}.
DFHPI0222	<i>date time applid</i> WEBSERVICE name was not specified or is too long in BUNDLE <i>bundlename</i> .
DFHPI9715E	Expected keyword 'keyword' missing in line 'line'.
DFHPI9716E	Field 'name' not found for array 'array'.
DFHPI9717E	Unsupported content found after OCCURS DEPENDING ON field 'name'.
DFHPI9718E	Use of OCCURS DEPENDING ON requires use of DATA-TRUNCATION=ENABLED.
DFHPI9719E	Unsupported content found after group item 'name' with OCCURS DEPENDING ON clause.
DFHPI9720E	Unsupported keyword "UNBOUNDED" found in an OCCURS clause.

Table 21. New messages in CICS Transaction Server for z/OS, Version 5 Release 2 (continued)

Message number	Message text
DFHPI9721W	The parameter CCSID=1200 is not supported when <i>assistant</i> is used.
DFHPI9722E	The parameter CHAR-MULTIPLIER= <i>value</i> is not supported in combination with CCSID=1200.
DFHPI9723E	UTF-16 is not supported when parameter LANG=PLI-OTHER is used.
DFHPI9724E	Type <i>type</i> requires a minimum mapping level of <i>required-mapping-level</i> , but mapping level <i>actual-mapping-level</i> was specified.
DFHRL0133	<i>date time applid tranid</i> The CICS resource lifecycle manager failed to create the BUNDLE resource <i>bundle_name</i> because the <i>path_name</i> definition file was empty.
DFHRL0134 I	<i>date time applid userid</i> The CICS resource lifecycle manager has started to create BUNDLE <i>bundle_name</i> with bundle ID <i>bundle_id</i> and version <i>bundle_major.ver.bundle_minor.ver.bundle_micro.ver</i> on platform <i>platform_id</i> .
DFHRL0135 E	<i>date time applid tranid</i> The CICS resource lifecycle manager failed to associate { <i>an entry point</i> <i>a policy scope</i> } for resource_type resource <i>resource_name</i> in BUNDLE <i>bundle_name</i> because CICS does not support platform { <i>entry points.</i> <i>policy scopes.</i> }
DFHSJ1200	<i>date time applid</i> BUNDLE <i>bundlename</i> has successfully installed JVMSERVER <i>jvmserver</i> { <i>in a Disabled state.</i> <i>in a Disabled state.</i> }.
DFHSJ1203	DISABLE request for JVMSERVER <i>jvmserver</i> has been rejected.
DFHSO0137	<i>date time applid</i> BUNDLE <i>bundlename</i> has successfully installed TCPIPSERVICE <i>tcipservice</i> as { <i>Enabled</i> <i>Disabled</i> }.
DFHSO0140	IMMCLOSE request for TCPIPSERVICE <i>tcipservice</i> has been rejected.
DFHWB0803	<i>date time applid</i> HFSFILE path in URIMAP <i>urimap</i> is too long in BUNDLE <i>bundlename</i> .
DFHWB0804	<i>date time applid</i> BUNDLE <i>bundlename</i> failed to set URIMAP resource <i>urimap</i> as an application entry point because CICS does not support { <i>USAGE(CLIENT)</i> <i>USAGE(ATOM)</i> } for this resource type.
DFHWB0805	<i>date time applid</i> BUNDLE <i>currentbundlename</i> was unable to set the URIMAP <i>resourcenname</i> as an entry point because the resource is already defined as an entry point by BUNDLE <i>bundlename</i> .
DFHWB0806	<i>date time applid</i> BUNDLE <i>bundlename</i> has { <i>associated</i> <i>disassociated</i> } an application entry point from application (<i>applicationname</i>), version (<i>majorversion.minorversion.microversion</i>) on platform (<i>platformname</i>) with URIMAP <i>urimapname</i> .
DFHWB0807	<i>date time applid</i> BUNDLE <i>bundlename</i> has made { <i>available</i> <i>unavailable</i> } the application entry point for URIMAP <i>urimapname</i> with operation (<i>operationname</i>) for application (<i>applicationname</i>), version (<i>majorversion.minorversion.microversion</i>) on platform (<i>platformname</i>).
DFHWB0808	<i>date time applid</i> BUNDLE <i>bundlename</i> has failed to set URIMAP <i>urimapname</i> as an entry point because { <i>the URIMAP does not exist.</i> <i>an internal error occurred.</i> <i>the URIMAP resource name is invalid.</i> <i>the URIMAP resource is already defined as an application entry point.</i> }
DFHWB1580	<i>date time applid userid</i> The availability status of URIMAP <i>urimap</i> has { <i>been set to available</i> <i>been set to unavailable</i> <i>reverted to none</i> } following a change to an application entry point.
EYUNL0152W	<i>date time applid</i> Get Topology for private resource { <i>UNKNOWN</i> <i>PROGRAM</i> <i>LIBRARY</i> } failed, COMMAND= <i>cmdname</i> RESP= <i>respcode</i> RESP2= <i>reasoncode</i> .
EYUPM007I	<i>date time applid</i> The { <i>RTADEF</i> <i>STATDEF</i> } (<i>defname</i>) has been successfully deactivated manually for Context(<i>plexname</i>) Scope(<i>sysname</i>).
EYUPM008I	<i>date time applid</i> The { <i>RTADEF</i> <i>STATDEF</i> } (<i>defname</i>) has been successfully reactivated manually for Context(<i>plexname</i>) Scope(<i>sysname</i>).
EYUPP007I	<i>date time applid</i> RTADEF (<i>defname</i>) for APSPEC(<i>specname</i>) has been successfully deactivated manually for Context(<i>plexname</i>) Scope(<i>sysname</i>).

