zSecure™ – Experiences in IBM® zPET

David Buehl
Phil Peters

z/OS® Platform Evaluation Test / Integration Test

Trademarks

Agenda

- IBM Security zSecure Suite Overview
- zSecure Components
- Review of Components we use
- Basic Panels
- Summary

IBM Security zSecure Suite - Overview

- The IBM Security zSecure Suite is a mainframe security administration, compliance and audit family of solutions.
- Formerly IBM Tivoli zSecure Suite
- http://www.ibm.com/software/tivoli/products/zsecure/
- Simon Dodge NYRUG 10/2009 http://www.stuhenderson.com/Handouts/Leveraging_zSecure_NYRUG_2009Oct.pdf

zSecure components

- **Security zSecure Admin ***
  - **Adds a user-friendly layer over RACF® to help improve administration and reporting**

- **Security zSecure Audit for ACF2**
  - **Enables analysis and reporting on mainframe security events (ACF2), auditing detects exposures**

- **Security zSecure Audit for RACF ***
  - **Enables analysis and reporting on mainframe security events (RACF), auditing detects exposures**

- **Security zSecure Audit for Top Secret**
  - **Enables analysis and reporting on mainframe security events (TSS), auditing detects exposures**

zSecure components

- **Security zSecure Alert for ACF2**
  - **Can detect/prevent intrusions and identify misconfigurations through real-time mainframe (ACF2) threat monitoring**
- **Security zSecure Alert for RACF**
  - **Can detect/prevent intrusions and identify misconfigurations through real-time mainframe (RACF) threat monitoring**

zSecure components

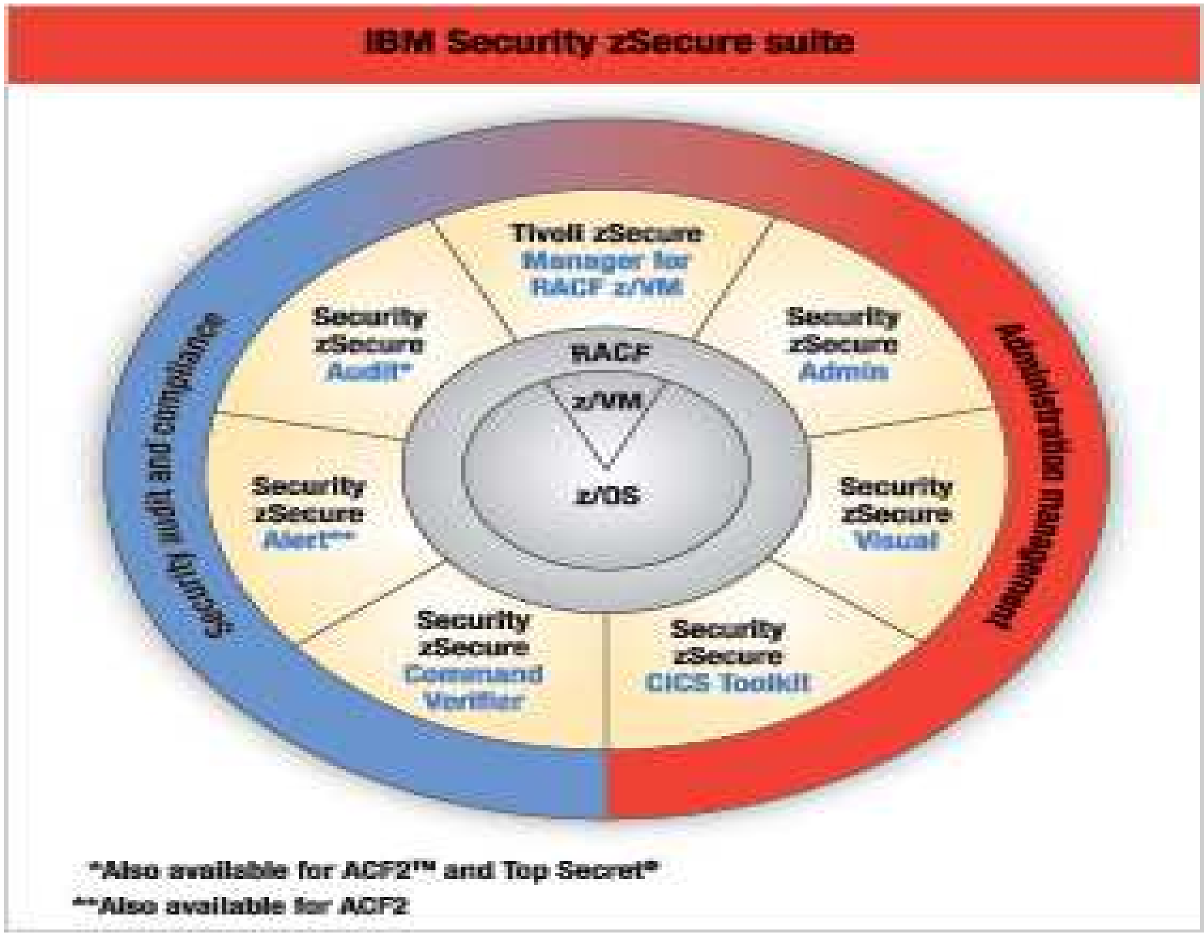
- **Security zSecure CICS® Toolkit**
  - **Helps free RACF resources from routine administrative tasks through a CICS interface**

- **Security zSecure Command Verifier**
  - **Helps enforce mainframe compliance to policies through granular controls for RACF commands**

- **Security zSecure Visual**
  - **Enables cost savings by decentralizing RACF administration through a Microsoft Windows-based GUI**

