IBM – CICS Workshop

IBM

L02 – CICS-Security Request Recording

Lab Version V0.1

October, 2022

Overview

Security request recording (SRR) can be used to help you diagnose CICS®
security issues.

What sort of issues can security request recording help you solve?

Many security problems are straightforward to solve. The ICH408I messages give details of the
user ID, RACF® profile, RACF class, and the required access. Associated DFHXS1111 and
DFHXS1117 message help identify the user so that the problem can be identified and if necessary
access granted.

Some problems are more difficult to solve. Often these problems occur as a result of a help desk
problem that the system programmer needs to investigate. These problems might include various
complexities:

- The application that is being investigated might traverse multiple regions, multiple LPARs, or even
  multiple sysplexes.
- There might not be any messages that are associated with the reason that causes a security failure.
- The application might grant access to something when it mustn't.

Lab Scenario

In our scenario, you are a system programmer and need to configure SEC=YES for all your CICS
regions. But the application does not work after the change and you can't check some CICS
resources, either. Then, you turn on the security request recording function and check the RACF classes and
profiles caused the errors and issue correct RACF commands to make the application work.

Lab Requirements

Please note that there are often several ways to perform functions in and for CICS. This lab exercise will present one of the ways. If you are familiar with CICS, you will notice that some of the statements are general, and not necessarily true for every situation.

This lab uses the PCOMM and CICS Explorer. If you are not familiar with these, please contact one of the lab instructors for assistance.

The following are other assumptions made in this lab exercise.

- **CICS TS V6.1:** This lab exercise only works in CICS V6.1. You have your own z/OS image you can change all resources in four CICS regions.

- **Login:** A TSO userid is available with the appropriate password provided, and you will also use the same TSO userid with the z/OS Explorer.

- The **CICS Explorer:** In the lab environment we have installed the CICS Explorer to configure CICS resources and the security request recording function.

Lab Step Overview

Part 1: Try the CICS bank sample application (hereafter CBSA) in 4 CICS regions
Logon to the CICS61T1 and run the transaction OMEN. Then, try to browse customer number with "1" and display the account "1" in menus. Make sure no problems happen there.

Part 2: Change the SIT parameters of all CICS regions and restart them
Set "SEC=YES" on all CICS regions.

Part 3: Try again the CBSA and check errors
Try to browse the customer number, "1" in the customer inquiry menu and see the application making errors.

Part 4: Configure the Journal for the CICS Security Request Recording (SRR)
Create the journal model to create the DFHSECR journal.

Part 5: In the CICS Explorer, setup the SRR for a CEMT transaction and browse journals
Setup the SRR for the CEMT transaction in the CICS Explorer and issue "CEMT I JO" command in a CICS region.

Part 6: Check the SRR result and issue RACF commands to browse journals by CEMT
Check the SRR CSV file and create a RACF command to resolve the journal "Not found" error in CICS.

Part 7: Turn on the SRR for the ODCS transaction in all CICS regions
In the region view of CICS Explorer, turn on the SRR log for ODCS transaction in all four CICS regions.

Part 8: Check the SRR result and issue RACF commands to resolve ODCS errors
Check the SRR CSV file and create a RACF command to resolve the ODCS transaction error.

Part 9: Summary
This is a recap of the steps performed in this lab exercise and answers for quizzes.

Part 0: Check the CICS Explorer Connection to CICS

In this part of the lab exercise you will configure the connection between the CICS Explorer running on your workstation to CICS running on z/OS.

Start the CICS Explorer

___1. From the **desktop**, **double-click** the **CICS Explorer** icon to start the Explorer if it is not already running.

___2. When you start the Explorer, if you are prompted for a workspace, click the **OK** button to select the default.

___3. If the Explorer shows you a **Welcome page** click the **Workbench icon** in the upper-right corner to go to the workbench. Then **maximize** the Explorer window.

Verify that you have an FTP connection to z/OS in your CICS Explorer

___4. If you have not already created connections to the z/OS host system, check the connection as in the screen shot. Both the **Remote System Explorer** and **CMCI** connections should be started and active.
       IP : zos.dev / CMCI port : 6611 / User : IBMUSER / Password : sys1
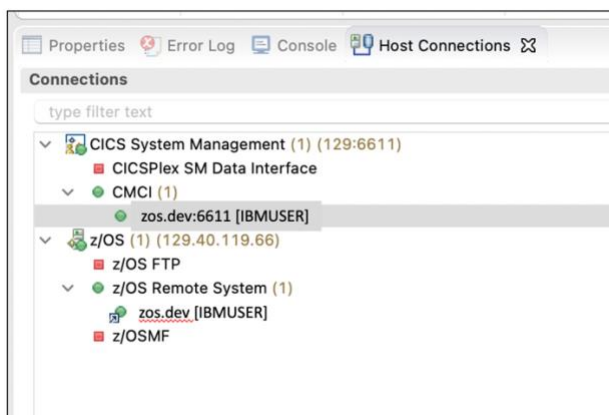
Part 1: Try the CICS bank sample application (hereafter CBSA) in 4 CICS regions

In this part of the lab exercise you will try the CICS bank sample application.

