



Tivoli



Session 11

Systeme Z

La Gestion Globale de la Sécurité au niveau du Système d'Information, de bout en bout

François Lèbe
Michael Cable

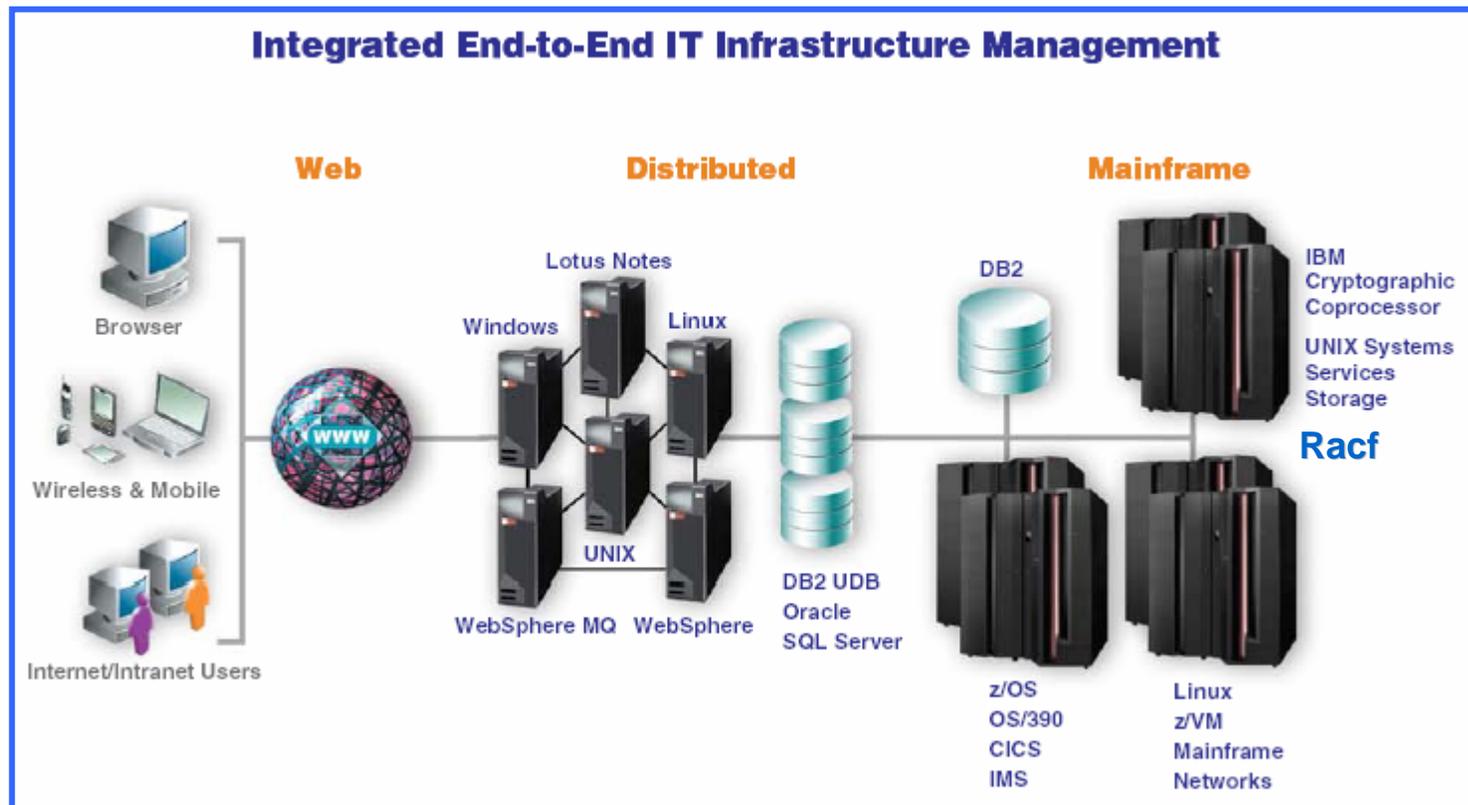
francois.lebe@fr.ibm.com
michael.cable@be.ibm.com

