

# Simple zSecure CARLa Code for Powerful Results - Lab -

Mark S Hahn  
IBM

March 12, 2012  
Session Number 10341



Visit [www.SHARE-SEC.com](http://www.SHARE-SEC.com)  
for more information on  
the SHARE Security &  
Compliance Project

## Trademarks

The following are trademarks of the International Business Machines Corporation in the United States and/or other countries.

- z/OS
- RACF

\* Registered trademarks of IBM Corporation

**The following are trademarks or registered trademarks of other companies.**

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

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

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.  
All other products may be trademarks or registered trademarks of their respective companies.

### Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the 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.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.



## Scope of Lab



Show how

- Get started
- Write programs
- Panels can be used to build reports
- Use panels to prototype reports
- Find fields of interest
- Capture built programs and jobstreams



## Lab Userids



- We have
  - SHARC26
  - SHARC27
  - SHARC28
  - SHARC29
  - SHARC30
- Password is firstpw





## Setup



- Build and populate CKFREEZE
  - Already done for you –  
'SHARE.ZSEC12.C2POLICE.CKFREEZE'
- Optional
  - Build and populate RACF Unload
    - Some restrictions apply – beyond scope of course
- Working papers
  - Use RESULTS for reports
  - Use PRT for displays



## Getting Started



- CO.C – Command > Command
  - Type your program
- Basic CARLa program
  - NEWLIST TYPE=
  - SELECT and/or EXCLUDE
  - (SORT) LIST
- GO (command line)
  - Run your program





## Getting Started – Selecting Datasets



- SE.1 (or setup files)
- Select  
Active backup RACF data base and live SMF data sets
- PF3 back to main menu



## Sample RACF



- NEWLIST TYPE=RACF
  - SELECT SEGMENT=BASE AND (OPERATIONS OR SPECIAL OR AUDITOR)
  - SORTLIST KEY(8) NAME SPECIAL OPERATIONS AUDITOR
- NEWLIST TYPE=RACF TITLE='2 Privileges'
  - SELECT SEGMENT=BASE SPECIAL OPERATIONS
  - SELECT SEGMENT=BASE SPECIAL AUDITOR
  - SELECT SEGMENT=BASE AUDITOR OPERATIONS
  - SORTLIST KEY(8) NAME SPECIAL OPERATIONS AUDITOR
- NEWLIST TYPE=RACF EMPTYLIST='No one with all 3'
  - SELECT SEGMENT=BASE AUDITOR OPERATIONS SPECIAL
  - SORTLIST KEY(8) NAME SPECIAL OPERATIONS AUDITOR





## Sample SMF



```
Newlist TYPE=SMF emptylist='No violations'
Select event=violation

Sortlist Name Jobname time(5) date(5) eventdesc
```

```
***** Top of Data *****
S M F   R E C O R D   L I S T I N G       9Mar12 21:07 to   9Mar12 21:59

Full Name           Jobname  Time  Date  Event description
MARK S HAHN         ZSEC00A  21:59  9Mar  Resource access (Failure:Profile requi
SHARE USER          SHARA01  21:07  9Mar  Resource access (Failure:Insufficient
***** Bottom of Data *****
```



## Using Panels to Prototype



```
zSecure Admin+Audit for RACF - RACF          0.0 s CPU, RC=8
Command ==>                                start panel

      Add new general resource profile or segment

Show general profiles that fit all of the following criteria
Class name . . . . XFACILIT      (class or filter)
Resource profile .

Owned by . . . . .      (group or userid, or filter)
Installation data .      (substring or *)

Additional selection criteria
  Profile fields      Access list      Segment presence      Absence
Output/run options
  Show segments      All      Enable full ACL      Specify scope
/ Summarize by class
  Print format      Customize title      Send as e-mail
    Background run      Full detail form      Sort differently      Narrow print
    Print ACL      Resolve to users      Incl operations      Print names
```