Try the CICS Bank Sample Application

___**1.** Open a session in the PCOMM, and type "**L CICS61T1**" to logon.

___**2.** Clear the screen and type "OMEN" to start the main screen.

```
BNK1MA              CICS Bank Sample Application - Main Menu

Select an option. Then press Enter.

Action . . . . _   1.   Display/Delete/Update CUSTOMER information
                   2.   Display/Delete ACCOUNT information
                   3.   Create CUSTOMER
                   4.   Create ACCOUNT
                   5.   Update ACCOUNT
                   6.   Credit/Debit funds to an ACCOUNT
                   7.   Transfer funds

                   A.   Look up Accounts with Customer Number

















F3=Exit    F12=Cancel
```

___**3.** Try to display the customer number 1 and the account number 1. Also, you can create customer and account numbers as you want to test the CICS Bank Sample Application. (CBSA)

Part 2: Change the SIT parameters of all CICS regions and restart them

To make the RACF security issues, SEC=YES is set in all four CICS61* regions. (CICS61T1, CICS61A1, CICS61A2, CICS61F1)

___**1.** From **the PCOMM**, logon TSO.
L TSO
TSO User : IBMUSER / password : SYS1

___**2.** In CICS.CICS61.SYSIN, update all SIT members which have the same names as CICS regions.
SEC=YES

___**3.** Restart CICS regions in SDSF:

=S;DA;PRE CICS61*
/S STO61
/S STA61

The STO61 procedure will cancel four CICS regions and the STA61 procedure will start four CICS regions. (CICS61T1, CICS61A1, CICS61A2, CICS61F1)

Part 3: Try again the CBSA and check errors

In this part of the lab exercise, we will try the CBSA application again and see an application error and you can't see the journal resource by using CEMT command. \

Retry the CBSA

___**4.** In the CICS61T1, run **OMEN**, select **menu 1**, put **1** into the **customer number** field, and check the application error message as follows:

```
 BNK1DC           CICS Bank Sample Application - Display Customer.

 Provide a CUSTOMER number. Then press Enter.

 CUSTOMER NUMBER 1

 Sort Code
 Customer Number
 Customer Name
 Customer Address


 Customer D.O.B.      /    /
 Credit Score
 CS Review Date       /    /




 DFHAC2206 21:06:11 CICS61T1 Transaction ODCS failed with abend AZI6. Updates
  to local recoverable resources backed out. DFHAC2261 System 61A2 sent message
  (sense code 0824089E). 'DFHAC2206 21:06:11 CICS61A2 Transaction ODCS failed
  with abend HBNK. Updates to local recoverable resources backed out.'.
```
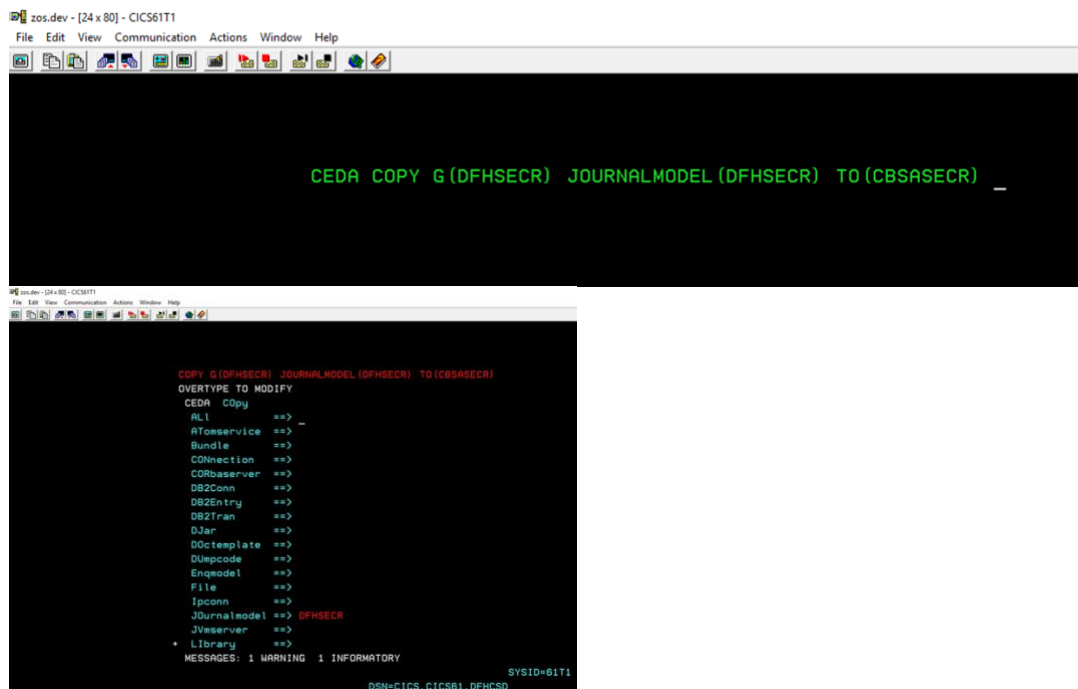
Part 4: Configure the Journal for the CICS Security Request Recording (SRR)

The CICS Security Request Recording (CSRR) writes the logs to the journal, DFHSECR. We will configure a journal model to create a DASD only log stream for this journal.

Define a journal model in CICS

___**1.** In any CICS region, define a new journal model, **DFHSECR** and add it to the CICS group list.

CEDA COPY G(DFHSECR) JOURNALMODEL(DFHSECR) TO(CBSASECR)

CEDA ADD G(CBSASECR) LIST(61LIST)

___**2.** Restart all CICS regions to install the DFHSECR to all CICS regions.

> **/S STO61**
> **/S STA61**

Define a logstream model in the z/OS logger

___**3.** Create a logstream model for the journal model, **DFHSECR**.

CICS.CICS61.JCL(DFHSECR)

```
//DFHILGSR JOB CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID,REGION=0M
//DFHILG6  EXEC PGM=IXCMIAPU
//SYSPRINT DD SYSOUT=*
//SYSIN    DD *
 DATA TYPE(LOGR) REPORT(YES)
 /* User journals              */
 DEFINE LOGSTREAM NAME(#####.STREAM.@@@@@)
     MODEL(YES)
     DASDONLY(YES)
     MAXBUFSIZE(64000)
     AUTODELETE(YES)
     RETPD(1)
/*
```

Quiz 1 : What values should replace ##### and @@@@@ in the above JCL?

