



IBM Security zSecure Suite: Getting started with CARLa

White Paper

July 2011

Ori Pomerantz
orip@us.ibm.com

© Copyright IBM Corp. 2011. All Rights Reserved.

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

IBM, the IBM logo, and ibm.com are 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.

Trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

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.

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

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

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

UNIX is a registered trademark of The Open Group 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.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

References in this publication to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth, savings or other results.

Table of contents

Introduction	1
Acknowledgements	1
Audience	1
1 Running CARLa Reports	2
2 Reporting on groups	3
2.1 Report	3
2.2 Explanation	3
2.3 Result	4
3 Formatting and selecting specific profiles	5
3.1 Report	5
3.2 Explanation	5
3.3 Result	6
4 Reporting fields from multiple profile segments	7
4.1 Report	7
4.2 Explanation	7
4.3 Result	8
5 Reporting fields from multiple profiles	9
5.1 Report	9
5.2 Explanation	9
5.3 Result	10
6 Creating reports that use ISPF	11
6.1 Report	11
6.2 Explanation	11
6.3 Result	12

7 Learning from system reports	13
8 Automating administration	14
8.1 Selecting the current state as input	14
8.2 Identifying inactive accounts	15
8.2.1 Report	15
8.2.2 Explanation	15
8.3 Creating the RACF commands	16
8.3.1 Report	16
8.3.2 Explanation	16
8.4 Running the RACF commands	17
References	19
Guides	19
Training	19

Introduction

CARLa is the main reporting engine that is used within IBM Security zSecure. This white paper shows you how to customize reports within IBM Security zSecure to ease auditing and administration for central security personnel.

For more information about this subject, see the Redbook *z/OS Mainframe Security Audit Management using IBM Tivoli zSecure*, Appendix B.

Additional information is available in chapters 12 and 13 of *IBM Security zSecure Admin and Audit for RACF*. If you do not have access to the IBM network to obtain a copy of this book, send an email to tivzos@us.ibm.com.

The best method to learn CARLa is to take the class, *IBM Tivoli zSecure CARLa Auditing and Reporting Language (TK231)*. This white paper is intended as a stop-gap measure to help professionals who have not had the opportunity to take the class yet.

Acknowledgements

I would like to acknowledge the Help to Tom Zeehandelaar and Mark Hahn in writing this white paper. Any remaining errors are my own.

Audience

This paper is for implementers, auditors, and administrators who use zSecure to produce security-related reports.

1 Running CARLa Reports

Follow these steps to run a CARLa report:

1. Start the IBM Security zSecure user interface.
2. Type **CO** to run CARLa commands.
3. Type **C** to type a command and run it immediately.
4. Type a CARLa report in the multiline text area. An example of a report is in the next section.
5. Enter the command **GO**.
6. After you see the report output, click F3 twice to return to the report area.



Tip: You can see a demonstration of these steps in an IBM Education Assistant module that is available at the following website:

```
http://publib.boulder.ibm.com/infocenter/ieduasst/tivv1r0/  
index.jsp?topic=/com.ibm.iea.zsec/zsec/1.11/audit/  
run_carla_report/run_carla_report_viewlet_swf.html
```

2 Reporting on groups

This section shows a simple report with all the entities of a particular type, in this case, groups.

2.1 Report

To report on groups, run this CARLa report:

```
newlist type=RACF
      select class=group segment=base
      sortlist key connects
```

2.2 Explanation

To interpret the lines in the report, look at each line.

```
newlist type=RACF
```

This line tells the CARLa interpreter to start a new report. This line also indicates that the report is based on RACF information.

```
      select class=group segment=base
```

This line selects a group report. By default, a CARLa RACF report contains one line for each segment of each profile of the selected type. Here, **segment=base** specifies that only base segments are selected. Groups are displayed once even if they have multiple segments.

By default reports show all the entities of a particular type.

```
      sortlist key connects
```

The list includes the following fields and their order:

- **key**: The name of each profile.
- **connects**: The users connected to each group. This field includes the user ID, the user authorization level to the group, any special authorizations, and additional fields.

2.3 Result

The resulting report contains groups and the users within them, similar to Figure 1.

```

BROWSE - ORI.C2R1FD8.REPORT ----- LINE 0000 0.1 s CPU, RC=0
COMMAND ==> _ SCROLL ==> 0001
***** Top of Data *****
P R O F I L E   L I S T I N G   20 May 2011 15:17

Profile  User/Grp Auth      R SOA AG Uacc      Revokedt      Resumedt
ADB210
ADB610
ADCD
ADMIN    FIN1      USE                NONE
         FIN2      USE                NONE
         ADM2      USE                NONE
         ADM1      USE                READ
ADSM
AJV
AJV118

```

Figure 1: Groups and connected users report

3 Formatting and selecting specific profiles

In this section, you learn how to format reports. You also learn how to select specific profiles instead of producing a full report on all the entities of a particular type.

