Virtual CICS user group: Newsletter 11

Welcome to the Virtual CICS user group newsletter. The Virtual CICS user group at www.fundi.com/virtualcics is an independently-operated vendor-neutral site run by and for the CICS user community.

Virtual CICS user group presentation

The latest webinar from the Virtual CICS user group was entitled, “CICS security”, and was presented by Colin Pearce, Vice President at Bank of America.

Colin has been an MVS and CICS Systems Programmer for 30 years and has been teaching for over 20 years. He has written a number of MVS and CICS courses and has given them in many different parts of the world. Colin has spent the majority of his career working within the banking environment. He has worked in England, South Africa, Qatar, Australia, and Singapore.

Colin Pearce started his presentation to the user group by looking at what’s defined in the System Initialization Table (DFHSIT*xx*):

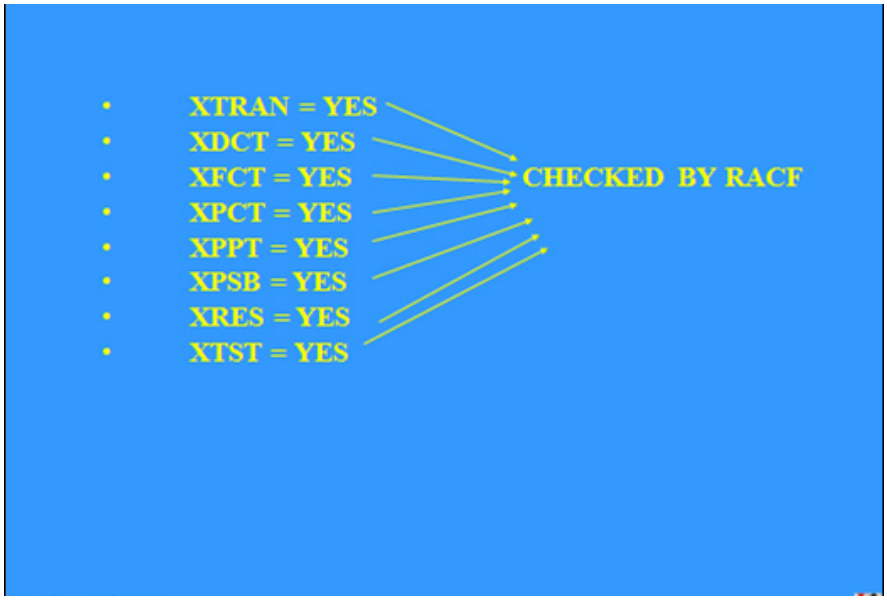
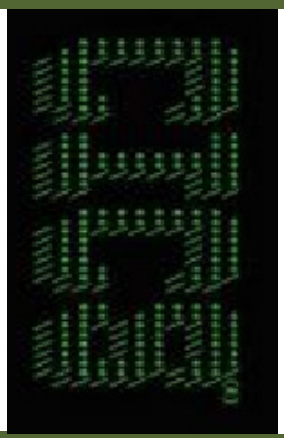


Figure 1: Resource-level security

```
DFHSIT TYPE = CSECT
       SEC = NO/YES
       SECPRFX = NO/YES
       DFLTUSER = USER
       RESSEC=ALWAYS/ASIS
       XAPPC = NO/YES
       XCMD = YES/NO/CLASSNAME
       XCFGROUP {DFHIR000/NAME}
       XDB2 = NO/CLASSNAME
       XHFS = (YES/NO)
       XRES = (NO/YES/
CLASSNAME
       XTRAN = YES/NO/CLASSNAME
```

Contents:



```
XPSB = YES/NO/CLASSNAME
XDCT = YES/NO/CLASSNAME
XFCT = YES/NO/CLASSNAME
XJCT = YES/NO/CLASSNAME
XPCT = YES/NO/CLASSNAME
XPPT = YES/NO/CLASSNAME
XTST = YES/NO/CLASSNAME
XUSER = YES/NO
```

Colin said that options affecting the whole CICS system included:

- SEC = NO – no security checking is performed. Signons cannot take place.

  YES – security checking for all users. CICS requires a level of authorization appropriate to intent. The SP commands are also affected, READ is required for INQUIRE and COLLECT, and UPDATE is needed for DISCARD, SET, and PERFORM.

- SECPRFX = NO – CICS does not prefix the resource names in authorization requests it passes to RACF from this CICS region.

