



IBM Software Group

The System z security hub: RACF administration

Rob van Hoboken

zSecure Architect

Rob.vanHoboken@nl.ibm.com

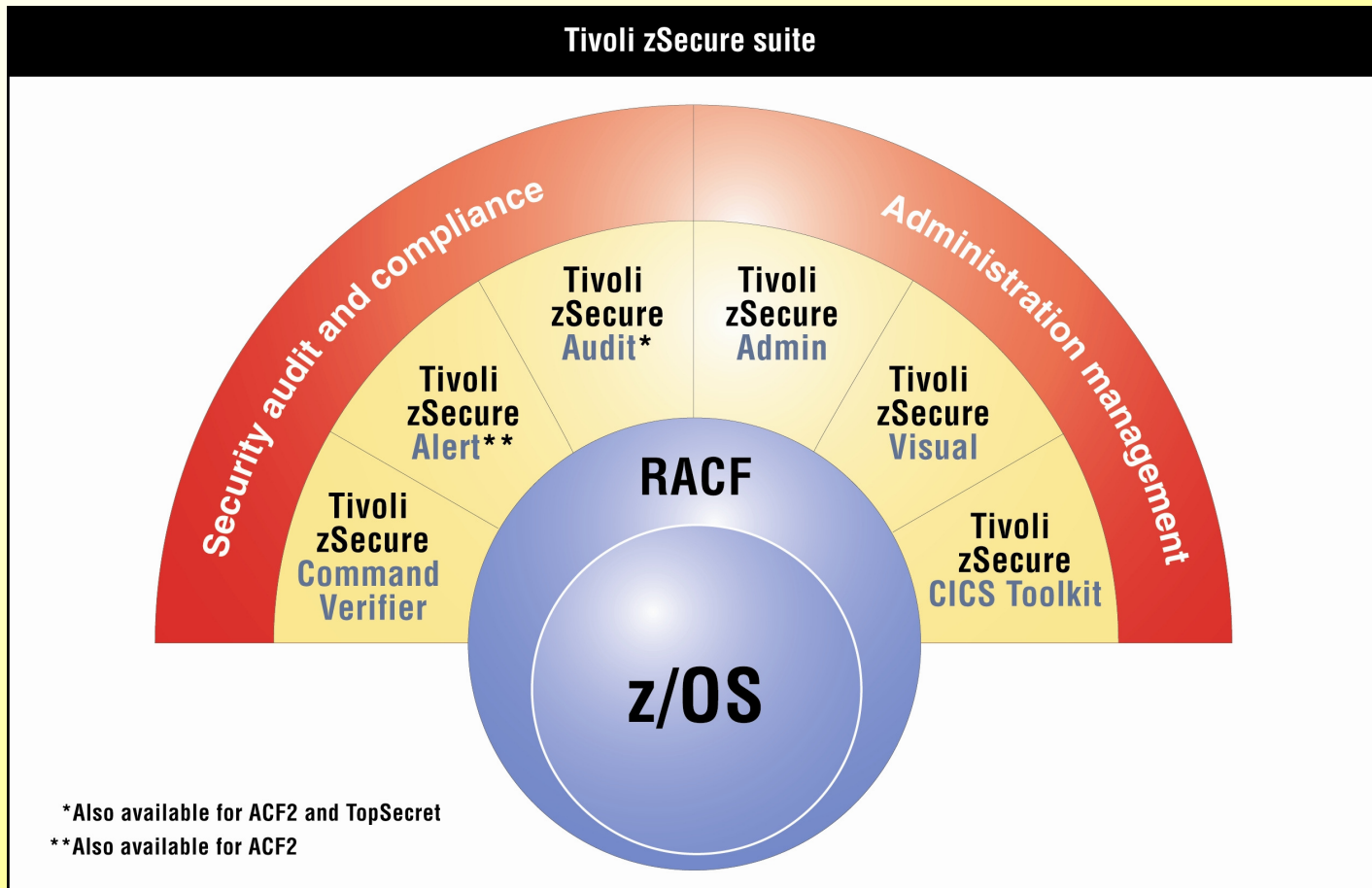


@business on demand.

