Adrian Enrique Hernandez Contreras
SWAT Team Consultant
ahernan@mx1.ibm.com

zEnterprise.

A New Dimension in Computing

IBM Security Solutions sobre System z

Problemas típicos de seguridad en Mainframe

- Auditoria y cumplimiento de regulaciones (PCI, SOX) y gobernabilidad de mainframes
  - Normalmente en constante auditoria

- Administrador de RACF durante una auditoria
  - Explicar a un auditor como trabaja un mainframe
  - Procesar múltiples solicitudes de reportes de RACF y SMF dentro de 24 hrs
  - Escribir grandes cantidades de código para crear todos los reportes solicitados
  - Descargar todos los reportes que se crearon a la PC para enviarlos por mail
  - Emplear tiempo en las juntas de auditoria para explicar el significado de los report
  - Este ciclo se repite durante toda la auditoria

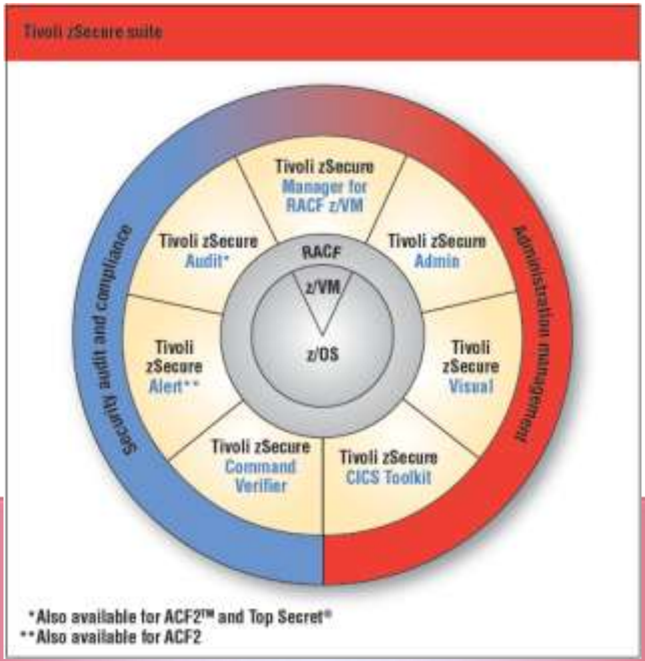
- A pesar de que RACF es formalmente un ambiente de seguridad muy efectivo existen algunas asperezas en el sistema
  - Sin una interfaz de usuario, los administradores de seguridad pierden tiempo al administrar RACF

Tivoli Security - Mainframe

IBM Tivoli zSecure Suite

* Also available for ACF2 and Top Secret

** Also available for ACF2


Tivoli zSecure suite
Tivoli zSecure Manager for RACF z/VM
Tivoli zSecure Audit*
Tivoli zSecure Admin
Tivoli zSecure Alert**
Tivoli zSecure Visual
Tivoli zSecure Command Verifier
Tivoli zSecure CICS Toolkit
RACF
z/VM
z/OS
Security audit and compliance
Administration management
*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Monitoreo, Auditoría y Reporteo de la seguridad de la organización

Administración empresarial de identidades y accesos

Tivoli Security Information and Event Manager (TSIEM)

Tivoli Security Operations Manager (TSOM)

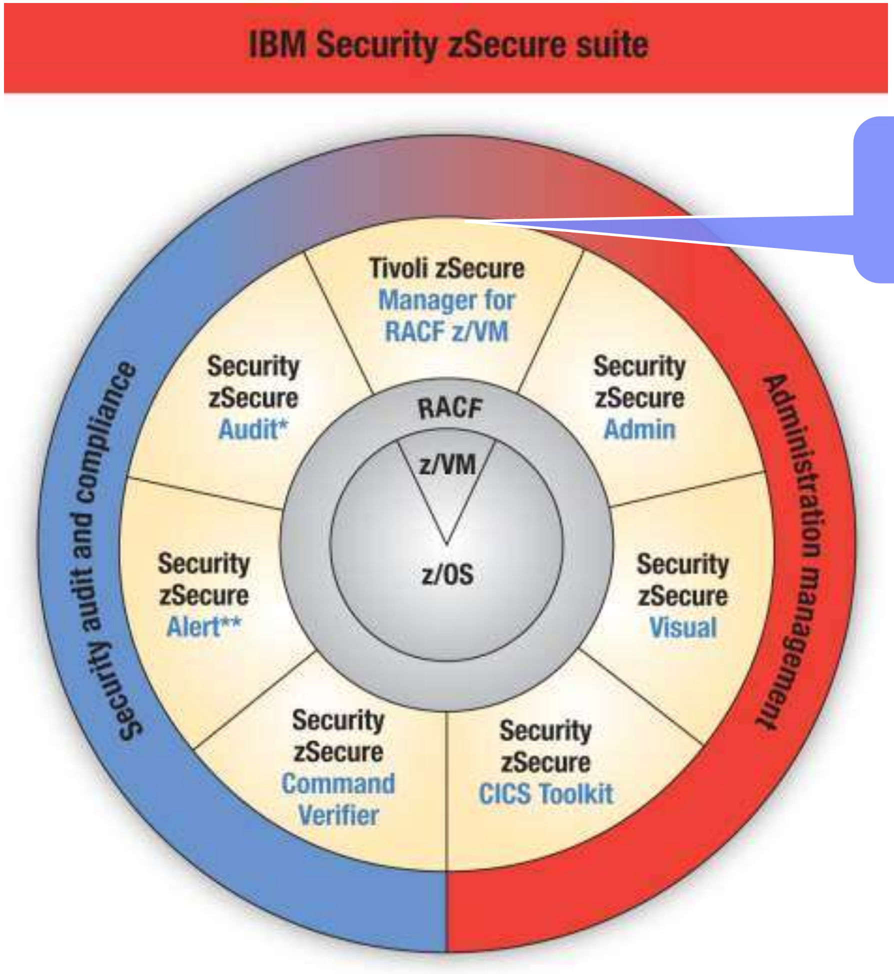
Tivoli Identity Manager (TIM) for z/OS

Tivoli Federated Identity Manager (TFIM) for z/OS

Tivoli Directory Server (TDS) for z/OS

Tivoli Directory Integrator (TDI) for z/OS

IBM Security zSecure Suite Overview


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

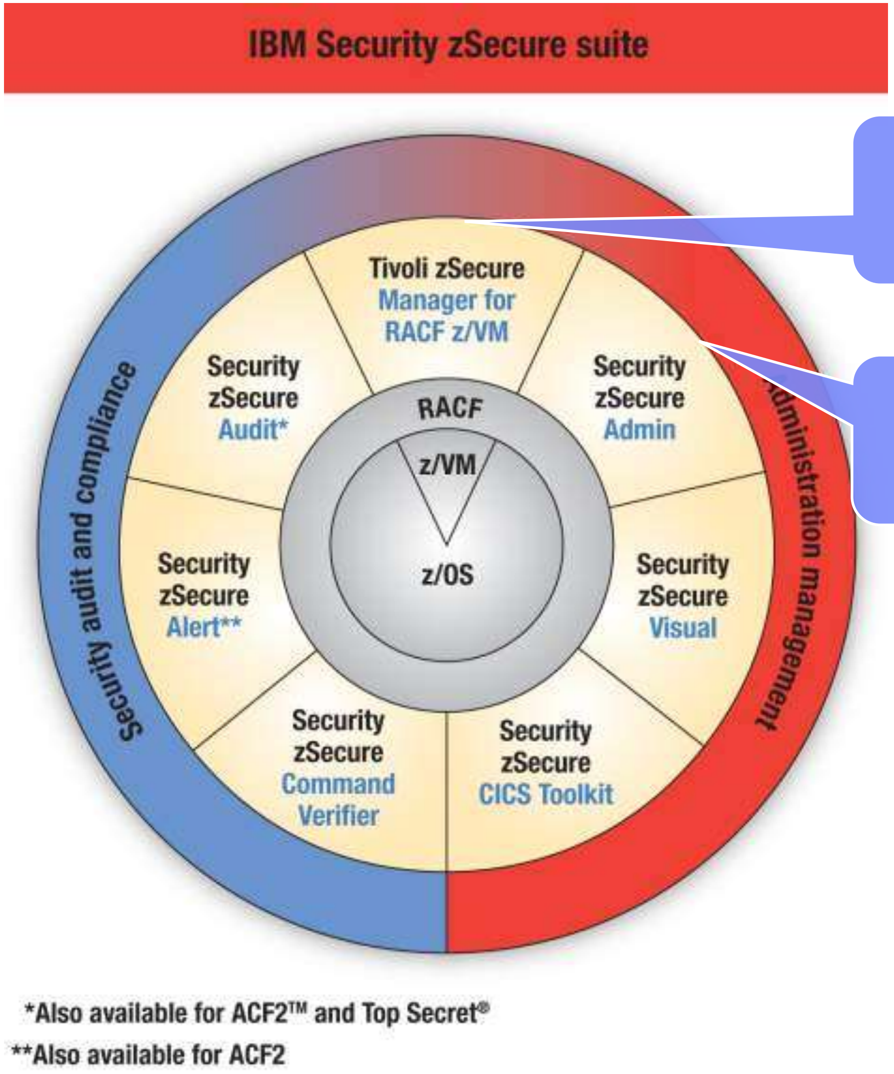
Administración y Auditoría para RACF en el ambiente VM

*Also available for ACF2™ and Top Secret®

**Also available for ACF2

Nota: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

IBM Security zSecure Suite Overview

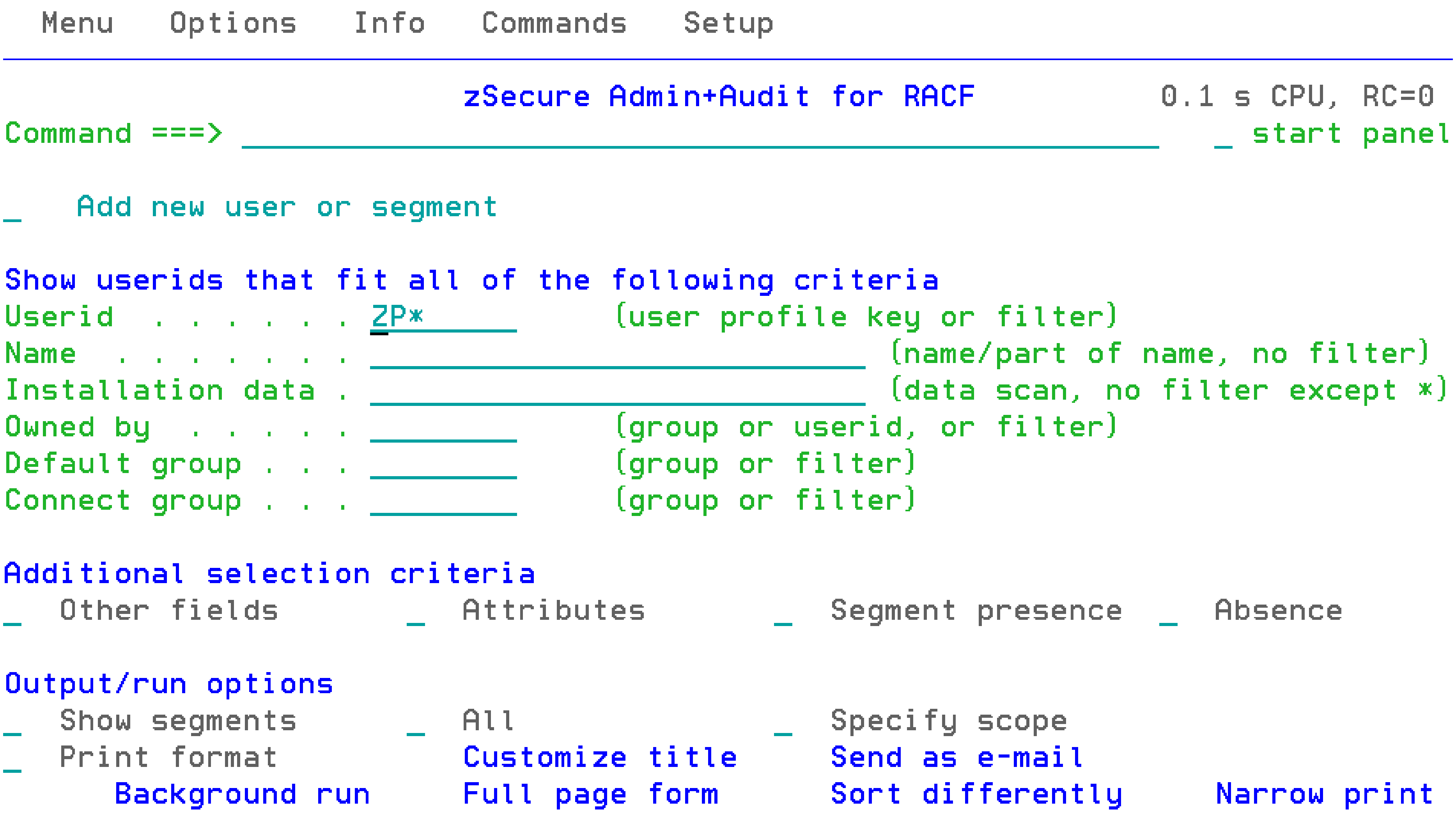

IBM Security zSecure suite
Tivoli zSecure Manager for RACF z/VM
Security zSecure Audit*
Security zSecure Admin
RACF
z/VM
z/OS
Security zSecure Alert**
Security zSecure Visual
Security zSecure Command Verifier
Security zSecure CICS Toolkit
Security audit and compliance
Administration management
*Also available for ACF2™ and Top Secret®
**Also available for ACF2

Administración y Auditoría para RACF en el ambiente VM

Permite administrar RACF de una manera mas eficiente y efectiva usando menos recursos