3.1 Report

This CARLa report shows you how to select specific profiles and how to format the output.

```
newlist type=RACF tt='top title',
        title='Second line title, which can be longer'
select class=group segment=base mask=om*
sortlist creadate key(8,'GroupID')
```



Note: Most of this report is identical to the previous one. The parts in **bold** are new.

3.2 Explanation

This is the explanation of the CARLa code:

```
newlist type=RACF tt='top title',
        title='Second line title, which can be longer'
```

The comma specifies that the next value is still part of the **newlist** line.

```
select class=group segment=base mask=om*
```

This line selects a group report. The **mask** keyword limits the groups to those groups whose names start with **OM**.

```
sortlist creadate key(8,'GroupID')
```

The list is sorted by group creation date, followed by the key. The key is displayed in eight characters (space padded if there are fewer than eight characters), and the column is titled **GroupID**.

3.3 Result

The resulting report is similar to Figure 2, if your system has any groups that start with OM.

```
***** Top of Data *****
top title 20 May 2011 16:03
Second line title, which can be longer

CreateDate GroupID
 8 Jun 1995 OMVSGRP
22 Apr 2008 OMVS
22 Apr 2008 OMVSCONN
***** Bottom of Data *****
```

Figure 2: Second group report

4 Reporting fields from multiple profile segments

In this section, you learn to combine fields from multiple segments of the same profile.

4.1 Report

This CARLa report shows how to combine fields from multiple segments of the same profile:

```
newlist type=RACF
  select class=user segment=omvs uid>0
  sortlist uid(5) key(8) :tcommand
```

4.2 Explanation

This is the explanation of the CARLa code:

```
newlist type=RACF
  select class=user segment=omvs uid>0
```

This report displays user information. The **segment=omvs** specifies to the CARLa interpreter to search for information in the OMVS segment of the user profile. This segment contains information related to the UNIX subsystem. The **uid>0** restricts the report to users with a UNIX UID of more than zero (those users who do not have root permissions).

```
sortlist uid(5) key(8) :tcommand
```

This line specifies the information included in the report: the UNIX user ID, the z/OS user ID, and **:tcommand**. The colon (:) specifies that the field searched is in a different segment. The **tcommand** field is the default TSO command, part of the TSO segment.

4.3 Result

If you have users with OMVS accounts, your result is similar to Figure 3. As you can see, the command field is not an OMVS command, but a TSO command.

```
***** Top of Data *****
P R O F I L E   L I S T I N G   28 Apr 2011 16:53

Uid   Profile  Command
  1 CRMBHJ1  INIT#FB CLPFX(CRMBHJ1)
  1 UNIXMAP1
  2 CRMBMR3
  2 SMFTS19
  2 SMFTS20
 50 RCCSLIN  INIT#FB CLPFX(CRMBERT)  clib(ispf.ispclub)
101 USER1   ispf
102 USER2
103 USER3
104 USER4
105 USER5
110 CRMBERT  INIT#FB CLPFX(CRMBERT)  plib(ispf.ispclub)
```

Figure 3: User report that uses multiple segments

5 Reporting fields from multiple profiles

In this section, you learn to combine fields from different profiles.

5.1 Report

This CARLa code shows how to combine fields from different profiles.

```
newlist type=RACF
  select class=dataset segment=base
  sortlist key(20,'DS profile') creadate(10,'DS date'),
  owner owner:creadate(10,'Owner date')
```

5.2 Explanation

This is the explanation of the CARLa code:

```
newlist type=RACF
  select class=dataset segment=base
```

This report displays information from data set profiles.

```
sortlist key(20,'DS profile') creadate(10,'DS date'),
```

The profile name in this report is 20 characters long. Longer profile names are truncated.

```
owner owner:creadate(10,'Owner date')
```

The **owner** is the user or group that owns the data set profile. This value is part of the data set profile. The value, **owner:creadate**, is the creation date of that owner profile. You can use the same syntax (**owner:<field>**) to specify other fields. For example, **owner:uid** gives the OMVS user ID of the owner, in case it is a user with an OMVS segment.