If you don't know the answer, please check it at the last page of this document.

Part 5: In the CICS Explorer, setup the SRR for a CEMT transaction and try to browse journals by CEMT

In this part, you will turn on the SRR in the CICS explorer and try to capture the logs from a CEMT transaction.

Turn on the SRR in the CICS Explorer for a CEMT transaction

___**1.** Open the CICS Explorer and select the **CICS SM** perspective.
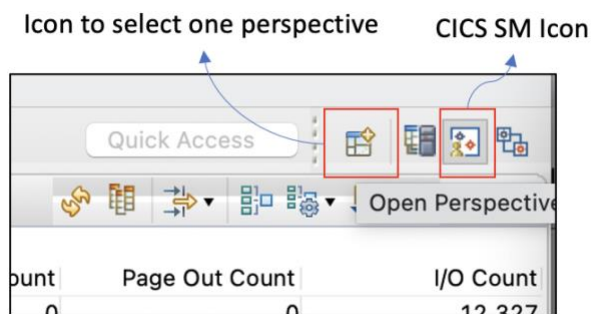
___**2.** Click "Regions" after selecting the CPSM61PX context and the Operations Menu.

___**3.** Open a SRR session by right clicking on CICS61T1.
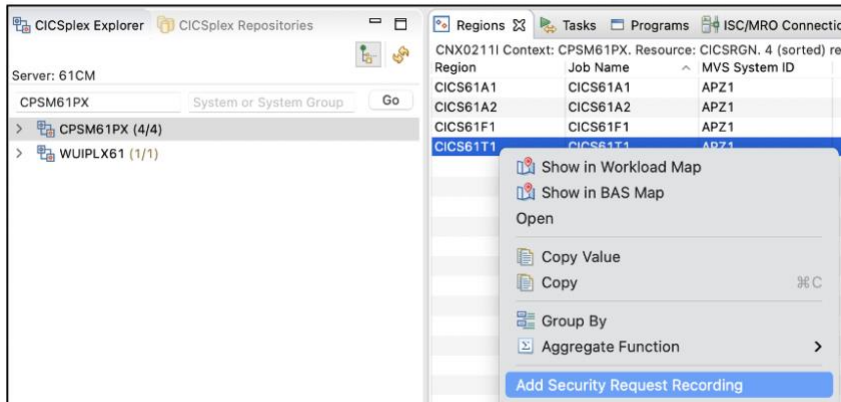
___**4.** Put **CEMT** in the Name field, **5** in Maximum field and **CEMT** in the "Transaction ID" field. Then click OK.
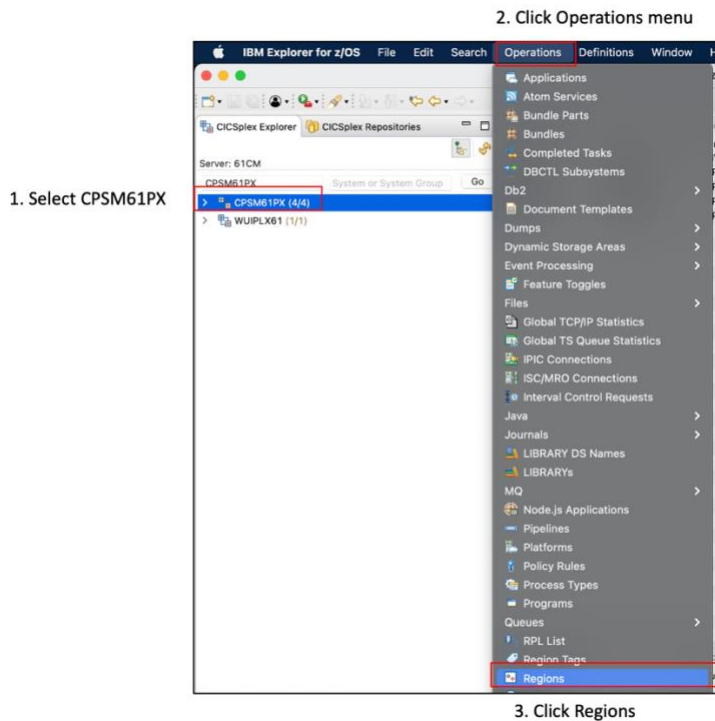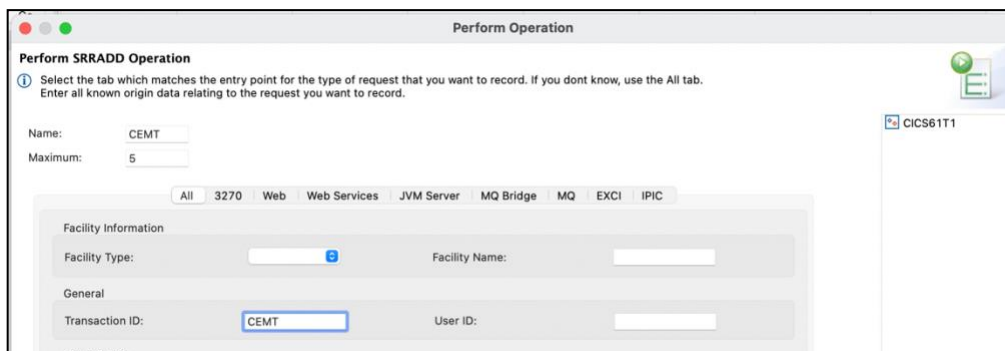

