Congreso de Software IBM 2010

Construyendo un planeta más inteligente

IBMAGINA

Un planeta más inteligente necesita software más inteligente

Tino Veiga

Client Technical Professional

IBMAGINA

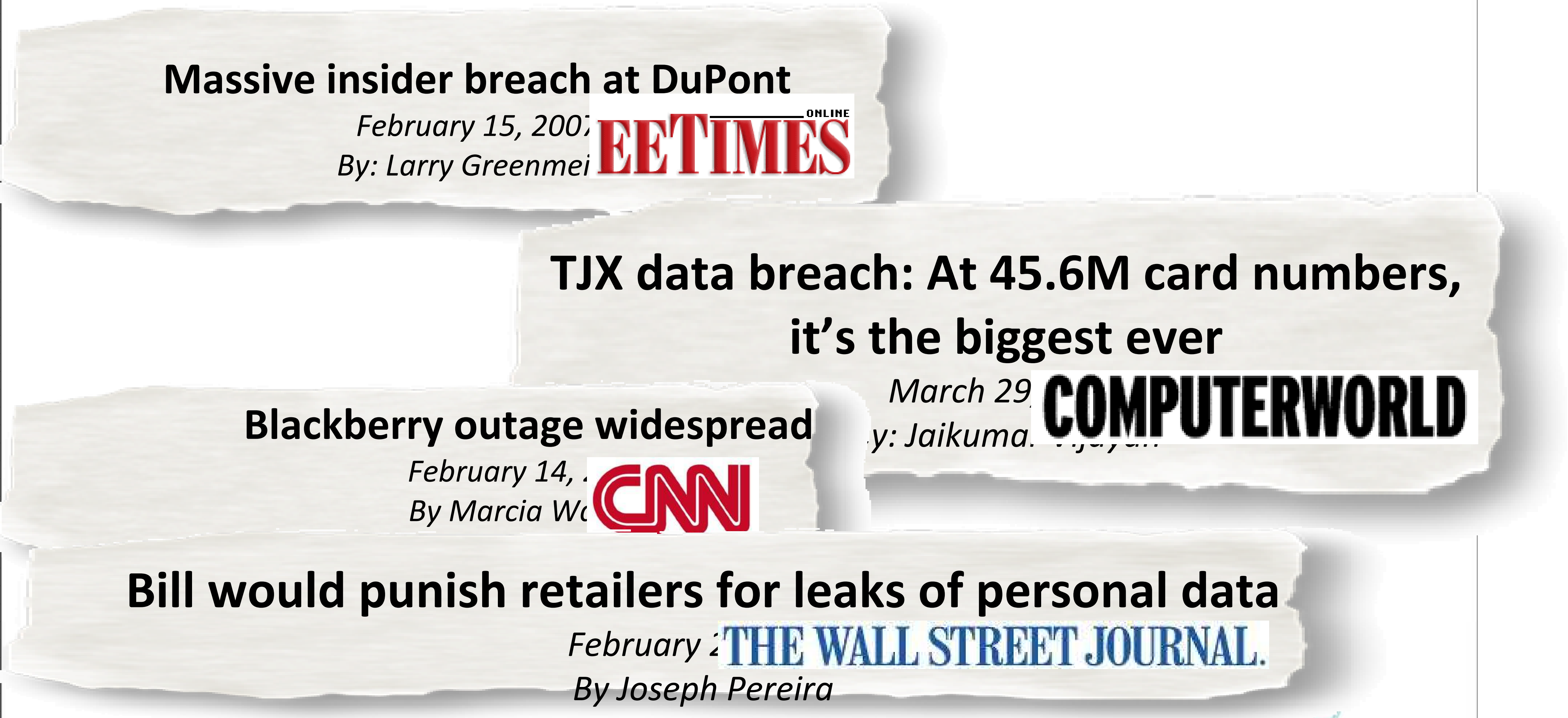
Un planeta más inteligente necesita software más inteligente

Suite zSecure

Gestión Integral de la Seguridad

Un planeta más inteligente necesita software más inteligente

Hace tiempo que el mundo no es seguro para las TIC



Massive insider breach at DuPont

February 15, 2007

By: Larry Greenmei

EETIMES ONLINE

TJX data breach: At 45.6M card numbers, it's the biggest ever

March 29,

y: Jaikuma

COMPUTERWORLD

Blackberry outage widespread

February 14,

By Marcia W

CNN

Bill would punish retailers for leaks of personal data

February 2

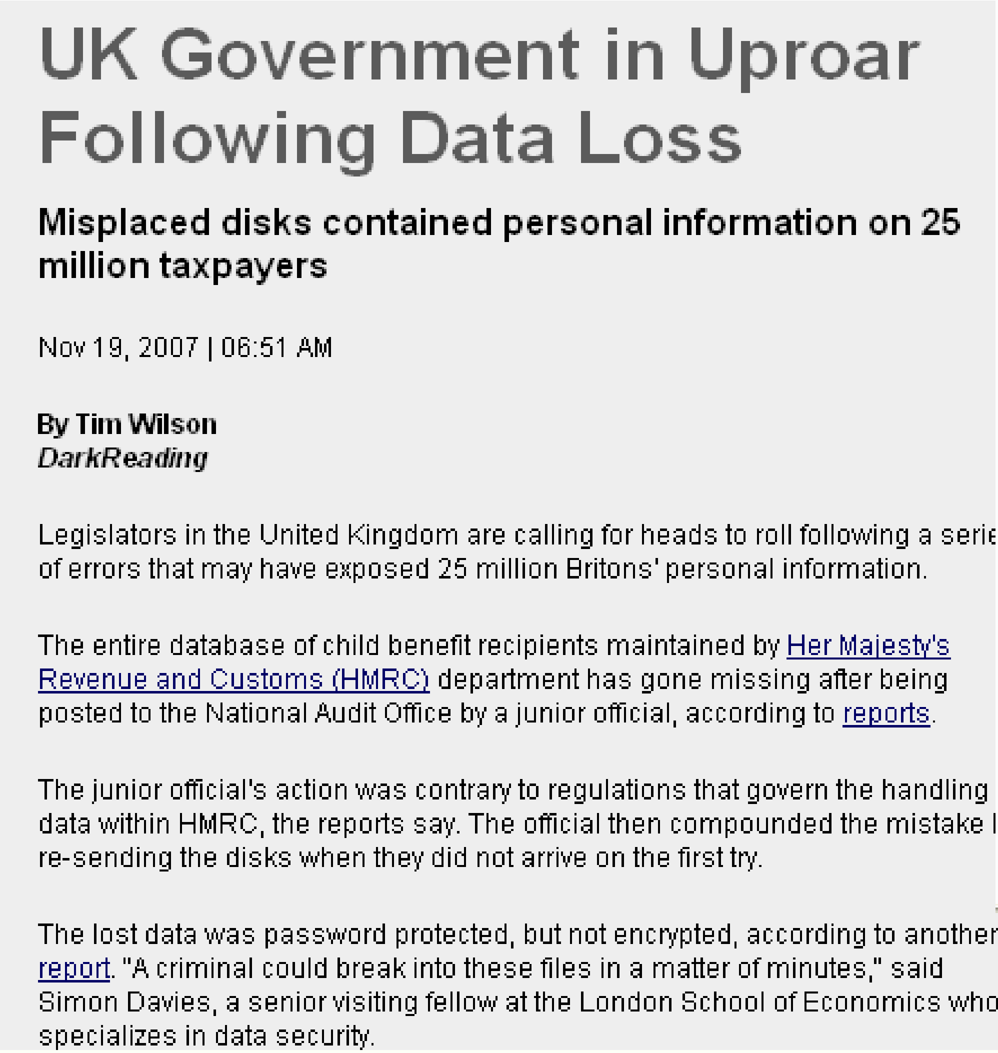
By Joseph Pereira

THE WALL STREET JOURNAL.

iTunes back to normal after holiday traffic quadruples
ABC News: December 28, 2006

IBMAGINA
Un planeta más inteligente necesita software más inteligente

.. no solo en US…



UK Government in Uproar Following Data Loss

Misplaced disks contained personal information on 25 million taxpayers

Nov 19, 2007 | 06:51 AM

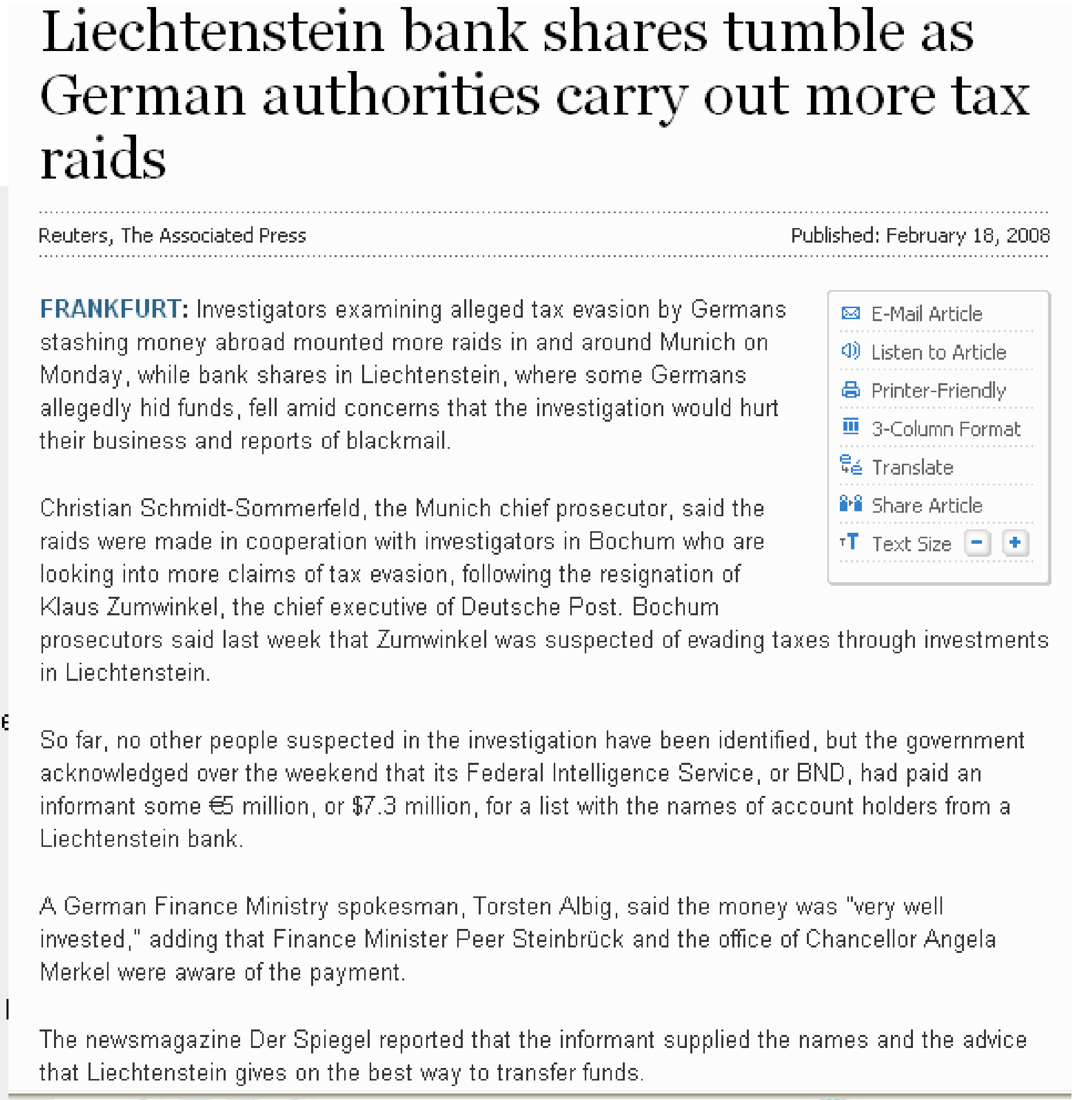
By Tim Wilson
DarkReading

Legislators in the United Kingdom are calling for heads to roll following a serie of errors that may have exposed 25 million Britons' personal information.

The entire database of child benefit recipients maintained by Her Majesty's Revenue and Customs (HMRC) department has gone missing after being posted to the National Audit Office by a junior official, according to reports.

The junior official's action was contrary to regulations that govern the handling data within HMRC, the reports say. The official then compounded the mistake l re-sending the disks when they did not arrive on the first try.

The lost data was password protected, but not encrypted, according to another report. "A criminal could break into these files in a matter of minutes," said Simon Davies, a senior visiting fellow at the London School of Economics who specializes in data security.



Liechtenstein bank shares tumble as German authorities carry out more tax raids

Reuters, The Associated Press — Published: February 18, 2008

FRANKFURT: Investigators examining alleged tax evasion by Germans stashing money abroad mounted more raids in and around Munich on Monday, while bank shares in Liechtenstein, where some Germans allegedly hid funds, fell amid concerns that the investigation would hurt their business and reports of blackmail.

Christian Schmidt-Sommerfeld, the Munich chief prosecutor, said the raids were made in cooperation with investigators in Bochum who are looking into more claims of tax evasion, following the resignation of Klaus Zumwinkel, the chief executive of Deutsche Post. Bochum prosecutors said last week that Zumwinkel was suspected of evading taxes through investments in Liechtenstein.

So far, no other people suspected in the investigation have been identified, but the government acknowledged over the weekend that its Federal Intelligence Service, or BND, had paid an informant some €5 million, or $7.3 million, for a list with the names of account holders from a Liechtenstein bank.

A German Finance Ministry spokesman, Torsten Albig, said the money was "very well invested," adding that Finance Minister Peer Steinbrück and the office of Chancellor Angela Merkel were aware of the payment.

The newsmagazine Der Spiegel reported that the informant supplied the names and the advice that Liechtenstein gives on the best way to transfer funds.

IBMAGINA
Un planeta más inteligente necesita software más inteligente

¿Y hoy en dia ?

IBM

SECURITYWEEK
INTERNET AND ENTERPRISE SECURITY NEWS, INSIGHTS & ANALYSIS

By Mike Lennon on Aug 25, 2010

IBM X-Force Report: Global Security Threats Reach Record Levels

IBM released its **X-Force 2010 Mid-Year Trend and Risk Report** today, which showed record threat levels in almost every area.

Web vulnerabilities lead the way, representing more than half of the **4,396** publicly disclosed vulnerabilities documented by the X-Force Research & Development team in the first half of 2010. This represents a **36 percent increase** over the same time period last year,with **55 percent** of the disclosed vulnerabilities having **no** vendor-supplied **patch** at the end of the period.

IBM®

Keep in mind that these figures don’t include custom-developed Web applications, which can also contain vulnerabilities.

On the positive side, the report noted that organizations were doing more to identify and disclose security vulnerabilities than in the past, helping to drive more open collaboration to identify and eliminate vulnerabilities before cyber criminals can exploit them.

IBMAGINA
Un planeta más inteligente necesita software más inteligente

¿Que está en riesgo?

- Marca Comercial
- Propiedad Intelectual
- Exposiciones Legales y Regulatorias
- Información del Cliente
- La confianza del Cliente
- El coste de remediar los problemas
- La interrupción del Negocio
- El trabajo

IBMAGINA

Un planeta más inteligente necesita software más inteligente

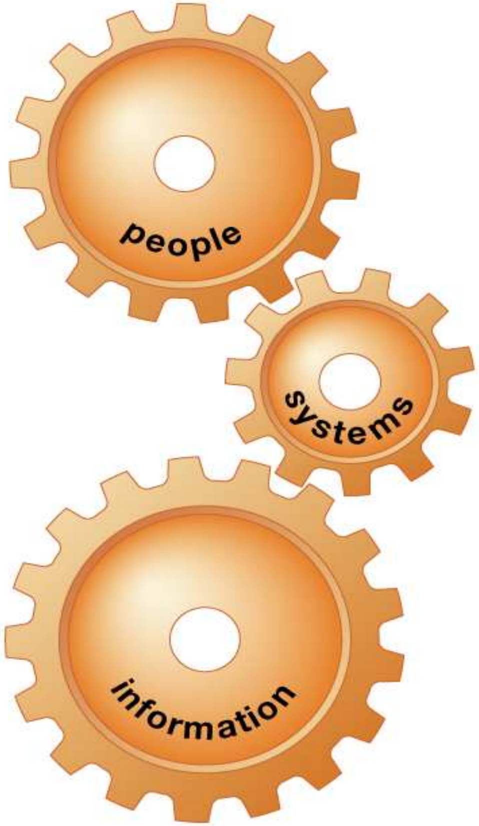
Retos en la seguridad de la información

El reto de negocio consiste en comprender si:

La información se usa adecuadamente

- Los sistemas de IT se usan/gestionan de manera eficiente y apropiada
- Los requisitos marcados por normas y/o políticas internas se cumplen
- La seguridad es efectiva y no interfiere con la continuidad del negocio

Y posteriormente arreglar los problemas



Visibilidad, Control, Automatización

IBMAGINA
Un planeta más inteligente necesita software más inteligente

Diferentes niveles de seguridad

Red

- Seguridad mínima
  - Estoy seguro de que mis sistemas están protegidos
- Alertas en tiempo real
  - Necesito saber rápidamente cuando ocurre un ataque, de manera que pueda tomar medidas inmediatamente
- Auditoría
  - Realizamos pruebas de penetración anualmente
- Monitorización
  - Revisamos los logs