1^{er} et 2 octobre 2007

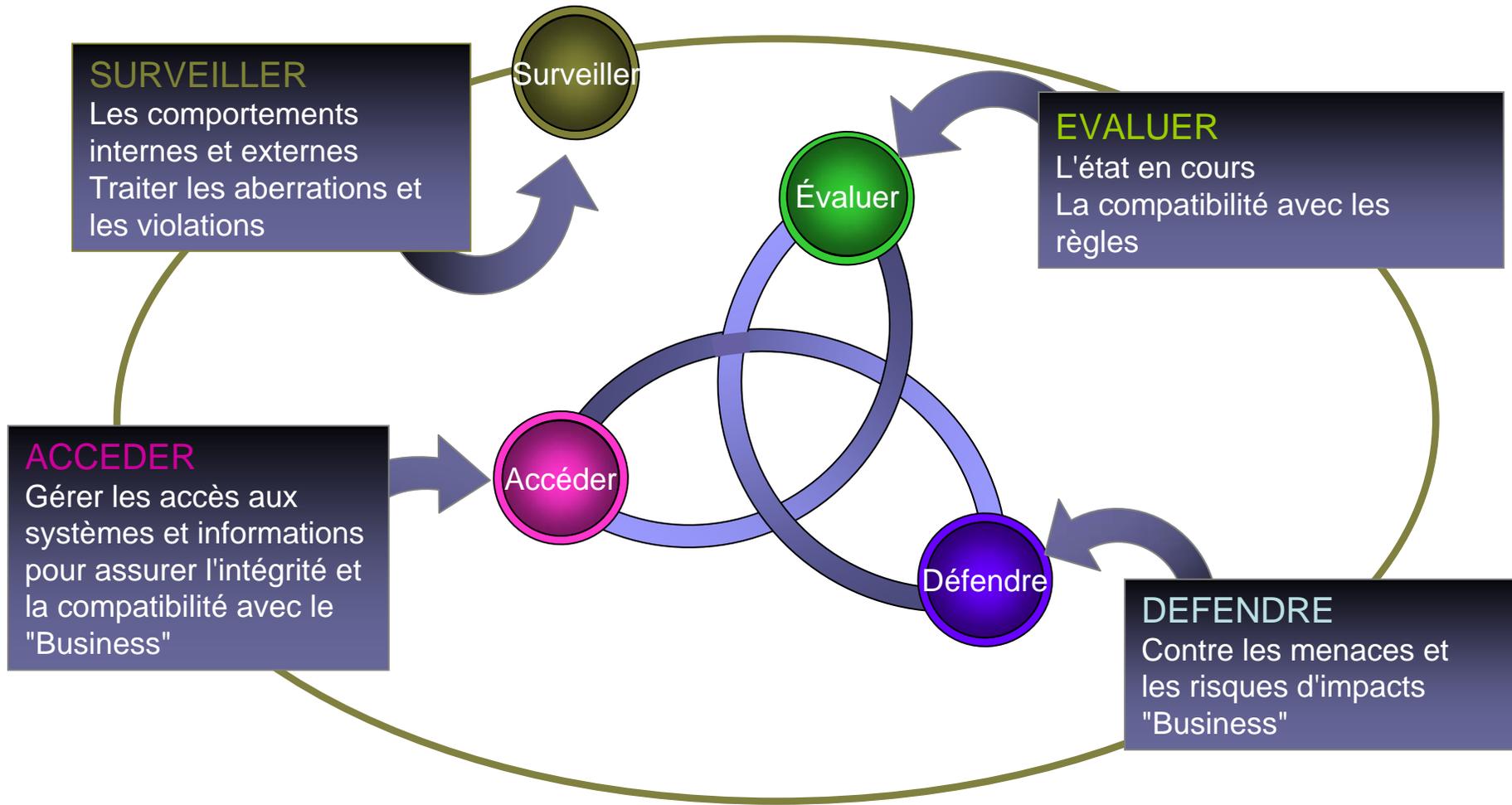


Sécurité du Système d'Information : De bout en bout

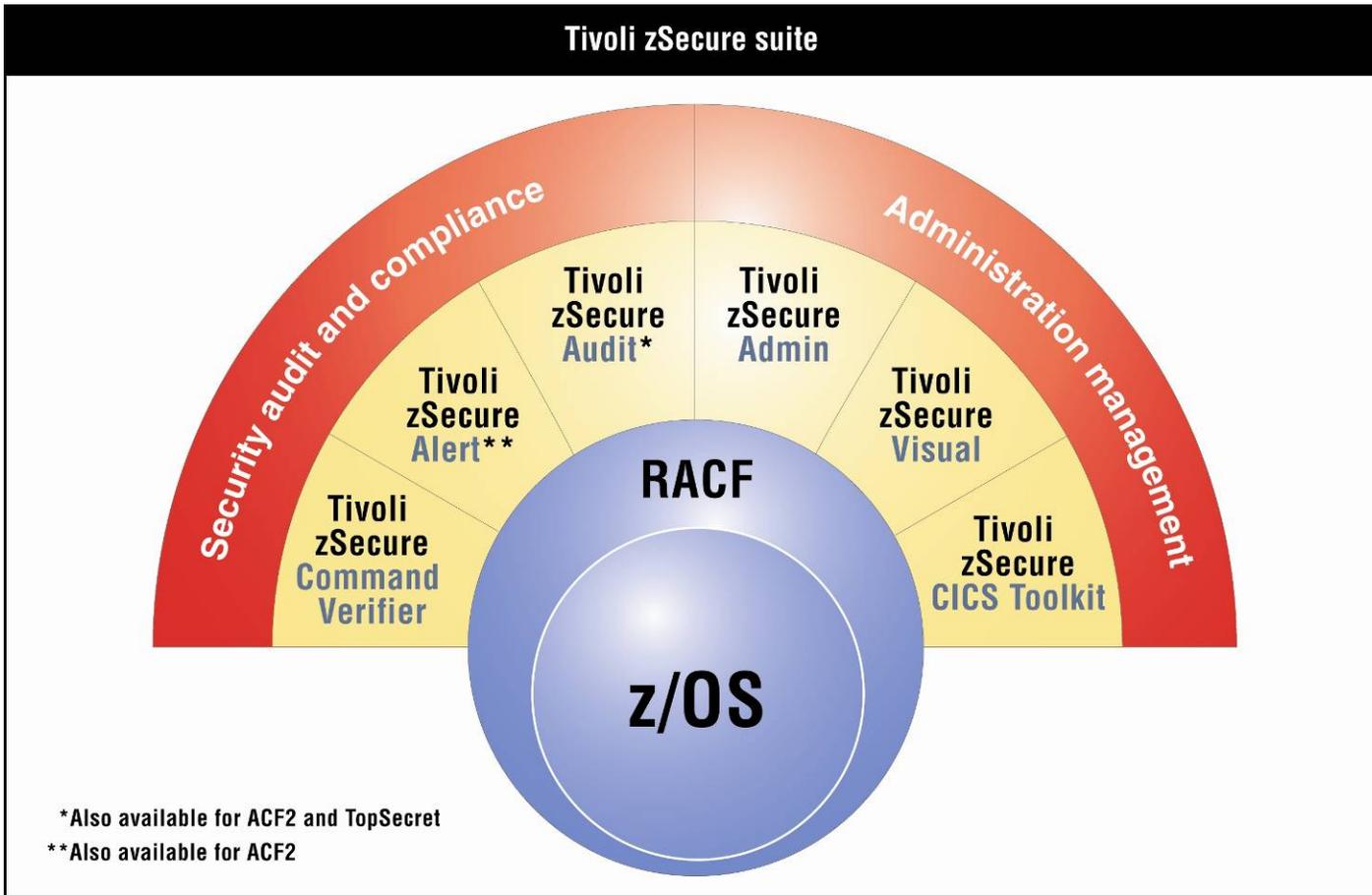
- Gérer les accès externes aux Systèmes & Applications z/OS
- Garantir les privilèges de bout en bout
- Administrer RACF et les Systèmes dans ce contexte
- Autoriser le "Business"



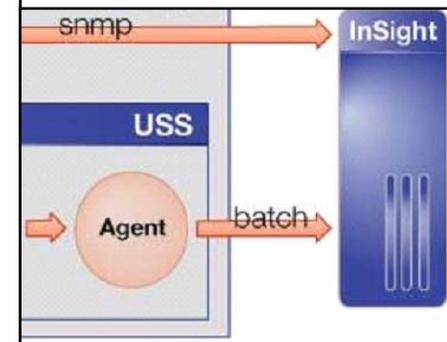
La vision et la stratégie IBM concernant la sécurité