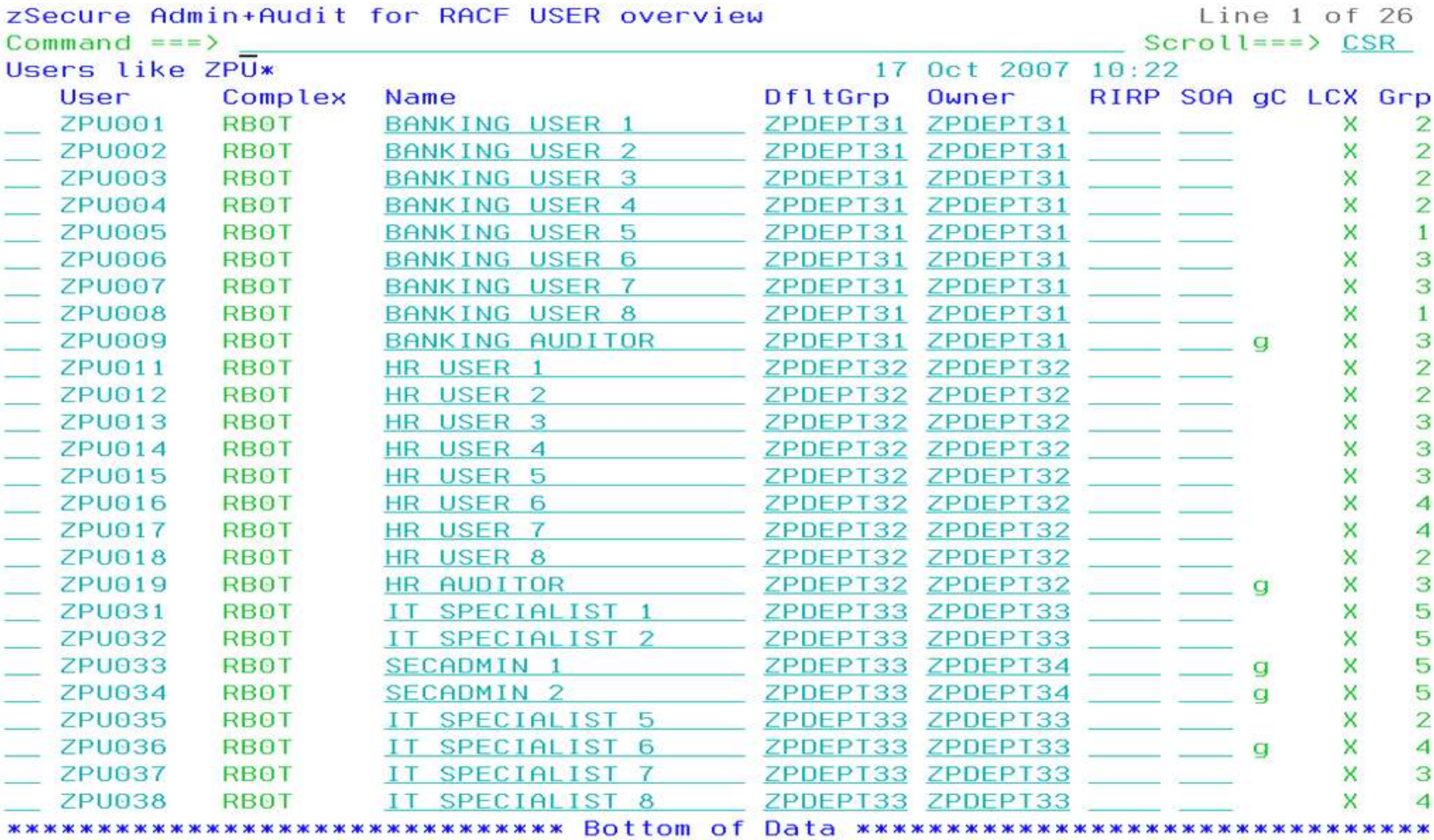
Nota: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

Búsqueda de usuarios sencilla



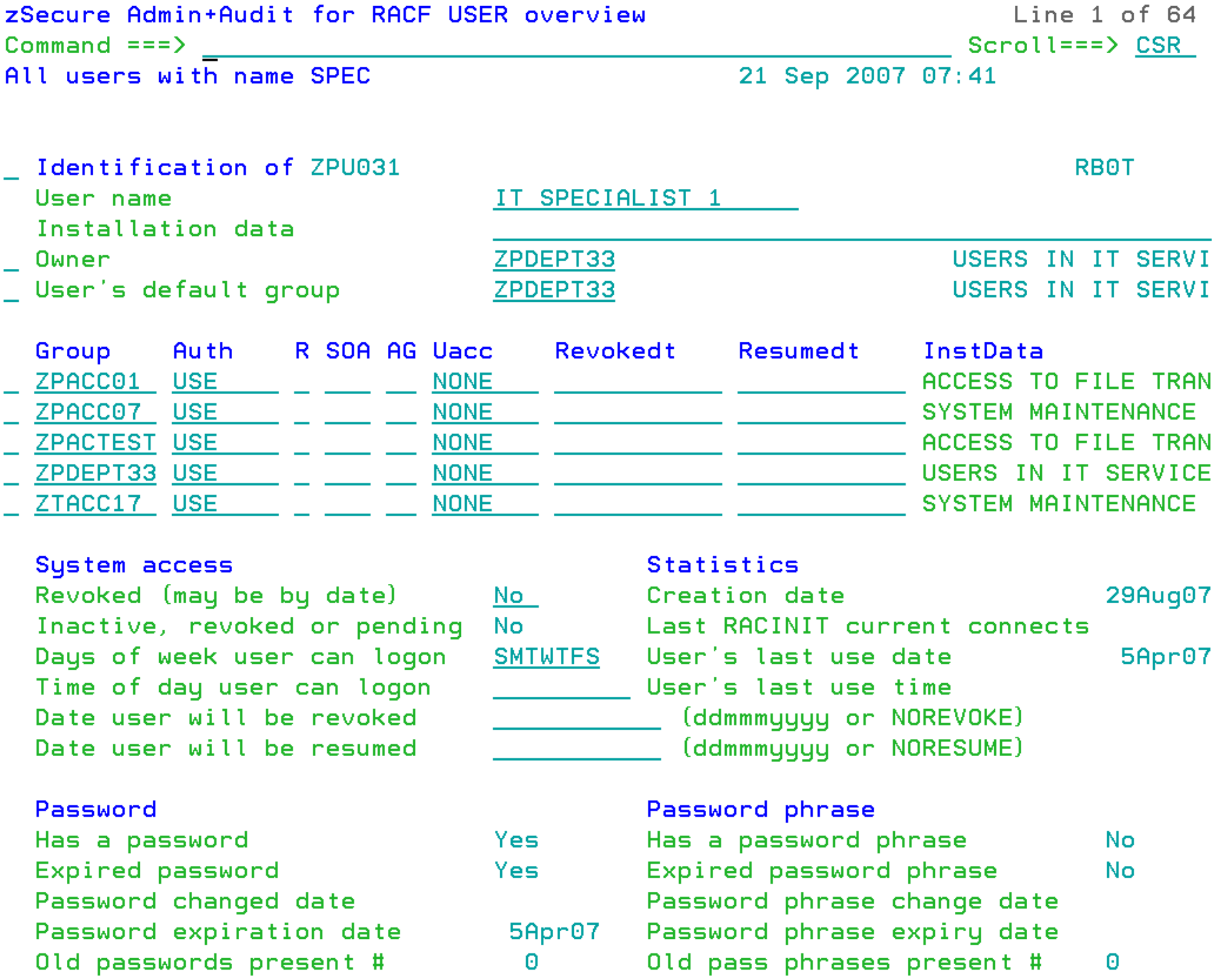
```
  Menu    Options    Info    Commands    Setup

                         zSecure Admin+Audit for RACF          0.1 s CPU, RC=0
Command ===> __________________________________________________   _ start panel

_   Add new user or segment

Show userids that fit all of the following criteria
Userid  . . . . . . ZP*_____     (user profile key or filter)
Name  . . . . . . . ___________________________ (name/part of name, no filter)
Installation data . ___________________________ (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
```

Administración amigable de RACF



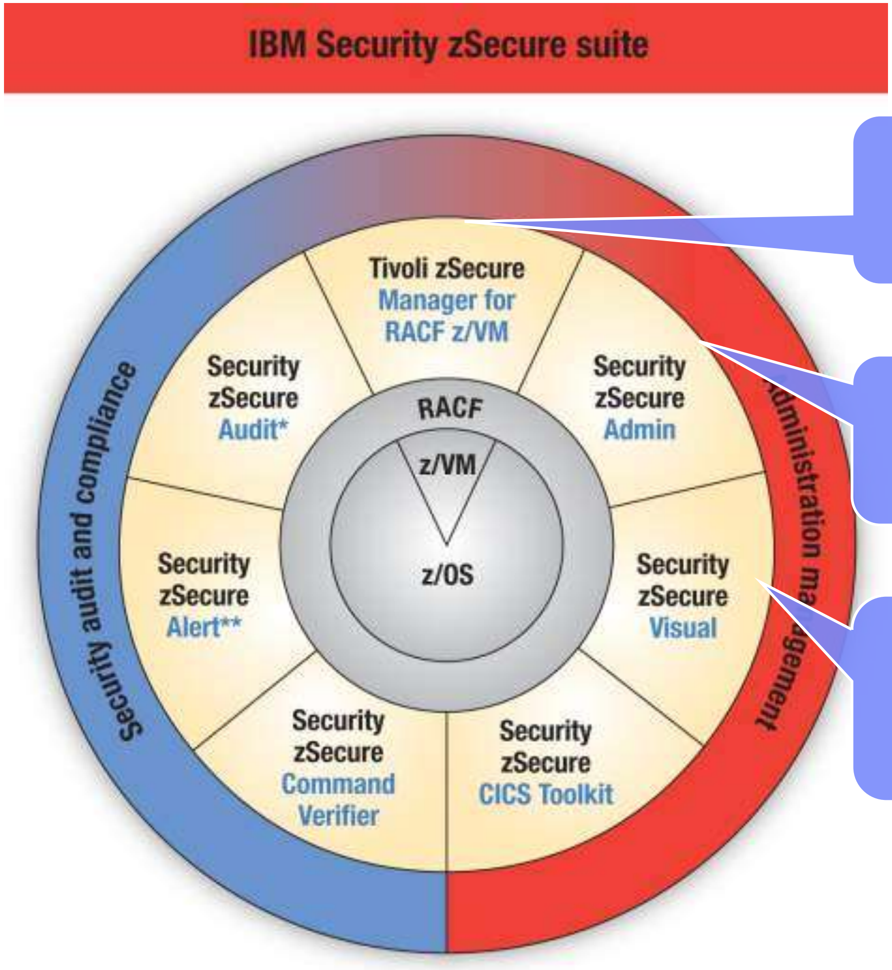
```
zSecure Admin+Audit for RACF USER overview                          Line 1 of 26
Command ===> _________________________________________________ Scroll===> CSR_
Users like ZPU*                                         17 Oct 2007 10:22
    User      Complex   Name                  DfltGrp   Owner     RIRP  SOA  gC LCX Grp
___ ZPU001    RBOT      BANKING USER 1        ZPDEPT31  ZPDEPT31  ____  ___       X   2
___ ZPU002    RBOT      BANKING USER 2        ZPDEPT31  ZPDEPT31  ____  ___       X   2
___ ZPU003    RBOT      BANKING USER 3        ZPDEPT31  ZPDEPT31  ____  ___       X   2
___ ZPU004    RBOT      BANKING USER 4        ZPDEPT31  ZPDEPT31  ____  ___       X   2
___ ZPU005    RBOT      BANKING USER 5        ZPDEPT31  ZPDEPT31  ____  ___       X   1
___ ZPU006    RBOT      BANKING USER 6        ZPDEPT31  ZPDEPT31  ____  ___       X   3
___ ZPU007    RBOT      BANKING USER 7        ZPDEPT31  ZPDEPT31  ____  ___       X   3
___ ZPU008    RBOT      BANKING USER 8        ZPDEPT31  ZPDEPT31  ____  ___       X   1
___ ZPU009    RBOT      BANKING AUDITOR       ZPDEPT31  ZPDEPT31  ____  ___  g    X   3
___ ZPU011    RBOT      HR USER 1             ZPDEPT32  ZPDEPT32  ____  ___       X   2
___ ZPU012    RBOT      HR USER 2             ZPDEPT32  ZPDEPT32  ____  ___       X   2
___ ZPU013    RBOT      HR USER 3             ZPDEPT32  ZPDEPT32  ____  ___       X   3
___ ZPU014    RBOT      HR USER 4             ZPDEPT32  ZPDEPT32  ____  ___       X   3
___ ZPU015    RBOT      HR USER 5             ZPDEPT32  ZPDEPT32  ____  ___       X   3
___ ZPU016    RBOT      HR USER 6             ZPDEPT32  ZPDEPT32  ____  ___       X   4
___ ZPU017    RBOT      HR USER 7             ZPDEPT32  ZPDEPT32  ____  ___       X   4
___ ZPU018    RBOT      HR USER 8             ZPDEPT32  ZPDEPT32  ____  ___       X   2
___ ZPU019    RBOT      HR AUDITOR            ZPDEPT32  ZPDEPT32  ____  ___  g    X   3
___ ZPU031    RBOT      IT SPECIALIST 1       ZPDEPT33  ZPDEPT33  ____  ___       X   5
___ ZPU032    RBOT      IT SPECIALIST 2       ZPDEPT33  ZPDEPT33  ____  ___       X   5
___ ZPU033    RBOT      SECADMIN 1            ZPDEPT33  ZPDEPT34  ____  ___  g    X   5
___ ZPU034    RBOT      SECADMIN 2            ZPDEPT33  ZPDEPT34  ____  ___  g    X   5
___ ZPU035    RBOT      IT SPECIALIST 5       ZPDEPT33  ZPDEPT33  ____  ___       X   2
___ ZPU036    RBOT      IT SPECIALIST 6       ZPDEPT33  ZPDEPT33  ____  ___  g    X   4
___ ZPU037    RBOT      IT SPECIALIST 7       ZPDEPT33  ZPDEPT33  ____  ___       X   3
___ ZPU038    RBOT      IT SPECIALIST 8       ZPDEPT33  ZPDEPT33  ____  ___       X   4
******************************* Bottom of Data ********************************
```

Mostrar características de un usuario



```
zSecure Admin+Audit for RACF USER overview                        Line 1 of 64
Command ===> _________________________________________________ Scroll===> CSR
All users with name SPEC                        21 Sep 2007 07:41


_ Identification of ZPU031                                            RBOT
  User name                     IT SPECIALIST 1
  Installation data
_ Owner                         ZPDEPT33                      USERS IN IT SERVI
_ User's default group          ZPDEPT33                      USERS IN IT SERVI

  Group    Auth     R SOA AG Uacc     Revokedt    Resumedt    InstData
_ ZPACC01  USE      _ ___ __ NONE     ___________ ___________ ACCESS TO FILE TRAN
_ ZPACC07  USE      _ ___ __ NONE     ___________ ___________ SYSTEM MAINTENANCE
_ ZPACTEST USE      _ ___ __ NONE     ___________ ___________ ACCESS TO FILE TRAN
_ ZPDEPT33 USE      _ ___ __ NONE     ___________ ___________ USERS IN IT SERVICE
_ ZTACC17  USE      _ ___ __ NONE     ___________ ___________ SYSTEM MAINTENANCE

  System access                           Statistics
  Revoked (may be by date)      No        Creation date                 29Aug07
  Inactive, revoked or pending  No        Last RACINIT current connects
  Days of week user can logon   SMTWTFS   User's last use date           5Apr07
  Time of day user can logon    _________ User's last use time
  Date user will be revoked     ___________ (ddmmmyyyy or NOREVOKE)
  Date user will be resumed     ___________ (ddmmmyyyy or NORESUME)

  Password                                Password phrase
  Has a password                Yes       Has a password phrase         No
  Expired password              Yes       Expired password phrase       No
  Password changed date                   Password phrase change date
  Password expiration date       5Apr07   Password phrase expiry date
  Old passwords present #         0       Old pass phrases present #    0
```