Table 21. New messages in CICS Transaction Server for z/OS, Version 5 Release 2 (continued)

Message number	Message text
EYUPP008I	<i>date time applid</i> RTADEF (<i>defname</i>) for APSPEC(<i>specname</i>) has been successfully reactivated manually for Context(<i>plexname</i>) Scope(<i>sysname</i>).
EYUWI0011E	<i>date time applid</i> WLM warmstart AOR normalization could not complete for all AORSCOPEs in all workloads for CONTEXT (<i>plexname</i>).
EYUWI0012E	<i>date time applid</i> WLM warmstart AOR normalization could not complete for AORSCOPE (<i>csysgrp</i>) in all workloads for CONTEXT (<i>plexname</i>).
EYUXD0718E	EYUDREP does not contain a CMASDEF record. The upgrade process has been terminated.
EYUXD0719I	Non maintenance point CICSplex <i>nnnnn</i> records not converted.
EYUXD0720E	EYU9XDU1 MP plex list {getmain freemain} failed. The upgrade process has been terminated.

Some of these new CICS messages are issued when actions such as installing and discarding are performed on private LIBRARY resources. The new messages provide the same information as for the corresponding actions on public LIBRARY resources, but they also state the platform, application, and application version to which the private LIBRARY resource applies, so that you can audit or troubleshoot the actions in the relevant context. Table 22 shows which new messages for private LIBRARY resources correspond to which existing CICS messages for public LIBRARY resources.

Table 22. Messages for private LIBRARY resources and public LIBRARY resources. Shows which new messages for private LIBRARY resources correspond to which existing CICS messages for public LIBRARY resources.

Public LIBRARY resource message (existing)	Private LIBRARY resource message (new)
DFHLD0501	DFHLD0508
DFHLD0502	DFHLD0509
DFHLD0505	DFHLD0510
DFHLD0503	DFHLD0514
DFHLD0504	DFHLD0515
DFHLD0505	DFHLD0510
DFHLD0512	DFHLD0516
DFHLD0513	DFHLD0517
DFHLD0523	DFHLD0526
DFHLD0524	DFHLD0527
DFHLD0525	DFHLD0528
DFHLD0710	DFHLD0733
DFHLD0711	DFHLD0734
DFHLD0712	DFHLD0735
DFHLD0713	DFHLD0736
DFHLD0715	DFHLD0737
DFHLD0720	DFHLD0738
DFHLD0721	DFHLD0739
DFHLD0722	DFHLD0740

Table 22. Messages for private LIBRARY resources and public LIBRARY resources (continued). Shows which new messages for private LIBRARY resources correspond to which existing CICS messages for public LIBRARY resources.

Public LIBRARY resource message (existing)	Private LIBRARY resource message (new)
DFHLD0723	DFHLD0741
DFHLD0724	DFHLD0742
DFHLD0725	DFHLD0743
DFHLD0730	DFHLD0744
DFHLD0731	DFHLD0745
DFHLD0732	DFHLD0746

Chapter 42. Deleted abend codes

These abend codes are discontinued in CICS Transaction Server for z/OS, Version 5 Release 2.

No abend codes were deleted in CICS Transaction Server for z/OS, Version 5 Release 2.

Chapter 43. New abend codes

These abend codes are new for CICS Transaction Server for z/OS, Version 5 Release 2.

Abend code	Abend text
AFDO	An attempt was made to attach a transaction specifying DFHFERN as the program to be given control, but the transaction was not internally attached by CICS. DFHFERN is for use by CICS system transaction CFCR. This transaction is used to disable a file defined in a CICS bundle.
AFDP	CICS failed to disable a file defined in a CICS bundle.
AXSE	The CICS security token service has been called without a channel.
AXSF	The CICS security token service encountered a severe error.
AXSG	The DFHSAML program is not running in CICS key.

Part 6. Appendixes

Notices

This information was developed for products and services offered in the U.S.A. IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply in the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore this statement may not apply to you.

This publication could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Licensees of this program who want to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact IBM United Kingdom Laboratories, MP151, Hursley Park, Winchester, Hampshire, England, SO21 2JN.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Programming License Agreement, or any equivalent agreement between us.

Privacy Policy Considerations

IBM Software products, including software as a service solutions, ("Software Offerings") may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering's use of cookies is set forth below.

CICSplex SM Web User Interface :

For the WUI main interface: Depending upon the configurations deployed, this Software Offering may use session and persistent cookies that collect each user's user name and other personally identifiable information for purposes of session management, authentication, enhanced user usability, or other usage tracking or functional purposes. These cookies cannot be disabled.

For the WUI Data Interface: Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's user name and other personally identifiable information for purposes of session management, authentication, or other usage tracking or functional purposes. These cookies cannot be disabled.

For the WUI Hello World page: Depending upon the configurations deployed, this Software Offering may use session cookies that collect no personally identifiable information. These cookies cannot be disabled.

For CICS Explorer: Depending upon the configurations deployed, this Software Offering may use session and persistent preferences that collect each user's user name and password, for purposes of session management, authentication, and single sign-on configuration. These preferences cannot be disabled, although storing a user's password on disk in encrypted form can only be enabled by the user's explicit action to check a check box during sign-on.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, see IBM's Privacy Policy at <http://www.ibm.com/privacy> and IBM's Online Privacy Statement at <http://www.ibm.com/privacy/details> the section entitled "Cookies, Web Beacons and Other Technologies" and the "IBM Software Products and Software-as-a-Service Privacy Statement" at <http://www-01.ibm.com/software/info/product-privacy/>.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information at www.ibm.com/legal/copytrade.shtml.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Bibliography

