Session 04

Introducing
The IBM Tivoli zSecure Suite

Prepared by Patrick Kappeler
IBM Consulting IT Specialist
kappeler@fr.ibm.com

Redbooks
International Technical Support Organization

z Security Update

Trademarks

See url http://www.ibm.com/legal/copytrade.shtml for a list of trademarks

The following are trademarks or registered trademarks of other companies.

Java and all Java-related trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows and Windows NT are registered trademarks of Microsoft Corporation.

UNIX is a registered trademark of The Open Group in the United States and other countries.

SET and Secure Electronic Transaction are trademarks owned by SET Secure Electronic Transaction LLC.

* All other products may be trademarks or registered trademarks of their respective companies.

Notes:

Performance is in Internal Throughput Rate (ITR) ratio based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput improvements equivalent to the performance ratios stated here.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

All customer examples cited or described in this presentation are presented as illustrations of the manner in which some customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics will vary depending on individual customer configurations and conditions.

This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Prices subject to change without notice. Contact your IBM representative or Business Partner for the most current pricing in your geography.

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

Agenda

- zSecure Admin
- zSecure Visual
- zSecure CICS Toolkit
- zSecure Audit
- zSecure Alert
- zSecure Comand Verifier
- Tivoli Compliance Insight Manager (TCIM)

Consul – A Part Of IBM Tivoli

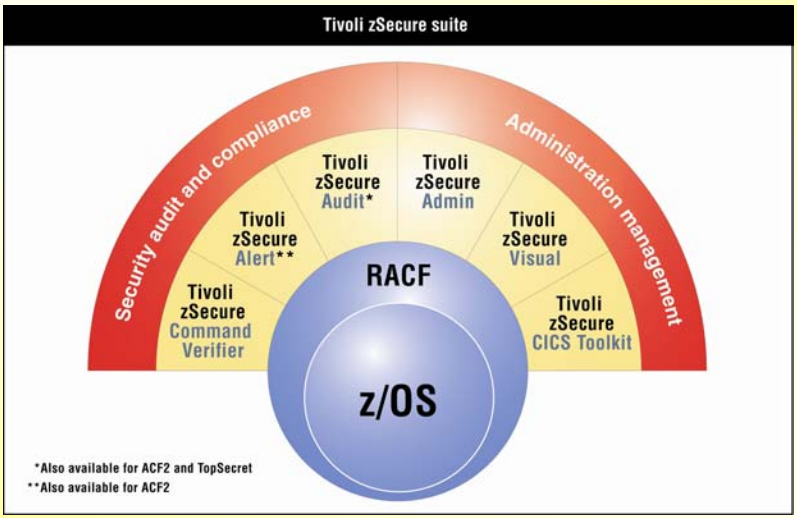
consul

- Founded in 1986
- Privately held software company
- 89 employees in US and Europe
- Over 350 customers worldwide
- Patent pending W7 compliance methodology
- Parent company in Delft, Netherlands; US subsidiary in Herndon, VA

- *Acquisition has closed effective January 22, 2007*
- *Consul executive team integrated into IBM Tivoli leadership*
- *Consul development and service team retained and expanded*
- *Consul solutions (Consul InSight and zSecure) are shipping as Tivoli products*

Introducing The IBM Tivoli zSecure Suite

On July 3, 2007, IBM announced:


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

*Also available for ACF2 and TopSecret

**Also available for ACF2

Additions we needed:

– Add-on security tools for automating admin and audit

– Enterprise-wide identity and access management

– Monitor, audit and compliance tools with enterprise view

New: ITSO redp4355

Enterprise Security Monitoring and Audit Reporting

A cornerstone for Tivoli's z/OS Security strategy

Enterprise Identity and Access Management

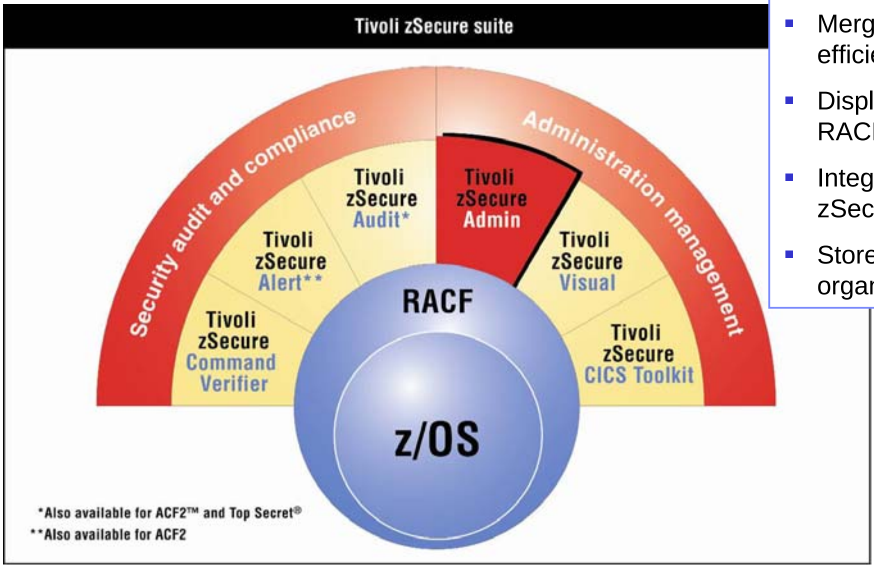
Tivoli Compliance Insight Manager (TCIM)	**Tivoli Security Operations Manager (TSOM)**	**Tivoli Identity Manager (TIM) for z/OS**	**Tivoli Federated Identity Manager for z/OS**	**Tivoli Directory Server for z/OS**	**Tivoli Directory Integrator (TDI) for z/OS**

IBM Tivoli zSecure Admin

Enables more efficient and effective RACF administration, using significantly less resources

Highlights:

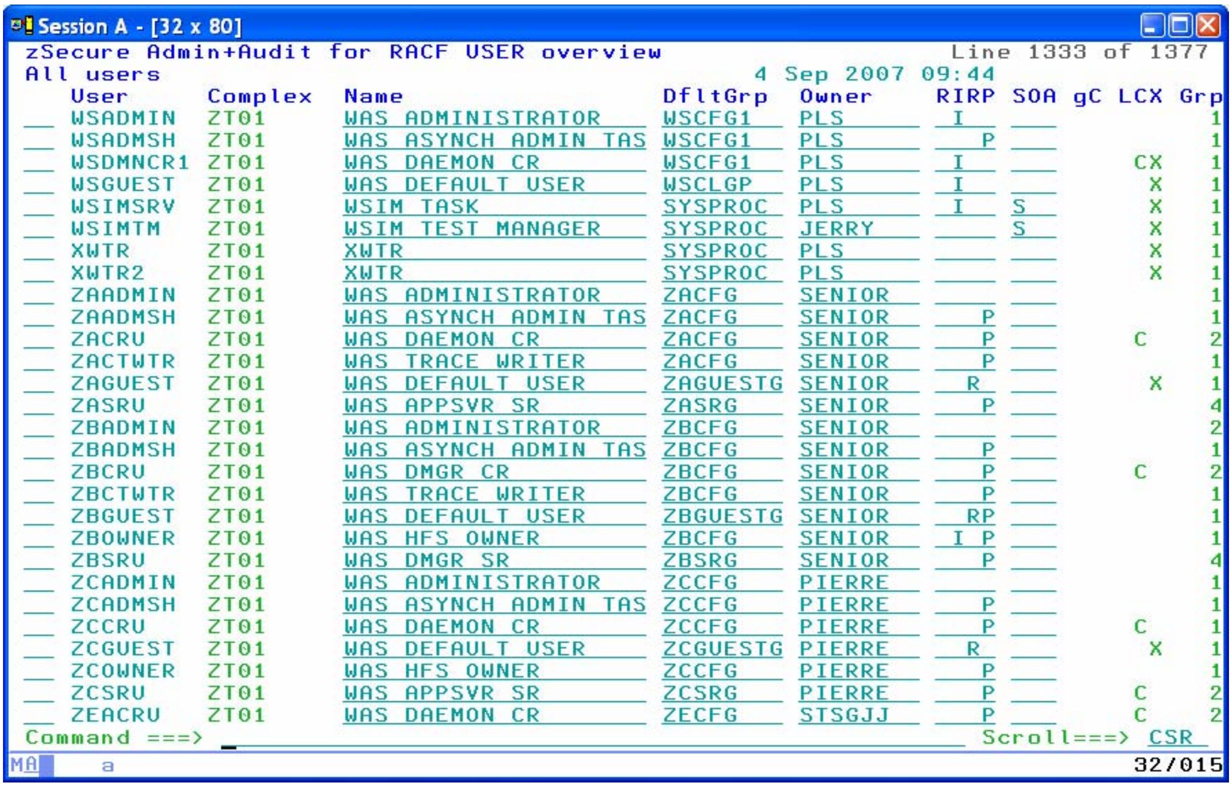
- Automate routine tasks to simplify administration
- Identify and analyze problems to minimize threats
- Merge databases quickly and efficiently
- Display data from the active (live) RACF database
- Integrates smoothly with IBM Tivoli zSecure Audit
- Store non-RACF data to reduce organizational costs


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

*Also available for ACF2™ and Top Secret®

**Also available for ACF2

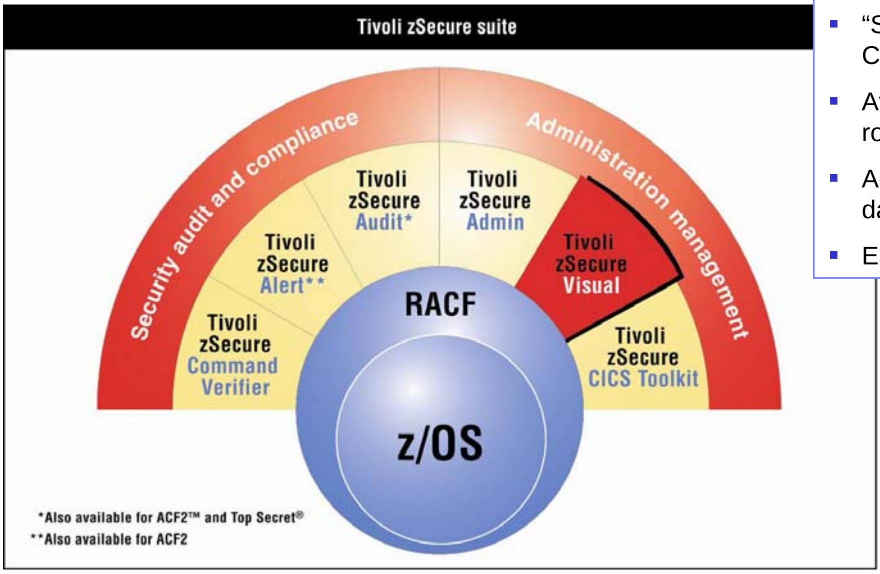
IBM Tivoli zSecure Admin



```
zSecure Admin+Audit for RACF USER overview                     Line 1333 of 1377
All users                                       4 Sep 2007 09:44
   User     Complex  Name                 DfltGrp  Owner    RIRP SOA gC LCX Grp
__ WSADMIN  ZT01     WAS ADMINISTRATOR    WSCFG1   PLS       I                 1
__ WSADMSH  ZT01     WAS ASYNCH ADMIN TAS WSCFG1   PLS         P               1
__ WSDMNCR1 ZT01     WAS DAEMON CR        WSCFG1   PLS       I           CX    1
__ WSGUEST  ZT01     WAS DEFAULT USER     WSCLGP   PLS       I            X    1
__ WSIMSRV  ZT01     WSIM TASK            SYSPROC  PLS       I   S        X    1
__ WSIMTM   ZT01     WSIM TEST MANAGER    SYSPROC  JERRY         S        X    1
__ XWTR     ZT01     XWTR                 SYSPROC  PLS                    X    1
__ XWTR2    ZT01     XWTR                 SYSPROC  PLS                    X    1
__ ZAADMIN  ZT01     WAS ADMINISTRATOR    ZACFG    SENIOR                      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                      2
__ ZBADMSH  ZT01     WAS ASYNCH ADMIN TAS ZBCFG    SENIOR      P               1
__ ZBCRU    ZT01     WAS DMGR CR          ZBCFG    SENIOR      P         C     2
__ ZBCTWTR  ZT01     WAS TRACE WRITER     ZBCFG    SENIOR      P               1
__ ZBGUEST  ZT01     WAS DEFAULT USER     ZBGUESTG SENIOR     RP               1
__ ZBOWNER  ZT01     WAS HFS OWNER        ZBCFG    SENIOR    I P               1
__ ZBSRU    ZT01     WAS DMGR SR          ZBSRG    SENIOR      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      P               1
__ ZCSRU    ZT01     WAS APPSVR SR        ZCSRG    PIERRE      P         C     2
__ ZEACRU   ZT01     WAS DAEMON CR        ZECFG    STSGJJ      P         C     2
Command ===> _                                                 Scroll===> CSR
MA      a                                                                 32/015
```

IBM Tivoli zSecure Visual

Reduces the need for scarce, RACF-trained expertise through a Microsoft Windows–based GUI for RACF administration