5.3 Result

In this report, you see the data set profiles in the RACF database, their creation dates, the names of their owners, and the creation dates of the owner profiles. An example is shown in Figure 4.

```

***** Top of Data *****
P R O F I L E   L I S T I N G   28 Apr 2011 17:15

DS profile           DS date   Owner    Owner date
ADB210.*.**          21Jan2005  ADB210   19Jul2002
ADB610.*.**          21Jan2005  ADB610   26May2000
ADCD.*.**            21Jan2005  ADCD     19Jul2002
ADM1.**              21Jan2005  ADM1     07Sep2001
ADSM.*.**            21Jan2005  SYS1     07Jul2003
AJV.*.**             21Jan2005  AJV      07Sep2001
AJV118.*.**          21Jan2005  AJV118   07Sep2001
ANF.*.**              21Jan2005  SYSAUTH  24Jul2001
ANF.SANFLOAD         21Jan2005  SYSAUTH  24Jul2001
AOP.*.**              21Jan2005  SYSAUTH  24Jul2001
AOX.*.**              21Jan2005  AOX      01Dec2004

```

Figure 4: Report that uses information from multiple profiles

6 Creating reports that use ISPF

In this section, you learn to create reports that use ISPF. These reports show a summary, and users can expand lines to see additional details.

6.1 Report

This CARLa reports shows how to create a report that uses ISPF.

```
newlist type=RACF
  select class=dataset segment=base
  display key(20,'DS profile') creadate(10,'DS date'),
  owner(detail) owner:creadate(10,'Owner
date',detail)
```

6.2 Explanation

This is the explanation of the CARLa code:

```
newlist type=RACF
  select class=dataset segment=base
  display key(20,'DS profile') creadate(10,'DS date'),
```

The **display** command creates an ISPF report.

```
  owner(detail) owner:creadate(10,'Owner
date',detail)
```

The **detail** display modifier in a **display** command specifies fields that belong in the detail screen when the user selects a specific entry.

6.3 Result

The initial result contains only the data set profile name and the creation date, as shown in Figure 5.

```

IBM Security zSecure RACF display                                0 s elapsed, 0.1 s CPU
Command ==> _____ Scroll==> PAGE
                                                    28 Apr 2011 17:37

   DS profile           DS date
  ___ ADB210.*.**        21Jan2005
  ___ ADB610.*.**        21Jan2005
  ___ ADCD.*.**         21Jan2005
  ___ ADM1.**           21Jan2005
  S AD SM.*.**         21Jan2005
  ___ AJV.*.**          21Jan2005
  ___ AJV118.*.**       21Jan2005
    
```

Figure 5: ISPF report

To view the details for a particular data set profile (in this case, the owner and the owner creation date), type **S** beside that profile. This action gives a details report, similar to Figure 6.

```

IBM Security zSecure RACF display                                Line 1 of 1
Command ==> _____ Scroll==> PAGE
                                                    28 Apr 2011 17:37

   DS profile           DS date
   AD SM.*.**          21Jan2005
   Owner      Owner date
  _ SYS1      07Jul2003
***** Bottom of Data *****
    
```

Figure 6: ISPF report detail

7 Learning from system reports

One method to learn programming languages is to look at existing programs. The zSecure user interface contains several CARLa programs. In this section, you learn how to view the CARLa code for existing reports.

First, create a report. If the report is in print format, press F3 to view the results panel. If it is in ISPF format, press F3 and type the command **results** to view the results panel. Then, select to view the COMMANDS file. It contains the CARLa code that produced the report, as shown in Figure 7.

```
000001 n  n=baser0 segment=base required allowrestrict,
000002 ,
000003 ll=79 tt="RACF class ",
000004 st="All profiles"
000005 def singledsn("Only one data set per volume",flag,p) boolean,
000006 where(singleds)
000007 s c=general and s=base
000008 sortlist class(tt,page) " - complex"(tt,page) complex(tt,page),
000009 stamp(tt),
000010 ,
000011 searchkey(nd) key(31,wrap) proftype(1) | warning(1,hb),
000012 uacc owner auditlvl gauditlvl(allowrestrict),defdate(7,"Created"),
000013 notify(7) auditpriority,
000014 / " *"(ne) | idstar,
000015 / " Level: "(notempty) no0level(hor,0),
000016 / " Volser: "(notempty) volser(63,hor,ww),
000017 / , " Data: "(notempty) instdata(63,wrap),
```

Figure 7: CARLa for a system report about general resource profiles



Note: Keywords can be shortened in CARLa. For example, line 7 is equivalent to this line:

```
select class=general and segment=base
```

8 Automating administration

In addition to producing reports, CARLa can produce commands to automate various administrative tasks. This section shows how to automatically disable unused accounts.

8.1 Selecting the current state as input

With zSecure, you can produce reports on the current state or on historical data. To produce commands that relate to the current state, follow these steps:

1. Type the command `=SE.1` to specify the source of information for zSecure.
2. Type `S` beside the active backup RACF database. Type `U` beside any other input files that are currently selected.

```

zSecure Admin+Audit for RACF - Setup - Row 1 from 15
Command ==> _____ Scroll ==> CSR
(Un)select (U/S) set of input files or work with a set (B, E, R, I, D or F)

```

	Description	Complex	
<input type="checkbox"/>	zSecure 1.9 Audit Class	ED02	selected
<input type="checkbox"/>	zSecure 1.9 Basic Classes	ED02	selected
<input type="checkbox"/>	Active backup RACF data base and live SMF data sets	ED02	



Tip: You can use the primary RACF database. However, in many installations the backup database is preferable.