- **zSecure Manager for RACF z/VM**
  - **Provides combined audit and administration functionality for the VM environment**

zSecure components



IBM Security zSecure suite

Security audit and compliance
Administration management
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
RACF
z/VM
z/OS

Also available for ACF2™ and Top Secret
**Also available for ACF2

IBM Security zSecure Admin – benefits

- User friendly panel driven interface to administer and report on RACF profiles and security settings
- Multiple RACF environments are viewable in the same report
- RACF profile fields can be changed by typing over values in reports
- Mass updates for multiple users or groups at the same time
- Can check if a userid has access to a dataset or resource
- Powerful CARLa language for running reports in batch
- Ability to access copies of RACF database

IBM Security zSecure Admin – benefits

- Can easily recreate deleted profiles or create new profiles with same attributes as old ones
- List your RACF settings and tables (SETR, CDT etc) as well as z/OS security settings (APF list, IPL parms ,etc)
- View TCP/IP stack info
- List Digital Certificate info
- RACF Offline allows you to issue RACF commands against an offline RACF database
- Access Monitor lets you report on past accesses regardless of audit settings, including accesses allowed via GAT. Past access info for several days, weeks, months, etc can be consolidated into one input dataset

IBM Security zSecure Admin – tasks we do

- List Started Tasks with Trusted/Privileged attribute
- List userids with UID 0
- List dataset/general resource profiles with a specific userid/group in access list
- List userids that haven't accessed the system in specific amount of time
- List userids that have accessed the system within the past year that don't have a flag in DATA field
- List userids with RACF privileges
- List userids in NONPET group sorted by last access
- List active RACF classes that don't have any profiles
- List inactive classes that do have a profile

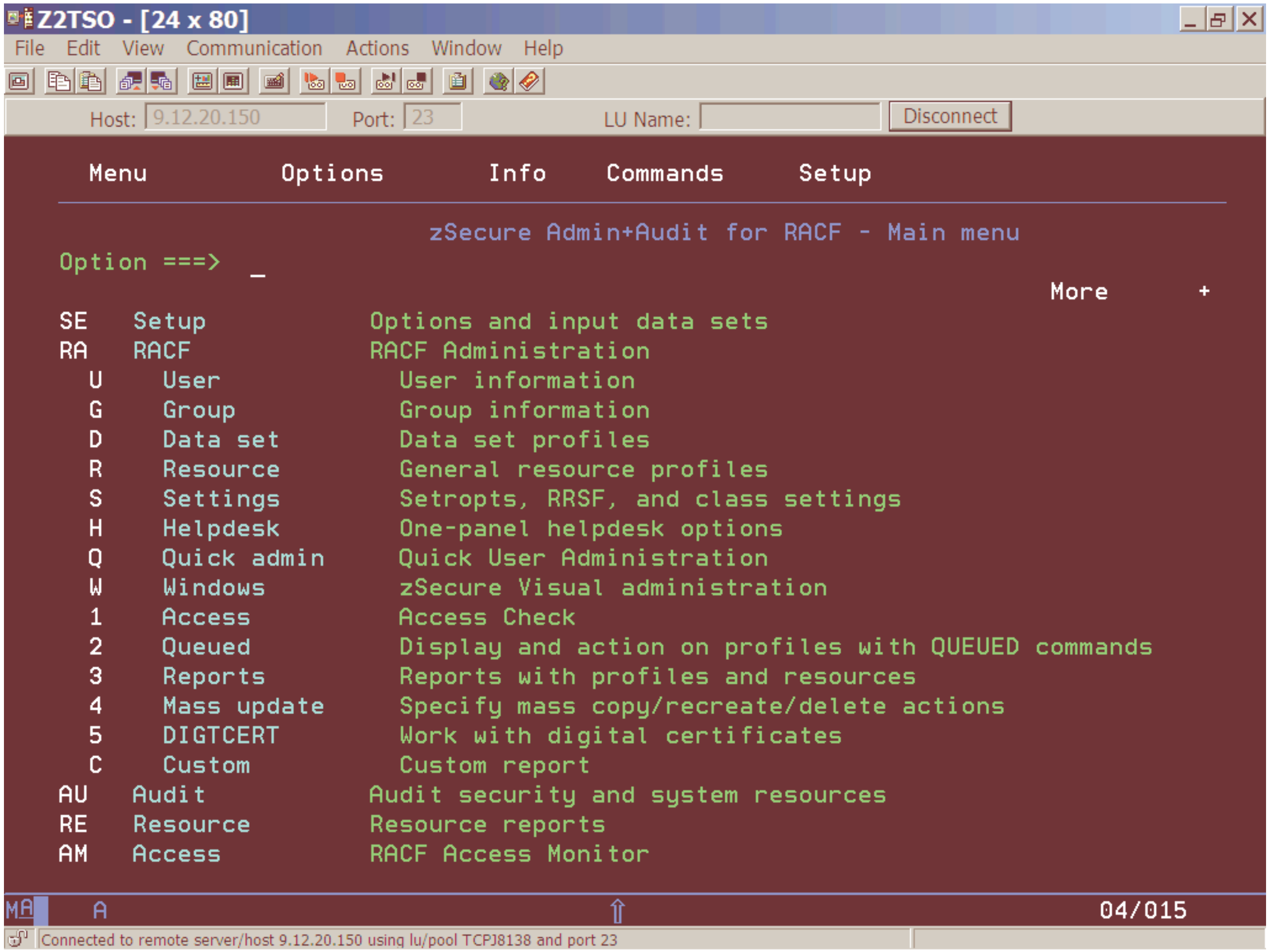
IBM Security zSecure Admin – tasks we do