© 2003 IBM Corporation

Introducing the IBM Tivoli zSecure Suite

Making z/OS security management more effective



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

Security administration is not easy

- Situation:
 - ▶ Technical users perform administration
 - ▶ User administration by non-technical users
 - ▶ Technical aspects of security by technical teams
- Best Solution Available?:
 - ▶ Use RACF commands via ISPF
 - Output is not easy to interpret
 - ▶ Use unloaded RACF database in DB2
 - Information not up to date

zSecure Solution

- Easy RACF administration – zSecure Admin
 - ▶ Overview of profiles, show context of security
 - ▶ Overtyping fields to make corrections
 - ▶ Reports showing differences and effective security
- Actual information from active RACF database



RACF LISTUSER (LU) command output

```

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 ***

```



zSecure Admin: Overview of user profiles

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

32/015



Details of a user profile

```

Session A - [32 x 80]
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 SDA AG Uacc      Revokedt      Resumedt      InstData
- ZACFG    USE      -   -   - NONE      -             -             -

System access
Revoked (may be by date)      No
Inactive, revoked or pending Yes
Days of week user can logon  SMTWTFS
Time of day user can logon   _____
Date user will be revoked    _____ (ddmmyyyy or NOREVOKE)
Date user will be resumed    _____ (ddmmyyyy or NORESUME)

Statistics
Creation date                 29Sep05
Last RACINIT current connects 11Sep07
User's last use date          11Sep07
User's last use time          10:46

Password
Has a password                Yes
Expired password              No
Password changed date         29Sep05
Password expiration date      _____
Old passwords present #       0
Failed password attempts #    0
Password interval             _____
Password interval in effect   _____
Mixed case password          No

Password phrase
Has a password phrase         No
Expired password phrase       No
Password phrase change date   _____
Password phrase expiry date   _____
Old pass phrases present #    0

Command ==> _____ Scroll==> CSR
M@ a                                                                32/015
  
```

Access granted to the user via Permit and Connect

```
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
Mâ a 32/015
```

Compare access between users

```
Session A - [32 x 80]
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
--- BPX.SUPERUSER          ZAADMIN ZBADMIN
--- IRR.LISTUSER          READ  NONE
                          NONE  READ
***** Bottom of Data *****
Command ==>
Scroll==> CSR
Mâ a 32/015
```


Make changes by typing over the data

```

Session A - [32 x 80]
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    C    1
  ZAADMSSH ZT01      WAS ASYNCH ADMIN TAS             ZACFG    SENIOR   P     S    C    1
  ZACRU     ZT01      WAS DAEMON CR                     ZACFG    SENIOR   P     S    C    2
  ZACTWTR   ZT01      WAS TRACE WRITER                  ZACFG    SENIOR   P     S    C    1
  ZAGUEST   ZT01      WAS DEFAULT USER                 ZAGUESTG SENIOR   R     S    X    1
  ZASRU     ZT01      WAS APPSVR SR                     ZASRG    SENIOR   P     S    C    4
  ZBADMIN   ZT01      WAS ADMINISTRATOR                 ZBCFG    SENIOR   rI    S    C    2
  ZBADMSSH ZT01      WAS ASYNCH ADMIN TAS             ZBCFG    SENIOR   P     S    C    1
  ZBCRU     ZT01      WAS DMGR CR                       ZBCFG    SENIOR   I P   S    C    2
  ZBCTWTR   ZT01      WAS TRACE WRITER                  ZBCFG    SENIOR   P     S    C    1
  ZBGUEST   ZT01      WAS DEFAULT USER                 ZBGUESTG SENIOR   IRP   S    C    1
  ZBOWNER   ZT01      WAS HFS OWNER                     ZBCFG    SENIOR   I P   S    C    1
  ZBSRU     ZT01      WAS DMGR SR                       ZBSRG    SENIOR   I P   S    C    4
  ZCADMIN   ZT01      WAS ADMINISTRATOR                 ZCCFG    PIERRE   P     S    C    1
  ZCADMSSH ZT01      WAS ASYNCH ADMIN TAS             ZCCFG    PIERRE   P     S    C    1
  ZCCRU     ZT01      WAS DAEMON CR                     ZCCFG    PIERRE   P     S    C    1
  ZCGUEST   ZT01      WAS DEFAULT USER                 ZCGUESTG PIERRE   R     S    X    1
  ZCOWNER   ZT01      WAS HFS OWNER                     ZCCFG    PIERRE   I P   S    C    1
  ZCSRU     ZT01      WAS APPSVR SR                     ZCSRG    PIERRE   P     S    C    2
  ZDACRU    ZT01      WAS DAEMON CR                     ZDCFG    STSGJJ   P     S    C    2
  ZDADMIN   ZT01      WAS ADMINISTRATOR                 ZDCFG    STSGJJ   I     S    C    1
  ZDASRU    ZT01      WAS APPSVR SR                     ZDSRG    STSGJJ   P     S    C    3
  ZDDBU     ZT01      ZD CELL DB USER                  ZDCFG    STSGJJ   I     S    C    1
  ZDGUEST   ZT01      WAS DEFAULT USER                 ZDGUESTG STSGJJ   IRP   S    C    1
  ZDOWNER   ZT01      WAS HFS OWNER                     ZDCFG    STSGJJ   I P   S    C    1
  ZEACRU    ZT01      WAS DAEMON CR                     ZECFG    STSGJJ   P     S    C    2
  ZEADMIN   ZT01      WAS ADMINISTRATOR                 ZECFG    STSGJJ   P     S    C    2
  ZEADMSSH ZT01      WAS ASYNCH ADMIN TAS             ZECFG    STSGJJ   I P   S    C    1
Command ==>