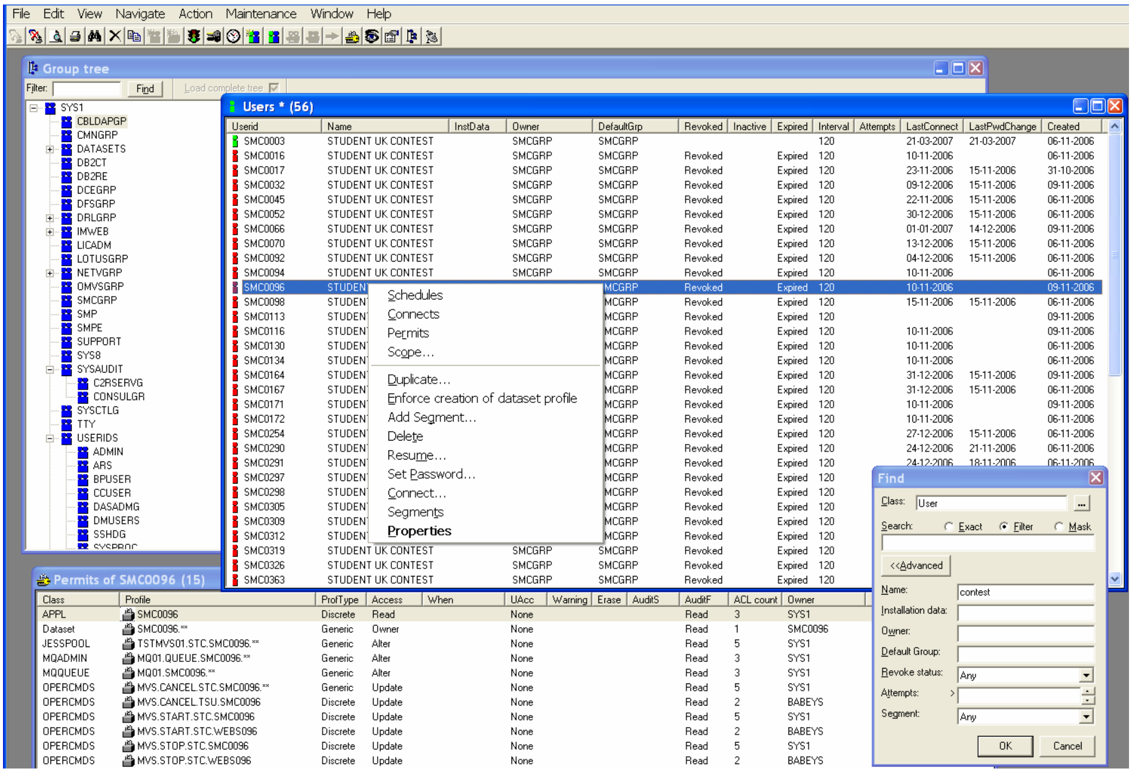
Tivoli zSecure suite
Security audit and compliance
Administration management
Tivoli zSecure Audit*
Tivoli zSecure Admin
Tivoli zSecure Alert**
Tivoli zSecure Visual
Tivoli zSecure Command Verifier
Tivoli zSecure CICS Toolkit
RACF
z/OS

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

Highlights:

- Decentralize RACF administration to optimize resources
- “Scope Down” Administrative Capabilities
- Avoid need for TSO/ISPF rollouts
- Administer from a live RACF database
- Easy Cloning of user templates

IBM Tivoli zSecure Visual



SYS1
CBLDAPGP
CMNGRP
DATASETS
DB2CT
DB2RE
DCEGRP
DFSGRP
DRLGRP
IMWEB
LICADM
LOTUSGRP
NETVGRP
OMVSGRP
SMCGRP
SMP
SMPE
SUPPORT
SYS8
SYSAUDIT
C2RSERVG
CONSULGR
SYSCTLG
TTY
USERIDS
ADMIN
ARS
BPUSER
CCUSER
DASADMG
DMUSERS
SSHDG
SYSPROC

Users * (56)

Userid	Name	InstData	Owner	DefaultGrp	Revoked	Inactive	Expired	Interval	Attempts	LastConnect	LastPwdChange	Created
SMC0003	STUDENT UK CONTEST		SMCGRP	SMCGRP				120		21-03-2007	21-03-2007	06-11-2006
SMC0016	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		10-11-2006		06-11-2006
SMC0017	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		23-11-2006	15-11-2006	31-10-2006
SMC0032	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		09-12-2006	15-11-2006	09-11-2006
SMC0045	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		22-11-2006	15-11-2006	06-11-2006
SMC0052	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		30-12-2006	15-11-2006	06-11-2006
SMC0066	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		01-01-2007	14-12-2006	09-11-2006
SMC0070	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		13-12-2006	15-11-2006	06-11-2006
SMC0092	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		04-12-2006	15-11-2006	06-11-2006
SMC0094	STUDENT UK CONTEST		SMCGRP	SMCGRP	Revoked		Expired	120		10-11-2006		06-11-2006
SMC0096	STUDEN			MCGRP	Revoked		Expired	120		10-11-2006		09-11-2006
SMC0098	STUDEN			MCGRP	Revoked		Expired	120		15-11-2006	15-11-2006	06-11-2006
SMC0113	STUDEN			MCGRP	Revoked		Expired	120				09-11-2006
SMC0116	STUDEN			MCGRP	Revoked		Expired	120		10-11-2006		09-11-2006
SMC0130	STUDEN			MCGRP	Revoked		Expired	120		10-11-2006		06-11-2006
SMC0134	STUDEN			MCGRP	Revoked		Expired	120		10-11-2006		06-11-2006
SMC0164	STUDEN			MCGRP	Revoked		Expired	120		31-12-2006	15-11-2006	09-11-2006
SMC0167	STUDEN			MCGRP	Revoked		Expired	120		31-12-2006	15-11-2006	06-11-2006
SMC0171	STUDEN			MCGRP	Revoked		Expired	120		10-11-2006		09-11-2006
SMC0172	STUDEN			MCGRP	Revoked		Expired	120		10-11-2006		06-11-2006
SMC0254	STUDEN			MCGRP	Revoked		Expired	120		27-12-2006	15-11-2006	06-11-2006
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

