CICS Transaction Server for z/OS
Version 6

What's New

Note

Before using this information and the product it supports, read the information in Product Legal Notices.

This edition applies to the IBM® CICS® Transaction Server for z/OS®, Version 6 (product number 5655-YA1) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

About this PDF

"What's New" is a summary of the new features and capabilities of CICS Transaction Server for z/OS. Details of how to use these features is provided in the rest of the product documentation. It also summarizes any changes to CICS externals, such as the application programming interface, for this version of CICS TS. *What's New* is aimed at application programmers and system programmers who need to understand the scope of the new release.

For details of the terms and notation used in this book, see Conventions and terminology used in the CICS documentation in IBM Documentation.

Date of this PDF

This PDF was created on 2024-06-11 (Year-Month-Date).

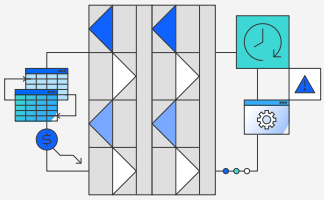
Chapter 1. What's new in CICS TS 6.2?

CICS Transaction Server for z/OS, Version 6 enables development teams to create powerful mixed-language applications, while allowing the operational teams to manage these applications from a single point of control.

On this page, find out what CICS TS 6.2 offers. You might also like to refer to the CICS Transaction Server for z/OS Version 6.2 announcement letter. Find the capabilities of CICS TS 6.1 in What's New for CICS TS 6.1.

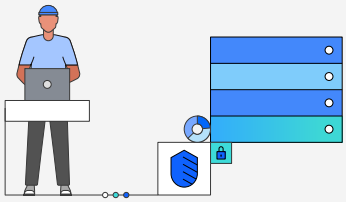
For a summary of capabilities that were introduced before CICS Transaction Server for z/OS, Version 6, see Changes between releases in Upgrading. (In PDF, it's in *Upgrading CICS*. New features in CICS Explorer® are described in the CICS Explorer product documentation.

Release highlights



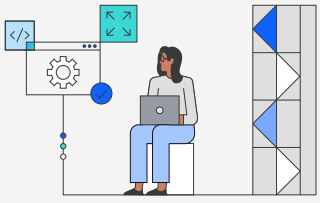
Reduced cost of management and resilience

CICS administrators can further optimize applications with threadsafe access to shared data tables and reduce volumes of data written to SMF. They can automate more with CICS policies and Ansible, and use functions of IBM Z to continue to improve resilience and scalability.



Improved security and compliance management

System programmers and security administrators can migrate to and maintain a zero trust strategy easily with new features such as security discovery, security definition capture, and new security defaults of transactions. TLS support is also extended for enhanced security.



Enhanced developer productivity

Developers can use new features in the latest versions of Java, Jakarta, Spring Boot, and Node.js to modernize and extend applications in CICS.

All the enhancements at a glance

Some enhancements are shown under more than one category; the information is the same in all cases.

- For the developer experience:
  - “Support for Java 17” on page 3
  - “Support for Jakarta Enterprise Edition 10” on page 3
  - “Enhanced container support” on page 3

- "Machine translation of documentation" on page 13
- "Archived publications added to CICS documentation" on page 13
- "Enhanced information" on page 13
- "PDF" on page 13

For the developer experience

- "Support for Java 17" on page 3
- "Support for Jakarta Enterprise Edition 10" on page 3
- "Enhanced container support" on page 3
- "Support for Node.js 18" on page 3
- "Support for Liberty collectives" on page 3

Support for Java™ 17

This release adds support for Java 17 using IBM Semeru Runtime Certified Edition for z/OS. A minimum version of 17.0.7.0 is required.

Java 17 is not supported for use with SAML JVM servers at all CICS releases. To enable Db2® type 2 connectivity with Java 17, add `LIBPATH_SUFFIX=/usr/lpp/db2v12/jdbc/lib` to the JVM profile.

Java 8 and Java 11 continue to be supported.

Learn more...

Support for Jakarta Enterprise Edition 10

The CICS Liberty JVM server now supports Jakarta Enterprise Edition (EE) 10.

Learn more...

Enhanced container support

CICS API, EXCI, JCICS API and JCICSX API support prepending data to the existing data in a container. New option PREPEND is introduced on **`PUT CONTAINER (CHANNEL)`**, **`PUT64 CONTAINER`**, and **`PUT CONTAINER (EXCI)`** commands. New methods `prepend()` and `prependString()` are introduced to the JCICS `container` class. New methods `appendWith()`, `prepend()`, and `prependWith()` are introduced to JCICSX classes `BITContainer` and `WritableBITContainer` and a new method `prepend()` is introduced to JCICSX classes `CHARContainer`, `WritableCHARContainer`, and `WritableContainer`.

Learn more...

Support for Node.js 18

Developers can use Node.js 18 to build microservices and web applications using the latest JavaScript features and frameworks, with optimized access to CICS TS programs by using the ibm-cics-api API. This support requires IBM Open Enterprise SDK for Node.js 18.

Learn more...

Support for Liberty collectives

In a system that hosts multiple Liberty servers, including Liberty JVM servers, it can be useful to manage and monitor these servers, and their applications, from a centralized administrative control point.

Learn more...

For system management

- " New DFHRL messages for GRPLIST installation of BUNDLE resources" on page 4
- "Enhanced support for GRPLIST" on page 4

New DFHRL messages for GRPLIST installation of BUNDLE resources

New messages DFHRL0137I and DFHRL0138W indicate whether all GRPLIST-defined BUNDLE resources are installed and reached their target status, as defined by the STATUS attribute on their BUNDLE resource definitions. The new messages help you to determine when a CICS region is open for business and ready for workload to be routed its way.

DFHRL0137I indicates a successful GRPLIST installation of BUNDLE resources that are at their target initial status. DFHRL0138W is issued if one or more BUNDLEs failed to be installed; you can refer to previous DFHAM4938 messages to identify the failed BUNDLEs.

Learn more...

Enhanced support for GRPLIST

You can now retrieve GRPLIST in a number of ways:

- Regions view of CICS Explorer
- CEMT INQUIRE SYSTEM
- INQUIRE SYSTEM SPI command
- CICSPlex SM **CICS region** (CICSRGN) view

This enhancement provides you with alternatives to obtain the names of the lists containing resource definition groups that are loaded during system initialization for a CICS cold start.

Learn more...

Enhancements to CICS policies

- New option to set the WLMHEALTH time interval is supported by the **Set z/OS WLM health open status** system rule action.

  You can now change the region's WLMHEALTH time interval as part of the system rule action. This enhancement makes it easier for you to manage the z/OS WLM health of a CICS region by using a variety of policy system rules.

  This capability is also available on CICS TS 6.1 with APAR PH58295.

  Learn more ...
- A new system rule, transaction class queued tasks, monitors when the number of tasks queuing for membership to a TRANCLASS approaches the TRANCLASS purge threshold and enables CICS to take a policy action in response. This policy system rule can give you an early warning on the situation and take precautionary measures.

  Learn more ...

Health check on stabilized functions

Out-of-date technology inside CICS TS for z/OS is often stabilized and might be reduced in capability or discontinued in a future release. Stabilized functions that are still in use might expose CICS to potential risks, reduction of performance, or constraints in capability. It is highly recommended that you upgrade to modern technology and functions and make the most of new CICS capabilities.

A new health check, CICS_STABILIZED_FUNCTIONS can alert you to the use of outdated, stabilized technology and functions in your CICS regions.

Learn more ...

Resilience to surging requests for TRANCLASS-managed transactions

Transaction classes control the maximum number of tasks that can be dispatched and queued for transactions that belong to an active transaction class. In an ideal situation, a CICS region with well-tuned transaction classes handles workloads by dispatching and queuing tasks so that requests are served within an expected response time. However, in an abnormal situation - for example, if tasks have built up as a result of a slow-down or a surge of requests into the CICS region - further requests are purged according to the PURGETRESH of the TRANCLASS and transaction abends occur. CICS TS 6.2 introduces several enhancements including the capability to monitor queued tasks so that you are aware of the situation and the option to control TRANCLASS purge actions.

A new system rule, transaction class queued tasks, monitors when the number of tasks queuing for membership to a TRANCLASS approaches the TRANCLASS purge threshold and enables CICS to take a policy action in response. This policy system rule can give you an early warning on the situation and take precautionary measures.

Instead of resolving to the purge action of an AKCC abend as it did in previous CICS releases, CICS TS 6.2 can discard a request to start a transaction when its associated TRANCLASS has reached the purge threshold. This avoids unnecessary transaction abends that would otherwise occur and consume even more from a constrained system. To support this enhancement, the TRANCLASS resource definition has a new attribute PURGEACTION through which you can set the purge action to DISCARD or ABEND. CICS API, SPI, and statistics have been enhanced to support PURGEACTION. In a workload routing environment, it is important to ensure a consistent use of purge action for a workload. See The queue algorithm and The link neutral queue algorithm.

Learn more...

- Transaction class queued tasks system rule
- TRANCLASS resources
- Using PURGETHRESH and PURGEACTION

CICSPlex® SM can now process type 71 ENF events for a CICSplex

This enhancement can help to reduce a significant amount of system overload that would otherwise occur for processing large numbers of type 71 ENF events.

RACF sends a type 71 ENF signal to listeners when a **CONNECT**, **REMOVE**, or **REVOKE** command changes a users' resource authorization, or when a user ID is revoked as a result of too many failed password attempts. A CMAS can now listen for type 71 ENF events and make type 71 ENF event data available for its connected MAS regions to consume. This means that MAS regions can obtain type 71 ENF event data directly from the owning CMAS, without the need to register as a type 71 ENF event listener themselves.

A new option CPSM is introduced on the RACFSYNC system initialization parameter. A MAS region must be started with RACFSYNC=CPSM so that it does not register as a type 71 ENF event listener but still processes type 71 ENF event data obtained from its connected CMAS.

For CICSPlex SM security, when a CMAS region that is set with RACFSYNC=YES receives a type 71 ENF event, security information for the affected user ID is rebuilt the next time the user ID is used, irrespective of the setting of the SECTIMEOUT parameter.

Learn more ...

CICS opens TCPIPSERVICE automatically after a TCP/IP restart

Available with z/OS 2.5 and higher, ENF event code 80 signals when a TCP/IP stack and its extended services have been fully initialized. CICS can now respond to ENF 80 events and automatically set the TCPIPSERVICE status back to OPEN if it was set to CLOSED as a result of an outage of TCP/IP.

Learn more...

Integration of CICS and CICSPlex SM shutdowns

You can now use **PERFORM SHUTDOWN** and **PERFORM SHUTDOWN IMMEDIATE**, or their CEMT equivalents, directly on CMAS and MAS regions. In processing the command, CICS shuts down the CMAS or stops the MAS agent code as part of the shutdown process. The integration of CICS and CICSPlex SM shutdowns makes system management of CICSPlex SM environments easier.

Learn more...

Monitoring use of CICSPlex SM Data Repository

You are now alerted when the CICSPlex SM Data Repository EYUDREP exceeds 70% of its capacity so that you have time to review the space allocation for the data set to ensure that it has sufficient capacity for intended system operations.

The owning CMAS issues message EYUXD1032 when EYUDREP exceeds 70% of its available extents in either of its DATA or INDEX components.

Learn more...

Suppress SMF records with zero-counting fields

Transaction and Program statistics that contain zero count fields following a reset are suppressed for interval, requested, and requested reset type statistics. This reduces SMF volume at most of the times that CICS statistics are being generated, retaining the ability to use CICS statistics as a way to inventory CICS resources.

Learn more...

Updated CMCI JVM server requirements

CMCI JVM server now requires Java version 11 or later.

Expanded Ansible® IBM z/OS CICS collection to automate CICS resource and region actions

CICS TS 6.2 extends the IBM z/OS CICS collection collection that was introduced in CICS TS 6.1 (see “Ansible IBM z/OS CICS collection to automate CICS resource and region actions” on page 44) and provided modules for working with the CICS TS system management CMCI REST API. The collection is extended to provide a set of modules for provisioning and managing CICS TS data sets and utilities. You can use these Ansible modules to create automation tasks that provision, start, stop, and deprovision a CICS region. Sample playbooks show you how to do this with the latest version of the Ansible IBM z/OS CICS collection.

The IBM z/OS CICS collection collection is developed as an open-source project at IBM z/OS CICS collection GitHub and is available on Ansible Galaxy and Ansible Automation Hub.

Learn more...

Operator for CICS integration with Red Hat® OpenShift® Container Platform

IBM CICS Transaction Server Operator Collection (CICS TS Operator Collection) can drive Ansible CICS region provisioning through the Red Hat OpenShift Container Platform interface. Through z/OS Cloud Broker, you can provision an instance of a CICS TS region and manage CICS TS resources in Red Hat OpenShift Container Platform.

Learn more...

For security

- “Zero trust enhancements” on page 7

- "TLS enhancements" on page 8
- "New options on SIGNON, CHANGE PASSWORD, and CHANGE PHRASE reveal more sign-on information" on page 9
- "New options on XPPT allow you to secure remote programs at a lower cost" on page 9
- "Command security checking removed for INQUIRE TERMINAL, INQUIRE NETNAME, and SET TERMINAL when programs or tasks inquire on or set their own terminals" on page 9
- "Enhancements to surrogate security for JCL job submissions to the JES internal reader" on page 9
- "CICSPlex SM can now process type 71 ENF events for a CICSplex" on page 5
- "Mandatory initialization parameters for WUI or SMSSJ if security is active" on page 10
- "Monitoring and statistics fields to audit QUERY SECURITY LOGMESSAGE(NOLOG) requests" on page 10
- "Updated WS-Security requirements" on page 10

Zero trust enhancements

To conform with a zero trust strategy and various compliance regulations such as PCI-DSS, you need to protect your sensitive data. In CICS this means enabling resource security and command security in regions where sensitive data exists, and configuring RACF with profiles to protect your resources so that they can only be accessed by users who have a business reason to do so. The user needs to be connected to a group (role) that needs access to one or more transactions and other resources that represent an application.

CICS provides security discovery for easier migration to zero trust, enables command and resource security for both CICS and user transactions to conform with zero trust, and eases maintenance of zero trust with security definition capture (SDC) and security definition validation (SDV).

- Use **CICS security discovery** to identify security definitions that are required for resource security in production regions.

  With security discovery, you analyze RACF definitions, optionally with usage data (security discovery data) by using the **Security Discovery** perspective in CICS Explorer and convert the resulting security metadata back to RACF commands to implement resource security. Currently it has some restrictions.

  You can work with SDD using the **Security Discovery Records** view in CICS Explorer or the INQUIRE SECDISCOVERY, PERFORM SECDISCOVERY WRITE, and SET SECDISCOVERY SPI commands.

  Learn more ...

- After implementing required security definitions, **enable command security (CMDSEC) and resource security (RESSEC)** in production.

  All CICS transactions, excluding CJXA and CICSPlex SM transactions (CO**), are defined with `CMDSEC(YES)` and `RESSEC(YES)` to conform with this practice.

  Existing user transaction definitions stay unchanged, but new transaction use `CMDSEC(YES)` and `RESSEC(YES)` by default.

  You must review and update security definitions for potential command and resource security checking. For instructions, see Review security definitions for command and resource security implementation.

  Learn more about CICS transaction changes ...

  Learn more about TRANSACTION changes ...

- Use **CICS security definition capture (SDC)** to capture security definitions that are required for command and resource security, even during development.

  After you have migrated to a zero trust strategy, you can identify and implement required changes to security definitions when there's a code change before pushing the changes to a production region with full CICS security.

You can further automate and integrate that process into your CI/CD (continuous integration/continuous delivery) pipeline as part of a DevSecOps approach. CICS offers an example implementation of a full CI pipeline, known as **security definition validation (SDV)**.

Learn more ...

TLS enhancements

- Default cipher suite specification file for outbound web requests.

  The `com.ibm.cics.web.defaultcipherfile` feature toggle is extended to apply to URIMAP resources with no ciphers specified.

  Message DFHWB1561 is issued to indicate that a URIMAP defined with `CIPHERS()` is being installed and list the ciphers that CICS uses instead.

  This capability is also available in CICS TS 6.1 with APAR PH60212.

  Learn more ...

- SIT parameter `CERTEXPIRYWARN` allows CICS to warn about expiring certificates in the certificate chain.

  The new `CERTEXPIRYWARN` SIT parameter allows CICS to warn about such expiring certificates so that you can take action before the certificate expires and the TLS connection fails.

  `CERTEXPIRYWARN` checks only certificates that are sent by the partner system through TLS connections. For CICS managed certificates, that is, certificates defined in RACF, use the RACF_CERTIFICATE_EXPIRATION check provided by IBM Health Checker for z/OS instead.

  When `CERTEXPIRYWARN` is enabled in web owning regions, CICS issues message DFHSO1100I when the certificate is about to expire within a specified range of days. CICS also issues a trace entry if the SO trace level is set to 2.

  Learn more ...

- Key rings can be more easily shared between CICS regions.

  KEYRING system initialization parameter accepts more formats of key ring name so that you can use key rings that are not owned by the current region user ID.

  This capability is also available in CICS TS 5.5 and 5.6 with APAR PH49253, and CICS TS 6.1 with APAR PH49261.

  Learn more ...

- Minimum key size used during TLS handshakes is increased.

  For increased key strength, CICS uses a minimum key size of 256 for ECC keys and 2048 for RSA, DSA and Diffie-Hellman keys during TLS handshakes. You must increase the key sizes within your certificates. Otherwise, the TLS handshake fails and message DFHSO0123 is issued with a return code of 508.

  To continue using a small key size, set feature toggle `com.ibm.cics.tls.minimumkeystrength=1024`. This feature toggle allows you to set a minimum key size for ECC, RSA, DSA, and Diffie-Hellman keys during TLS handshakes. This feature toggle is also available in CICS TS 5.4, 5.5, 5.6 with APAR PH50175, and 6.1 with APAR PH51719.

  Learn more ...

- Sysplex caching for TLS 1.3 is supported.

  Sharing information about the SSL session across different CICS regions in a sysplex is particularly useful when HTTP requests are being routed across a set of CICS regions by using TCP/IP connection workload balancing techniques, such as TCP/IP port sharing or Sysplex Distributor. CICS now supports sysplex caching for TLS 1.3 in addition to previous support for sysplex caching in earlier versions of TLS.

  Learn more...

- HTTP strict transport security (HSTS) is supported.

  HTTP strict transport security (HSTS) helps servers prevent man-in-the-middle attacks by instructing compliant user agents to only interact with the server through secure connections (HTTPS).

  You can now configure a CICS server to use HSTS with a set of `com.ibm.cics.web.hsts` feature toggles.

  This feature is also available in CICS TS 5.5 and 5.6 with APAR PH55369, and 6.1 with APAR PH55370.

  Learn more...

New options on SIGNON, CHANGE PASSWORD, and CHANGE PHRASE reveal more sign-on information

New options CHANGETIME, DAYSLEFT, EXPIRYTIME, INVALIDCOUNT, and LASTUSETIME are added to SIGNON, CHANGE PASSWORD, and CHANGE PHRASE commands. These options reveal more sign-on information, for example, the last time the password or password phrase was changed, the last time the user ID was accessed, when the password or password phrase will expire, and the number of times when an invalid password or password phrase was entered.

Messages DFHCE3549 and DFHSN1100 are also updated to show the number of previous failed attempts to sign on, and the date and time the user ID was last accessed.

The new options on **CHANGE PASSWORD** and **CHANGE PHRASE** are also available in CICS TS 5.5 and 5.6 with APAR PH59546, and 6.1 with APAR PH59547.

New options on XPPT allow you to secure remote programs at a lower cost

A new option DPLONLY is added to the XPPT system initialization parameter. By specifying DPLONLY on XPPT (XPPT=(YES,DPLONLY) or XPPT=(*class_name*,DPLONLY)), CICS checks only the first program that is linked by the mirror program (DFHMIRS) during distributed program link (DPL). This can reduce the security cost while retaining control over remotely linked programs.

The ALL (default) option maintains the behavior in CICS TS 6.1 and earlier. When ALL is specified over DPLONLY, CICS performs the security check on *all* invoked programs.

Learn more ...

Command security checking removed for INQUIRE TERMINAL, INQUIRE NETNAME, and SET TERMINAL when programs or tasks inquire on or set their own terminals

For **INQUIRE TERMINAL**, **INQUIRE NETNAME**, and **SET TERMINAL**, command security checking is not performed if the task or program that issues the command was started or attached to the same terminal that is being inquired or modified by the command, with a few exceptions. This is because resource security checking was already performed on the terminal when the program or task was started or attached to the terminal. With this enhancement, programs or tasks that inquire or set their own terminals won't need full access to these commands. Therefore, it not just simplifies the security management, but also improves security by avoiding granting more access than is necessary.

Learn more ...

Enhancements to surrogate security for JCL job submissions to the JES internal reader

Surrogate security for JCL job submissions to the internal reader is now streamlined under the control of the XUSER system initialization parameter and is enabled by default. As a result, the `com.ibm.cics.spool.surrogate.check={true|false}` feature toggle is removed.

A new system initialization parameter, INTRDRJOBUSER is introduced. It specifies a default job user ID to be used when you submit a JCL job using **SPOOL** commands and the JOB card does not specify the USER parameter. The default of INTRDRJOBUSER is to use the task user ID, but you can specify INTRDRJOBUSER=REGION to use the CICS region user ID instead. The INTRDRJOBUSER system initialization parameter replaces the feature toggle `com.ibm.cics.spool.defaultjobuser={region|task}`.

Learn more ...

Mandatory initialization parameters for WUI or SMSSJ if security is active

For a CICSPlex SM WUI server (CPSMCONN=WUI), TCPIPSSL is now mandatory if security is active.

For a CICS System Management Single Server (SMSS) defined with CPSMCONN=SMSSJ, CMCISSL is mandatory if security is active.

Learn more about WUI initialization parameters ...

Learn more about SMSS options ...

CICSPlex SM can now process type 71 ENF events for a CICSplex

This enhancement can help to reduce a significant amount of system overload that would otherwise occur for processing large numbers of type 71 ENF events.

RACF sends a type 71 ENF signal to listeners when a **CONNECT**, **REMOVE**, or **REVOKE** command changes a users' resource authorization, or when a user ID is revoked as a result of too many failed password attempts. A CMAS can now listen for type 71 ENF events and make type 71 ENF event data available for its connected MAS regions to consume. This means that MAS regions can obtain type 71 ENF event data directly from the owning CMAS, without the need to register as a type 71 ENF event listener themselves.

A new option CPSM is introduced on the RACFSYNC system initialization parameter. A MAS region must be started with RACFSYNC=CPSM so that it does not register as a type 71 ENF event listener but still processes type 71 ENF event data obtained from its connected CMAS.

For CICSPlex SM security, when a CMAS region that is set with RACFSYNC=YES receives a type 71 ENF event, security information for the affected user ID is rebuilt the next time the user ID is used, irrespective of the setting of the SECTIMEOUT parameter.

Learn more ...

Monitoring and statistics fields to audit QUERY SECURITY LOGMESSAGE(NOLOG) requests

The **QUERY SECURITY** command allows you to query the security authorization of a user to access a resource. For enhanced protection against brute-force attacks, new monitoring and statistics fields are introduced so that you can still monitor the **QUERY SECURITY** requests even when violation messages are inhibited:

- The statistics field XSG_AUTHOR_FAIL_NL_NA (DFHSTUP name **Failed authorizations NOLOG NOTAUTH**) and monitoring field XSNLNACT to record the number of **QUERY SECURITY LOGMESSAGE(NOLOG)** requests that succeeded but returned no authority on READ, UPDATE, CONTROL or ALTER.
- The statistics field XSG_AUTHOR_FAIL_NL_NF (DFHSTUP name **Failed authorizations NOLOG NOTFND**) and monitoring field XSNLNFCT to record the number of **QUERY SECURITY LOGMESSAGE(NOLOG)** requests that failed with response code 13 NOTFND and reason code 5 or 8.

Learn more about security statistics

Learn more...

Updated WS-Security requirements

The IBM XML Toolkit for z/OS prerequisite has been updated to v1.11.

Learn more...

For performance

- "Read and browse requests to shared data tables are threadsafe" on page 11
- "CICSPlex SM can now process type 71 ENF events for a CICSplex" on page 5

Read and browse requests to shared data tables are threadsafe

The following commands, when used to access a CICS maintained or user maintained shared data table, can now run on an open TCB as well as on the QR TCB:

- READ (without the UPDATE option)
- STARTBR
- READNEXT (without the UPDATE option)
- READPREV (without the UPDATE option)
- ENDBR
- RESETBR

Commands that update a shared data table (READ with UPDATE, REWRITE, READNEXT with UPDATE, READPREV with UPDATE, DELETE, WRITE) are not threadsafe and continue to run only on the QR TCB. The loading of shared data tables is also unaffected by this change and executes always on the QR TCB.

The use of threadsafe READ and BROWSE access to shared data tables, thereby allowing file control requests to have cross memory access on open TCBs, can only be achieved when both the AOR and the FOR are at CICS TS 6.2 or higher.

Learn more...

CICSPlex SM can now process type 71 ENF events for a CICSplex

This enhancement can help to reduce a significant amount of system overload that would otherwise occur for processing large numbers of type 71 ENF events.

RACF sends a type 71 ENF signal to listeners when a **CONNECT**, **REMOVE**, or **REVOKE** command changes a users' resource authorization, or when a user ID is revoked as a result of too many failed password attempts. A CMAS can now listen for type 71 ENF events and make type 71 ENF event data available for its connected MAS regions to consume. This means that MAS regions can obtain type 71 ENF event data directly from the owning CMAS, without the need to register as a type 71 ENF event listener themselves.