```

Security administrators make mistakes

- Situation:
 - ▶ Security management outsourced
 - ▶ User administration delegated to non-technical users
 - ▶ Departments with their own applications, responsibility and security administrators
- Best Solution Available?:
 - ▶ Solution (?): implement GROUP SPECIAL, GROUP AUDITOR
 - Impractical when profile ownership is not clearly specified in RACF

zSecure Solution

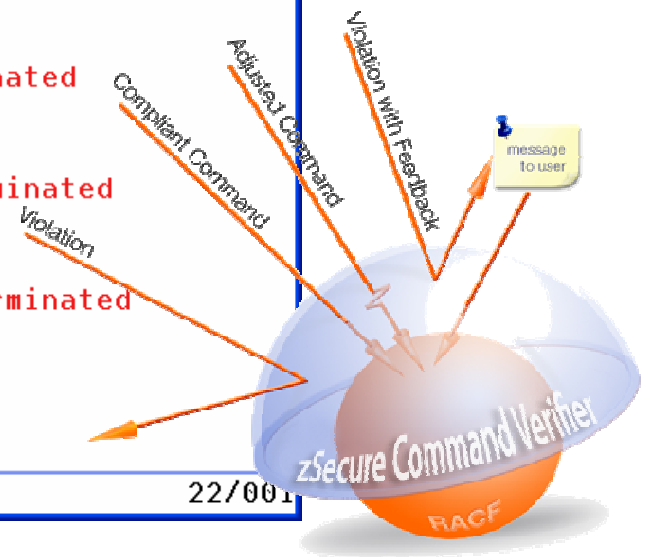
- RACF command screening – zSecure Command Verifier
 - ▶ Each security change verified against granular policy
 - Using masks for classes and profiles
 - ▶ Inappropriate commands prevented
 - ▶ Missing or incorrect parameters can be fixed
 - ▶ Even controls command by system special users



zSecure Command Verifier

Prevent
commands
that would
cripple your
security

```
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
```



Decentralized security administration

- Situation:
 - ▶ Password administration by helpdesk
 - ▶ User administration delegated to non-technical users
 - ▶ Departments with their own applications, responsibility and security administrators
- Best Solution Available?:
 - ▶ Write ISPF/Rexx front-end
 - ▶ Front-end using unloaded RACF info on Windows/Unix
 - ▶ Implement identity management solution

zSecure Solution

- Graphical user interface: zSecure Visual
 - ▶ Windows GUI for RACF management
 - ▶ Work with active RACF information
 - ▶ Supports scoping for decentralized administration



zSecure Visual – leveraging a GUI for RACF

The screenshot displays the zSecure Visual interface. On the left is a 'Group tree' showing a hierarchy of groups under 'SYS1'. The main window shows a list of 56 users, including 'STUDENT UK CONTEST' users and 'STUDEN' users with various roles like 'Schedules', 'Connects', and 'Properties'. A 'Find' dialog box is open, showing search criteria for a 'User' class with the name 'contest'. Below the user list is a table titled '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
OPERCMD5	MVS.CANCEL.STC.SMC0096.**	Generic	Update		None				Read	5	SYS1
OPERCMD5	MVS.CANCEL.TSU.SMC0096	Discrete	Update		None				Read	2	BABEYS
OPERCMD5	MVS.START.STC.SMC0096	Discrete	Update		None				Read	5	SYS1
OPERCMD5	MVS.START.STC.WEBS096	Discrete	Update		None				Read	2	BABEYS
OPERCMD5	MVS.STOP.STC.SMC0096	Discrete	Update		None				Read	5	SYS1
OPERCMD5	MVS.STOP.STC.WEBS096	Discrete	Update		None				Read	2	BABEYS