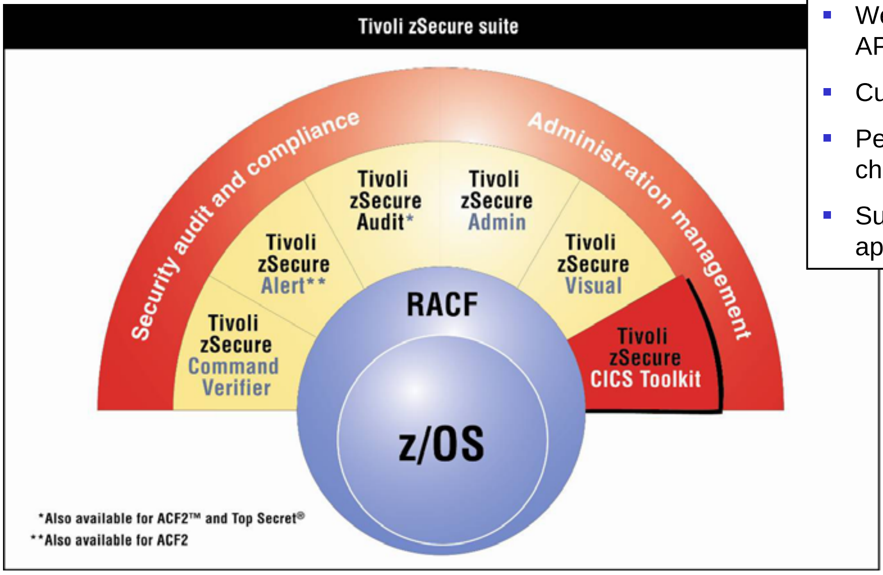
OK Cancel

IBM Tivoli zSecure CICS Toolkit

Allows you to perform mainframe administrative tasks from a CICS environment, freeing up native-RACF resources

Highlights:

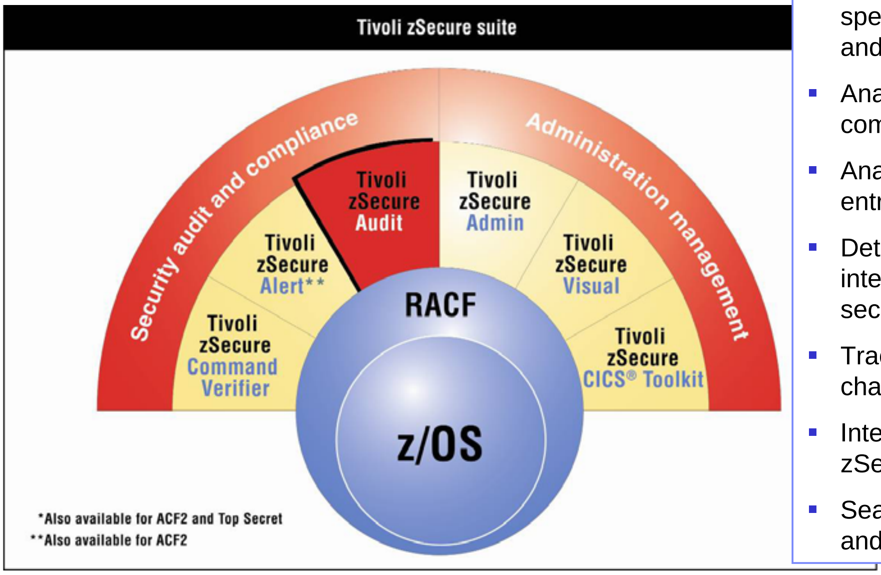
- RACF administration from a CICS interface
- Web-enablement CICS-RACF API
- Customize screens
- Perform resource access checks
- Support security of legacy applications


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

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

IBM Tivoli zSecure Audit

Compliance and audit solution that enables you to automatically analyze and report on security events and detect security exposures

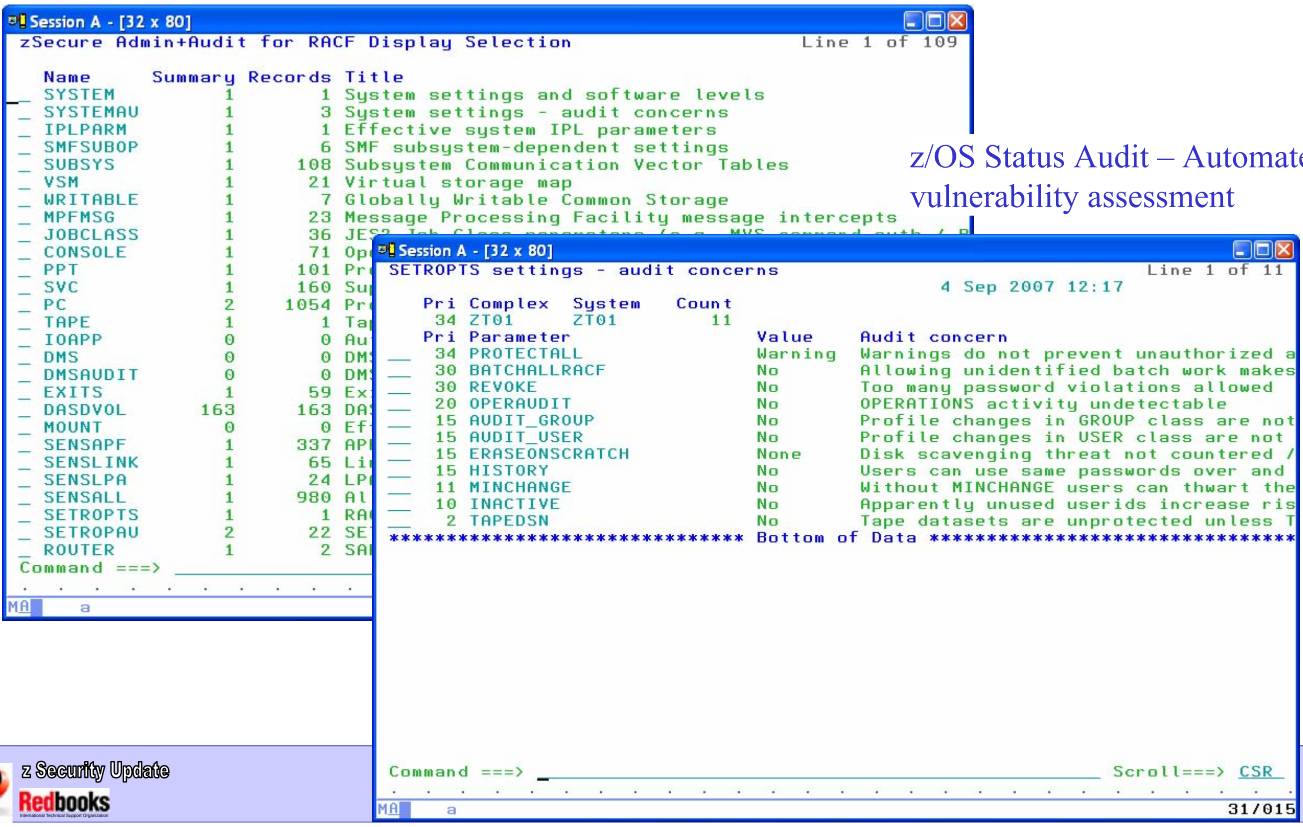

Tivoli zSecure suite
Security audit and compliance
Administration management
Tivoli zSecure Audit
Tivoli zSecure Admin
Tivoli zSecure Alert**
Tivoli zSecure Visual
Tivoli zSecure Command Verifier
Tivoli zSecure CICS® Toolkit
RACF
z/OS
*Also available for ACF2 and Top Secret
**Also available for ACF2

