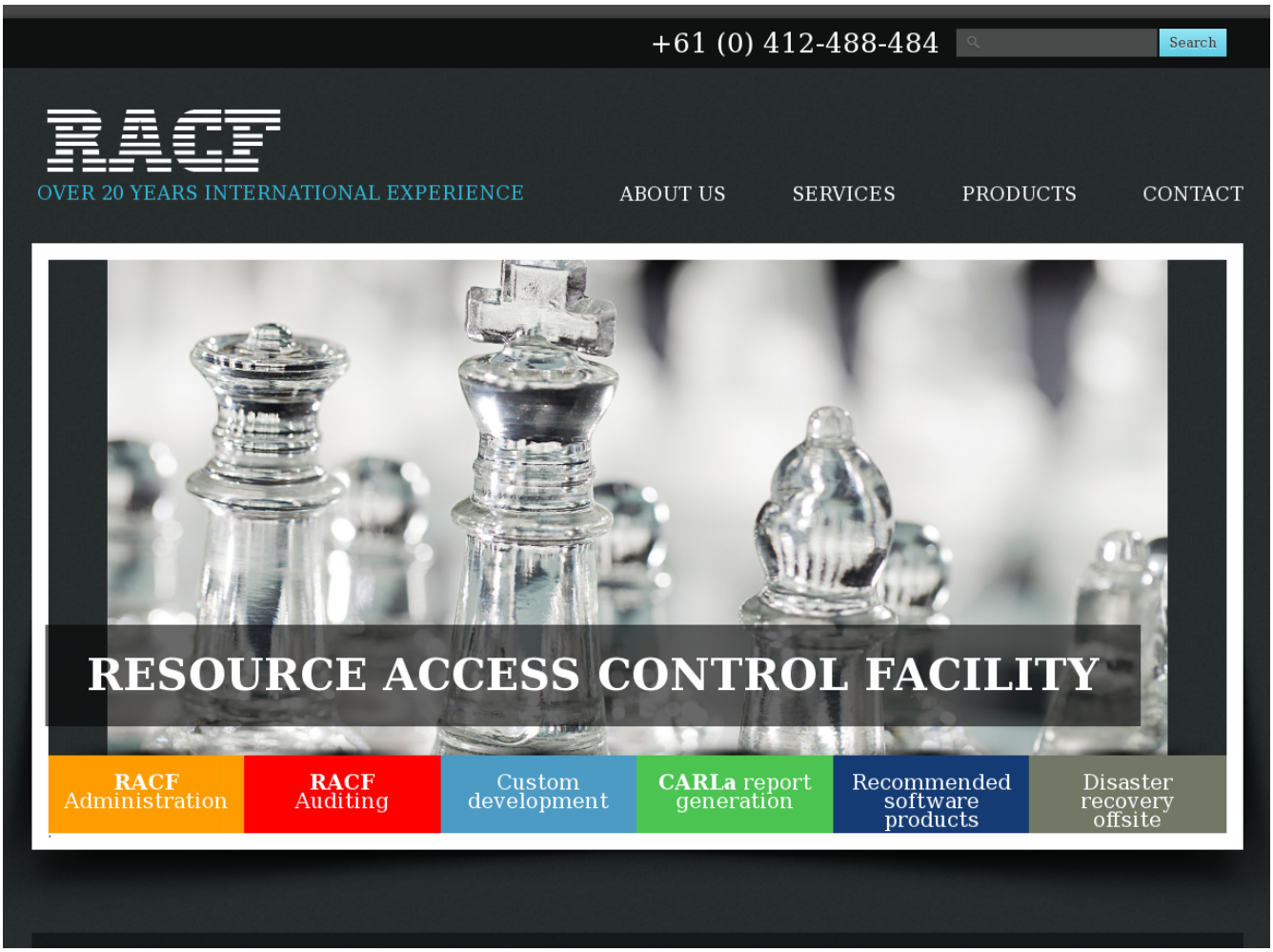
WWW.RACF.NET.AU presents:

Forget *Free Willy*, how about free RACF!

a white-paper created by Mike Cairns



For more information, contact us at info@racf.net.au or call 0412 488 484

"A review of the various freeware utilities available to help audit and administer the IBM Security Server (RACF) environment."