- List active classes (and their POSIT numbers) that are not RACLISTed
- Show IPL parms used at last IPL
- Show software levels of RACF, MVS, JES, HSM etc
- Report on APF datasets not on volume listed
- Delete all of the userids connected to a specific group along with all of their dataset profiles under their userid hlq, remove group connections and accesses, and build commands to alter owner fields of things they own
- List Digital Certificates sorted by end date
- List all resources accessed by a specific userid
- List usage of the GAT

IBM Security zSecure Audit – tasks we do

- List all userids that had an audit record in the previous day that do not have a specific flag in DATA field
- List all accesses due to WARNING in the previous day
- List use of RACF privileges in the previous day
- List all accesses of a specific userid that were logged in SMF the previous day
- For a specific class, list the count of times each userid accessed a profile in the class the previous day

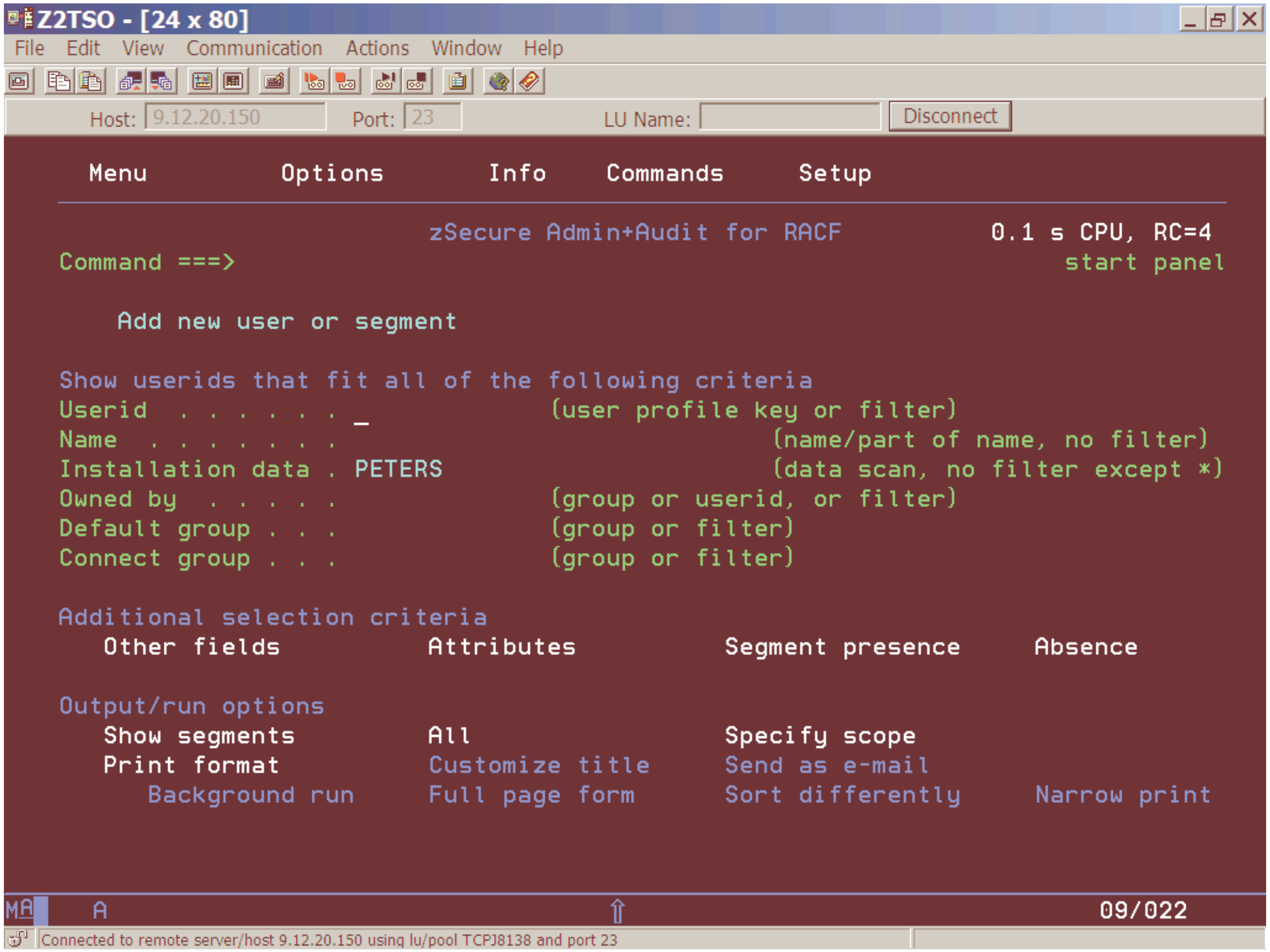
IBM Security zSecure Main Menu with RACF Administration section expanded



```
     Menu          Options        Info     Commands      Setup

                           zSecure Admin+Audit for RACF - Main menu
 Option ===> _
                                                                     More        +
 SE   Setup               Options and input data sets
 RA   RACF                RACF Administration
   U    User                User information
   G    Group               Group information
   D    Data set            Data set profiles
   R    Resource            General resource profiles
   S    Settings            Setropts, RRSF, and class settings
   H    Helpdesk            One-panel helpdesk options
   Q    Quick admin         Quick User Administration
   W    Windows             zSecure Visual administration
   1    Access              Access Check
   2    Queued              Display and action on profiles with QUEUED commands
   3    Reports             Reports with profiles and resources
   4    Mass update         Specify mass copy/recreate/delete actions
   5    DIGTCERT            Work with digital certificates
   C    Custom              Custom report
 AU   Audit               Audit security and system resources
 RE   Resource            Resource reports
 AM   Access              RACF Access Monitor

MA     A                                  ⇧                                04/015
```