A new option CPSM is introduced on the RACFSYNC system initialization parameter. A MAS region must be started with RACFSYNC=CPSM so that it does not register as a type 71 ENF event listener but still processes type 71 ENF event data obtained from its connected CMAS.

For CICSPlex SM security, when a CMAS region that is set with RACFSYNC=YES receives a type 71 ENF event, security information for the affected user ID is rebuilt the next time the user ID is used, irrespective of the setting of the SECTIMEOUT parameter.

Learn more ...

For resilience

- "Enhanced SOS protection and monitoring of z/OS MEMLIMIT storage in the 64-bit addressing range" on page 11
- "Resilience to surging requests for TRANCLASS-managed transactions" on page 5
- "Suppress SMF records with zero-counting fields" on page 6
- "Sysplex caching for TLS 1.3 is supported" on page 12
- "Enhanced exploitation of Instruction Execution Protection" on page 12

Enhanced SOS protection and monitoring of z/OS MEMLIMIT storage in the 64-bit addressing range

CICS introduces the capability to monitor the part of 64-bit z/OS storage that is allocated by the z/OS MEMLIMIT parameter. CICS periodically monitors the state of unallocated z/OS storage available to the CICS region in its z/OS address space, against a short-on-storage (SOS) threshold set by the new system initialization parameter Z0SS0S64UNALL0C. CICS issues console messages to notify you of

SOS conditions. You can use system policy rules that are triggered by these SOS messages, with an action to set the z/OS WLM health value to 0, so as to limit new work coming to the affected region.

Storage manager global statistics include new fields that report on the state of unallocated storage in the z/OS MEMLIMIT storage and on SOS conditions that have occurred to it. These statistics help you understand your current use of the z/OS MEMLIMIT storage, track fluctuations in the storage usage overtime, and identify and avoid SOS conditions that might occur.

Learn more...

Resilience to surging requests for TRANCLASS-managed transactions

Transaction classes control the maximum number of tasks that can be dispatched and queued for transactions that belong to an active transaction class. In an ideal situation, a CICS region with well-tuned transaction classes handles workloads by dispatching and queuing tasks so that requests are served within an expected response time. However, in an abnormal situation - for example, if tasks have built up as a result of a slow-down or a surge of requests into the CICS region - further requests are purged according to the PURGETRESH of the TRANCLASS and transaction abends occur. CICS TS 6.2 introduces several enhancements including the capability to monitor queued tasks so that you are aware of the situation and the option to control TRANCLASS purge actions.

A new system rule, transaction class queued tasks, monitors when the number of tasks queuing for membership to a TRANCLASS approaches the TRANCLASS purge threshold and enables CICS to take a policy action in response. This policy system rule can give you an early warning on the situation and take precautionary measures.

Instead of resolving to the purge action of an AKCC abend as it did in previous CICS releases, CICS TS 6.2 can discard a request to start a transaction when its associated TRANCLASS has reached the purge threshold. This avoids unnecessary transaction abends that would otherwise occur and consume even more from a constrained system. To support this enhancement, the TRANCLASS resource definition has a new attribute PURGEACTION through which you can set the purge action to DISCARD or ABEND. CICS API, SPI, and statistics have been enhanced to support PURGEACTION. In a workload routing environment, it is important to ensure a consistent use of purge action for a workload. See The queue algorithm and The link neutral queue algorithm.

Learn more...

- Transaction class queued tasks system rule
- TRANCLASS resources
- Using PURGETHRESH and PURGEACTION

Suppress SMF records with zero-counting fields

Transaction and Program statistics that contain zero count fields following a reset are suppressed for interval, requested, and requested reset type statistics. This reduces SMF volume at most of the times that CICS statistics are being generated, retaining the ability to use CICS statistics as a way to inventory CICS resources.

Learn more...

Sysplex caching for TLS 1.3 is supported

Sharing information about the SSL session across different CICS regions in a sysplex is particularly useful when HTTP requests are being routed across a set of CICS regions by using TCP/IP connection workload balancing techniques, such as TCP/IP port sharing or Sysplex Distributor. CICS now supports sysplex caching for TLS 1.3 in addition to previous support for sysplex caching in earlier versions of TLS.

Learn more...

Enhanced exploitation of Instruction Execution Protection

This release introduces further CICS exploitation of Instruction Execution Protection (IEP) beyond its use for CICS-managed storage and CICS dynamic storage areas (DSAs). Now the majority of requests for z/OS storage issued by CICS for its own internal purposes have been converted to use

a STORAGE OBTAIN call that specifies that non-executable storage is used, thereby protecting CICS internal use of z/OS storage from errors such as stack overflow and malicious attacks. This applies to 24-bit, 31-bit, and 64-bit z/OS storage. Protection is provided if CICS is running on a level of IBM Z hardware and operating system that support IEP regardless of the setting of feature toggle `com.ibm.cics.sm.iep`. The feature toggle only controls whether IEP is applied to CICS-managed storage and CICS DSAs.

Learn more...

For documentation and other information

Version 6 documentation

This documentation covers both CICS TS 6.2 and CICS TS 6.1. Differences between the releases are highlighted with tags in both HTML and PDF, like this: 6.2 and 6.1.

The release tags indicate functional difference between Version 6 releases. They do not imply applicability for Version 5 releases. Refer to Upgrading or the CICS TS Version 5 documentation for clarification.

Machine translation of documentation

CICS online documentation and IBM Documentation Offline are now translated in languages other than English: Brazilian Portuguese, French, German, Italian, Japanese, Korean, Simplified Chinese, and Spanish. PDF documentation is not currently translated.

Archived publications added to CICS documentation

Some archived IBM publications, including the *IBM 3270 Data Stream Programmers Reference*, are provided for download from Archived CICS documentation. These publications are referenced by some CICS messages and are provided as-is.

Enhanced information

Some areas of the documentation are rewritten to make them easier to work with:

- Trace information. Terms related to trace are consolidated and explained in Terms to understand about CICS trace. A new section How it works: Tracing in CICS expands the explanation of basic concepts such as trace points, trace levels, trace destinations, and different types of CICS trace. z/OS trace is now covered in Using z/OS trace for problem determination.
- Security information. All Security for Java applications documentation is re-written. How it works topics, examples, or both are added for security of JCICSX applications, Java APIs, Java threads and tasks, and so on. Configuration tasks are added for syncToOSThread, LDAP, and OAuth 2.0. Diagrams and best practices are added to most of the documentation about securing CICS.

PDF

Any information in IBM Docs that is not available in PDF is listed in Documentation in PDF. Some of the biggest PDFs are split to make them easier to work with. *CICS Messages* is now in 3 parts. The *Diagnosis Reference* is split into *Component Reference*, *Domain Reference*, and *Executable Module Reference*.

Learn more...

Chapter 2. Changes to CICS externals in CICS TS 6.2

Every release of CICS introduces changes to the elements that you see and work with, collectively known as the CICS *externals*. These include commands, transactions, resources, system initialization parameters, messages, trace, and user exits, and more. This page summarizes the changes for CICS TS 6.2.

For a summary of changes across all supported releases, see Changes between releases in the Upgrading information. (In PDF, it's in *Upgrading CICS*.

Changes to installing

- New compatibility groups DFHCOMPK and DFHCOMK2 introduced for sharing CSD with earlier releases.
- Shared data table changes:
  - DFHDTCV is removed. It is now link-edited as part of DFHDTSVC.
  - DFHDTSVC is supplied in SDFHAUTH instead of SDFHLINK, and it is no longer LPA eligible.

Changes to security

Table 1. Changes to security in CICS TS 6.2

Area	**6.2**
Authentication	**NEW:** • NEW SIT parameter CERTEXPIRYWARN allows CICS to warn about expiring certificates received from the partner system over TLS connections. A new message DFHSO1100I is returned to provide diagnostic information about the expiring certificate. A new trace point (SO 0863) is provided to return diagnostic information about the exporting certificate. **CHANGED:** • New options CHANGETIME, DAYSLEFT, EXPIRYTIME, INVALIDCOUNT, and LASTUSETIME added to SIGNON, CHANGE PASSWORD, and CHANGE PHRASE commands to reveal more information about the sign-on user ID and password.

Table 1. Changes to security in CICS TS 6.2 (continued)	
Area	**6.2**
Authorization	**CHANGED:** • To conform with a zero trust strategy, all CICS transactions, excluding CJXA and CICSPlex SM transactions (CO**), are defined with CMDSEC(YES) and RESSEC(YES) to enable command security and resource security. For a list of CICS transactions that require extra security configuration, see CICS transactions subject to security checking. • To conform with a zero trust strategy, the default values of CMDSEC and RESSEC attributes are changed to YES for all newly defined TRANSACTION resources. • CICS security discovery helps you identify security definitions that are required for resource security and hence eases the migration to zero trust. As part of the security discovery support: – The new **Security Discovery** perspective in CICS Explorer provides support for security discovery analysis. – The new **Security Discovery Records** view in CICS Explorer or new SPI commands (**INQUIRE SECDISCOVERY**, **PERFORM SECDISCOVERY**, and **SET SECDISCOVERY**) help you collect the security discovery data (SDD). • To maintain a zero trust strategy: – Security definition capture (SDC) identifies security definitions that would be required if security were on during development. – Security definition validation (SDV) is the CICS-supplied example implementation of a full CI pipeline that utilizes SDC within its automated testing stage and initiates an approval process for security changes. • CICS surrogate user checking is made if system initialization parameter **XUSER=YES** is in effect. The default job user ID for a JOB card that is submitted, without a USER parameter, by using **SPOOL** commands to the internal reader, is subject to the INTRDRJOBUSER system initialization parameter instead of a feature toggle that is now made obsolete. By the default of INTRDRJOBUSER, the task user ID is assumed while in 5.5 through 6.1 the CICS region user ID is assumed. • Command security checking removed for **INQUIRE TERMINAL**, **INQUIRE NETNAME**, and **SET TERMINAL** commands when programs or tasks inquire or set their own terminals, with a few exceptions.

Table 1. Changes to security in CICS TS 6.2 (continued)	
Area	**6.2**
Confidentiality	**NEW:** • New message DFHIS2041 indicates an attempt to acquire the named IPCONN failed because of unsecured TCPIP connections with a partner system that is located outside the sysplex. • Feature toggle `com.ibm.cics.tls.minimumkeystrength` allows you to set a minimum key size for ECC, RSA, DSA, and Diffie-Hellman keys during TLS handshakes. **CHANGED:** • The **KEYRING** SIT parameter accepts more formats of key ring names, which allows you to specify key rings that are not owned by the region user ID. • Sysplex caching for TLS 1.3 is supported. See SSLCACHE system initialization parameter. • CICS sets a minimum key size of 256 for ECC keys and 2048 for RSA, DSA and Diffie-Hellman keys during TLS handshakes. If a smaller key is used, the TLS handshake fails and message DFHSO0123 is issued with a return code of 508. Take action as described in Increase minimum key size for TLS connections. • Feature toggle `com.ibm.cics.web.defaultcipherfile` is extended to apply to URIMAP resources with no ciphers specified. • Cipher suites that use NULL, Triple DES (3DES) and RC4 encryption are removed from the sample default cipher suite specification file (`defaultciphers.xml`) that CICS supplies. See “Changes to samples” on page 36. • For a CICSPlex SM WUI server (CPSMCONN=WUI), initialization parameter **TCPIPSSL** is now mandatory if security is active. • For a CICS System Management Single Server (SMSS) defined with CPSMCONN=SMSSJ, initialization parameter **CMCISSL** is mandatory if security is active.
Integrity	**NEW:** HTTP strict transport security (HSTS) is supported when CICS acts as a server.
Auditing	**CHANGED:** • For the **QUERY SECURITY** command, CICS statistics and monitoring data are recorded even when logging is disabled. • New CICS health check CICS_STABILIZED_FUNCTIONS checks whether any outdated, stabilized technology, capabilities, or functions are used in the CICS region.
Performance	**CHANGED:** • New DPL0NLY option on **XPPT** allows you to secure remote program at a lower cost. • CICSPlex SM can now process type 71 ENF events for a CICSplex. A CMAS that is started with the system initialization parameter **RACFSYNC=YES** listens for type 71 ENF events and propagates them to its connected MAS regions that are started with the system initialization parameter **RACFSYNC=CPSM**.

Changes to RACF classes

No changes in CICS TS 6.2.

Changes to compiler and translator support

Table 2. Changes to compiler and translator support in CICS TS 6.2	
Support	**6.2**
Compiler	No changes in this release.
Translator	**CHANGED:** • The translator will no longer attempt to overcome spelling mistakes by substituting what it thinks was meant. Instead, the translator will fail with return code 8. The translator will still check for synonyms.

Changes to EXEC CICS API

*Table 3. Changes to **EXEC CICS** commands in CICS TS 6.2*	
EXEC CICS command	**6.2**
CHANGE PASSWORD	**CHANGED:** • New INVREQ with RESP2 value of 32. • New options CHANGETIME, DAYSLEFT, EXPIRYTIME, INVALIDCOUNT, and LASTUSETIME added to reveal more information about the user ID's password or password phrase.
CHANGE PHRASE	**CHANGED:** • New INVREQ with RESP2 value of 32. • New options CHANGETIME, DAYSLEFT, EXPIRYTIME, INVALIDCOUNT, and LASTUSETIME added to reveal more information about the user ID's password or password phrase.
PUT CONTAINER (CHANNEL)	**CHANGED:** New option PREPEND requests that the data passed is prepended to the existing data in the container.
PUT64 CONTAINER	**CHANGED:** New option PREPEND requests that the data passed is prepended to the existing data in the container.
QUERY SECURITY	**CHANGED:** • Enhanced protection. Monitoring and statistics are recorded for this command. • New INVREQ with RESP2 value of 13.
RUN TRANSID	**CHANGED:** New condition NOSTART with RESP2 value of 1, which is returned when the PURGETHRESH limit has been reached for the TRANCLASS to which the TRANSID belongs and, based on the PURGEACTION setting, CICS discards any request to start new transactions belonging to the TRANCLASS.
SIGNON	**CHANGED:** New options CHANGETIME, DAYSLEFT, EXPIRYTIME, INVALIDCOUNT, and LASTUSETIME added to reveal more information about the user ID's password or password phrase.
START ATTACH	**CHANGED:** New condition NOSTART with RESP2 value of 1, which is returned when the PURGETHRESH limit has been reached for the TRANCLASS to which the TRANSID belongs and, based on the PURGEACTION setting, CICS discards any request to start new transactions belonging to the TRANCLASS.

*Table 3. Changes to **EXEC CICS** commands in CICS TS 6.2 (continued)*	
EXEC CICS command	**6.2**
START BREXIT	**CHANGED:** New condition NOSTART with RESP2 value of 1, which is returned when the PURGETHRESH limit has been reached for the TRANCLASS to which the TRANSID belongs and, based on the PURGEACTION setting, CICS discards any request to start new transactions belonging to the TRANCLASS.
WRITEQ TD	**CHANGED:** New NOTAUTH with RESP2 value of 103.

Changes to JCICS API

Methods and classes that were previously deprecated are removed in CICS TS 6.2. You must change any applications that use these methods and classes before you move to CICS TS 6.2.

Table 4. Changes to JCICS classes and methods in CICS TS 6.2		
Class	**Methods**	**6.2**
AsyncService AsyncServiceImpl	`runTransactionId()`	**CHANGED:** New `StartFailedException` is thrown when the start of a transaction is prevented because its associated TRANCLASS has reached the purge threshold and the TRANCLASS specifies PURGEACTION(DISCARD).
Channel	`getContainerNames()`	**CHANGED:** The method `getContainerNames()` cannot throw a `ContainerErrorException`. The throws declaration for `ContainerErrorException` is removed from the method signature. If your application uses this method and handles the `ContainerErrorException`, the catch block can be removed.

Container	`prepend(byte[] byteArrayData)`
	`prepend(byte[] byteArrayData, java.lang.String fromCodePage)`
	`prependString(java.lang.String stringData)`
		NEW: The `prepend` methods add data to the beginning of existing data in a container.

Changes to JCICSX API

Table 5. Changes to JCICSX classes and methods in CICS TS 6.2		
Class	**Methods**	**6.2**
`WriteableContainer`	`prepend(T)`	**NEW:** The `prepend` methods adds data to the beginning of existing data in a container.

`BITContainer`
`WritableBITContainer`
	`appendWith(com.ibm.cics.jcicsx.Serializer, int, T)`
	`prepend(byte[])`
	`prependWith(com.ibm.cics.jcicsx.Serializer, T)`
		NEW: The `appendWith` methods add data to the end of existing data in a container.
		NEW: The `prepend` and `prependWith` methods add data to the beginning of existing data in a container.

Table 5. Changes to JCICSX classes and methods in CICS TS 6.2 (continued)		
Class	**Methods**	**6.2**

`CHARContainer`
`WritableCHARContainer`
`WritableContainer`
	`prepend(java.lang.String)`	**NEW:** The `prepend` method adds data to the beginning of existing data in a container.

Changes to CICS support for application programming languages

Table 6. Changes to CICS support for application programming languages in CICS TS 6.2	
Product name (PID)	**6.2**
IBM Open Enterprise SDK for Node.js, 18.0 (5655-NOJ)	**NEW:** Enabled support
IBM Open Enterprise SDK for Node.js, 12.0 (5655-NOD)	**CHANGED:** Removed support

Changes to Liberty features

Table 7. New, changed, and deprecated Liberty features in CICS TS 6.2	
Feature	**6.2**
`federatedRegistry-1.0`	**NEW:** Allows the federation of one or more user registries.
`collectiveController-1.0`	**NEW:** Allows a server to become the controller for a management collective.
`collectiveMember-1.0`	**NEW:** Enables a server to be a member of a management collective.
`clusterMember-1.0`	**NEW:** Allows a collective member to participate in a static cluster.
`dynamicRouting-1.0`	**NEW:** Enables a server to run a REST service to which the WebSphere® plug-in for Apache and IHS can connect in order to dynamically route to all servers in the Liberty collective.
`healthAnalyzer-1.0`	**NEW:** Provides health data collection for the health manager.
`healthManager-1.0`	**NEW:** Provides health monitoring and automatic actions based on health policies.

Changes to CICS EXCI

Table 8. Changes to the external CICS interface (EXCI) commands in CICS TS 6.2.	
Command	**6.2**
PUT CONTAINER (EXCI)	**CHANGED:** New option PREPEND requests that the data passed is prepended to the existing data in the container.

Changes to JVM server profile options

Table 9. Changes to JVM server profile options in CICS TS 6.2

Option	6.2
JAF_REGISTRATION	**OBSOLETE:** CICS automatically adds the Jakarta Activation Framework (JAF) capability into the JVM server run-time, as necessary. Before Java 11, this technology was included in the JRE.
JAXB_REGISTRATION	**OBSOLETE:** CICS automatically adds the Jakarta XML Binding API (JAXB) capability into the JVM server run-time, as necessary. Before Java 11, this technology was included in the JRE.

Changes to JVM system properties

Table 10. Changes to JVM system properties in CICS TS 6.2

Property	6.2
com.ibm.cics.jvmserver.wlp.server.keystore.location	**NEW:** For Liberty and CMCI JVM servers only. Overrides the default Liberty keystore configuration.
com.ibm.cics.jvmserver.wlp.server.keystore.type	**NEW:** For Liberty and CMCI JVM servers only. Overrides the type in the Liberty keystore configuration.
com.ibm.cics.jvmserver.cmci.user.agent.white.list	**OBSOLETE:** Replaced by com.ibm.cics.jvmserver.cmci.user.agent.allow.list
com.ibm.cics.jvmserver.cmci.user.agent.white.list.monitor.interval	**OBSOLETE:** Replaced by com.ibm.cics.jvmserver.cmci.user.agent.allow.list.monitor.interval
com.ibm.cics.jvmserver.cmci.user.agent.white.list.reject.text	**OBSOLETE:** Replaced by com.ibm.cics.jvmserver.cmci.user.agent.allow.list.reject.text

Changes to context containers

No changes in CICS TS 6.2.

Changes to CICS assistants

Table 11. Changes to the CICS web services assistants, XML assistants, and JSON assistants in CICS TS 6.2

Assistant	6.2
DFHJS2LS	**CHANGED:**
DFHLS2JS	**CHANGED:**
DFHLS2SC	**CHANGED:**
DFHLS2WS	**CHANGED:**
DFHSC2LS	**CHANGED:**
DFHWS2LS	**CHANGED:**

Changes to SIT parameters

Table 12. Changes to system initialization parameters in this release	
SIT parameter	**6.2**
CERTEXPIRYWARN	**NEW:** Specifies whether CICS warns about expiring certificates received from the partner system over TLS connections, and if so, how many days ahead of the expiry.
INTRDRJOBUSER	**NEW:** Instructs whether to use the task user ID or the CICS region user ID as the default job user ID for a JOB card that is submitted, without a **USER** parameter, by using **SPOOL** commands to the internal reader. The default is **INTRDRJOBUSER=TASK**, which means that the task user ID is assumed.
KEYRING	**CHANGED:** The parameter accepts more formats of key ring names, which allows you to specify key rings that are not owned by the region user ID.
RACFSYNC	**CHANGED:** New option CPSM, which specifies that a MAS does not register as a type 71 ENF event listener but obtains type 71 ENF event data directly from its owning CMAS.
TRTABSZ	**CHANGED:** The minimum value that can be specified for TRTABSZ has been increased from 1024 KB to 12288 KB (12 MB).
XPPT	**CHANGED:** New options ALL and DPLONLY. DPLONLY specifies that CICS performs the security check only on the first program that is linked by the mirror program (DFHMIRS) during distributed program link (DPL). ALL specifies that all invoked programs are checked, which is the same behavior as in CICS TS 6.1 and earlier.
ZOSMONINTERVAL	**NEW:** Specifies the sampling interval, in seconds, for the CICS z/OS storage monitor task.
ZOSSOSNEWTCB	**NEW:** Specifies the action that CICS takes in response to a new open TCB that is being attached directly by CICS when the z/OS user region storage or extended user region storage is in a short-on-storage (SOS) condition.
ZOSSOS24UNALLOC	**NEW:** Specifies SOS thresholds in KB for the total amount of unallocated z/OS user region storage and for the largest contiguous storage area available in it.
ZOSSOS31UNALLOC	**NEW:** Specifies SOS thresholds in KB for the total amount of unallocated z/OS extended user region storage and for the largest contiguous storage area available in it.
ZOSSOS64UNALLOC	**NEW:** Specifies an SOS threshold in MB for the amount of unallocated z/OS MEMLIMIT storage in the 64-bit addressing range.

Changes to CICS storage

No changes in CICS TS 6.2.

Changes to toggle-enabled features

Table 13. Changes to toggle-enabled features in CICS TS 6.2	
Feature toggle	**6.2**
com.ibm.cics.cmci.jvmserver={true|false}	**REMOVED:** Replaced by the CMCIPROVIDER WUI server initialization parameter.
com.ibm.cics.cpsm.bas.largecicsplex={true|false}	**CHANGED:** The default is changed from false to true.

Table 13. Changes to toggle-enabled features in CICS TS 6.2 (continued)	
Feature toggle	**6.2**
com.ibm.cics.db2.origindata={true|false}	**NEW:** Gives you the option to disable the passing of adapter origin data to Db2 for adapter tracking.
com.ibm.cics.mvssm.mon.interval ={0|60,1-60}	**REMOVED:** Replaced by the **ZOSMONINTERVAL** system initialization parameter.
com.ibm.cics.mvssm.sos24.minavailable.contiguous ={32,1-1024}	**REMOVED:** Replaced by the **ZOSSOS24UNALLOC** system initialization parameter.
com.ibm.cics.mvssm.sos24.minavailable.total ={64,1-1024}	**REMOVED:** Replaced by the **ZOSSOS24UNALLOC** system initialization parameter.
com.ibm.cics.mvssm.sos31.minavailable.contiguous ={64,1-16384}	**REMOVED:** Replaced by the **ZOSSOS31UNALLOC** system initialization parameter.
com.ibm.cics.mvssm.sos31.minavailable.total ={128,1-16384}	**REMOVED:** Replaced by the **ZOSSOS31UNALLOC** system initialization parameter.
com.ibm.cics.mvssm.sos.wait={true|false}	**REMOVED:** Replaced by the **ZOSSOSNEWTCB** system initialization parameter.
com.ibm.cics.sdt.support.precicsts62={true|false}	**NEW:** To support upgrading to CICS TS 6.2 Shared Data Tables by allowing a rolling upgrade.
com.ibm.cics.spool.surrogate.check={true|false}	**REMOVED:** When **XUSER=YES** is in effect, surrogate user checking is always performed.
com.ibm.cics.tls.minimumkeystrength={1024|2048}	**CHANGED:** The default value is changed from 1024 to 2048.
com.ibm.cics.web.defaultcipherfile={true|false}	**CHANGED:** Extended to apply to URIMAP resources with no ciphers specified.
com.ibm.cics.web.hsts.includesubdomains.*TCPIPS*={true|false}	**NEW:** Controls whether to extend HTTP strict transport security (HSTS) to sub-domains of the specified TCPIPSERVICE.
com.ibm.cics.web.hsts.max-age.*TCPIPS*={*seconds*|-1}	**NEW:** Sets HSTS for an individual TCPIPSERVICE to override the region wide setting.
com.ibm.cics.web.hsts.includesubdomains ={true|false}	**NEW:** Controls whether to extend HSTS to the sub-domains of the CICS server.
com.ibm.cics.web.hsts.max-age=*seconds*	**NEW:** Activates and sets HSTS for a CICS region.