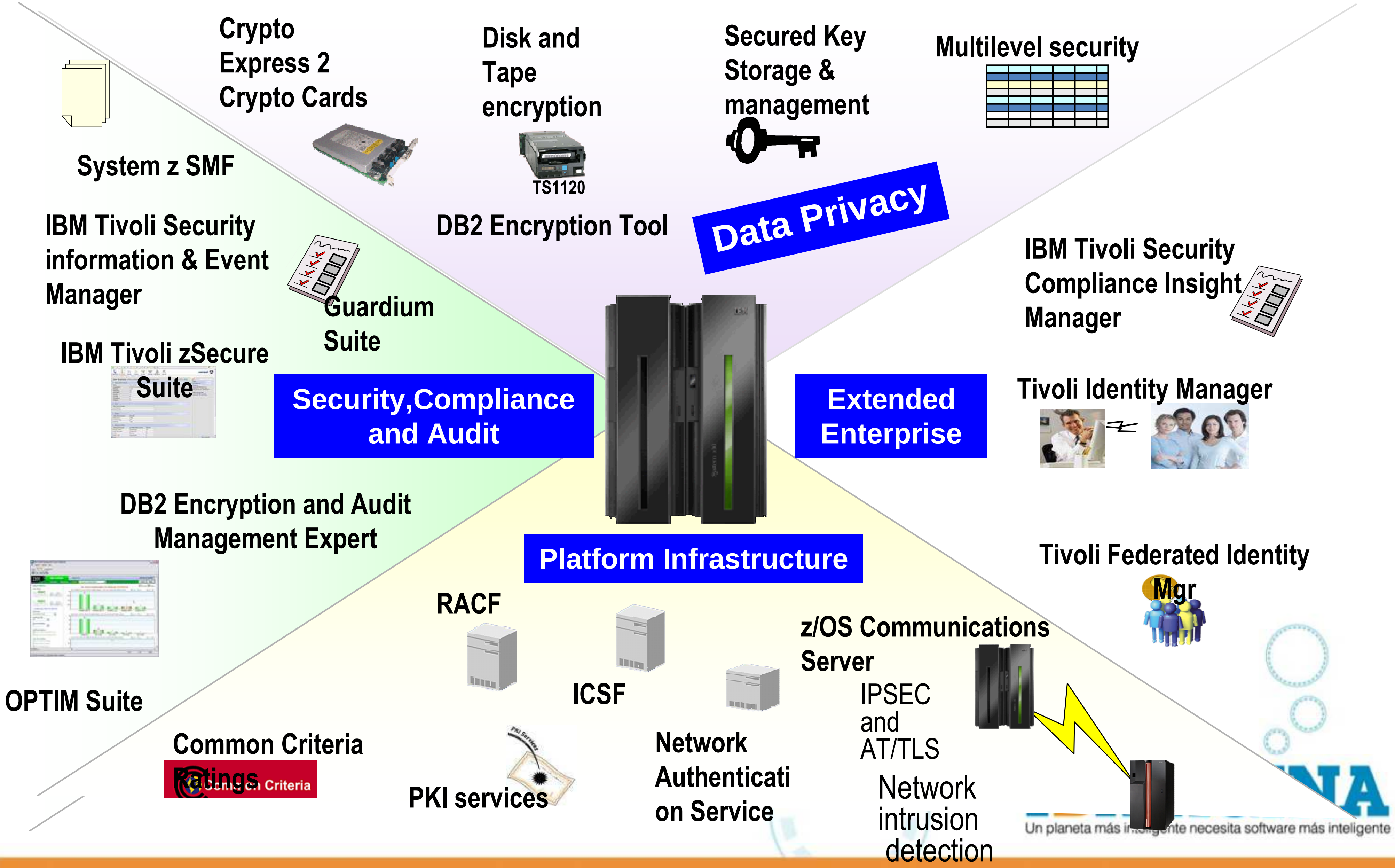
Diferentes niveles de seguridad

Mainframe

- Seguridad mínima
  - Estoy seguro de que mi gente no hace nada mal
- Auditoría
  - Necesito saber en donde están las exposiciones de seguridad
  - La conformidad con normas debe ser revisada de vez en cuando
- Monitorización
  - Se en donde están mis exposiciones de seguridad
  - Quiero estar seguro de que no sucede nada malo
- Alertas en tiempo real
  - Necesito saber rápidamente cuando ocurre algo inesperado, de manera que pueda reaccionar a tiempo

IBMAGINA
Un planeta más inteligente necesita software más inteligente

Elementos de Seguridad en System z



Crypto Express 2 Crypto Cards

Disk and Tape encryption

TS1120

Secured Key Storage & management

Multilevel security

System z SMF

DB2 Encryption Tool

Data Privacy

IBM Tivoli Security information & Event Manager

Guardium Suite

IBM Tivoli zSecure Suite

IBM Tivoli Security Compliance Insight Manager

Security,Compliance and Audit

Extended Enterprise

Tivoli Identity Manager

DB2 Encryption and Audit Management Expert

Platform Infrastructure

Tivoli Federated Identity Mgr

OPTIM Suite

RACF

ICSF

z/OS Communications Server

IPSEC and AT/TLS

Common Criteria Ratings

Common Criteria

PKI services

Network Authentication Service

Network intrusion detection

Un planeta más inteligente necesita software más inteligente

Informes de z/OS y RACF

- Eventos
  - Identificación de acciones y cambios
  - Tipicamente de registros de SMF
- Estados
  - Muestra definiciones, como las de privilegios especiales
  - Demasiado volumen de salida, riesgo de perdida de foco

Informes efectivos de z/OS y RACF

- **Detección de cambios**
  - **Detectar diferencias con informes previos**
  - **Cambios no detectados cuando se salta o se pierde un informe**

- **Verificación en base a referencias**
  - **Mostrar cuando las definiciones no cumplen los estándares**
  - **Típicamente se realiza comparando el estado contra una referencia base**

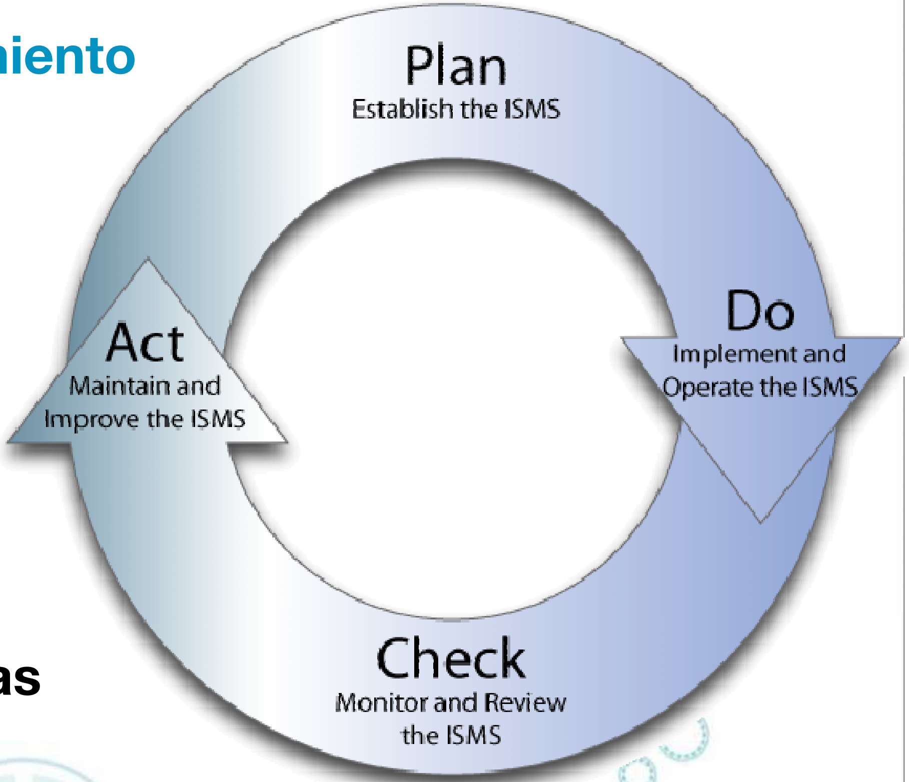
La automatización permite pasar de la
Auditoría
a la
Monitorización

IBMAGINA
Un planeta más inteligente necesita software más inteligente

Estándares de implantación
Documentos de referencia base

[ISO27001 Recommendations](#)
[for Information Security Management Systems (ISMS)](#)

- Describe los valores requeridos
  - Lista las excepciones aprobadas
- Cuando todos los sistemas está en cumplimiento
  - No se necesita ninguna acción
- Si se encuentra una discrepancia
  - Revertir el cambio o actualizar la referencia base
- La referencia base se convierte en la documentación para las implantaciones
  - Los informes mostrarán las discrepancias hasta que se solucionen
- Distribución via correo electrónico o publicación Web


Plan
Establish the ISMS
Do
Implement and Operate the ISMS
Check
Monitor and Review the ISMS
Act
Maintain and Improve the ISMS

IBMAGINA
Un planeta más inteligente necesita software más inteligente

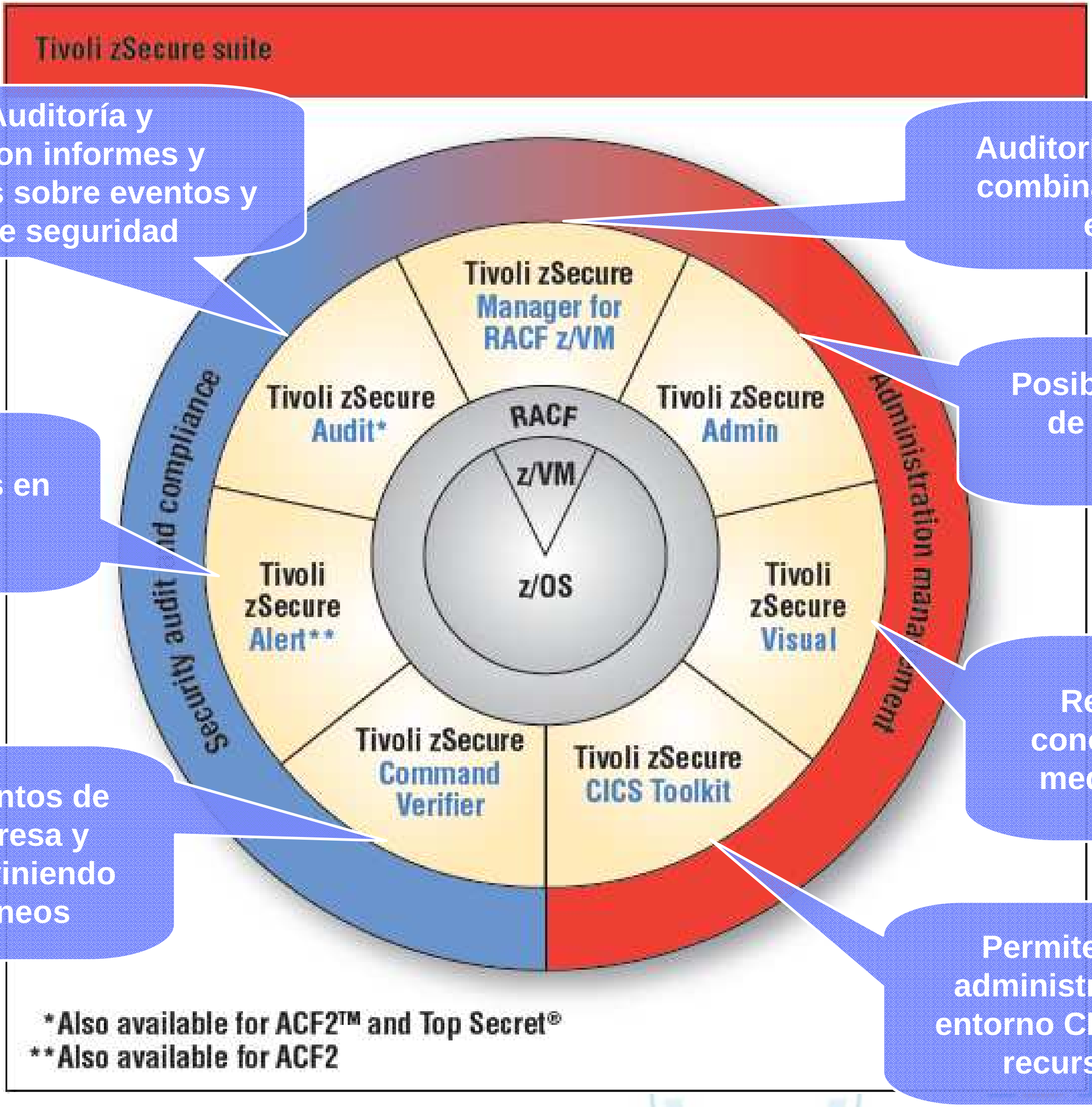
La suite IBM Tivoli zSecure

Solución de Auditoría y cumplimientos con informes y análisis automáticos sobre eventos y exposiciones de seguridad

Auditoría y Administración combinadas para RACF en entornos VM

Posibilita una administración de RACF mas eficiente y efectiva

Monitoriza amenazas en tiempo real


Tivoli zSecure suite
Security audit and compliance
Administration management
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

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

Reduce la necesidad de conocimientos de 3270, por medio de un GUI Windows

Fuerza cumplimientos de políticas de empresa y regulaciones, previniendo comandos erroneos

Permite realizar la administración desde entorno CICS, liberando recursos RACF

Un planeta más inteligente necesita software más inteligente

Caso de estudio: Cumplimientos

- Requerimientos Sarbanes Oxley o Basilea
  - Monitorizar cambios en sistema o seguridad (RACF o ACF2)
  - Monitorizar a los usuarios privilegiados
  - Monitorizar establecimiento de conexión irregulares
  - Verifizar paramentros de sistema contra una referencia base
  - Verifizar usuarios con alta autoridad sobre aplicaciones

- Soluciones disponibles?:
  - Costosa verificación diaria
  - Creación manual de “queries” e informes
  - Dificultades en la referencia base contra el estado real

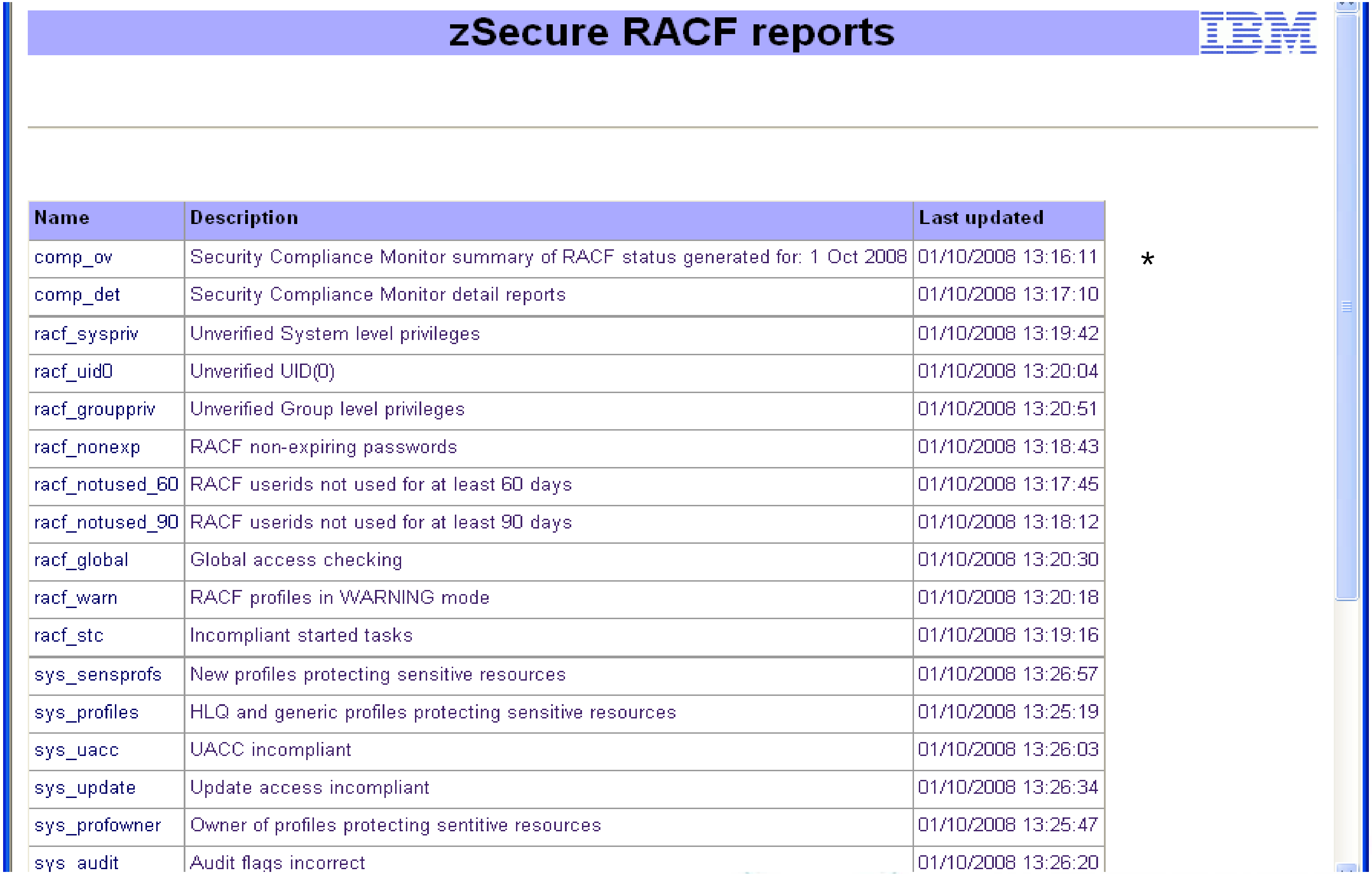
Solución zSecure

- Informes personalizados de zSecure Audit
  - Referencias base documentan los estandares de implantación de la seguridad
    - Muestran parámetros en conflicto
    - Los cambios aprobados deben estar reflejados en la referencia base
    - Los cambios inapropiados saldrán reflejados hasta que se solucionen