Connected to remote server/host 9.12.20.150 using lu/pool TCPJ8138 and port 23

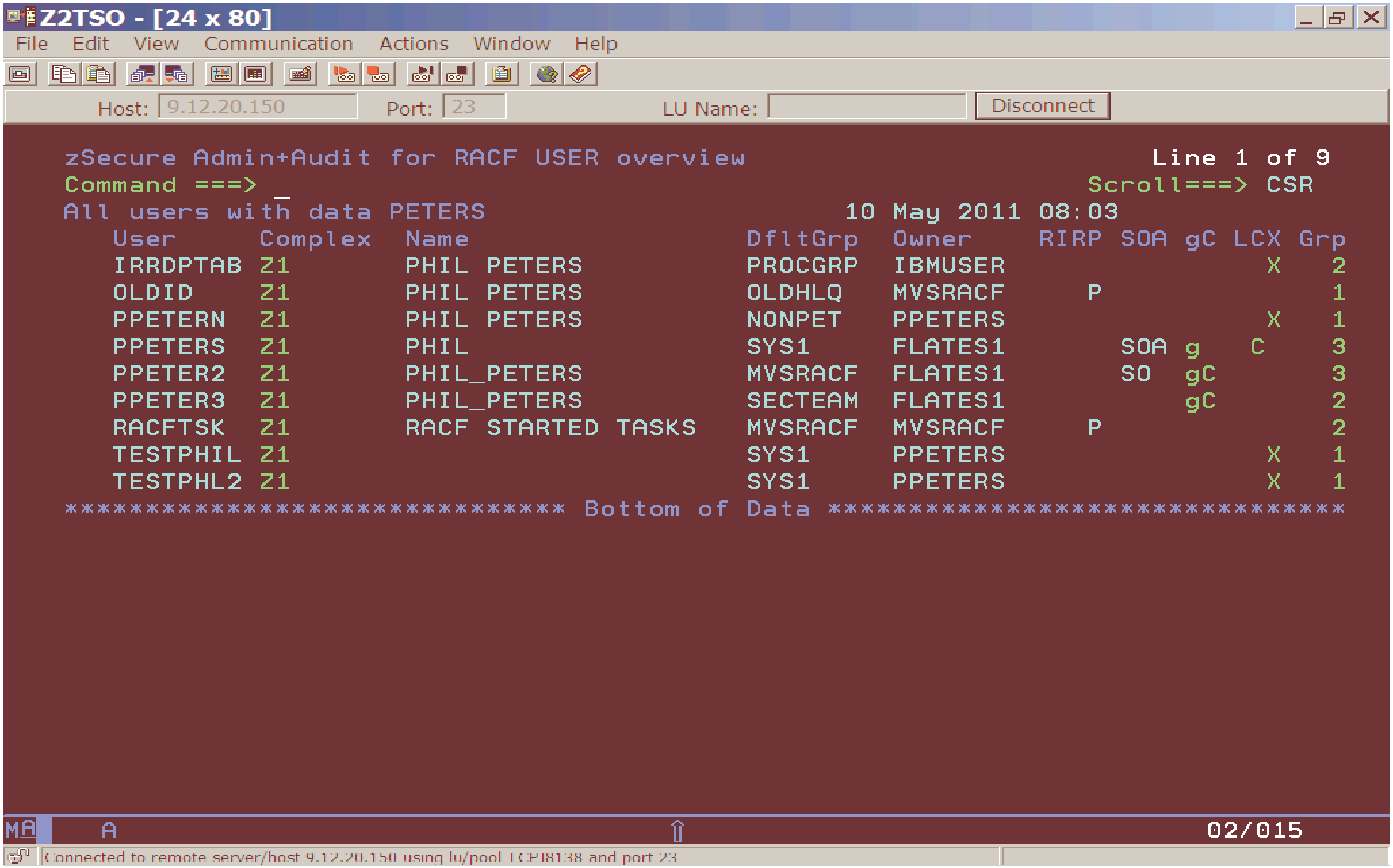
RA.U Panel with “PETERS” as the value for the Installation Data selection criteria



```
  Menu         Options        Info     Commands      Setup
 ------------------------------------------------------------------------
                          zSecure Admin+Audit for RACF           0.1 s CPU, RC=4
 Command ===>                                                        start panel

     Add new user or segment

 Show userids that fit all of the following criteria
 Userid  . . . . . . . _                (user profile key or filter)
 Name  . . . . . . . .                               (name/part of name, no filter)
 Installation data . PETERS                          (data scan, no filter except *)
 Owned by  . . . . . .                  (group or userid, or filter)
 Default group . . .                    (group or filter)
 Connect group . . .                    (group or filter)

 Additional selection criteria
    Other fields             Attributes           Segment presence      Absence

 Output/run options
    Show segments            All                  Specify scope
    Print format             Customize title      Send as e-mail
       Background run        Full page form       Sort differently      Narrow print

MA     A                                                                   09/022
```