Changes to resource definitions

Table 14. Changes to resource definitions in CICS TS 6.2	
Resource	**6.2**
TRANCLASS	**CHANGED:** New attribute **PURGEACTION** is provided to specify the action CICS is to take on a request to start a transaction when its associated TRANCLASS has reached the purge threshold. In such situations, CICS default action has previously been starting and then abending the requested transaction, but now you can allow CICS to discard the request without starting the transaction.
TRANSACTION	**CHANGED:** The default values of CMDSEC and RESSEC are changed to YES.

Table 15. Changes to resource definition groups in CICS TS 6.2	
Group	**6.2**
DFH$XSD	**NEW:** This new sample group contains resources required by security definition capture (SDC), which needs configuration.
DFHCMAC	**CHANGED:** Transaction CMAC is removed from this group because it's changed to a category 3 transaction.
DFHCLNT	**CHANGED:** TRANCLASS definition DFHCOMCL now specifies PURGEACTION(ABEND).
DFHCOMK2	**NEW:** Resource definition group that needs to be installed after DFHCOMPK for compatibility with CICS TS 6.1, 5.6, 5.4, 5.3, and 5.2 if definitions from the DFHISCT group were used.
DFHCOMPK	**NEW:** Resource definition group required for compatibility with CICS TS 6.1, 5.6, 5.4, 5.3, and 5.2.
DFHEDF	**CHANGED:** TRANCLASS definitions DFHEDFTC and DFHEDFTO now specify PURGEACTION(ABEND).
DFHINDT	**CHANGED:** TRANCLASS definition DFHTCIND now specifies PURGEACTION(ABEND).
DFHISCQ	**CHANGED:** TRANCLASS definition DFHTCQPX now specifies PURGEACTION(ABEND).
DFHISCT	**CHANGED:** TRANCLASS definitions DFHTCLQ2 and DFHTCLSX now specify PURGEACTION(ABEND).
DFHPIPE	**CHANGED:** • Programs added: IXMI58DA, IXMI58D1, IXMI58IN, IXMI58UC, IXM4C58 • Programs removed: IXMI38DA, IXMI38D1, IXMI38IN, IXMI38UC, IXM4C57
DFHTCL	**CHANGED:** The following TRANCLASS definitions now specify PURGEACTION(ABEND): • DFHTCL01 through DFHTCL010 • DFHTSDEL
DFHXSD	**NEW:** This new group contains resources required by security definition capture (SDC).

Changes to CEMT

For changes to the other CICS transactions, see “Changes to CICS transactions” on page 24.

Table 16. Changes to CEMT in CICS TS 6.2	
Command	**6.2**
CEMT INQUIRE SYSTEM	**CHANGED:** New option GRPLIST, showing the names of the lists containing resource definition groups that are loaded during system initialization for a CICS cold start.
CEMT INQUIRE TCLASS	**CHANGED:** New option **PURGEACTION**, to determine the purge action that CICS is to take on a request to start a transaction when its associated TRANCLASS has reached the purge threshold. In such situations, CICS default action has previously been starting and then abending the requested transaction, but now you can allow CICS to discard the request without starting the transaction.
CEMT PERFORM SHUTDOWN CEMT PERFORM SHUTDOWN IMMEDIATE	**CHANGED:** When the command is issued against a CMAS, CICS shuts down the CMAS as part of the shutdown process of the region. When it is issued against a MAS, CICS stops the MAS agent code as part of the shutdown process.
CEMT SET TCLASS	**CHANGED:** New option **PURGEACTION**, to set the purge action that CICS is to take on a request to start a transaction when its associated TRANCLASS has reached the purge threshold. In such situations, CICS default action has previously been starting and then abending the requested transaction, but now you can allow CICS to discard the request without starting the transaction.

Changes to CICS transactions

For changes to CEMT, see “Changes to CEMT” on page 24.

Table 17. Changes to CICStransactions, other than CEMT, in CICS TS 6.2	
Transaction	**6.2**
All CICS transactions, excluding CJXA and CICSPlex SM transactions (CO**)	**CHANGED:** Default settings are now RESSEC(YES) and CMDSEC(YES).
CEDA	**CHANGED:** CEDA enforces uppercase translation on the NETNAMEQ attribute.
CETR	**CHANGED:** The minimum value that can be specified for the internal trace table size has been increased from 1024 KB to 12288 KB (12 MB).
CHLP, CMAC	**CHANGED:** Changed to Category 3 transactions from Category 2 transactions.
CXSD	**NEW:** Allows security request recording (SRR) to be enabled during the lifecycle of the testing of an application. This enables the user to drive manual testing whilst gathering the security requests subsequently exercised by the testing.

Changes to CICS SPI

Table 18. Changes to the system programming interface commands in CICS TS 6.2	
Command	**6.2**
COLLECT STATISTICS EXTRACT STATISTICS	**CHANGED:** New NOTFND with RESP2 value of 3 to indicate that the performance class data for a task is not available.
CREATE TRANSACTION	**CHANGED:** The default values of CMDSEC and RESSEC are changed to YES.
INQUIRE SYSTEM	**CHANGED:** New option GRPLIST, showing the names of the lists containing resource definition groups that are loaded during system initialization for a CICS cold start.
INQUIRE SECDISCOVERY	**NEW:** Retrieves information about the current state of CICS security discovery.
INQUIRE TERMINAL	**CHANGED:** New option TNHOST, showing the host name returned by the connected TN3270 client.
INQUIRE TRANCLASS	**CHANGED:** New option **PURGEACTION**, to determine the purge action that CICS is to take on a request to start a transaction when its associated TRANCLASS has reached the purge threshold. In such situations, CICS default action has previously been starting and then abending the requested transaction, but now you can allow CICS to discard the request without starting the transaction.
SET SECDISCOVERY	**NEW:** Activates or deactivates CICS security discovery, or sets the resource classes whose access requests are to be discovered.
PERFORM SECDISCOVERY WRITE	**NEW:** Immediately writes out the current set of security discovery data.
PERFORM SHUTDOWN PERFORM SHUTDOWN IMMEDIATE	**CHANGED:** When the command is issued against a CMAS, CICS shuts down the CMAS as part of the shutdown process of the region. When it is issued against a MAS, CICS stops the MAS agent code as part of the shutdown process.

Table 18. Changes to the system programming interface commands in CICS TS 6.2 (continued)	
Command	**6.2**
SET TRANCLASS	**CHANGED:** New option **PURGEACTION**, to set the purge action that CICS is to take on a request to start a transaction when its associated TRANCLASS has reached the purge threshold. In such situations, CICS default action has previously been starting and then abending the requested transaction, but now you can allow CICS to discard the request without starting the transaction. New INVREQ RESP2 value of 4, indicating that PURGEACTION has an invalid value.

Changes to JVM profiles

No changes in CICS TS 6.2.

Changes to CICS utilities

Table 19. Changes to CICS utilities in CICS TS 6.2	
Utility	**6.2**
DFH0STAT	**Security report** **New fields:** Failed authorizations NOLOG NOTAUTH Failed authorizations NOLOG NOTFND
DFH0STAT	**User region, extended user region and MEMLIMIT storage monitoring report** **CHANGED:** • Renamed from **MVS user region and extended user region storage report** • Reports on the z/OS MEMLIMIT storage in the 64-bit addressing range, under the heading **MEMLIMIT**
DFH0STAT	**Transaction Classes report** **New field:** Purge A (Purge action)
DFHSTUP	**Security domain global statistics** **New fields:** Failed authorizations NOLOG NOTAUTH Failed authorizations NOLOG NOTFND

Table 19. Changes to CICS utilities in CICS TS 6.2 (continued)	
Utility	**6.2**
DFHSTUP	**Storage manager global statistics** **CHANGED:** The report name is changed to **User region, extended user region and MEMLIMIT storage monitoring** from MVS™ user region and extended user region storage. **New fields:** • SOS duration • Times SOS Reports on the z/OS MEMLIMIT storage in the 64-bit addressing range, under the heading **MEMLIMIT**: • State • Current® unallocated • LWM unallocated • Last date and time SOS • SOS duration • Times SOS
DFHSTUP	**Transaction class resource statistics** **New field:** Purge A (Purge action)

Changes to GLUEs and TRUEs

No changes in CICS TS 6.2.

Changes to XPI functions

Table 20. Changes to XPI functions in this release	
Command	**6.2**
Enqueue domain The ENQUEUE function	**CHANGED:** New EXCEPTION reason code NO_TRANSACTION_ENVIRONMENT, which is returned when an XPI ENQ request attempts to obtain an EXECSTRN or EXECADDR ENQ without a transaction environment.
Transaction management The INQUIRE_TCLASS call	**CHANGED:** New option PURGE_ACTION, which returns the PURGEACTION value of the TRANCLASS resource definition.

Changes to user-replaceable programs

No changes in CICS TS 6.2.

Changes to control tables

No changes in CICS TS 6.2.

Changes to CICS policies

Table 21. Changes to policy system rules in CICS TS 6.2.	
System rule	**6.2**
All system rules	**CHANGED:** New option to set the WLM health interval is provided with the **Set z/OS WLM health open status** system rule action.
Transaction class queued tasks	**NEW:** This new system rule enables you to take a policy action as the number of tasks queuing for membership to a TRANCLASS goes above or below a specified threshold represented by a percentage of the maximum number of user tasks in the queue.

Changes to event processing adapters and formats

No changes in CICS TS 6.2.

Changes to installation and definition of CICSPlex SM

- The record size of EYUHIST* data sets has increased from RECORDSIZE(3748 3752) to RECORDSIZE(3756 3760). The EYUJHIST sample has been updated to reflect this change.

Changes to configuration and initialization of CICSPlex SM

Table 22. Changes to CICSPlex SM WUI server initialization parameters (WUIPARM) in CICS TS 6.2.	
WUIPARM parameter	**6.2**
CMCIPROVIDER(JVMSERVER|CICS)	**NEW:** New WUI server initialization parameter that specifies whether to use the CMCI JVM server to facilitate CMCI in the WUI region.
TCPIPSSL	**CHANGED:** If the WUI server has CICS security active (SEC=YES in the system initialization parameter), TCPIPSSL is mandatory.
TCPIPHOSTNAME	**DEPRECATED:** TCPIPHOSTNAME is no longer required.
TCPIPHTTPHOST	**DEPRECATED**

Table 23. Changes to CMCI in CICS TS 6.2	
Change	**6.2**
Enablement of the CMCI JVM server	**CHANGED:** Enablement of the CMCI JVM server is now set by the WUI initialization parameter CMCIPROVIDER(JVMSERVER|CICS) instead of through a feature toggle. The CMCI JVM server is still enabled by default but you can switch it off by setting CMCIPROVIDER(CICS) and opt to use the basic CMCI.
Enhancements to the CMCI GraphQL API	**CHANGED:** Added support for the following resources: • BRFACIL • FEPICONN • FEPINODE • FEPIPOOL • FEPIPROP • FEPITRGT • MODENAME • SECDISC

Changes to CICSPlex SM behavior and operation

Table 24. Changes to CICSPlex SM behavior and operation in CICS TS 6.2.	
CICSPlex SM feature	**6.2**
CMAS and MAS	**CHANGED:** • CICSPlex SM can now process type 71 ENF events for a CICSplex. A CMAS that is started with the system initialization parameter **RACFSYNC=YES** listens for type 71 ENF events and make them available to its connected MAS regions that are started with the system initialization parameter **RACFSYNC=CPSM**. When the CMAS receives a type 71 ENF event, security information for the affected user ID is rebuilt the next time the user ID is used, irrespective of the setting of the **SECTIMEOUT** parameter. • You can now use **PERFORM SHUTDOWN** and **PERFORM SHUTDOWN IMMEDIATE** directly on CMAS and MAS regions. In processing the command, CICS shuts down the CMAS or stops the MAS agent code as part of the shutdown process.
CICSPlex SM WUI	**CHANGED:** Some terms used in CICSPlex SM WUI are updated; for example, to reflect changed product names, such as IBM MQ in place of WebSphere MQ.

Changes to CICSPlex SM resource tables

Enhancements to CICSPlex SM resource tables are typically populated to related CICSPlex SM views. In Table 25 on page 29, where applicable, the changed CICSPlex SM views are also listed.

Table 25. Changes to the resource tables provided by CICSPlex SM in CICS TS 6.2.		
Resource table	**Related view**	**6.2**
All	Not applicable	**CHANGED:** Some terms used in CICSPlex SM resource tables are updated; for example, to reflect changed product names, such as IBM MQ in place of WebSphere MQ.
CICSRGN	CICS region (CICSRGN) view	**CHANGED:** • New field **Current Time of Day** with resource table attribute name CURRTIME, indicating the CICS ABSTIME time of day of the region. • New field **Cold Start Resource Group Lists** with resource table attribute name GRPLIST, showing the names of the lists containing resource definition groups that are loaded during system initialization for a CICS cold start.
HTASK	Completed tasks (history) (HTASK) view	**CHANGED:** New field **TRANCLASS tasks** with resource table attribute name TCLSTSKS to indicate the total number of active and queued tasks in the associated TRANCLASS when a task is attached.
SECDISC	Not applicable	**NEW:** Resource table for CICS security discovery status.
TASK	Active tasks (TASK) view	**CHANGED:** New field **TRANCLASS tasks** with resource table attribute name TCLSTSKS to indicate the total number of active and queued tasks in the associated TRANCLASS when a task is attached.
TERMNL	Terminals (TERMNL) view	**CHANGED:** New field **Host name** with resource table attribute name TNHOST, showing the host name returned by the connected TN3270 client.

Table 25. Changes to the resource tables provided by CICSPlex SM in CICS TS 6.2. (continued)		
Resource table	**Related view**	**6.2**
TRANCLAS	Transaction class (TRANCLAS) view	**CHANGED:** New field **Purge action** with resource table attribute name PURGEACTION, displaying the PURGEACTION value of the TRANCLASS resource definition.
TRNCLDEF	Transaction class definition (TRNCLDEF) view	**CHANGED:** New field **Purge action** with resource table attribute name PURGEACTION, displaying the PURGEACTION value of the TRANCLASS resource definition.

Changes to CICS monitoring

Table 26. Changes to monitoring data in CICS TS 6.2.	
Data	**6.2**
Performance data in group DFHTASK	**CHANGED:** **NEW FIELDS:** • 048 XSNLNACT to track the number of QUERY **SECURITY LOGMESSAGE(NOLOG)** requests that succeeded but returned no authority on READ, UPDATE, CONTROL or ALTER. • 049 XSNLNFCT to track the number of **QUERY SECURITY LOGMESSAGE(NOLOG)** requests that failed with response code 13 NOTFND and reason code 5 or 8. • 185 TCLSTSKS to indicate the total number of active and queued tasks in the associated TRANCLASS when a task is attached.

Changes to CICS statistics

In Table 27 on page 30, the field name is a unique identifier for each statistic field, and where applicable, the DFHSTUP name is also given.

Table 27. Changes to CICS statistics in CICS TS 6.2.	
Statistics	**6.2**
JVMSERVERs	**NEW FIELDS:** • SJS_JVMSERVER_THREAD_WLP_ACTV to track the number of CICS threads currently active in Liberty.
Security domain	**NEW FIELDS:** • XSG_AUTHOR_FAIL_NL_NA, with DFHSTUP name **Failed authorizations NOLOG NOTAUTH**, to track the number of QUERY **SECURITY LOGMESSAGE(NOLOG)** requests that succeeded but returned no authority on READ, UPDATE, CONTROL or ALTER. • XSG_AUTHOR_FAIL_NL_NF, with DFHSTUP name **Failed authorizations NOLOG NOTFND**, to track the number of **QUERY SECURITY LOGMESSAGE(NOLOG)** requests that failed with response code 13 NOTFND and reason code 5 or 8.

Table 27. Changes to CICS statistics in CICS TS 6.2. (continued)	
Statistics	**6.2**
Storage manager	**NEW FIELDS:** **For the z/OS user region storage** • SMSMVS24SOSTIME, with DFHSTUP name **SOS duration** • SMSMVS24SOSCOUNT, with DFHSTUP name **Times SOS** **For the z/OS extended user region storage** • SMSMVS31SOSTIME, with DFHSTUP name **SOS duration** • SMSMVS31SOSCOUNT, with DFHSTUP name **Times SOS** **For the z/OS MEMLIMIT storage** • SMSMVS64STATE, with DFHSTUP name **State** • SMSMVS64UNALLOC, with DFHSTUP name **Current unallocated** • SMSMVS64UNALLOCLWM, with DFHSTUP name **LWM unallocated** • SMSMVS64LASTSOSTIMELOCAL, with DFHSTUP name **Last date and time SOS** • SMSMVS64LASTSOSTIMEUTC • SMSMVS64SOSTIME, with DFHSTUP name **SOS duration** • SMSMVS64SOSCOUNT, with DFHSTUP name **Times SOS** DFH0STAT and DFHSTUP report them under the heading **MEMLIMIT**.
Storage manager	**CHANGED FIELDS:** The following storage SOS statistics are subject to the **ZOSSOSNEWTCB** system initialization parameter. They are populated when **ZOSSOSNEWTCB=DELAY** is in effect, but are all zero under **ZOSSOSNEWTCB=NODELAY**. • SMSMVS24WAITTIME and SMSMVS31WAITTIME, with DFHSTUP name **Time tasks waited because SOS** • SMSMVS24NUMWAITS and SMSMVS31NUMWAITS, with DFHSTUP name **Current tasks waiting because SOS** • SMSMVS24NUMWAITSHWM and SMSMVS31NUMWAITSHWM, with DFHSTUP name **Peak tasks waiting because SOS** • SMSMVS24TOTALNUMWAITS and SMSMVS31TOTALNUMWAITS, with DFHSTUP name **Total waits because SOS**
Transaction class (TCLASS)	**NEW FIELD:** • XMCPUA, with DFHSTUP name **Purge A**, which indicates the purge action that CICS takes for a request of starting a transaction in the named transaction class when the transaction class has reached the purge threshold.
Suppress Statistics	**NEW:** • Transaction and Program statistics containing zero count fields following a reset will be suppressed. This applies to interval, requested, and requested reset type statistics.

Changes to CICS messages

DFH52nn

Removed:

- DFH5290W
- DFH5291E
- DFH5292W
- DFH5293W
- DFH5294E
- DFH5296W

DFH55nn

New:

- DFH5565E is issued if a problem is found in the input to the DFHCSDUP offline utility, and the default value is assumed.

DFHACnnnn

New:

- DFHAC2059 is issued for a discarded request to start a transaction because the TRANCLASS PURGETHRESH has been reached and the PURGEACTION is discard.

DFHAMnnnn

Changed:

- DFHAM4838 is changed to show group information when appropriate.

DFHAPnnnn

Changed:

- DFHAP1301 is changed to show that another symptom can be that LE has detected a loop.

DFHCAnnnn

New:

- DFHCA5565W is issued if a problem is found in the input to the **EXEC CICS CREATE** command, and the default value is assumed.

Changed:

- DFHCA4838 is changed to show group information when appropriate.

Removed:

- DFHCA5290W
- DFHCA5291E
- DFHCA5293W
- DFHCA5294E
- DFHCA5296W

DFHCEnnnn

Changed:

- DFHCE3549 is changed to show the number of previous failed attempts to sign on, and the date and time the user ID was last accessed.

DFHFCnnnn

New:

- DFHFC0437 indicates that a data table request for a file resource has encountered a NOSPACE condition.

DFHHnnnn

New:

- DFHH0009E is issued when one or more stabilized functions are being used in a CICS region.

- DFHH0415 is issued when the attempt to execute the health checks for the CICS Resource Configuration has not completed successfully.
- DFHH0506 is issued when the attempt to execute the health checks for the CICS Resource Configuration has not completed successfully.
- DFHH0604 is issued when the attempt to execute the health checks for the CICS USS configuration has not completed successfully.
- DFHH0709 is issued when the attempt to execute the health checks for CICS Resource Security has not completed successfully.
- DFHH0811 is issued when the attempt to execute the health checks for CICS Category 3 Transactions has not completed successfully.
- DFHH0951 indicates that XRF is in use.
- DFHH0952 indicates that APPC password expiration management (PEM) is in use.
- DFHH0953 indicates that CICS Service Flow Runtime is in use.
- DFHH0954 indicates that the DFHWBCLI web client interface is in use.
- DFHH0955 indicates that SAML is using the Security Token Service.
- DFHH0957 is issued when the health check on stabilized functions did not complete successfully.
- DFHH0958 indicates that ONC RPC is in use.
- DFHH0959 indicates that CICS system events are being used.
- DFHH0960 indicates that CICS debugging tools sockets interface is in use.
- DFHH0961 indicates that Enterprise Bundle Archive (EBA) files are in use.
- DFHH0962 indicates that CICSPlex SM RTA MRM function is in use.
- DFHH0963 indicates that CICSPlex SM RTA SAM function is in use.
- DFHH0964 indicates that a pipeline that is configured to use a JVMSERVER is installed.
- DFHH0965 indicates that the CICS Application Debugging Profile Manager is being used.

DFHISnnnn

New:

- DFHIS2013 indicates the server APPLID that is used in a High Availability (HA) IPCONN connection.
- DFHIS2041 indicates an attempt to acquire the named IPCONN failed because of unsecured TCPIP connections with a partner system that is located outside the sysplex.

DFHMEnnnn

New:

- DFHME0142 indicates a message write failure due to a D23 abend in WTO processing.

DFHMPnnnn

New:

- DFHMP2019 indicates that the CICS-managed platform domain failed to create a policy in a BUNDLE resource due to an invalid WLM health open status value that is specified in the policy rule.

DFHMQnnnn

New:

- DFHMQ0797E is issued when temporary storage queue DFHCKBR is required but its TSMODEL definition has not been defined or installed in the system.
- DFHMQ0798E is issued when the CICS-MQ 3270 bridge issued a request to start a transaction, and the request is discarded.

DFHPAnnnn

New:

- DFHPA2012I indicates the resource overrides file name that is set in the **RESOVERRIDES** SIT parameter, and is issued preceding DFHPA2011E when **RESOVERRIDES** specifies an invalid resource overrides file name.

DFHRLnnnn

New:

- DFHRL0137I is issued when all GRPLIST defined BUNDLE resources have reached their target initial status.
- DFHRL0138W is issued when one or more GRPLIST defined BUNDLE resources have failed to reach their target initial status.

DFHSJnnnn

Changed:

- DFHSJ0914E logs a JVMSERVER initialization failure that results from insufficient unallocated 64-bit z/OS virtual storage available at the time of the JVMSERVER initialization.

DFHSMnnnn

New:

- DFHSM0154I is issued by the CICS z/OS storage monitor task to inform the size of unallocated z/OS MEMLIMIT storage when the task detects a significant change in the storage tier level.
- DFHSM0155W reports a short-on-storage (SOS) condition that is occurring in the z/OS MEMLIMIT storage.
- DFHSM0156I indicates the end of the SOS condition in the z/OS MEMLIMIT storage, and the storage is not constrained.

DFHSNnnnn

Changed:

- DFHSN1100 is changed to show the security attributes for the signed-on user ID in the group ID. It also shows the number of previous failed attempts to sign on, and the date and time the user ID was last accessed.

DFHSOnnnn

New:

- DFHSO1100I provides diagnostic information about an expiring certificate that is received from the partner system over a TLS connection.
- DFHSO0175W is issued when System SSL has been initialized within the region but ICSF was unavailable.

DFHTPnnnn

New:

- DFHTP4175 indicates a message routing failure due to an invalid or unlocatable remote system ID.

DFHWBnnnn

New:

- DFHWB1561 indicates that the URIMAP resource was defined with `CIPHERS()` and lists the ciphers that CICS used instead.

Changed:

- DFHWB0112I is changed so that it isn't issued when the region does not support outbound HTTPS connections. This ensures the message is issued only when there is an actual problem of processing the `defaultciphers.xml` file.

DFHXMnnnn

New:

- DFHXM0206 indicates the number of purges that occurred to a specific transaction class in the last interval, regardless of its purge action.

DFHXSnnnn

New:

- DFHXS1600 indicates that the security discovery recording has been activated.
- DFHXS1601 indicates that the security discovery recording has been deactivated.
- DFHXS1602 reports the current state of security discovery.
- DFHXS1603 reports a list of all the resource classes that are currently set to discover access.
- DFHXS1604 indicates that the current set of security discovery data (SDD) has been written to the DFHSECD log stream.
- DFHXS1605 indicates that there was a failure when writing the Security Discovery Data to the DFHSECD log stream.

DFHYMnnnn

New:

- DFHYM1024E indicates that an unexpected operator has been found in the resource overrides file.

Changes to CICSPlex SM messages

EYUCInnnn

New:

- EYUCI0103E is issued when the system initialization parameter **RACFSYNC=CPSM** is erroneously set in a CMAS. **RACFSYNC=CPSM** is intended for MAS regions.

EYUCPnnnn

New:

- EYUCP0034I identifies the maintenance point for a CICSplex.
- EYUCP0035I identifies the CICSplex that a CMAS manages and the maintenance point for this CICSplex.
- EYUCP0036I is issued when a CMAS is removed from a CICSplex.

EYUCRnnnn

New:

- EYUCR0011E is issued when a CMAS is unable to obtain ENF71 records from the underlying CICS region and is therefore unable to receive and process newer ENF71 events from RACF®.
- EYUCR0012E is issued when a CMAS detects an internal error during ENF71 record propagation to subordinate MAS regions.

EYUXDnnnn

New:

- EYUXD1032W is issued when the EYUDREP data set has exceeded 70% of its extent availability.