IBMAGINA

Un planeta más inteligente necesita software más inteligente

Informes RACF en Web

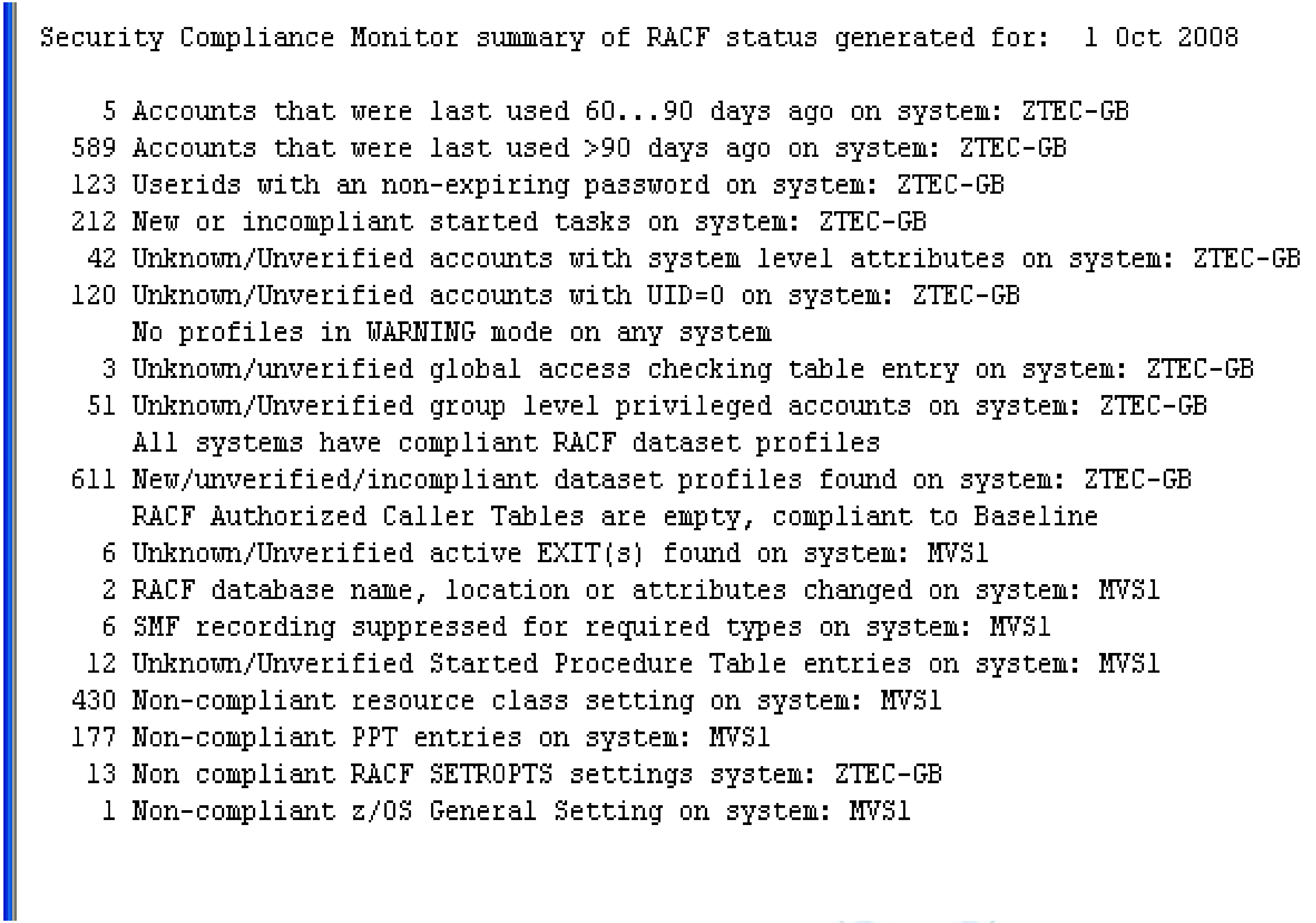


zSecure RACF reports

Name	Description	Last updated
comp_ov	Security Compliance Monitor summary of RACF status generated for: 1 Oct 2008	01/10/2008 13:16:11
comp_det	Security Compliance Monitor detail reports	01/10/2008 13:17:10
racf_syspriv	Unverified System level privileges	01/10/2008 13:19:42
racf_uid0	Unverified UID(0)	01/10/2008 13:20:04
racf_grouppriv	Unverified Group level privileges	01/10/2008 13:20:51
racf_nonexp	RACF non-expiring passwords	01/10/2008 13:18:43
racf_notused_60	RACF userids not used for at least 60 days	01/10/2008 13:17:45
racf_notused_90	RACF userids not used for at least 90 days	01/10/2008 13:18:12
racf_global	Global access checking	01/10/2008 13:20:30
racf_warn	RACF profiles in WARNING mode	01/10/2008 13:20:18
racf_stc	Incompliant started tasks	01/10/2008 13:19:16
sys_sensprofs	New profiles protecting sensitive resources	01/10/2008 13:26:57
sys_profiles	HLQ and generic profiles protecting sensitive resources	01/10/2008 13:25:19
sys_uacc	UACC incompliant	01/10/2008 13:26:03
sys_update	Update access incompliant	01/10/2008 13:26:34
sys_profowner	Owner of profiles protecting sentitive resources	01/10/2008 13:25:47
sys_audit	Audit flags incorrect	01/10/2008 13:26:20

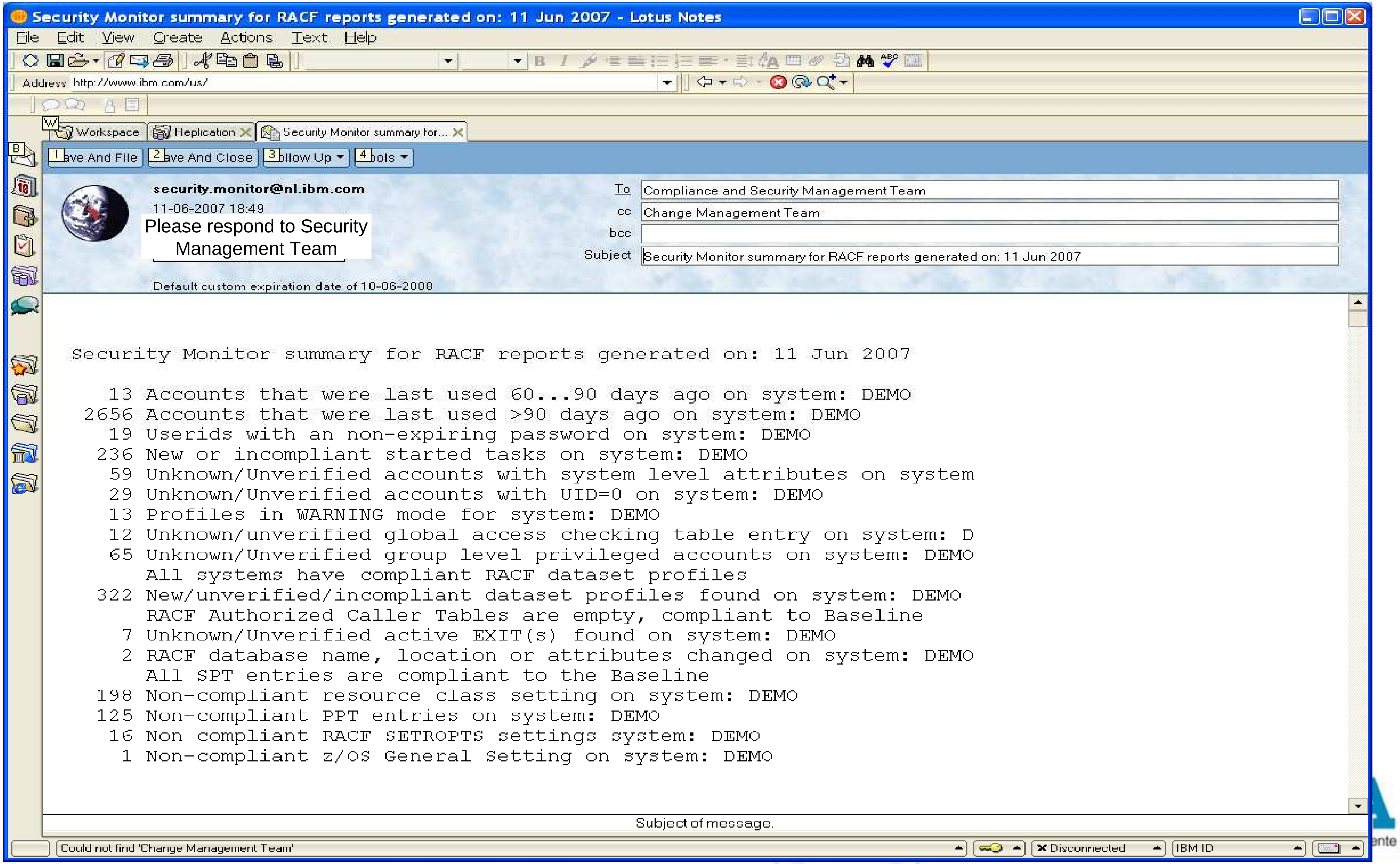
*

Sumario de cumplimientos



```
Security Compliance Monitor summary of RACF status generated for:  1 Oct 2008

    5 Accounts that were last used 60...90 days ago on system: ZTEC-GB
  589 Accounts that were last used >90 days ago on system: ZTEC-GB
  123 Userids with an non-expiring password on system: ZTEC-GB
  212 New or incompliant started tasks on system: ZTEC-GB
   42 Unknown/Unverified accounts with system level attributes on system: ZTEC-GB
  120 Unknown/Unverified accounts with UID=0 on system: ZTEC-GB
      No profiles in WARNING mode on any system
    3 Unknown/unverified global access checking table entry on system: ZTEC-GB
   51 Unknown/Unverified group level privileged accounts on system: ZTEC-GB
      All systems have compliant RACF dataset profiles
  611 New/unverified/incompliant dataset profiles found on system: ZTEC-GB
      RACF Authorized Caller Tables are empty, compliant to Baseline
    6 Unknown/Unverified active EXIT(s) found on system: MVS1
    2 RACF database name, location or attributes changed on system: MVS1
    6 SMF recording suppressed for required types on system: MVS1
   12 Unknown/Unverified Started Procedure Table entries on system: MVS1
  430 Non-compliant resource class setting on system: MVS1
  177 Non-compliant PPT entries on system: MVS1
   13 Non compliant RACF SETROPTS settings system: ZTEC-GB
    1 Non-compliant z/OS General Setting on system: MVS1
```

Envío electrónico de informes



Security Monitor summary for RACF reports generated on: 11 Jun 2007 - Lotus Notes
File Edit View Create Actions Text Help
Address http://www.ibm.com/us/
Workspace
Replication
Security Monitor summary for...
Save And File
Save And Close
Follow Up
Tools

security.monitor@nl.ibm.com
11-06-2007 18:49

Please respond to Security Management Team

Default custom expiration date of 10-06-2008

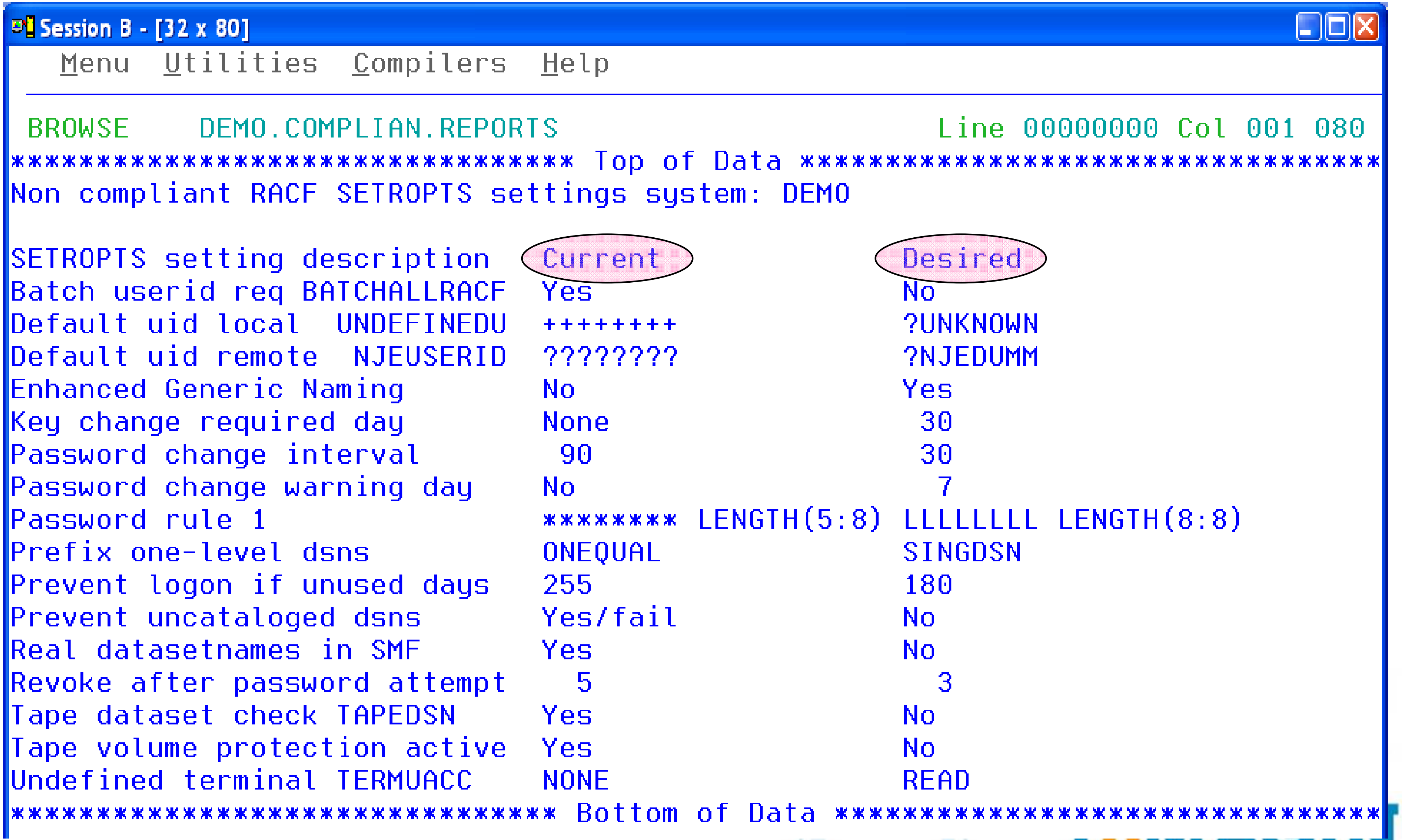
To: Compliance and Security Management Team
cc: Change Management Team
bcc:
Subject: Security Monitor summary for RACF reports generated on: 11 Jun 2007

```
Security Monitor summary for RACF reports generated on: 11 Jun 2007

   13 Accounts that were last used 60...90 days ago on system: DEMO
 2656 Accounts that were last used >90 days ago on system: DEMO
   19 Userids with an non-expiring password on system: DEMO
  236 New or incompliant started tasks on system: DEMO
   59 Unknown/Unverified accounts with system level attributes on system
   29 Unknown/Unverified accounts with UID=0 on system: DEMO
   13 Profiles in WARNING mode for system: DEMO
   12 Unknown/unverified global access checking table entry on system: D
   65 Unknown/Unverified group level privileged accounts on system: DEMO
      All systems have compliant RACF dataset profiles
  322 New/unverified/incompliant dataset profiles found on system: DEMO
      RACF Authorized Caller Tables are empty, compliant to Baseline
    7 Unknown/Unverified active EXIT(s) found on system: DEMO
    2 RACF database name, location or attributes changed on system: DEMO
      All SPT entries are compliant to the Baseline
  198 Non-compliant resource class setting on system: DEMO
  125 Non-compliant PPT entries on system: DEMO
   16 Non compliant RACF SETROPTS settings system: DEMO
    1 Non-compliant z/OS General Setting on system: DEMO
```

Subject of message.

Could not find 'Change Management Team'

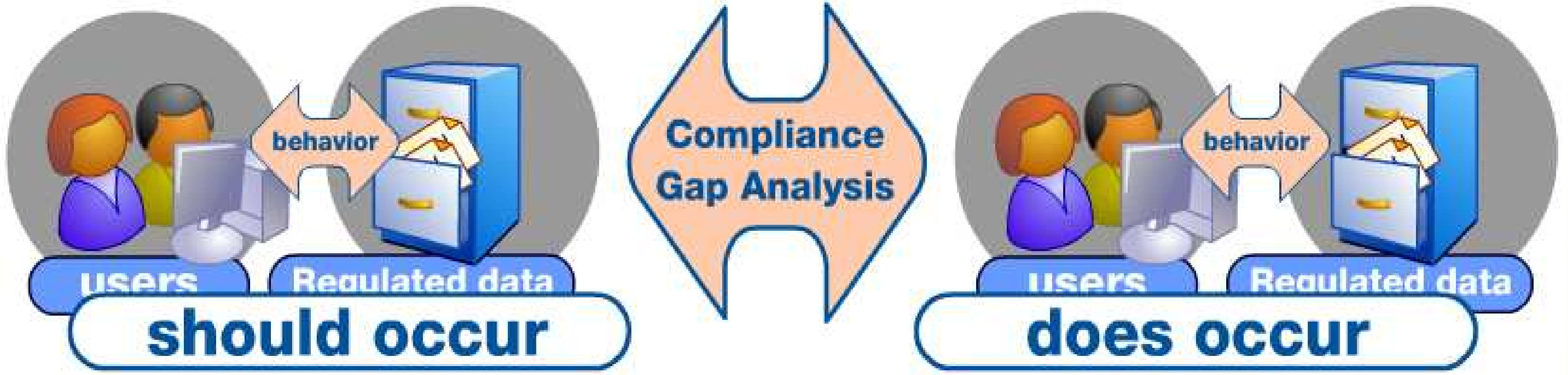
Verificación contra referencia base



```
 BROWSE    DEMO.COMPLIAN.REPORTS                      Line 00000000 Col 001 080
********************************* Top of Data **********************************
Non compliant RACF SETROPTS settings system: DEMO

SETROPTS setting description   Current              Desired
Batch userid req BATCHALLRACF  Yes                  No
Default uid local  UNDEFINEDU  ++++++++             ?UNKNOWN
Default uid remote  NJEUSERID  ????????             ?NJEDUMM
Enhanced Generic Naming        No                   Yes
Key change required day        None                  30
Password change interval        90                   30
Password change warning day    No                     7
Password rule 1                ******** LENGTH(5:8) LLLLLLLL LENGTH(8:8)
Prefix one-level dsns          ONEQUAL              SINGDSN
Prevent logon if unused days   255                  180
Prevent uncataloged dsns       Yes/fail             No
Real datasetnames in SMF       Yes                  No
Revoke after password attempt    5                    3
Tape dataset check TAPEDSN     Yes                  No
Tape volume protection active  Yes                  No
Undefined terminal TERMUACC    NONE                 READ
******************************** Bottom of Data ********************************
```

Solución

- Solución: Informes automatizados para >25 LPARs
  - Excepciones sumarizadas en correo electrónico
  - Informes de detalle disponibles para revisión o archivado
  - Verificación diaria



IBMAGINA
Un planeta más inteligente necesita software más inteligente

Caso de estudio: Informes varios (Basilea, SOX, PCI, etc..)