Connected to remote server/host 9.12.20.150 using lu/pool TCPJ8138 and port 23

User IDs containing “PETERS” in the Installation Data field



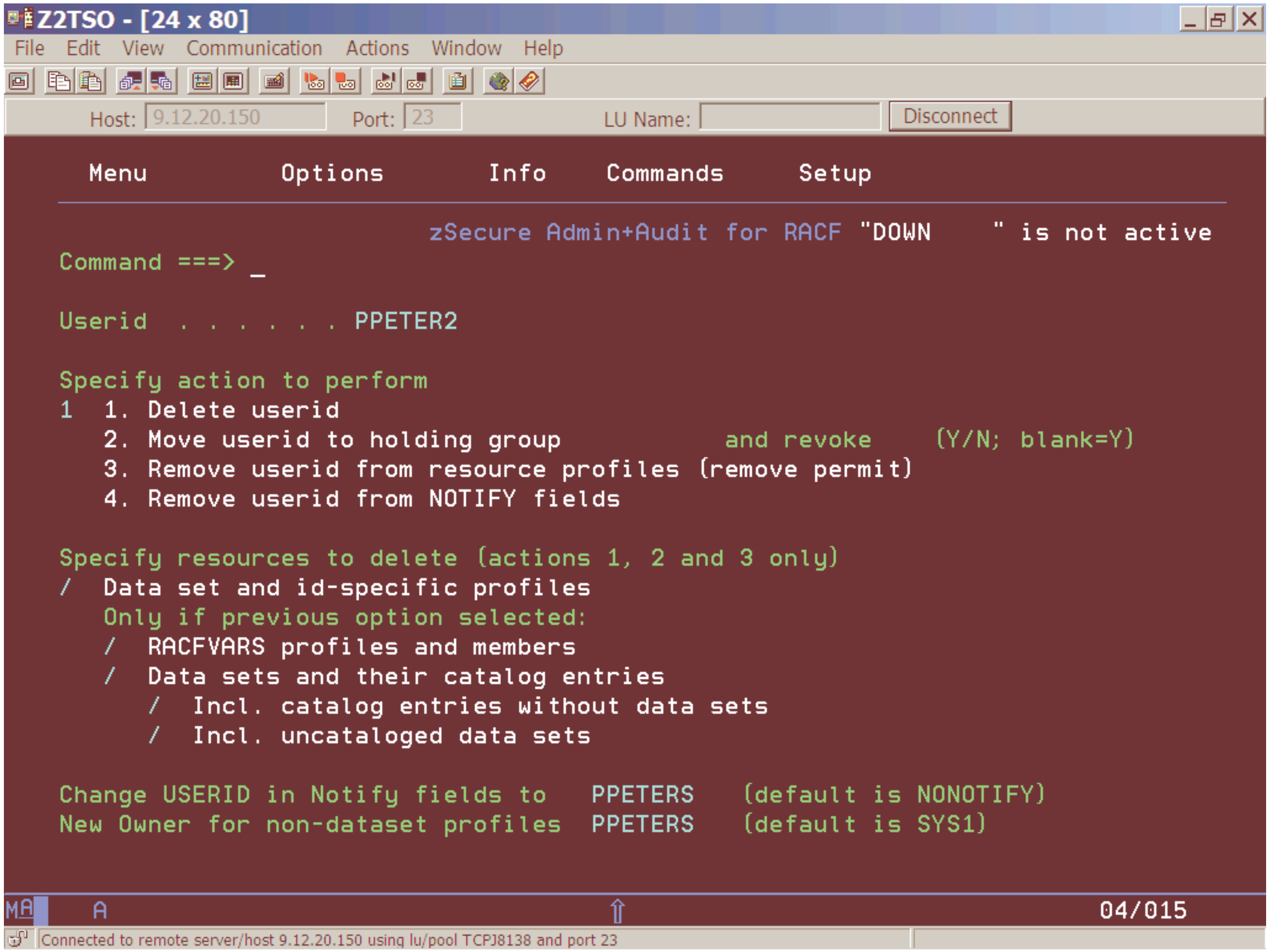
Host: 9.12.20.150 Port: 23 LU Name:

```
zSecure Admin+Audit for RACF USER overview                         Line 1 of 9
Command ===> _                                                 Scroll===> CSR
All users with data PETERS                      10 May 2011 08:03
   User     Complex  Name                 DfltGrp  Owner    RIRP SOA gC LCX Grp
   IRRDPTAB Z1       PHIL PETERS          PROCGRP  IBMUSER                X   2
   OLDID    Z1       PHIL PETERS          OLDHLQ   MVSRACF    P               1
   PPETERN  Z1       PHIL PETERS          NONPET   PPETERS                X   1
   PPETERS  Z1       PHIL                 SYS1     FLATES1       SOA g   C    3
   PPETER2  Z1       PHIL_PETERS          MVSRACF  FLATES1       SO  gC       3
   PPETER3  Z1       PHIL_PETERS          SECTEAM  FLATES1           gC       2
   RACFTSK  Z1       RACF STARTED TASKS   MVSRACF  MVSRACF    P               2
   TESTPHIL Z1                            SYS1     PPETERS                X   1
   TESTPHL2 Z1                            SYS1     PPETERS                X   1
******************************* Bottom of Data ********************************
```

```
MA     A                                                                02/015
```