  YES – CICS prefixes the resource names with its RACF userid when passing authorization requests to RACF.

- DFLTUSER = CICSUSER – used with SEC = YES, to be assigned to each terminal before logon.

- RESSEC = ALWAYS – forces resource security checking for all lower-level resources. This is not recommended because extra overhead could be incurred for a resource check for every transaction. Use ASIS, to allow the RESSEC option in the Transaction definition to control resource security.

The Class Descriptors in RACF that control the access to CICS resources can be listed with the SETROPTS LIST command. This is issued within the TSO environment.

The RACF command SETR CLASSACT may need to be issued if the classes are not activated.

For transactions that are attached:

```
XTRAN = YES/NO/CLASSNAME
```

specifies whether attached transactions will be checked by RACF. YES indicates the default RACF Classnames will be used. T and G are used as prefixes for the CLASSNAMES (TCICSTRN and GCICSTRN. CLASSNAME allows for a 1-7 character user-defined name that can be utilized. This name must be defined in the RACF Class Descriptor Table ICHRCDE. The first 1-4 characters must be unique, because RACF stores only the first four characters on the RACF database.

XTRAN=PRODTRN would generate TPRODTRN and GPRODTRN

With SEC=YES and XTRAN=YES or CLASSNAME, CICS issues an authorization request for every attached transaction. The T Classname allows for individual profiles and the G Classname allows for group profiles, where many transactions can be grouped together, having common security requirements.

```
XPSB = YES/NO/CLASSNAME
```

specifies whether DL1 PSB entries will be checked by RACF and the Classname that will be used. P and Q are used as prefixes for the CLASSNAMES (PCICSPSB and QCICSPSB)

```
XDCT = YES/NO/CLASSNAME
```

specifies whether Transient Data Queue entries will be checked by RACF and the Classname that will be used. D and E are used as prefixes for the CLASSNAMES (DCICSDCT and ECICSDCT).

XDB2 requires a user-defined Classname for all DB2ENTRY defined resources via CEDA.

```
XFCT = YES/NO/CLASSNAME
```

specifies whether File Control Table entries will be checked by RACF and the Classname that will be used. F and H are used as prefixes for the CLASSNAMES (FCICSFCT and HCICSFCT).

```
XJCT = YES/NO/CLASSNAME
```

specifies whether Journal Control Table entries will be checked by RACF and the Classname that will be used. J and K are used as prefixes for the CLASSNAMES (JCICSJCT and KCICSJCT).

`XPCT = YES/NO, CLASSNAME`

specifies whether EXEC CICS STARTED transactions that do not specify a termid, will be checked by RACF and the classname that will be used. A and B are used as prefixes for the CLASSNAMES (ACICSPCT and BCICSPCT).

`XPPT = YES/NO, CLASSNAME`

specifies whether PROGRAM ENTRIES will be checked by RACF and the Classname that will be used. M and N are used as prefixes for the CLASSNAMES (MCICSPPT and NCICSPPT).

`XTST = YES/NO, CLASSNAME`

specifies whether Temporary Storage Table entries will be checked by RACF. The queue entries specifies under TYPE=SECURITY. S and U (SCICSTST and UCICSTST) are used as prefixes for the CLASSNAMES. Temporary Storage Queues are defined with Transaction Server V1.3.

In all cases the default 4-character Classname that RACF uses is CICS.

`XAPPC = NO/YES`

specifies session security for APPC Sessions. The Classname is APPCLU.

`XCMD = YES/NO,CLASSNAME`

specifies whether SP commands, such as INQUIRE, SET, DISCARD, PERFORM, or COLLECT will be checked by RACF. The CICS assigned prefix is C and V for the CLASSNAMES. REQUIRES CMDSEC = YES in the transaction definition.

`XRES = YES/NO, CLASSNAME`

specifies whether access to the CICS Document Templates entries will be checked by RACF. (RCICSRES and WCICSRES)

The actual profile name passed to RACF is the name of the Docutemplate resource definition for the CICS Document Template.

This security checking is only performed if you have SEC(YES) in the System Initialization Table and RESSEC(YES) specified for the Transaction definition.

`XCFGROUP =DFHIR000/NAME`

specifies the name of the cross-system coupling facility (XCF) group to be joined by this region.

CICS executes as an application under VTAM. Each CICS system is known to VTAM by a unique name. This is called the APPLID. This 1-8 character APPLID can be specified in one of two places:

1 The System Initialization Table (DFHSIT*xx*)

2 The Override Facility

This APPLID is used by CICS with the inter-system communication facility and the multi-region option facility, and is used in the APPL class by RACF to determine whether a user is permitted to access the CICS region.