Changes to abend codes

New abend codes

- **AASB** occurs when module DFHAMAO, while processing resource overrides, calls module DFHPUPD to apply any dependent defaults to a modified resource definition and receives an unexpected response.
- **AITQ** occurs when a transaction is purged, during the processing of a request, while waiting for a response from a connected subsystem over an IPIC connection.
- **AMQT** occurs when temporary storage queue DFHCKBR is required but the TSMODEL definition for it does not exist.
- **ANQG** occurs when an XPI ENQ request attempts to obtain an EXECSTRN or EXECADDR ENQ without a transaction environment.

- **AXMT** occurs when an attempt has been made to run the CICS internal system task CXMT as a user transaction, or run its associated program DFHXMCHK under a different transaction ID.
- **AXMV** occurs when the CICS internal task that monitors TRANCLASS purges encounters an unexpected error.

Changes to samples

Table 28. Changes to the samples provided with CICS TS 6.2.

Sample	**6.2**
`/security/ciphers/defaultciphers.xml`	**CHANGED:** Cipher suites that use NULL, Triple DES (3DES) and RC4 encryption are removed from the file. If you have your own unchanged copy of `defaultciphers.xml` in `USSCONFIG/security/ciphers` from a previous release, it is recommended that you copy the new version from `USSHOME/security/ciphers` to `USSCONFIG/security/ciphers`. The following cipher suites are removed: • 003B - TLS_RSA_WITH_NULL_SHA256 • C001 - TLS_ECDH_ECDSA_WITH_NULL_SHA • C002 - TLS_ECDH_ECDSA_WITH_RC4_128_SHA • C003 - TLS_ECDH_ECDSA_WITH_3DES_EDE_CBC_SHA • C006 - TLS_ECDHE_ECDSA_WITH_NULL_SHA • C007 - TLS_ECDHE_ECDSA_WITH_RC4_128_SHA • C008 - TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA • C010 - TLS_ECDHE_RSA_WITH_NULL_SHA • C011 - TLS_ECDHE_RSA_WITH_RC4_128_SHA • C012 - TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA • C00B - TLS_ECDH_RSA_WITH_NULL_SHA • C00C - TLS_ECDH_RSA_WITH_RC4_128_SHA • C00D - TLS_ECDH_RSA_WITH_3DES_EDE_CBC_SHA

Changes to documentation

Table 29. Changes to the documentation provided with CICS TS 6.2.

Documentation	**6.2**
Downloadable (offline) documentation	**CHANGED:** IBM Knowledge Center-Customer Installed (KC-CI) is replaced by IBM Documentation Offline.
Online documentation	**NEW:** archived IBM publications that are referenced by some CICS messages (for example, the *IBM 3270 Data Stream Programmers Reference*) are available for download from Archived CICS documentation. **NEW:** documentation covers both CICS TS 6.2 and CICS TS 6.1. Tags highlight differences between releases.
Securing CICS	**CHANGED:** Diagrams, explanations, and best practices continue to be added to this part of the documentation.

Table 29. Changes to the documentation provided with CICS TS 6.2. (continued)	
Documentation	**6.2**
Troubleshooting	**CHANGED:** Enhancements to trace information, including a new trace term topic and new section How it works: Tracing in CICS. z/OS trace is now covered in Using z/OS trace for problem determination.
PDF	**CHANGED:** large PDFs are split into more manageable ones. *CICS Messages* is now in 3 parts. *Diagnosis Reference* is split into *Component Reference*, *Domain Reference*, and *Executable Module Reference*. **NEW:** documentation covers both CICS TS 6.2 and CICS TS 6.1. Tags highlight differences between releases.

Chapter 3. What's new in CICS TS 6.1?

CICS Transaction Server for z/OS, Version 6 enables development teams to create powerful mixed-language applications, while allowing the operational teams to manage these applications from a single point of control.

On this page, find out what CICS TS 6.1 offers. You might also like to refer to the CICS Transaction Server for z/OS Version 6.1 announcement letter. Continue the journey with the capabilities of CICS TS 6.2 in What's New for CICS TS 6.2.

For a summary of new capabilities in previous versions, see Changes between releases. New features in CICS Explorer are described in the CICS Explorer product documentation.

All the enhancements at a glance

Some enhancements are shown under more than one category; the information is the same in all cases.

Service indicates that the capability is available through APAR after the General Availability of CICS TS 6.1.

- For installation:
  - "ServerPac installation using z/OSMF" on page 41
- For the developer experience:
  - "@CICSProgram annotation now available for use with OSGi JVM servers" on page 41
  - "Easier system management, efficient application development, and advanced client authentication available in single CICS regions with CMCI JVM server" on page 41
  - "STACKTRACE action for PERFORM JVMSERVER" on page 42
  - "Alternative Liberty install" on page 42
  - "Infusing AI into CICS applications" on page 42
  - "Updates to the JVM profiles" on page 42
  - "Improved handling of unexpected errors in JVM servers" on page 42
  - "Support for Node.js 18" on page 43
  - "Liberty JVM server bundle processing improvements" on page 43
  - "Support for Java 11" on page 43
  - Service "Support for Java 17" on page 43
  - "Support for Liberty collectives" on page 43
- For system management:
  - "Ansible IBM z/OS CICS collection to automate CICS resource and region actions" on page 44
  - "Infusing AI into CICS applications" on page 42
  - "Support for force purge of transaction CDBT" on page 44
  - "New SPI command to overwrite the user correlator data" on page 45
  - "Enhancements to CICS policies" on page 45. Some of these enhancements are also provided on other CICS releases through APAR.
  - "Override resource definitions" on page 46. Also provided on other CICS releases through APAR.
  - "Monitoring auxiliary temporary storage usage" on page 46. Also provided on other CICS releases through APAR.

  - “WRITE OPERATOR enhanced to support writing messages to a specific console” on page 55
  - “Improved temporary storage expiry processing” on page 55
  - “Improved processing of WS-AT requests” on page 55
- For documentation:
  - “For documentation and other information” on page 56

For installation

ServerPac installation using z/OSMF

You can now receive CICS as a ServerPac in z/OSMF Software Management portable software instance format. This enables you to deploy the installation using z/OSMF Software Management and ServerPac Workflows instead of the ServerPac ISPF dialog.

Learn more...

For developer experience

- “@CICSProgram annotation now available for use with OSGi JVM servers” on page 41
- “Easier system management, efficient application development, and advanced client authentication available in single CICS regions with CMCI JVM server” on page 41
- “STACKTRACE action for PERFORM JVMSERVER” on page 42
- “Alternative Liberty install” on page 42
- “Infusing AI into CICS applications” on page 42
- “Updates to the JVM profiles” on page 42
- “Support for Liberty collectives” on page 43
- “Improved handling of unexpected errors in JVM servers” on page 42
- “Support for Node.js 18” on page 43
- “Liberty JVM server bundle processing improvements” on page 43
- “Support for Java 11” on page 43
- Service “Support for Java 17” on page 43
- “Support for Liberty collectives” on page 43

`@CICSProgram` annotation now available for use with OSGi JVM servers

First introduced for the Link-to-Liberty capability, this annotation offers a more convenient and less error-prone alternative to the `CICS-MainClass` approach for designating Java methods as the target of CICS PROGRAM LINKs.

Learn more...

Easier system management, efficient application development, and advanced client authentication available in single CICS regions with CMCI JVM server

The CICS Management Client Interface (CMCI) is a set of APIs that enable management of your CICS regions using tools such as CICS Explorer. When served from a JVM server, the CMCI provides additional capabilities such as multi-factor authentication (MFA), the GraphQL API, and the CICS bundle deployment API.

The CMCI JVM server is now able to be configured in a single CICS region outside of a CICSPlex SM environment to create an SMSS, enabling the following features:

- Enhanced security offered by multi-factor authentication (MFA), even in SMSS environments. Users can now sign on to an SMSS with MFA credentials in CICS Explorer for Aqua 3.2 (Fix Pack 5.5.20).

- Easier system management with the CMCI GraphQL API, which supports queries about multiple CICS resources and inter-resource relationships in a single request. CICS Explorer as of Fix Pack 5.5.20 also uses the GraphQL API to provide the aggregation function when connected to SMSS regions at CICS TS 5.6 with APAR PH35122, or a later release.
- Efficient application development with the CICS bundle deployment API, which allows Java developers to use the CICS-provided Gradle or Maven plug-ins to deploy bundles into single CICS development environment. This way, developers can see their application changes reflected in a running CICS region within seconds, and integrate the CICS bundle build and deployment into a toolchain to increase productivity, whilst the system programmer retains control.

Learn more...

STACKTRACE action for PERFORM JVMSERVER

JVM server administration is enhanced with the addition of a new action for the **PERFORM JVMSERVER** command. JVM STACKTRACE offers facilities to take a stacktrace of CICS task that is running in a JVM server.

Learn more...

Alternative Liberty install

If you choose, you can now specify a different value for WLP_INSTALL_DIR in your JVM profile to use an alternative version of Liberty - one that is not supplied with CICS.

Learn more ...

Infusing AI into CICS applications

Applications that run in CICS TS can make more timely and better decisions, and achieve improved business outcomes, by capitalizing on AI within their transactions.

IBM zSystems and the IBM Integrated Accelerator for AI incorporated in IBM z16™ can optimize the processing of machine learning and deep learning algorithms. In particular, the centralized on-chip AI accelerator on IBM z16 leverages AI at speed and scale, and is designed to provide high performance and consistent low latency inferencing for processing transactional workloads, such as those run on CICS TS.

Enterprises using any in-service release of CICS TS can exploit those capabilities by choosing suitable AI models. When using deep learning AI models, enterprises can leverage the IBM Integrated Accelerator for AI by using existing options for invoking AI models in their applications.

Learn more ...

Updates to the JVM profiles

The supplied sample profiles for a CMCI JVM server are updated as follows:

- The sample for a CMCI JVM server in a WUI region is changed to add `-Dcom.ibm.ws.zos.core.angelRequiredServices=SAFCRED,PRODMGR,ZOSAIO`.
- A new sample profile for a CMCI JVM server in a single CICS region has the `angelRequiredServices` property set as follows: `-Dcom.ibm.ws.zos.core.angelRequiredServices=SAFCRED,PRODMGR,ZOSAIO`.

Learn more...

Improved handling of unexpected errors in JVM servers

This function improves the handling of errors that cause the Java virtual machine (JVM) or Language Environment® Enclave, managed by a JVM server resource, to stop unexpected. When a POSIX signal or abend is received into the runtime of the JVM server, it is restarted.

Learn more...

Support for Node.js 18

Developers can use Node.js 18 to build microservices and web applications using the latest JavaScript features and frameworks, with optimized access to CICS TS programs with the ibm-cics-api API. This support requires IBM Open Enterprise SDK for Node.js.

Learn more...

Liberty JVM server bundle processing improvements

This function improves the processing of bundle parts that are installed into Liberty JVM servers. CICS avoids invalidating the Liberty `workarea` cache by preserving the contents of `installedApps.xml` when enabling a Liberty JVM server. The location of `installedApps.xml` and the `installedApps` directory is changed to the Liberty configuration directory (`${liberty.config.dir}`).

Learn more...

Support for Java 11

This release adds support for Java 11 using IBM Semeru Runtime Certified Edition for z/OS. A minimum version of 11.0.15.0 is required. The CICS documentation will be updated to describe considerations for using Java 11.

Java 8 continues to be supported.

Learn more ...

Support for Java 17

Service Available with APAR PH55279.

CICS supports Java 17 using IBM Semeru Runtime Certified Edition for z/OS. A minimum version of 17.0.7.0 is required.

Java 17 is not supported for use with SAML JVM servers at all CICS releases.

To enable Db2 type 2 connectivity when you are running Java 17, add `LIBPATH_SUFFIX=/usr/lpp/db2v12/jdbc/lib` to the JVM profile.

Java 8 and Java 11 continue to be supported.

Learn more ...

Support for Liberty collectives

In a system that hosts multiple Liberty servers, including Liberty JVM servers, it can be useful to manage and monitor these servers, and their applications, from a centralized administrative control point.

Learn more...

For system management

- “Ansible IBM z/OS CICS collection to automate CICS resource and region actions” on page 44
- “Infusing AI into CICS applications” on page 42
- “Support for force purge of transaction CDBT” on page 44
- “New SPI command to overwrite the user correlator data” on page 45
- “Enhancements to CICS policies” on page 45. Some of these enhancements are also provided on other CICS releases through APAR.
- “Override resource definitions” on page 46. Also provided on other CICS releases through APAR.
- “Monitoring auxiliary temporary storage usage” on page 46. Also provided on other CICS releases through APAR.
- “Enhanced adapter tracking for CICS Db2 applications” on page 47. Also provided on other CICS releases through APAR.

- “Inquire on 64-bit storage that belongs to a task” on page 47
- “Support for daisy-chaining of non-terminal-related START requests” on page 47
- “Easier system management, efficient application development, and advanced client authentication available in single CICS regions with CMCI JVM server” on page 41
- “Classify CICS regions by using region tagging” on page 47
- “Messages reporting changes to APPC and IRC log names” on page 48. Also provided on other CICS releases through APAR.
- “Automatic recovery of failed user journals” on page 48
- Service “Prepare for a future release of CICS TS” on page 48
- “Enabling multiple client URIMAPs that point to the same endpoint” on page 48. Also provided on other CICS releases through APAR.
- “Running the Link3270 bridge with a custom transaction ID” on page 48
- “Automating the process of defining CICS application resources with CICS Transaction Server resource builder” on page 49

Ansible IBM z/OS CICS collection to automate CICS resource and region actions

Red Hat Ansible is a popular open-source tool to automate configuration management and deployments on IBM z/OS and many other platforms with a consistent approach, architecture, and set of skills. It supports automation tasks through Ansible playbooks, which you can run from command line interfaces (CLI), browser dashboards, within editors, or DevOps pipelines.

The IBM z/OS CICS collection collection uses the CMCI REST API to automate tasks in either a CICSPlex System Manager environment or a single CICS region that is not part of a CICSPlex SM. The automation tasks can define, install, and perform actions on CICS definitions and resources such as creating a PROGRAM definition, installing and updating it, and then deleting the definition.

To use this collection, a CICS management client interface (CMCI) (CMCI) connection is required in the CICSPlex SM or the single CICS region.

The IBM z/OS CICS collection collection is developed as an open-source project at IBM z/OS CICS collection GitHub and is available on Ansible Galaxy and Ansible Automation Hub.

Learn more...

Infusing AI into CICS applications

Applications that run in CICS TS can make more timely and better decisions, and achieve improved business outcomes, by capitalizing on AI within their transactions.

IBM zSystems and the IBM Integrated Accelerator for AI incorporated in IBM z16 can optimize the processing of machine learning and deep learning algorithms. In particular, the centralized on-chip AI accelerator on IBM z16 leverages AI at speed and scale, and is designed to provide high performance and consistent low latency inferencing for processing transactional workloads, such as those run on CICS TS.

Enterprises using any in-service release of CICS TS can exploit those capabilities by choosing suitable AI models. When using deep learning AI models, enterprises can leverage the IBM Integrated Accelerator for AI by using existing options for invoking AI models in their applications.

Learn more ...

Support for force purge of transaction CDBT

If a CDBT task is waiting on the DBCTL resource DLSUSPND, you can now issue a request to force purge CDBT.

Learn more...

New SPI command to overwrite the user correlator data

A new SPI command **SET ASSOCIATION USERCORRDATA** provides a way to overwrite the user correlator data of the originating task.

A global user exit program that runs in the originating task can now overwrite the USERCORRDATA field with user-defined user correlator data (for example, from HTTP headers or IBM MQ messages). The global user exit program must issue **INQ ASSOCIATION USERCORRDATA** to retrieve any existing user correlator data. Then, the program must issue **SET ASSOCIATION USERCORRDATA** to overwrite the USERCORRDATA field after consideration of any existing data that might have been set by a previous global user exit program.

Learn more...

Enhancements to CICS policies

- Ability to specify Transaction ID and User ID conditions for policy task rules.

  When you define a policy task rule, you can now limit this rule to be triggered when status changes are made in relation to a specific transaction or a range of transactions, a specific user ID or a range of user IDs, or both. To specify this limit, you can set **Transaction ID** and **User ID** filters in the Condition section in the Rules tab of the Policy definition editor.

  This capability is also available on CICS TS 5.4, 5.5, and 5.6 with APAR PH26145.

  Learn more...
- New option ALL added to the following types of policy task rules:
  - File requests
  - Storage allocation
  - Storage requests
  - TD queue requests
  - TS queue requests

  This enhancement allows you to apply a threshold to the total cumulative count.

  Learn more...
- New task rule type: Container storage.

  Use this rule type to define a threshold for the amount of container storage allocated to a user task, and take an automatic action when the threshold is exceeded. This rule does not apply to EXCI containers or BTS containers.

  This capability is also available on CICS TS 5.6 with APAR PH29187.

  Learn more ...
- New system rule type: Transaction dump threshold.

  Use this rule type to set a maximum threshold for the total number of transaction dumps in a CICS region and take an automatic action when the threshold is exceeded.

  With this system rule, you can monitor transaction dumps and prevent excessive dumping in a CICS region.

  This capability is also available on CICS TS 5.6 with APAR PH34348.

  Learn more...
- New system rule type: Compound condition.

  Use this rule type when you want to define a system rule that specifies two or more conditions. CICS takes the defined action when all the specified conditions are met. Note that only selected condition types can be specified for compound condition system rules.

  Learn more ...
- Enhanced support for policy statistics.

The sample statistics program DFH0STAT can now produce Policy reports. The Policy report shows information and statistics about installed policy rules in the region. In support for this enhancement, the **EXTRACT STATISTICS** system programming command supports a new RESTYPE option POLICY and a new SUBRESTYPE option POLICYRULE, which can be used to obtain statistics about a policy rule that is contained in a POLICY resource.

In addition, two new system programming commands **INQUIRE POLICY** and **INQUIRE POLICYRULE** have been introduced to support inquiries on information about installed POLICY resources and the policy rules contained within.

Learn more...

- Enhanced data capture for policy events emitted for transaction abend system rules.

  When a transaction abend system rule is triggered, the name of the program to which the unhandled transaction abend occurred is now captured and contained in container DFHEP.DATA.00005. However, the program name data is not captured for the other system rules, so DFHEP.DATA.00005 remains 8 blanks for them.

  Learn more...

- Service New option to set the WLMHEALTH time interval is supported by the Set z/OS WLM health open status system rule action.

  Available with APAR PH58295

  You can now change the region's WLMHEALTH time interval as part of the system rule action. This enhancement makes it easier for you to manage the z/OS WLM health of a CICS region by using a variety of policy system rules.

  Learn more...

Override resource definitions

You can provide a consistent approach to the creation of certain resources by applying environment-specific overrides through a resource overrides file. You can override the resource definition for any supported resource type that can be defined by using resource definition online (RDO). You specify the required overrides in a resource overrides file that is loaded during CICS startup. The overrides are applied when CICS resources are installed.

This support is intended for infrequent system-wide changes to tailor the resources for a specific CICS environment.

If this support is in use and the resource overrides file includes override rules for specified resource types, resource overrides are applied to the relevant resources when they are installed. Therefore, you must consider the effects of resource overrides when you install resources.

This capability is also available on CICS TS 5.6 with APAR PH30590.

Learn more...

Monitoring auxiliary temporary storage usage

You are now alerted when auxiliary temporary storage data set usage is approaching a high percentage of its capacity so that you have time to free up storage before the auxiliary temporary storage becomes full.

CICS issues message DFHTS1316 when 75% or more of the maximum auxiliary temporary storage is in use, and message DFHTS1317 when storage usage falls below 70% of the maximum auxiliary temporary storage.

New statistics are available in Temporary storage: Global statistics to provide information about the current and peak percentage of auxiliary temporary storage being used.

This capability is partially available on CICS TS 5.6 with APAR PH28145.

Learn more...

Enhanced adapter tracking for CICS Db2 applications

The CICS Db2 attachment facility is enhanced to pass adapter data to Db2. If a CICS task that is accessing Db2 has adapter data in the CICS origin data, the adapter ID is passed as **appl-longname** and the adapter data is passed as an **accounting-string**. Db2 writes the data in its SMF accounting records and the data is also available online through the Db2 special registers CURRENT CLIENT_APPLNAME and CURRENT CLIENT_ACCTNG. This capability requires Db2 12 with APAR PH31447 or higher.

Service With APAR PH52668, you can disable the passing of adapter origin data to Db2 by specifying the feature toggle`com.ibm.cics.db2.origindata=false`

This capability is also available on CICS TS 5.4 through 5.6 with APARs PH30252 and PH49408.

Learn more...

Inquire on 64-bit storage that belongs to a task

A new SPI command, INQUIRE STORAGE64, and a new DFHSMMCX XPI call, INQUIRE_TASK_STORAGE64, can be used to retrieve information about 64-bit task storage.

Learn more...

Support for daisy-chaining of non-terminal-related START requests

Routing programs can now indicate daisy-chaining support of non-terminal-related **START** requests. If you are using a user-written distributed routing program to daisy chain non-terminal **START** requests over APPC connections, you must change the program to put the value Y into the DYRDCYN field (which replaces the DYRFILL1 field) in the DFHDYPDS copybook.

Learn more ...

Easier system management, efficient application development, and advanced client authentication available in single CICS regions with CMCI JVM server

The CICS Management Client Interface (CMCI) is a set of APIs that enable management of your CICS regions using tools such as CICS Explorer. When served from a JVM server, the CMCI provides additional capabilities such as multi-factor authentication (MFA), the GraphQL API, and the CICS bundle deployment API.

The CMCI JVM server is now able to be configured in a single CICS region outside of a CICSPlex SM environment to create an SMSS, enabling the following features:

- Enhanced security offered by multi-factor authentication (MFA), even in SMSS environments. Users can now sign on to an SMSS with MFA credentials in CICS Explorer for Aqua 3.2 (Fix Pack 5.5.20).
- Easier system management with the CMCI GraphQL API, which supports queries about multiple CICS resources and inter-resource relationships in a single request. CICS Explorer as of Fix Pack 5.5.20 also uses the GraphQL API to provide the aggregation function when connected to SMSS regions at CICS TS 5.6 with APAR PH35122, or a later release.
- Efficient application development with the CICS bundle deployment API, which allows Java developers to use the CICS-provided Gradle or Maven plug-ins to deploy bundles into single CICS development environment. This way, developers can see their application changes reflected in a running CICS region within seconds, and integrate the CICS bundle build and deployment into a toolchain to increase productivity, whilst the system programmer retains control.

Learn more...

Classify CICS regions by using region tagging

CICS regions can now be tagged or classified according to the key attributes of APPLID, region user ID, or job name. These tags can use exact or combine with specific wildcard characters, which you can use with any existing naming conventions. These tags can be viewed by using the **INQUIRE TAG** system command. They are also recorded in the SMF 1154 record.

In addition to classifying regions, the CICS region tag facility can be used to control the running of selected health checks. Region health check status is available through the **INQUIRE SYSTEM** or **CEMT INQUIRE SYSTEM** commands.

Learn more...

Messages reporting changes to APPC and IRC log names

DFHRS2112 messages are issued when log name mismatches are detected for connections by using the APPC and IRC protocols. The message explanation provides advice about how to resynchronize any outstanding units of work but it can be difficult to work out what caused the mismatch and how to prevent a recurrence. To help you diagnose log name mismatches, the following three messages that report changes to log names are introduced:

- DFHRM0240 reports the local log name that is set during CICS initialization and sent to a remote system when CICS establishes an APPC or IRC connection.
- DFHRM0241 reports a log name that has been set for an APPC or IRC connection.
- DFHRM0242 reports a log name that has been deleted for an APPC or IRC connection.

This capability is also available on CICS TS 5.3, 5.4, 5.5, and 5.6 with APAR PH03691.

Learn more...

Automatic recovery of failed user journals

When a log stream failure occurs, in addition to issuing message **DFHLG0772** and taking a system dump, CICS now attaches CLGR at the time **DFHLG0772** is issued. The new transaction CLGR attempts to recover and reset the failed user journal automatically for up to 60 minutes. This gives you an opportunity to fix the log stream problem, then allowing CICS to automatically recover journals for you. However, this feature comes with a cost in potential more system dumps being taken following a failed user journal, but you can control the number of system dumps taken.

Learn more...

Prepare for a future release of CICS TS

Service Available with APAR PH54840.

The DFHCSVC and DFHIRP modules for future CICS TS releases have been shipped as modules DFHNCSVC and DFHNIRP on current releases ahead of the general availability of the newest CICS TS release. If you wish to install the future release modules DFHCSVC and DFHIRP to fit in with your scheduled z/OS IPLs, follow the instruction here.

Enabling multiple client URIMAPs that point to the same endpoint

Multiple client URIMAPs that point to the same host, port and path can now be installed and enabled in a CICS region. This enhancement removes the limitation in earlier CICS releases that only one client URIMAP for an endpoint can be enabled in a CICS region. As best practice, always use a URIMAP by name.

This capability is also available on CICS TS 5.4, 5.5, and 5.6 with APAR PH44683.

Learn more ...

Running the Link3270 bridge with a custom transaction ID

The Link3270 bridge runs under CSMI by default. If you want to use a transaction ID other than CSMI for the Link3270 bridge, specify an INITPARM system initialization parameter for program DFHL3270.

Learn more...

Automating the process of defining CICS application resources with CICS Transaction Server resource builder

CICS Transaction Server resource builder is a DevOps utility, complementary to the CSD update batch utility program DFHCSDUP, that provides a way to automate the creation and maintenance of CICS application resource definitions by using a configuration-as-code approach.