Connected to remote server/host 9.12.20.150 using lu/pool TCPJ8138 and port 23

RACF -> 4 Mass Update -> 4 Delete user

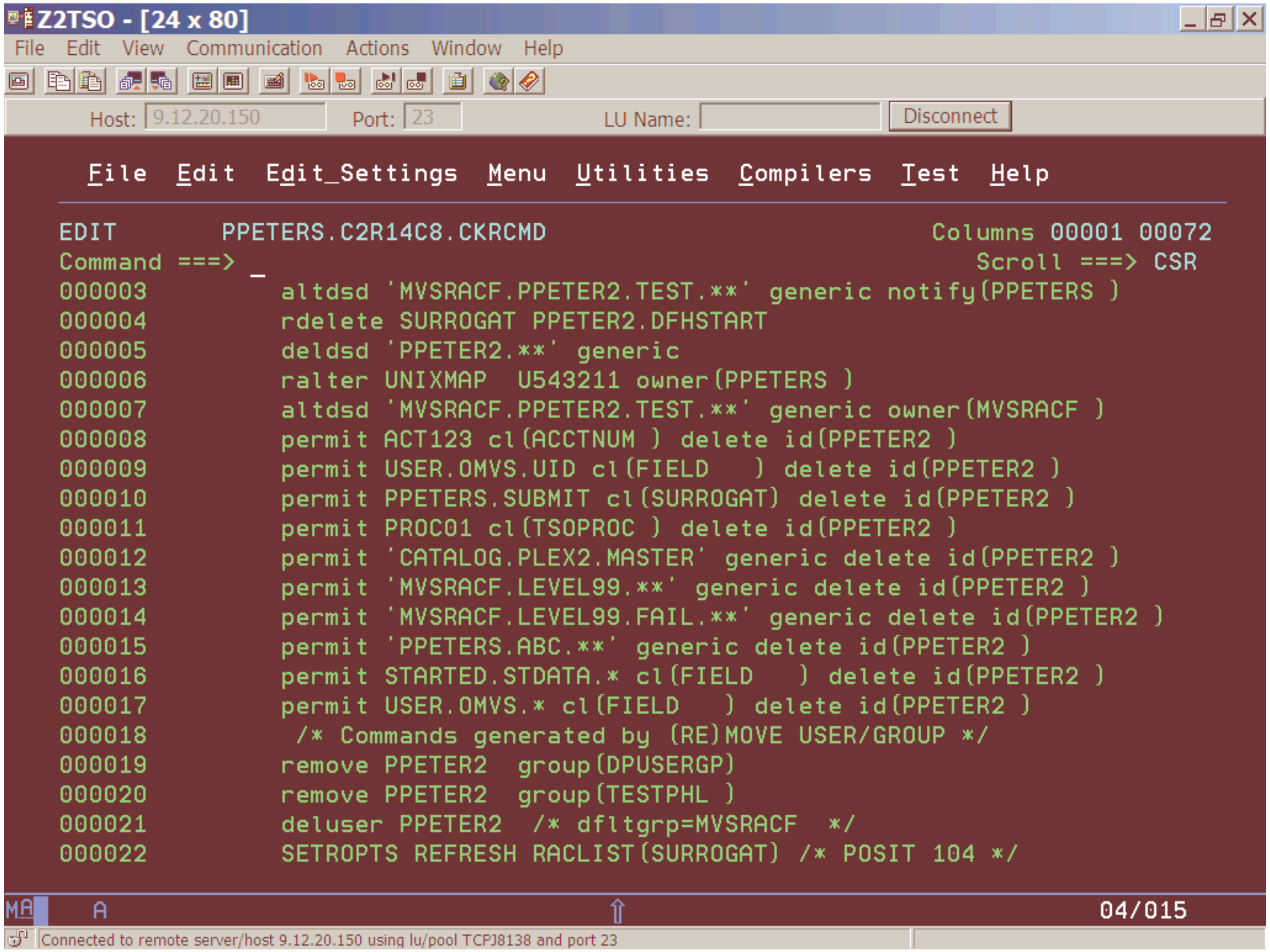


Host: 9.12.20.150 Port: 23 LU Name:

```
  Menu         Options       Info     Commands     Setup
 ------------------------------------------------------------------------------
                             zSecure Admin+Audit for RACF "DOWN    " is not active
 Command ===> _

 Userid  . . . . . . PPETER2

 Specify action to perform
 1  1. Delete userid
    2. Move userid to holding group           and revoke    (Y/N; blank=Y)
    3. Remove userid from resource profiles (remove permit)
    4. Remove userid from NOTIFY fields

 Specify resources to delete (actions 1, 2 and 3 only)
 /  Data set and id-specific profiles
    Only if previous option selected:
    /  RACFVARS profiles and members
    /  Data sets and their catalog entries
       /  Incl. catalog entries without data sets
       /  Incl. uncataloged data sets

 Change USERID in Notify fields to    PPETERS   (default is NONOTIFY)
 New Owner for non-dataset profiles   PPETERS   (default is SYS1)

MA    A                                ⇑                            04/015
```