___**5.** Select the **Security Request Recording** menu in the **Operations** menu.
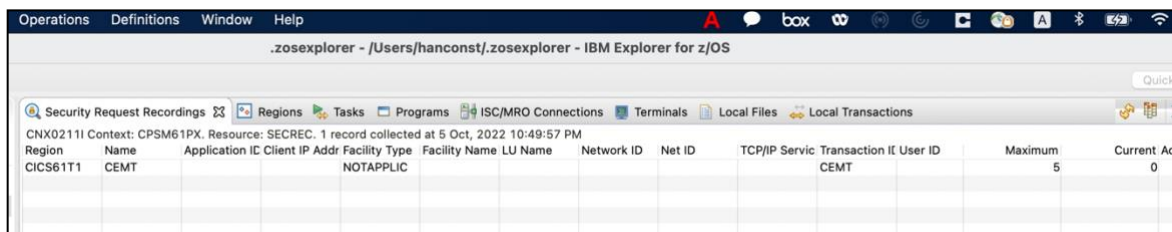
___**6.** Logon to the CICS61T1, Clear Screen and Run "**CEMT I JO**(*)" multiple times in CICS61T1 and check the "Current" filed in the Security Request Recording view. **Don't forget to start the CEMT transaction from the clear screen!!!!**
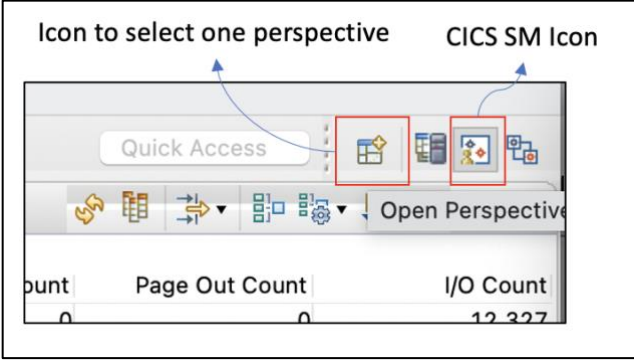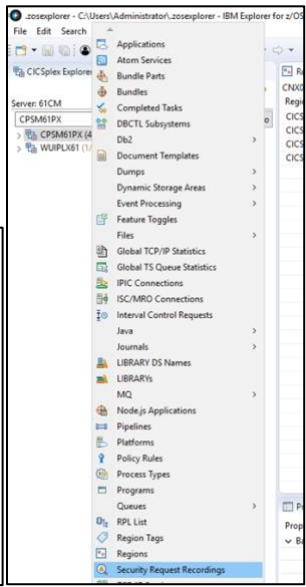
Check the value is increased at the "Current" field in the "Security Request Recording" view of the "Operation" menu.

NOTE: CEMT is a conversational transaction. To get a new security request recording for CEMT, you need to type the CEMT transaction again from the initial screen.

The "I JO(*)" screen is an active started task and new entering in this screen is not a new transaction, so you can't see any number increase in the Current field.

Part 6: Check the SRR result and issue RACF commands to browse journals by CEMT

In this step you will check the generated report and find out RACF profile and class names which caused the "NOT FOUND" exception for your "CEMT I JO(*)" command.

Run the batch job to generate a CSV file and view it in the VS Code

___1. From **the TSO, run the batch JCL to extract the SRR logs and write to a CSV file.**

CICS.CICS61.JCL(DFHSRRPC)

```
//DFH$SRRP JOB CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID,REGION=0M
// SET CSV='/cics/cics61/srrCEMT.csv'
// SET LOGSTRM=DFHSECR.STREAM.NAME
// SET HLQ=IBMUSER.GM02.CTS61BT.CICS
//*******************************************************************
//* Ensure that CSV file is deleted without nonzero RC             *
//*******************************************************************
//CREATE   EXEC PGM=IEFBR14
//CSV      DD PATHOPTS=(ORDWR,OCREAT),
//            PATHMODE=(SIRUSR,SIWUSR),
//            PATHDISP=(KEEP,KEEP),PATH='&CSV'
//DELETE   EXEC PGM=IEFBR14,COND=EVEN
//CSV      DD PATHDISP=(DELETE,DELETE),PATH='&CSV'
//*******************************************************************
//* Convert logstream to CSV file                                 *
//*******************************************************************
//SRR      EXEC PGM=DFHSRR,REGION=4M
//STEPLIB  DD DISP=SHR,DSN=&HLQ..SDFHLINK
//DFHSECR  DD DSNAME=&LOGSTRM.,DCB=BLKSIZE=32760,
//            SUBSYS=(LOGR,DFHLGCNV)
//DFHCSV   DD PATHOPTS=(OWRONLY,OCREAT),
//            PATHMODE=(SIRUSR,SIWUSR),
//            PATHDISP=(KEEP,DELETE),FILEDATA=TEXT,
//            RECFM=VB,LRECL=1024,BLKSIZE=32760,
//            PATH='&CSV'
//SUMMARY  DD SYSOUT=*
//RECORD   DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SORTWK01 DD UNIT=SYSDA,SPACE=(CYL,(4))
//SORTWK02 DD UNIT=SYSDA,SPACE=(CYL,(4))
//SORTWK03 DD UNIT=SYSDA,SPACE=(CYL,(4))
//SORTWK04 DD UNIT=SYSDA,SPACE=(CYL,(4))
//SYSIN    DD *
MATCHID=CEMT
/*
//*******************************************************************
```

```
//* Tag CSV file as EBCDIC data                                          *
//*******************************************************************
//TAG      EXEC PGM=BPXBATCH,PARM='sh chtag -t -c IBM-1047 &CSV'
//STDOUT   DD SYSOUT=*
//STDERR   DD SYSOUT=*
```