IBM Security zSecure Suite Overview


IBM Security zSecure suite
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
Security audit and compliance
dministration ma
gement

Administración y Auditoría para RACF en el ambiente VM

Permite administrar RACF de una manera mas eficiente y efectiva usando menos recursos

Reduce la necesidad de los recursos con habilidades en RACF (escasos) a través de una interfaz en Windows para administrar RACF

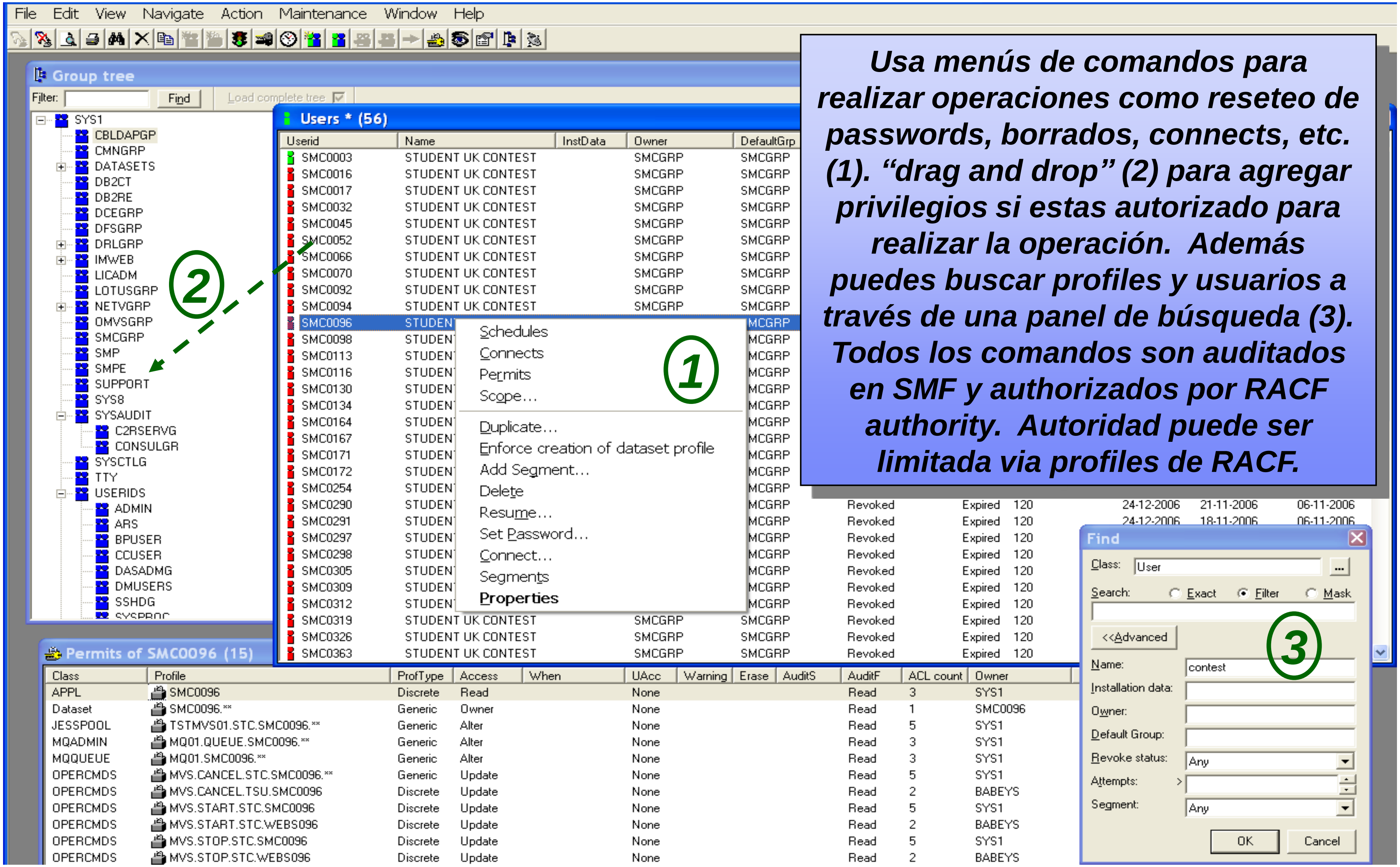
*Also available for ACF2™ and Top Secret®

**Also available for ACF2

Nota: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

zVisual lleva RACF a un ambiente empresarial

Usa menús de comandos para realizar operaciones como reseteo de passwords, borrados, connects, etc. (1). "drag and drop" (2) para agregar privilegios si estas autorizado para realizar la operación. Además puedes buscar profiles y usuarios a través de una panel de búsqueda (3). Todos los comandos son auditados en SMF y authorizados por RACF authority. Autoridad puede ser limitada via profiles de RACF.



Userid	Name	InstData	Owner	DefaultGrp						
SMC0003	STUDENT UK CONTEST		SMCGRP	SMCGRP						
SMC0016	STUDENT UK CONTEST		SMCGRP	SMCGRP						
SMC0017	STUDENT UK CONTEST		SMCGRP	SMCGRP						
SMC0032	STUDENT UK CONTEST		SMCGRP	SMCGRP						
SMC0045	STUDENT UK CONTEST		SMCGRP	SMCGRP						
SMC0052	STUDENT UK CONTEST		SMCGRP	SMCGRP						
SMC0066	STUDENT UK CONTEST		SMCGRP	SMCGRP						
SMC0070	STUDENT UK CONTEST		SMCGRP	SMCGRP						
SMC0092	STUDENT UK CONTEST		SMCGRP	SMCGRP						
SMC0094	STUDENT UK CONTEST		SMCGRP	SMCGRP						
SMC0096	STUDEN			MCGRP						
SMC0098	STUDEN			MCGRP						
SMC0113	STUDEN			MCGRP						
SMC0116	STUDEN			MCGRP						
SMC0130	STUDEN			MCGRP						
SMC0134	STUDEN			MCGRP						
SMC0164	STUDEN			MCGRP						
SMC0167	STUDEN			MCGRP						
SMC0171	STUDEN			MCGRP						
SMC0172	STUDEN			MCGRP						
SMC0254	STUDEN			MCGRP						
SMC0290	STUDEN			MCGRP	Revoked	Expired	120	24-12-2006	21-11-2006	06-11-2006
SMC0291	STUDEN			MCGRP	Revoked	Expired	120	24-12-2006	18-11-2006	06-11-2006
SMC0297	STUDEN			MCGRP	Revoked	Expired	120			
SMC0298	STUDEN			MCGRP	Revoked	Expired	120			
SMC0305	STUDEN			MCGRP	Revoked	Expired	120			
SMC0309	STUDEN			MCGRP	Revoked	Expired	120			
SMC0312	STUDEN			MCGRP	Revoked	Expired	120			
SMC0319	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked	Expired	120			
SMC0326	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked	Expired	120			
SMC0363	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked	Expired	120			

Permits of SMC0096 (15)

Class	Profile	ProfType	Access	When	UAcc	Warning	Erase	AuditS	AuditF	ACL count	Owner
APPL	SMC0096	Discrete	Read		None				Read	3	SYS1
Dataset	SMC0096.**	Generic	Owner		None				Read	1	SMC0096
JESSPOOL	TSTMVS01.STC.SMC0096.**	Generic	Alter		None				Read	5	SYS1
MQADMIN	MQ01.QUEUE.SMC0096.**	Generic	Alter		None				Read	3	SYS1
MQQUEUE	MQ01.SMC0096.**	Generic	Alter		None				Read	3	SYS1
OPERCMDS	MVS.CANCEL.STC.SMC0096.**	Generic	Update		None				Read	5	SYS1
OPERCMDS	MVS.CANCEL.TSU.SMC0096	Discrete	Update		None				Read	2	BABEYS
OPERCMDS	MVS.START.STC.SMC0096	Discrete	Update		None				Read	5	SYS1
OPERCMDS	MVS.START.STC.WEBS096	Discrete	Update		None				Read	2	BABEYS
OPERCMDS	MVS.STOP.STC.SMC0096	Discrete	Update		None				Read	5	SYS1
OPERCMDS	MVS.STOP.STC.WEBS096	Discrete	Update		None				Read	2	BABEYS

Find

Class: User ...

Search: ○ Exact ● Filter ○ Mask

<<Advanced

Name: contest

Installation data:

Owner:

Default Group:

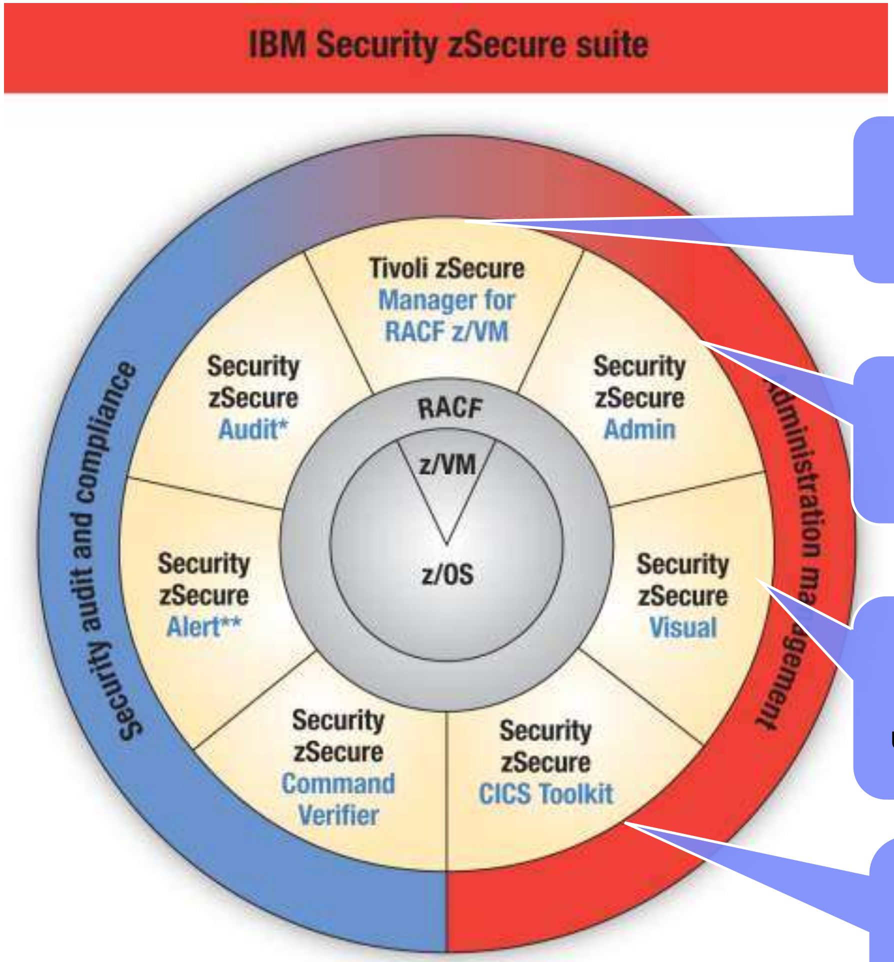
Revoke status: Any

Attempts: >

Segment: Any

OK Cancel

IBM Security zSecure Suite Overview


IBM Security zSecure suite
Security audit and compliance
dministration ma
gement
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

Administración y Auditoría para RACF en el ambiente VM

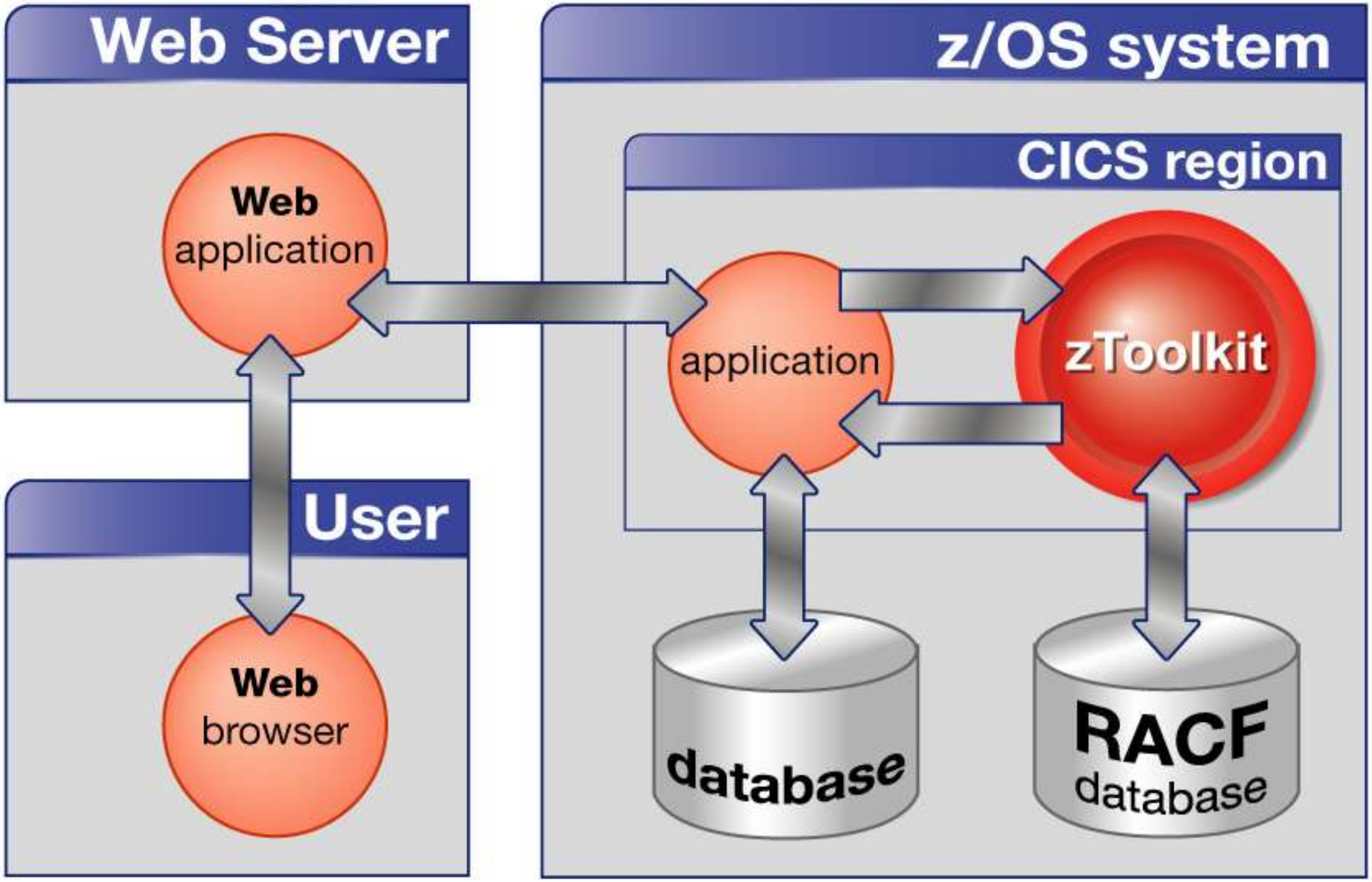
Permite administrar RACF de una manera mas eficiente y efectiva usando menos recursos