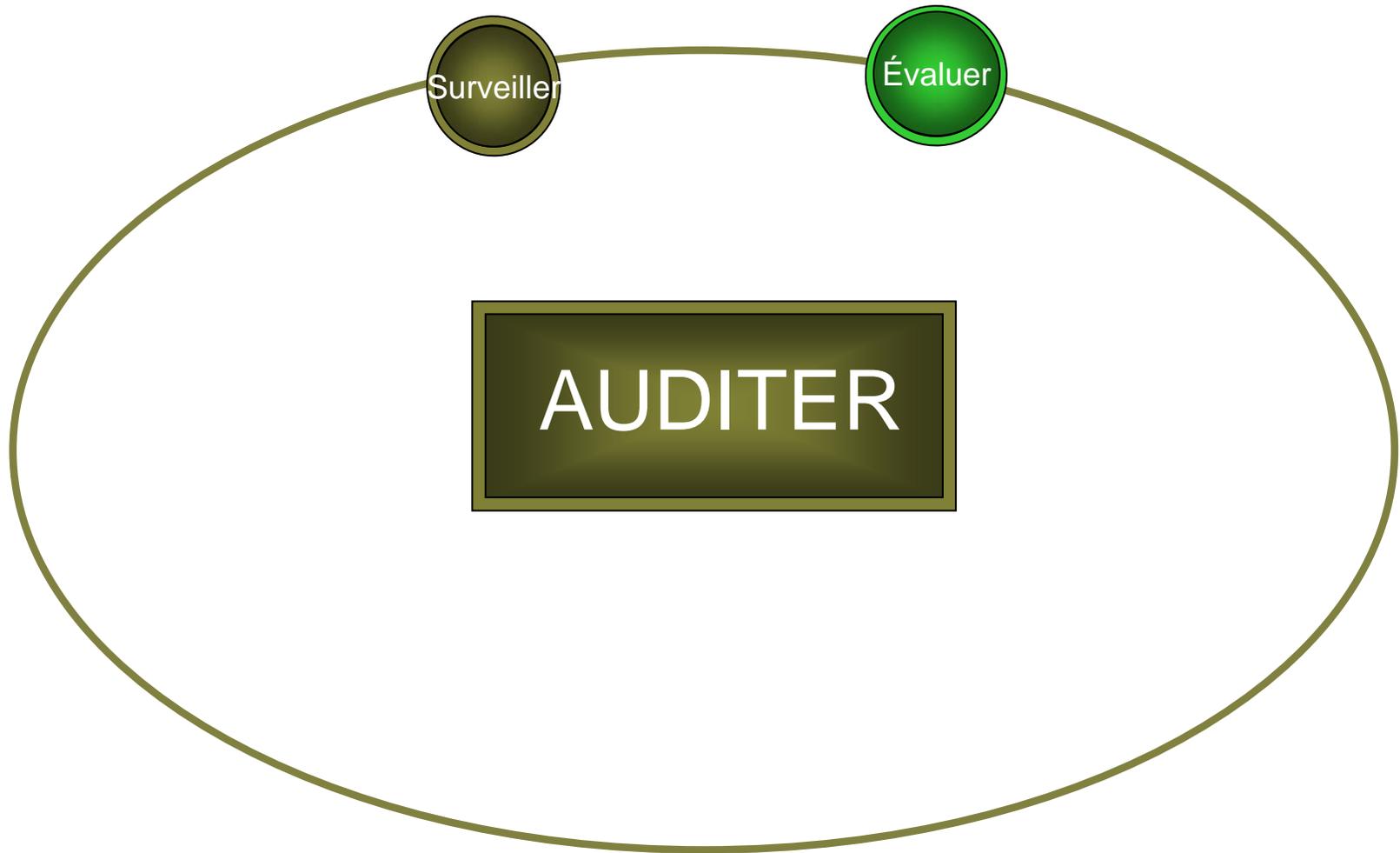
L'application de la stratégie sur z/OS : la Suite zSecure