Highlights:

- Live analysis of critical information
- Beyond just z/OS and RACF analysis
- Customize reports to meet specific needs with flexible report and alert language
- Analyze SMF log files to create a comprehensive audit trail
- Analyze RACF profiles and ACF2 entries to get fast answers
- Detect system changes and integrity breaches to minimize security risks
- Track and monitor baseline changes for RACF and ACF2
- Integrated remediation with Tivoli zSecure Admin
- Seamless links to enterprise audit and compliance

IBM Tivoli zSecure Audit

z/OS Status Audit – Detailed reports



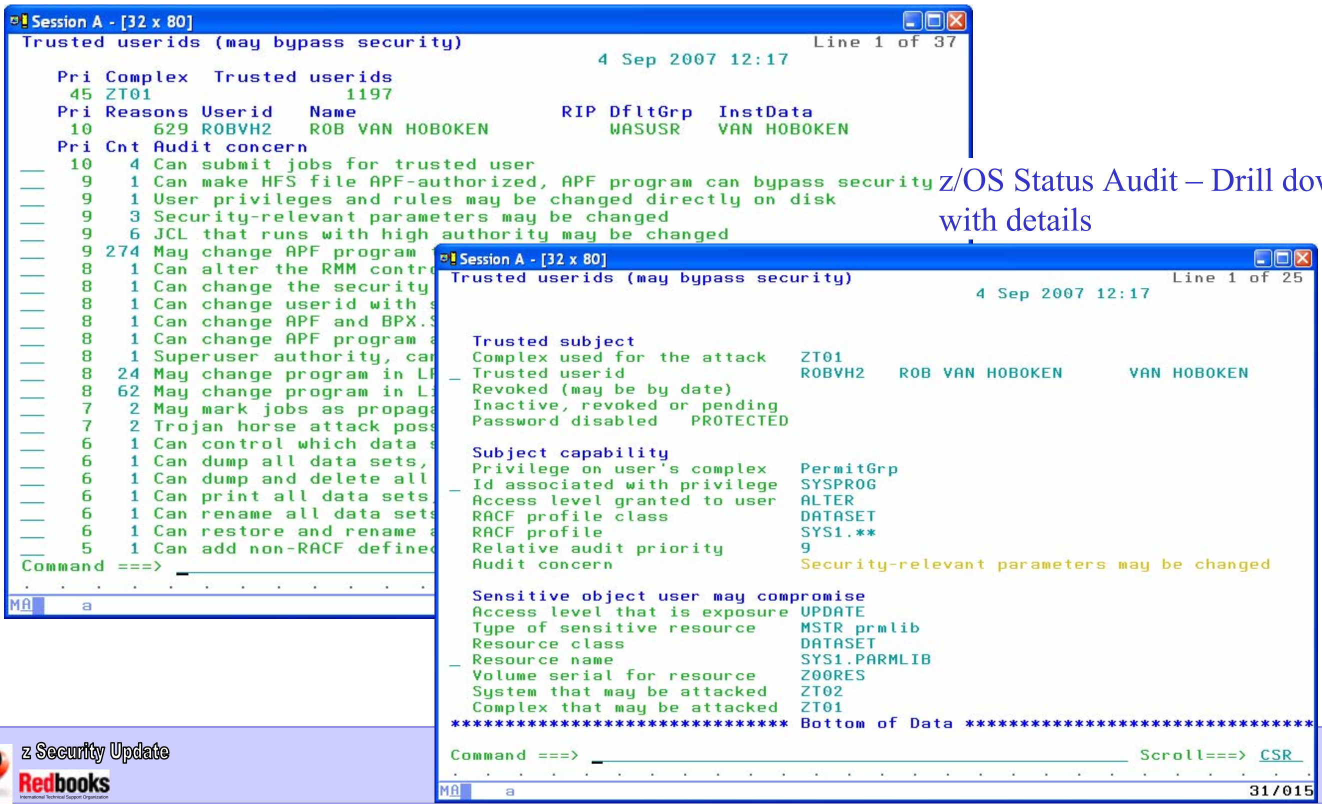
```
zSecure Admin+Audit for RACF Display Selection                  Line 1 of 109

   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 / R
_  CONSOLE         1      71 Op
_  PPT             1     101 Pr
_  SVC             1     160 Su
_  PC              2    1054 Pr
_  TAPE            1       1 Ta
_  IOAPP           0       0 Au
_  DMS             0       0 DM
_  DMSAUDIT        0       0 DM
_  EXITS           1      59 Ex
_  DASDVOL       163     163 DA
_  MOUNT           0       0 Ef
_  SENSAPF         1     337 AP
_  SENSLINK        1      65 Li
_  SENSLPA         1      24 LP
_  SENSALL         1     980 Al
_  SETROPTS        1       1 RA
_  SETROPAU        2      22 SE
_  ROUTER          1       2 SA
Command ===> ____________
MA     a
```

z/OS Status Audit – Automated vulnerability assessment

```
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
```

IBM Tivoli zSecure Audit

z/OS Status Audit – Trusted userID report



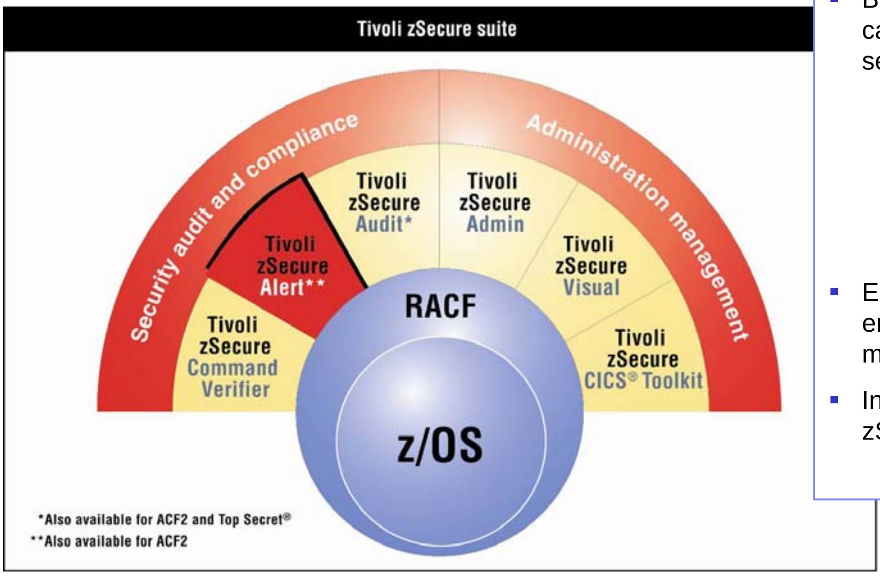
```
Session A - [32 x 80]
Trusted userids (may bypass security)                              Line 1 of 37
                                                        4 Sep 2007 12:17
   Pri Complex  Trusted userids
    45 ZT01                1197
   Pri Reasons Userid    Name                       RIP DfltGrp  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
__   8   1 Can alter the RMM contr
__   8   1 Can change the security
__   8   1 Can change userid with s
__   8   1 Can change APF and BPX.S
__   8   1 Can change APF program a
__   8   1 Superuser authority, can
__   8  24 May change program in LP
__   8  62 May change program in Li
__   7   2 May mark jobs as propaga
__   7   2 Trojan horse attack poss
__   6   1 Can control which data s
__   6   1 Can dump all data sets,
__   6   1 Can dump and delete all
__   6   1 Can print all data sets,
__   6   1 Can rename all data sets
__   6   1 Can restore and rename a
__   5   1 Can add non-RACF defined
Command ===> _
MA     a
```