Forget *Free Willy*, how about free RACF!

first published February 2007 – Xephon RACF Update

Many organizations today use vendor products to assist in the management of security in the IBM mainframe system. But what do you do if, for whatever reason, your installation chooses not to implement a vendor product and you're stuck with basic IBM supplied RACF interfaces?

There is no doubt that the best-of-breed vendor tools provide a great productivity boost to the RACF administrator while helping to ensure that the RACF system is maintained effectively and securely. There will never be a real substitute for the high-end functions provided by some of these products. However, there are many freely-available tools and utilities that can substitute for much of the basic functionality of some vendor products.

In this series of articles we will discuss the pros and cons of the various commonly-used freeware tools, as well as some of the locally-developed processes that many installations choose over a purchased solution.

To start with, here's an overview of the 'problem'. RACF as provided by IBM has an ISPF panel interface that had its last major re-write for RACF 1.9 over 10 years ago now. Although the interface is functional, and continues to be enhanced to support new RACF features, many competent RACF administrators quickly discover its shortcomings when doing 'power admin', ie requiring to make many changes to RACF definitions in one pass. As a panel driven interface, one of the fundamental limitations is the restriction of only being able to view or work with one RACF profile at a time.

Say, for example, I needed to grant a specific RACF group access to many datasets. While I could use the *Search* facility and generate a CLIST of commands, that approach is limited by the available parameters of the RACF `SEARCH` command. If the list of dataset profiles I need to manipulate does not easily fall into one `SEARCH`, multiple steps will be required.

Another common example would be the need to connect many userids to a group, or many groups to a userid – similar issues present themselves. Basically the panel interface is very good at issuing one RACF command at a time; not so useful for 'power admin'.

Most of the utilities explored here fall into what I refer to as the 'offline' category of software. That is, they are primarily used away from the mainframe, on a desktop PC system, and process data extracted from the mainframe, presenting summaries and analysis of this data. Having said that though, analysis of this kind of data can be used to drive processes or generate actual RACF commands in order to implement RACF change, or 'power admin', as previously defined.

THE UTILITIES

We will compare the main functionality of three popular sets of utilities:

• Nigel Pentland's Downloads Page: http://www.racf.co.uk/

• Cory Curtis' RACF Utilities: http://home.earthlink.net/~cgcurtis/.

• And no comparison would be complete without a look at the granddaddy of them all, the ever increasing set of 'unofficial' utilities created within IBM and available from

the RACF 'goodies' page: http://www-03.ibm.com/servers/eserver/zseries/zos/racf/goodies.html.

There are far too many utilities provided just amongst these three sources to cover completely in one article. So today we will focus primarily on the RACF data side of the picture – in subsequent articles we will explore the OMVS hierarchical filesystem tools, the SMF audit tools, and the many point solutions available for other purposes.

THE PENTLAND UTILITIES

Although Nigel's current documentation provides only a change history of these tools dating back to May 2000 Release 1.00, I remember using the previous generation of text-only (now changed to HTML) output reports generated by these tools prior to that. Even then, almost 10 years ago, it was obvious that Nigel had an insight into what most RACF administrators wanted to know about their system, and how to present this in an easily digestible format.

I tested the main batch reporting function using the simplest possible set-up as documented in the 'readme.htm' on the racf.co.uk main page. If I were using these all the time in my work, I would set up a more robust set of directories for my prod, test, etc systems as recommended in the documentation – specifically for the comparison type utilities (ie RACF35) that can compare profiles from two different databases – where a directory structure is necessary:

1. Place a copy of your RACF unload file, often referred to as the 'flat file' (the output of the IRRDBU00 program), in a working directory on your PC. Use the CRLF/ASCII and text download options of your favourite mainframe file transfer program for this. This must be the 'raw' output from IRRDBU00 – no post-processing or sorting.
2. Unzip the racf.zip and reports.zip from Nigel's downloads into the same directory.
3. Place a copy of the racf.ini settings file from the downloads page into the same directory.
4. Edit the racf.ini with a text editor, update the name of the unload file from step 1, the line: input_file=your_irrdbu00_output.txt
5. Open a DOS command line window, change to your working directory, and invoke the reports.bat file.
6. Wait a while – and you're done. It's that simple.