- Los Auditores
  - Piden una larga lista de informes
    - Esperan una rápida respuesta
  - Normalmente lleva dias generar un informe
  - Se usan los perfiles RACF o registros SMF records

- Soluciones Disponibles?:
  - Usar IRRDBU00
    - Descarga de la BD de RACF
  - Exportar a DB2
  - Ejecutar un SQL
  - Importar en Excel

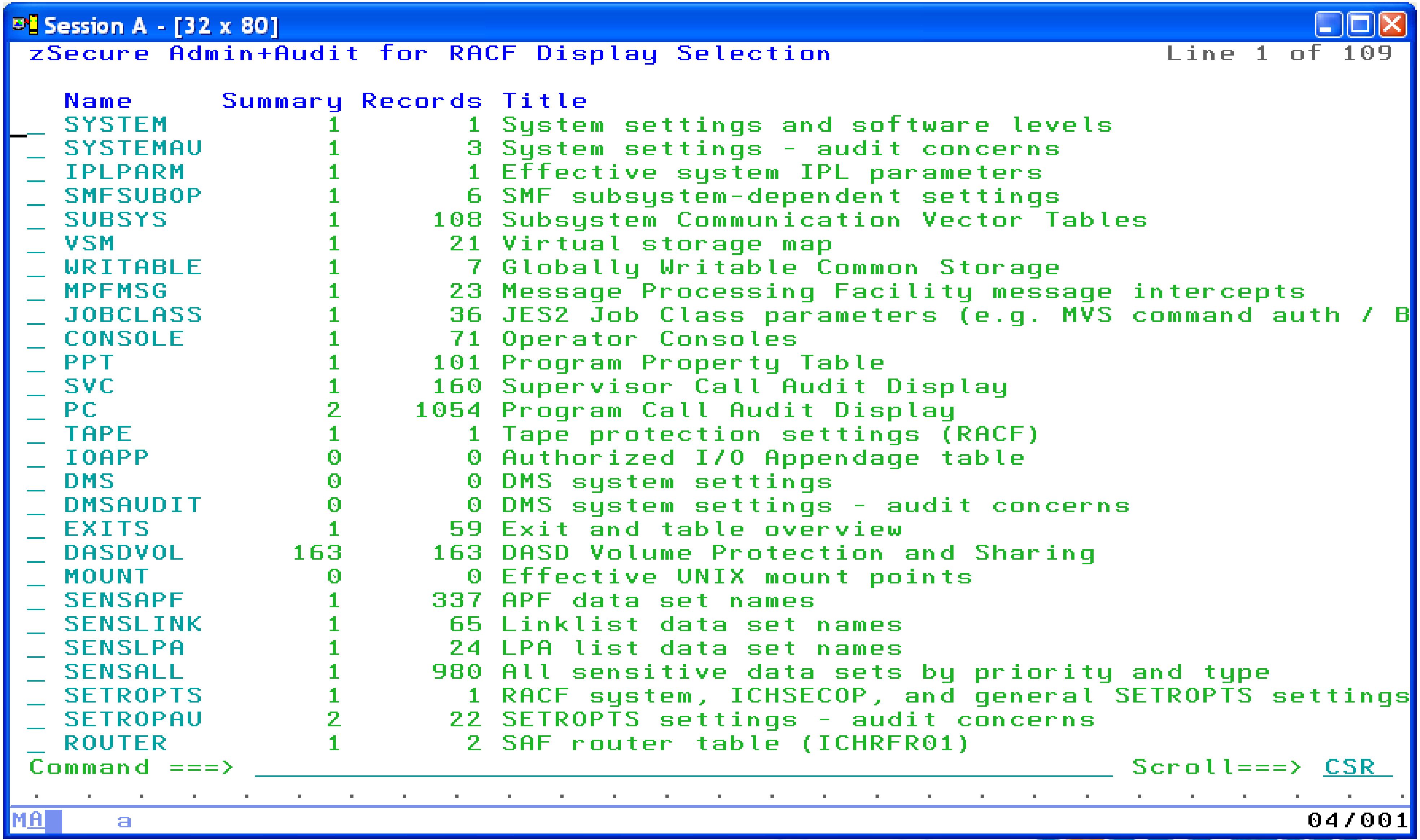
zSecure Solution

- Informes estándar de zSecure Audit
  - Muchos disponibles de inmediato
  - Otros se pueden componer con ayuda de paneles
  - También se pueden construir por medio de CARLa
- Citas de clientes:
  - Antes de zSecure, nos llevaba 3 días construir un informe.
  - Ahora con zSecure Audit, lo tenemos en 30 minutos.
  - Podemos contestar preguntas en el mismo día y los auditores quedan satisfechos

IBMAGINA

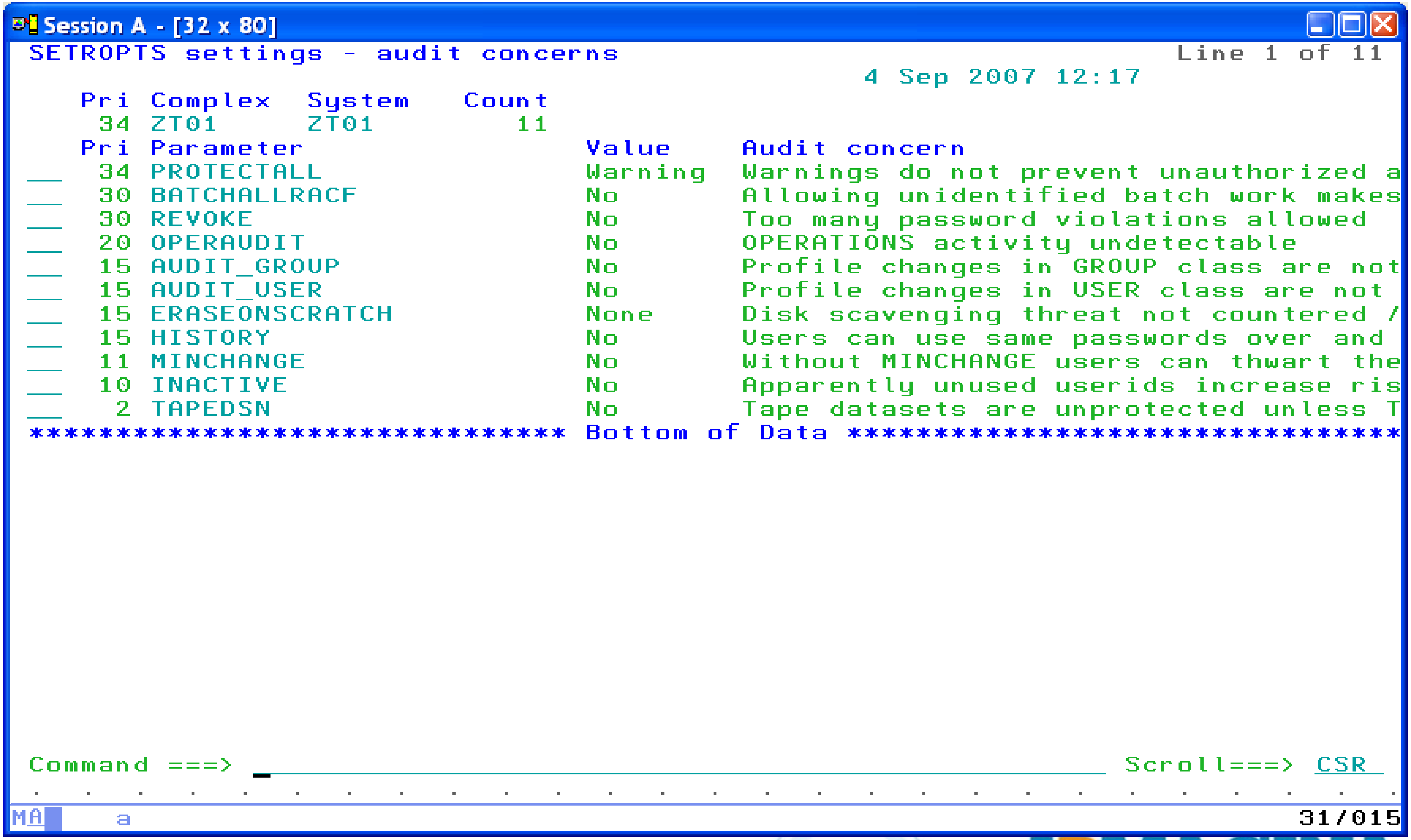
Un planeta más inteligente necesita software más inteligente

Informes detallados de estado de z/OS



```
 zSecure Admin+Audit for RACF Display Selection                    Line 1 of 109

   Name     Summary Records Title
 _ SYSTEM         1       1 System settings and software levels
 _ SYSTEMAU       1       3 System settings - audit concerns
 _ IPLPARM        1       1 Effective system IPL parameters
 _ SMFSUBOP       1       6 SMF subsystem-dependent settings
 _ SUBSYS         1     108 Subsystem Communication Vector Tables
 _ VSM            1      21 Virtual storage map
 _ WRITABLE       1       7 Globally Writable Common Storage
 _ MPFMSG         1      23 Message Processing Facility message intercepts
 _ JOBCLASS       1      36 JES2 Job Class parameters (e.g. MVS command auth / B
 _ CONSOLE        1      71 Operator Consoles
 _ PPT            1     101 Program Property Table
 _ SVC            1     160 Supervisor Call Audit Display
 _ PC             2    1054 Program Call Audit Display
 _ TAPE           1       1 Tape protection settings (RACF)
 _ IOAPP          0       0 Authorized I/O Appendage table
 _ DMS            0       0 DMS system settings
 _ DMSAUDIT       0       0 DMS system settings - audit concerns
 _ EXITS          1      59 Exit and table overview
 _ DASDVOL      163     163 DASD Volume Protection and Sharing
 _ MOUNT          0       0 Effective UNIX mount points
 _ SENSAPF        1     337 APF data set names
 _ SENSLINK       1      65 Linklist data set names
 _ SENSLPA        1      24 LPA list data set names
 _ SENSALL        1     980 All sensitive data sets by priority and type
 _ SETROPTS       1       1 RACF system, ICHSECOP, and general SETROPTS settings
 _ SETROPAU       2      22 SETROPTS settings - audit concerns
 _ ROUTER         1       2 SAF router table (ICHRFR01)
 Command ===> ________________________________________________ Scroll===> CSR_

 MA      a                                                              04/001
```

Evaluación de vulnerabilidades automática

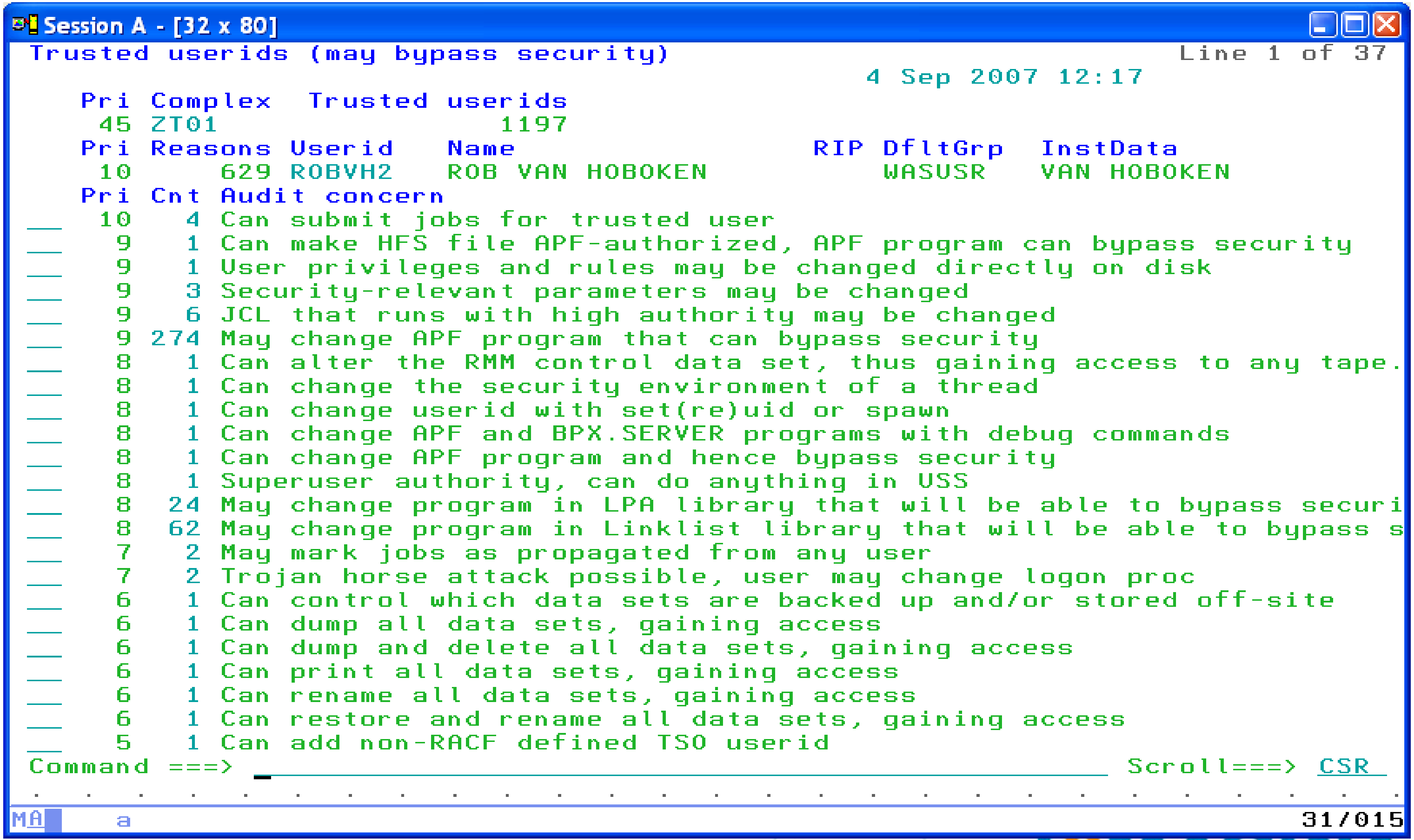


```
SETROPTS settings - audit concerns                                 Line 1 of 11
                                                     4 Sep 2007 12:17

   Pri Complex  System   Count
    34 ZT01     ZT01        11
   Pri Parameter                 Value     Audit concern
___ 34 PROTECTALL                Warning   Warnings do not prevent unauthorized a
___ 30 BATCHALLRACF              No        Allowing unidentified batch work makes
___ 30 REVOKE                    No        Too many password violations allowed
___ 20 OPERAUDIT                 No        OPERATIONS activity undetectable
___ 15 AUDIT_GROUP               No        Profile changes in GROUP class are not
___ 15 AUDIT_USER                No        Profile changes in USER class are not
___ 15 ERASEONSCRATCH            None      Disk scavenging threat not countered /
___ 15 HISTORY                   No        Users can use same passwords over and
___ 11 MINCHANGE                 No        Without MINCHANGE users can thwart the
___ 10 INACTIVE                  No        Apparently unused userids increase ris
___  2 TAPEDSN                   No        Tape datasets are unprotected unless T
******************************* Bottom of Data ********************************

Command ===> _________________________________________________ Scroll===> CSR_

MA      a                                                                31/015
```

IBMAGINA

Un planeta más inteligente necesita software más inteligente

Informe de usuarios privilegiados



```
 Trusted userids (may bypass security)                             Line 1 of 37
                                                 4 Sep 2007 12:17
    Pri Complex  Trusted userids
     45 ZT01                1197
    Pri Reasons Userid   Name                 RIP DfltGrp  InstData
     10     629 ROBVH2   ROB VAN HOBOKEN          WASUSR   VAN HOBOKEN
    Pri Cnt Audit concern
 ___ 10   4 Can submit jobs for trusted user
 ___  9   1 Can make HFS file APF-authorized, APF program can bypass security
 ___  9   1 User privileges and rules may be changed directly on disk
 ___  9   3 Security-relevant parameters may be changed
 ___  9   6 JCL that runs with high authority may be changed
 ___  9 274 May change APF program that can bypass security
 ___  8   1 Can alter the RMM control data set, thus gaining access to any tape.
 ___  8   1 Can change the security environment of a thread
 ___  8   1 Can change userid with set(re)uid or spawn
 ___  8   1 Can change APF and BPX.SERVER programs with debug commands
 ___  8   1 Can change APF program and hence bypass security
 ___  8   1 Superuser authority, can do anything in USS
 ___  8  24 May change program in LPA library that will be able to bypass securi
 ___  8  62 May change program in Linklist library that will be able to bypass s
 ___  7   2 May mark jobs as propagated from any user
 ___  7   2 Trojan horse attack possible, user may change logon proc
 ___  6   1 Can control which data sets are backed up and/or stored off-site
 ___  6   1 Can dump all data sets, gaining access
 ___  6   1 Can dump and delete all data sets, gaining access
 ___  6   1 Can print all data sets, gaining access
 ___  6   1 Can rename all data sets, gaining access
 ___  6   1 Can restore and rename all data sets, gaining access
 ___  5   1 Can add non-RACF defined TSO userid
 Command ===> _________________________________________________ Scroll===> CSR
MA     a                                                                 31/015
```

Un planeta más inteligente necesita software más inteligente

Si los controles de acceso no son suficientes

- Situación:
  - Muchos técnicos con acceso a datos de negocio
  - Los datos financieros se deben mantener confidenciales para prevenir mal uso interno
  - Posibilitar que los técnicos realicen su trabajo

- Solución disponible?:
  - Acceso restrigido a datos finacieros
    - Los administradores de almacenamiento y sistemas pueden leer los datos de negocio
    - Los administradores de seguridad se dan la autoridad a si mismos
    - Los administradores de datos pueden concederse accesos impropios
  - Reducción de acceso a ususarios privilegiados
    - Puede causar limitaciones técnicas
    - Si pierdo mi acceso … no puedo hacer …..