Connected to remote server/host 9.12.20.150 using lu/pool TCPJ8138 and port 23

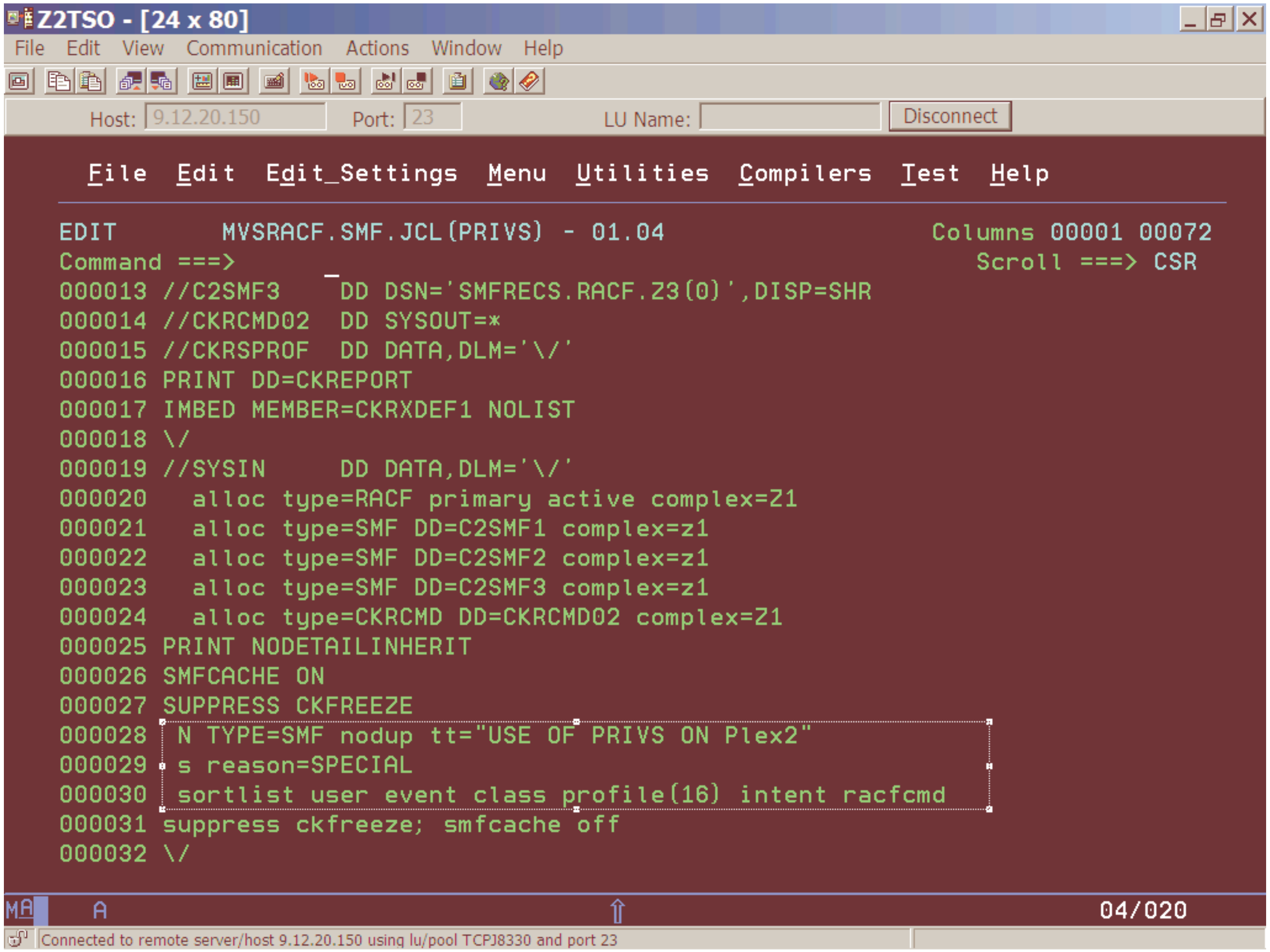
Commands generated from the previous panel



```
   File  Edit  Edit_Settings  Menu  Utilities  Compilers  Test  Help

EDIT       PPETERS.C2R14C8.CKRCMD                        Columns 00001 00072
Command ===> _                                              Scroll ===> CSR
000003        altdsd 'MVSRACF.PPETER2.TEST.**' generic notify(PPETERS )
000004        rdelete SURROGAT PPETER2.DFHSTART
000005        deldsd 'PPETER2.**' generic
000006        ralter UNIXMAP  U543211 owner(PPETERS )
000007        altdsd 'MVSRACF.PPETER2.TEST.**' generic owner(MVSRACF )
000008        permit ACT123 cl(ACCTNUM ) delete id(PPETER2 )
000009        permit USER.OMVS.UID cl(FIELD   ) delete id(PPETER2 )
000010        permit PPETERS.SUBMIT cl(SURROGAT) delete id(PPETER2 )
000011        permit PROC01 cl(TSOPROC ) delete id(PPETER2 )
000012        permit 'CATALOG.PLEX2.MASTER' generic delete id(PPETER2 )
000013        permit 'MVSRACF.LEVEL99.**' generic delete id(PPETER2 )
000014        permit 'MVSRACF.LEVEL99.FAIL.**' generic delete id(PPETER2 )
000015        permit 'PPETERS.ABC.**' generic delete id(PPETER2 )
000016        permit STARTED.STDATA.* cl(FIELD   ) delete id(PPETER2 )
000017        permit USER.OMVS.* cl(FIELD   ) delete id(PPETER2 )
000018         /* Commands generated by (RE)MOVE USER/GROUP */
000019        remove PPETER2  group(DPUSERGP)
000020        remove PPETER2  group(TESTPHL )
000021        deluser PPETER2  /* dfltgrp=MVSRACF  */
000022        SETROPTS REFRESH RACLIST(SURROGAT) /* POSIT 104 */

MA     A                                                          04/015
```