CICS books for CICS Transaction Server for z/OS

General

CICS Transaction Server for z/OS Program Directory, GI13-3326
CICS Transaction Server for z/OS What's New, GC34-7302
CICS Transaction Server for z/OS Upgrading from CICS TS Version 3.1, GC34-7296
CICS Transaction Server for z/OS Upgrading from CICS TS Version 3.2, GC34-7297
CICS Transaction Server for z/OS Upgrading from CICS TS Version 4.1, GC34-7298
CICS Transaction Server for z/OS Upgrading from CICS TS Version 4.2, GC34-7299
CICS Transaction Server for z/OS Upgrading from CICS TS Version 5.1, GC34-7300
CICS Transaction Server for z/OS Installation Guide, GC34-7279

Access to CICS

CICS Internet Guide, SC34-7281
CICS Web Services Guide, SC34-7301

Administration

CICS System Definition Guide, SC34-7293
CICS Customization Guide, SC34-7269
CICS Resource Definition Guide, SC34-7290
CICS Operations and Utilities Guide, SC34-7285
CICS RACF Security Guide, SC34-7288
CICS Supplied Transactions, SC34-7292

Programming

CICS Application Programming Guide, SC34-7266
CICS Application Programming Reference, SC34-7267
CICS System Programming Reference, SC34-7294
CICS Front End Programming Interface User's Guide, SC34-7277
CICS C++ OO Class Libraries, SC34-7270
CICS Distributed Transaction Programming Guide, SC34-7275
CICS Business Transaction Services, SC34-7268
Java Applications in CICS, SC34-7282

Diagnosis

CICS Problem Determination Guide, GC34-7287
CICS Performance Guide, SC34-7286
CICS Messages and Codes Vol 1, GC34-7283
CICS Messages and Codes Vol 2, GC34-7284
CICS Diagnosis Reference, GC34-7274
CICS Recovery and Restart Guide, SC34-7289
CICS Data Areas, GC34-7271
CICS Trace Entries, SC34-7295
CICS Debugging Tools Interfaces Reference, GC34-7273

Communication

CICS Intercommunication Guide, SC34-7280
CICS External Interfaces Guide, SC34-7276

Databases

CICS DB2 Guide, SC34-7272

CICS IMS™ Database Control Guide, SC34-7278

CICS Shared Data Tables Guide, SC34-7291

CICSplex SM books for CICS Transaction Server for z/OS

General

CICSplex SM Concepts and Planning, SC34-7306

CICSplex SM Web User Interface Guide, SC34-7316

Administration and Management

CICSplex SM Administration, SC34-7303

CICSplex SM Operations Views Reference, SC34-7312

CICSplex SM Monitor Views Reference, SC34-7311

CICSplex SM Managing Workloads, SC34-7309

CICSplex SM Managing Resource Usage, SC34-7308

CICSplex SM Managing Business Applications, SC34-7307

Programming

CICSplex SM Application Programming Guide, SC34-7304

CICSplex SM Application Programming Reference, SC34-7305

Diagnosis

CICSplex SM Resource Tables Reference Vol 1, SC34-7314

CICSplex SM Resource Tables Reference Vol 2, SC34-7315

CICSplex SM Messages and Codes, GC34-7310

CICSplex SM Problem Determination, GC34-7313

Other CICS publications

The following publications contain further information about CICS, but are not provided as part of CICS Transaction Server for z/OS, Version 5 Release 2.

Designing and Programming CICS Applications, ISBN: 1-56592-676-5

CICS Application Migration Aid Guide, SC33-0768

CICS Family: API Structure, SC33-1007

CICS Family: Client/Server Programming, SC33-1435

CICS Family: Interproduct Communication, SC34-6853

CICS Family: Communicating from CICS on System/390, SC34-6854

CICS Transaction Gateway for z/OS Administration, SC34-5528

CICS Family: General Information, GC33-0155

CICS 4.1 Sample Applications Guide, SC33-1173

CICS/ESA 3.3 XRF Guide , SC33-0661

Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully.

You can perform most tasks required to set up, run, and maintain your CICS system in one of these ways:

- using a 3270 emulator logged on to CICS
- using a 3270 emulator logged on to TSO
- using a 3270 emulator as an MVS system console

IBM Personal Communications provides 3270 emulation with accessibility features for people with disabilities. You can use this product to provide the accessibility features you need in your CICS system.

Index

A

abend codes, deleted 161
abend codes, new 163
activation module 4
Application Associated Data exit,
new 45
APPLICATION option 10
 CEMT INQUIRE URIMAP
 command 35
 EXTRACT STATISTICS command 23
 INQUIRE URIMAP command 28
application programming interface
 ASSIGN (changed) 9
 BIF DEEDIT (made threadsafe) 12
 BIF DIGEST (made threadsafe) 12
 CHANGE PASSWORD (made
 threadsafe) 12
 changed commands 9
 DEFINE COUNTER (made
 threadsafe) 12
 DEFINE DOUNTER (made
 threadsafe) 12
 DELETE (made threadsafe) 12
 DELETE COUNTER (made
 threadsafe) 12
 DELETE DOUNTER (made
 threadsafe) 12
 DELETEQ TD (made threadsafe) 12
 DELETEQ TS (made threadsafe) 12
 ENDBR (made threadsafe) 12
 EXEC DLI (made threadsafe) 12
 EXTRACT CERTIFICATE (made
 threadsafe) 12
 EXTRACT TCPIP (made
 threadsafe) 12
 GET CONTAINER (changed) 9
 GET COUNTER (made
 threadsafe) 12
 GET DOUNTER (made
 threadsafe) 12
 JCICS support 13
 LINK (changed) 9
 LOAD PROGRAM (changed) 9
 made threadsafe 12
 new commands 11
 PUT CONTAINER (changed) 9
 QUERY COUNTER (made
 threadsafe) 12
 QUERY DOUNTER (made
 threadsafe) 12
 QUERY SECURITY (made
 threadsafe) 12
 READ (made threadsafe) 12
 READNEXT (made threadsafe) 12
 READPREV (made threadsafe) 12
 READQ TD (made threadsafe) 12
 READQ TS (made threadsafe) 12
 RESETBR (made threadsafe) 12
 REWIND COUNTER (made
 threadsafe) 12