___**2.** From the **z/OS Explorer**, the **Remote System Explorer** perspective, the **Remote Systems** view, **right-click** on **/cics/cics61/srrCEMT.csv**, and select "Open with" "Text Editor".
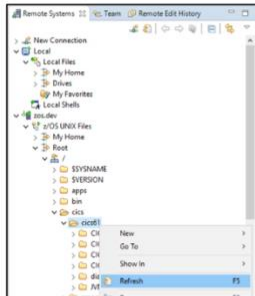
Select the /cics/cics61,
right click and refresh
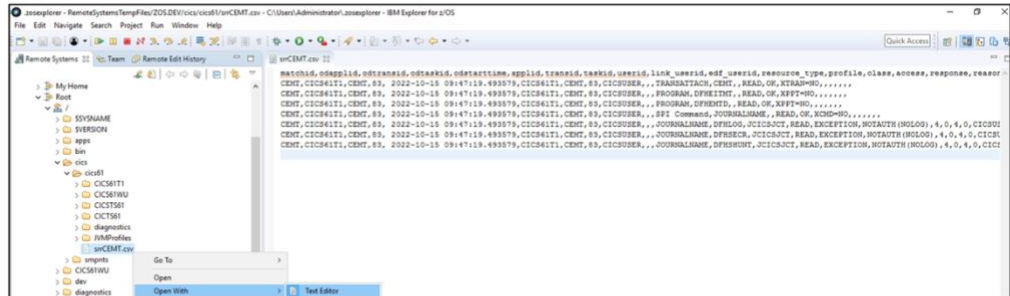
Select the file, srrCEMT.csv then, right click, Open with "Text Editor".
Check the NOTAUTH message and get the RACF class name : @@@@@@@@

___**3.** Check exception records with the **profile** and **class** information and use them for manipulating RACF commands to resolve the CEMT "Not Found" issue.

Change @@@@@@@@ to the found RACF class name and issue them in =6 menu.

```
--------------------------------------------------------------------------------
RDEFINE @@@@@@@@ DFHSECR  UACC(NONE) NOTIFY(IBMUSER)
RDEFINE @@@@@@@@ DFHSHUNT UACC(NONE) NOTIFY(IBMUSER)
RDEFINE @@@@@@@@ DFHLOG   UACC(NONE) NOTIFY(IBMUSER)

PERMIT DFHSECR  CLASS(@@@@@@@@) ID(CICSUSER) ACCESS(READ)
PERMIT DFHSHUNT CLASS(@@@@@@@@) ID(CICSUSER) ACCESS(READ)
PERMIT DFHLOG   CLASS(@@@@@@@@) ID(CICSUSER) ACCESS(READ)

SETROPTS RACLIST(@@@@@@@@) REFRESH
--------------------------------------------------------------------------------
```

Quiz 2 : What value is for @@@@@@@@?

Issue the CEMT command again

___**4.** From the **CICS region, issue the command "CEMT I JO(*)".**

```
I JO(*) _
STATUS:  RESULTS - OVERTYPE TO MODIFY
  Jou(DFHLOG  ) Mvs Ena      Str(STCSYS.CICS61T1.DFHLOG    )
  Jou(DFHSECR ) Mvs Ena      Str(DFHSECR.STREAM.CICS       )
  Jou(DFHSHUNT) Mvs Ena      Str(STCSYS.CICS61T1.DFHSHUNT  )




                                         SYSID=61T1 APPLID=CICS61T1
  RESPONSE: NORMAL                       TIME: 00.04.23  DATE: 10/06/22
PF  1 HELP        3 END        5 VAR        7 SBH 8 SFH 9 MSG 10 SB 11 SF
```

Now you can see the journal resources in the CEMT command!

Part 7: Turn on the SRR for the ODCS transaction in all CICS regions

Now it's time to resolve the ODCS transaction errors. You will define the SRR for ODCS transactions in all CICS regions because the ODCS transaction are routed to one of CICS region and connected to one FOR region.

Turn on the SRR in the CICS Explorer for a CEMT transaction

___**1.** Open the CICS Explorer and select the **CICS SM** perspective.
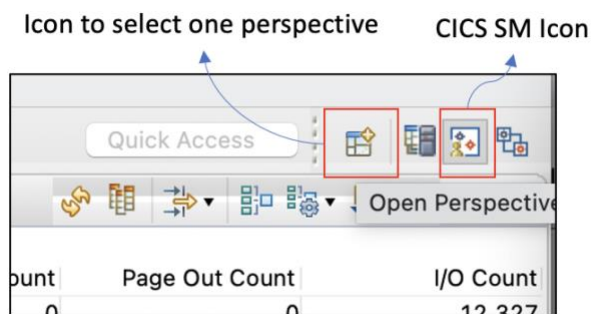
___**2.** Click "Regions" after selecting the CPSM61PX context and the Operations Menu.
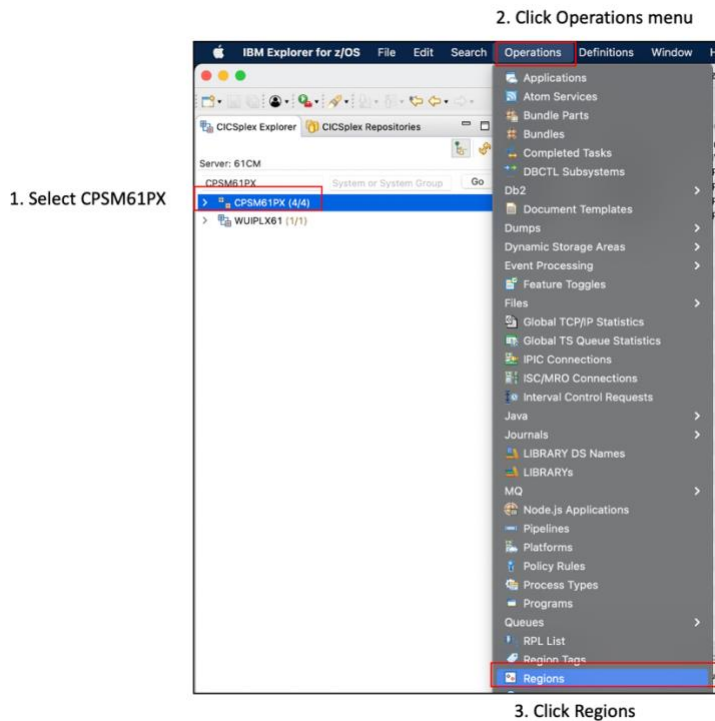
___**3.** Open a SRR session with right clicking after selecting all CICS regions.