Reduce la necesidad de los recursos con habilidades en RACF (escasos) a través de una interfaz en Windows para administrar RACF

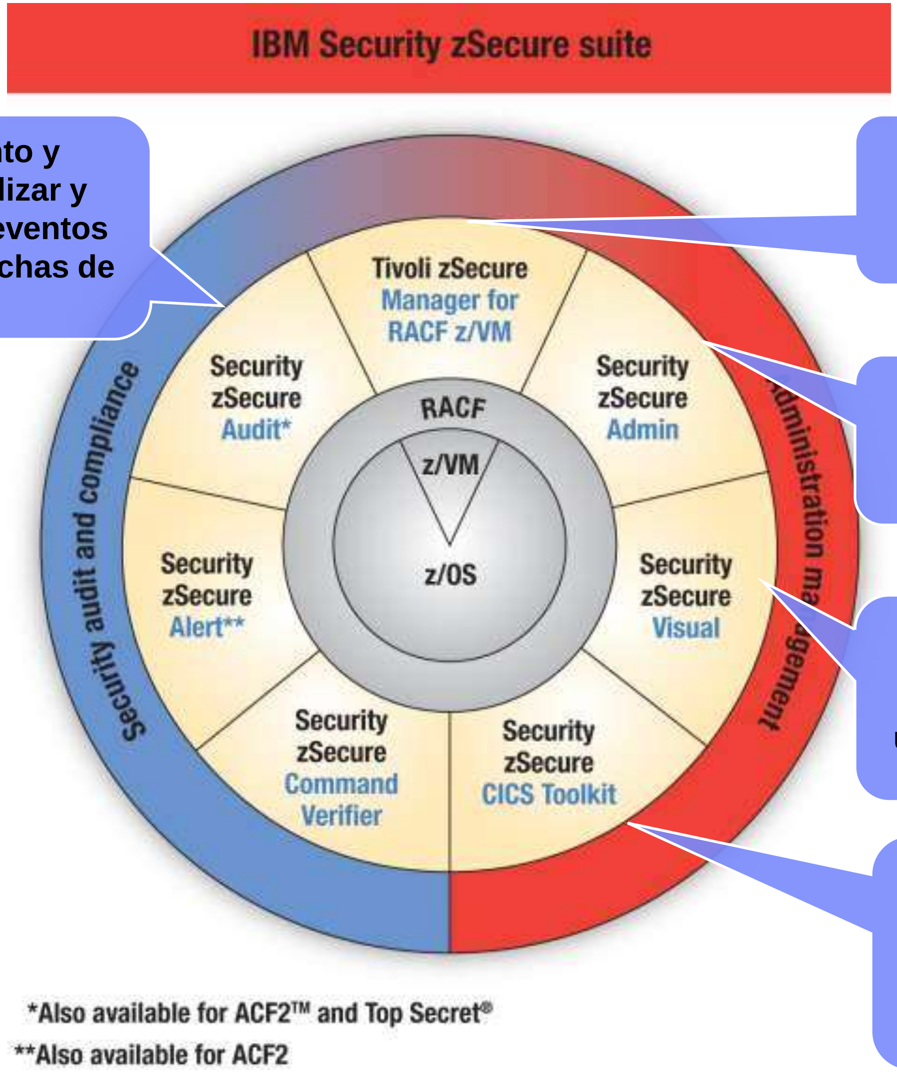
Permite llevar a cabo tareas administrativas desde el ambiente CICS, liberándolos recursos de RACF nativos

Nota: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

CICS Toolkit permite que cualquier aplicación Web use RACF



IBM Security zSecure Suite Overview


IBM Security zSecure suite
Security audit and compliance
dministration ma
gement
Tivoli zSecure Manager for RACF z/VM
Security zSecure Admin
Security zSecure Visual
Security zSecure CICS Toolkit
Security zSecure Command Verifier
Security zSecure Alert**
Security zSecure Audit*
RACF
z/VM
z/OS

*Also available for ACF2™ and Top Secret®

**Also available for ACF2

Solución de cumplimiento y auditoría que permite analizar y reportar automáticamente eventos de seguridad y detectar brechas de seguridad

Administración y Auditoría para RACF en el ambiente VM

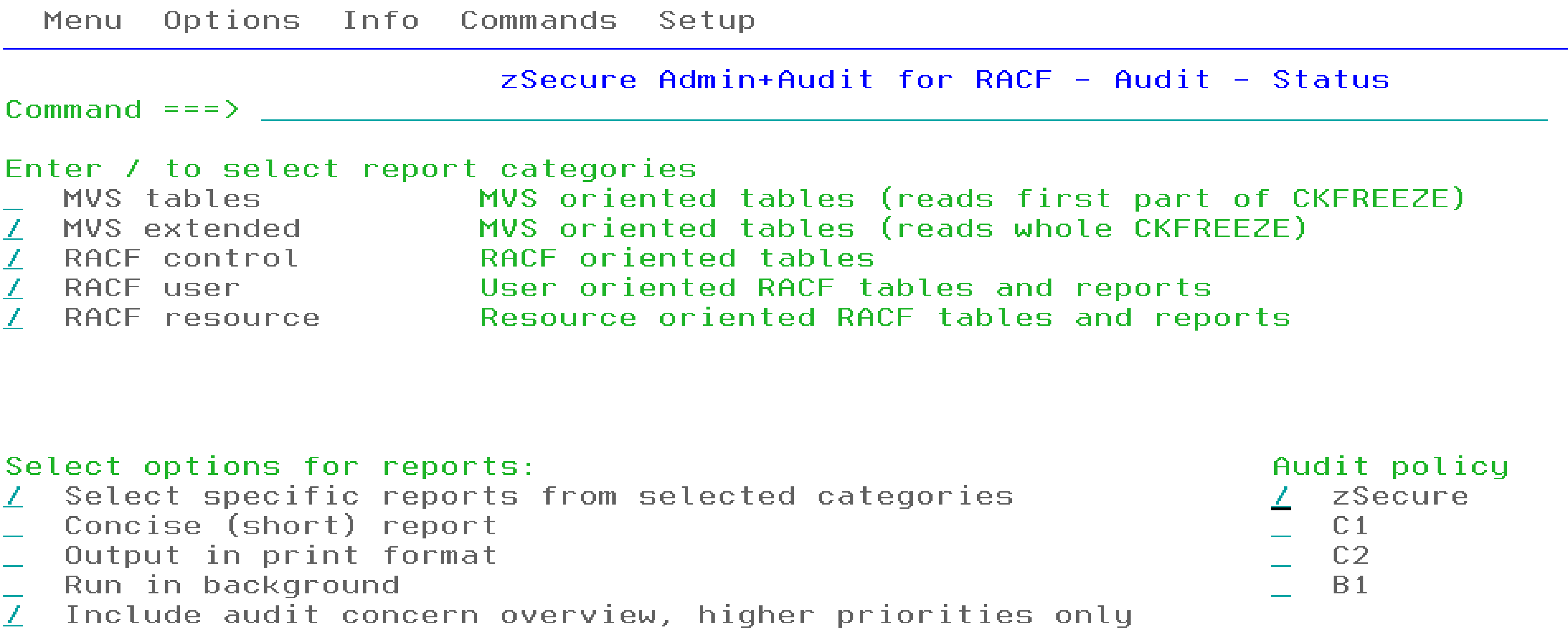
Permite administrar RACF de una manera mas eficiente y efectiva usando menos recursos

Reduce la necesidad de los recursos con habilidades en RACF (escasos) a través de una interfaz en Windows para administrar RACF

Permite llevar a cabo tareas administrativas desde el ambiente CICS, liberándolos recursos de RACF nativos

Nota: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

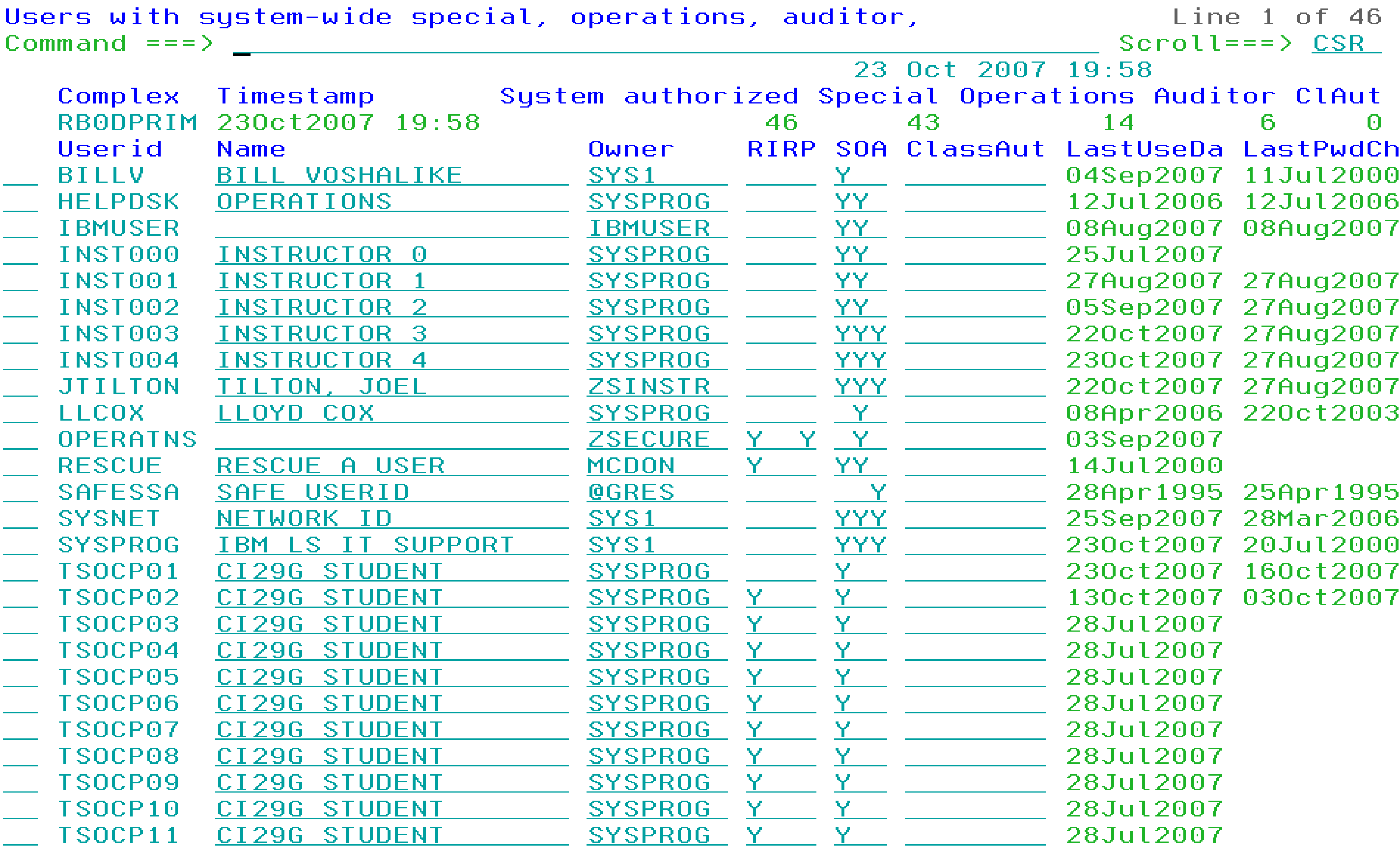
Selección de política de seguridad



```
  Menu   Options   Info   Commands   Setup

                         zSecure Admin+Audit for RACF - Audit - Status
Command ===> ________________________________________________________________

Enter / to select report categories
_  MVS tables              MVS oriented tables (reads first part of CKFREEZE)
/  MVS extended            MVS oriented tables (reads whole CKFREEZE)
/  RACF control            RACF oriented tables
/  RACF user               User oriented RACF tables and reports
/  RACF resource           Resource oriented RACF tables and reports



Select options for reports:                                     Audit policy
/  Select specific reports from selected categories             /  zSecure
_  Concise (short) report                                       _  C1
_  Output in print format                                       _  C2
_  Run in background                                            _  B1
/  Include audit concern overview, higher priorities only
```