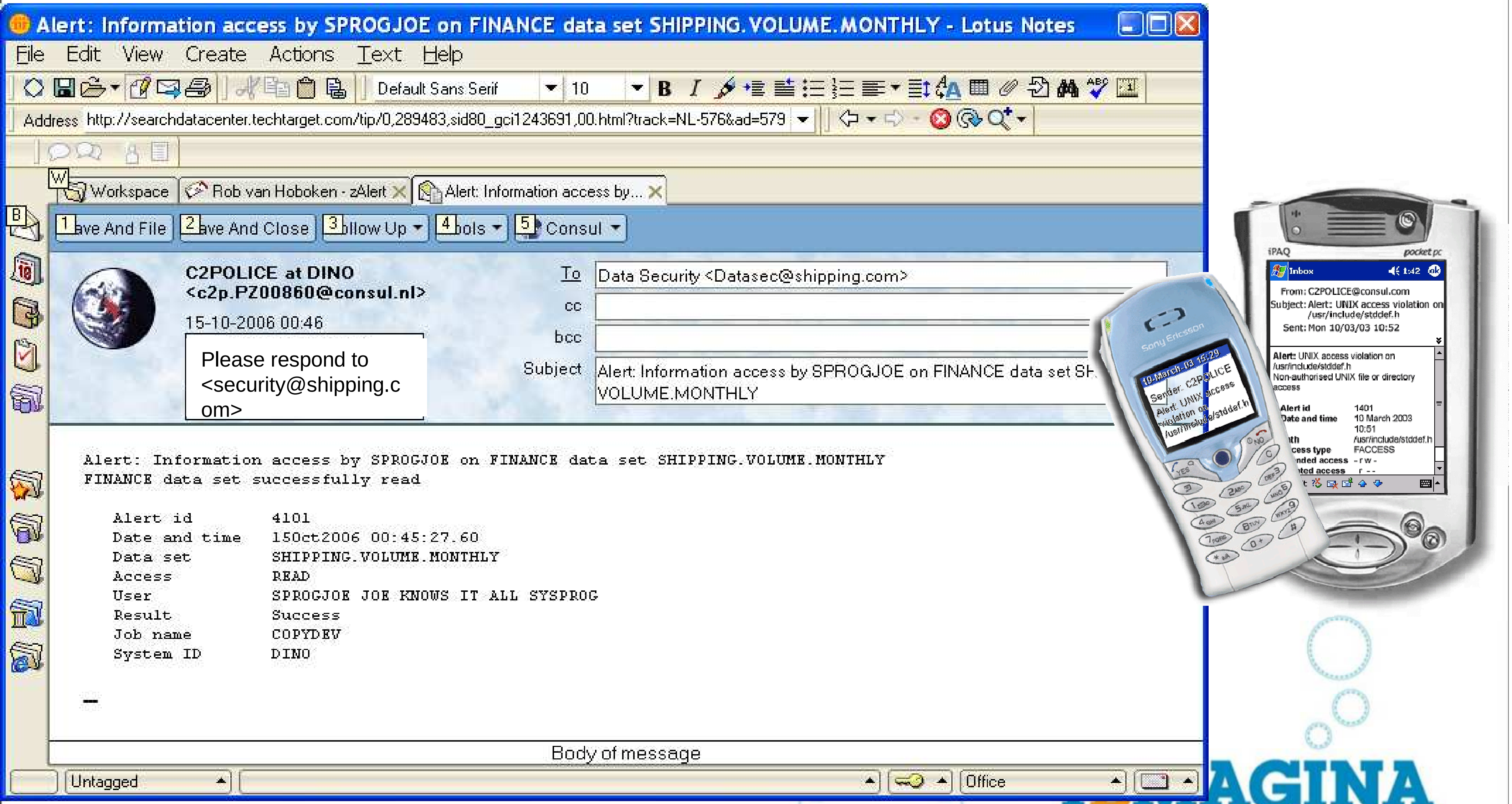
- Alertas en tiempo real como controles compensatorios
  - zSecure Alert
    - Reduce la necesidad de separar accesos
    - Los “sysprogs” mantienen su autoridad
    - Sin batallas políticas o reorganizaciones costosas
    - Rápida instalación y visibilidad

zSecure Solution

IBMAGINA

Un planeta más inteligente necesita software más inteligente

zSecure Alert lanza alertas sobre accesos peligrosos


Alert: Information access by SPROGJOE on FINANCE data set SHIPPING.VOLUME.MONTHLY - Lotus Notes
File Edit View Create Actions Text Help
Default Sans Serif
10
Address http://searchdatacenter.techtarget.com/tip/0,289483,sid80_gci1243691,00.html?track=NL-576&ad=579
Workspace
Rob van Hoboken - zAlert
Alert: Information access by...
Save And File
Save And Close
Follow Up
Tools
Consul
Untagged
Office
Body of message
iPAQ
pocket pc
Inbox
1:42
ok
Sony Ericsson

C2POLICE at DINO
<c2p.PZ00860@consul.nl>

15-10-2006 00:46

Please respond to <security@shipping.com>

To: Data Security <Datasec@shipping.com>

cc:

bcc:

Subject: Alert: Information access by SPROGJOE on FINANCE data set SHIPPING.VOLUME.MONTHLY

```
Alert: Information access by SPROGJOE on FINANCE data set SHIPPING.VOLUME.MONTHLY
FINANCE data set successfully read

   Alert id          4101
   Date and time     15Oct2006 00:45:27.60
   Data set          SHIPPING.VOLUME.MONTHLY
   Access            READ
   User              SPROGJOE JOE KNOWS IT ALL SYSPROG
   Result            Success
   Job name          COPYDEV
   System ID         DINO

–
```

10-March-03 15:29
Sender: C2POLICE
Alert: UNIX access violation on /usr/include/stddef.h

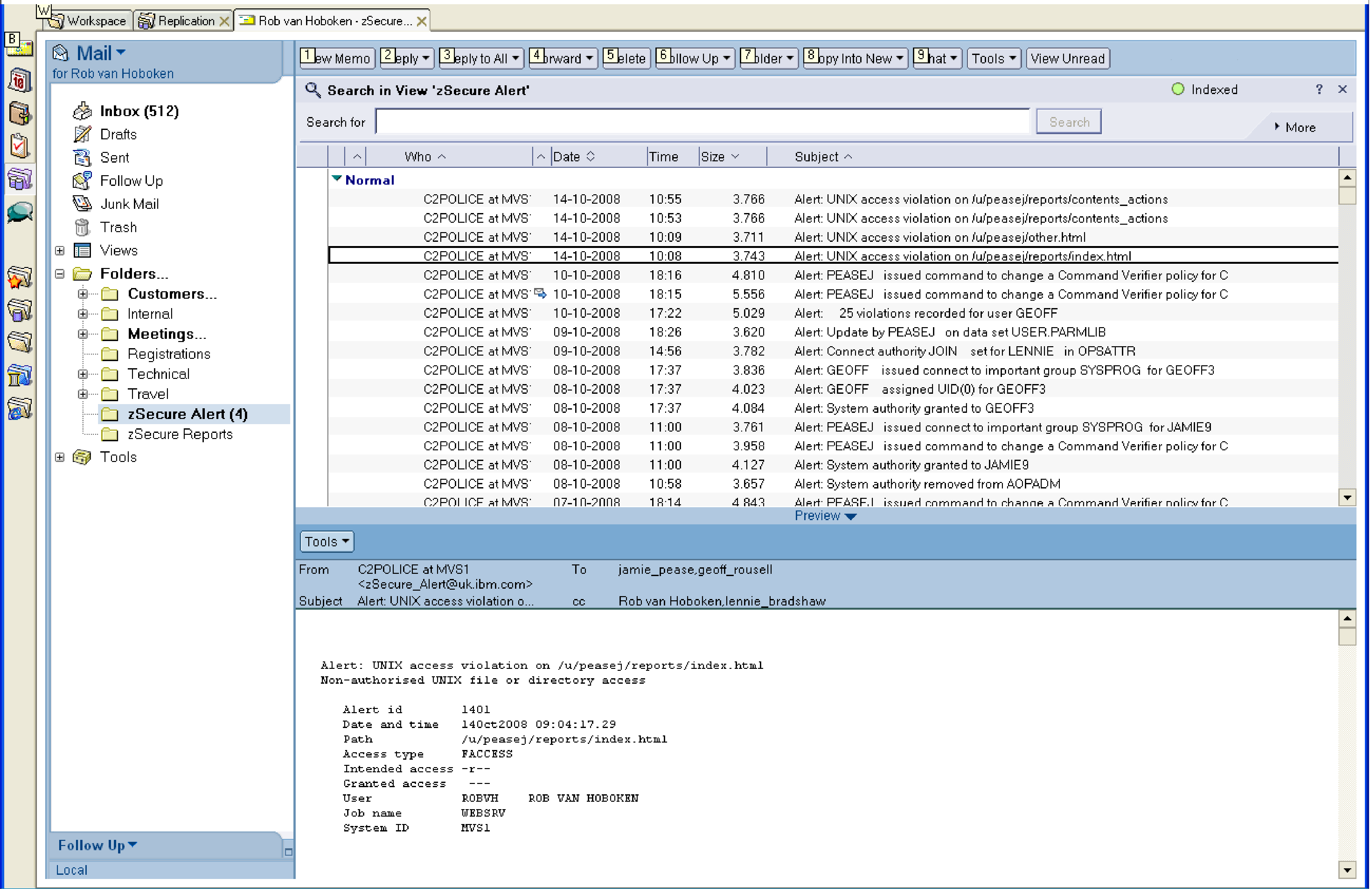
From: C2POLICE@consul.com
Subject: Alert: UNIX access violation on /usr/include/stddef.h
Sent: Mon 10/03/03 10:52

Alert: UNIX access violation on /usr/include/stddef.h
Non-authorised UNIX file or directory access

```
Alert id            1401
Date and time       10 March 2003
                    10:51
th                  /usr/include/stddef.h
ccess type          FACCESS
nded access         - r w -
nted access         r - -
```

Un planeta más inteligente necesita software más inteligente

Ejemplo de alertas



Who	Date	Time	Size	Subject
C2POLICE at MVS'	14-10-2008	10:55	3.766	Alert: UNIX access violation on /u/peasej/reports/contents_actions
C2POLICE at MVS'	14-10-2008	10:53	3.766	Alert: UNIX access violation on /u/peasej/reports/contents_actions
C2POLICE at MVS'	14-10-2008	10:09	3.711	Alert: UNIX access violation on /u/peasej/other.html
C2POLICE at MVS'	14-10-2008	10:08	3.743	Alert: UNIX access violation on /u/peasej/reports/index.html
C2POLICE at MVS'	10-10-2008	18:16	4.810	Alert: PEASEJ issued command to change a Command Verifier policy for C
C2POLICE at MVS'	10-10-2008	18:15	5.556	Alert: PEASEJ issued command to change a Command Verifier policy for C
C2POLICE at MVS'	10-10-2008	17:22	5.029	Alert: 25 violations recorded for user GEOFF
C2POLICE at MVS'	09-10-2008	18:26	3.620	Alert: Update by PEASEJ on data set USER.PARMLIB
C2POLICE at MVS'	09-10-2008	14:56	3.782	Alert: Connect authority JOIN set for LENNIE in OPSATTR
C2POLICE at MVS'	08-10-2008	17:37	3.836	Alert: GEOFF issued connect to important group SYSPROG for GEOFF3
C2POLICE at MVS'	08-10-2008	17:37	4.023	Alert: GEOFF assigned UID(0) for GEOFF3
C2POLICE at MVS'	08-10-2008	17:37	4.084	Alert: System authority granted to GEOFF3
C2POLICE at MVS'	08-10-2008	11:00	3.761	Alert: PEASEJ issued connect to important group SYSPROG for JAMIE9
C2POLICE at MVS'	08-10-2008	11:00	3.958	Alert: PEASEJ issued command to change a Command Verifier policy for C
C2POLICE at MVS'	08-10-2008	11:00	4.127	Alert: System authority granted to JAMIE9
C2POLICE at MVS'	08-10-2008	10:58	3.657	Alert: System authority removed from AOPADM
C2POLICE at MVS'	07-10-2008	18:14	4.843	Alert: PEASEJ issued command to change a Command Verifier policy for C

From	C2POLICE at MVS1 <zSecure_Alert@uk.ibm.com>	To	jamie_pease,geoff_rousell
Subject	Alert: UNIX access violation o...	cc	Rob van Hoboken,lennie_bradshaw

```
Alert: UNIX access violation on /u/peasej/reports/index.html
Non-authorised UNIX file or directory access

   Alert id          1401
   Date and time     14Oct2008 09:04:17.29
   Path              /u/peasej/reports/index.html
   Access type       FACCESS
   Intended access   -r--
   Granted access     ---
   User              ROBVH     ROB VAN HOBOKEN
   Job name          WEBSRV
   System ID         MVS1
```

La administración de Seguridad no es sencilla

- Situación:
  - La administración de seguridad se realiza por usuarios técnicos
  - La de usuarios no siempre
  - Los aspectos técnicos los manejan equipos tecnicos
  - Todo esto requiere personas y esfuerzo

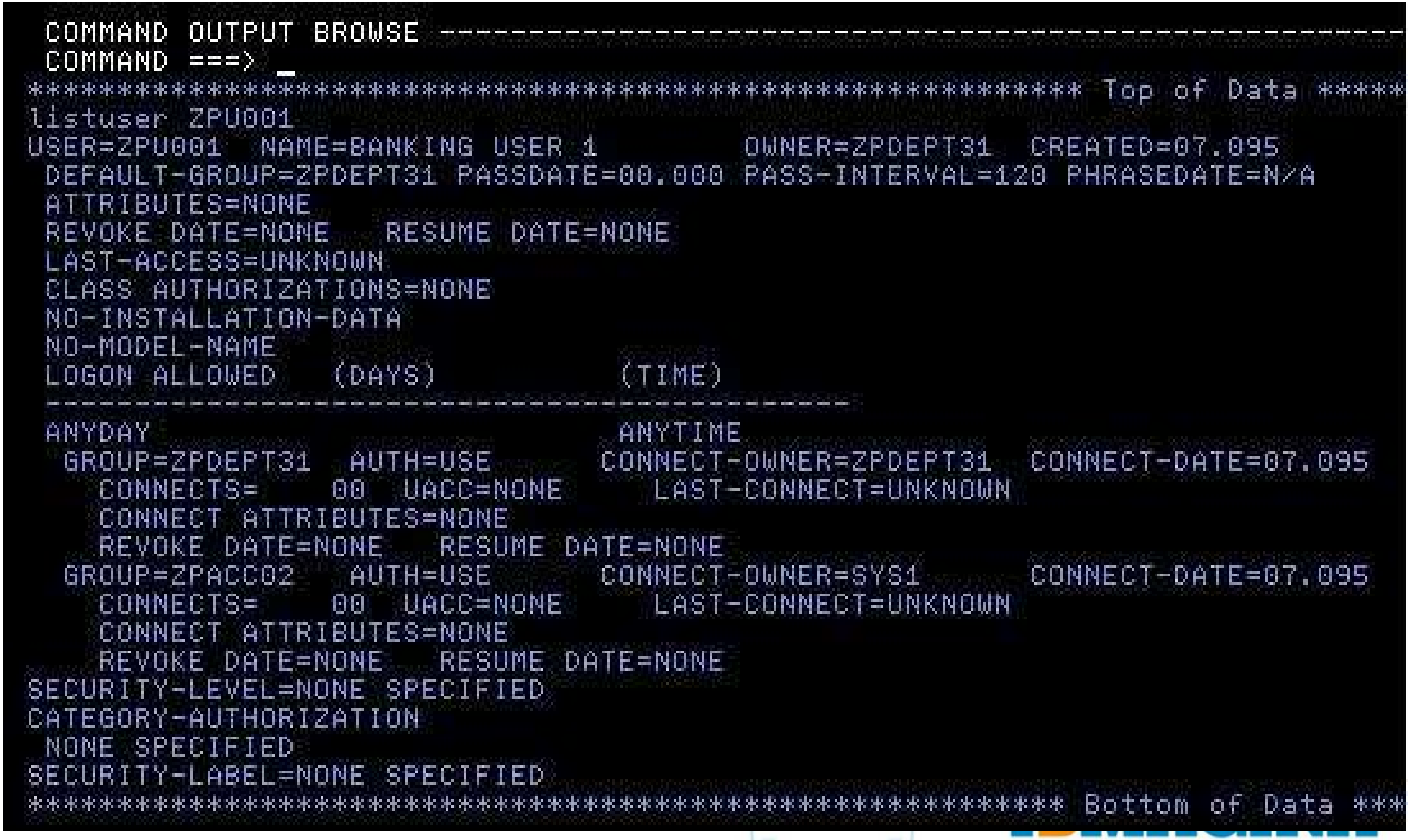
- Solution disponible?:
  - Uso de comandos RACF via ISPF
    - La salidad no suele ser amigable
  - Uso de la DB de RACF descargada en DB2
    - Información no actualizada

zSecure Solution

- Fácil administración de RACF – zSecure Admin
  - Visión de los profiles, contexto de seguridad
  - Modificación en contexto de campos
  - Informes con diferencias y seguridd efectiva
- Información actual de la DB activa de RACF
- Simulación de reorganizaciones de RACF por medio de la opción RACF Offline

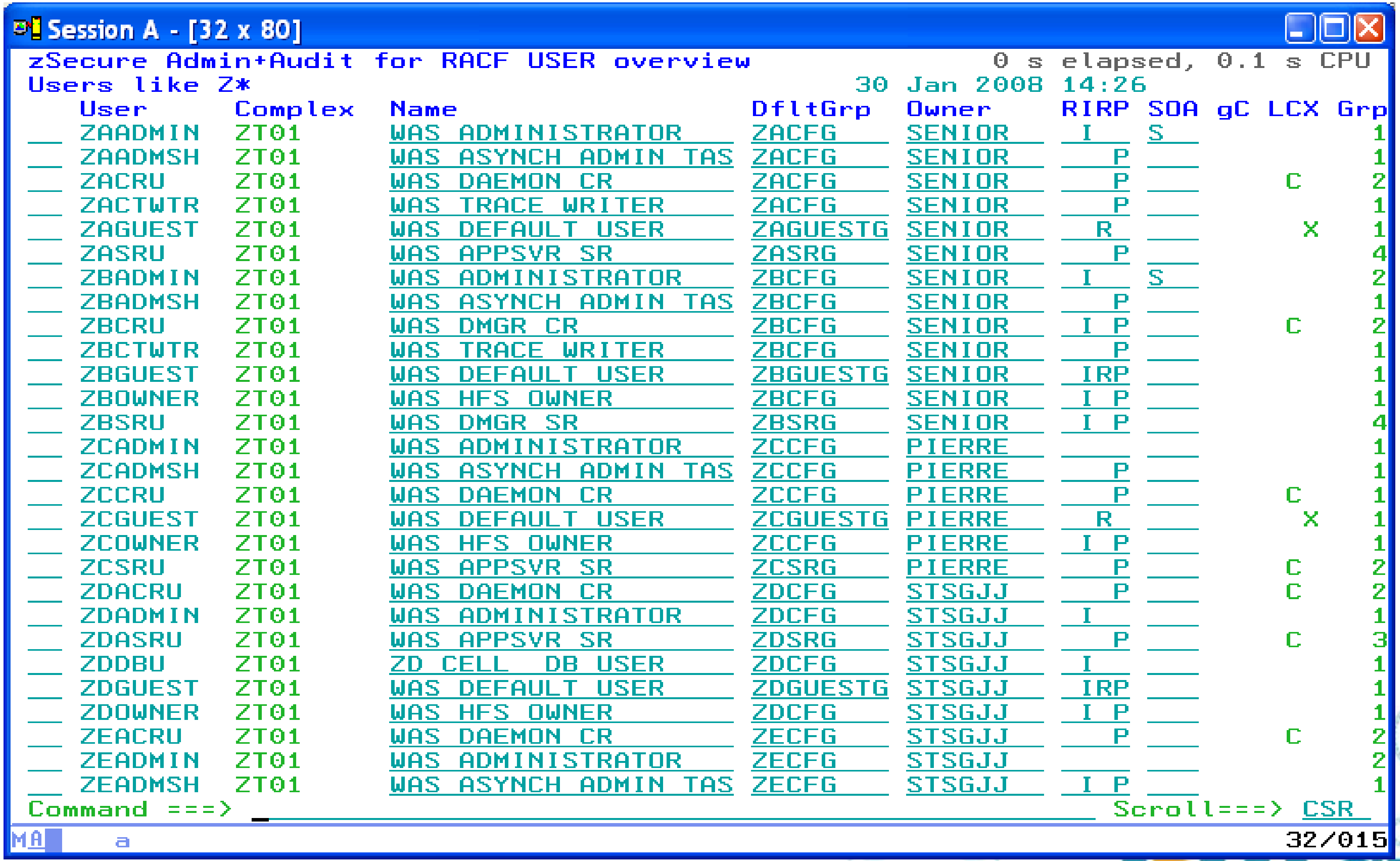
MAGINA
nteligente necesita software más inteligente