___**4.** Put **ODCS** in the Name field, **5** in Maximum field and **CICSUSER** in the "User ID" field. Then click OK.

___**5.** Select the **Security Request Recording** menu in the **Operations** menu.

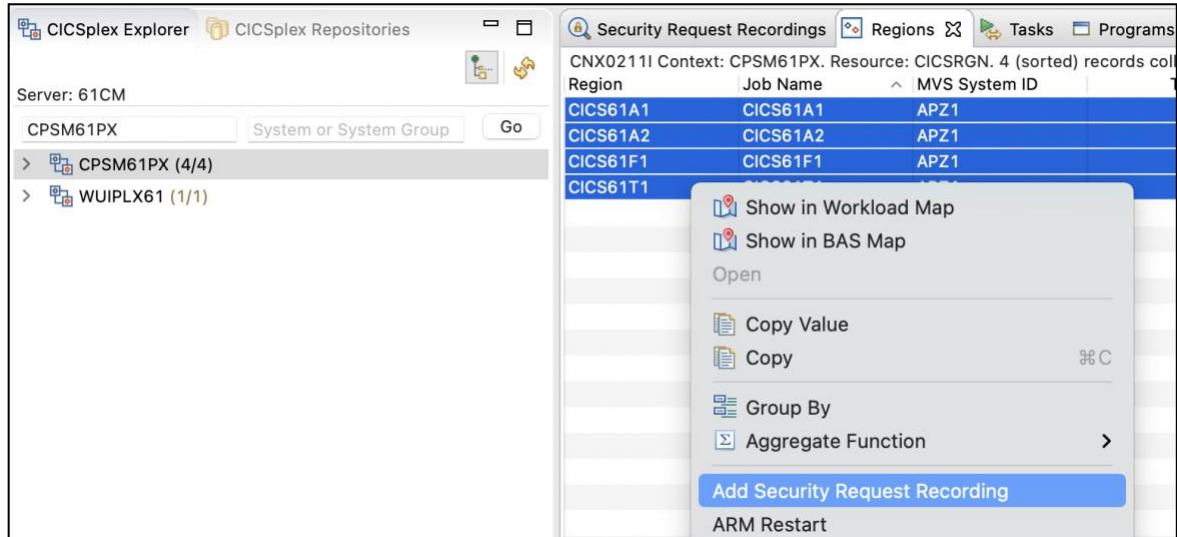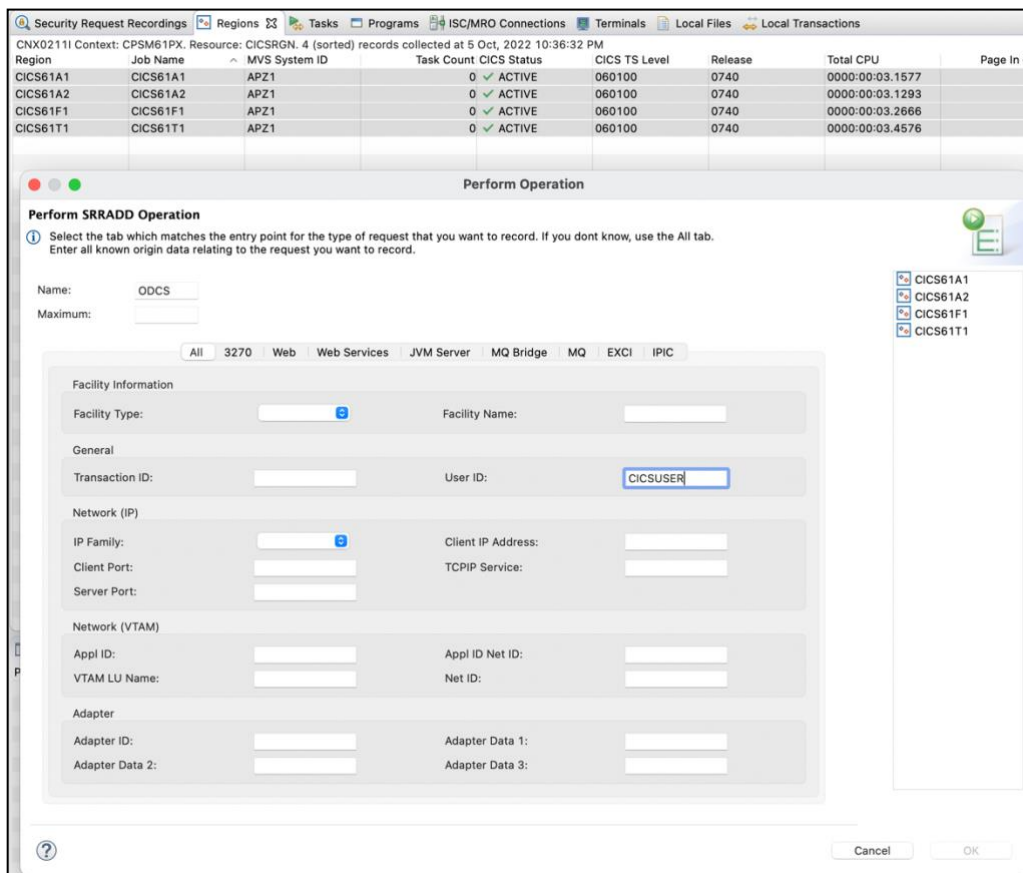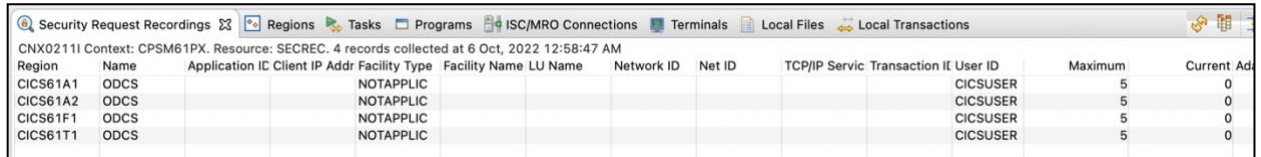| Region	Name	Application IC	Client IP Addr	Facility Type	Facility Name	LU Name	Network ID	Net ID	TCP/IP Servic	Transaction IC	User ID	Maximum	Current	Ad
CICS61A1	ODCS			NOTAPPLIC							CICSUSER	5	0	
CICS61A2	ODCS			NOTAPPLIC							CICSUSER	5	0	
CICS61F1	ODCS			NOTAPPLIC							CICSUSER	5	0	
CICS61T1	ODCS			NOTAPPLIC							CICSUSER	5	0	