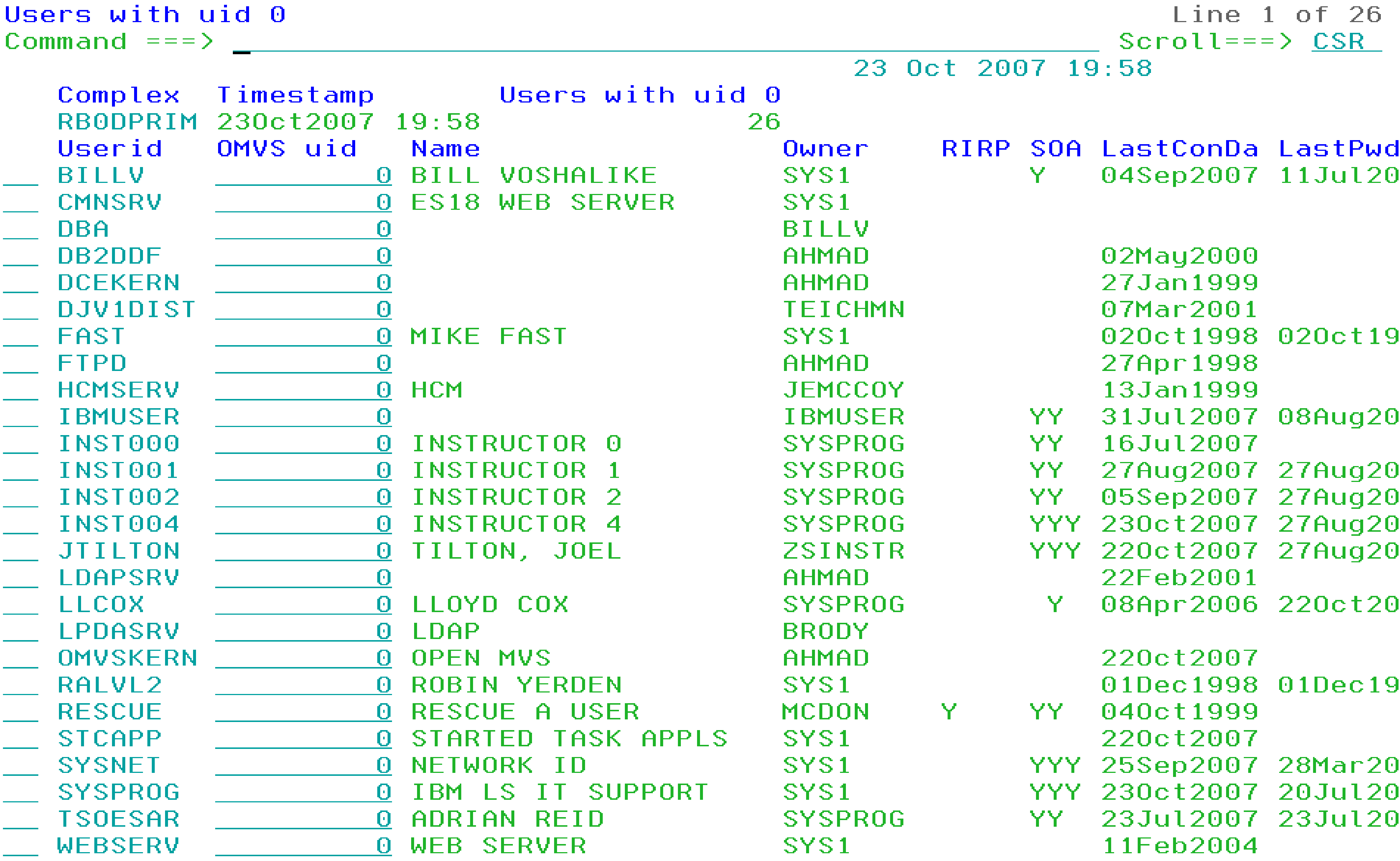
Active primary RACF data base & ckfreeze used for input

Reporte de los usuarios con privilegios



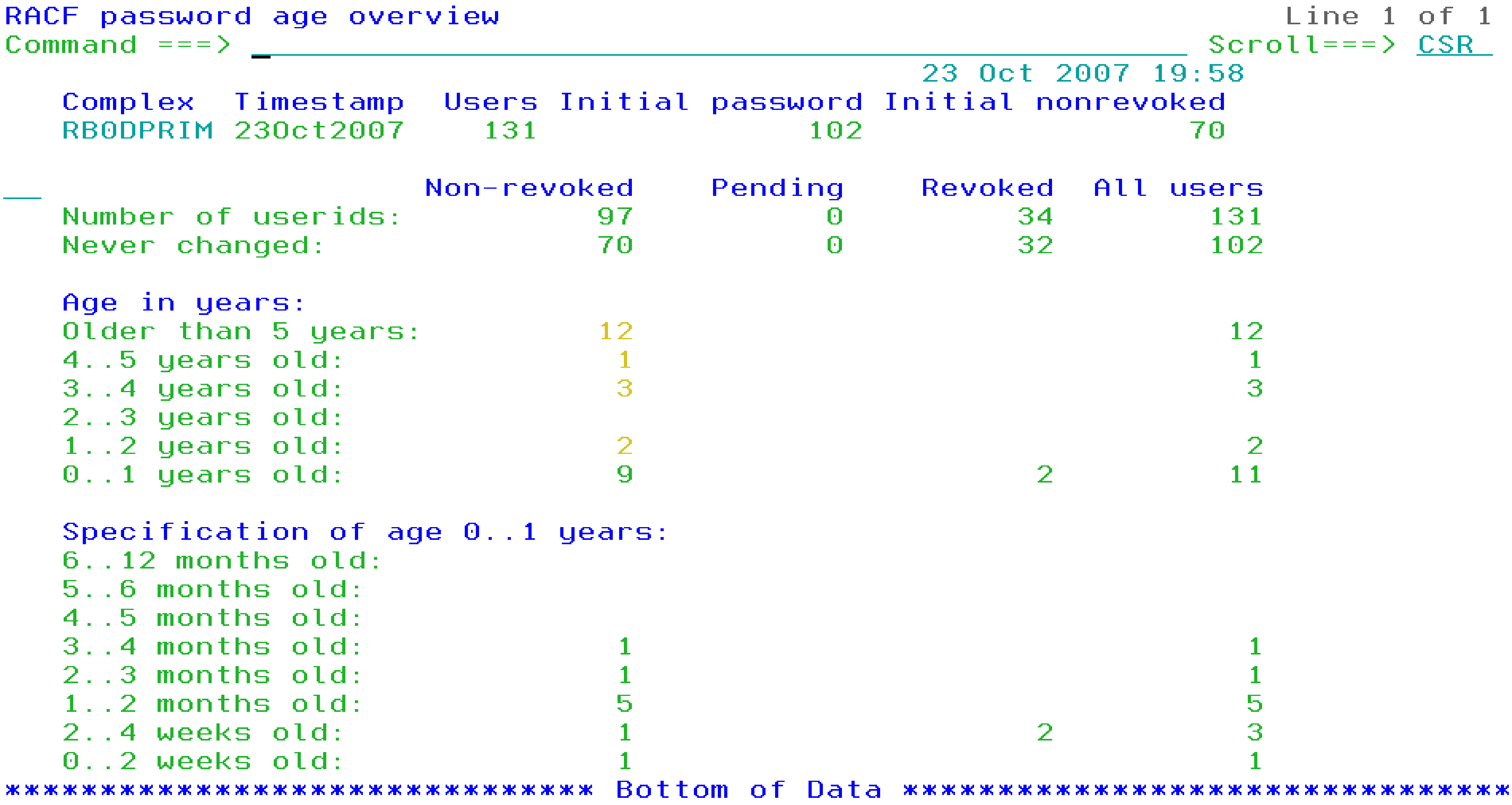
```
Users with system-wide special, operations, auditor,              Line 1 of 46
Command ===> _                                                 Scroll===> CSR
                                                17 Oct 2007 19:58
   Complex  Timestamp        System authorized Special Operations Auditor ClAut
   RB0DPRIM 23Oct2007 19:58                46      43         14       6     0
   Userid   Name                 Owner    RIRP SOA ClassAut LastUseDa LastPwdCh
   BILLV    BILL VOSHALIKE       SYS1          Y            04Sep2007 11Jul2000
   HELPDSK  OPERATIONS           SYSPROG       YY           12Jul2006 12Jul2006
   IBMUSER                       IBMUSER       YY           08Aug2007 08Aug2007
   INST000  INSTRUCTOR 0         SYSPROG       YY           25Jul2007
   INST001  INSTRUCTOR 1         SYSPROG       YY           27Aug2007 27Aug2007
   INST002  INSTRUCTOR 2         SYSPROG       YY           05Sep2007 27Aug2007
   INST003  INSTRUCTOR 3         SYSPROG       YYY          22Oct2007 27Aug2007
   INST004  INSTRUCTOR 4         SYSPROG       YYY          23Oct2007 27Aug2007
   JTILTON  TILTON, JOEL         ZSINSTR       YYY          22Oct2007 27Aug2007
   LLCOX    LLOYD COX            SYSPROG        Y           08Apr2006 22Oct2003
   OPERATNS                      ZSECURE  Y  Y  Y           03Sep2007
   RESCUE   RESCUE A USER        MCDON    Y    YY           14Jul2000
   SAFESSA  SAFE USERID          @GRES           Y          28Apr1995 25Apr1995
   SYSNET   NETWORK ID           SYS1          YYY          25Sep2007 28Mar2006
   SYSPROG  IBM LS IT SUPPORT    SYS1          YYY          23Oct2007 20Jul2000
   TSOCP01  CI29G STUDENT        SYSPROG       Y            23Oct2007 16Oct2007
   TSOCP02  CI29G STUDENT        SYSPROG  Y    Y            13Oct2007 03Oct2007
   TSOCP03  CI29G STUDENT        SYSPROG  Y    Y            28Jul2007
   TSOCP04  CI29G STUDENT        SYSPROG  Y    Y            28Jul2007
   TSOCP05  CI29G STUDENT        SYSPROG  Y    Y            28Jul2007
   TSOCP06  CI29G STUDENT        SYSPROG  Y    Y            28Jul2007
   TSOCP07  CI29G STUDENT        SYSPROG  Y    Y            28Jul2007
   TSOCP08  CI29G STUDENT        SYSPROG  Y    Y            28Jul2007
   TSOCP09  CI29G STUDENT        SYSPROG  Y    Y            28Jul2007
   TSOCP10  CI29G STUDENT        SYSPROG  Y    Y            28Jul2007
   TSOCP11  CI29G STUDENT        SYSPROG  Y    Y            28Jul2007
```

Evaluar quien tiene el uid 0



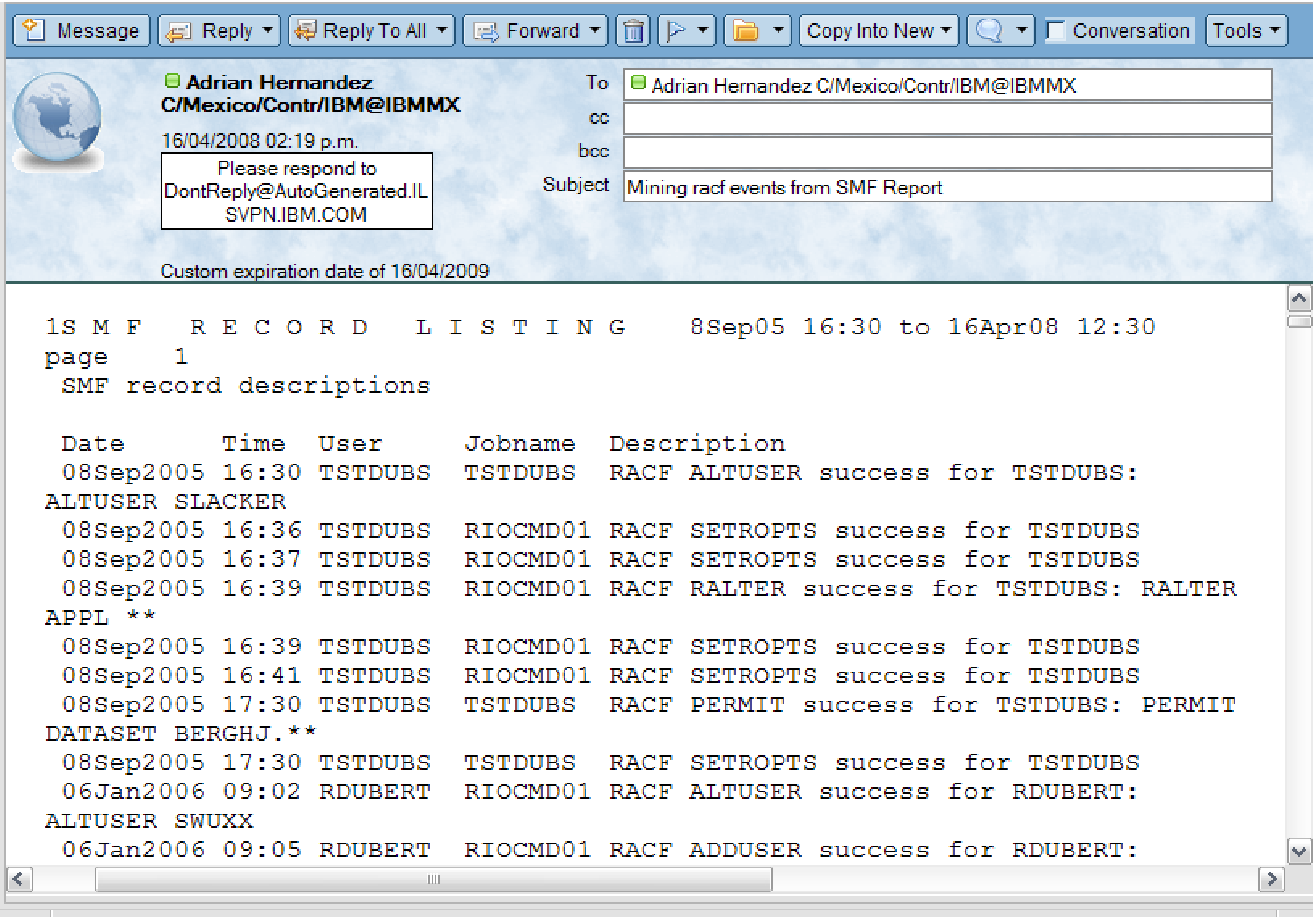
```
Users with uid 0                                                  Line 1 of 26
Command ===> _________________________________________________ Scroll===> CSR
                                                 23 Oct 2007 19:58
    Complex  Timestamp        Users with uid 0
    RB0DPRIM 23Oct2007 19:58              26
    Userid   OMVS uid  Name                  Owner    RIRP SOA LastConDa LastPwd
___ BILLV    _________0 BILL VOSHALIKE        SYS1          Y   04Sep2007 11Jul20
___ CMNSRV   _________0 ES18 WEB SERVER       SYS1
___ DBA      _________0                       BILLV
___ DB2DDF   _________0                       AHMAD             02May2000
___ DCEKERN  _________0                       AHMAD             27Jan1999
___ DJV1DIST _________0                       TEICHMN           07Mar2001
___ FAST     _________0 MIKE FAST             SYS1              02Oct1998 02Oct19
___ FTPD     _________0                       AHMAD             27Apr1998
___ HCMSERV  _________0 HCM                   JEMCCOY           13Jan1999
___ IBMUSER  _________0                       IBMUSER       YY  31Jul2007 08Aug20
___ INST000  _________0 INSTRUCTOR 0          SYSPROG       YY  16Jul2007
___ INST001  _________0 INSTRUCTOR 1          SYSPROG       YY  27Aug2007 27Aug20
___ INST002  _________0 INSTRUCTOR 2          SYSPROG       YY  05Sep2007 27Aug20
___ INST004  _________0 INSTRUCTOR 4          SYSPROG       YYY 23Oct2007 27Aug20
___ JTILTON  _________0 TILTON, JOEL          ZSINSTR       YYY 22Oct2007 27Aug20
___ LDAPSRV  _________0                       AHMAD             22Feb2001
___ LLCOX    _________0 LLOYD COX             SYSPROG        Y  08Apr2006 22Oct20
___ LPDASRV  _________0 LDAP                  BRODY
___ OMVSKERN _________0 OPEN MVS              AHMAD             22Oct2007
___ RALVL2   _________0 ROBIN YERDEN          SYS1              01Dec1998 01Dec19
___ RESCUE   _________0 RESCUE A USER         MCDON    Y    YY  04Oct1999
___ STCAPP   _________0 STARTED TASK APPLS    SYS1              22Oct2007
___ SYSNET   _________0 NETWORK ID            SYS1          YYY 25Sep2007 28Mar20
___ SYSPROG  _________0 IBM LS IT SUPPORT     SYS1          YYY 23Oct2007 20Jul20
___ TSOESAR  _________0 ADRIAN REID           SYSPROG       YY  23Jul2007 23Jul20
___ WEBSERV  _________0 WEB SERVER            SYS1              11Feb2004
```

Detectar usuarios que no han cambiado password



```
RACF password age overview                                         Line 1 of 1
Command ===> _________________________________________________ Scroll===> CSR
                                                23 Oct 2007 19:58
   Complex  Timestamp  Users Initial password Initial nonrevoked
   RBODPRIM 23Oct2007    131              102                 70

__                    Non-revoked    Pending    Revoked  All users
   Number of userids:          97          0         34        131
   Never changed:              70          0         32        102

   Age in years:
   Older than 5 years:         12                               12
   4..5 years old:              1                                1
   3..4 years old:              3                                3
   2..3 years old:
   1..2 years old:              2                                2
   0..1 years old:              9                     2         11

   Specification of age 0..1 years:
   6..12 months old:
   5..6 months old:
   4..5 months old:
   3..4 months old:             1                                1
   2..3 months old:             1                                1
   1..2 months old:             5                                5
   2..4 weeks old:              1                     2          3
   0..2 weeks old:              1                                1
******************************* Bottom of Data *********************************
```

Reportes – Texto (email)



Adrian Hernandez C/Mexico/Contr/IBM@IBMMX

16/04/2008 02:19 p.m.