There is no mechanism, as supplied, that forces the user of the online system to sign on. As soon as a logon request is received, CICS, by default, will execute the good morning transaction CSGM, which in turn, by default, executes DFHGMM. This displays a CICS screen. The user must still issue a signon.

CESN is provided for the signon. This allows for the Userid/Password to be entered and validated by RACF. A Newpassword and a different RACF Group can also be entered.

CICS has the DFLTUSER SIT option to force a user to signon, if the Dfltuser Userid has UACC(none)

In order to check which transaction is being executed as the good morning message, check the GMTRAN option in The SIT.

Access to CICS for terminals can be controlled at sign-on time, in two ways.

1 System-wide TERMINAL GTERMINL

CICS restricts operator sign-on to specific terminals defined by:

```
RDEFINE TERMINAL (L001 L002)
UACC (READ)
```

2 System Wide TERMINAL (READ)

CICS does not restrict operator logon and sign-on. The TERMUACC or NOTERMUACC keyword on the ADDGROUP command follows the system-wide access with TERMINAL. With undefined terminals, NOTERMUACC forces, for the group, the need for explicit authority to use any terminals.

For Telnet access, the Logical Unit addresses are defined to TCP/IP in the Profile.

Protecting the transactions is achieved by defining them to TCICSTRN or GCICSTRN.

Transactions that have the same access characteristics would be defined to GCICSTRN.

Individual transactions that have specific needs would be defined to TCICSTRN.

Users would then need to be PERMITTED to access the protected transactions.

For individual resources, such as programs and files, the security access is handled with Resource Level Security.

The System Initialization Table option RESSEC=ALWAYS is not recommended. This forces Resource Security checking for all transactions, whether the individual transactions has it turned on or off.

The better way is to code RESSEC=ASIS in the SIT and then CEDA DEFINE TRANSACTION command must specify RESSEC=YES.

Of course if SEC=YES has been defined in the SIT and Update access is required, then ACCESS(UPDATE) must be specified in the profile.

It must be understood that the moment RESSEC = YES is specified at the transaction level, access to all lower level resources is checked, regardless of which resources need to be protected.

The SIT option PLTPIUSR can specify how security will be checked for all programs executing in the PLTPI during the third stage of Initialization. If it's set to NONE, then the CICS Userid is used as validation. This is referred to as surrogate authority

This SIT option PLTPISEC can specify how security will be checked for all START requests issued from the programs executing in the PLTPI during the third stage of initialization. If it's set to NONE, then the CICS Userid is used as validation. This again is surrogate authority.

During shutdown, the PLTSD programs run under the authority of the transaction that issued the shutdown. This is usually the Master Terminal command CEMT.

All Transient Data ATI requests (transactions initiated via the Trigger level), run under the Userid associated with the definition of the queue in the DCT.

The CICS SIT option SDTRAN invokes CESD and program DFHCESD. It is designed to assist with the Shutdown process of purging long-running tasks.

The RACF Userid can have a CICS SEGMENT. This information is specified usually when the Userid is defined to RACF. Most of the information is now no longer valid having been superseded by other newer options. The CICS SEGMENT is defined to RACF with the ADDUSER command.

The QUERY SECURITY command is available at the Command Level Interface, and therefore can be issued by any programmer using the API (Application Programming Interface).

This command allows a programmer to check whether access is allowed

against a resource before the actual request against the resource is made. It is only used with RACF.

Resources can be checked in either of the following ways.

- Resources in CICS Resource Classes
- Resources in User-Defined Resource Classes.

The Userid used is the one currently assigned to the Terminal. If no Userid is assigned then the Default Terminal Userid is used. CICS will return to the application whether access is allowed or denied, it is up to the program to act upon the information.

The SIGNON/SIGNOFF commands provide a programmable interface to the Signon and Signoff process. It provides for the specification of a new password during signon and RACF can respond with a variety of return values:

- The supplied password is incorrect
- A new password is required
- A new password is not acceptable
- The Userid is revoked
- The Userid is not authorized to the Terminal
- The userid is not authorized to the Application.

It allows an installation to provide a customized designed signon.

CICS offers RACF controls to the resources that would be accessed via INQUIRE, SET, PERFORM, COLLECT, and DISCARD.