z/OS Status Audit – Drill down with details

```
Session A - [32 x 80]
Trusted userids (may bypass security)                              Line 1 of 25
                                                        4 Sep 2007 12:17


   Trusted subject
   Complex used for the attack    ZT01
 _ Trusted userid                 ROBVH2    ROB VAN HOBOKEN        VAN HOBOKEN
   Revoked (may be by date)
   Inactive, revoked or pending
   Password disabled   PROTECTED

   Subject capability
   Privilege on user's complex    PermitGrp
 _ Id associated with privilege   SYSPROG
   Access level granted to user   ALTER
   RACF profile class             DATASET
   RACF profile                   SYS1.**
   Relative audit priority        9
   Audit concern                  Security-relevant parameters may be changed

   Sensitive object user may compromise
   Access level that is exposure  UPDATE
   Type of sensitive resource     MSTR prmlib
   Resource class                 DATASET
 _ Resource name                  SYS1.PARMLIB
   Volume serial for resource     Z00RES
   System that may be attacked    ZT02
   Complex that may be attacked   ZT01
****************************** Bottom of Data ******************************

Command ===> _                                                  Scroll===> CSR
MA     a                                                                 31/015
```

IBM Tivoli zSecure Alert

Real-time mainframe threat monitoring allowing you to monitor intruders and identify mis-configurations that could hamper your compliance efforts


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

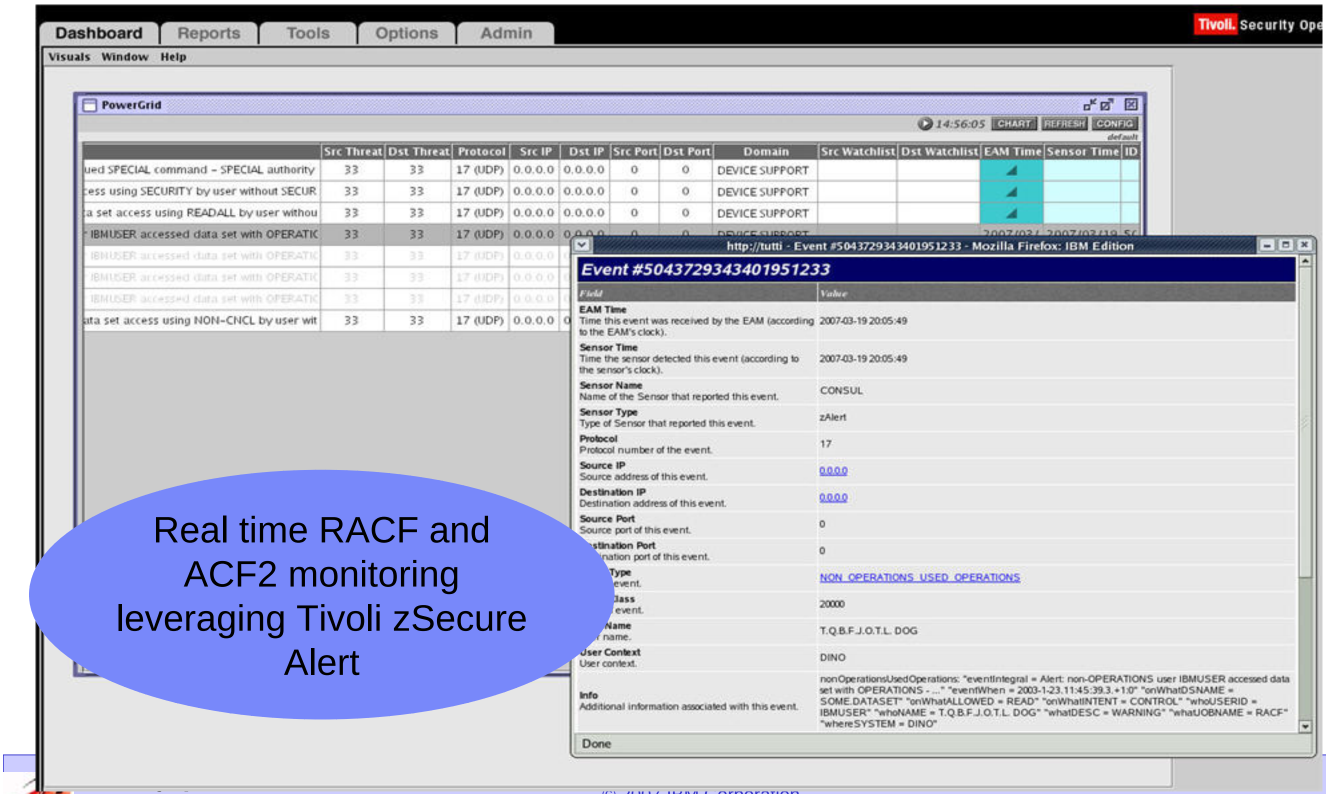
*Also available for ACF2 and Top Secret®
**Also available for ACF2

Highlights:

- Threat knowledge base with parameters from your active configurations
- Broad range of monitoring capabilities, including monitoring sensitive data for misuse on:
  - z/OS
  - IBM RACF
  - CA ACF2 and
  - z/OS UNIX subsystems.
- Easily send critical alerts to enterprise audit, compliance and monitoring solutions
- Integrated remediation with Tivoli zSecure Admin