Find mis-configuration and vulnerabilities

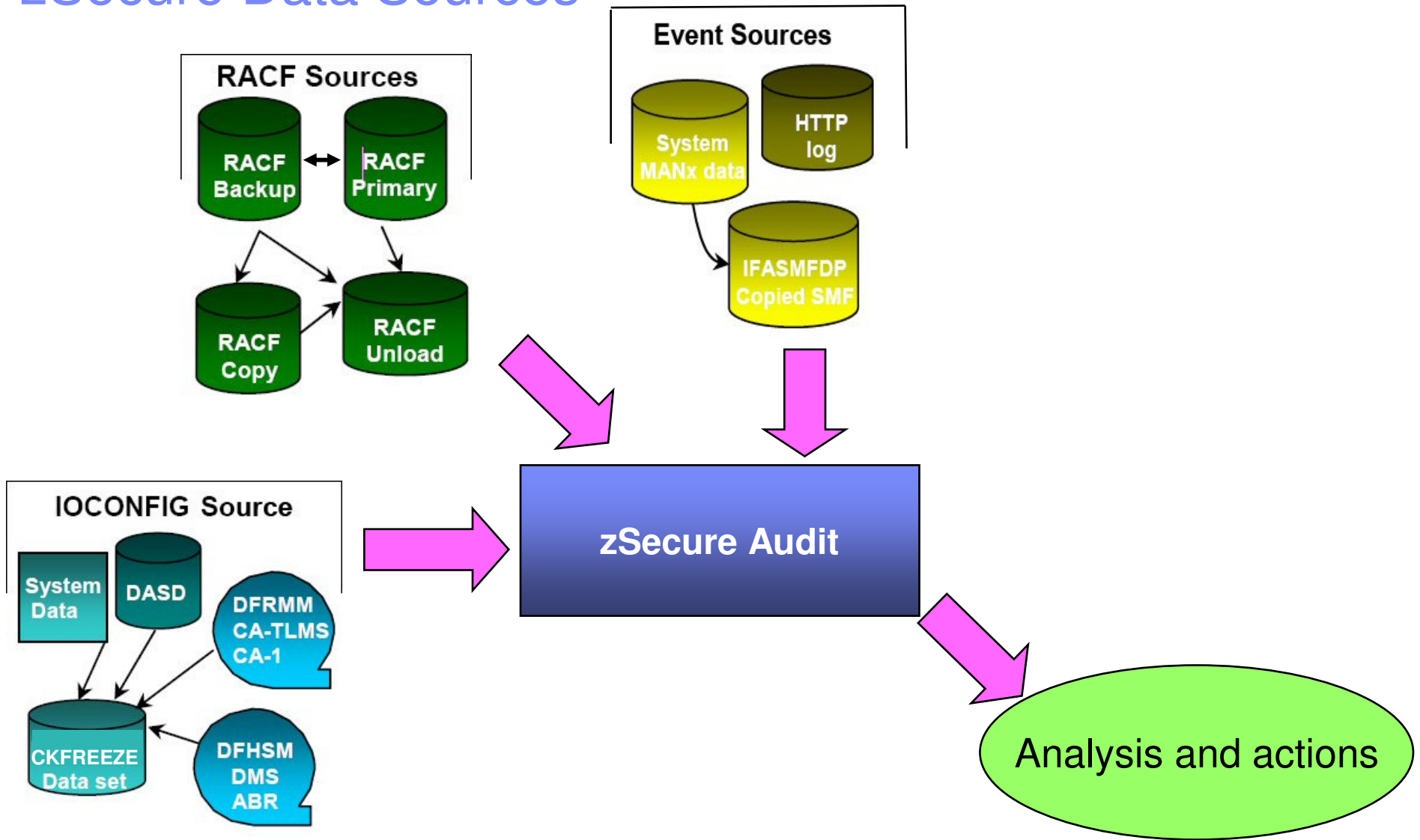
- Situation:
 - ▶ z/OS and RACF protect each other
 - System datasets must be protected...
 - ▶ Verifying the protection is time consuming
- Best Solution Available?:
 - ▶ Individual reports for RACF, PARMLIB, UNIX....
 - Manual correlation and verification?
 - ▶ Annual external audit