Salida del comando LISTUSER



```
 COMMAND OUTPUT BROWSE --------------------------------------------------
 COMMAND ===> _
*********************************************************** Top of Data *****
listuser ZPU001
USER=ZPU001  NAME=BANKING USER 1        OWNER=ZPDEPT31  CREATED=07.095
 DEFAULT-GROUP=ZPDEPT31 PASSDATE=00.000 PASS-INTERVAL=120 PHRASEDATE=N/A
 ATTRIBUTES=NONE
 REVOKE DATE=NONE   RESUME DATE=NONE
 LAST-ACCESS=UNKNOWN
 CLASS AUTHORIZATIONS=NONE
 NO-INSTALLATION-DATA
 NO-MODEL-NAME
 LOGON ALLOWED   (DAYS)          (TIME)
 ---------------------------------------------
 ANYDAY                          ANYTIME
  GROUP=ZPDEPT31  AUTH=USE      CONNECT-OWNER=ZPDEPT31  CONNECT-DATE=07.095
    CONNECTS=    00  UACC=NONE     LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
  GROUP=ZPACC02   AUTH=USE      CONNECT-OWNER=SYS1      CONNECT-DATE=07.095
    CONNECTS=    00  UACC=NONE     LAST-CONNECT=UNKNOWN
    CONNECT ATTRIBUTES=NONE
    REVOKE DATE=NONE   RESUME DATE=NONE
SECURITY-LEVEL=NONE SPECIFIED
CATEGORY-AUTHORIZATION
 NONE SPECIFIED
SECURITY-LABEL=NONE SPECIFIED
********************************************************** Bottom of Data ***
```

Visión de los perfiles de usuario



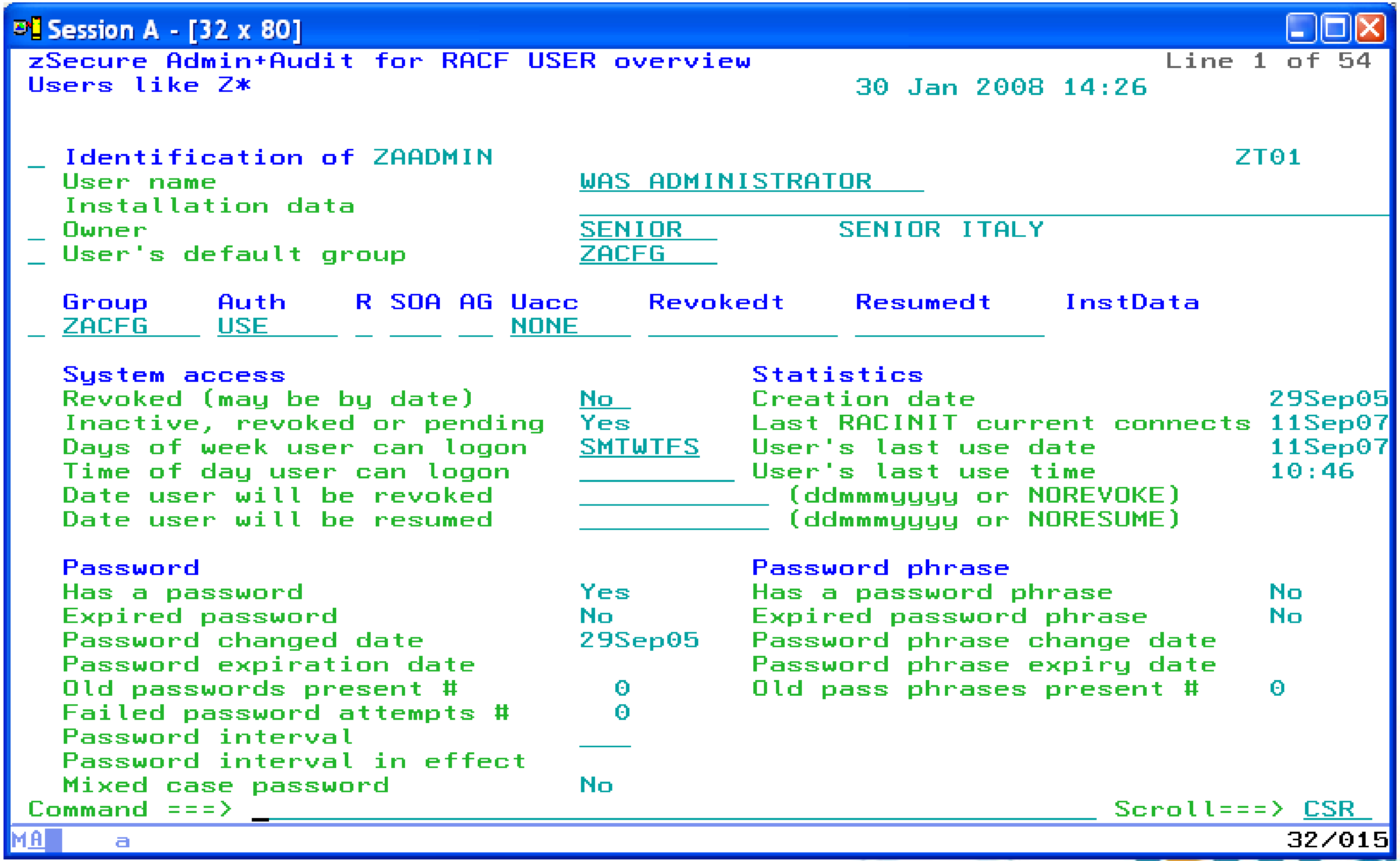
Session A - [32 x 80]

```
zSecure Admin+Audit for RACF USER overview             0 s elapsed, 0.1 s CPU
Users like Z*                                  30 Jan 2008 14:26
   User     Complex  Name                 DfltGrp  Owner    RIRP SOA gC LCX Grp
__ ZAADMIN  ZT01     WAS ADMINISTRATOR    ZACFG    SENIOR    I   S            1
__ ZAADMSH  ZT01     WAS ASYNCH ADMIN TAS ZACFG    SENIOR      P              1
__ ZACRU    ZT01     WAS DAEMON CR        ZACFG    SENIOR      P         C    2
__ ZACTWTR  ZT01     WAS TRACE WRITER     ZACFG    SENIOR      P              1
__ ZAGUEST  ZT01     WAS DEFAULT USER     ZAGUESTG SENIOR     R           X   1
__ ZASRU    ZT01     WAS APPSVR SR        ZASRG    SENIOR      P              4
__ ZBADMIN  ZT01     WAS ADMINISTRATOR    ZBCFG    SENIOR    I   S            2
__ ZBADMSH  ZT01     WAS ASYNCH ADMIN TAS ZBCFG    SENIOR      P              1
__ ZBCRU    ZT01     WAS DMGR CR          ZBCFG    SENIOR    I P         C    2
__ ZBCTWTR  ZT01     WAS TRACE WRITER     ZBCFG    SENIOR      P              1
__ ZBGUEST  ZT01     WAS DEFAULT USER     ZBGUESTG SENIOR    IRP              1
__ ZBOWNER  ZT01     WAS HFS OWNER        ZBCFG    SENIOR    I P              1
__ ZBSRU    ZT01     WAS DMGR SR          ZBSRG    SENIOR    I P              4
__ ZCADMIN  ZT01     WAS ADMINISTRATOR    ZCCFG    PIERRE                     1
__ ZCADMSH  ZT01     WAS ASYNCH ADMIN TAS ZCCFG    PIERRE      P              1
__ ZCCRU    ZT01     WAS DAEMON CR        ZCCFG    PIERRE      P         C    1
__ ZCGUEST  ZT01     WAS DEFAULT USER     ZCGUESTG PIERRE     R           X   1
__ ZCOWNER  ZT01     WAS HFS OWNER        ZCCFG    PIERRE    I P              1
__ ZCSRU    ZT01     WAS APPSVR SR        ZCSRG    PIERRE      P         C    2
__ ZDACRU   ZT01     WAS DAEMON CR        ZDCFG    STSGJJ      P         C    2
__ ZDADMIN  ZT01     WAS ADMINISTRATOR    ZDCFG    STSGJJ    I                1
__ ZDASRU   ZT01     WAS APPSVR SR        ZDSRG    STSGJJ      P         C    3
__ ZDDBU    ZT01     ZD CELL  DB USER     ZDCFG    STSGJJ    I                1
__ ZDGUEST  ZT01     WAS DEFAULT USER     ZDGUESTG STSGJJ    IRP              1
__ ZDOWNER  ZT01     WAS HFS OWNER        ZDCFG    STSGJJ    I P              1
__ ZEACRU   ZT01     WAS DAEMON CR        ZECFG    STSGJJ      P         C    2
__ ZEADMIN  ZT01     WAS ADMINISTRATOR    ZECFG    STSGJJ                     2
__ ZEADMSH  ZT01     WAS ASYNCH ADMIN TAS ZECFG    STSGJJ    I P              1
Command ===> _                                                 Scroll===> CSR
MA    a                                                                  32/015
```

IBMAGINA

Un planeta más inteligente necesita software más inteligente

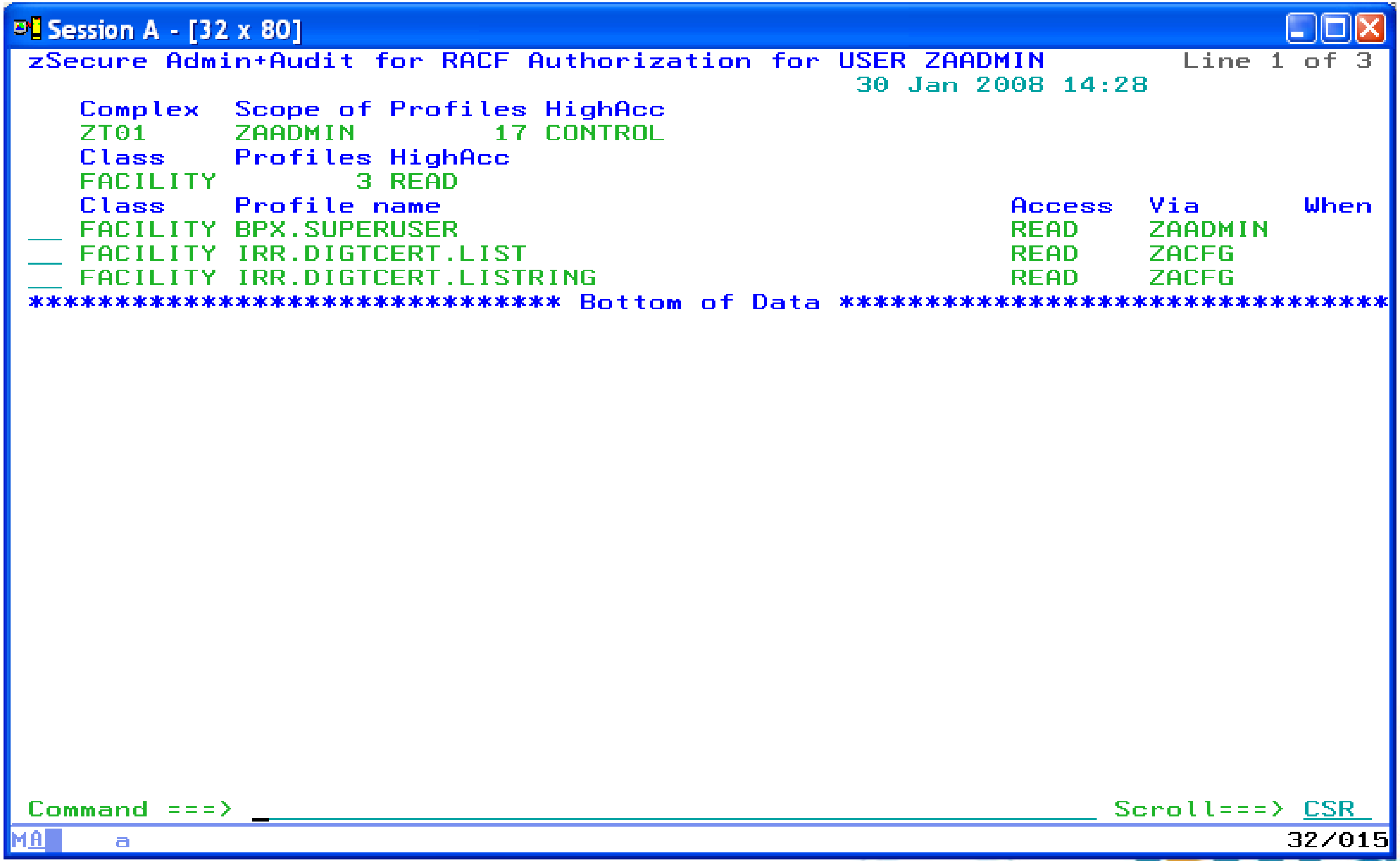
Detalles de un perfil de usario



```
zSecure Admin+Audit for RACF USER overview                        Line 1 of 54
Users like Z*                                   30 Jan 2008 14:26


_ Identification of ZAADMIN                                           ZT01
  User name                     WAS ADMINISTRATOR
  Installation data
_ Owner                         SENIOR         SENIOR ITALY
_ User's default group          ZACFG

  Group    Auth     R SOA AG Uacc    Revokedt    Resumedt    InstData
_ ZACFG    USE                NONE

  System access                           Statistics
  Revoked (may be by date)      No        Creation date                 29Sep05
  Inactive, revoked or pending  Yes       Last RACINIT current connects 11Sep07
  Days of week user can logon   SMTWTFS   User's last use date          11Sep07
  Time of day user can logon              User's last use time          10:46
  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              No        Expired password phrase       No
  Password changed date         29Sep05   Password phrase change date
  Password expiration date                Password phrase expiry date
  Old passwords present #         0       Old pass phrases present #    0
  Failed password attempts #      0
  Password interval
  Password interval in effect
  Mixed case password           No
Command ===> _                                                 Scroll===> CSR
MA    a                                                                 32/015
```

Un planeta más inteligente necesita software más inteligente

Accesos permitidos



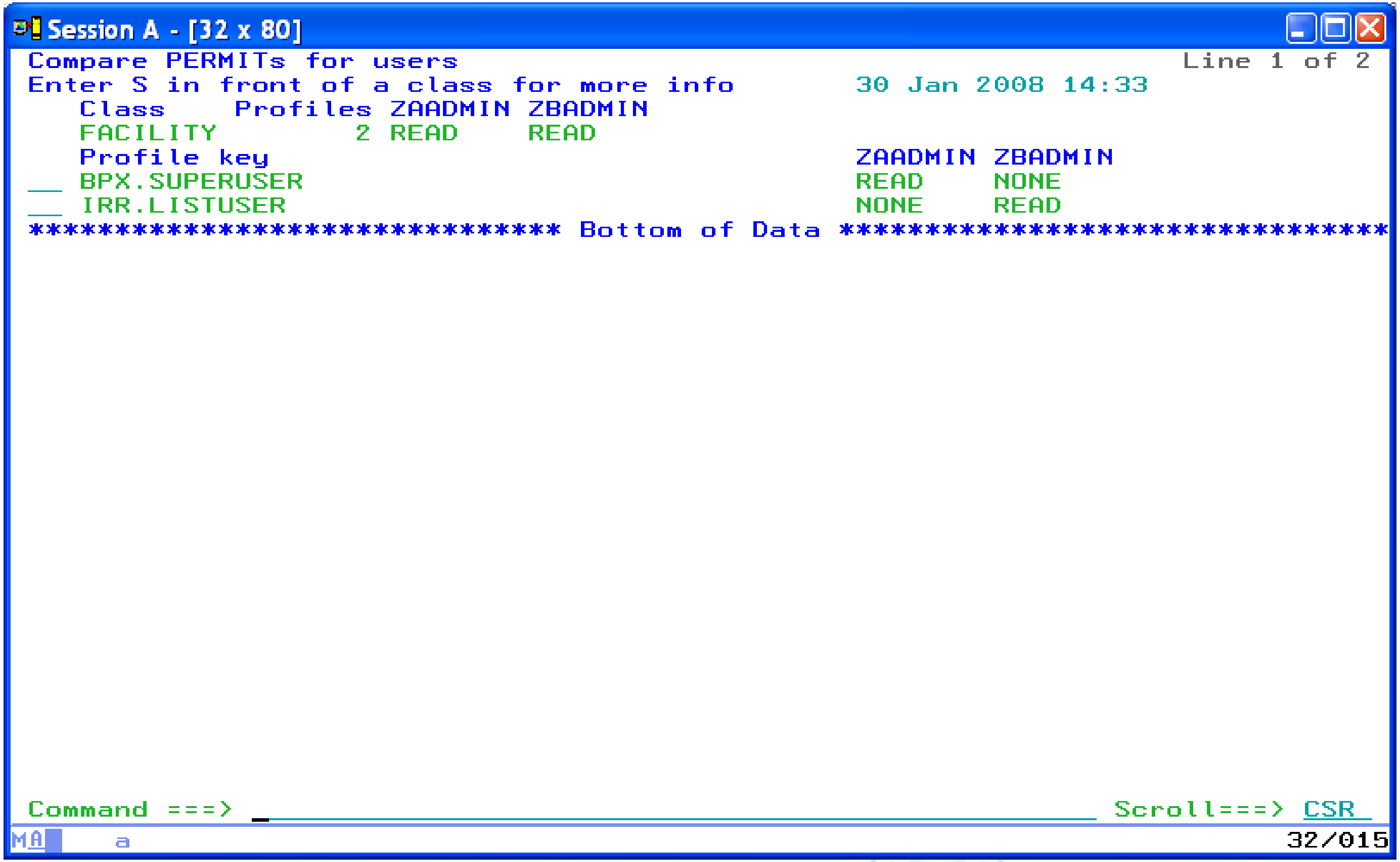
Session A - [32 x 80]

```
zSecure Admin+Audit for RACF Authorization for USER ZAADMIN       Line 1 of 3
                                                  30 Jan 2008 14:28

   Complex   Scope of Profiles HighAcc
   ZT01      ZAADMIN        17 CONTROL
   Class     Profiles HighAcc
   FACILITY         3 READ
   Class     Profile name                                  Access  Via      When
__ FACILITY BPX.SUPERUSER                                  READ    ZAADMIN
__ FACILITY IRR.DIGTCERT.LIST                              READ    ZACFG
__ FACILITY IRR.DIGTCERT.LISTRING                          READ    ZACFG
******************************* Bottom of Data ********************************









































Command ===> _                                                 Scroll===> CSR
MA      a                                                              32/015
```