Please respond to DontReply@AutoGenerated.ILSVPN.IBM.COM

Custom expiration date of 16/04/2009

To: Adrian Hernandez C/Mexico/Contr/IBM@IBMMX

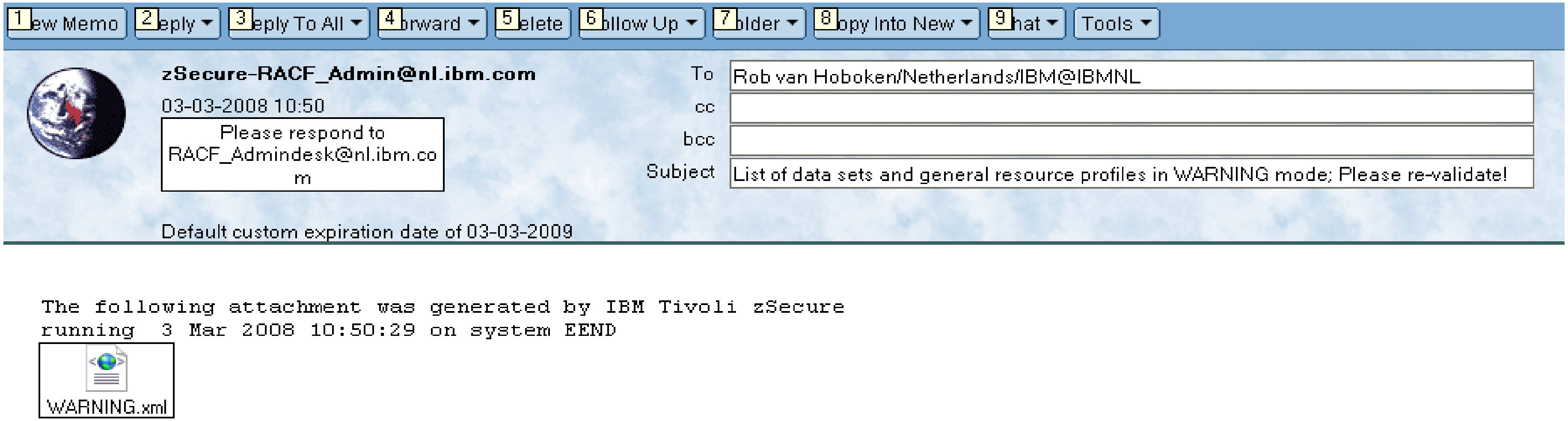
cc:

bcc:

Subject: Mining racf events from SMF Report

```
1S M F   R E C O R D   L I S T I N G   8Sep05 16:30 to 16Apr08 12:30
page     1
 SMF record descriptions

 Date         Time  User      Jobname   Description
 08Sep2005 16:30 TSTDUBS  TSTDUBS  RACF ALTUSER success for TSTDUBS:
ALTUSER SLACKER
 08Sep2005 16:36 TSTDUBS  RIOCMD01 RACF SETROPTS success for TSTDUBS
 08Sep2005 16:37 TSTDUBS  RIOCMD01 RACF SETROPTS success for TSTDUBS
 08Sep2005 16:39 TSTDUBS  RIOCMD01 RACF RALTER success for TSTDUBS: RALTER
APPL **
 08Sep2005 16:39 TSTDUBS  RIOCMD01 RACF SETROPTS success for TSTDUBS
 08Sep2005 16:41 TSTDUBS  RIOCMD01 RACF SETROPTS success for TSTDUBS
 08Sep2005 17:30 TSTDUBS  TSTDUBS  RACF PERMIT success for TSTDUBS: PERMIT
DATASET BERGHJ.**
 08Sep2005 17:30 TSTDUBS  TSTDUBS  RACF SETROPTS success for TSTDUBS
 06Jan2006 09:02 RDUBERT  RIOCMD01 RACF ALTUSER success for RDUBERT:
ALTUSER SWUXX
 06Jan2006 09:05 RDUBERT  RIOCMD01 RACF ADDUSER success for RDUBERT:
```

Reportes - XML (adjunto en email)



zSecure-RACF_Admin@nl.ibm.com

03-03-2008 10:50

Please respond to RACF_Admindesk@nl.ibm.com

Default custom expiration date of 03-03-2009

To Rob van Hoboken/Netherlands/IBM@IBMNL

cc

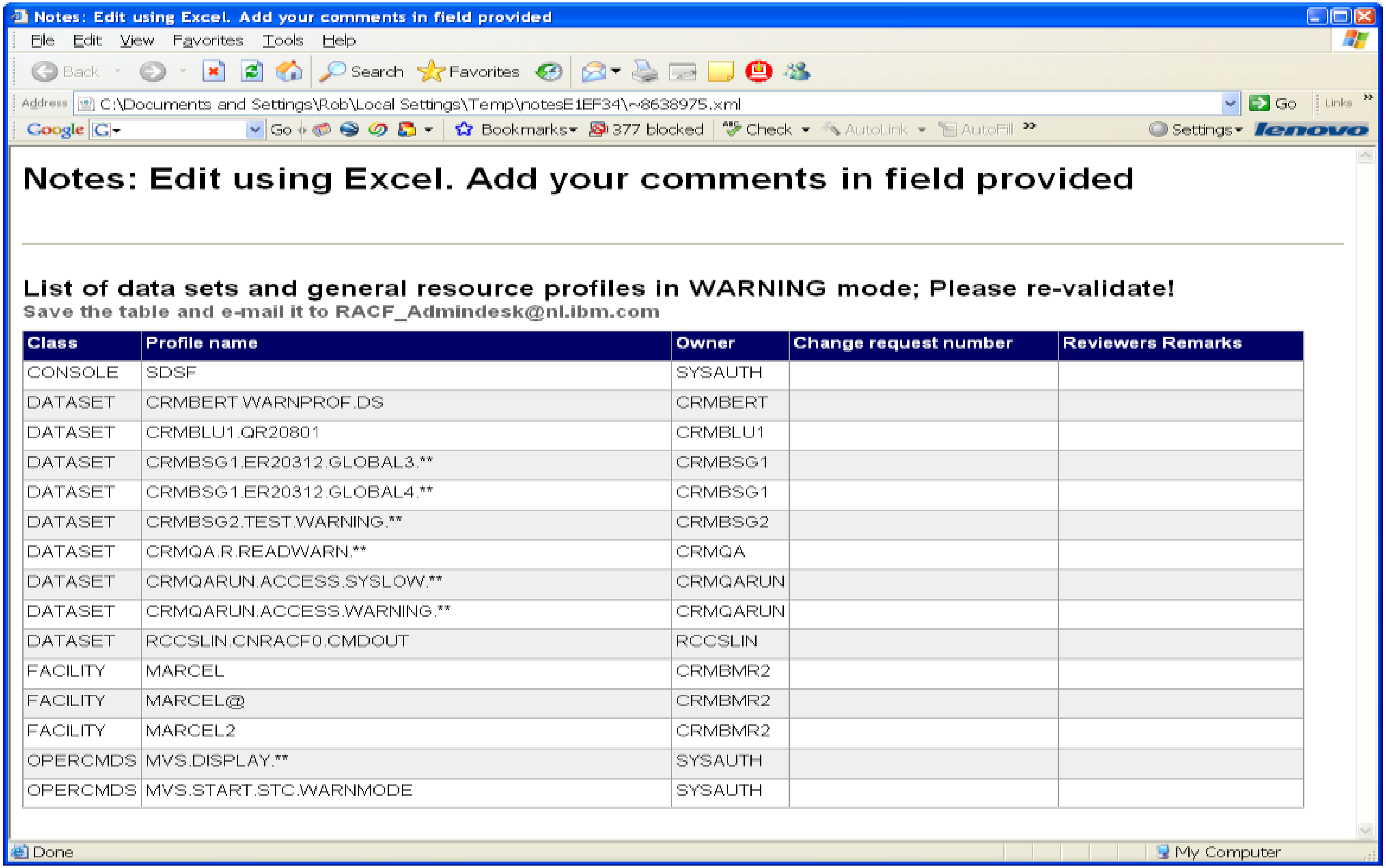
bcc

Subject List of data sets and general resource profiles in WARNING mode; Please re-validate!

```
The following attachment was generated by IBM Tivoli zSecure
running  3 Mar 2008 10:50:29 on system EEND
```

WARNING.xml

Reporte XML - Internet Explorer



Notes: Edit using Excel. Add your comments in field provided
File Edit View Favorites Tools Help
Back
Search
Favorites
Address
C:\Documents and Settings\Rob\Local Settings\Temp\notesE1EF34\~8638975.xml
Go
Links
Google
Go
Bookmarks
377 blocked
Check
AutoLink
AutoFill
Settings
lenovo
Done
My Computer

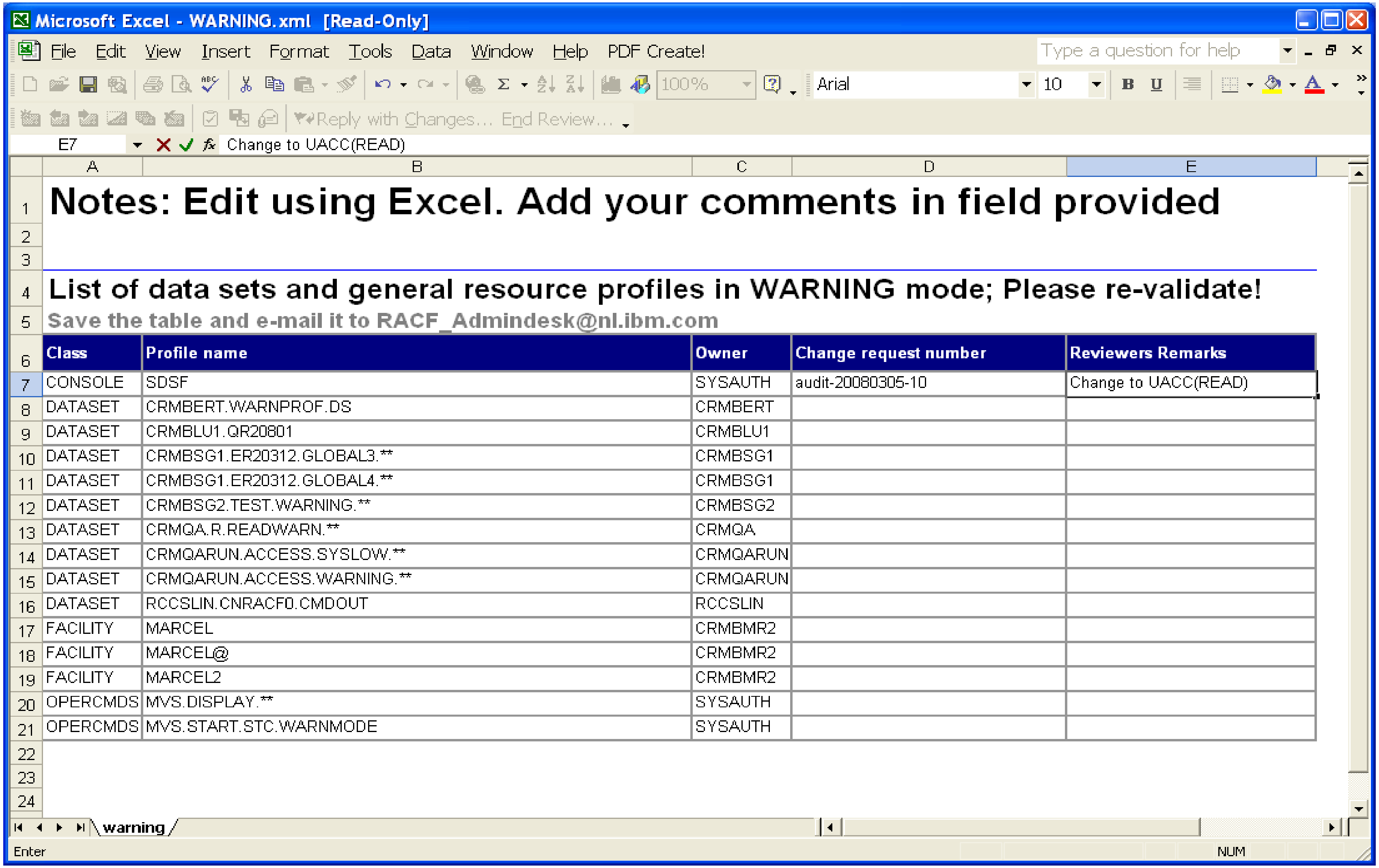
Notes: Edit using Excel. Add your comments in field provided

List of data sets and general resource profiles in WARNING mode; Please re-validate!