IBM Tivoli zSecure Alert

Integration with Tivoli Security Operations Manager



	Src Threat	Dst Threat	Protocol	Src IP	Dst IP	Src Port	Dst Port	Domain	Src Watchlist	Dst Watchlist	EAM Time	Sensor Time	ID
ued SPECIAL command – SPECIAL authority	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT					
:ess using SECURITY by user without SECUR	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT					
:a set access using READALL by user withou	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT					
: IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0	0.0.0.0	0	0	DEVICE SUPPORT			2007/03/	2007/03/19	5C
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0									
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0									
IBMUSER accessed data set with OPERATIC	33	33	17 (UDP)	0.0.0.0									
ata set access using NON-CNCL by user wit	33	33	17 (UDP)	0.0.0.0	0								

http://tutti - Event #5043729343401951233 - Mozilla Firefox: IBM Edition

Event #5043729343401951233

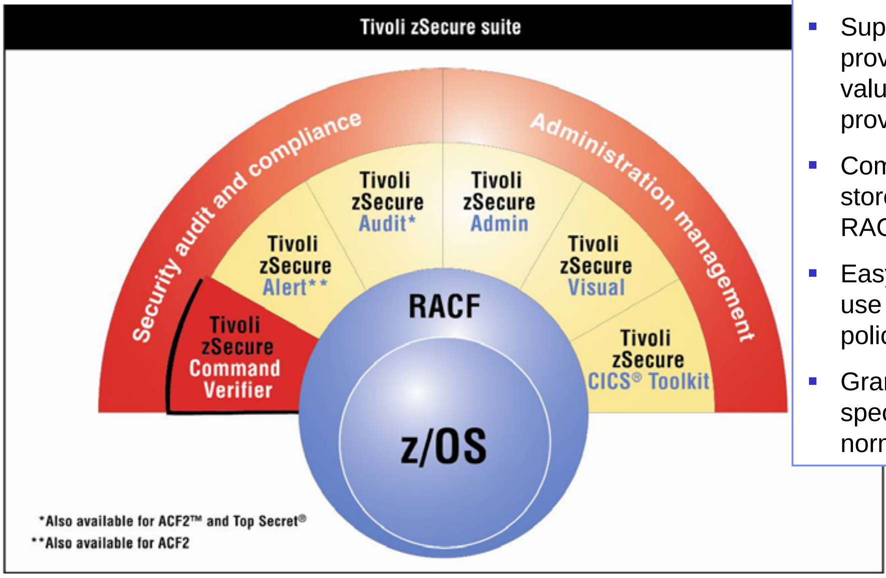
Field	Value
EAM Time Time this event was received by the EAM (according to the EAM's clock).	2007-03-19 20:05:49
Sensor Time Time the sensor detected this event (according to the sensor's clock).	2007-03-19 20:05:49
Sensor Name Name of the Sensor that reported this event.	CONSUL
Sensor Type Type of Sensor 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
stination Port ination port of this event.	0
Type event.	NON_OPERATIONS_USED_OPERATIONS
lass event.	20000
Name r 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"

Done

Real time RACF and ACF2 monitoring leveraging Tivoli zSecure Alert

IBM Tivoli zSecure Command Verifier

Policy enforcement solution that enforces compliance to company and regulatory policies by preventing erroneous commands


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

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

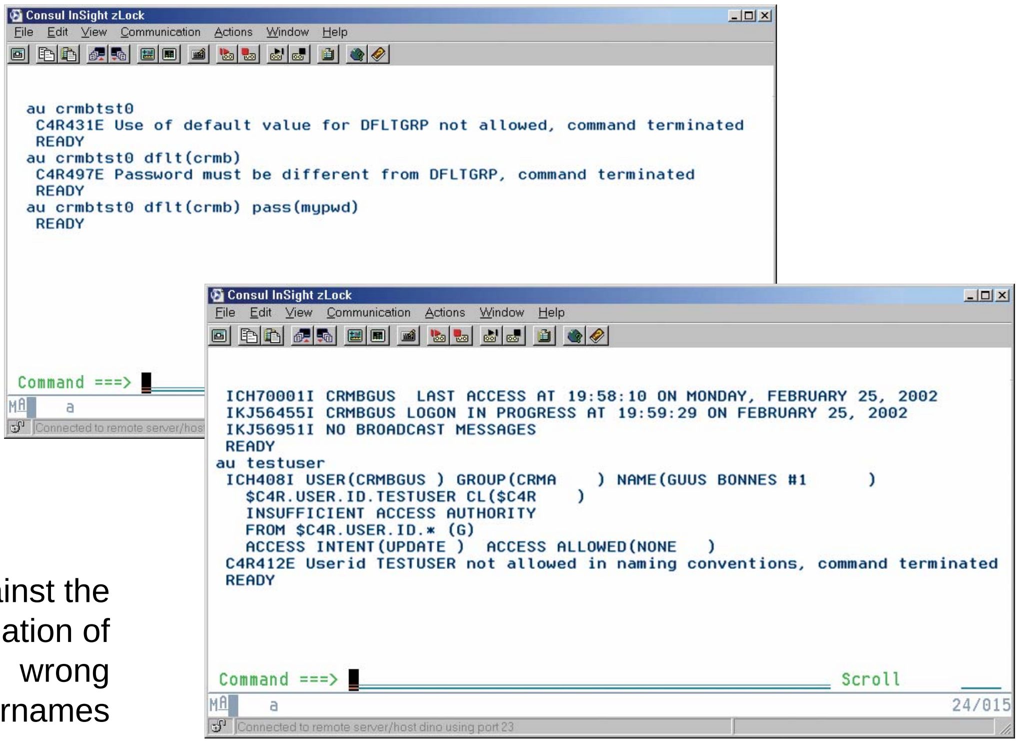
Highlights:

- Prevent noncompliant administrative command execution
- Supports policy definitions to provide mandatory and default values for which RACF does not provide appropriate defaults
- Command Audit Trail feature stores changes to profiles in the RACF database
- Easy independent installation for use on all systems for which policies must be enforced
- Grant users granular access to specific commands they would normally be unable to access

IBM Tivoli zSecure Command Verifier

…Against the creation of default passwords

…Against the creation of wrong usernames



Consul InSight zLock
File Edit View Communication Actions Window Help

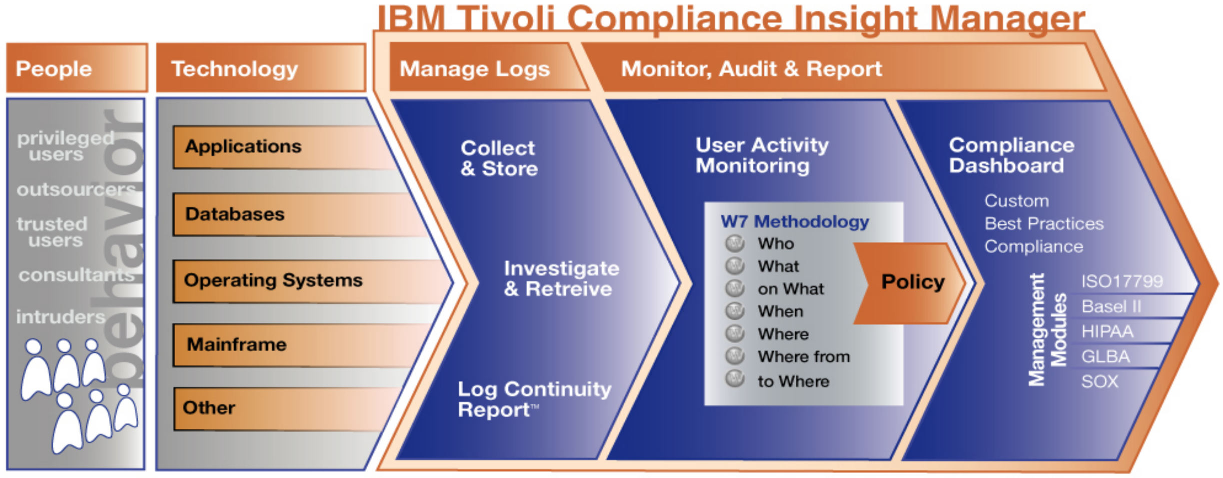
```
au crmbtst0
 C4R431E Use of default value for DFLTGRP not allowed, command terminated
 READY
au crmbtst0 dflt(crmb)
 C4R497E Password must be different from DFLTGRP, command terminated
 READY
au crmbtst0 dflt(crmb) pass(mypwd)
 READY

Command ===>
MA    a
Connected to remote server/hos
```