# Using Panels to Prototype



```

zSecure Admin+Audit for RACF General resource overvie  0 s elapsed, 0.0 s CPU
Command ==> Scroll==> CSR
Class XFACILIT                                     9 Mar 2012 22:44
  Class      Profile key                          T  UACC      Owner      S/F W
XFACILIT CKF.ADMIN                                NONE   ZSEC00A    R
XFACILIT CKF.AUDIT                                NONE   ZSEC00A    R
XFACILIT CKR.READALL                              NONE   JACK       R
XFACILIT C4R.DATASET.ACL./GROUP.**                 G UPDATE  SYSPROG    R
XFACILIT C4R.DATASET.TYPE.DISCRETE.**              G UPDATE  SYSPROG    R
XFACILIT C4R.DATASET.UACC.NONE.**                 G UPDATE  SYSPROG    R
XFACILIT C4R.DATASET.UACC.READ.**                 G UPDATE  SYSPROG    R
XFACILIT C4R.DATASET.UACC.**                       G UPDATE  SYSPROG    R
XFACILIT C4R.EXEMPT                               UPDATE    SYSPROG    R
XFACILIT C4R.USER./DFLTGRP.**                      G UPDATE  SYSPROG    R
XFACILIT C4R.USER./OWNER.**                       G UPDATE  SYSPROG    R
XFACILIT C4R.USER./PASSWORD.**                   G UPDATE  SYSPROG    R
XFACILIT C4R.USER.NAME.**                        G UPDATE  SYSPROG    R
XFACILIT C4R.USER.OMVS.UID.0000000000.*.*        G UPDATE  SYSPROG    R
XFACILIT C4R.USER.PASSWORD.=DFLTGRP              UPDATE    SYSPROG    R
XFACILIT C4R.USER.PASSWORD.=USERID              UPDATE    SYSPROG    R
XFACILIT C4R.*./UACC.**                           G UPDATE  SYSPROG    R
XFACILIT C4R.*.ATTR.WARNING.**                   G UPDATE  SYSPROG    R
XFACILIT C4R.*.INSTDATA.**                       G UPDATE  SYSPROG    R
XFACILIT HZS.SI.QUERY                             READ     STEVEM     R
  
```



```

zSecure Admin+Audit for RACF - RACF                0.0 s CPU, RC=8
Command ==> Results                                start panel

  Add new general resource profile or segment

Show general profiles that fit all of the following criteria
Class name . . . . XFACILIT      (class or filter)
  
```

```

Enter a selection in front of a highlighted line below:
SYSPRINT  messages
REPORT    printable reports
CKRTSPRT  output from the last TSO command(s)
CKRCMD    queued TSO commands
CKR2PASS  queued commands for zSecure Admin+Audit for RACF
COMMANDS  zSecure Admin+Audit for RACF input commands from last query
SPFLIST   printable output from PRT primary command
OPTIONS   set print options
  
```





## Customize the prototype (save it)



```
EDIT          ZSEC00A.CKRCARLA.CNTL(@ZSEC00A) - 01.00          Columns 00001 00072
Command ==>                               Scroll ==> CSR
***** ***** Top of Data *****
=NOTE= Enter GO or RUN to execute commands, SUB or SUBMIT to generate batch job
=NOTE= CREATE or REPLACE to save these commands in your own dataset
000001 n      i=base n=baserd required allowrestrict t=:tl nodetailinherit,
000002      helppanel=c2rt3rtd detailhelppanel=c2rt3rde,
000003      sumhelppanel=c2rt3rsd nosuminherit,
000004      st="Class XFACILIT"
000005      def singledsn("Only one data set per volume",flag,p) boolean,
000006      where(singleds)
000007      s c=general and s=base c=XFACILIT
000008      define _cnt_Profiles("Profiles") count
000009      define _cnt_DiscreteProfiles("Discrete") count where discrete
000010      . . . . .
```



## Capture For Later Batch Run



- Return to selection panel
- Select Print format
  - And if available: Background run
  - If not, ENTER, PF3 twice and then select Background run
- Select option 2 (edit JCL)
- Save it off





## Find Your Own Fields to Report



- COMMAND line:
  - FIELDS

```
zSecure Admin+Audit for RACF Display Selection      0 s elapsed, 0.0 s CPU
Command ==>                                         Scroll==> CSR
```

```

Name      Summary Records Title
BUILTIN    60      2854 Builtin field definitions by newlist type
TEMPLATE    1      535 RACF template definitions
***** Bottom of Data *****
```



## Select FIELDS > BUILTIN



- BUILTIN

```
Builtin field definitions by newlist type      Line 41 of 60
Command ==>                                   Scroll==> CSR
                                           9 Mar 2012 22:14
```

Type	T2	Fields	Rpt	Mod	Sub	Trn	Tag
RACF	RC	553	127	201	44		1
RACF_ACCESS	RA	21	1	1			61
ROUTER	RT	13					13
SETROPTS	IO	83		60			9
SETROPTS_CLASS	IC	20	1	9			11
SMF	SM	386	125				5
SMFOPT	SO	29	11				18
SPT	SP	12					17
SUBSYS	SS	47	15				26
SVC	SV	64	17				25
SYSTEM	SY	460	44	60			8
TEMPLATE	TM	36					10
TRUSTED	TR	20					56
UNIX	UN	59	6				55
VSM	VM	11					29
ZSECNODE	ZN	27					75









## Audit > Verify



- Very useful
- Beyond scope of this lab
- How to fix missing CKFREEZE dataset Setup Files (se.1)



## Summary



- Scope of Lab
- Introduction to zSecure Audit and zSecure Admin
- Use of panels to prototype code
- Finding FIELDS to report on
- Pieces of the audit puzzle
- Hands on
- Summary