Save the table and e-mail it to RACF_Admindesk@nl.ibm.com

Class	Profile name	Owner	Change request number	Reviewers Remarks
CONSOLE	SDSF	SYSAUTH		
DATASET	CRMBERT.WARNPROF.DS	CRMBERT		
DATASET	CRMBLU1.QR20801	CRMBLU1		
DATASET	CRMBSG1.ER20312.GLOBAL3.**	CRMBSG1		
DATASET	CRMBSG1.ER20312.GLOBAL4.**	CRMBSG1		
DATASET	CRMBSG2.TEST.WARNING.**	CRMBSG2		
DATASET	CRMQA.R.READWARN.**	CRMQA		
DATASET	CRMQARUN.ACCESS.SYSLOW.**	CRMQARUN		
DATASET	CRMQARUN.ACCESS.WARNING.**	CRMQARUN		
DATASET	RCCSLIN.CNRACF0.CMDOUT	RCCSLIN		
FACILITY	MARCEL	CRMBMR2		
FACILITY	MARCEL@	CRMBMR2		
FACILITY	MARCEL2	CRMBMR2		
OPERCMDS	MVS.DISPLAY.**	SYSAUTH		
OPERCMDS	MVS.START.STC.WARNMODE	SYSAUTH		

Reporte XML- MS Excel


Microsoft Excel - WARNING.xml [Read-Only]
File Edit View Insert Format Tools Data Window Help PDF Create!
Type a question for help
100%
Arial
10
Reply with Changes... End Review...
E7
Change to UACC(READ)
warning
Enter
NUM

Notes: Edit using Excel. Add your comments in field provided

List of data sets and general resource profiles in WARNING mode; Please re-validate!

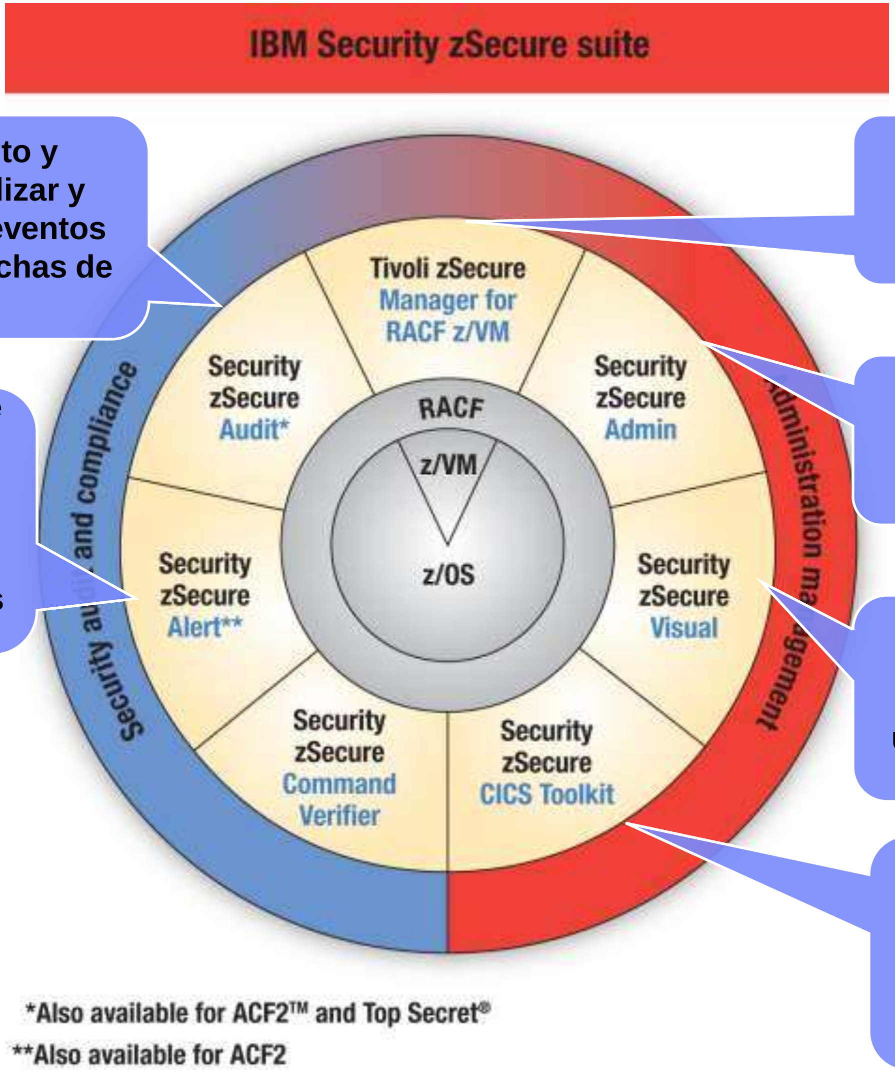
Save the table and e-mail it to RACF_Admindesk@nl.ibm.com

Class	Profile name	Owner	Change request number	Reviewers Remarks
CONSOLE	SDSF	SYSAUTH	audit-20080305-10	Change to UACC(READ)
DATASET	CRMBERT.WARNPROF.DS	CRMBERT		
DATASET	CRMBLU1.QR20801	CRMBLU1		
DATASET	CRMBSG1.ER20312.GLOBAL3.**	CRMBSG1		
DATASET	CRMBSG1.ER20312.GLOBAL4.**	CRMBSG1		
DATASET	CRMBSG2.TEST.WARNING.**	CRMBSG2		
DATASET	CRMQA.R.READWARN.**	CRMQA		
DATASET	CRMQARUN.ACCESS.SYSLOW.**	CRMQARUN		
DATASET	CRMQARUN.ACCESS.WARNING.**	CRMQARUN		
DATASET	RCCSLIN.CNRACF0.CMDOUT	RCCSLIN		
FACILITY	MARCEL	CRMBMR2		
FACILITY	MARCEL@	CRMBMR2		
FACILITY	MARCEL2	CRMBMR2		
OPERCMDS	MVS.DISPLAY.**	SYSAUTH		
OPERCMDS	MVS.START.STC.WARNMODE	SYSAUTH		

IBM Security zSecure Suite Overview

Solución de cumplimiento y auditoría que permite analizar y reportar automáticamente eventos de seguridad y detectar brechas de seguridad

Monitoreo en tiempo real de amenazas en el mainframe que permite monitorear intrusos e identificar errores de configuración que pueden obstaculizar los esfuerzos de cumplimiento



*Also available for ACF2™ and Top Secret®

**Also available for ACF2

Administración y Auditoría para RACF en el ambiente VM

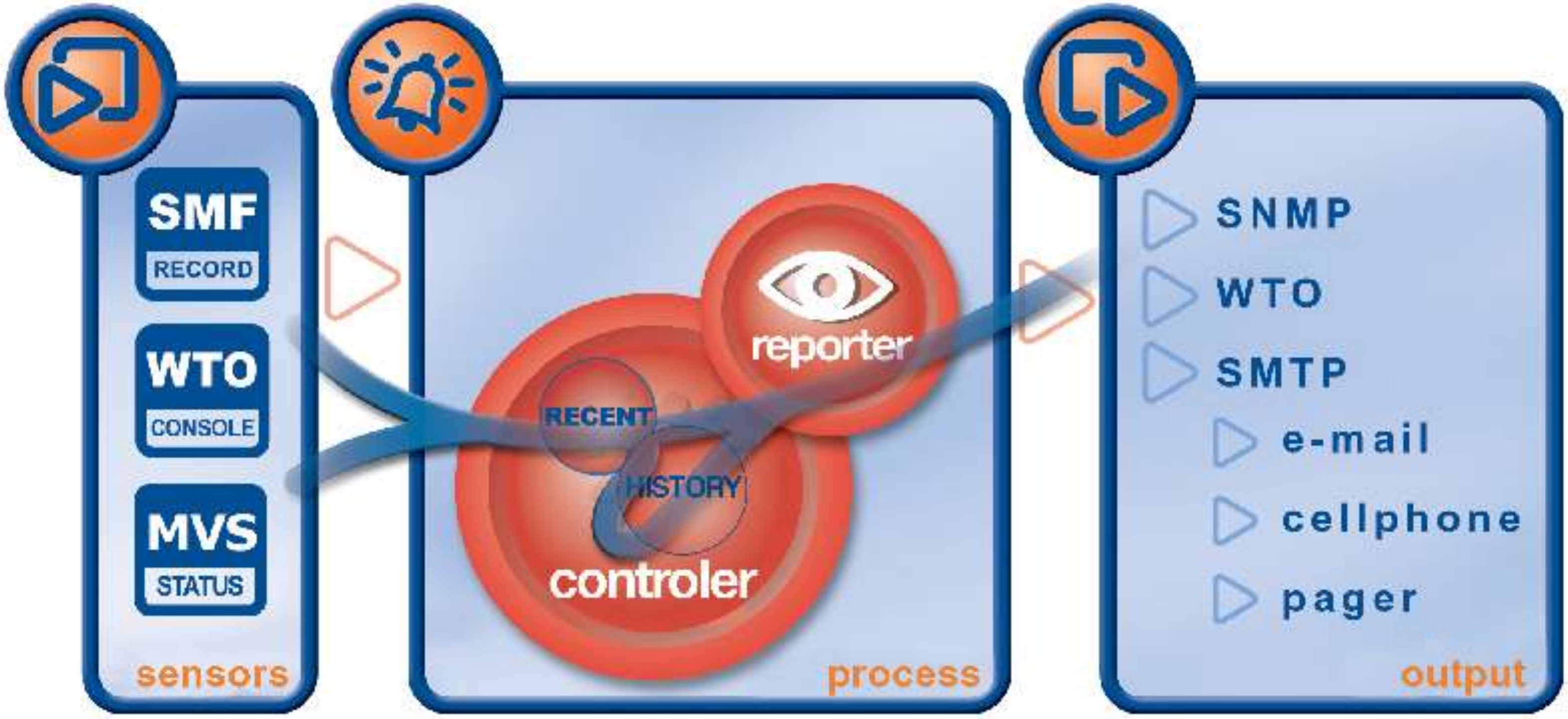
Permite administrar RACF de una manera mas eficiente y efectiva usando menos recursos

Reduce la necesidad de los recursos con habilidades en RACF (escasos) a través de una interfaz en Windows para administrar RACF

Permite llevar a cabo tareas administrativas desde el ambiente CICS, liberándolos recursos de RACF nativos

Nota: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

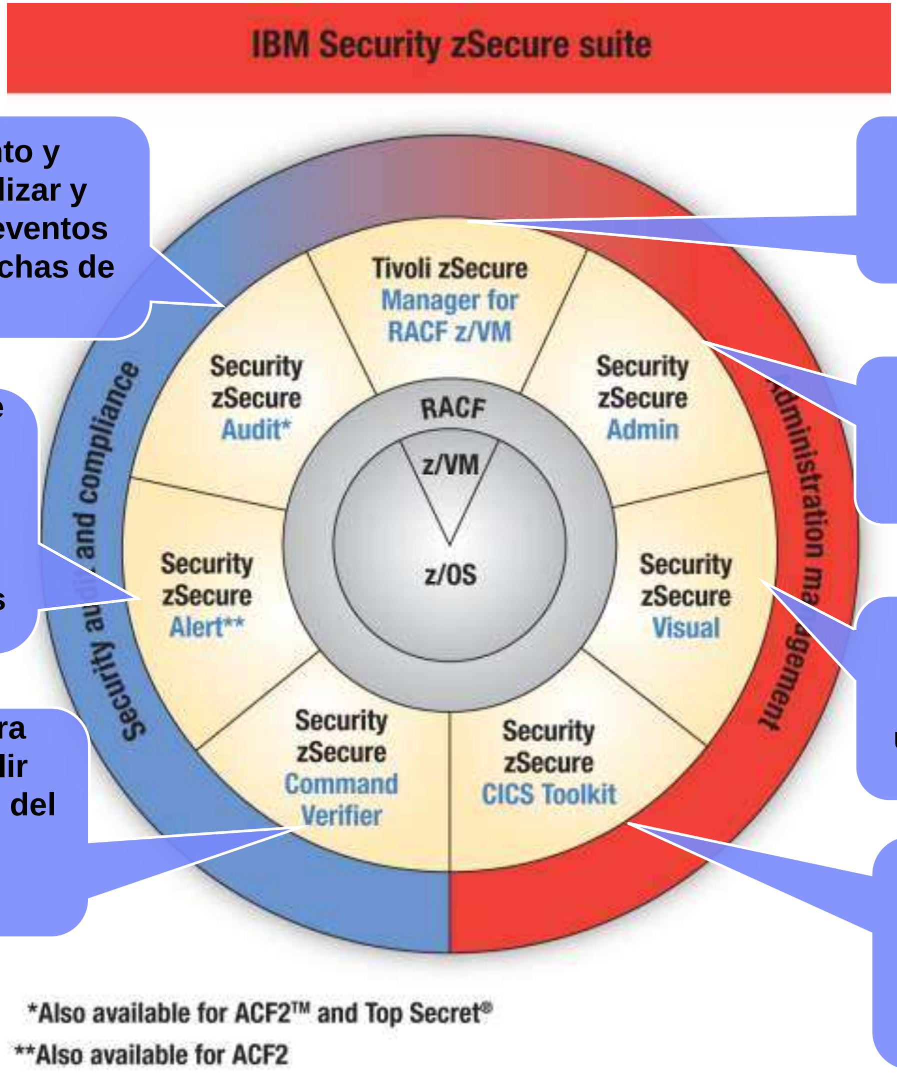
zAlert – Flujo de la información



Tipos de alertas - zSecure Alert

- Inicios de sesión no deseados e intentos
  - Inicios de sesión de usuarios desconocidos
  - Inicios de sesión con el userid de emergencia
  - Inicio de sesión con superusuarios de UNIX
- Comportamientos de usuarios que violan la política de seguridad
  - Reciclado de password
  - Uso de usuarios por medio de comandos USS con uid 0, por ejemplo: su
  - Administrador propaga su autoridad
- Actividad sospechosa sobre el subsistema UNIX
  - Violaciones de acceso a archivos
  - Asignacion de atributos de programas o APF
  - Lectura o escritura global especifica
- Cambios que violan la política de seguridad
  - Adición o eliminación de autoridades del sistema
  - Revocar userids de producción
  - Otorgamiento de acceso universal excesivo
  - Deshabilitar opciones de seguridad del sistema (SETROPTS)
  - Deshabilitar Audit trail
- Recursos principales del sistema en riesgo
  - Actualización del dataset del sistema
  - Adición dinámica de dataset APF
  - Los buffers del SMF se saturan, riesgo de perdida de datos
  - Tareas iniciadas sin autoridad especifica

IBM Security zSecure Suite Overview



*Also available for ACF2™ and Top Secret®

**Also available for ACF2

Solución de cumplimiento y auditoría que permite analizar y reportar automáticamente eventos de seguridad y detectar brechas de seguridad

Monitoreo en tiempo real de amenazas en el mainframe que permite monitorear intrusos e identificar errores de configuración que pueden obstaculizar los esfuerzos de cumplimiento

Solución de seguridad para aplicar un política y cumplir con regulaciones internas o del mercado previniendo la ejecución de comandos erróneos

Administración y Auditoría para RACF en el ambiente VM

Permite administrar RACF de una manera mas eficiente y efectiva usando menos recursos