8.2 Identifying inactive accounts

8.2.1 Report

To identify inactive accounts, run this CARLa report:

```
newlist type=RACF nopage
      select class=user last_connect_date<TODAY-90
not (revoked) ,
      segment=base
list key
```

8.2.2 Explanation

This is the explanation of the CARLa code:

- **nopage**: This keyword instructs CARLa not to produce page titles, column titles, page numbers, and other formatting characters.
- **last_connect_date<TODAY-90**: This expression restricts the user list to those users who have not connected in the last 90 days.
- **not(revoked)**: This expression restricts the list to users who are not currently revoked.
- **segment=base**: This value is for looking only at the base segments of user profiles. Otherwise, the report includes inactive users multiple times, one for every segment in the profile.
- **list**: This command produces an unsorted list, in contrast to **sortlist**. Not sorting saves the processing cost of sorting the list. The **list** command also suppresses the column titles and page numbers, leaving only the report title, which is suppressed here by **nopage**.

8.3 Creating the RACF commands

8.3.1 Report

The RACF command to revoke a user is:

```
altuser <user ID> revoke
```

This report generates these commands:

```
newlist type=RACF nopage file=ckrcmd
      select class=user last_connect_date<TODAY-90
not(revoked),
      segment=base
list "altuser" key(0) "revoke"
```

8.3.2 Explanation

This is the explanation of the CARLa code:

- **file=ckrcmd**: Sends the output to CKRCMD, the default command file created by CARLa.
- **"altuser"** and **"revoke"**: These strings are displayed in the output unchanged.
- **key(0)**: This keyword specifies the profile key, the user ID, without any padding with spaces. Padding improves readability for human tasks, but it is not useful for RACF commands.

8.4 Running the RACF commands

Generate and run the RACF commands using these steps:

1. Run the CARLa report. The result is a list of commands.

```

EDIT          ORI.C2R1FD8.CKRCMD                      Columns 00001 00072
Command ==> _____ Scroll ==> 0001
Press PF3, enter R at the cursor location, press ENTER to run these commands
==MSG> -Warning- The UNDO command is not available until you change
==MSG> your edit profile using the command RECOVERY ON.
000001        /* CKRCMD file CKR1CMD complex ED02 generated 20 May 2011 16:45
000002        altuser AAAA revoke
000003        altuser APPC revoke
000004        altuser AUT01 revoke
000005        altuser AUT02 revoke
000006        altuser CICSA revoke
000007        altuser CNG240X revoke
000008        altuser CNG250X revoke
000009        altuser CNMCSSIR revoke

```

2. Press F3. The commands are in CKRCMD. Type **R** beside CKRCMD to run the commands.

Menu	Options	Info	Commands	Setup
------	---------	------	----------	-------

```

zSecure Admin+Audit for RACF - Results
Command ==> _____

The following selections are supported:
  B Browse file                S Default action (for each file)
  E Edit file                  R Run commands
  P Print file                 J Submit Job to execute commands
  V View file                  M E-mail report
  W Write file into seq. or partitioned data set

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

```

- The commands run as if you typed them manually from the TSO command line. The output is captured in a data set.

```
BROWSE      ORI.C2R1FD8.CKRTSPRT                               Line 00000 Command failed
Command ==> _____ Scroll ==> PAGE
***** Top of Data *****
=====
=== Multiple TSO command output file - scroll max down for overview ===
=== Input data set ORI.C2R1FD8.CKRCMD                               ===
=====
=== Commands for local node
=====
/* CKRCMD file CKR1CMD complex ED02 generated 20 May 2011 16:45 */

===== 20May11 16:48:34.74168 start record 2 =====
altuser AAAA revoke
C4R502E Revoke of user not allowed, command terminated
CKX962F Command failed, return code 8 (decimal)

===== 20May11 16:48:34.78397 start record 3 =====
altuser APPC revoke
C4R502E Revoke of user not allowed, command terminated
CKX962F Command failed, return code 8 (decimal)
```

References

Guides

- *z/OS Mainframe Security and Audit Management using IBM Tivoli zSecure, Appendix B*

<http://www.redbooks.ibm.com/redbooks/SG247633/wwhelp/wwhimpl/js/html/wwhelp.htm>

- *IBM Security zSecure Admin and Audit for RACF*, chapters 12 and 13

If you do not have access to the IBM network, email tivzos@us.ibm.com.

Training

- *IBM Tivoli zSecure CARLa Auditing and Reporting Language (TK231)*

http://www-304.ibm.com/jct03001c/services/learning/ites.wss/us/en?pageType=course_description&courseCode=TK231