With CICS resource builder, system programmers can create resource models in YAML that describe which resources and attributes developers are allowed to specify and how to specify them (for example, by enforcing naming conventions on particular attributes). System programmers provide application developers with these resource standards by generating a resource definition schema from the resource models, which is used by developers in their IDEs to create valid application resource definitions in YAML. CICS resource builder builds the application resource definitions that are defined in YAML into a DFHCSDUP commands file to be consumed by the DFHCSDUP utility program, which runs to update the CICS system definitions data set (CSD) for a CICS region.

CICS resource builder makes it easier for system programmers to enforce best practices and organization standards. Application developers can also enjoy a guided and controlled experience for creating and modifying CICS resource definitions in which they can have the confidence to be standards-compliant and pre-approved.

Learn more at Automating the process of defining CICS application resources with CICS Transaction Server resource builder and the CICS resource builder product documentation.

For security

- “TLS enhancements” on page 49. Some of these enhancements are also provided on other CICS releases through APAR.
- “New parameter GMEXITOPT on ASSIGN” on page 51
- “Instruction Execution Protection (IEP) for dynamic storage areas (DSAs)” on page 51
- “Enhanced support for IBM Health Checker for z/OS” on page 51
- “Simplifying Category 1 transaction security” on page 51
- “Classify CICS regions by using region tagging” on page 47
- “Improved security diagnosis with security request recording (SRR)” on page 51
- “Compliance data collection with SMF 1154 subtype 80 records” on page 52
- Service “New options on CHANGE PASSWORD and CHANGE PHRASE reveal more sign-on information” on page 52

TLS enhancements

- CICS supports TLS 1.3 for improved TCP/IP security.

  TLS 1.3 does not support sysplex caching by specifying the SYSPLEX option on the **SSLCACHE** SIT parameter.

  To assist with migration to TLS 1.3, CICS provides the new **MAXTLSLEVEL** system initialization parameter that specifies the maximum TLS protocol for secure TCP/IP connections.

  Learn more...

- Changing TLS protocol levels or ciphers is simplified with new statistics and monitoring data

  Improvements to CICS statistics and monitoring allow you to collect detailed data about which ciphers and TLS protocols are in use before changing the ciphers or TLS protocol levels. TLS protocols include both CICS-configured TLS and AT-TLS.

  New cipher resource statistics and the enhanced TCP/IP global statistics reveal what TLS protocol levels and ciphers are being used in your system.

  Improved monitoring information allows you to identify individual tasks that use specific TLS protocol levels or ciphers, and what system they are connected to:

  - New monitoring fields called SOTLSLVL and SOFLAG are available in performance class data. For more information, see Performance data in group DFHSOCK.
  - New monitoring fields called MNR_URIMAP_TLSLVL and MNR_URIMAP_FLAG are available in transaction resource class data. For more information, see Transaction resource class data: Listing of data fields.

  Learn more...

- Default cipher suite specification file for outbound web requests.

  A new feature toggle, `com.ibm.cics.web.defaultcipherfile`, enables CICS to use a set of ciphers from the default cipher suite specification file `defaultciphers.xml` instead of the default list of two-digit ciphers (3538392F3233). This allows a greater set of ciphers to be used for outbound requests without having to create a URIMAP for each potential endpoint. If the feature toggle is enabled but a problem exists with the `defaultciphers.xml` file, message DFHWB0112 is issued and CICS reverts to using the default list of two-digit ciphers. This capability is also available in CICS TS 5.6 with APAR PH38091.

  With APAR PH60212, the `com.ibm.cics.web.defaultcipherfile` feature toggle is extended to apply to URIMAP resources with no ciphers specified. Message DFHWB1561 is issued to indicate that a URIMAP defined with `CIPHERS()` is being installed and list the ciphers that CICS uses instead.

  Learn more...

- Service Key rings can be shared between regions in an easier way.

  APAR PH49261 required

  With the support of more acceptable formats of key ring names on the KEYRING system initialization parameter, you can now use key rings that are not owned by the current region user ID. To share a key ring owned by one region user ID with another region, grant that other region authority to use the key ring.

  This capability is also available on CICS TS 5.5 and 5.6 with APAR PH49253.

  Learn more...

- Service Minimum key size can be set during TLS handshakes for increased key strength.

  APAR PH51719 required

  With the new feature toggle `com.ibm.cics.tls.minimumkeystrength`, you can set a minimum key size for ECC, RSA, DSA, and Diffie-Hellman keys during TLS handshakes to increase the key strength.

  This feature is also available in CICS TS 5.4, 5.5, and 5.6 with APAR PH50175.

  Learn more...

- Service HTTP strict transport security (HSTS) is supported.

  APAR PH55370 required

  HTTP strict transport security (HSTS) helps servers prevent man-in-the-middle attacks by instructing compliant user agents to only interact with the server through secure connections (HTTPS).

  You can now configure a CICS server to use HSTS with a set of `com.ibm.cics.web.hsts` feature toggles.

  This feature is also available in CICS TS 5.5 and 5.6 with APAR PH55369.

  Learn more...

New parameter GMEXITOPT on ASSIGN

New parameter **GMEXITOPT** is added to the **ASSIGN** command to show the GMTRAN terminal session behavior option on a PF3 or PF15.

Learn more...

Instruction Execution Protection (IEP) for dynamic storage areas (DSAs)

Instruction Execution Protection allows storage to be allocated in a non-executable state. This helps to protect systems from malicious attacks or from errors, such as stack overflow.

If the hardware and the version of z/OS that CICS runs on support Instruction Execution Protection (IEP), CICS can use IEP to protect certain dynamic storage areas (DSAs) from instruction execution. IEP is supported on z/OS 2.4 and above. z/OS 2.4 and z/OS 2.5 require APAR PH39134. By default, DSA protection is off; activate it with a feature toggle `com.ibm.cics.sm.iep=true`.

It is still possible to request storage that is not protected from instruction execution, for example, for GLUE and TRUE work areas or for dynamic storage for assembler programs. To enable this, there are four new DSAs: PCDSA, PUDSA, EPCDSA, and EPUDSA. These four DSAs, along with the existing RDSA and ERDSA, are never protected from instruction execution. Depending on the attributes of the program, CICS loads the program into one of the four new DSAs or into the RDSA or ERDSA. When IEP is enabled, all other DSAs are protected from instruction execution.

In a related change, the ETDSA is removed and any storage that was allocated from this DSA is now allocated from the ECDSA.

Although the allocation of storage used by individual tasks running in the CICS region is not increased by IEP, the distribution of that storage within the DSAs is changed and you should expect an increase in DSA storage requirements.

Learn more...

Enhanced support for IBM Health Checker for z/OS

CICS TS now supports several health checks that define best practices for CICS TS security. If a CICS region becomes non-compliant with these security best practices, warning or exception messages are issued so that you can take corrective actions.

Learn more...

Simplifying Category 1 transaction security

Previously, when starting a CICS TS Category 1 transaction, a call to RACF validated that the configuration was correct. RACF is no longer checked when starting a CICS Category 1 transaction. This change improves security as only CICS determines that a Category 1 transaction can run. This change also simplifies configuration and upgrades because there is no need to define the Category 1 transactions to RACF, which might create misconfiguration. You will need to define the CICS region user ID to RACF to confirm the ID that is used for running CICS Category 1 transactions. Surrogacy definition is still required as documented in Surrogate security.

Learn more...

Improved security diagnosis with security request recording (SRR)

Security request recording (SRR) collects trace data about security settings in CICS regions by recording security checks conducted by one or more requests. You can use it to diagnose complex security problems.

You can use CICS Explorer or the SPI command (**SET SECRECORDING**) to enable SRR.

A batch utility and sample JCL are provided to output the logged data to a summary report and a `.csv` file for diagnosis.

Learn more...

New message DFHXS1117 reveals more information about security violations

A new message DFHXS1117 is introduced to provide additional diagnostic information, where available, for security violations. The data includes the association data, including origin information related to a security violation.

Learn more...

Compliance data collection with SMF 1154 subtype 80 records

To assist evidence providers in collecting evidence for auditors, CICS is able to collect compliance data as part of z/OS compliance evidence collection.

CICS regions can generate an SMF 1154 subtype 80 record in response to ENF86 triggered by the z/OSMF Compliance REST API. This provides much of the data usually requested by an auditor. The data is securely written to SMF. This compliance data can be formatted using a CICS sample, or can be consumed by the IBM Z® Security and Compliance Center.

Learn more...

New options on `CHANGE PASSWORD` and `CHANGE PHRASE` reveal more sign-on information

Service APAR PH59547 required

New options `CHANGETIME`, `DAYSLEFT`, `EXPIRYTIME`, `INVALIDCOUNT`, and `LASTUSETIME` are added to CHANGE PASSWORD and CHANGE PHRASE commands. These options reveal more sign-on information, for example, the last time the password or password phrase was changed, the last time the user ID was accessed, when the password or password phrase will expire, and the number of times when an invalid password or password phrase was entered.

This capability is also available in CICS TS 5.5 and 5.6 with APAR PH59546.

For performance

- "Support for association data of DPL requests by EXCI clients" on page 52
- "Enhanced capability for monitoring shared pool TS queue usage" on page 52

Support for association data of DPL requests by EXCI clients

You can now identify the job names of DPL requests by EXCI clients from their performance records. If a task was initiated by an EXCI client, in the performance record of the DPL request, field 374 (PHAPPLID) contains the EXCI job name, field 378 (PHCOUNT) contains a value of 1, and field 376 (PHTRANNO) has a value of 0.

As the performance record of a DPL request can provide association data for DPL requests by EXCI clients as well as for CICS-to-CICS DPL requests, you can distinguish whether PHAPPLID contains a CICS applid or an EXCI job name as follows:

- If PHCOUNT is 1, PHTRANNO is 0, and PHAPPLID is not blank, the PHAPPLID value is the EXCI job name.
- If PHTRANNO is not 0, the record is of a CICS-to-CICS DPL request, and the PHAPPLID value is a CICS applid.

Learn more...

Enhanced capability for monitoring shared pool TS queue usage

This enhancement makes it easier for you to monitor capacity usage change for shared pool TS queues. When the percentage of entries or elements in use in a pool structure reaches a specified threshold, DFHXQ0422 or DFHXQ0423 is issued. When the percentage of entries or elements in use drops below a threshold, DFHXQ0420 or DFHXQ0421 is issued.

This capability is also available on CICS TS 5.6 with APAR PH28145.

Learn more...

For resilience

Enhanced outbound web support: `WEB OPEN URIMAP` command can use cached IP address and HTTP information

The **`EXEC CICS WEB OPEN URIMAP`** command is enhanced to use the cached IP address that is held in the URIMAP after the initial connection was established. It uses this address for subsequent outbound web requests that use the same URIMAP, thus eliminating unnecessary DNS lookups. If a connection that uses the cached IP address fails, **`WEB OPEN`** performs a DNS lookup and updates the URIMAP with the IP address upon a successful connection. If you want to reset or remove the cached IP address that is held in the URIMAP, disable and then re-enable the URIMAP to force CICS to perform a DNS lookup. If you have multiple URIMAPs that reference the same HOST, then only one of the URIMAPs needs to be disabled and re-enabled in order to reset the cached IP address for all of them. The **`EXEC CICS INVOKE SERVICE`** command also benefits from the IP address caching if a URIMAP is used.

If you also specify the HTTPVNUM and HTTPRNUM options with **`WEB OPEN URIMAP`**, or if you issue **`WEB SEND`** with the ACTION(EXPECT) or CHUNKING option, CICS obtains the HTTP version information when it opens the connection. It caches the host HTTP information for subsequent outbound requests that use the same URIMAP, thus reducing HTTP OPTIONS requests.

Learn more ...

Cap on concurrent TLS handshakes

CICS limits the number of concurrent TLS handshakes to 90% of the **`MAXSSLTCBS`** value specified at startup. If the maximum limit is reached, a task that is requesting a TLS handshake is suspended with a resource name of S8TLSHS of resource type DSWC.

To help you monitor concurrent TLS handshakes in a CICS region, new statistics are introduced in TCP/IP Global statistics. These statistics provide information about the maximum, current, and peak numbers of TLS handshakes that are running in parallel or that are waiting.

This enhancement helps avoid issues such as high CPU, MAXTASK, or lack of S8 TCBs when many TLS handshakes are performed concurrently. It also allows in-flight web alias or pipeline tasks to obtain an available S8 TCB in order to send a reply back to the client in the same situation.

Learn more...

START CHANNEL supports NOCHECK and PROTECT options

This enhancement makes it easier to migrate from passing data by interval control (START FROM) to passing data by using a channel (START CHANNEL). When you use a channel to pass data for a START request, you can now use the NOCHECK option to indicate that the request must be shipped to a remote system and no response is expected by the starting task, thus improving CICS performance.

With the PROTECT option, you can make the START request effectively recoverable by instructing the starting task to take a syncpoint before committing the START request.

Learn more...

Extended short on storage (SOS) notification

CICS has long provided monitoring and short on storage (SOS) support for CICS-managed storage in dynamic storage areas (DSAs), which includes the capability of the CICS storage manager domain to notify other CICS domains so that they can take action upon an SOS event in CICS DSAs. In CICS TS 5.6, the CICS storage manager domain was enhanced to monitor the use of user region (24-bit) and extended user region (31-bit) MVS storage not managed by CICS, but this enhancement did not support SOS notification to other domains. In CICS TS 6.2, the SOS notification is enhanced to provide the same notification support for MVS storage SOS events as for CICS DSA SOS events.

The DFHUS domain is notified of z/OS MVS SOS conditions so that any eligible user ID and its associated attributes are freed, including RACF control blocks. The freeing of these control blocks is normally subject to USRDELAY processing, but in the event of an SOS condition in 31-bit MVS storage, these control blocks are now freed immediately by the US and XS domains.

The Region status domain is notified of z/OS SOS conditions so that CICSPlex SM factors z/OS SOS conditions into its routing algorithm, in the same way as it does for CICS-managed storage SOS conditions.

Support for passing XID to Db2

Service APAR PH47996 required

A new DB2ENTRY attribute SHARELOCKS is provided to enable CICS to pass an XID to Db2 and instruct Db2 to share locks between threads that pass the same XID. Using the same XID, other threads that originate from other CICS regions or from other transaction managers such as IMS TM can access Db2 in the same global unit of work (UOW). The XID token is not used for recovery between CICS and Db2. The passing of an XID involves a partial signon to Db2 for each UOW. This action closes cursors, so held cursors across syncpoints are not supported when the passing of an XID is enabled. Applications will have to reposition cursors after a syncpoint. Passing an XID avoids having to deal with UOW affinities.

This capability is also available on CICS TS 5.5 and 5.6 with APAR PH39766, but is facilitated by feature toggle `com.ibm.cics.db2.sharelocks={true|false}`.

Learn more ...

Enhanced shared data tables

The capacity of shared data tables is increased. Shared data tables no longer use the two control data spaces named DFHDT001 (which was used for table entry descriptors and backout elements) and DFHDT002 (which was used for index nodes), and instead are now using 64-bit storage to hold this control information. The use of 64-bit storage to hold the entry descriptors, backout elements, and index nodes removes the constraint on the number of records that can be stored. The records continue to be stored in 31-bit data spaces. Now, two more data spaces are available to hold the records.

Previously, the number of records that could be stored was governed by the size of the key of the records. For example, previously a 45-byte key would mean a limit of 36 million records per file owning region (FOR), and this limit on index information was reached long before all the data space storage available to hold the records was consumed.

Previously, up to 98 data spaces could be used per FOR to hold the records. Now that is increased to 100 data spaces.

You can use the new system initialization parameter **SDTMEMLIMIT** to set the maximum amount of storage above the bar that is available for shared data tables to use for control information. You can use SPI commands INQUIRE SYSTEM SDTMEMLIMIT and SET SYSTEM SDTMEMLIMIT and their CEMT equivalents to inquire or increase the SDTMEMLIMIT value.

Learn more...

Enhanced CICS event processing support

Application events now support the PUT64 CONTAINER capture point. You can capture and emit events when your application program issues an **EXEC CICS PUT64 CONTAINER** command or when it invokes one of the two put methods or the putString method in the JCICS com.ibm.cics.server.Container class.

Learn more...

Changes to CICSPlex SM sysplex optimized workload routing behavior

The default behavior of CICSPlex SM workload management routing algorithms has been updated to increase the likelihood that work is routed to healthy, local target regions. This change applies only to the QUEUE and GOAL algorithms, not to the link neutral variants (LNQUEUE and LNGOAL).

Where a routing region might be subject to surges of extremely high frequency, short duration transactions, workload batching might occur. A new feature toggle, `com.ibm.cics.cpsm.wlm.surgeresist={true|false}`, has been introduced to mitigate these surges by reducing the likelihood that recently selected target regions are reselected. Enabling this feature toggle increases the average routing cost per transaction, but restores the routing behavior of CICSPlex SM at CICS TS 5.6 before APAR PH30768 is applied.

Learn more ...

WRITE OPERATOR enhanced to support writing messages to a specific console

The **WRITE OPERATOR** API command supports a new option **CONSNAME**, which you can use to specify a specific console to receive messages. This option enables messages to be sent to a specific console.

Learn more...

Improved temporary storage expiry processing

The processing of expired temporary storage queues has been improved as follows:

- Firstly, the processing of main and auxiliary tsqueues is separated from the processing of shared tsqueues so that they use separate calculated intervals.
- Secondly, for shared tsqueues, an internal queue is used to hold when the last scan was performed. The internal queue is used to prevent a CICS region from scanning shared TS queues if another CICS region has performed such a scan within the previous minute. This means that even if multiple CICS regions are using a shared TS pool, each with TS models installed that specify short expiry intervals, the shared queues are never scanned more frequently than once per minute.
- Thirdly, the CICS-MQ interface has been improved to only employ a DFHCKBR tsmodel with a nonzero expiry interval when the MQ bridge has been started; otherwise, it has a zero expiry interval. This avoids unwanted tsqueue scans.

This capability is also available on CICS TS 5.6 with APAR PH40863 and PH40409.

Improved processing of WS-AT requests

A new transaction CPIW is introduced to handle WS-AT protocol messages. The DFHRSURI URIMAP is changed to specify TRANSCTION(CPIW) by default. CPIW tasks should not be put into a TCLASS. This allows WS-AT protocol messages to always be handled even if the limit of concurrent application requests has been reached.

If you are using a customized version of DFHRSURI that no longer specifies TRANSACTION(CPIH), no action is needed, and you can continue to use your customized DFHRSURI unchanged.

However, if the CSD is being shared with a back level region, see Changes to resource definitions to determine if any action is necessary.

Learn more...

For documentation and other information

There are enhancements to the CICS content:

- CICS online documentation and IBM Documentation Offline are now automatically translated in various languages other than English: Brazilian Portuguese, French, German, Italian, Japanese, Korean, Simplified Chinese, and Spanish. PDF documentation is not currently translated.

Learn more...

Chapter 4. Changes to CICS externals in CICS TS 6.1

Every release of CICS introduces changes to the elements that you see and work with, collectively known as the CICS *externals*. These include commands, transactions, resources, system initialization parameters, messages, trace, and user exits, and more. This page summarizes the changes for CICS TS 6.1.

For a summary of changes across all supported releases, see Changes between releases in the Upgrading information. (In PDF, it's in *Upgrading CICS*.

Changes to installing

- The DFHIFTG1 and DFHIFTGS installation jobs have been removed.
- DFHEITAB and DFHEITBS modules are not LPA eligible.

Changes to security

Table 30. Changes to security in CICS TS 6.1

Area	**6.1**
Authentication	**CHANGED:** • New option GMEXITOPT on ASSIGN shows the GMTRAN terminal session behavior option on a PF3 or PF15. Service **CHANGED with APAR:** • **APAR PH59547:** New options CHANGETIME, DAYSLEFT, EXPIRYTIME, INVALIDCOUNT, and LASTUSETIME added to CHANGE PASSWORD, and CHANGE PHRASE commands to reveal more information about the sign-on user ID and password.
Authorization	**NEW:** • Security request recording is available to troubleshoot authorization failures • New message DFHXS1117 provides additional diagnostic information about security violations. **REMOVED:** • Authorization check for Category 1 transactions is removed. There's no need to define Category 1 transaction to RACF anymore.
Integrity	**NEW:** • Instruction execution protection Service **NEW with APAR:** • **APAR PH55370:** HTTP strict transport security (HSTS) is supported when CICS acts as a server.

Table 30. Changes to security in CICS TS 6.1 (continued)	
Area	**6.1**
Confidentiality	**NEW:** • TLS 1.3 is supported. This capability requires z/OS 2.4 or higher. See Enabling TLS 1.3 in CICS. • MAXTLSLEVEL system initialization parameter is available. • Feature toggle `com.ibm.cics.web.defaultcipherfile` allows you to use ciphers from the default cipher suite specification file (`defaultciphers.xml`) for outbound web requests. It applies to outbound HTTP requests using **`EXEC CICS WEB OPEN`** or **`EXEC CICS INVOKE SERVICE`** commands that do not specify `CIPHERS` or `URIMAP`. Service **NEW with APAR:** • **APAR PH51719:** Feature toggle `com.ibm.cics.tls.minimumkeystrength` allows CICS to set the minimum key size during TLS handshakes for increased key strength. **CHANGED:** • Statistics and monitoring data about TLS protocol levels and ciphers including: – New fields SOTLSLVL and SOFLAG in Performance data in group DFHSOCK. – New fields MNR_URIMAP_TLSLVL and MNR_URIMAP_FLAG in Transaction resource class data: Listing of data fields. – New cipher resource statistics provide details of the ciphers that are in use. – TLS protocol level usage is available in the TCP/IP global statistics. • MINTLSLEVEL system initialization parameter: **NEW OPTION:** TLS13 **REMOVED OPTIONS:** TLS10, TLS10ONLY **STABILIZED OPTION:** TLS 1.1 • Improved TLS diagnostics including: – New fields SOTLSLVL and SOFLAG in Performance data in group DFHSOCK. – New fields MNR_URIMAP_TLSLVL and MNR_URIMAP_FLAG in Transaction resource class data: Listing of data fields. – New message DFHXS1117 provides additional diagnostic information. Service **CHANGED with APAR:** • **APAR PH49261:** KEYRING system initialization parameter accepts more formats of key ring names to allow use of key rings that are not owned by the region user ID. • **APAR PH60212:** The feature toggle `com.ibm.cics.web.defaultcipherfile` is extended to apply to URIMAP resources with no ciphers specified.

Table 30. Changes to security in CICS TS 6.1 (continued)	
Area	**6.1**
Auditing	**NEW:** • Classifying CICS regions with region tagging • CICS regions can generate an SMF 1154 subtype 80 record in response to ENF86 triggered by the z/OSMF Compliance REST API. **CHANGED:** • New CICS health checks that define best practices for CICS security: – CICS_CAT3_CONFIGURATION – CICS_REGION_CONFIGURATION – CICS_RESOURCE_CONFIGURATION – CICS_RESOURCE_SECURITY – CICS_USS_CONFIGURATION
Deprecated and removed	**REMOVED:** • ENCRYPTION system initialization parameter • XSNEX global user exit **DEPRECATED:** • Numeric ciphers

Changes to RACF classes

No changes in this release.

Changes to CICS support for application programming languages

Table 31. Changes to CICS support for application programming languages in CICS TS 6.1	
Product name (PID)	**6.1**
IBM Open Enterprise SDK for Node.js, 18.0 (5655-NOJ)	**NEW:** Enabled support
IBM Open Enterprise SDK for Node.js, 12.0 (5655-NOD)	**CHANGED:**Removed support

Changes to compiler and translator support

No changes in this release.

Changes to EXEC CICS API

*Table 32. Changes to **EXEC CICS** commands in CICS TS 6.1*	
API	**6.1**
ASSIGN	**CHANGED:** New parameters • **GMEXITOPT** returns the terminal session behavior option set for the SIT parameter GMTRAN.

*Table 32. Changes to **EXEC CICS** commands in CICS TS 6.1 (continued)*	
API	**6.1**
CHANGE PASSWORD	**CHANGED:** • New NOTAUTH with RESP2 value of 1, indicating that the PASSWORD field, the NEWPASSWORD field, or both are blank. • New NOTAUTH with RESP2 value of 17, indicating that the USERID is not authorized to use the application. Service **CHANGED with APAR:** • **APAR PH51378:** New INVREQ with RESP2 value of 32. • **APAR PH59547:** New options CHANGETIME, DAYSLEFT, EXPIRYTIME, INVALIDCOUNT, and LASTUSETIME added to reveal more information about the user ID's password or password phrase.
CHANGE PHRASE	**CHANGED:** • New NOTAUTH with RESP2 value of 1, indicating that the PHRASE field, the NEWPHRASE field, or both are blank. • New NOTAUTH with RESP2 value of 17, indicating that the USERID is not authorized to use the application. Service **CHANGED with APAR:** • **APAR PH51378:** New INVREQ with RESP2 value of 32. • **APAR PH59547:** New options CHANGETIME, DAYSLEFT, EXPIRYTIME, INVALIDCOUNT, and LASTUSETIME added to reveal more information about the user ID's password or password phrase.
GETMAIN	**CHANGED:** New option EXECUTABLE in support of Instruction Execution Protection
GETMAIN64	**CHANGED:** New option EXECUTABLE in support of Instruction Execution Protection
START CHANNEL	**CHANGED:** New options NOCHECK and PROTECT.
WEB OPEN	**CHANGED:** WEB OPEN URIMAP uses the cached IP address and HTTP information obtained with the initial connection, for subsequent outbound web requests that use the same URIMAP. **DEPRECATED:** Numeric CIPHERS deprecated. Use XML cipher suite files as the replacement.
WRITE OPERATOR	**CHANGED:** New option CONSNAME, to specify a specific console to which messages are sent. With the addition of CONSNAME, the following conditions are introduced: • New INVREQs with RESP2 values of 7 and 8, indicating that the specified CONSNAME value is not valid • New ERROR with RESP2 value of 1, indicating that the MVS WTO command issued by CICS for the **WRITE OPERATOR** request has returned an error.