application programming interface
(*continued*)
 REWIND DOUNTER (made
 threadsafe) 12
 REWRITE (made threadsafe) 12
 SIGNOFF (made threadsafe) 12
 SIGNON (made threadsafe) 12
 START (changed) 9
 START CHANNEL (changed) 9
 STARTBR (made threadsafe) 12
 SYNCPOINT (made threadsafe) 12
 SYNCPOINT ROLLBACK (made
 threadsafe) 12
 UNLOCK (made threadsafe) 12
 UPDATE COUNTER (made
 threadsafe) 12
 UPDATE DOUNTER (made
 threadsafe) 12
 VERIFY PASSWORD (changed) 9
 VERIFY PASSWORD (made
 threadsafe) 12
 VERIFY PHRASE (changed) 9
 WAIT JOURNALNAME (made
 threadsafe) 12
 WAIT JOURNALNUM (made
 threadsafe) 12
 WRITE (made threadsafe) 12
 WRITE JOURNALNAME (made
 threadsafe) 12
 WRITE JOURNALNUM (made
 threadsafe) 12
 WRITEQ TD (made threadsafe) 12
 WRITEQ TS (made threadsafe) 12
application programs
 compiler support 83
APPLID system initialization
 parameter 5
APPLMAJORVER option
 CEMT INQUIRE URIMAP
 command 35
 EXTRACT STATISTICS command 23
 INQUIRE URIMAP command 28
APPLMICROVER option
 CEMT INQUIRE URIMAP
 command 35
 EXTRACT STATISTICS command 23
 INQUIRE URIMAP command 28
APPLMINORVER option
 CEMT INQUIRE URIMAP
 command 35
 EXTRACT STATISTICS command 23
 INQUIRE URIMAP command 28
ASSIGN command 9, 10
ATOMSERVICE resource definition 17
AVAILABLE
 CEMT INQUIRE URIMAP 35
 CEMT SET BUNDLE 36
AVAILSTATUS
 CEMT INQUIRE BUNDLE 34
 CEMT INQUIRE URIMAP 35

AVAILSTATUS option
 INQUIRE URIMAP command 28
 SET BUNDLE command 24, 29

B

BIF DEEDIT command 12
BIF DIGEST command 12
BUNDLE resource definition 17
Business Transaction Services (BTS)
 upgrading 85

C

CBSRVNM 57
CDSASZE 76
CEMT
 upgrading 33
CEMT commands 37
 DISCARD ATOMSERVICE (new) 37
 DISCARD BUNDLE (new) 37
 DISCARD IPCONN (new) 37
 DISCARD JVMSERVER (new) 37
 DISCARD LIBRARY (new) 37
 DISCARD MQCONN (new) 37
 INQUIRE ATOMSERVICE (new) 37
 INQUIRE BUNDLE (new) 37
 INQUIRE CLASSCACHE
 (changed) 33
 INQUIRE DISPATCHER
 (changed) 33
 INQUIRE EPADAPTER (new) 37
 INQUIRE EPADAPTERSET (new) 37
 INQUIRE EVENTBINDING (new) 37
 INQUIRE EVENTPROCESS (new) 37
 INQUIRE IPCONN (new) 37
 INQUIRE JVM (changed) 33
 INQUIRE JVMSERVER (new) 37
 INQUIRE LIBRARY (new) 37
 INQUIRE MONITOR (changed) 33
 INQUIRE MQCONN (new) 37
 INQUIRE MQINI (new) 37
 INQUIRE TEMPSTORAGE (new) 37
 INQUIRE TSMODEL (changed) 33
 INQUIRE TSQNAME (changed) 33
 INQUIRE TSQUEUE (changed) 33
 INQUIRE XMLTRANSFORM
 (new) 37
 PERFORM JVMPOOL (new) 37
 PERFORM STATISTICS (changed) 33
 SET ATOMSERVICE (new) 37
 SET BUNDLE (new) 37
 SET DISPATCHER (changed) 33
 SET DOCTEMPLATE (new) 37
 SET EPADAPTER (new) 37
 SET EPADAPTERSET (new) 37
 SET EVENTBINDING (new) 37
 SET EVENTPROCESS (new) 37
 SET IPCONN (new) 37
 SET JVMPOOL (changed) 33