zSecure Solution

- zSecure Audit takes information from RACF, z/OS, UNIX
 - ▶ Identifies inconsistencies and vulnerabilities
 - ▶ Shows the privileged users that can change z/OS, RACF
 - Or bypass security
 - ▶ Adhoc reports via ISPF
 - ▶ Automatic reporting and monitoring in batch jobs



zSecure Data Sources



z/OS Status Audit – detailed reports

```

Session A - [32 x 80]
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_

Mâ a 04/001

```


Automated vulnerability assessment

```

Session A - [32 x 80]
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_
Mâ a                                                                    31/015

```

Trusted Userid Report

```

Session A - [32 x 80]
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 TS0 userid
Command ==> _____ Scroll==> CSR
MA a                                                                    31/015

```

If access controls are not strong enough

- Situation:
 - ▶ Too many technicians with access to business databases
 - ▶ Must keep financial data confidential to prevent insider trading
 - ▶ Allow technicians to do their work
- Best Solution Available?:
 - ▶ Need to restrict access to financial data
 - Storage admin and sysprogs reading business datasets
 - Security admins granting themselves authority
 - Data security administrators granting improper access
 - ▶ Access reduction for privileged users
 - Impractical due to technical limitations
 - If you remove my ability to I cannot commit to

zSecure Solution

- Real-time alert as mitigating control – zSecure Alert
 - ▶ Reduce need to implement separation of access
 - ▶ sysprogs keep their “must be able to read/change anything” status
 - ▶ No need for political battle or costly re-orgs
 - ▶ Quick install, instant visibility



zSecure Alert issues alert for dangerous access

Alert: Information access by SPROGJOE on FINANCE data set SHIPPING.VOLUME.MONTHLY - Lotus Notes

File Edit View Create Actions Text Help

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...

1 Save And File 2 Save And Close 3 Follow Up 4 Tools 5 Consul

C2POLICE at DINO
 <c2p.PZ00860@consul.nl>
 15-10-2006 00:46

To: Data Security <Datasec@shipping.com>
 cc:
 bcc:
 Subject: Alert: Information access by SPROGJOE on FINANCE data set SHIPPING.VOLUME.MONTHLY

Please respond to <security@shipping.com>

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

Body of message

Untagged Office



Integration with Tivoli Security Operations Manager

The screenshot shows the Tivoli Security Operations Manager interface. At the top, there are navigation tabs: Dashboard, Reports, Tools, Options, and Admin. Below these is a menu bar with Visuals, Window, and Help. The main content area displays a table of events under the 'PowerGrid' window. The table has columns for Src Threat, Dst Threat, Protocol, Src IP, Dst IP, Src Port, Dst Port, Domain, Src Watchlist, Dst Watchlist, EAM Time, and Sensor Time ID. Several rows show events related to 'IBMUUSER accessed data set with OPERATIC'. An event details window is open, showing the following information:

Field	Value
EAM Time	Time this event was received by the EAM (according to the EAM's clock). 2007-03-19 20:05:49
Sensor Time	Time the sensor detected this event (according to the sensor's clock). 2007-03-19 20:05:49
Sensor Name	Name of the Sensor that reported this event. CONSUL
Sensor Type	Type of Sensor that reported this event. zAlert
Protocol	Protocol number of the event. 17
Source IP	Source address of this event. 0.0.0.0
Destination IP	Destination address of this event. 0.0.0.0
Source Port	Source port of this event. 0
Destination Port	Destination port of this event. 0
Event Type	Type of event. NON_OPERATIONS_USED_OPERATIONS
Event Class	Class of event. 20000
User Name	User name. T.Q.B.F.J.O.T.L DOG
User Context	User context. DINO
Info	Additional information associated with this event. nonOperationsUsedOperations: "eventIntegral = Alert: non-OPERATIONS user IBMUSER accessed data set with OPERATIONS - ..." "eventWhen = 2003-1-23 11:45:39.3+1:0" "onWhatDSNAME = SOME.DATASET" "onWhatALLOWED = READ" "onWhatINTENT = CONTROL" "whoUSERID = IBMUSER" "whoNAME = T.Q.B.F.J.O.T.L DOG" "whatDESC = WARNING" "whatJOBNAME = RACF" "whereSYSTEM = DINO"