The racf103.exe program (searching for duplicate name fields) took an extremely long time to execute and hogged my entire CPU for the duration, so go and have a few cups of coffee while you wait for the reports.bat file to finish its work – or comment it out of the reports.bat file before you run it. Nigel has done some work to reduce the CPU priority of this program in a forthcoming release, so this problem should be resolved soon. Mind you, I was running on a database containing about 30,000 userids, I certainly could never do this analysis manually, so no matter how long it takes it's better than anything else I have at my disposal. When reports.bat is complete, open up the reports.htm file in the working directory using your favourite browser and you have a comprehensive overview of the RACF database.

I'm not going to try to cover every report that the Pentland utilities can produce, Doc Farmer provided an excellent overview of these for Xephon's RACF Update in a two-part series during 2003 – see your archives if you missed it ('Pentland utilities', issues 31 and 32, February and May 2003).

What I will do instead is highlight the reports I found most useful when conducting a real audit of a production system:

• RACF03 – group structure; gives me an immediate visual representation of the group tree structure; a very handy overview.

• RACF05 – expired users; allows me to instantly assess whether we have an issue with 'dead' userids clogging up the RACF database.

• RACF24 – revoked users; same comment as RACF05 above.

• RACF32 – WARNING report; I can quickly make an assessment of whether RACF protection is really active, or just defined.

• RACF38 – general audit report; a truly great report. I can assess the scale of use and spread of the RACF user attributes SPECIAL, OPERATIONS, and AUDITOR at a glance. I can then see whether group scope via group SPECIAL is in use. I get an immediate feel for the amount of control exercised over the granting of group connections from the 'Group Connection other than USE' report. Unusual password intervals and userids with the PROTECTED, RESTRICTED, and UAUDIT attribute are always of value in forming an initial impression of a new system – even a full DSMON report gives me only some of these details.

• RACF42 – DISCRETE profile with ALTER access; this is always a great 'gotcha' for a RACF auditor and regularly finds its way into the final audit report.

• RACF59 – profiles with non-default audit attributes; always useful to see whether anything other than default auditing is in place.

• RACF65 – general resource class reports; this is run multiple times, each time against a specific resource class, and produces an HTML file called racf65.htm, which is then renamed by reports.bat to be class-name.htm. The supplied reports.bat processes 20 of the most commonly found classes of interest. I like to run this myself against any other classes I find active that represent critical system control points, eg TSOAUTH, DSNR, etc. The report presents an easily interpreted view of the profiles and their access lists. Very useful and much better than trawling around in the RACF panels or issuing TSO RACF commands.

• RACF68 – APF-authorized datasets; this report requires the output of the DSMON utility in the working directory, the supplied reports.bat expects this to be in a file named simply 'dsmon'. I found this report a little misleading because I hoped it would reveal the dataset profile protecting each APF-defined library; however, what it seems to expect is that all APF libraries have a matching fully-qualified RACF dataset profile. Now, to me, this is a good idea (that all APF libraries have matching profiles), but not a reasonable assumption. However, I appreciate the complexity of writing code to do the RACF generic pattern matching and I would be seriously surprised and impressed to see that implemented in a free utility. Still, a useful report all the same.

• RACF105 – STARTED task userids; a very useful way tolook at definitions in the STARTED class – by the associated userid rather than just the profile name.

• RACF106 – UID(0) UserIDs; again, something a proper RACF audit should always look for. Both this and the STARTED report above list the PROTECTED attribute status for all userids – a pure piece of genius that, and vital for a real understanding of the underlying security implications of these highly-privileged users.