- CEMT commands (*continued*)
 - SET JVMSERVER (new) 37
 - SET MQCONN (new) 37
 - SET XMLTRANSFORM (new) 37
 - CEMT DISCARD ATOMSERVICE
 - command 37
 - CEMT DISCARD BUNDLE
 - command 37
 - CEMT DISCARD IPCONN command 37
 - CEMT DISCARD JVMSERVER
 - command 37
 - CEMT DISCARD LIBRARY
 - command 37
 - CEMT DISCARD MQCONN
 - command 37
 - CEMT INQUIRE ATOMSERVICE
 - command 37
 - CEMT INQUIRE BUNDLE command 37
 - CEMT INQUIRE EPADAPTER
 - command 37
 - CEMT INQUIRE EPADAPTERSET
 - command 37
 - CEMT INQUIRE EVENTBINDING
 - command 37
 - CEMT INQUIRE EVENTPROCESS
 - command 37
 - CEMT INQUIRE IPCONN command 37
 - CEMT INQUIRE JVMSERVER
 - (changed) 33
 - CEMT INQUIRE JVMSERVER
 - command 37
 - CEMT INQUIRE LIBRARY (changed) 33
 - CEMT INQUIRE LIBRARY command 37
 - CEMT INQUIRE MQCONN
 - command 37
 - CEMT INQUIRE MQINI command 37
 - CEMT INQUIRE TEMPSTORAGE
 - command 37
 - CEMT INQUIRE URIMAP 33
 - CEMT INQUIRE URIMAP (changed) 33
 - CEMT INQUIRE XMLTRANSFORM
 - command 37
 - CEMT PERFORM DUMP 33
 - CEMT PERFORM JVMPPOOL
 - command 37
 - CEMT PERFORM SNAP 33
 - CEMT SET ATOMSERVICE
 - command 37
 - CEMT SET BUNDLE command 37
 - CEMT SET DOCTEMPLATE
 - command 37
 - CEMT SET EPADAPTER command 37
 - CEMT SET EPADAPTERSET
 - command 37
 - CEMT SET EVENTBINDING
 - command 37
 - CEMT SET EVENTPROCESS
 - command 37
 - CEMT SET IPCONN command 37
 - CEMT SET JVMSERVER command 37
 - CEMT SET MQCONN command 37
 - CEMT SET XMLTRANSFORM
 - command 37
 - CEMT, changes 33
 - CHANGE PASSWORD command 12
 - changed CEMT commands 33
 - changed CSD groups
 - DFHPGAIP 17
 - changed global user exit programs
 - XRSINDI 44
 - changed messages 147
 - changed system initialization
 - parameters 5
 - changes
 - affecting the SPI 19
 - to user-replaceable programs 51
 - CICS Explorer
 - upgrading 81
 - CICS management client interface (CMCI)
 - upgrading 39
 - CICS_HOME system initialization
 - parameter 6
 - CICS-supplied transactions
 - CEMT INQUIRE JVMSERVER (changed) 33
 - CEMT INQUIRE LIBRARY (changed) 33
 - CEMT INQUIRE URIMAP (changed) 33
 - CEPD 69
 - CEPF 69
 - CEPH 69
 - CEPM 69
 - CEPQ 69
 - CEPT 69
 - CESL 69
 - CFCR 69
 - changed CEMT commands 33
 - changes to CEMT 33
 - changes to CSFE 41
 - CICS-supplied transactions
 - DFH\$CAT1 CLIST 69
 - CIS4 69
 - CISB 69
 - CISC 69
 - CISD 69
 - CISE 69
 - CISM 69
 - CISQ 69
 - CISR 69
 - CISS 69
 - CIST 69
 - CISU 69
 - CISX 69
 - CJGC 69
 - CJPI 69
 - CJSR 69
 - CRLR 69
 - new CEMT commands 37
 - new RACF category 1
 - transactions 69
 - obsolete CEMT command options 33
 - upgrading 33, 41
 - CICS-WebSphere MQ adapter 95
 - CICS-WebSphere MQ connection 95
 - CICSplex SM
 - connecting to previous releases 125
 - class paths for JVM 91
 - CLINTCP system initialization
 - parameter 6
 - cloud
 - security 67, 69
 - compiler support 83
 - CONFDATA system initialization
 - parameter 5
 - control tables
 - upgrading 18
 - CREATE IPCONN command 20
 - CREATE PROGRAM command 20
 - CREATE TCPIP SERVICE command 20
 - CRLSERVER system initialization
 - parameter 6
 - CSD
 - sharing between releases 77
 - CSD, upgrading 74
 - SCAN function 75
 - CSDLSRNO system initialization
 - parameter 5
 - CSFE, changes 41
 - CVDA values 11
 - AVAILABLE
 - INQUIRE URIMAP command 28
 - NONE
 - INQUIRE URIMAP command 28
- ## D
- data conversion
 - upgrading 73
 - data sets
 - start up 4
 - DB2
 - attachment facility 97
 - upgrading 97
 - DB2WAIT 57
 - DEFINE COUNTER command 12
 - DEFINE D COUNTER command 12
 - DELETE command 12
 - DELETE COUNTER command 12
 - DELETE D COUNTER command 12
 - deletedabend codes 161
 - deleted messages 145
 - DELETEQ TD command 12
 - DELETEQ TS command 12
 - DFH\$CCI (obsolete CSD group) 16
 - DFH\$EJB (obsolete CSD group) 16
 - DFH\$EJB2 (obsolete CSD group) 16
 - DFH\$IIOP (obsolete CSD group) 16
 - DFH\$JAVA (obsolete CSD group) 16
 - DFH\$JVM (obsolete CSD group) 16
 - DFHADET (obsolete CSD group) 16
 - DFHADST (obsolete CSD group) 16
 - DFHCNV
 - upgrading 18
 - DFHCOMPB (obsolete CSD group) 16
 - DFHCOMP C, compatibility group 77
 - DFHCOMP D, compatibility group 77
 - DFHCOMP E, compatibility group 77
 - DFHCOMP F, compatibility group 77
 - DFHCOMP G, compatibility group 77
 - DFHCSDUP
 - upgrading 55
 - DFHCSVCupgrading 89
 - DFHDCT, obsolete 18
 - DFHEJBU (obsolete CSD group) 16
 - DFHFCRL, CSD group 17
 - DFHIIOP (obsolete CSD group) 16
 - DFHIRPupgrading 89
 - DFHJVM DD card 91
 - DFHJVMCD 91

- DFHJVMRO 91
- DFHLRQ data set 85
 - migrating 85
- DFHMCT monitoring control table
 - upgrading 18
- DFHPDxxx
 - upgrading 55
- DFHPGADX 17
- DFHPGAHX 17
- DFHPGAIP 17
- DFHPGALX 17
- DFHPGAOX 17
- DFHSIT, default system initialization table 5
- DFHSJJ8O 91
- DFHSTUP
 - upgrading 55
- DFHTUxxx
 - upgrading 55
- DFHUEPAR
 - upgrading 44
- dfjvmcd.props 91
- DSAs
 - setting the size of 76