Operators need access to the profiles that cover these resources.

INQUIRE and COLLECT require READ access. SET, PERFORM, and DISCARD require UPDATE access

These same processes affect supplied transactions CEDF and CECI.

All three transactions require:

```
CMDSEC = YES
```

IBM does not allow changes to the supplied transactions in the CSD, so these will have to be copied and modified.

```
XCMD = YES
```

specified in the SIT.

There are four stages of security with Interregion Communication:

- Bind-time security
- Link security
- Attach or user security
- Resource-level security

LUTYPE 6.2 links provide a PASSWORD. The successful binding of any type of session always causes LINK SECURITY values to be established for the session.

Each pair of communicating systems must have the same password.

The BIND PASSWORD is protected in the following ways:

1 The BIND PASSWORD is never transmitted between systems.

2 CICS does not store a readable copy of the password, either on the CSD or in internal control blocks.

3 The BIND PASSWORD field in CEDA DEFINED CONNECTION is a non-display field.

A copy of Colin Pearce's presentation is available for download from the Virtual CICS user group Web site at www.fundi.com/virtualcics/presentations/CICSsecurityNov12.pdf.

You can see and hear the whole user group meeting by downloading the WMV file from www.fundi.com/virtualims/presentations/2012-11-06meeting.wmv.

Meeting dates

The following meeting date

has been arranged for the Virtual CICS user group:

- On 15 January 2013 at 10:30am CST, Andy Bates, CICS TS Product Line Manager at IBM, and Ted Caffarelli, IBM CICS Tools Product Line Manager at IBM will be talking about CICS V5.1 – Portfolio Update.

We will be using Citrix GoToMeeting for the user group meetings.

Recordings of meetings are available for download from our Web site for people who were unable to attend the meeting.

Recent CICS articles

CICS 101: CICS Resources and Tables by Phyllis Donofrio in *Enterprise Tech Journal* (October/November). You can find the article at http://enterprisesystemsmedia.com/article/cics-101-cics-resources-and-tables.

CICS Explorer for z/VSE Eases CICS Transaction Server Monitoring Challenges by August Madlener in *Enterprise Tech Journal* (October/November). You can find the article at http://enterprisesystemsmedia.com/article/cics-explorer-for-z-vse-eases-cics-transaction-server-monitoring-challenges.

CICS news

Matter of Fact Software has announced Version 2 of CICS JS/Server, its CICS Web Document API that allows Web applications to be built and served right out of CICS. Writing the user interfaces for such applications can be facilitated by using Open Source Javascript Libraries and Toolkits such as Dojo Toolkit, JQuery, YUI Library, Scriptaculous, D3JS, and MooTools. CICS JS/Server V2 also supports bespoke content so you can define and serve your own plugins and other content using the software. Full details can be found at www.plexspy.co.uk/content/Press-Release-November-2012.pdf.

Compuware has announced PurePath for z/OS CICS (part of its Compuware APM (Application Performance Management) for Mainframe) for monitoring CICS application transactions in a CICS region or CICSPlex. It automatically discovers, maps, and monitors all CICS transactions through distributed tier and mainframe applications. Full details can be found at www.compuware.com/about/release/711947/compuware-lights-up-the-mainframe-with-the-industrys-first-deep-transaction-management-solution-for-zos-applications.

IBM has announced CICS TS Version 5.1

CICS Explorer Version 5.1, CICS Interdependency Analyzer for z/OS V5.1, CICS Deployment Assistant for z/OS V5.1, CICS Performance Analyzer for z/OS V5.1, CICS Configuration Manager for z/OS V5.1, and CICS VSAM Recovery for z/OS V5.1.

IBM CICS Transaction Gateway for z/OS V9.0, CICS TG for Multiplatforms V9.0, and CICS TG Desktop Edition V9.0.

IBM Session Manager V3.2.

About the Virtual CICS user group

The Virtual CICS user group was established as a way for individuals using IBM's CICS TS systems to exchange information, learn new techniques, and advance their skills with the product.

The Web site at www.fundi.com/virtualcics provides a central point for coordinating periodic meetings (which contain technically-oriented topics presented in a webinar format), and provides articles, discussions, links, and other resources of interest to IBM CICS practitioners. Anyone with an interest in CICS is welcome to join the Virtual CICS user group and share in the knowledge exchange.

To share ideas, and for further information, contact trevor@itech-ed.com.

The Virtual CICS user group is free to its members.