CNX0211I Context: CPSM61PX. Resource: SECREC. 4 records collected at 6 Oct, 2022 12:58:47 AM

Security Request Recordings Regions Tasks Programs ISC/MRO Connections Terminals Local Files Local Transactions

Now you can see the four new records being activated for the user ID, **CICSUSER**.

___**6.** Test the inquiry process of customer number again with OMEN transaction. OMEN ➔ Select menu 1 ➔ Put 1 in the customer number field.

```
BNK1DC            CICS Bank Sample Application - Display Customer.

Provide a CUSTOMER number. Then press Enter.

CUSTOMER NUMBER  1

Sort Code
Customer Number
Customer Name
Customer Address


Customer D.O.B.     /    /
Credit Score
CS Review Date      /    /




DFHAC2206 21:06:11 CICS61T1 Transaction ODCS failed with abend AZI6. Updates
  to local recoverable resources backed out. DFHAC2261 System 61A2 sent message
  (sense code 0824089E). 'DFHAC2206 21:06:11 CICS61A2 Transaction ODCS failed
  with abend HBNK. Updates to local recoverable resources backed out.'.
```

Part 8: Check the SRR result and issue RACF commands to resolve ODCS errors

In this part of the exercise, you will check the SRR report and get information to compose RACF commands to resolve the security error of ODCS transaction.

Run the batch job to generate a CSV file and view it in the VS Code

___7. From **the TSO, run the batch JCL to extract the SRR logs and write to a CSV file.**

CICS.CICS61.JCL(DFHSRRPC)

```
//DFHSRRPO JOB CLASS=A,MSGCLASS=X,NOTIFY=&SYSUID,REGION=0M
// SET CSV='/cics/cics61/srrODCS.csv'
// SET LOGSTRM=DFHSECR.STREAM.NAME
// SET HLQ= IBMUSER.GM02.CTS61BT.CICS
//********************************************************************
//* Ensure that CSV file is deleted without nonzero RC             *
//********************************************************************
//CREATE   EXEC PGM=IEFBR14
//CSV      DD PATHOPTS=(ORDWR,OCREAT),
//            PATHMODE=(SIRUSR,SIWUSR),
//            PATHDISP=(KEEP,KEEP),PATH='&CSV'
//DELETE   EXEC PGM=IEFBR14,COND=EVEN
//CSV      DD PATHDISP=(DELETE,DELETE),PATH='&CSV'
//********************************************************************
//* Convert logstream to CSV file                                 *
//********************************************************************
//SRR      EXEC PGM=DFHSRR,REGION=4M
//STEPLIB  DD DISP=SHR,DSN=&HLQ..SDFHLINK
//DFHSECR  DD DSNAME=&LOGSTRM.,DCB=BLKSIZE=32760,
//            SUBSYS=(LOGR,DFHLGCNV)
//DFHCSV   DD PATHOPTS=(OWRONLY,OCREAT),
//            PATHMODE=(SIRUSR,SIWUSR),
//            PATHDISP=(KEEP,DELETE),FILEDATA=TEXT,
//            RECFM=VB,LRECL=1024,BLKSIZE=32760,
//            PATH='&CSV'
//SUMMARY  DD SYSOUT=*
//RECORD   DD SYSOUT=*
//SYSPRINT DD SYSOUT=*
//SYSOUT   DD SYSOUT=*
//SYSUDUMP DD SYSOUT=*
//SORTWK01 DD UNIT=SYSDA,SPACE=(CYL,(4))
//SORTWK02 DD UNIT=SYSDA,SPACE=(CYL,(4))
//SORTWK03 DD UNIT=SYSDA,SPACE=(CYL,(4))
//SORTWK04 DD UNIT=SYSDA,SPACE=(CYL,(4))
//SYSIN    DD *
MATCHID=ODCS
/*
//********************************************************************
```

```
//* Tag CSV file as EBCDIC data                                          *
//*******************************************************************
//TAG      EXEC PGM=BPXBATCH,PARM='sh chtag -t -c IBM-1047 &CSV'
//STDOUT   DD SYSOUT=*
//STDERR   DD SYSOUT=*
```