E

- ECDSASZE 76
- EDSALIM system initialization
 - parameter 5
- EJBCRECT 57
- EJBMTHCT 57
- EJBREMCT 57
- EJBROLEPRFX system initialization
 - parameter 5
- EJBSACCT 57
- EJBSPACT 57
- EJBTOTCT 57
- ENABLE PROGRAM command 20
- ENCRYPTION system initialization
 - parameter 5
- ENDBR command 12
- enterprise beans
 - upgrading 91
- ERDSASZE 76
- ERRORMSG option
 - ASSIGN command 9
- ERRORMSGELN option
 - ASSIGN command 9
- ESDSASZE 76
- EUDSASZE 76
- EXEC CICS commands
 - API commands, changed 9
 - API commands, made threadsafe 12
 - API commands, new 11
 - SPI command options, obsolete 19
 - SPI commands, changed 20
 - SPI commands, new 30
 - SPI commands, obsolete 19
- EXEC CICS commandsDISCARD
 - PROGRAMDISCARD TRANSACTION
 - DISCARD PROGRAM (made threadsafe) 31
 - DISCARD TRANSACTION (made threadsafe) 31
 - SPI commands, made threadsafe 31
- EXEC DLI command 12

- exit programming interface (XPI)
 - new calls 49
 - upgrading 48
- EXPIRYINTMIN attribute
 - TSMODEL definition 21
- EXTRACT CERTIFICATE command 12
- EXTRACT TCPIP command 12

F

- FCLJ gate 5
- FCQRONLY system initialization
 - parameter 5, 6
- FILE resource definition 16

G

- GENERICTCPS option 27
- GET CONTAINER command 9
- GET COUNTER command 12
- GET DCOUNTER command 12
- global user exits
 - changed programs 44
 - new programs 45
 - upgrading 44

H

- HTTP client open exit, new 45
- HTTP client send exit, new 45

I

- ICVTSD system initialization
 - parameter 5
- IIOPLISTENER system initialization
 - parameter 5
- initialization programs 51
- INITPARM system initialization
 - parameter 5
- INQUIRE ASSOCIATION 20
- INQUIRE BUNDLE 20
- INQUIRE BUNDLE command 20
- INQUIRE BUNDLEPART command 20
- INQUIRE CAPTURESPEC command 20
- INQUIRE CLASSCACHE CEMT
 - command 33
- INQUIRE DISPATCHER CEMT
 - command 33
- INQUIRE DISPATCHER command 20
- INQUIRE DSNAM 20
- INQUIRE EVENTBINDING
 - (changed) 20
- INQUIRE FILE command 31
- INQUIRE IPCONN command 20
- INQUIRE JVM CEMT command 33
- INQUIRE JVMSERVER command 20
- INQUIRE LIBRARY 20
- INQUIRE MONITOR CEMT
 - command 33
- INQUIRE PROGRAM command
 - (changed) 20
- INQUIRE SYSTEM command 20
- INQUIRE TCIPSERVICE command 20
- INQUIRE TRACEDEST command 31

- INQUIRE TRACEFLAG command 31
- INQUIRE TRACETYPE (changed) 20
- INQUIRE TRACETYPE command 31
- INQUIRE TSMODEL CEMT
 - command 33
- INQUIRE TSQNAME CEMT
 - command 33
- INQUIRE TSQUEUE CEMT
 - command 33
- INQUIRE UOWLINK command 20
- INQUIRE WEB command 31
- interregion communication program (DFHIRP)upgrading 89
- IPCONN resource definition 16, 17
- IPIC connection intersystem queues exit, new 45

J

- J8CPUT 57
- J9CPUT 57
- Java
 - upgrading 91
- Java applications
 - upgrading 91
- JCICS classes 13
- JCICS methods 13
- JCL 4
- JVM
 - class paths
 - for shared class cache 91
 - resettable (no longer used) 91
 - shared class cache 91
 - upgrading 91
- JVM profiles
 - upgrading 91
- JVMPROFILEDIR system initialization
 - parameter 5
- JVMSERVER resource definition 17

L

- LIBRARY resource definition 17
- LINK command 9
- LINKLEVEL option
 - ASSIGN command 10
- LOAD PROGRAM command 9
- LOCAL 11
- LOCALCCSID system initialization
 - parameter 6
- LOGREPSTATUS 20
- LSRPOOL resource definition 16
- LSRPOOLID 15

M

- macro resource definition
 - upgrading 18
- MAJORVERSION option 10
- master JVM 91
- MAXJTDLY 57
- MAXJVMTCBS system initialization
 - parameter 5
- MAXSSLTCBS system initialization
 - parameter 6
- MEMLIMIT 3

MESSAGECASE option
 INQUIRE SYSTEM command 27
 messages, changed 147
 messages, deleted 145
 messages, new 153
 MICROVERSION option 10
 migrate 49
 migrating
 SAML 103
 MINORVERSION option 10
 MLXSCTM 57
 MNIDN system initialization
 parameter 6
 MNSUBSYS system initialization
 parameter 5
 monitoring control table, DFHMCT
 upgrading 18
 monitoring data, obsolete 57
 MQCONN resource definition 17
 MQCONN system initialization
 parameter 5
 MRO (multiregion
 operation)upgrading 89
 MSGCASE system initialization
 parameter 5
 multiregion operation
 (MRO)upgrading 89
 MVSSMFID option
 INQUIRE SYSTEM command 27
 MVSSYSNAME option
 INQUIRE SYSTEM command 27
 MXT system initialization parameter 5