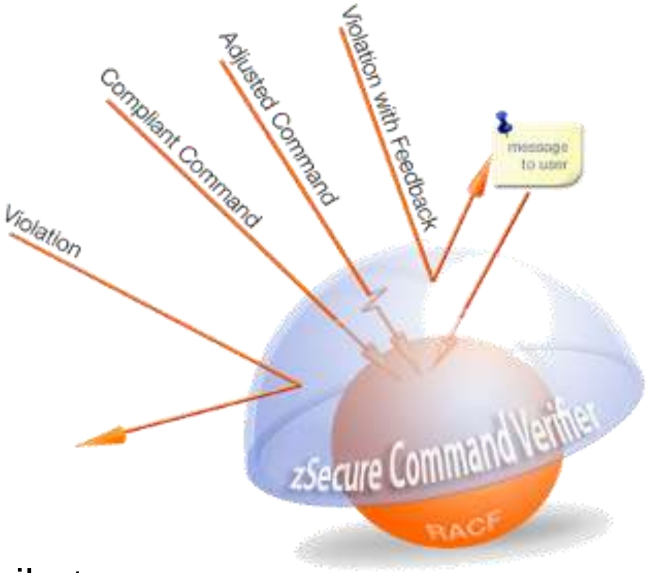
Reduce la necesidad de los recursos con habilidades en RACF (escasos) a través de una interfaz en Windows para administrar RACF

Permite llevar a cabo tareas administrativas desde el ambiente CICS, liberándolos recursos de RACF nativos

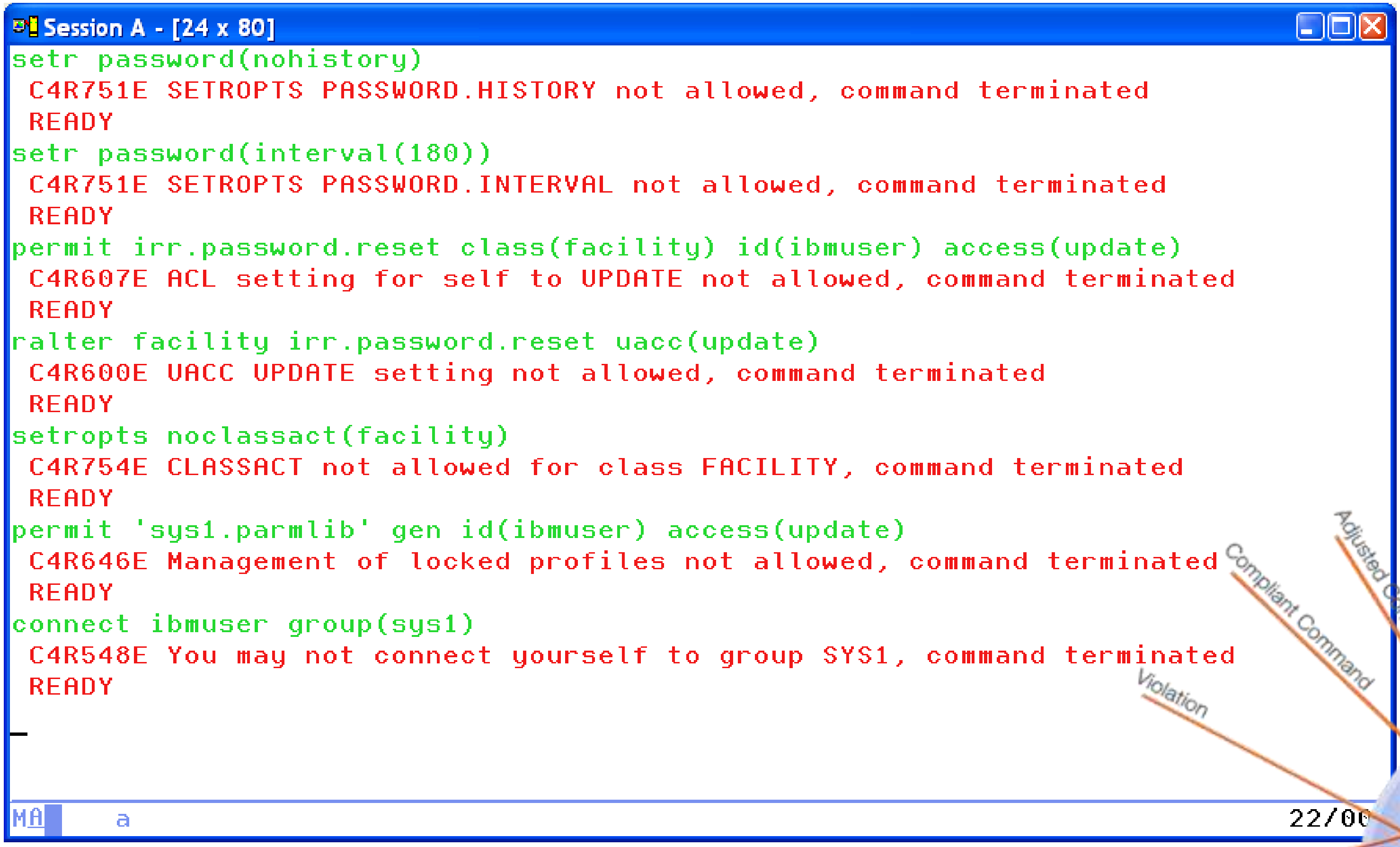
Nota: ACF2 and Top Secret are either registered trademarks or trademarks of CA, Inc. or one of its subsidiaries.

Command Verifier protege RACF y más

- Control completo sobre todos los comandos RACF
  - **SOX Compliance & otras regulaciones**
- Control sobre la ejecución de comandos
- Hace cumplir los estandares de la instalacción
  - Convenciones del nombramiento
  - Defaults para valores faltantes
  - Valores obligatorios
  - Estandares de niveles de acceso
  - Incremento de autoridad no permitida
    - Grupo special no puede pasar a lo largo de los atributos
  - Previene cambios a las listas de control de acceso (ACL)
  - Previene el uso de palabras clave (Trusted, Privileged)
  - Previene cambios en la configuración de RACF (SETROPTS)
- Logs a SMF (opcional)
- Audit trail en los profiles de RACF (opcional)

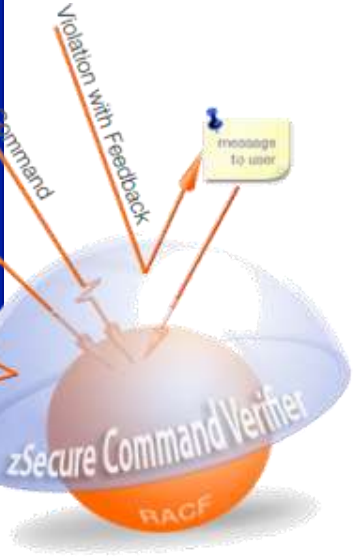


SOX Compliance usando Command Verifier



Session A - [24 x 80]

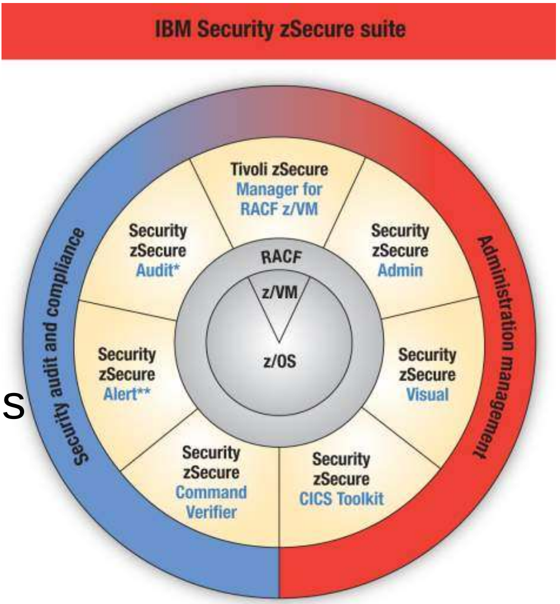
```
setr password(nohistory)
 C4R751E SETROPTS PASSWORD.HISTORY not allowed, command terminated
 READY
setr password(interval(180))
 C4R751E SETROPTS PASSWORD.INTERVAL not allowed, command terminated
 READY
permit irr.password.reset class(facility) id(ibmuser) access(update)
 C4R607E ACL setting for self to UPDATE not allowed, command terminated
 READY
ralter facility irr.password.reset uacc(update)
 C4R600E UACC UPDATE setting not allowed, command terminated
 READY
setropts noclassact(facility)
 C4R754E CLASSACT not allowed for class FACILITY, command terminated
 READY
permit 'sys1.parmlib' gen id(ibmuser) access(update)
 C4R646E Management of locked profiles not allowed, command terminated
 READY
connect ibmuser group(sys1)
 C4R548E You may not connect yourself to group SYS1, command terminated
 READY
_

MA      a                                                          22/00
```



Prevenir la ejecución de comandos que pueden corromper la seguridad del sistema

Beneficios de Seguridad de la suite zSecure
Consolidar y centralizar la gestión de la Seguridad

- **Simplificar la administración de seguridad y aprovisionamiento:**
  - Reducir el tiempo de administración, esfuerzo y costo
  - Habilitar administración descentralizada
  - Tiempo de respuesta rápido
  - Reducir el tiempo de entrenamiento necesario para nuevos administradores
  - Aplicar la política de seguridad e implementarlas mejores practicas
- **Automatizar auditoría, monitoreo y cumplimiento:**
  - Pasar auditorias de manera mas sencilla, mejorar postura de seguridad.
  - Ahorrar tiempo y costos mejorando la seguridad y el manejo de incidentes para gestionar el riesgo
  - Incrementar la efectividad operacional
- **Reducir costos y mejorar ROI**


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

धन्यवाद

Hindi

Hindi

多謝

Traditional Chinese

ขอบคุณ

Thai

Спасибо

Russian

Thank You

English

Gracias

Spanish

Obrigado

Brazilian Portuguese

شكرا

Arabic

Grazie

Italian

多谢

Simplified Chinese

Danke

German

Merci

French

நன்றி

Tamil

Tamil

ありがとうございました

Japanese

감사합니다

Korean

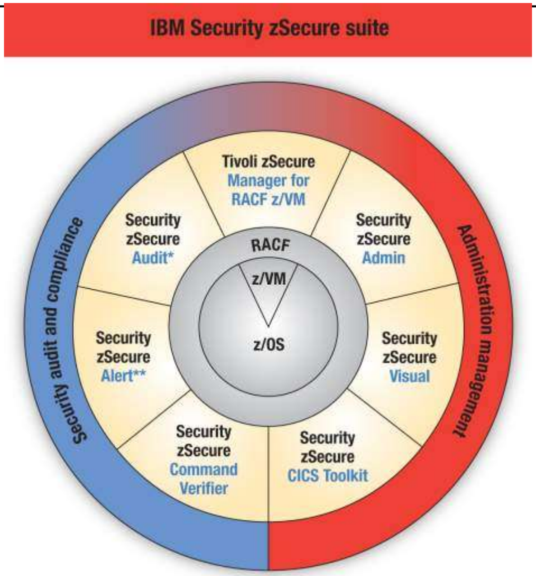
zEnterprise.

A New Dimension in Computing

Backup Product Charts

Security zSecure Suite

The zSecure Suite adds a user-friendly layer onto the mainframe that enables superior administration coupled with audit, alert and monitoring capabilities for z/OS Resource Access Control Facility (RACF)



IBM Security zSecure suite
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
Security audit and compliance
Administration management

Key Features

- **The zSecure suite improves mainframe security, improves the efficiency of administration and enhances the ability for the mainframe to be the hub of enterprise security.**
- Administration and provisioning:
  - **Admin** enhances security administration and user management for RACF
  - **Visual** offers a Windows GUI to RACF
  - **CICS Toolkit** for Extensibility with CICS support
- Audit, monitoring and compliance:
  - **Command Verifier** offers automated security monitoring, protection
  - **Alert** provides intrusion detection and alerting.
  - **Audit** provides event detection, analysis & reporting and system integrity audit & analysis

Benefits Summary

- Administration and provisioning:
  - Reduce administration time, effort and cost
  - Enable de-central administration
  - Quick response time, enabling business
  - Reduce training time needed for new administrators
- Audit, monitoring and compliance:
  - Pass audits more easily, improve security posture
  - Save time and costs through improved security and incident handling
  - Increase operational effectiveness

Tivoli Security Solution Offering for zEnterprise

- Enforce security policy compliance and reduce security vulnerabilities
- Centrally manage & protect access to applications, business services, infrastructure & data
- Leverage the mainframe as your Enterprise Security Hub

Tivoli zSecure Suite

- Cost-effective security administration, security policy enforcement, automated auditing and compliance to detect threats and reduce risk

NEW!

Tivoli zSecure Manager for RACF z/VM

- Mainframe audit solution for the enterprise security hub for analysis and reporting
- Mainframe administration enables efficient and effective RACF administration

NEW!

Tivoli Access Family

- Strengthen application security with centralized access control
- Secure collaboration and information sharing with web & federated SSO
- Enable B2C user self services and Cloud/SaaS access control
- Simplify mainframe application integration with security run-time services
- Protect data access with entitlement management and enforcement

Includes:
Tivoli Identity and Access Assurance solution
Tivoli Identity Manager for Linux on System z
Tivoli Security Management for z/OS

Lo nuevo en zSecure Suite 1.12

- Soporta RACF Remote Sharing Facility (RRSF)
- Aplicar comandos a multiples profiles
- Administración de z/OS UNIX
- Nuevo roporte y reporteo de registros SMF
- Habilidad para enviar alertas a un syslog UNIX
- Soporte de alertas TCP/IP y auditoria
- Soporta z/OS V1.12 y las nuevas capacidades de RACF:
  - Soporte de los nuevos campos de RACF y nuevos valores para certificados
  - Soporte a nuevos exits dinamicos para incrementar la seguridad
  - Suporte para la extensión de Distinguished Names (DN) de 1024 bytes
- Soporte DBCS (Double Byte Character Set) para esfuerzos de cumplimiento
- Y mas…

¿Qué hace Tivoli zSecure Manager for RACF z/VM V1.11?

IBM Tivoli zSecure Manager for RACF z/VM V1.11 permite administración y auditoría para el ambiente VM del mainframe:

- Las tareas de gestión del ambiente z/VM toman tiempo, con esta solución se pueden hacer estas tareas en un solo paso sin necesidad de conocimientos profundos de los comandos de RACF.
- Identifica y previene problemas en RACF antes de que se conviertan en una amenaza a la seguridad y cumplimiento
- Creación de registros de auditoría sin un esfuerzo (importante) manual
- Generación de reportes customizados.
- Suporte de recursos z/VM (minidisks, etc)