Connected to remote server/host 9.12.20.150 using lu/pool TCPJ8138 and port 23

Audit job to list privileged activity

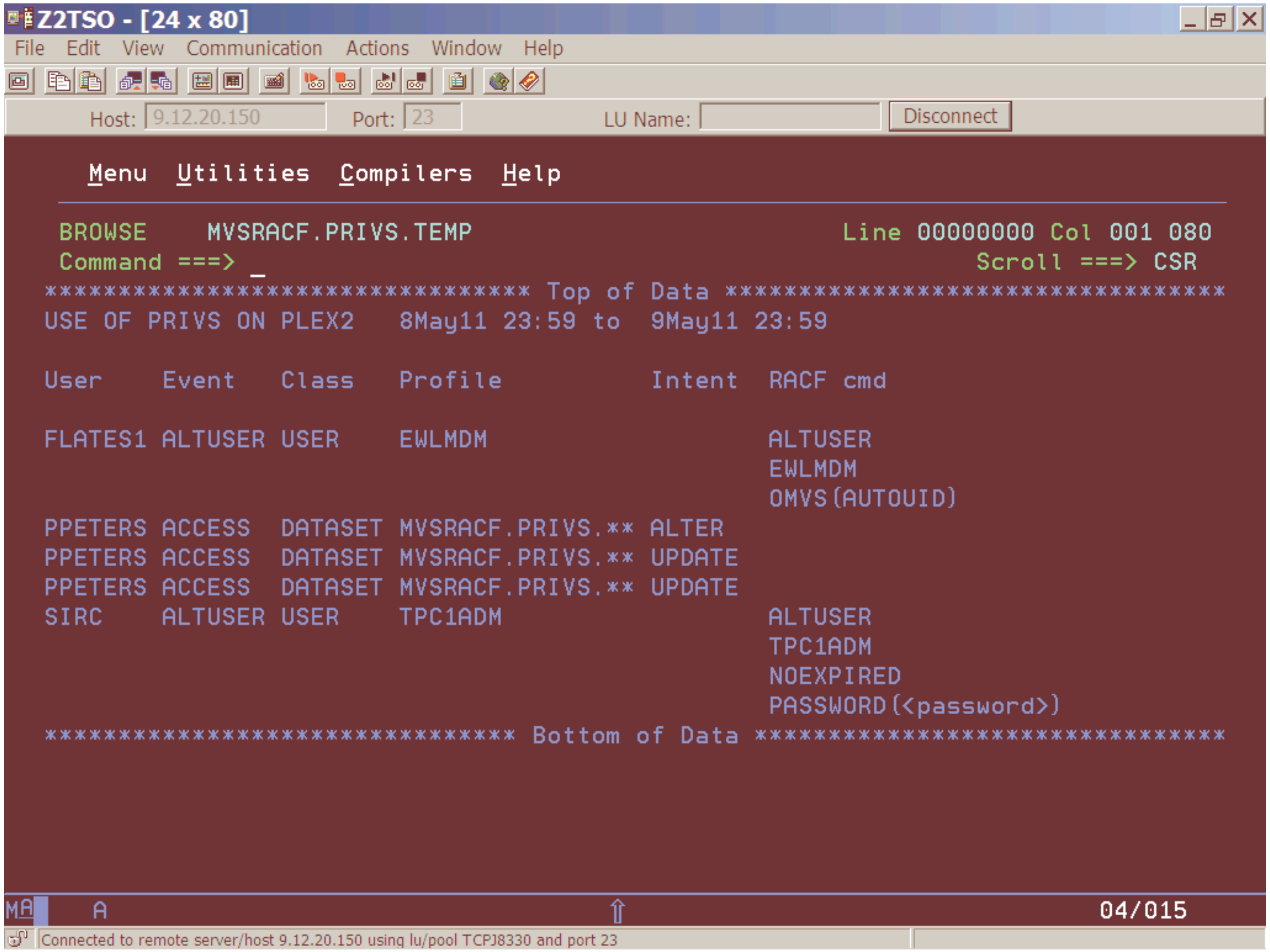

Z2TSO - [24 x 80]
File Edit View Communication Actions Window Help
Disconnect
File Edit Edit_Settings Menu Utilities Compilers Test Help
MA
A

Host: 9.12.20.150 Port: 23 LU Name:

```
EDIT       MVSRACF.SMF.JCL(PRIVS) - 01.04              Columns 00001 00072
Command ===>                                              Scroll ===> CSR
       //C2SMF3      DD DSN='SMFRECS.RACF.Z3(0)',DISP=SHR
       //CKRCMD02  DD SYSOUT=*
       //CKRSPROF  DD DATA,DLM='\/'
       PRINT DD=CKREPORT
       IMBED MEMBER=CKRXDEF1 NOLIST
       \/
       //SYSIN     DD DATA,DLM='\/'
         alloc type=RACF primary active complex=Z1
         alloc type=SMF DD=C2SMF1 complex=z1
         alloc type=SMF DD=C2SMF2 complex=z1
         alloc type=SMF DD=C2SMF3 complex=z1
         alloc type=CKRCMD DD=CKRCMD02 complex=Z1
       PRINT NODETAILINHERIT
       SMFCACHE ON
       SUPPRESS CKFREEZE
        N TYPE=SMF nodup tt="USE OF PRIVS ON Plex2"
        s reason=SPECIAL
        sortlist user event class profile(16) intent racfcmd
       suppress ckfreeze; smfcache off
       \/
                                                                   04/020
```

Connected to remote server/host 9.12.20.150 using lu/pool TCPJ8330 and port 23

RACF Privilege Report



Host: 9.12.20.150 Port: 23 LU Name:

```
   Menu  Utilities  Compilers  Help

 BROWSE    MVSRACF.PRIVS.TEMP                          Line 00000000 Col 001 080
 Command ===> _                                                 Scroll ===> CSR
********************************* Top of Data **********************************
USE OF PRIVS ON PLEX2   8May11 23:59 to  9May11 23:59

User    Event   Class   Profile          Intent  RACF cmd

FLATES1 ALTUSER USER    EWLMDM                   ALTUSER
                                                 EWLMDM
                                                 OMVS(AUTOUID)
PPETERS ACCESS  DATASET MVSRACF.PRIVS.** ALTER
PPETERS ACCESS  DATASET MVSRACF.PRIVS.** UPDATE
PPETERS ACCESS  DATASET MVSRACF.PRIVS.** UPDATE
SIRC    ALTUSER USER    TPC1ADM                  ALTUSER
                                                 TPC1ADM
                                                 NOEXPIRED
                                                 PASSWORD(<password>)
******************************** Bottom of Data ********************************
```

```
MA    A                              ⇧                              04/015
```

Connected to remote server/host 9.12.20.150 using lu/pool TCPJ8330 and port 23

Summary

- We’ve only implemented Admin and Audit
- Very user friendly
- Very beneficial for controlling our RACF environment