*Table 32. Changes to **EXEC CICS** commands in CICS TS 6.1 (continued)*	
API	**6.1**
VERIFY PASSWORD	**CHANGED:** • New NOTAUTH with RESP2 value of 1, indicating that the PASSWORD field is blank. • New NOTAUTH with RESP2 value of 17, indicating that the USERID is not authorized to use the application.
VERIFY PHRASE	**CHANGED:** • New NOTAUTH with RESP2 value of 1, indicating that the PHRASE field is blank. • New NOTAUTH with RESP2 value of 17, indicating that the USERID is not authorized to use the application.

Table 33. Changes to macros in CICS TS 6.1	
Macro	**6.1**
DFHEIENT macro	**CHANGED:** New option DATA_EXECUTABLE to request that dynamic storage is not protected from instruction execution.

Changes to CICS EXCI

No changes in CICS TS 6.1.

Changes to the JCICS API: removed classes and methods

Table 34. Previously deprecated methods and classes which have been removed. Any applications that use these methods and classes must be changed before moving to CICS TS 6.1.

Class/Interface	Methods	6.1
Program	`link(IByteBuffer)` `link(IByteBuffer, IByteBuffer)`	**REMOVED:** The previously deprecated methods `link(com.ibm.record.IByteBuffer)` and `link(com.ibm.record.IByteBuffer, com.ibm.record.IByteBuffer)` have been removed from the class `com.ibm.cics.server.Program`. Any OSGi dependencies or code dependencies on the `com.ibm.record` package should be removed from customer applications and builds. Correspondingly, the JAR file `${USS_HOME}/lib/com.ibm.record.jar` has been removed from the CICS installation. To ease migration of these changes, the package `com.ibm.record` (now empty) is declared as exported by the `com.ibm.cics.server` bundle. This avoids the need for repackaging or recompiling applications that express an unnecessary dependency on that package. If, however, your application genuinely uses these methods at runtime, you must rewrite that application - the API is no longer supported by CICS.

CicsSecurityManager	`checkMultiCast(InetAddress, byte)`
	`checkAwtEventQueueAccess()`
	`checkMemberAccess(Class<?> theClass, int which)`
	`checkSystemClipboardAccess()`
	`checkTopLevelWindow(Object window)`
		REMOVED: These methods override methods in `java.lang.SecurityManager`, which are deprecated by Java. They have now been removed from the `CicsSecurityManager.java` class.
		
		The `checkTopLevelWindow(Object window)` method always returned true, and the other methods were no-operation methods.
		
		If your application calls these methods, you should instead invoke `checkPermission(java.security.Permission)` as recommended by the Javadoc for these methods.

Table 34. Previously deprecated methods and classes which have been removed. Any applications that use these methods and classes must be changed before moving to CICS TS 6.1. (continued)

Class/Interface	Methods	6.1
TerminalPrincipalFacilityExtended		**REMOVED:** This entire class is removed. This class was provided in CICS TS 1.3 to support additional functionality for the `TerminalPrincipalFacility` class, when using the Enterprise Toolkit for OS/390® (Java program objects). In CICS TS 2.1 and later, for interpreted Java (JVM programs), the additional functionality is now available directly in the `TerminalPrincipalFacility` class. Applications that call this class should be changed to call the same method from the `TerminalPrincipalFacility` class.
TerminalPrincipalFacility	`waitTerminal()`	**REMOVED:** The previously deprecated method `waitTerminal()` is removed. All methods in the class are synchronous so there is never a need to wait for the terminal. The deprecated method was a no operation method. Calls to this method should be removed from your application as it is no longer supported by CICS.
HttpHeader	`getHeader()`	**REMOVED:** The previously deprecated method `getHeader()` is removed. This deprecated method returns the name of the HTTP header by calling method `getName()`. If your application uses this method, you must rewrite that application to call `getName()` directly because it is no longer supported in CICS.
Task	`disableTaskTrace()` `enableTaskTrace()`	**REMOVED:** The previously-deprecated methods `disableTaskTrace()` and `enableTaskTrace()` are removed. These deprecated methods currently throw an exception with a message saying `Method is not supported in this release of CICS TS`. Calls to both methods should be removed from your application because they are no longer supported by CICS.

Table 34. Previously deprecated methods and classes which have been removed. Any applications that use these methods and classes must be changed before moving to CICS TS 6.1. (continued)

Class/Interface	Methods	6.1
Container	`put(String stringData)`	**REMOVED:** The previously-deprecated method `put(String stringData)` is removed. This deprecated method risked exhibiting unexpected behavior due to the way the underlying container was created. Replace calls to this method with `putString(String stringData)`.
ILongHolder		**REMOVED:** This entire class is removed.
AbendError		**REMOVED:** This entire class is removed.
UnknownCicsError		**REMOVED:** This entire class is removed.

Changes to the JCICS holder classes

Table 35. A number of classes which were used to hold data for objects (such as the CWA, TSQ items, file records, the commarea, and more) previously exposed public data fields. These fields were deprecated at CICS TS 5.1 and must now be accessed using an appropriate getter or setter method. Direct access to these fields has now been removed.

Class	Removed field(s)	Getter(s)	Setter(s)
CWAHolder	public byte[] value;	public byte[] getValue() public String getStringValue()	public void setValue(byte[] bytes)
DataHolder	public byte[] value;	public byte[] getValue() public String getStringValue()	public void setValue(byte[] value) public void set String Value(String value ToSet)
ItemHolder	public byte[] value;	public byte[] getValue() public String getStringValue()	public void setValue(byte[] bytes)
KeyHolder	public byte[] value;	public byte[] getValue() public String getStringValue()	public void setValue(byte[] newValue)
RecordHolder	public byte[] value;	public byte[] getValue() public String getStringValue()	public void setValue(byte[] bytes)
RetrievedData	public byte[] data; public String transId; public String termId; public byte[]queue;	public byte[] getData() public String getStringData() public String getTransId() public String getTermId() public byte[] getQueue() public String getStringQueue()	public void setValue(byte[] bytes) public void setTransid(String newTransId) public void setTermid(String newTermId) public void setQueueName(byte[] newQueueName)
RetrievedDataHolder	public RetrievedData value;	public RetrievedData getValue()	public void setValue(Retrieved Data newValue)
TCTUAHolder	public byte[] value;	public byte[] getValue() public String getStringValue()	protected void setValue(byte[] newValue)
TWAHolder	public byte[] value;	public byte[] getValue() public String getStringValue()	public void setValue(byte[] newValue)
CommAreaHolder	public byte[] value;	public byte[] getValue()	public void setValue(byte[] newCommarea) public String getStringValue()

Changes to the JCICS API - new, changed, and deprecated functions

Table 36. New, changed, and deprecated JCICS API functions in CICS TS 6.1

Function	**6.1**
`com.ibm.cics.server.jar`	**Changed:** Reduced footprint from 873K to 448K. If you are writing an application using RMI over IIOP, you need to include `com.ibm.cics.delegate.jar` (83K) and `com.ibm.cics.common.log.jar` (8K) to allow error information to flow back to the client.
CICS Exceptions	**Changed:** Exceptions include a public constructor, enabling applications to mimic any errors thrown by the JCICS API for unit testing.
Classes	**6.1**
Container	**Changed:** `get()` and `getNoConvert(...)` calls now require `LengthErrorException` to be handled at compile time.

Resource classes:
• ESDS
• KSDS
• NameResource
• Service
• WebService
• File
• RRDS
• KeyedFile
• Program
• TSQ
• TDQ
	New:
	These resources have a new name-bearing constructor allowing the resource to be created and named in one statement. For example:
	`new ESDS(name);`
	`new Program(name);`

Data holder classes: • CWAHolder • DataHolder • ItemHolder • KeyHolder • RecordHolder • RetrievedData • RetrievedDataHolder • TCTUAHolder • TWAHolder • CommAreaHolder	**New:** All holder-types have setters and getters to allow full manipulation of the data held within each holder. These setters and getters facilitate unit testing of application code. For more information, see Changes to the JCICS API - changes to the JCICS holder classes.
Task	**Deprecated:** Direct access to `PrintWriter` data members: `fixedOutForJVMLifetime`, `fixedErrForJVMLifetime`, `err`, `out`. Setter and getter methods for these deprecated data members are available to replace direct data member access. **New:** `getStartCode()` returns a stronger-typed **`StartCode`** enum value. **Deprecated:** `int getSTARTCODE()` - use `getStartCode()` instead. **Deprecated:** Method `getQNAME()` always returns null.
StartCode	**New:** Provides more explicit detail returned from the `Task.getStartCode()` method.
Version	**New:** Support of the `comparable<Version>` interface **New:** Constructor `Version(String versionString)`

Table 36. New, changed, and deprecated JCICS API functions in CICS TS 6.1 (continued)	
Function	**6.1**
API	**New:** Application code can check the version of `com.ibm.cics.server.jar` it is running against, with `Version getCicsServerApiVersion()`

ContainerIterator	**Deprecated:**
	`Object getOwner()`
	New:
	`Channel getChannel()`

Channel	**Changed:**
	It is possible to turn off explicit checking for the existence of underlying CICS container resources performed as default by `channel.getContainer(…)` calls by setting a new system property. Turning off explicit checking can reduce CPU usage.
	New:
	System property `-Dcom.ibm.cics.server.container.existence.checking.default=false` controls existence checking at a JVM level.
	New:
	`channel.setContainerExistenceCheckingEnabled(boolean);` controls existence checking at a channel level.
	New:
	`channel.getContainer(String containerName,boolean existenceChecking);` explicitly controls if existence checking is performed or not, instead of allowing defaults that are set in the channel or system property to have any effect.
	New:
	`container.exists();` explicitly checks for the existence of the underlying CICS container resource.
	New:
	`channel.isContainerExistenceCheckingEnabled();` checks if implicit checking for the existence of the underlying CICS container resource is enabled or disabled on future calls to `channel.getContainer`
	New:
	`channel.getContainerNames();` returns a list of all the names of existing CICS containers associated with a channel.
	Deprecated:
	`ContainerIterator`, `Channel.getContainerIterator`, `Task.getContainerIterator`

IsCICS	**New:** getApiStatus (boolean lateBind); set `lateBind` to `true` if late binding to a CICS transaction is to be performed for current task and status is currently CICS_REGION_BUT_API_DISALLOWED.

Changes to Liberty features

Table 37. Newly-supported Liberty features in CICS TS 6.1	
Feature	**6.1**
`batchSMFLogging-1.0`	**NEW:** Collects SMF 120 information about Java batch jobs
`collectiveController-1.0`	**NEW:** Allows a server to become the controller for a management collective.
`collectiveMember-1.0`	**NEW:** Enables a server to be a member of a management collective.
`clusterMember-1.0`	**NEW:** Allows a collective member to participate in a static cluster.
`dynamicRouting-1.0`	**NEW:** Enables a server to run a REST service to which the WebSphere plug-in for Apache and IHS can connect in order to dynamically route to all servers in the liberty collective.
`healthAnalyzer-1.0`	**NEW:** Provides health data collection for the health manager.
`healthManager-1.0`	**NEW:** Provides health monitoring and automatic actions based on health policies.

Table 37. Newly-supported Liberty features in CICS TS 6.1 (continued)	
Feature	**6.1**
`zosRequestLogging-1.0`	**NEW:** Collects HTTP request information and writes an SMF 120 record for each request

Changes to JVM server profile options

Application programmers

No changes in CICS TS 6.1.

Changes to JVM system properties

Application programmers

Table 38. Changes to JVM system properties in CICS TS 6.1	
Property	**6.1**
`-Dcom.ibm.ws.zos.core.angelRequiredServices`	**NEW:** Specifies which z/OS authorized services should be checked to see if they are available to the Liberty server being started.
`-Dcom.ibm.cics.jvmserver.wlp.security.subject.create={true|false}`	**NEW:** Allows the user to turn off Java security subject creation when performing a `LINK` to Liberty.
`-Dcom.ibm.cics.server.container.existence.checking.default`	**NEW:** Allows the user to turn off explicit checking for the existence of underlying CICS container resources performed as default by `channel.getContainer(...)` calls.
`-Dcom.ibm.cics.jvmserver.wlp.wab`	**DEPRECATED:** This property is no longer respected and can be removed from the JVM profile. CICS automatically installs the `wab-1.0` feature when `servlet-3.1` or below is installed, and removes it when `servlet-4.0` or higher is installed.

Changes to context containers

Table 39. Changes to the context containers used in a PIPELINE	
Container	**6.1**
DFHWS-URIMAP	**NEW:** In a requester PIPELINE, DFHWS-URIMAP contains the 8-character name of the URIMAP used on the **`INVOKE SERVICE`** command, or 8 blanks if a URIMAP was not specified. For a provider PIPELINE, DFHWS-URIMAP contains the 8-character name of the URIMAP that matched the inbound request. You cannot change the contents of this container.

Changes to the CICS assistants

No changes in this release.

Changes to SIT parameters

Table 40. Changes to system initialization parameters in CICS TS 6.1	
SIT	**6.1**
CPSMCONN	**CHANGED:** New option SMSSJ. **CPSMCONN**=SMSSJ initializes a single CICS region that is not part of a CICSplex as a CICS System Management Single Server (SMSS) and automatically creates a Liberty JVM server named EYUCMCIJ as the CMCI JVM server of the region.
DTRPGM	**CHANGED:** When **DTRPGM=NONE** is specified, no routing program is invoked. If you are using a routing program with the name of NONE, you must rename the program and change the **DTRPGM** setting accordingly.
ENCRYPTION	**REMOVED:** With the changes to enable support of TLS 1.3, the need for the ENCRYPTION parameter is removed.
EPCDSASZE	**NEW:** Specifies the size of the EPCDSA dynamic storage area.
EPUDSASZE	**NEW:** Specifies the size of the EPUDSA dynamic storage area.
KEYRING	Service **CHANGED with APAR:** • **APAR PH49261:** The parameter accepts more formats of key ring names, which allows you to specify key rings that are not owned by the region user ID.
MINTLSLEVEL	**CHANGED:** The option to set TLS 1.0 or TLS 1.1 is removed for **MINTLSLEVEL**.
MAXTLSLEVEL	**NEW: MAXTLSLEVEL** defines the maximum level of TLS currently in operation. Review the Enabling TLS 1.3 in CICS documentation before enabling TLS 1.3 on your system.
PCDSASZE	**NEW:** Specifies the size of the PCDSA dynamic storage area.
PUDSASZE	**NEW:** Specifies the size of the PUDSA dynamic storage area.
RESOVERRIDES	**NEW:** Specifies the name of the resource overrides file.
SDTMEMLIMIT	**NEW:** Specifies a limit to the amount of storage above the bar that is available for shared data tables to use for control information (entry descriptors, backout elements, and index nodes).

Changes to CICS storage

Table 41. Changes to CICS storage in CICS TS 6.1	
Storage area	**6.1**
ETDSA	**REMOVED:** Any storage that was allocated from this DSA is now allocated from the ECDSA.
PCDSA, PUDSA, EPCDSA, and EPUDSA	**NEW:** To enable the allocation of storage that is not protected from instruction execution. These DSAs have new subpools and some subpools that have moved from the CSDA, SDSA and their equivalent extended DSAs. See CICS dynamic storage areas (DSAs).
Subpools LDPGM, LDEPGM, LDRES, LDERES, LDNRS, LDENRS, LDNUC, and LDENUC	**CHANGED:** These subpools are now allocated in PCSDA, PUDSA, and their equivalent extended DSAs.

Table 41. Changes to CICS storage in CICS TS 6.1 (continued)	
Storage area	**6.1**
CDSA, SDSA, ECDSA, ESDSA locations	**CHANGED:** Loader Domain functions ACQUIRE_PROGRAM, RELEASE_PROGRAM, INQUIRE_PROGRAM, GET_NEXT_PROGRAM, GET_NEXT_INSTANCE, and IDENTIFY_PROGRAM return the location of the program to the caller. These locations will change, the CDSA will become the PCDSA, the ECDSA will become the EPCDSA, the SDSA will become the PUDSA and the ESDSA will become the EPUDSA. Although the names of the DSA equated have changed, the equate values have not changed.

Changes to toggle-enabled features

Table 42. Changes to toggle-enabled features in CICS TS 6.1	
Feature toggle	**6.1**
com.ibm.cics.resourceoverrides.file={*name*.yaml}	**REMOVED:** Replaced by RESOVERRIDES system initialization parameter. See RESOVERRIDES system initialization parameter.
com.ibm.cics.db2.origindata={true|false}	Service **NEW (APAR PH52668):** Gives you the option to disable the passing of adapter origin data to Db2 for adapter tracking.
com.ibm.cics.db2.sharelocks={true|false}	**REMOVED:** Replaced by DB2ENTRY attribute SHARELOCKS.
com.ibm.cics.ds.freeussprocesses={true|false}	Service **NEW (APAR PH56193):** Handling of USS processes. Intended for use only under guidance from IBM service personnel.
com.ibm.cics.container.hash={true|false}	**REMOVED:** Hashing always used.
com.ibm.cics.cpsm.bas.largecicsplex={true|false}	**CHANGED:** The default is changed from true to false.
com.ibm.cics.cpsm.wlm.surgeresist={true|false}	**NEW:** When applied to CICSPlex SM WLM routing regions, this feature toggle takes effect for the QUEUE and GOAL WLM algorithms when using CICSPlex SM sysplex optimized workload routing. It has no effect when applied to target regions. When the feature toggle is set to true, surges of extremely high frequency, short duration transactions can be mitigated by reducing the likelihood that recently selected target regions are reselected. Enabling this feature toggle increases the average routing cost per transaction, but restores the routing behavior of CICSPlex SM at CICS TS 5.6 before APAR PH30768 is applied. See “Changes to CICSPlex SM sysplex optimized workload routing behavior” on page 55.
com.ibm.cics.sm.iep={true|false}	**NEW:** Enables instruction execution protection for certain CICS DSAs. See Instruction execution protection.
com.ibm.cics.tls.minimumkeystrength={1024|2048}	Service **NEW (APAR PH51719):** Sets the minimum key size allowed during TLS handshakes.
com.ibm.cics.web.defaultcipherfile={true|false}	• **NEW:** Use defaultciphers.xml as a default set of ciphers for outbound web requests. See Default cipher file for outbound web requests. • Service **CHANGED (APAR PH60212):** Extended to apply to URIMAP resources with no ciphers specified.
com.ibm.cics.web.hsts.includesubdomains.*TCPIPS*={true|false}	Service **NEW (APAR PH55370):** Controls whether to extend HTTP strict transport security (HSTS) to sub-domains of the specified TCPIPSERVICE.
com.ibm.cics.web.hsts.max-age.*TCPIPS*={*seconds*|-1}	Service **NEW (APAR PH55370):** Sets HSTS for an individual TCPIPSERVICE to override the region wide setting.
com.ibm.cics.web.hsts.includesubdomains={true|false}	Service **NEW (APAR PH55370):** Controls whether to extend HSTS to the sub-domains of the CICS server.
com.ibm.cics.web.hsts.max-age=*seconds*	Service **NEW (APAR PH55370):** Activates and sets HSTS for a CICS region.

Changes to resource definitions

Table 43. Changes to resource definitions in CICS TS 6.1	
Resource	**6.1**
URIMAP	**CHANGED:** Added support for enabling multiple client URIMAPs that point to the same endpoint (that is, the same host, port and path) in a CICS region.
DFHWSATH, DFHWSATR, DFHWSATX and DFHPIRS program definitions	**CHANGED:** These program definitions are moved from group DFHWSAT to group DFHPIPE. You no longer need to install your own versions of these program definitions because DFHPIPE is part of DFHLIST.
URIMAP definition DFHRSURI	**CHANGED:** URIMAP DFHRSURI now specifies TRANSCTION(CPIW) instead of CPIH. If you are using a customized version of DFHRSURI that no longer specifies TRANSACTION(CPIH), no action is needed and you can continue to use your customized DFHRSURI unchanged. However, if the CSD is being shared with a back level region, see Changes to resource definitions to determine if any action is necessary.

Changes to CICS transactions

Table 44. Changes to CICStransactions in CICS TS 6.1	
Transaction	**6.1**
CDBT	**CHANGED:** The SPURGE attribute has been changed from SPURGE(NO) to SPURGE(YES).
CEPD	**CHANGED:** Enhanced to generate an SMF type 110 subtype 1 CICS monitoring record every 2000 events processed by CEPD tasks in the region.
CJSA	**CHANGED:** The SHUTDOWN attribute has been changed from SHUTDOWN(DISABLED) to SHUTDOWN(ENABLED).
CJSU	**CHANGED:** The SHUTDOWN attribute has been changed from SHUTDOWN(DISABLED) to SHUTDOWN(ENABLED).
CLGR	**NEW:** Category 1 transaction for automatic recovery of CICS user journals.
CPIW	**NEW:** Category 2 transaction to handle WS-AT protocol messages. It is a direct clone of CPIH. URIMAP DFHRSURI now specifies TRANSCTION(CPIW) instead of CPIH.
CSGM	**CHANGED:** Moved from a category 2 to a category 3 transaction to match CESL and CESN.

Changes to CEMT

Table 45. Changes to CEMT in CICS TS 6.1	
Command	**6.1**
CEMT INQUIRE DB2ENTRY	**CHANGED:** New option SHARELOCKS indicates whether CICS will pass an XID to Db2 to allow Db2 to share locks with any other thread that passes the same XID.
CEMT INQUIRE DSAS	**CHANGED:** New options PCDSASIZE, PUDSASIZE, EPCDSASIZE, EPUDSASIZE in support of Instruction Execution Protection. ETDSASIZE is removed.

Table 45. Changes to CEMT in CICS TS 6.1 (continued)	
Command	**6.1**
CEMT INQUIRE SYSTEM	**CHANGED:** New option SDTMEMLIMIT that shows the maximum amount of storage above the bar that CICS makes available for shared data tables to use for control information (entry descriptors, backout elements, and index nodes). **CHANGED:** New option SRRTASKS to show number of security request recordings. **CHANGED:** New option HEALTHCHECK to indicate if health checks are excluded as part of the CICS region tagging capability.
CEMT INQUIRE TASK	**CHANGED:** New option SRRSTATUS with values of SRRACTIVE and SRRINACTIVE to show the security request recording status of active or inactive.
CEMT SET DB2ENTRY	**CHANGED:** New option SHARELOCKS sets whether CICS will pass an XID to Db2 to allow Db2 to share locks with any other thread that passes the same XID.
CEMT SET DSAS	**CHANGED:** The DSAs that are covered by DSALIMIT and EDSALIMIT include the new DSAs that are never protected from instruction execution. ETDSA is removed so no longer included.
CEMT SET SYSTEM	**CHANGED:** New option SDTMEMLIMIT to set the maximum amount of storage above the bar that CICS makes available for shared data tables to use for control information (entry descriptors, backout elements, and index nodes).
CEMT SET TASK	**CHANGED:** New option SRRSTATUS with values of SRRACTIVE and SRRINACTIVE to set security request recording status to active or inactive.

Changes to CICS SPI

Table 46. Changes to the system programming interface commands in CICS TS 6.1	
Command	**6.1**
CREATE DB2ENTRY	**CHANGED:** New option SHARELOCKS to enable CICS to pass an XID to Db2 and instruct Db2 to share locks between threads that pass the same XID.
ENABLE PROGRAM	**CHANGED:** New options GAEXECUTABLE and TAEXECUTABLE are in support of Instruction Execution Protection.
EXTRACT STATISTICS	**CHANGED:** New option POLICY combined with new option POLICYRULE to obtain statistics about a policy rule that is contained in a POLICY resource.
INQUIRE ASSOCIATION	**CHANGED:** Enhanced support for Liberty. The association data user ID value now reflects the final user ID value used in secure Liberty transactions, instead of the initial user ID.
INQUIRE DB2ENTRY	**CHANGED:** New option SHARELOCKS, indicating whether CICS will pass an XID to Db2 to allow Db2 to share locks with any other thread that passes the same XID.