IBMAGINA

Un planeta más inteligente necesita software más inteligente

Comparación de usuarios

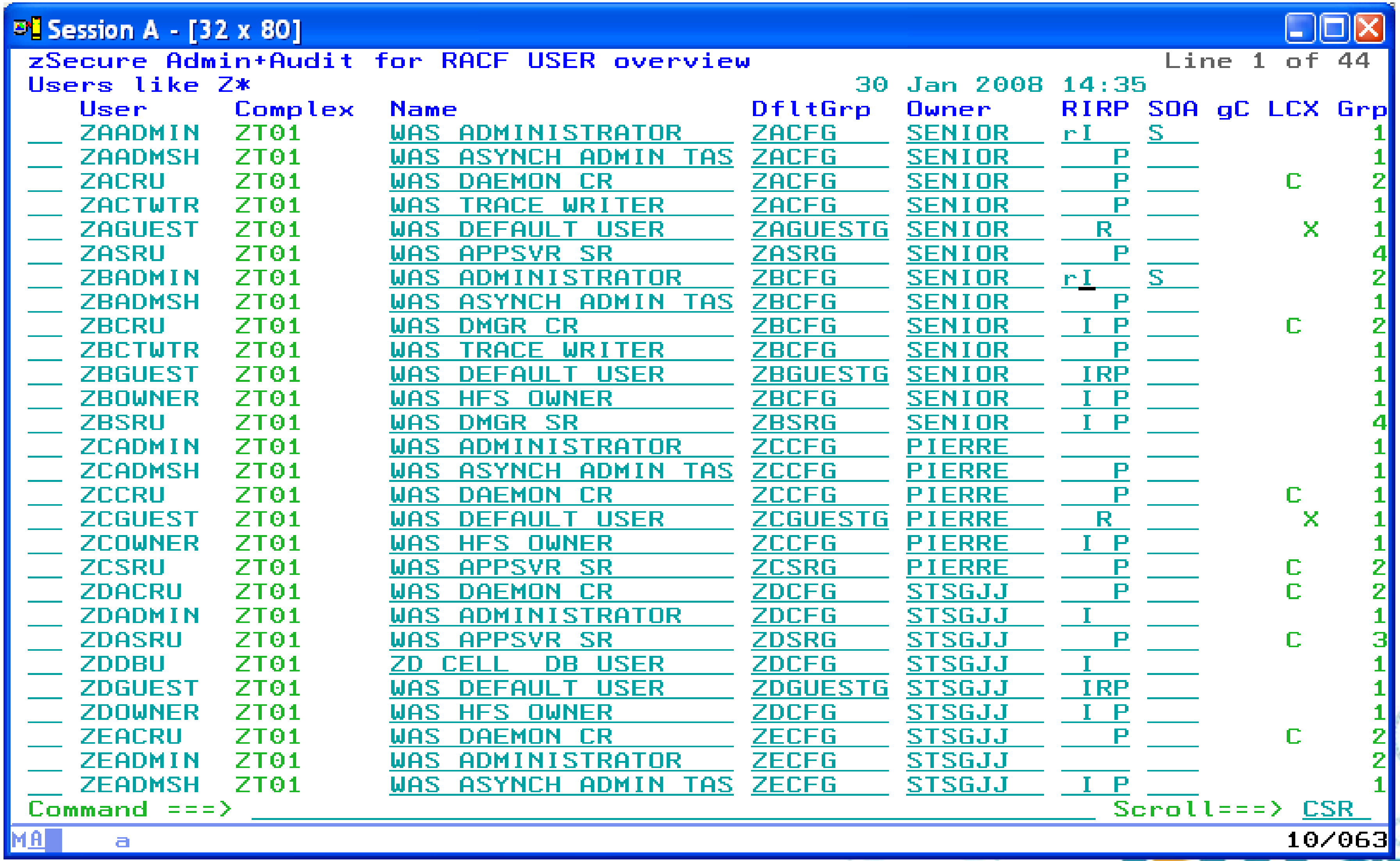


```
Compare PERMITs for users                                           Line 1 of 2
Enter S in front of a class for more info        30 Jan 2008 14:33
   Class     Profiles ZAADMIN ZBADMIN
   FACILITY         2 READ    READ
   Profile key                                   ZAADMIN ZBADMIN
__ BPX.SUPERUSER                                 READ    NONE
__ IRR.LISTUSER                                  NONE    READ
******************************* Bottom of Data ********************************









Command ===> _                                                 Scroll===> CSR
MA      a                                                               32/015
```

IBMAGINA

Un planeta más inteligente necesita software más inteligente

Cambiando en contexto



```
zSecure Admin+Audit for RACF USER overview                        Line 1 of 44
Users like Z*                                   30 Jan 2008 14:35
   User     Complex  Name                 DfltGrp  Owner    RIRP SOA gC LCX Grp
__ ZAADMIN  ZT01     WAS ADMINISTRATOR    ZACFG    SENIOR   rI   S            1
__ ZAADMSH  ZT01     WAS ASYNCH ADMIN TAS ZACFG    SENIOR      P              1
__ ZACRU    ZT01     WAS DAEMON CR        ZACFG    SENIOR      P         C    2
__ ZACTWTR  ZT01     WAS TRACE WRITER     ZACFG    SENIOR      P              1
__ ZAGUEST  ZT01     WAS DEFAULT USER     ZAGUESTG SENIOR     R           X   1
__ ZASRU    ZT01     WAS APPSVR SR        ZASRG    SENIOR      P              4
__ ZBADMIN  ZT01     WAS ADMINISTRATOR    ZBCFG    SENIOR   rI   S            2
__ ZBADMSH  ZT01     WAS ASYNCH ADMIN TAS ZBCFG    SENIOR      P              1
__ ZBCRU    ZT01     WAS DMGR CR          ZBCFG    SENIOR    I P         C    2
__ ZBCTWTR  ZT01     WAS TRACE WRITER     ZBCFG    SENIOR      P              1
__ ZBGUEST  ZT01     WAS DEFAULT USER     ZBGUESTG SENIOR    IRP              1
__ ZBOWNER  ZT01     WAS HFS OWNER        ZBCFG    SENIOR    I P              1
__ ZBSRU    ZT01     WAS DMGR SR          ZBSRG    SENIOR    I P              4
__ ZCADMIN  ZT01     WAS ADMINISTRATOR    ZCCFG    PIERRE                     1
__ ZCADMSH  ZT01     WAS ASYNCH ADMIN TAS ZCCFG    PIERRE      P              1
__ ZCCRU    ZT01     WAS DAEMON CR        ZCCFG    PIERRE      P         C    1
__ ZCGUEST  ZT01     WAS DEFAULT USER     ZCGUESTG PIERRE     R           X   1
__ ZCOWNER  ZT01     WAS HFS OWNER        ZCCFG    PIERRE    I P              1
__ ZCSRU    ZT01     WAS APPSVR SR        ZCSRG    PIERRE      P         C    2
__ ZDACRU   ZT01     WAS DAEMON CR        ZDCFG    STSGJJ      P         C    2
__ ZDADMIN  ZT01     WAS ADMINISTRATOR    ZDCFG    STSGJJ    I                1
__ ZDASRU   ZT01     WAS APPSVR SR        ZDSRG    STSGJJ      P         C    3
__ ZDDBU    ZT01     ZD CELL  DB USER     ZDCFG    STSGJJ    I                1
__ ZDGUEST  ZT01     WAS DEFAULT USER     ZDGUESTG STSGJJ    IRP              1
__ ZDOWNER  ZT01     WAS HFS OWNER        ZDCFG    STSGJJ    I P              1
__ ZEACRU   ZT01     WAS DAEMON CR        ZECFG    STSGJJ      P         C    2
__ ZEADMIN  ZT01     WAS ADMINISTRATOR    ZECFG    STSGJJ                     2
__ ZEADMSH  ZT01     WAS ASYNCH ADMIN TAS ZECFG    STSGJJ    I P              1
Command ===>                                                   Scroll===> CSR
MA     a                                                                10/063
```

IBMAGINA

Un planeta más inteligente necesita software más inteligente

Proteger RACF de los Administradores

- Situación:
  - Gestión de la seguridad externalizada
  - Administración de usuarios delegada a personal no técnico
  - Departamentos con sus propias aplicaciones, responsibilidades y administradores de seguridad

- Solución Disponible?:
  - Implantar GROUP SPECIAL, GROUP AUDITOR
    - Poco práctica cuando los “ ownership” de perfiles no está claramente especificada en RACF
  - Desarrollo para construir los comandos de RACF
    - Se evita el tecleo directo pero los privilegios siguen inalterados

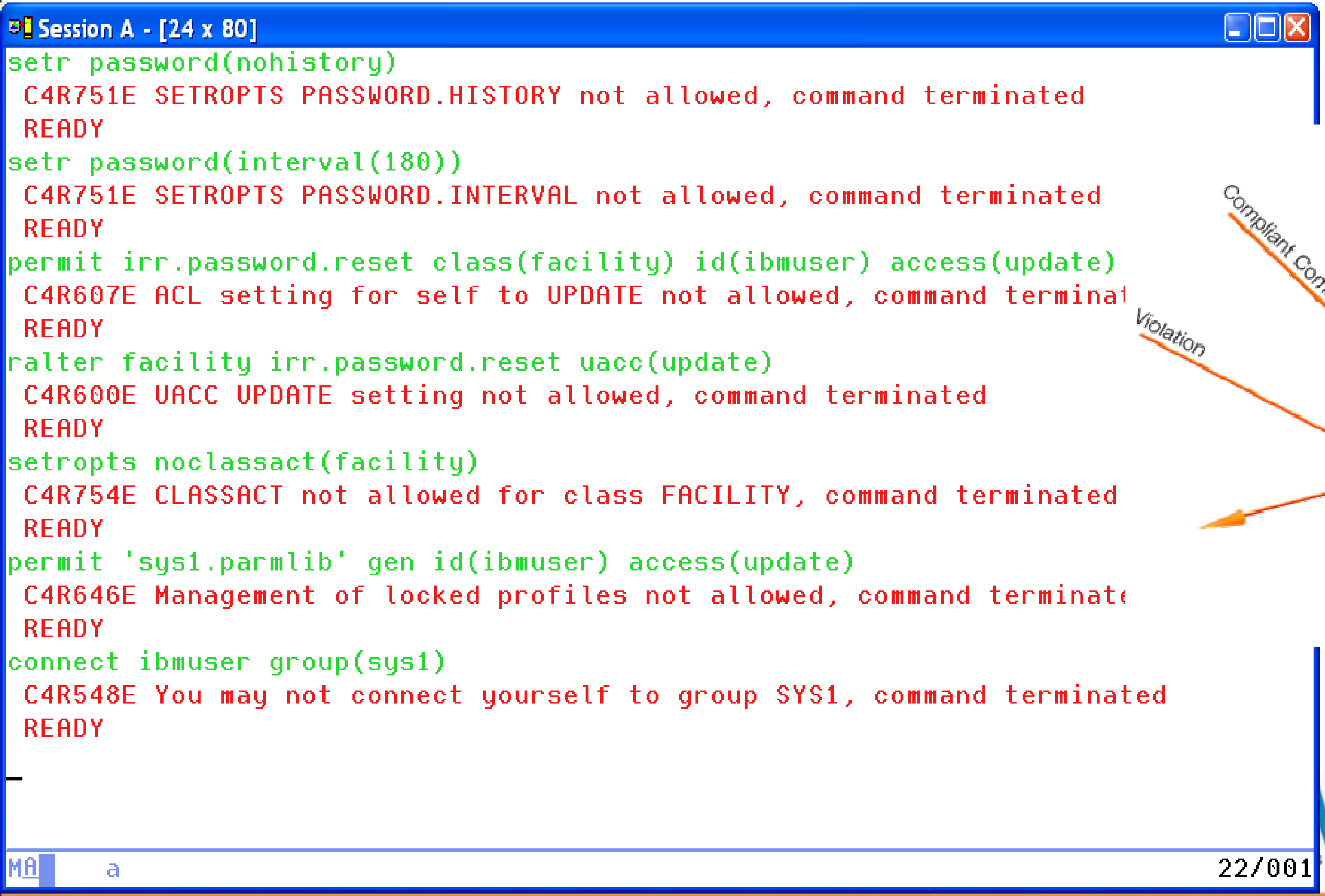
zSecure Solution

- Protección contra comandos RACF
  - zSecure Command Verifier
  - Cada cambio verificado contra politicas granulares
    - Usando mascaras para clases y perfiles RACF
  - Prevención de comandos inapropiados
  - Resolución de parámetros incorrectos u olvidados
  - Incluso controla a los usuarios privilegiados (Special)

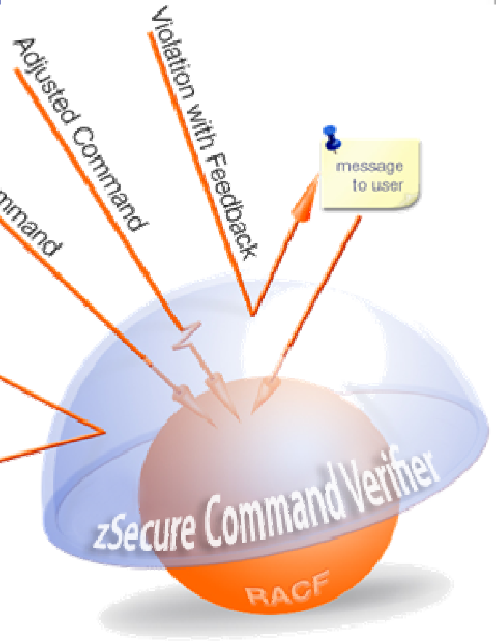
IBMAGINA

Un planeta más inteligente necesita software más inteligente

zSecure Command Verifier
Protección de comandos



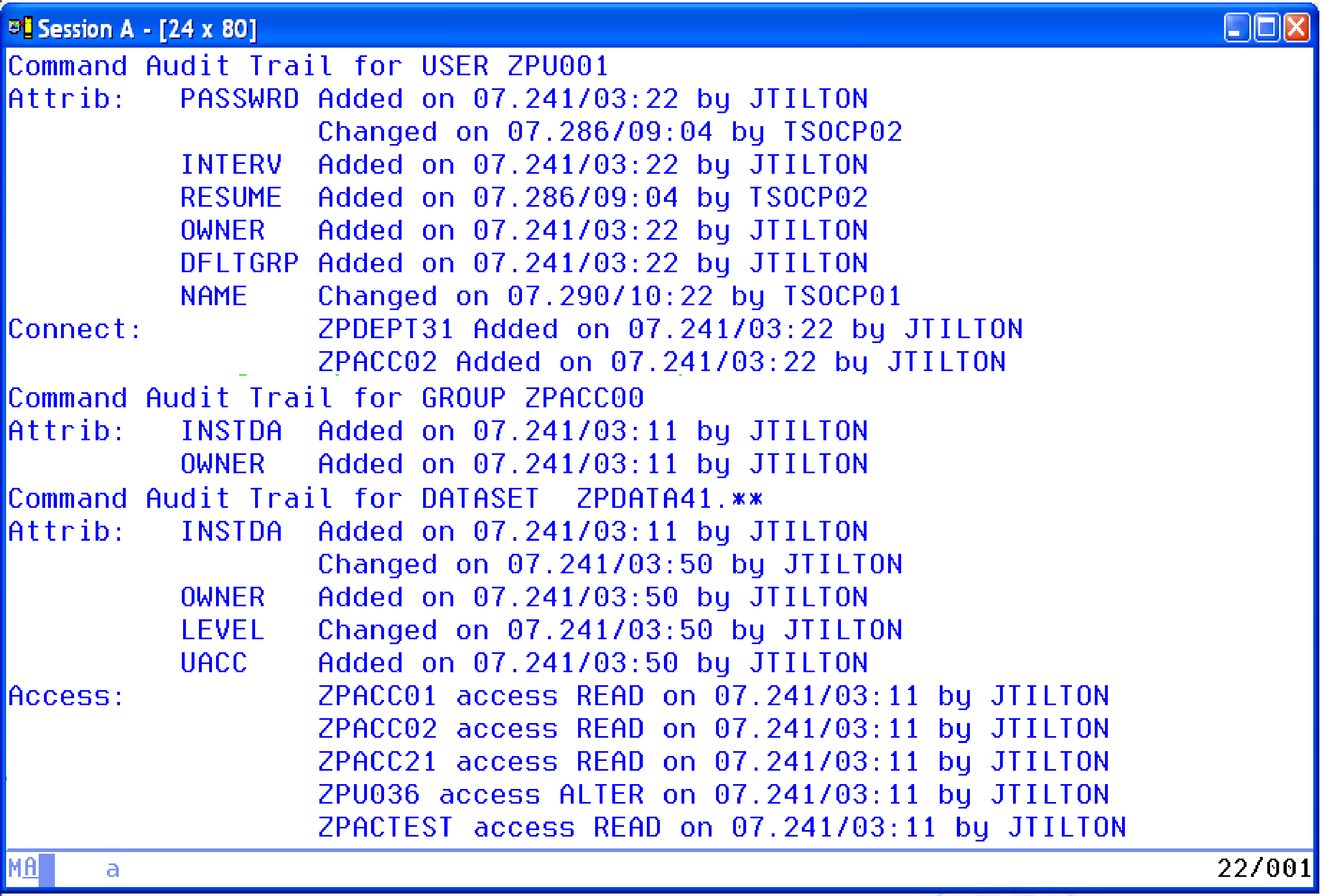
```
setr password(nohistory)
 C4R751E SETROPTS PASSWORD.HISTORY not allowed, command terminated
 READY
setr password(interval(180))
 C4R751E SETROPTS PASSWORD.INTERVAL not allowed, command terminated
 READY
permit irr.password.reset class(facility) id(ibmuser) access(update)
 C4R607E ACL setting for self to UPDATE not allowed, command terminat
 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 terminate
 READY
connect ibmuser group(sys1)
 C4R548E You may not connect yourself to group SYS1, command terminated
 READY

_

MA      a                                                        22/001
```