N

new abend codes 163
 new CEMT commands 37
 new CSD groups
 DFHFCRL 17
 new messages 153
 new resource definition attributes 16
 new resources 17
 new system initialization parameters 6
 new user-exit programs 45
 NOTAPPLIC
 CEMT INQUIRE URIMAP 35

O

obsolete CSD groups
 DFH\$CCI 16
 DFH\$EJB 16
 DFH\$EJB2 16
 DFH\$IIOP 16
 DFH\$JAVA 16
 DFH\$JVM 16
 DFHADET 16
 DFHADST 16
 DFHCOMPB 16
 DFHEJBU 16
 DFHIIOP 16
 obsolete system initialization
 parameters 5
 obsolete user-replaceable programs 51
 OO COBOL 83
 OPERATION option 10

OPERATION option (*continued*)
 CEMT INQUIRE URIMAP
 command 36
 INQUIRE URIMAP command 29
 OS/VS COBOL 83

P

PERFORM STATISTICS CEMT
 command 33
 PIPELINE resource definition 16
 PLATFORM option 10
 CEMT INQUIRE URIMAP
 command 36
 EXTRACT STATISTICS command 23
 INQUIRE URIMAP command 29
 PORT option
 INQUIRE UOWLINK command 28
 PROFILEDIR
 CEMT INQUIRE JVMSERVER 34
 program compatibility, SPI 19
 PROGRAM resource definition 16
 PSTYPE system initialization
 parameter 5
 PUT CONTAINER command 9

Q

QUERY COUNTER command 12
 QUERY DOUNTER command 12
 QUERY SECURITY command 12

R

RACFSYNC 6
 RDO
 obsolete attributes 15
 RDSASZE 76
 READ command 12
 READNEXT command 12
 READPREV command 12
 READQ TD command 12
 READQ TS command 12
 repository data set 85
 upgrading 85
 RESETBR command 12
 resettable JVM
 withdrawal 91
 resource definition
 changes 15
 resource definition (online)
 obsolete RDO attributes 15
 upgrading the CSD
 SCAN function 75
 resource definitions
 ATOMSERVICE (new) 17
 BUNDLE (new) 17
 changed 16
 FILE (changed) 16
 IPCONN (changed) 16
 IPCONN (new) 17
 JVMSERVER (new) 17
 LIBRARY (new) 17
 LSRPOOL (changed) 16
 MQCONN (new) 17
 new attributes 16

resource definitions (*continued*)

 new resources 17
 PIPELINE (changed) 16
 PROGRAM (changed) 16
 TCPIPSERVICE (changed) 16
 TSMODEL (changed) 16
 URIMAP (changed) 16
 RESYNC ENTRYNAME command 31
 REWIND COUNTER command 12
 REWIND DCOUNTER command 12
 REWRITE command 12

S

SAML
 migrating 103
 upgrading 103
 SCEERUN 91
 SCEERUN2 91
 SDFJAUTH 91
 SDSASZE 76
 SECVFYFREQ system initialization
 parameter 6
 SET DISPATCHER CEMT command 33
 SET JVMPOOL CEMT command 33
 SET PROGRAM command 20
 SET STATISTICS command 20
 SET SYSTEM command 20
 SET TASK command 31
 SET TRACEDEST command 31
 SET TRACEFLAG command 31
 SET TRACETYPE (changed) 20
 SET TRACETYPE command 31
 SET WEB command 31
 shareable application class path 91
 shared class cache 91
 shutdown programs 51
 SIGNOFF command 12
 SIGNON command 12
 SIT (system initialization table)
 parameters 5
 SMF 110 records
 upgrading 57
 SPECIFTCPS option 27
 SRVERCP system initialization
 parameter 6
 SSLCACHE system initialization
 parameter 6
 START CHANNEL command 9
 START command 9
 STARTBR command 12
 statistics 59
 changed 59
 new 61
 obsolete 59
 STRINGZONE option
 FORMATTIME command 11
 SYNCPOINT command 12
 SYNCPOINT ROLLBACK command 12
 system initialization parameters 5
 APPLID (changed) 5
 changed 5
 CICS_HOME (new) 6
 CLINTCP (new) 6
 CONFDATA (changed) 5
 CRLSERVER (new) 6
 CSDLSRNO (changed) 5

system initialization parameters
(continued)

EDSALIM (changed) 5
EJBROLEPRFX (obsolete) 5
ENCRYPTION (changed) 5
FCQRONLY (changed) 5
FCQRONLY (new) 6
ICVTSD (changed) 5
IIOPLISTENER (obsolete) 5
INITPARM (changed) 5
JVMPROFILEDIR (changed) 5
LOCALCCSID (new) 6
MAXJVMTCBS (obsolete) 5
MAXSSLTCBS (new) 6
MAXXPTCBS (obsolete) 5
MNIDN (new) 6
MNSUBSYS (obsolete) 5
MQCONN (changed) 5
MSGCASE (changed) 5
MXT (changed) 5
new 6
obsolete 5
PSTYPE (changed) 5
SECVFYFREQ (new) 6
SRVERCP (new) 6
SSLCACHE (new) 6
TBEXITS (changed) 5
TCTUALOC (changed) 5
TRTABSZ (changed) 5
TRTRANSZ (changed) 5
TSMMAINLIMIT (new) 6
UOWNETQL (changed) 5
USRDELAY (changed) 5
USSCONFIG (new) 6
XEJB (obsolete) 5
XHFS (new) 6
XRES (new) 6

system initialization table
default 5

system programming interface

changed commands 20
CREATE IPCONN (changed) 20
CREATE PROGRAM (changed) 20
CREATE TCPIP SERVICE
(changed) 20
ENABLE PROGRAM (changed) 20
INQUIRE ASSOCIATION
(changed) 20
INQUIRE BUNDLE (changed) 20
INQUIRE BUNDLEPART
(changed) 20
INQUIRE CAPTURESPEC
(changed) 20
INQUIRE DISPATCHER
(changed) 20
INQUIRE FILE (made threadsafe) 31
INQUIRE IPCONN (changed) 20
INQUIRE JVM SERVER (changed) 20
INQUIRE LIBRARY (changed) 20
INQUIRE PROGRAM (changed) 20
INQUIRE SYSTEM (changed) 20
INQUIRE TCPIP SERVICE
(changed) 20
INQUIRE TRACEDEST (made
threadsafe) 31
INQUIRE TRACEFLAG (made
threadsafe) 31

system programming interface (continued)