Table 46. Changes to the system programming interface commands in CICS TS 6.1 (continued)	
Command	**6.1**
INQUIRE FEATUREKEY	**CHANGED:** New option FILEPATH to show the path to the feature toggle configuration file that defines a feature toggle setting that is in effect in the CICS region.
INQUIRE SECRECORDING	**NEW:** New option to inquire on security data for compliance, configuration, and diagnosis.
INQUIRE POLICY	**NEW:** To retrieve information about an installed POLICY, or browse through all installed POLICY resources in the region.
INQUIRE POLICYRULE	**NEW:** To retrieve information about an installed policy rule, or browse through all installed rules contained in a policy.
INQUIRE STORAGE	**CHANGED:** New values PCSDSA, EPCDSA, PUDSA, and EPUDSA on the DSANAME option, in support of Instruction Execution Protection.
INQUIRE STORAGE64	**NEW:** To retrieve information about 64-bit task storage.
INQUIRE SUBPOOL	**CHANGED:** New values PCSDSA, EPCDSA, PUDSA, and EPUDSA on the DSANAME option, in support of Instruction Execution Protection. ETDSA is removed.
INQUIRE SYSTEM	**CHANGED:** New options HEALTHCHECK, EPCDSA, EPUDSA,PCSDSA, PUDSA, SRRTASKS, and SDTMEMLIMIT. ETDSA is removed.
INQUIRE TAG	**NEW:** To inquire on CICS region tags applied to the running region.
INQUIRE TASK	**CHANGED:** New SRRSTATUS option to show the security request recording status of SRRACTIVE or SRRINACTIVE.
PERFORM JVMSERVER	**CHANGED:** • New cvda value STACKTRACE supported for JVMACTION option to allow a stacktrace to be taken for a task running in a JVM server. • New option TASKID to specify the sequence number of the task to take a stacktrace of.
SET ASSOCIATION USERCORRDATA	**NEW:** To overwrite the user correlator data (USERCORRDATA field) of the originating task.
SET DB2ENTRY	**CHANGED:** New option SHARELOCKS to enable CICS to pass an XID to Db2 and instruct Db2 to share locks between threads that pass the same XID. New INVREQ RESP2 value of 20, indicating that an invalid SHARELOCKS value was specified.
SET SECRECORDING	**NEW:** New option to inquire on security data for compliance, configuration, and diagnosis.
SET SYSTEM	**CHANGED:** New option SDTMEMLIMIT to set the maximum amount of storage above the bar that CICS makes available for shared data tables to use for control information (entry descriptors, backout elements, and index nodes).
SET TAGS REFRESH	**NEW:** To refresh CICS region tags applied to the running region.
SET TASK	**CHANGED:** New SRRSTATUS option to set the security request recording status to SRRACTIVE or SRRINACTIVE.

Table 46. Changes to the system programming interface commands in CICS TS 6.1 (continued)	
Command	**6.1**
SET XMLTRANSFORM	**CHANGED:** New INVREQ RESP2 value of 8, indicating that the XML schema file for the XMLTRANSFORM cannot be found.

Changes to JVM profiles

Table 47. Changes to JVM profiles in CICS TS 6.1	
JVM profile	**6.1**
`EYUCMCIJ.jvmprofile`	**CHANGED:** The supplied sample profile for a CMCI JVM server in a WUI region is changed to add `-Dcom.ibm.ws.zos.core.angelRequiredServices=SAFCRED,PRODMGR,ZOSAIO`.
`EYUSMSSJ.jvmprofile`	**NEW:** A new supplied sample profile for a CMCI JVM server in a single CICS region. This new supplied sample profile for a CMCI JVM server in a single CICS region also has the `angelRequiredServices` property set as follows: `-Dcom.ibm.ws.zos.core.angelRequiredServices=SAFCRED,PRODMGR,ZOSAIO`.

Changes to CICS utilities

Table 48. Changes to CICS utilities in CICS TS 6.1	
Utility	**6.1**
DFH0STAT	**NEW REPORT:** Policy report
DFH0STAT	**Data Tables Storage report** **New fields:** Entries + Index - Storage Allocated Entries + Index - Storage In-Use **Removed fields:** Total - Storage Allocated Total - Storage In-Use
DFH0STAT	**Db2 Entries report** **New field:** DB2Entry Share Locks

Table 48. Changes to CICS utilities in CICS TS 6.1 (continued)	
Utility	**6.1**
DFH0STAT	**JVMSERVERs report** **New fields:** JVMSERVER code cache memory used JVMSERVER code cache memory alloc JVMSERVER data cache memory used JVMSERVER data cache memory alloc JVMSERVER class storage memory used JVMSERVER class storage memory alloc JVMSERVER classcache size JVMSERVER classcache free
DFH0STAT	**Storage below 16 MB (24-bit storage) report** **New fields:** User Region limit established Current User Region storage unallocated Current free storage above User Region limit **Changed fields:** Private Area size below 16MB: the field name is changed from Private Area Region size below 16MB. Peak LSQA/SWA storage allocated (SYS): the field name is changed from Max LSQA/SWA storage allocated below 16MB (SYS) and its field description is updated accordingly. Peak User Region storage allocated (VIRT): the field name is changed from Max User storage allocated below 16MB (VIRT) and its field description is updated accordingly. **Removed fields:** Private Area Storage available below 16MB Region size established from REGION= parameter RTM System Use

Table 48. Changes to CICS utilities in CICS TS 6.1 (continued)	
Utility	**6.1**
DFH0STAT	**Storage above 16 MB (31-bit storage) report** **New fields:** User Region limit established Current User Region storage unallocated Current free storage above User Region limit **Changed fields:** Private Area size above 16MB: the field name is changed from Private Area Region size above 16MB Peak LSQA/SWA storage allocated (SYS): the field name is changed from Max LSQA/SWA storage allocated above 16MB (SYS) and its field description is updated accordingly. Peak User Region storage allocated (EXT): the field name is changed from Max User storage allocated above 16MB (EXT) and its field description is updated accordingly. **Removed fields:** Private Area Storage available above 16MB
DFH0STAT	**Storage above 2 GB (64-bit storage) report** **Removed fields:** MEMLIMIT minus allocated to Private Memory Objects MEMLIMIT minus usable within Private Memory Objects

Table 48. Changes to CICS utilities in CICS TS 6.1 (continued)	
Utility	**6.1**
DFH0STAT	**TCP/IP report** **New fields:** Maximum parallel TLS handshakes Current parallel TLS handshakes Peak parallel TLS handshakes Maximum waiting TLS handshakes Current waiting TLS handshakes Peak waiting TLS handshakes Inbound: TLS 1.1 Inbound: TLS 1.2 Inbound: TLS 1.3 Inbound: Total Outbound: TLS 1.1 Outbound: TLS 1.2 Outbound: TLS 1.3 Outbound: Total Inbound: AT-TLS SSL 3 Inbound: AT-TLS 1.0 Inbound: AT-TLS 1.1 Inbound: AT-TLS 1.2 Inbound: AT-TLS 1.3 Outbound: AT-TLS SSL 3 Outbound: AT-TLS 1.0 Outbound: AT-TLS 1.1 Outbound: AT-TLS 1.2 Outbound: AT-TLS 1.3 **Changed fields:** Current number of outbound sockets: Its source field is changed to SOG-CURR-OUTB-SOCKETS. Peak number of outbound sockets: Its source field is changed to SOG-PEAK-OUTB-SOCKETS. **Removed fields:** SOG-CURR-PERS-OUTB-SOCKETS SOG-PEAK-BOTH-OUTB-SOCKETS SOG-PEAK-PERS-OUTB-SOCKETS SOG-PERS-OUTBOUND-CREATED
DFH0STAT	**Temporary Storage report** **New fields:** Current auxiliary storage usage % Peak auxiliary storage usage %
DFH0STAT	**Transaction Classes report** **New field:** Last At Max Act

Table 48. Changes to CICS utilities in CICS TS 6.1 (continued)	
Utility	**6.1**
DFHEISUP	**CHANGED:** DFHEISUP, Load module scanner is changed to be RMODE(ANY) instead of RMODE(24). This change allows DFHEISUP to use 31-bit virtual storage (above 16 MB but below 2 GB).
DFHSTUP	**CICS Db2 resource statistics** **New field:** D2R_SHARELOCKS
DFHSTUP	**Cipher statistics** **New fields:** Number, which indicates the cipher code TLS Inbound TLS Outbound AT-TLS Inbound AT-TLS Outbound
DFHSTUP	**JVMSERVER resource statistics** **New fields:** JVMSERVER code cache memory used JVMSERVER code cache memory alloc JVMSERVER data cache memory used JVMSERVER data cache memory alloc JVMSERVER class storage mem used JVMSERVER class storage mem alloc JVMSERVER classcache size JVMSERVER classcache free

Table 48. Changes to CICS utilities in CICS TS 6.1 (continued)	
Utility	**6.1**
DFHSTUP	**TCP/IP global statistics** **New fields:** Maximum parallel TLS handshakes Current parallel TLS handshakes Peak parallel TLS handshakes Maximum waiting TLS handshakes Current waiting TLS handshakes Peak waiting TLS handshakes **New fields showing TLS protocol handshakes:** Inbound: TLS 1.1 Inbound: TLS 1.2 Inbound: TLS 1.3 Inbound: Total Outbound: TLS 1.1 Outbound: TLS 1.2 Outbound: TLS 1.3 Outbound: Total Inbound: AT-TLS SSL 3 Inbound: AT-TLS 1.0 Inbound: AT-TLS 1.1 Inbound: AT-TLS 1.2 Inbound: AT-TLS 1.3 Outbound: AT-TLS SSL 3 Outbound: AT-TLS 1.0 Outbound: AT-TLS 1.1 Outbound: AT-TLS 1.2 Outbound: AT-TLS 1.3 Inbound: Full Inbound: Abbreviated Outbound: Full Outbound: Abbreviated **Changed fields:** SOG_CURR_OUTB_SOCKETS: Its DFHSTUP name is changed to **Current number of outbound sockets**. SOG_PEAK_OUTB_SOCKETS: Its DFHSTUP name is changed to **Peak number of outbound sockets**. **Removed fields:** SOG_CURR_PERS_OUTB_SOCKETS SOG_PEAK_BOTH_OUTB_SOCKETS SOG_PEAK_PERS_OUTB_SOCKETS SOG_PERS_OUTBOUND_CREATED

Table 48. Changes to CICS utilities in CICS TS 6.1 (continued)	
Utility	**6.1**
DFHSTUP	**Temporary storage global statistics** **New fields:** Current aux. temp storage usage % Peak aux. temp storage usage %
DFHSTUP	**Transaction class resource statistics** **New fields:** First at Max Act Last at Max Act

Changes to GLUEs and TRUEs

Table 49. Changes to global user exits and task-related user exits in CICS TS 6.1	
Exit	**6.1**
XSNEX	**REMOVED**

Changes to XPI functions

Table 50. Changes to XPI functions in CICS TS 6.1	
Command	**6.1**
Parameter domain (INQUIRE_FEATUREKEY)	**CHANGED:** New option FILEPATH.
Program management The INQUIRE_PROGRAM call	**CHANGED**: DFHPGISY LOCATION equates that can be used on INQUIRE_PROGRAM calls: PGIS_CDSA, PGIS_SDSA, PGIS_ECDSA and PGIS_ESDSA are replaced by PGIS_PCDSA, PGIS_PUDSA, PGIS_EPCDSA and PGIS_EPUDSA.
Program management The GET_NEXT_PROGRAM call	**CHANGED**: DFHPGISY LOCATION equates that can be used on GET_NEXT_PROGRAM calls: PGIS_CDSA, PGIS_SDSA, PGIS_ECDSA and PGIS_ESDSA are replaced by PGIS_PCDSA, PGIS_PUDSA, PGIS_EPCDSA and PGIS_EPUDSA.
Storage management (GETMAIN)	**NEW:** EXECUTABLE option in support of Instruction Execution Protection.
Storage management (INQUIRE_ELEMENT_LENGTH)	**NEW:** ADDRESS64, ELEMENT_ADDRESS64, and ELEMENT_LENGTH64 options.
Storage management (INQUIRE_TASK_STORAGE64)	**NEW:** New XPI call to request details of all elements of task-lifetime 64-bit storage belonging to a task.

Changes to user-replaceable programs

No changes in CICS TS 6.1.

Changes to control tables

No changes in CICS TS 6.1.

Changes to event processing adapters and formats

No changes in CICS TS 6.1.

Changes to installation and definition of CICSPlex SM

- The record size of EYUHIST* data sets has increased from RECORDSIZE(3680 3684) to RECORDSIZE(3748 3752). The EYUJHIST sample has been updated to reflect this change.

Changes to configuration and initialization of CICSPlex SM

Table 51. Changes to CICSPlex SM system parameters (EYUPARM) in CICS TS 6.1

EYUPARM parameter	**6.1**
	No changes in CICS TS 6.1.

Table 52. Changes to CICSPlex SM WUI server initialization parameters (WUIPARM) in CICS TS 6.1

WUIPARM parameter	**6.1**
TCPIPHOSTNAME	Service **DEPRECATED (APAR PH48544):** The hostname of the WUI server is the name of the host where the WUI is executing. It is no longer set by the **TCPIPHOSTNAME** WUI initialization parameter. The WUI uses relative URLs, and not embedded host names. **TCPIPHOSTNAME** is still required, but the value is ignored. This parameter is retrained for compatibility and will be removed in a later release.
TCPIPHTTPHOST	Service **DEPRECATED (APAR PH48544):** The hostname of the WUI server is the name of the host where the WUI is executing. The WUI uses relative URLs, and not embedded host names. If a value is specified on **TCPIPHTTPHOST**, it is ignored. This parameter is retrained for compatibility and will be removed in a later release.

Table 53. Changes to CMCI in CICS TS 6.1

Change	**6.1**
Enhancements to the CMCI GraphQL API	**CHANGED:** Added support for the following resources: • CSDINLST • SECREC • SYSTAG

Changes to CICSPlex SM behavior and operation

Table 54. Changes to CICSPlex SM behavior and operation in CICS TS 6.1	
CICSPlex SM feature	**6.1**
CICSPlex SM workload management	**CHANGED:** • CICSPlex SM workload management factors z/OS MVS SOS conditions into its routing algorithm, in the same way as it does for CICS-managed storage SOS conditions. • The default behavior of CICSPlex SM workload management routing algorithms has been updated to increase the likelihood that work is routed to healthy, local target regions. This change applies only to the QUEUE and GOAL algorithms, not to the link neutral variants (LNQUEUE and LNGOAL). See "Changes to CICSPlex SM sysplex optimized workload routing behavior" on page 55 for details.

Changes to CICSPlex SM resource tables

Enhancements to CICSPlex SM resource tables are typically populated to related CICSPlex SM views. In Table 55 on page 81, where applicable, the changed CICSPlex SM views are also listed.

Table 55. Changes to the resource tables provided by CICSPlex SM in CICS TS 6.1		
Resource table	**Related view**	**6.1**
CICSRGN	CICS region (CICSRGN) view	**CHANGED:** New resource table attribute SDTMEMLIMIT
DB2EDEF	DB2® entry definition (DB2EDEF) view	**CHANGED:** New resource table attribute SHARELOCKS
DB2ENTRY	DB2 entries (DB2ENTRY) view	**CHANGED:** New resource table attribute SHARELOCKS
DSNAME	Physical data sets for files (DSNAME) view	**REMOVED** actions: QUIESE is replaced by QUIESCE. UNQUIESE is replaced by UNQUIESCE. IMMQUIESE is replaced by IMMQUIESCE.
EMASSICK EMASWELL EMSTATUS	Not applicable	**CHANGED:** New values SOSMVS24, SOSMVS31 and SOSMVS64 added to SICKTYPE output valid values New resource table attributes SOSMVS24_TIM, SOSMVS31_TIM and SOSMVS64_TIM
FEATURE	Not applicable	**CHANGED:** New resource table attribute FILEPATH

Table 55. Changes to the resource tables provided by CICSPlex SM in CICS TS 6.1 (continued)		
Resource table	**Related view**	**6.1**
RULE	Not applicable	**CHANGED:** • New values transactionDump and containerstorage added to RULETYPE field. • Attributes COUNT and TIME are changed to indicate the values since the region started instead of within the current statistics interval. • New resource table attributes COUNTSTAT and TIMESTAT are added to indicate the values within the current statistics interval.
SECREC	Not applicable	**NEW:** Resource table for CICS security request recording data
TCPIPGBL	Not applicable	**DEPRECATED:** The following attributes are deprecated in CICS TS 6.1 but are retained for compatibility with earlier CICS releases: SOG_CURR_PERS_OUTB_SOCKETS SOG_PEAK_BOTH_OUTB_SOCKETS SOG_PEAK_PERS_OUTB_SOCKETS SOG_PERS_OUTBOUND_CREATED
TRANCLAS	Transaction class (TRANCLAS) view	**CHANGED:** New resource table attribute LASTATMAX

Changes to CICS monitoring

Table 56. Changes to monitoring data in CICS TS 6.1	
Data	**6.1**
Exception class data	**CHANGED:** New exception resource type DSWC, which has the following possible EXCMNRID values: • S8TLSHS: The maximum number of concurrent TLS handshakes has been reached. • XSPSWVFY: The maximum concurrent calls to RACF in the region has been reached. New exception resource type CONTAINR, which means that the threshold of a container storage policy task rule has been exceeded. New exception resource type TRANDUMP, which means that the threshold of a transaction dump threshold policy system rule has been exceeded.

Table 56. Changes to monitoring data in CICS TS 6.1 (continued)	
Data	**6.1**
Performance data in group DFHCICS	**CHANGED:** Enhanced to provide association data of DPL requests by EXCI clients. If a task was initiated by an EXCI client, in the performance record of the DPL request, field 374 (PHAPPLID) contains the EXCI job name, field 378 (PHCOUNT) contains a value of 1, and field 376 (PHTRANNO) has a value of 0. The data is populated to transaction resource class data and identity class data. Field 089 (USERID) is changed for Liberty such that the user ID value now reflects the final user ID value used in secure Liberty transactions, instead of the initial user ID.
Performance data in group DFHSOCK	**CHANGED:** **NEW FIELDS:** • 457 SOTLSLVL is available to identify the TLS level selected during the initial handshake for use on the inbound connection. • 458 SOFLAG is available to identify the socket flags, a string of 32 bits used for socket status information. **CHANGED FIELDS:** • 290 SOCNPSCT is clarified as a data field that indicates the total number of requests made by the user task to create an outbound socket. • 292 SONPSHWM is clarified as a data field that indicates the peak number of outbound sockets owned by the user task. **REMOVED FIELDS:** • 291 SOCPSCT • 293 SOPSHWM
Transaction resource class data: Listing of data fields	**CHANGED:** New URIMAP entry field MNR_URIMAP_TLSLVL is available to identify the TLS level selected during the initial handshake for use on an outbound connection. New URIMAP entry field MNR_URIMAP_FLAG is available to identify whether CICS-configured or AT-TLS was used for the outbound connection.

Changes to statistics

Table 57. Changes to statistics in CICS TS 6.1	
Statistics	**6.1**
CICS Db2	**NEW FIELD:** D2R_SHARELOCKS, with DFHSTUP name **Share Locks**, added to CICS Db2 resource statistics, indicating whether CICS will pass an XID to Db2 to allow Db2 to share locks with any other thread that passes the same XID.
Ciphers	**NEW FIELDS** showing the ciphers in use: SOC_CIPHER, with DFHSTUP name **Number**, indicating the cipher code SOC_TIMES_CICS_INB_USED, with DFHSTUP name **TLS Inbound** SOC_TIMES_CICS_OUTB_USED, with DFHSTUP name **TLS Outbound** SOC_TIMES_ATTLS_INB_USED, with DFHSTUP name **AT-TLS Inbound** SOC_TIMES_ATTLS_OUTB_USED, with DFHSTUP name **AT-TLS Outbound**

Table 57. Changes to statistics in CICS TS 6.1 (continued)	
Statistics	**6.1**
JVMSERVER	**NEW FIELDS** showing the memory currently used and allocated to the JIT code cache memory pool: SJS_JVMSERVER_CODE_CACHE_USED, with DFHSTUP name **JVMSERVER code cache memory used** SJS_JVMSERVER_CODE_CACHE_ALLOC, with DFHSTUP name **JVMSERVER code cache memory alloc** **NEW FIELDS** showing the memory currently used and allocated to the JIT data cache: SJS_JVMSERVER_DATA_CACHE_USED, with DFHSTUP name **JVMSERVER data cache memory used** SJS_JVMSERVER_DATA_CACHE_ALLOC, with DFHSTUP name **JVMSERVER data cache memory alloc** **NEW FIELDS** showing the memory currently used and allocated to the JVM class storage memory pool: SJS_JVMSERVER_CLASS_STRG_USED, with DFHSTUP name **JVMSERVER class storage mem used** SJS_JVMSERVER_CLASS_STRG_ALLOC, with DFHSTUP name **JVMSERVER class storage mem alloc** **NEW FIELDS** showing the size limit and current free space of the JVM's shared class cache: SJS_JVMSERVER_CLASSCACHE_SIZE, with DFHSTUP name **JVMSERVER classcache size** SJS_JVMSERVER_CLASSCACHE_FREE, with DFHSTUP name **JVMSERVER classcache free**
TCP/IP domain	**NEW FIELDS** added to TCP/IP global statistics, showing the maximum, current and peak numbers of TLS handshakes running in parallel: SOG_S8TLSHS_REQUESTS_MAX, with DFHSTUP name **Maximum parallel TLS handshakes** SOG_S8TLSHS_REQUESTS_CUR, with DFHSTUP name **Current parallel TLS handshakes** SOG_S8TLSHS_REQUESTS_PEAK, with DFHSTUP name **Peak parallel TLS handshakes**
TCP/IP domain	**NEW FIELDS** added to TCP/IP global statistics, showing the maximum, current and peak numbers of TLS handshakes in waiting: SOG_S8TLSHS_WAITERS_MAX, with DFHSTUP name **Maximum waiting TLS handshakes** SOG_S8TLSHS_WAITERS_CUR, with DFHSTUP name **Current waiting TLS handshakes** SOG_S8TLSHS_WAITERS_PEAK, with DFHSTUP name **Peak waiting TLS handshakes**

Table 57. Changes to statistics in CICS TS 6.1 (continued)	
Statistics	**6.1**
TCP/IP domain	**NEW FIELDS** added to TCP/IP global statistics, showing the total number of established inbound connections that have used CICS configured TLS protocol during the interval through, which can come from TCPIPSERVICE with SSL(YES) or SSL(CLIENTAUTH): SOG_TIMES_CICSTLS11_INB_USED, with DFHSTUP name **Inbound: TLS 1.1** SOG_TIMES_CICSTLS12_INB_USED, with DFHSTUP name **Inbound: TLS 1.2** SOG_TIMES_CICSTLS13_INB_USED, with DFHSTUP name **Inbound: TLS 1.3** SOG_TIMES_CICSTLSALL_INB_USED, with DFHSTUP name **Inbound: Total**
TCP/IP domain	**NEW FIELDS** added to TCP/IP global statistics, showing the total number of established outbound connections that have used CICS configured TLS protocol during the interval, which can come from URIMAP with USAGE(CLIENT) SCHEME(HTTPS) or WEB OPEN SCHEME(HTTPS): SOG_TIMES_CICSTLS11_OUTB_USED, with DFHSTUP name **Outbound: TLS 1.1** SOG_TIMES_CICSTLS12_OUTB_USED, with DFHSTUP name **Outbound: TLS 1.2** SOG_TIMES_CICSTLS13_OUTB_USED, with DFHSTUP name **Outbound: TLS 1.3** SOG_TIMES_CICSTLSALL_OUTB_USED, with DFHSTUP name **Outbound: Total**
TCP/IP domain	**NEW FIELDS** added to TCP/IP global statistics, showing the total number of established inbound connections that have used AT-TLS protocol during the interval, which can come from TCPIPSERVICE with SSL(ATTLSAWARE) or SSL(NO): SOG_TIMES_ATSSL3_INB_USED, with DFHSTUP name **Inbound: AT-TLS SSL 3** SOG_TIMES_ATTLS10_INB_USED, with DFHSTUP name **Inbound: AT-TLS 1.0** SOG_TIMES_ATTLS11_INB_USED, with DFHSTUP name **Inbound: AT-TLS 1.1** SOG_TIMES_ATTLS12_INB_USED, with DFHSTUP name **Inbound: AT-TLS 1.2** SOG_TIMES_ATTLS13_INB_USED, with DFHSTUP name **Inbound: AT-TLS 1.3**
TCP/IP domain	**NEW FIELDS** added to TCP/IP global statistics, showing the total number of established outbound connections that have used AT-TLS protocol during the interval, which can come from URIMAP with USAGE(CLIENT) SCHEME(HTTP) or WEB OPEN SCHEME(HTTP): SOG_TIMES_ATSSL3_OUTB_USED, with DFHSTUP name **Outbound: AT-TLS SSL 3** SOG_TIMES_ATTLS10_OUTB_USED, with DFHSTUP name **Outbound: AT-TLS 1.0** SOG_TIMES_ATTLS11_OUTB_USED, with DFHSTUP name **Outbound: AT-TLS 1.1** SOG_TIMES_ATTLS12_OUTB_USED, with DFHSTUP name **Outbound: AT-TLS 1.2** SOG_TIMES_ATTLS13_OUTB_USED, with DFHSTUP name **Outbound: AT-TLS 1.3**

Table 57. Changes to statistics in CICS TS 6.1 (continued)	
Statistics	**6.1**
TCP/IP domain	**NEW FIELDS** added to TCP/IP global statistics, showing the total number of CICS-configured TLS full and abbreviated handshakes for inbound and outbound connections: SOG_HANDSHAKES_FULL_INB, with DFHSTUP name **Inbound: Full** SOG_HANDSHAKES_ABBREV_INB, with DFHSTUP name **Inbound: Abbreviated** SOG_HANDSHAKES_FULL_OUTB, with DFHSTUP name **Outbound: Full** SOG_HANDSHAKES_ABBREV_OUTB, with DFHSTUP name **Outbound: Abbreviated**
TCP/IP domain	**CHANGED FIELDS:** The following fields in TCP/IP global statistics have their DFHSTUP names changed to clarify their use: SOG_CURR_OUTB_SOCKETS - its DFHSTUP name is changed to **Current number of outbound sockets**. SOG_PEAK_OUTB_SOCKETS - its DFHSTUP name is changed to **Peak number of outbound sockets**.
TCP/IP domain	**REMOVED FIELDS:** The following fields have been removed from TCP/IP global statistics: SOG_CURR_PERS_OUTB_SOCKETS SOG_PEAK_BOTH_OUTB_SOCKETS SOG_PEAK_PERS_OUTB_SOCKETS SOG_PERS_OUTBOUND_CREATED
Temporary storage	**NEW FIELDS** added to Temporary storage global statistics, showing the current and peak percentage of auxiliary temporary storage being used: TSGASU, with DFHSTUP name **Current aux. temp storage usage %** TSGASUPK, with DFHSTUP name **Peak aux. temp storage usage %**
Transaction class	**NEW FIELD** showing the last time in UTC, in store clock (STCK) value, that the transaction class has reached its maximum number of transactions that are allowed to be active. XMCGAMA, with DFHSTUP name **Last At MaxAct**

Changes to CICS messages

DFHnnnn

Removed:

- DFH7040
- DFH7049
- DFH7051
- DFH7052
- DFH7056
- DFH7062
- DFH7064
- DFH7068 through DFH7073

- DFH7079
- DFH7081
- DFH7087
- DFH7088
- DFH7090 through DFH7098
- DFH7202
- DFH7203
- DFH7211
- DFH7212
- DFH7214
- DFH7223
- DFH7224
- DFH7227
- DFH7231
- DFH7234
- DFH7236
- DFH7265
- DFH7266

DFHAMnnnn

New:

- DFHAM4968I indicates that one or more attributes of a resource were overridden.
- DFHAM4969E indicates that a resource failed to install because overrides resulted in an invalid resource definition.
- DFHAM4970I indicates that an override was applied to a resource definition attribute.
- DFHAM4971E indicates that resource overrides applied during GRPLIST installation resulted in invalid resource definitions.
- DFHAM4972E indicates that a resource override action is not valid because an attribute is null.
- DFHAM4973E indicates that a resource override action makes an attribute too long.
- DFHAM4990E indicates the deletion of a resource definition failed because it is a protected definition.