• RACF108, 109, and 112 are all digital certificate-related. This is very useful because gaining this information from RACF directly is still quite clumsy.

AND THERE'S MORE...

So everything we just looked at was provided by simply running one '.bat' file under DOS – comprehensive, eh? And that was only my selected favourites – the supplied reports.bat currently produces a total of 63 HTML reports. But the Pentland utilities do much more as well. Nigel believes the 'jewel in the crown' (and I quote him here) to be the RACF08 and the RACF11 utilities. We'll briefly demonstrate them here. RACF08 searches the RACF unload file using fields not supported by any native RACF interface – if you're looking for a user, you've forgotten their userid, but you're certain that either their installation data or name field contained a specific string. This is the utility for you! Here's an example:

```
C:\racf\reports>racf08 mike

UserID    Name                Installation Data
------    ----                -----------------
MSMIT     MIKE SMITH
MCAIR     MICHAEL CAIRNS      MIKE.CAIRNS
MIKEC     MICHAEL CAIRNS
```

RACF11 can replicate the access of a userid, including all attributes, direct permits in access lists, etc. Don't forget that most of the Pentland utilities are case sensitive, so to clone a RACF userid, you must specify the userid in upper case on the command line to RACF11. This caught me out the first time I tried it; simply issuing RACF11 with no parameters lists the valid command line parameters and notes this issue though – very helpful.

```
C:\racf\reports>racf11 AUDIT01
Preprocessing...
Compiling list of Access...
Do you wish to enumerate the 2 connected groups? [Y/N/?]
Enumerating access for user AUDIT01 ...
Enumerating access for group MAI01 ...
Enumerating access for group STAFF ...
Parsing HTML...
-
```

```
C:\racf\reports>type racf11.jcl
//RACFPC JOB ,'PC GENERATED JCL',
// CLASS=A,
// MSGCLASS=X,
// MSGLEVEL=(1,1),
// NOTIFY=&SYSUID
//*
//RACF EXEC PGM=IKJEFT01
//SYSTSPRT DD SYSOUT=A,HOLD=YES
//SYSTSIN DD *
PROFILE NOPREFIX
ALU AUDIT01 AUDITOR
CO AUDIT01 AUTHORITY(USE) GROUP(MAI01) OWNER(MAI01)
CO AUDIT01 AUTHORITY(USE) GROUP(STAFF) OWNER(STAFF)
ALU AUDIT01 DFLTGRP(STAFF)
/*
```

CORY CURTIS' RACF UTILITIES

I first encountered Cory's utilities via the RACF-L news/discussion e-mail group. Three utilities are provided:

1. RACF Export to MS-Access.
2. SMF Export to MS-Access.
3. RACF LDAP with SSL.

I followed the instructions on the utilities homepage to first test the RACF export to MS-Access utility:

1. Download and unzip the racf.zip file to a convenient directory. This contains the Access database.
2. File transfer your current SYS1.SAMPLIB(RACDBULD) dataset to C:\temp\temp\racdbuld.txt.
3. Open the RACF.mdb Access database and run the **First time run** macro.
4. File transfer the output of the IRRDBU00 program to C:\temp\temp\racf.txt.
5. Again in the RACF.mdb database, run the **One Step Import** macro.

That's all there is to it, you can now start using the full power of a relational database to analyse your RACF data. I found the process of loading the RACF data very smooth, following these instructions I

had a RACF unload file viewable in MSAccess in less than fifteen minutes and that includes generating and downloading the IRRDBU00 output and the SAMPLIB data. Cory even provides an Access macro to help you download the data from the mainframe if needed. As with all utilities of this kind, the input data must be transferred as plain ASCII text.

You only need to re-run the **First time run** macro when operating system upgrades change the record structure of the RACF flat file. You must copy the updated RACDBULD file from SAMPLIB first, of course. You can download fresher copies of the flat file at any time and just re-run the **One Step Import** macro.