INQUIRE TRACETYPE (made
threadsafe) 31
INQUIRE UOWLINK (changed) 20
INQUIRE URIMAP (changed) 20
INQUIRE WEB (made threadsafe) 31
made threadsafe 31
new commands 30
obsolete commands
CREATE CORBASERVER 19
CREATE DJAR 19
CREATE REQUESTMODEL 19
DISCARD CORBASERVER 19
DISCARD DJAR 19
DISCARD REQUESTMODEL 19
INQUIRE BEAN 19
INQUIRE CORBASERVER 19
INQUIRE DJAR 19
INQUIRE REQUESTMODEL 19
INQUIRE WORKREQUEST 19
SET CORBASERVER 19
SET WORKREQUEST 19
obsolete options
COLLECT STATISTICS 19
CREATE FILE 19
CREATE LSRPOOL 19
CREATE PROGRAM 19
CSD INSTALL 19
INQUIRE DISPATCHER 19
INQUIRE FILE 19
INQUIRE PROGRAM 19
PERFORM STATISTICS 19
SET DISPATCHER 19
SET FILE 19
SET PROGRAM 19

obsolete SPI command options 19

obsolete SPI commands 19

RESYNC ENTRYNAME (made
threadsafe) 31
SET PROGRAM (changed) 20
SET STATISTICS (changed) 20
SET SYSTEM (changed) 20
SET TASK (made threadsafe) 31
SET TRACEDEST (made
threadsafe) 31
SET TRACEFLAG (made
threadsafe) 31
SET TRACETYPE (made
threadsafe) 31
SET WEB (made threadsafe) 31

system programming interface (SPI) 19

T

task-related user exits
upgrading 45
TBEXITS system initialization
parameter 5
TCPIP SERVICE resource definition 16
TCTUALOC system initialization
parameter 5
trademarks 169
TRTABSZ system initialization
parameter 5
TRTRANSZ system initialization
parameter 5

TSMMAINLIMIT system initialization
parameter 6
TSMODEL definition
EXPIRYINTMIN attribute 21
TSMODEL resource definition 16

U

UDSASZE 76
UNAVAILABLE
CEMT SET BUNDLE 36
UNLOCK command 12
UOWNETQL system initialization
parameter 5
UPDATE COUNTER command 12
UPDATE DCOUNTER command 12
upgrading
SAML 103
upgrading CICSplex SM
upgrading a CMAS 135
upgrading a MAS 141
upgrading JSON assistant 101
upgrading the CSD 74
SCAN function 75
URIMAP definition
USAGE attribute 16
URIMAP resource definition 16
USAGE attribute
URIMAP definition 16
user-replaceable programs 51
changed user-replaceable
programs 51
obsolete user-replaceable
programs 51
USRDELAY system initialization
parameter 5
USSCONFIG system initialization
parameter 6
UTC 11

V

VERIFY PASSWORD command 9, 12
VERIFY PHRASE command 9

W

WAIT JOURNALNAME command 12
WAIT JOURNALNUM command 12
worker JVM 91
WRITE command 12
WRITE JOURNALNAME command 12
WRITE JOURNALNUM command 12
WRITEQ TD command 12
WRITEQ TS command 12

X

XAPADMGR, new user exit 45
XEJB system initialization parameter 5
XEP CAP 45
XHFS system initialization parameter 6
XISQUE, new user exit 45
XRES system initialization parameter 6
XWBAUTH, new user exit 45

XWBOPEN, new user exit 45
XWBSNDO, new user exit 45

Z

z/OS conversion services 73

Readers' Comments — We'd Like to Hear from You

CICS Transaction Server for z/OS
Version 5 Release 2
Upgrading from CICS TS Version 5.1

Publication No. GC34-7300-01

We appreciate your comments about this publication. Please comment on specific errors or omissions, accuracy, organization, subject matter, or completeness of this book. The comments you send should pertain to only the information in this manual or product and the way in which the information is presented.

For technical questions and information about products and prices, please contact your IBM branch office, your IBM business partner, or your authorized remarketer.

When you send comments to IBM, you grant IBM a nonexclusive right to use or distribute your comments in any way it believes appropriate without incurring any obligation to you. IBM or any other organizations will only use the personal information that you supply to contact you about the issues that you state on this form.

Comments:

Thank you for your support.

Submit your comments using one of these channels:

- Send your comments to the address on the reverse side of this form.
- Send a fax to the following number: +44 1962 816151
- Send your comments via email to: idrctf@uk.ibm.com

If you would like a response from IBM, please fill in the following information:

Name

Address

Company or Organization

Phone No.

Email address

Read
GC34-7300-01

s — We'd Like to Hear from You



Cut or Fold
Along Line

Fold and Tape

Please do not staple

Fold and Tape

PLACE
POSTAGE
STAMP
HERE

IBM United Kingdom Limited
User Technologies Department (MP189)
Hursley Park
Winchester
Hampshire
United Kingdom
SO21 2JN

Fold and Tape

Please do not staple

Fold and Tape



GC34-7300-01