___**8.** From the **z/OS Explorer**, the **Remote System Explorer** perspective, the **Remote Systems** view, refresh and **right-click** on **/cics/cics61/srrODCS.csv**, and "Open with" "Text Editor". Then, check the RACF class name in a NOTAUTH exception message.
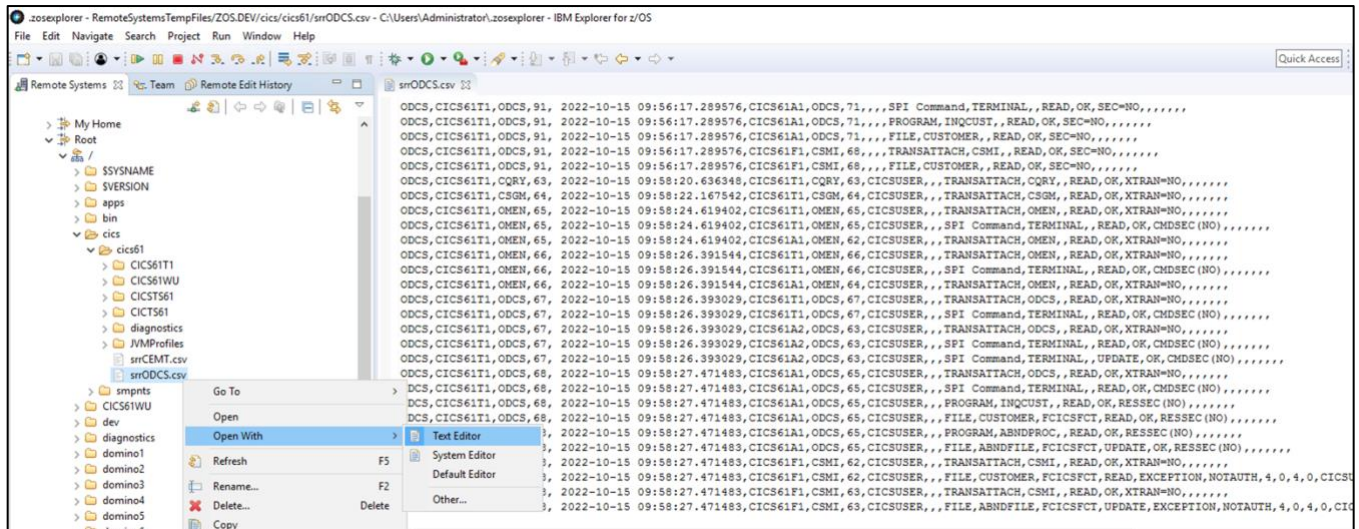
___**9.** Check exception records with the **profile** and **class** information and use them for manipulating RACF commands to resolve the transaction abend.

Change @@@@@@@@ and ######## to the RACF resource names and issue them in =6 menu.

RDEFINE @@@@@@@@ (CBSAFILE) UACC(NONE)
ADDMEM(ABNDFILE, ACCOUNT, ACCTCUST, CUSTOMER, PROCTRAN, REJTRAN)
 NOTIFY(IBMUSER)

PERMIT CBSAFILE CLASS(@@@@@@@@) ID(CICSUSER) ACCESS(UPDATE)
SETROPTS RACLIST(########) REFRESH

Check the link to find out file class names for group definition and refresh:
https://www.ibm.com/docs/en/cics-ts/6.1?topic=reference-summary-racf-classes-cics-resources

Quiz 3 : What values are for @@@@@@@@ and ########?

Test the customer inquiry process

___**10.** Test the inquiry process of customer number again with OMEN transaction. OMEN ➔ Select menu 1 ➔ Put 1 in the customer number field.

Don't use lower character for the "**OMEN**" transaction. Please use capital letters for all transactions. It's because the application abend couldn't change the UCTran attribute back to normal for your terminal.

```
BNK1DC           CICS Bank Sample Application - Display Customer.

Provide a CUSTOMER number. Then press Enter.

CUSTOMER NUMBER 0000000001

Sort Code        987654
Customer Number  0000000001
Customer Name    Dr Zsa G Higins
Customer Address 74 Joshua Mews, Portsmouth
                 test

Customer D.O.B.  22 / 02 / 1941
Credit Score     516
CS Review Date   01 / 10 / 2022




Customer lookup successful. <PF5> to Delete. <PF10> to Update.
F3=Exit    F12=Cancel
```

Now you can see the information of customer number, 1!

Part 9: Summary

Congratulations, you have resolved security errors by using the Security Request Recording function in CICS V6.1.

In this lab you performed the following steps:
- Configure the Security Request Recording function in CICS V6.1.
- Activate the recording for a transaction or for a user.
- Generate the CSV report and view it in the CSV extension of VS Code.
- Find out RACF resources to manipulate commands.
- Resolve the security issues!

Answers of Quizzes

Quiz 1 : What values should replace ##### and @@@@@ in the above JCL?

(#####.STREAM.@@@@@) ➔ (DFHSECR.STREAM.MODEL)

Quiz 2 : What value is for @@@@@@@@?

@@@@@@@@ ➔ JCICSJCT

Quiz 3 : What values are for @@@@@@@@ and ########?

@@@@@@@@ ➔ HCICSFCT, ######## ➔ FCICSFCT