The default file locations and input file names can be altered to suit your preferences – this is done by editing the Access Macros. Although I did not try doing this, a quick look at the Visual Basic code seems to indicate that this is a fairly painless process as well. The relevant variable names for each utility are documented on Cory's pages.

The version I tested (using data from a z/OS 1.4 system) generated 72 tables, provided five default queries and four forms. I'll admit now to not being much of an MS-Access user. I tested the forms by applying some filters and can see that these could be quite useful. However, I suspect that for any serious application you would want to create forms that suit your environment, and that those provided are really meant to serve as just examples of what could be done.

Executing the supplied queries, though, immediately produced results that I was more comfortable working with. I can see that with even a little practice one could create powerful reports of the sort that the Pentland utilities provide, with the added benefit of being 'tuned' to suit your unique RACF environment and naming conventions.

THE IBM RACF GOODIES

More than a dozen utilities are available now from the IBM free tools for RACF page. Having looked at Cory's and Nigel's efforts I wanted to find something I could directly compare functionality with and selected the DBU2MSXL tool for my first test.

DBU2MSXL provides an easy way to load the RACF flat file into MS-Excel. Once again I found the process relatively painless, very similar to Cory's Export to MS-Access in fact.

First obtain the dbu2msxl.zip from the IBM page and unpack this into a directory of your choice – some subdirectories are created for you. Read the supplied PDF documentation and follow the steps described for convenience below:

1. File transfer the SYS1.SAMPLIB(RACDBULD) file to the Sql subfolder in the usual manner. You can name the file anything but the suffix must be '.sql'.
2. Go to the Scripts directory and run the scrSQLS_cre.vbs script.
3. File transfer your IRRDBU00 output file to the Irrdbu directory. Again, any name is valid but the extension must be '.txt' – I called mine 'irrdbu00.txt'.
4. Now run the Main.vbs script from your working directory (where you unpacked the .zip file).

It's as simple as that – you should now have an Excel workbook named the same as your IRRDBU00 flat file input source (except with '.xls' instead of '.txt') in your working directory – in my case, irrdbu00.xls.

As with Cory's utilities the same issues apply when you upgrade z/OS release – you must download the RACDBULD data again and re-run the scrSQLS_cre.vbs script. Fresh copies of your IRRDBU00 file can be downloaded, but only one file at a time can exist in the Irrdbu subdirectory. The utility names the resultant worksheet after the source input file, so a useful procedure might be to place a datestamp in the filename, ie irrdbu00_070228.txt or similar, thus maintaining a 'history' of your RACF database in different Excel workbooks.

One thing to watch out for is that Main.vbs deletes all Excel files in its directory – so store your files somewhere else after creation if you wish to retain more than one copy. The first thing I did after opening the workbook and examining the list of sheets (one for each record type from the flat file) was to apply data filters to the sheets I was most interested in. I could then filter the data in a manner similar to that of MSAccess.

CONCLUSIONS

One issue I find with utilities that use the sample DB2 load cards contained in RACDBULD to generate SQL or other database schemas is that the end result tables/databases are tied to IBM's rather cryptic names for each RACF flat file record type. These are well documented in the RACF Macros and Interfaces book but, to my mind, they are rather difficult to interpret for a novice RACF administrator. My preference is to try to use 'intuitive' names for the various structures found in RACF, but that of course would make the data load process more complex for utilities like these.

All in all, these are an excellent set of rapidly deployed and easy-to-use RACF reporting tools. I believe that of the three facilities reviewed the Pentland tools offer the greatest functionality 'out of the box'; however, the flexibility provided by MS-Access or Excel may give these utilities an edge, depending on your requirements. Some of Nigel's utilities provide the added benefit of producing JCL output in order to assist the RACF administrator needing 'power tools' to enhance their productivity.

In the next issue we will continue to review utilities from other sources, as well as look at some SMF and Unix HFS-related utilities.

If you need any advice about effectively exploiting your System z investment through consulting, performance measurement and management improvement, staff training etc don't hesitate to contact us at info@racf.net.au for a confidential discussion.