MAGINA

s inteligente necesita software más inteligente

Registro de operaciones



```
Command Audit Trail for USER ZPU001
Attrib:    PASSWRD Added on 07.241/03:22 by JTILTON
                   Changed on 07.286/09:04 by TSOCP02
           INTERV  Added on 07.241/03:22 by JTILTON
           RESUME  Added on 07.286/09:04 by TSOCP02
           OWNER   Added on 07.241/03:22 by JTILTON
           DFLTGRP Added on 07.241/03:22 by JTILTON
           NAME    Changed on 07.290/10:22 by TSOCP01
Connect:           ZPDEPT31 Added on 07.241/03:22 by JTILTON
                   ZPACC02 Added on 07.241/03:22 by JTILTON
Command Audit Trail for GROUP ZPACC00
Attrib:    INSTDA  Added on 07.241/03:11 by JTILTON
           OWNER   Added on 07.241/03:11 by JTILTON
Command Audit Trail for DATASET  ZPDATA41.**
Attrib:    INSTDA  Added on 07.241/03:11 by JTILTON
                   Changed on 07.241/03:50 by JTILTON
           OWNER   Added on 07.241/03:50 by JTILTON
           LEVEL   Changed on 07.241/03:50 by JTILTON
           UACC    Added on 07.241/03:50 by JTILTON
Access:            ZPACC01 access READ on 07.241/03:11 by JTILTON
                   ZPACC02 access READ on 07.241/03:11 by JTILTON
                   ZPACC21 access READ on 07.241/03:11 by JTILTON
                   ZPU036 access ALTER on 07.241/03:11 by JTILTON
                   ZPACTEST access READ on 07.241/03:11 by JTILTON
MA     a                                                          22/001
```

Quien ha realizado cambios en los perfiles críticos

IBMAGINA

Un planeta más inteligente necesita software más inteligente

Mostrar activades z/OS en un contexto de negocio

- Los logs de SMF son demasiado técnicos para un auditor de negocio
  - – Terminología z
    - “Data set names” por ejemplo
  - – Usuarios sin la identificación o el rol
  - – Acciones (“events”) orientadas a RACF
    - RACINIT… SETROPTS
- SMF proporciona demasiados datos

- Que sucede?
  - – El auditor se orienta al fallo
  - – Los informes son manejados por los técnicos

- Tivoli Security Information and Event Manager (TSIEM)
- Antes Tivoli Compliance InSight Manager (TCIM)
  - – Clasifica todos los recurso y usuarios de diferentes entornos
    - Use el concepto agrupación: Los objetos se agrupan con una etiqueta
  - – Traduce eventos en terminos independientes de plataforma
  - – Aplica políticas de ***uso aceptable***
    - Identifica actividades no aceptables en objetos
      - – Politicas de excepción
    - Se puede focalizar en eventos no esperados
  - – Integra z/OS, RACF y DB2 con Windows, Unix, Firewall, SAP, …

Tivoli Solution

IBMAGINA
Un planeta más inteligente necesita software más inteligente

Recomendaciones de buenas prácticas sobre Gestión de Logs

CobiT 4

- Provide adequate audit trail for root-cause analysis
- Use logging and monitoring to detect unusual or abnormal activities
- Regularly review access, privileges, changes
- Monitor performance
- Verify backup completion

ISO 17799/27002

- Maintain audit logs for system access and use, changes, faults, corrections, capacity demands
- Review the results of monitoring activities regularly
- Ensure the accuracy of the logs

NIST 800-53

- Capture audit records
- Regularly review audit records for unusual activity and violations
- Automatically process audit records
- Protect audit information from unauthorized deletion
- Retain audit logs

PCI

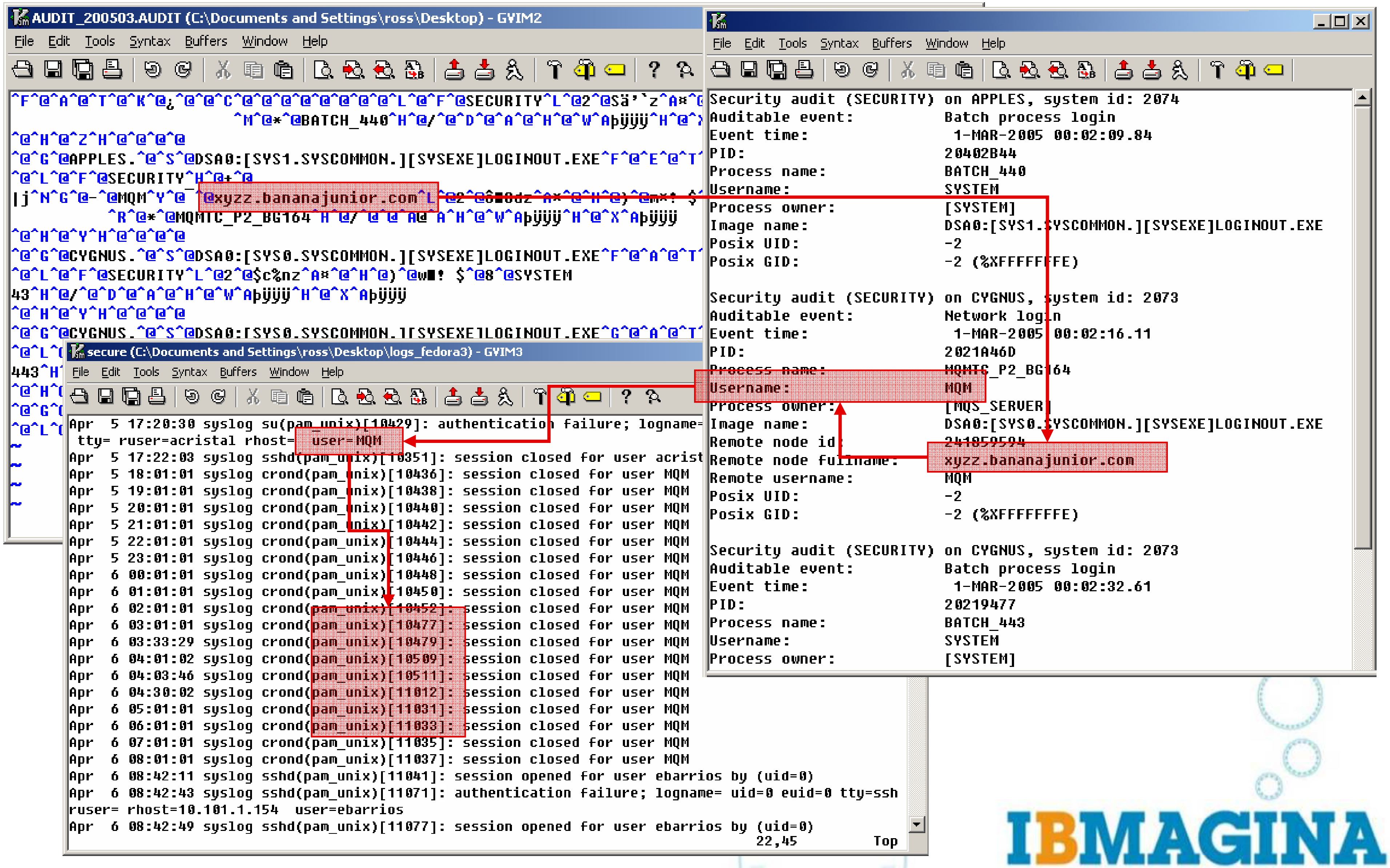
Requirement 10

- Logging and user activities tracking are critical
- Automate and secure audit trails for event reconstruction
- Review logs daily
- Retain audit trail history for at least one year

IBMAGINA

Un planeta más inteligente necesita software más inteligente

¿Como armonizamos esto ?



AUDIT_200503.AUDIT (C:\Documents and Settings\ross\Desktop) - GVIM2
File Edit Tools Syntax Buffers Window Help

```
^F^@^A^@^T^@^K^@¿^@^@^C^@^@^@^@^@^@^@^@^L^@^F^@SECURITY^L^@2^@Sä'`z^A¤^@
                         ^M^@*^@BATCH_440^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X
^@^H^@^Z^H^@^@^@^@
^@^G^@APPLES.^@^S^@DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^E^@^T^
^@^L^@^F^@SECURITY^H^@+^@
|j^N^G^@-^@MQM^Y^@ ^@xyzz.bananajunior.com^L^@2^@ô■0dz^A¤^@^H^@)^@m¤! $
           ^R^@*^@MQMTC_P2_BG164^H^@/^@^@^A@^A^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^F^@^A^@^T^
^@^L^@^F^@SECURITY^L^@2^@$c%nz^A¤^@^H^@)^@w■! $^@8^@SYSTEM
43^H^@/^@^D^@^A^@^H^@^W^Aþÿÿÿ^H^@^X^Aþÿÿÿ
^@^H^@^Y^H^@^@^@^@
^@^G^@CYGNUS.^@^S^@DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE^G^@^A^@^T^
^@^L^(
443^H^
^@^H^(
^@^G^(
^@^L^(
~
~
~
~
```

secure (C:\Documents and Settings\ross\Desktop\logs_fedora3) - GVIM3
File Edit Tools Syntax Buffers Window Help

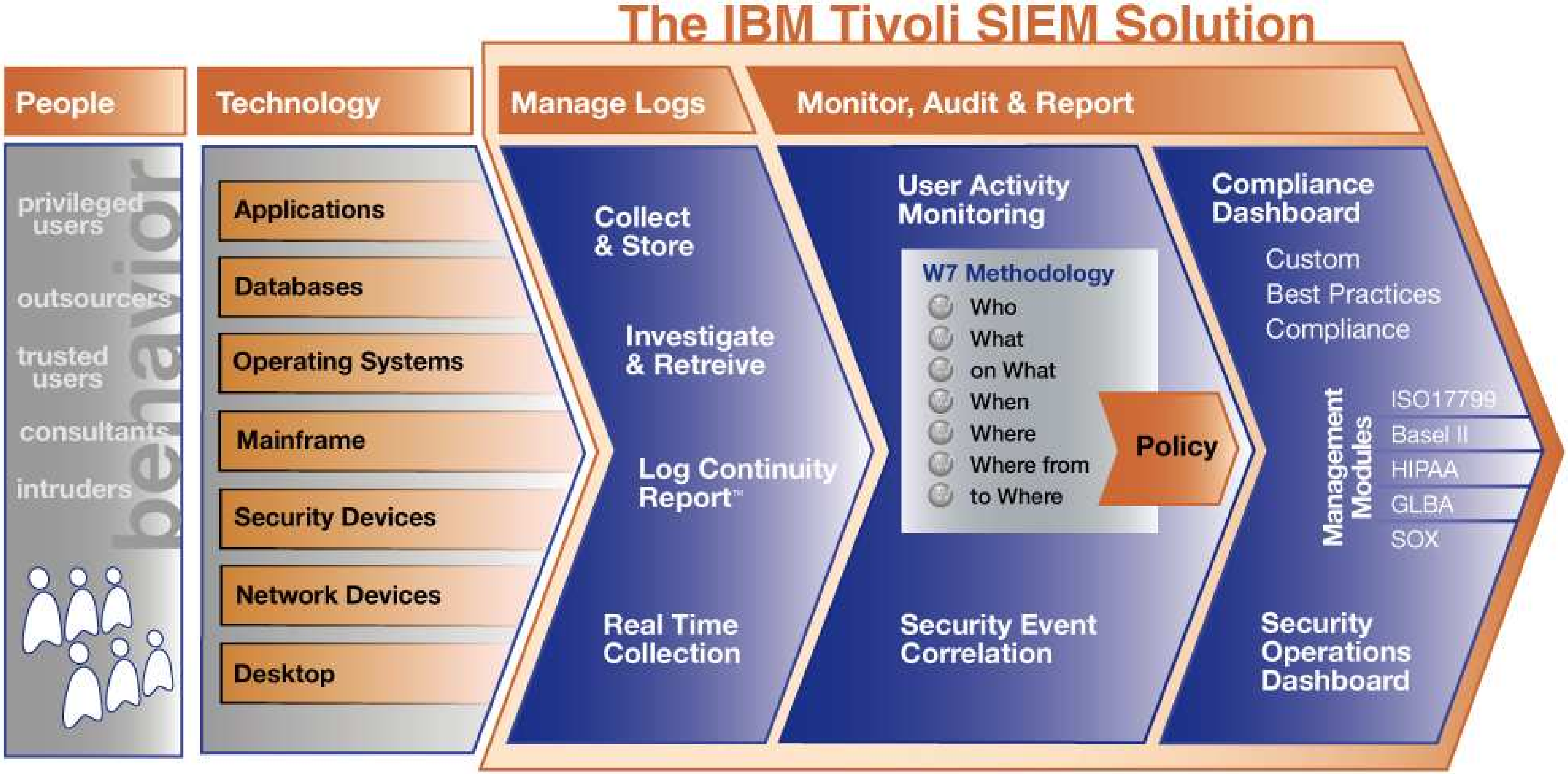
```
Apr  5 17:20:30 syslog su(pam_unix)[10429]: authentication failure; logname=
 tty= ruser=acristal rhost=  user=MQM
Apr  5 17:22:03 syslog sshd(pam_unix)[10351]: session closed for user acrist
Apr  5 18:01:01 syslog crond(pam_unix)[10436]: session closed for user MQM
Apr  5 19:01:01 syslog crond(pam_unix)[10438]: session closed for user MQM
Apr  5 20:01:01 syslog crond(pam_unix)[10440]: session closed for user MQM
Apr  5 21:01:01 syslog crond(pam_unix)[10442]: session closed for user MQM
Apr  5 22:01:01 syslog crond(pam_unix)[10444]: session closed for user MQM
Apr  5 23:01:01 syslog crond(pam_unix)[10446]: session closed for user MQM
Apr  6 00:01:01 syslog crond(pam_unix)[10448]: session closed for user MQM
Apr  6 01:01:01 syslog crond(pam_unix)[10450]: session closed for user MQM
Apr  6 02:01:01 syslog crond(pam_unix)[10452]: session closed for user MQM
Apr  6 03:01:01 syslog crond(pam_unix)[10477]: session closed for user MQM
Apr  6 03:33:29 syslog crond(pam_unix)[10479]: session closed for user MQM
Apr  6 04:01:02 syslog crond(pam_unix)[10509]: session closed for user MQM
Apr  6 04:03:46 syslog crond(pam_unix)[10511]: session closed for user MQM
Apr  6 04:30:02 syslog crond(pam_unix)[11012]: session closed for user MQM
Apr  6 05:01:01 syslog crond(pam_unix)[11031]: session closed for user MQM
Apr  6 06:01:01 syslog crond(pam_unix)[11033]: session closed for user MQM
Apr  6 07:01:01 syslog crond(pam_unix)[11035]: session closed for user MQM
Apr  6 08:01:01 syslog crond(pam_unix)[11037]: session closed for user MQM
Apr  6 08:42:11 syslog sshd(pam_unix)[11041]: session opened for user ebarrios by (uid=0)
Apr  6 08:42:43 syslog sshd(pam_unix)[11071]: authentication failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=10.101.1.154  user=ebarrios
Apr  6 08:42:49 syslog sshd(pam_unix)[11077]: session opened for user ebarrios by (uid=0)
                                                                      22,45          Top
```

```
Security audit (SECURITY) on APPLES, system id: 2074
Auditable event:          Batch process login
Event time:                1-MAR-2005 00:02:09.84
PID:                      20402B44
Process name:             BATCH_440
Username:                 SYSTEM
Process owner:            [SYSTEM]
Image name:               DSA0:[SYS1.SYSCOMMON.][SYSEXE]LOGINOUT.EXE
Posix UID:                -2
Posix GID:                -2 (%XFFFFFFFE)

Security audit (SECURITY) on CYGNUS, system id: 2073
Auditable event:          Network login
Event time:                1-MAR-2005 00:02:16.11
PID:                      2021A46D
Process name:             MQMTC_P2_BG164
Username:                 MQM
Process owner:            [MQS_SERVER]
Image name:               DSA0:[SYS0.SYSCOMMON.][SYSEXE]LOGINOUT.EXE
Remote node id:           241859594
Remote node fullname:     xyzz.bananajunior.com
Remote username:          MQM
Posix UID:                -2
Posix GID:                -2 (%XFFFFFFFE)

Security audit (SECURITY) on CYGNUS, system id: 2073
Auditable event:          Batch process login
Event time:                1-MAR-2005 00:02:32.61
PID:                      20219477
Process name:             BATCH_443
Username:                 SYSTEM
Process owner:            [SYSTEM]
```

IBMAGINA

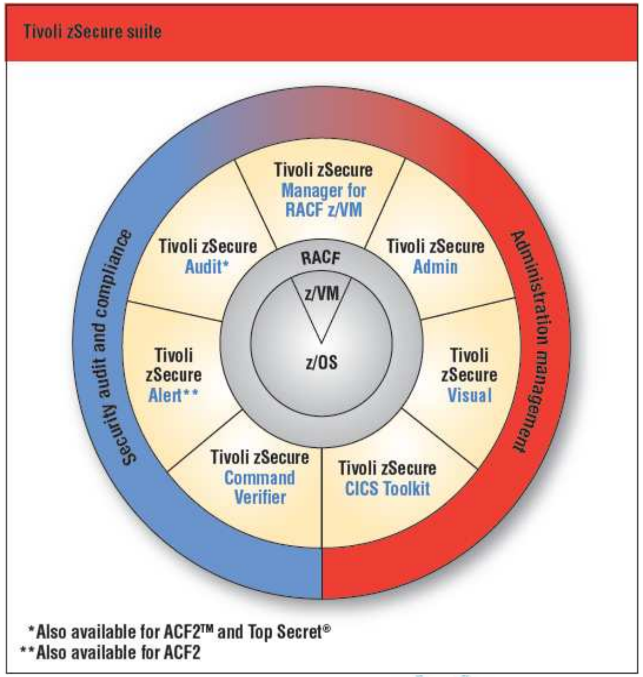
Un planeta más inteligente necesita software más inteligente

IBM Tivoli Security & Event Management (TSIEM)



zSecure : Sumario

- Retos y Realidades de la regulación
  - Las amenazas, regulación de cambios y usuarios privilegiados
- La suite zSecure –La seguridad RACF mas fácil
  - Administración
  - Auditoría y cumplimientos
  - Alertas en tiempo real
  - Intercepción de comandos
- También para RACF en z/VM,
  CA ACF2 y CA Top Secret


Tivoli zSecure suite
Security audit and compliance
Administration management
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

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

IBMAGINA
Un planeta más inteligente necesita software más inteligente

La suite zSecure optimiza la Gestión de la Seguridad de Mainframe de forma eficaz

IBMAGINA

Un planeta más inteligente necesita software más inteligente

Muchas gracias por su atención

IBMAGINA

Un planeta más inteligente necesita software más inteligente