Real time RACF and z/OS monitoring leveraging Tivoli zSecure Alert



Case study: SOX reports

- Sarbanes Oxley requirements
 - ▶ Monitor changes to operating system and security (RACF and ACF2)
 - ▶ Monitor activities of privileged users
 - ▶ Monitor irregular logons
 - ▶ Verify operating system parameters against baselines
 - ▶ Verify users with specific (high) application authority
- Best Solution Available?:
 - ▶ Costly daily verification
 - ▶ Manual creation of queries and reports
 - ▶ Difficulty in baselining versus current state

zSecure Solution

- zSecure Audit customized reporting
 - ▶ Baselines document the security implementation standards
 - Show parameters that are in conflict
 - Approved changes must be reflected in the baseline
 - Inappropriate changes will show up until they have been addressed



zSecure Audit: Statistics for the Compliance Manager

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 incompilant 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/incompilant 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'

zSecure Audit: Details for the Technical Specialist

```

Session B - [32 x 80]
Menu Utilities Compilers Help

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 *****

Command ==>
Scroll ==> CSR
MA b 32/015
    
```

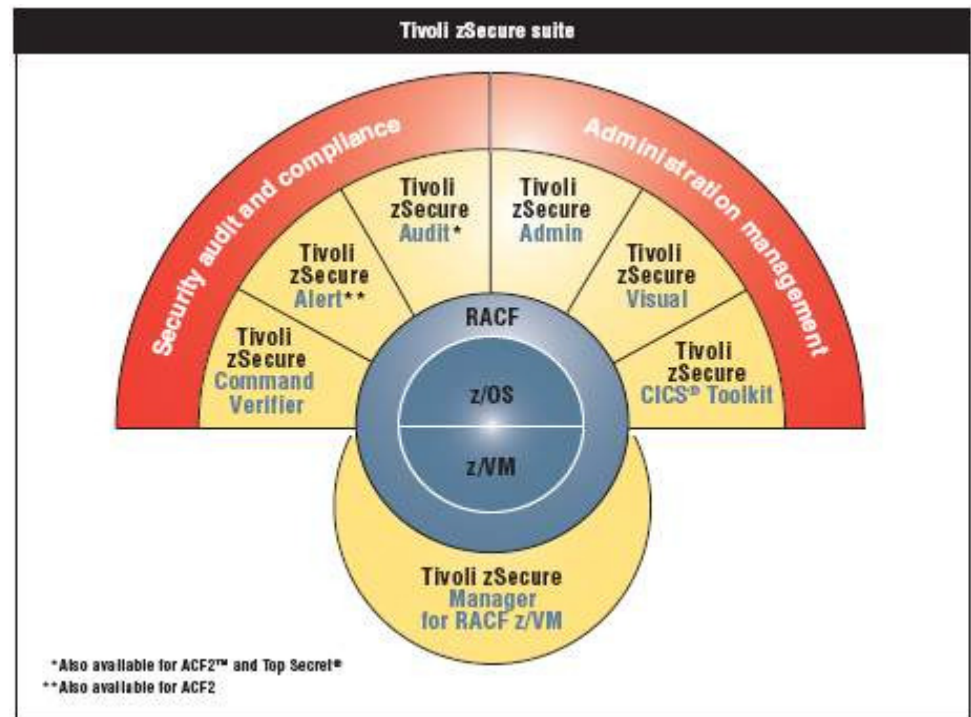

SOX report automation

- Solution: automated reporting for >25 LPARs
 - ▶ Exceptions summarized in an email
 - ▶ Detail reports available for review and archiving
 - ▶ Daily verification and maintenance < 0.5 FTE



Summary and Final Thoughts

- IBM Tivoli zSecure Suite – The Next Generation of RACF Security
- Regulation Challenges and Reality
 - ▶ The ever present auditor and privileged users
- The Tivoli zSecure Suite – Providing Futuristic RACF Security Today
 - ▶ Administration management
 - ▶ Security audit and compliance
 - ▶ Real-time alert
- Also for RACF on z/VM, CA ACF2 and CA Top Secret



Thank You for Joining Us today!

Go to www.ibm.com/software/systemz to:

- ▶ Replay this teleconference
- ▶ Replay previously broadcast teleconferences
- ▶ Register for upcoming events