Consul InSight zLock
File Edit View Communication Actions Window Help

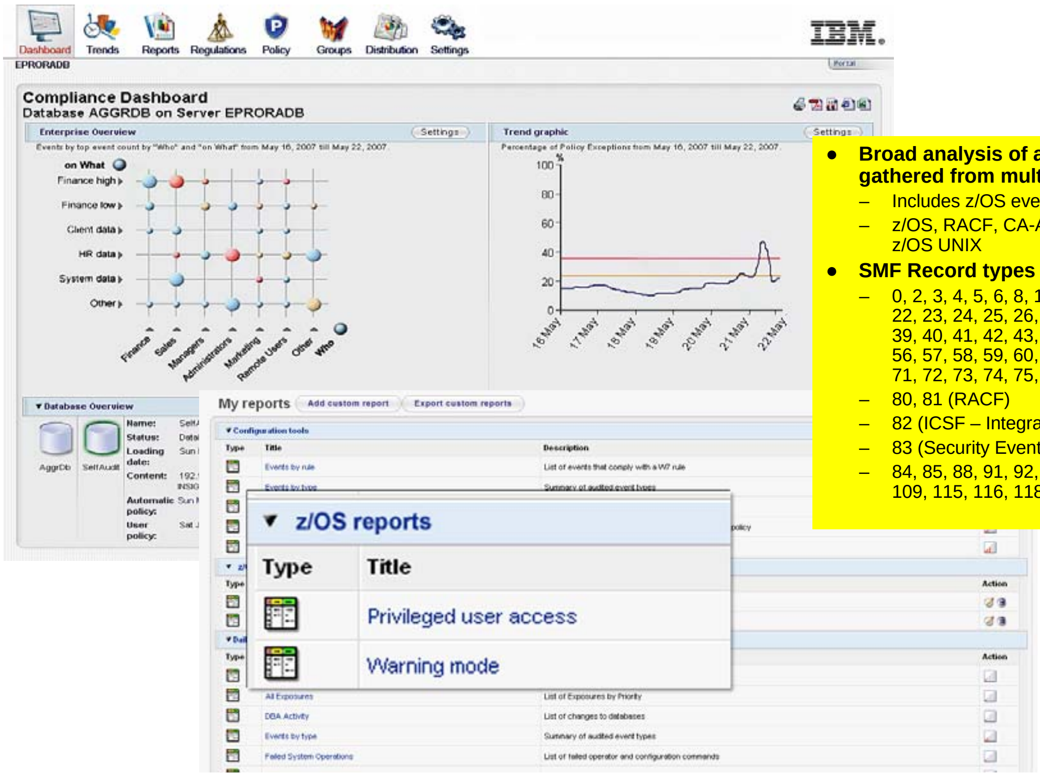
```
 ICH70001I CRMBGUS  LAST ACCESS AT 19:58:10 ON MONDAY, FEBRUARY 25, 2002
 IKJ56455I CRMBGUS LOGON IN PROGRESS AT 19:59:29 ON FEBRUARY 25, 2002
 IKJ56951I NO BROADCAST MESSAGES
 READY
au testuser
 ICH408I USER(CRMBGUS ) GROUP(CRMA    ) NAME(GUUS BONNES #1      )
   $C4R.USER.ID.TESTUSER CL($C4R    )
   INSUFFICIENT ACCESS AUTHORITY
   FROM $C4R.USER.ID.* (G)
   ACCESS INTENT(UPDATE )  ACCESS ALLOWED(NONE   )
 C4R412E Userid TESTUSER not allowed in naming conventions, command terminated
 READY

Command ===>                                                  Scroll
MA    a                                                       24/015
Connected to remote server/host dino using port 23
```

IBM Tivoli Compliance Insight Manager (TCIM)

- Integrate the Mainframe with TCIM Enterprise Compliance Dashboard
- W7 Patent Pending Analysis Engine
- PUMA (Privileged User Monitoring and Audit)



IBM Tivoli Compliance Insight Manager (TCIM)



EPRORADB

Compliance Dashboard
Database AGGRDB on Server EPRORADB

Enterprise Overview

Events by top event count by "Who" and "on What" from May 16, 2007 till May 22, 2007.

Percentage of Policy Exceptions from May 16, 2007 till May 22, 2007.

▾ Database Overview

AggrDb SelfAudit

Name: SelfA
Status: Data
Loading date: Sun
Content: 192. INSIG
Automatic policy: Sun
User policy: Sat

▾ Configuration tools

Type	Title	Description
	Events by rule	List of events that comply with a W7 rule
	Events by type	Summary of audited event types

▾ z/OS reports

Type	Title
	Privileged user access
	Warning mode

Type	Title	Description
	All Exposures	List of Exposures by Priority
	DBA Activity	List of changes to databases
	Events by type	Summary of audited event types
	Failed System Operations	List of failed operator and configuration commands

- **Broad analysis of activity and audit records gathered from multiple platforms**
  - Includes z/OS events in the enterprise dashboard!
  - z/OS, RACF, CA-ACF2, CA-Top Secret, DB2, TCPIP, z/OS UNIX
- **SMF Record types (mainframe logs) gathered**
  - 0, 2, 3, 4, 5, 6, 8, 10, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 28, 30, 31, 32, 33, 34, 35, 36, 27, 39, 40, 41, 42, 43, 45, 47, 48, 49, 50, 52, 53, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79
  - 80, 81 (RACF)
  - 82 (ICSF – Integrated Cryptographic Services Facility)
  - 83 (Security Events)
  - 84, 85, 88, 91, 92, 94, 96, 99, 100, 101, 103, 108, 109, 115, 116, 118, 119, 120

Thank You

Any Questions ?