DFHAPnnnn

New:

- DFHAP2001 identifies a copy member required for a PLT which was not located.
- DFHAP0007E indicates a mismatch in Instruction Execution Protection settings between CICS and LE.

DFHCAnnnn

New:

- DFHCA4968I indicates that one or more attributes of a resource were overridden.
- DFHCA4969E indicates that a resource failed to install because overrides resulted in an invalid resource definition.
- DFHCA4970I indicates that an override was applied to a resource attribute.
- DFHCA4972E indicates that a resource override action is not valid because an attribute is null.
- DFHCA4973E indicates that a resource override action makes an attribute too long.

DFHDUnnnn

New:

- DFHDU0104 indicates that a dumpcode has been added.
- DFHDU0105 indicates that a dumpcode has been replaced.
- DFHDU0106 indicates that a dumpcode has been discarded.

DFHFCnnnn

New:

- DFHFC0418 indicates that initialization of shared data tables failed because an attempt was made to set SDTMEMLIMIT to a value greater than 40% of MEMLIMIT.
- DFHFC0433 indicates that the amount of above-the-bar storage used by Shared Data Tables has reached a certain percentage (75% or more) of the SDTMEMLIMIT storage.
- DFHFC0434 indicates that the amount of above-the-bar storage used by Shared Data Tables has fallen below 70% of the SDTMEMLIMIT storage.

DFHHCnnnn

New:

- DFHHC0104W indicates that the CICS Health Checker encountered an unexpected error.

DFHHnnnn

New:

- DFHH0004 indicates one or more region configuration parameters are not optimally set.
- DFHH0005 indicates one or more resource configuration parameters is not optimally set.
- DFHH0006 indicates one or more USS file access permission settings is not optimally set.
- DFHH0007 indicate one or more resource security related SIT parameters are not optimally set.
- DFHH0304 indicate all region configuration parameters are correctly set.
- DFHH0305 indicates all resource configuration parameters are correctly set.
- DFHH0306 indicates that all relevant USS files are correctly secured.
- DFHH0307 indicates that all resource security SIT parameters are correctly set.
- DFHH0401 indicates SEC=NO has been specified as a SIT parameter.
- DFHH0402 indicates XTRAN=NO has been specified as a SIT parameter.
- DFHH0403 indicates XUSER=NO has been specified as a SIT parameter.
- DFHH0404 indicates CONFDATA=SHOW has been specified.
- DFHH0405 indicates MINTLSLEVEL is too low.
- DFHH0406 indicates HTTPSERVERHDR or HTTPSUSRAGENT or both are set to YES.
- DFHH0407 indicates CWA (Common Work Area) storage is not CICS key.
- DFHH0409 indicates RESSEC has been set to ASIS.
- DFHH0410 indicates RACFSYNC has been set to NO.
- DFHH0411 indicates DFLTUSER or KERBEROSUSER is same as region userid.
- DFHH0412 indicates GMTRAN allows users access to the default screen.
- DFHH0413 indicates it is possible to revoke the REGION userid.
- DFHH0414 indicates XCMD=NO has been specified.
- DFHH0501 indicates the default user can run sensitive transactions.
- DFHH0502 indicates default URM DFHISAIP is being used with IPIC TCPIPSERVICEs.
- DFHH0503 indicates clones of one or more sensitive transactions are installed.
- DFHH0504 indicates AUTHENTICATE no or basic is used for non-SSL TCPIPSERVICES.
- DFHH0601 indicates unauthorized access to USSCONFIG is allowed.
- DFHH0602 indicates unauthorized access to JVMPROFILE is allowed.
- DFHH0603 indicates unauthorized access to bundle files is allowed.

- DFHH0701 indicates XPCT=NO has been specified.
- DFHH0702 indicates XDCT=NO has been specified.
- DFHH0703 indicates XDB2=NO has been specified and Db2 could be used.
- DFHH0704 indicates XJCT=NO has been specified.
- DFHH0705 indicates XPPT=NO has been specified
- DFHH0706 indicates XTST=NO has been specified.
- DFHH0707 indicates XFCT=NO has been specified.
- DFHH0708 indicates XHFS=NO and at least one URIMAP uses static data.

DFHISnnnn

New:

- Service DFHIS2013 (APAR PH53315) indicates the server APPLID that is used in a High Availability (HA) IPCONN connection.

DFHLGnnnn

New:

- DFHLG0515 indicates that the maximum number of attempts to recover CICS user journals has been reached.
- DFHLG0516 indicates that the current instance of CLGR failed to automatically recover CICS user journals.

DFHMPnnnn

Changed:

- DFHMP2006 is issued for a failed installation of a compound condition system rule.

DFHMQnnnn

New:

- DFHMQ0224E indicates that CKAM failed to link to DFHMQMNS.
- Service DFHMQ0797E (APAR PH47961) is issued when temporary storage queue DFHCKBR is required but its TSMODEL definition has not been defined or installed in the system.

Changed:

- DFHMQ0107I is enhanced to include the name of the MQMONITOR in the message text if an MQMONITOR is associated with the CKTI that has been requested to end.
- DFHMQ0129E is enhanced to include the name of the MQMONITOR in the message text if an MQMONITOR is associated with the CKTI that has been terminated because of an unrecoverable abend.
- DFHMQ0700I is enhanced to include the name of the MQMONITOR in the message text if an MQMONITOR is associated with the CICS-MQ bridge that is in the progress of initialization.
- DFHMQ0704E is enhanced to include the name of the MQMONITOR in the message text if an MQMONITOR is associated with the CICS-MQ bridge that issued the error for the call.
- DFHMQ0713I is enhanced to include the name of the MQMONITOR in the message text if an MQMONITOR is associated with the CICS-MQ bridge that has terminated normally.
- DFHMQ0750E is enhanced to include the name of the MQMONITOR in the message text if an MQMONITOR is associated with the CICS-MQ bridge that has terminated abnormally due to an unexpected condition.

DFHPAnnnn

New:

- DFHPA2001E indicates insufficient 64-bit storage to process resource overrides.

- DFHPA2002I indicates that the resource overrides file is being read.
- DFHPA2003E indicates that resource overrides file could not be found.
- DFHPA2004E indicates that the resource overrides file could not be opened.
- DFHPA2005E indicates that the resource overrides file could not be read.
- DFHPA2007E indicates that the USSCONFIG value cannot be determined.
- DFHPA2008E indicates that the resource overrides file is too large.
- DFHPA2009E indicates insufficient 31-bit storage to process resource overrides.
- DFHPA2011E indicates that the RESOVERIDES system initialization parameter specifies an invalid resource overrides file name

DFHPInnnn

New:

- DFHPI0518 indicates that the CICS pipeline manager trust handler, DFHPITC, fails to find the required credentials in a web service request.

DFHRLnnnn

New:

- Service DFHRL0137I (APAR PH58296) is issued when all GRPLIST defined BUNDLE resources have reached their target initial status.
- Service DFHRL0138W (APAR PH58296) is issued when one or more GRPLIST defined BUNDLE resources have failed to reach their target initial status.

Changed:

- DFHRL2013 is enhanced to report the name of the CMAS that DFHDPLOY is connected through.

DFHRMnnnn

New:

- DFHRM0240 indicates the local log name that is set during CICS initialization and sent to a remote system when CICS establishes an APPC or IRC connection.
- DFHRM0241 indicates a log name that has been set for an APPC or IRC connection.
- DFHRM0242 indicates a log name that has been deleted for an APPC or IRC connection.

DFHRVnnnn

New:

- DFHRV0002 indicates that a severe error (code X'code') occurred in a module.
- DFHRV1000E indicates that the resource overrides file failed to parse.
- DFHRV1001W indicates that an override rule is for an obsolete resource type.
- DFHRV1002E indicates that an override rule specifies an invalid resource name.
- DFHRV1003E indicates that an override rule specifies an invalid attribute.
- DFHRV1004E indicates that an override rule specifies an invalid attribute value.
- DFHRV1005E indicates that an override rule specifies an invalid value for an integer attribute.
- DFHRV1006E indicates that an override rule specifies an integer attribute value outside its valid range.
- DFHRV1007E indicates that an override rule specifies an invalid CVDA attribute value.
- DFHRV1008E indicates that an override rule specifies an invalid override action.
- DFHRV1009E indicates that an override rule specifies an unsupported resource type.
- DFHRV1010E indicates that an override rule specifies an invalid symbol format in the attribute value.

- DFHRV1011E indicates that an override rule specifies an unsupported symbol name in the attribute value.
- DFHRV1012E indicates that an override rule specifies an invalid symbol substring in the attribute value.
- DFHRV1013E indicates that an override rule specifies an unsupported escape character in the attribute value.
- DFHRV1014E indicates that an override rule specifies an invalid null string in the attribute value.
- DFHRV1015E indicates that an override rule specifies an obsolete attribute.
- DFHRV1016W indicates that a resource overrides file with updated content was loaded during CICS restart.
- DFHRV1017E indicates that a resource overrides file is empty.

DFHSInnnn

New:

- DFHSI1610 indicates that DFHAMIO is not on the load library and resource overrides cannot be processed.
- DFHSI1611 indicates an error in DFHAMIO during resource override processing.
- DFHSI1612 indicates errors in the resource overrides file during resource override processing.
- DFHSI1801 indicates errors in the PLT that is used during the initialization of CICS.

DFHSMnnnn

New:

- DFHSM0136 indicates the size of the DSAs that are never protected from instruction execution.
- DFHSM0160I indicates that Instruction Execution Protection is available.
- DFHSM0161I indicates that Instruction Execution Protection is enabled for eligible CICS DSAs.

Removed:

- DFHSM0137
- DFHSM0138
- DFHSM0139
- DFHSM0140

DFHSNnnnn

Changed:

- DFHSN1100 changed to add the TN3270 IP Address to the message output.
- DFHSN1101

Removed:

- DFHSN1102

DFHSOnnnn

New:

- DFHSO0170A indicates that the specified TCPIPSERVICE cannot be opened because the default TCP/IP stack is not available.
- DFHSO0171A indicates that the specified TCPIPSERVICE cannot be opened because the specified TCP/IP stack is not available.
- DFHSO0200I is issued when the CICS sockets listener task starts accepting inbound TCP/IP connections.
- DFHSO0201I is issued when the CICS sockets listener task stops accepting new inbound HTTP connections.

- DFHSO0202I is issued when the CICS sockets listener task stops accepting all inbound TCP/IP connections.
- DFHSO0300 is issued when the client side of a TLS handshake failed during certificate validation.
- DFHSO0301 is issued when the client side of a TLS handshake failed to establish secure communication.
- DFHSO0302 is issued when the client side of a TLS handshake failed during certificate validation caused by a lack of a valid certificate.
- DFHSO0303 is issued when the client side of a TLS handshake failed during certificate validation caused by a lack of a valid certificate sent to the remote partner.
- DFHSO0304 is issued when the client side of a TLS handshake failed during certificate validation caused by an invalid certificate date.
- DFHSO0305 is issued when the client side of a TLS handshake failed during certificate validation caused by a missing key label.
- DFHSO0310 is issued when the client side of a TLS handshake failed during certificate validation caused by an internal error reported by the remote partner.
- DFHSO0399 is issued when the client side of a TLS handshake failed. The text in the message explains the error details.
- DFHSO0400 is issued when the server side of a TLS handshake failed during certificate validation.
- DFHSO0401 is issued when the server side of a TLS handshake failed to establish secure communication
- DFHSO0402 is issued when the server side of a TLS handshake failed during certificate validation caused by a lack of a valid certificate.
- DFHSO0403 is issued when the server side of a TLS handshake failed during certificate validation caused by a lack of a valid certificate sent to the remote partner.
- DFHSO0404 is issued when the server side of a TLS handshake failed during certificate validation caused by an invalid certificate date.
- DFHSO0405 is issued when the server side of a TLS handshake failed during certificate validation caused by a missing key label.
- DFHSO0410 is issued when the server side of a TLS handshake failed during certificate validation caused by an internal error reported by the remote partner.
- DFHSO0499 is issued when the server side of a TLS handshake failed. The text in the message explains the error details.

DFHSRnnnn

New:

- DFHSR0623 indicates that there is an attempt to execute an instruction from storage that is protected from instruction execution.

DFHTMnnnn

New:

- DFHTM1721 indicates errors in the PLT that is used during the shutdown of CICS.

DFHTPnnnn

New:

- Service DFHTP4175 (APAR PH43431) indicates a message routing failure due to an invalid or unlocatable remote system ID.

DFHTSnnnn

New:

- DFHTS1316 indicates that auxiliary temporary storage data set usage has reached 75% or more of the capacity.

- DFHTS1317 indicates that auxiliary temporary storage data set usage has fallen below 70% of the capacity.
- DFHTS1610 indicates that a scan of shared temporary storage queues has completed. The message shows the numbers of shared temporary storage queues scanned and deleted.

DFHWBnnnn

New:

- DFHWB0112I indicates that there was a problem processing the defaultciphers.xml file.

New with APAR:

- **APAR PH60212**: DFHWB1561 indicates that the URIMAP resource was defined with `CIPHERS( )` and lists the ciphers that CICS used instead.

Changed:

- DFHWB0763 is changed to indicate the name of the disabled URIMAP.

DFHXQnnnn

New:

- DFHXQ0420I indicates that the percentage of entries in use in the pool structure dropped below a specified threshold.
- DFHXQ0421I indicates that the percentage of elements in use in the pool structure dropped below a specified threshold.
- DFHXQ0422I indicates that the percentage of entries in use in the pool structure reached a specified threshold.
- DFHXQ0423I indicates that the percentage of elements in use in the pool structure reached a specified threshold.

DFHXSnnnn

New:

- DFHXS1117 indicates the association data, including origin information related to a security violation.

Changed:

- DFHXS1113 is removed as Category 1 transactions. No longer use RACF to determine access.
- DFHXS1201 either mentioned USERID or PASSWORD and now provide a more generic message to obscure which field was incorrect.
- DFHXS1206 either mentioned USERID or PASSWORD and now provide a more generic message to obscure which field was incorrect.
- DFHXS1215 either mentioned USERID or PASSWORD and now provide a more generic message to obscure which field was incorrect.
- DFHXS1404 is removed as Category 1 transactions. No longer use RACF to determine access.

Removed:

- DFHXS1205
- DFHXS1211

DFHYMnnnn

New:

- DFHYM1000E indicates that a resource type in the resource overrides file is too long or missing a delimiter.
- DFHYM1001E indicates that an override rule in the resource overrides file is missing the selector or overrides value.

- DFHYM1002E indicates that an attribute name in the resource overrides file is too long or missing a delimiter.
- DFHYM1003E indicates that an override action in the resource overrides file must start on a new line.
- DFHYM1004E indicates that a find override action in the resource overrides file is missing an associated replace action.
- DFHYM1005W indicates that an overrides mapping in the resource overrides file does not specify any attributes.
- DFHYM1006E indicates an invalid selector condition or override action for an attribute in the resource overrides file.
- DFHYM1007E indicates that a line delimiter is missing from the resource overrides file.
- DFHYM1008E indicates incorrect indentation in the resource overrides file.
- DFHYM1009E indicates that an attribute value must be enclosed in quotes in the resource overrides file.
- DFHYM1010E indicates a missing space before a comment in the resource overrides file.
- DFHYM1011E indicates unexpected data in the resource overrides file.
- DFHYM1012E indicates an invalid character because of a character encoding error in the resource overrides file.
- DFHYM1013E indicates an unsupported escape character in the resource overrides file.
- DFHYM1014E indicates an invalid override action-operator in a selector mapping in the resource overrides file.
- DFHYM1015E indicates an invalid selector condition-operator in an overrides mapping in the resource overrides file.
- DFHYM1016E indicates a duplicate attribute in a selector or overrides mapping in the resource overrides file.
- DFHYM1017E indicates that a resource override find action is missing a value in the resource overrides file.
- DFHYM1018E indicates an unsupported multiline indicator in the resource overrides file.
- DFHYM1019E indicates that the schemaVersion mapping is missing from the resource overrides file.
- DFHYM1020E indicates that the resourceOverrides mapping is missing from the resource overrides file.
- DFHYM1021E indicates that the schemaVersion mapping specifies an invalid schema name or version in the resource overrides file.
- DFHYM1022E indicates that a resource overrides schema version in the resource overrides file is not supported.
- DFHYM1023E indicates that the resource overrides file uses an unsupported code page.

Changes to CICSPlex SM messages

EYUNXnnnn

New:

- EYUNX0110W indicates that resources to be installed conflicted with existing URIMAP or TCPIPSERVICE resources.

Changed:

- EYUNX0013E is changed to also indicate invalid definition options for resources in a single CICS region configured with the CMCI JVM server (SMSS).

EYUXDnnnn

New:

- EYUXD0721I indicates the name of the CICSplex whose CICSplex context records will be removed from the CMAS EYUDREP data repository.
- EYUXD0722I indicates the name of the CICSplex whose CICSplex context records will be updated to the CMAS EYUDREP data repository.

EYUXLnnnn

Changed:

- EYUXL0003I has an editorial change in its message text. The phrase `version` is dropped from the message text. There is no functional change to this message.

Changes to abend codes

New abend codes

- Service AITQ (APAR PH52991) occurs when a transaction is purged, during the processing of a request, while waiting for a response from a connected subsystem over an IPIC connection.
- AKES occurs when an attempt is made to execute an instruction that is located in storage that is protected from instruction execution.
- Service AMQT (APAR PH47961) occurs when temporary storage queue DFHCKBR is required but the TSMODEL definition for it does not exist.
- ARZR occurs when a request stream task encountered a failure while trying to join with an existing target request stream task.
- AXS1 occurs when a user attempts to run a Category 1 transaction directly.

Changes to samples

Table 58. Changes to the samples provided with CICS TS 6.1

Sample	**6.1**
`strongciphers.xml`	**REMOVED:** Use of `strongciphers.xml` is replaced by customizing `allvalidciphers.xml` and `defaultciphers.xml` for use with CIPHERS attribute in resource definitions.
DFH$54J	**NEW:** JCL to output SMF 1154 Subtype 80 records
DFH$1154	**NEW:** REXX program to output SMF 1154 Subtype 80 records
DFH$MOLS	**CHANGED:** The UNLOAD function is enhanced to support DFHRMI fields in its output.

Changes to documentation

Table 59. Changes to the documentation provided with CICS TS 6.1.

Documentation	**6.1**
	6.1
Downloadable (offline) documentation	**NEW:** IBM Documentation Offline is now automatically translated.
Online documentation	**CHANGED:** IBM Knowledge Center is renamed to IBM Documentation. **NEW:** IBM Documentation is now automatically translated.

Table 59. Changes to the documentation provided with CICS TS 6.1. (continued)	
Documentation	**6.1**
Fundamentals	**NEW:** How it works: CICS storage **CHANGED** after general availability: The reference topics about CICS subpools in CICS DSAs, previously contained in How it works: CICS storage, are moved to System management reference. See Reference: CICS subpools in CICS DSAs.
Developing applications	**NEW:** Get started with Java in CICS
Security	**NEW:** structure and information
CICS TS Feature Pack for Dynamic Scripting V2.0	**REMOVED:** References removed from the documentation.
Scenario: Using business events to analyze application trends	**REMOVED:** References removed from the documentation.
PDFs	**NEW PDF:** • *Security for CICS* **CHANGED**: • *Configuring CICS* The Configuring REXX section has been removed from this PDF. This information is contained in *REXX for CICS TS User Guide and Reference*. **STABILIZED**: The following PDF is no longer produced: *RACF Security Guide*

Notices

This information was developed for products and services offered in the United States of America. This material might be available from IBM in other languages. However, you may be required to own a copy of the product or product version in that language in order to access it.

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 rights 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 grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
United States of America

For license inquiries regarding double-byte character set (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

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 jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore this statement may not apply to you.

This information 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.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

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 Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119 Armonk,
NY 10504-1785
United States of America

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 Client Relationship Agreement, IBM International Programming License Agreement, or any equivalent agreement between us.

The performance data discussed herein is presented as derived under specific operating conditions. Actual results may vary.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. The sample programs are provided "AS IS", without warranty of any kind. IBM shall not be liable for any damages arising out of your use of the sample programs.

Programming interface information

IBM CICS supplies some documentation that can be considered to be Programming Interfaces, and some documentation that cannot be considered to be a Programming Interface.

Programming Interfaces that allow the customer to write programs to obtain the services of CICS Transaction Server for z/OS, Version 6 are included in the following sections of the online product documentation:

- Developing applications
- Developing system programs
- Securing CICS
- Developing for external interfaces
- Application development reference
- Reference: system programming
- Reference: connectivity

Information that is NOT intended to be used as a Programming Interface of CICS Transaction Server for z/OS, Version 6, but that might be misconstrued as Programming Interfaces, is included in the following sections of the online product documentation:

- Troubleshooting and support
- CICS TS diagnostics reference

If you access the CICS documentation in manuals in PDF format, Programming Interfaces that allow the customer to write programs to obtain the services of CICS Transaction Server for z/OS, Version 6 are included in the following manuals:

- Application Programming Guide and Application Programming Reference

- Business Transaction Services
- Customization Guide
- C++ OO Class Libraries
- Debugging Tools Interfaces Reference
- Distributed Transaction Programming Guide
- External Interfaces Guide
- Front End Programming Interface Guide
- IMS Database Control Guide
- Installation Guide
- Security Guide
- CICS Transactions
- CICSPlex System Manager (CICSPlex SM) Managing Workloads
- CICSPlex SM Managing Resource Usage
- CICSPlex SM Application Programming Guide and Application Programming Reference
- Java Applications in CICS

If you access the CICS documentation in manuals in PDF format, information that is NOT intended to be used as a Programming Interface of CICS Transaction Server for z/OS, Version 6, but that might be misconstrued as Programming Interfaces, is included in the following manuals:

- Data Areas
- Diagnosis Reference
- Problem Determination Guide
- CICSPlex SM Problem Determination Guide

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.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Apache, Apache Axis2, Apache Maven, Apache Ivy, the Apache Software Foundation (ASF) logo, and the ASF feather logo are trademarks of Apache Software Foundation.

Gradle and the Gradlephant logo are registered trademark of Gradle, Inc. and its subsidiaries in the United States and/or other countries.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

The registered trademark Linux® is used pursuant to a sublicense from the Linux Foundation, the exclusive licensee of Linus Torvalds, owner of the mark on a worldwide basis.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Red Hat, and Hibernate® are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Spring Boot is a trademark of Pivotal Software, Inc. in the United States and other countries.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Zowe™, the Zowe logo and the Open Mainframe Project™ are trademarks of The Linux Foundation.

The Stack Exchange name and logos are trademarks of Stack Exchange Inc.

Red Hat, JBoss, OpenShift, Fedora, Hibernate, Ansible, CloudForms, RHCA, RHCE, RHCSA, Ceph, and Gluster are trademarks or registered trademarks of Red Hat, Inc. or its subsidiaries in the United States and other countries.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability
These terms and conditions are in addition to any terms of use for the IBM website.

Personal use
You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use
You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights
Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM online privacy statement

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 (PII) is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect PII. If this Software Offering uses cookies to collect PII, specific information about this offering's use of cookies is set forth below:

For the CICSPlex SM Web User Interface (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 PII for purposes of session management, authentication, enhanced user usability, or other usage tracking or functional purposes. These cookies cannot be disabled.

For the CICSPlex SM Web User Interface (data interface):
Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user's user name and other PII for purposes of session management, authentication, or other usage tracking or functional purposes. These cookies cannot be disabled.

For the CICSPlex SM Web User Interface ("hello world" page):
Depending upon the configurations deployed, this Software Offering may use session cookies that do not collect PII. 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 PII 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 Privacy Policy and IBM Online Privacy Statement, the section entitled *Cookies, Web Beacons and Other Technologies* and the IBM Software Products and Software-as-a-Service Privacy Statement.