- SURVEILLER
- DEFENDRE
- ACCEDER
- EVALUER
- De bout en bout

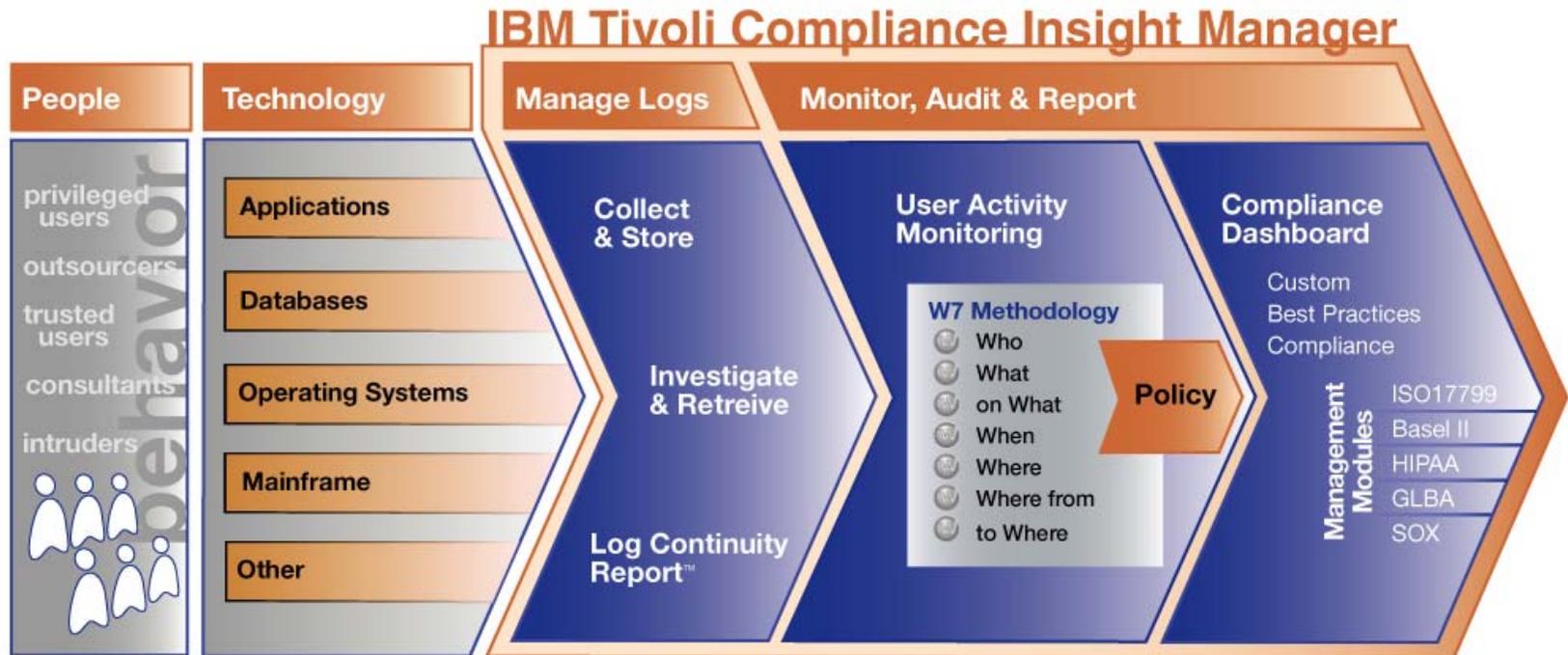


Audit de conformité & Audit des événements (connaître pour défendre & agir)



Audit global : Tivoli zSecure Compliance Insight Manager

- Globalise le suivi de la conformité (rapports z/OS)
- Intègre le Mainframe dans le tableau de bord de TCIM (Enterprise Compliance Dashboard)
- Analyse par la méthodologie dite des "W7" (Patent Pending Analysis Engine)
- Contrôle la présence des informations (logs)
- Prend en charge z/OS (Système), RACF (Database), DB2, TCPIP, USS ... (enregistrements SMF)



Audit global : Tivoli zSecure Compliance Insight Manager

Dashboard
 Trends
 Reports
 Regulations
 Policy
 Groups
 Distribution
 Settings

EPRORADB
Portal

Compliance Dashboard

Database AGGRDB on Server EPRORADB

Enterprise Overview Settings

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

on What

Finance high	●	●	●	●	●	●	●	●	●
Finance low	●	●	●	●	●	●	●	●	●
Client data	●	●	●	●	●	●	●	●	●
HR data	●	●	●	●	●	●	●	●	●
System data	●	●	●	●	●	●	●	●	●
Other	●	●	●	●	●	●	●	●	●

Finance Sales Managers Administrators Marketing Remote Users Other Who

Database Overview

	AggrDb	Name: SelfAudit
	SelfAudit	Status: Database loaded successfully
		Loading date: Sun May 13 2007 20:00:53 GMT+02:00
		Content: 192.168.88.133 (InSightPortal), INSIGHTTEST (InSight, Unavailable, iView), INSIGHTTEST\INSIGHTTEST (Windows)
		Automatic policy: Sun May 13 2007 19:58:27 GMT+02:00
		User policy: Sat Jan 01 2000 01:00:00 GMT+01:00

Trend graphic Settings

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

Where To DINO (OS/390) Other Platforms (10)

Incident Tracking

This event is not tracked yet. Its unique event-id is: DINO.105\ZGBXRG1.194087

- Click [here](#) to open the ticketing service. (change)
- Copy the event information into the ticket.

Event Id : DINO.105\ZGBXRG1.194087

When : Fri Feb 22 2002 00:24:16 GMT+01:00 - Week Nights

fromWhere : DINO (OS/390) - Other Platforms

Who : CRMQAP1 (CRMQAP1) - Other Sources

Where : DINO (OS/390) - Other Platforms

What : Grant: Profile / Failure - Administration

WhereTo : DINO (OS/390) - Other Platforms

onWhat : PROFILE: - / CERT001.** - Configuration

3) Enter the ticket number and press [submit].

[Click here to see all incidents.](#)

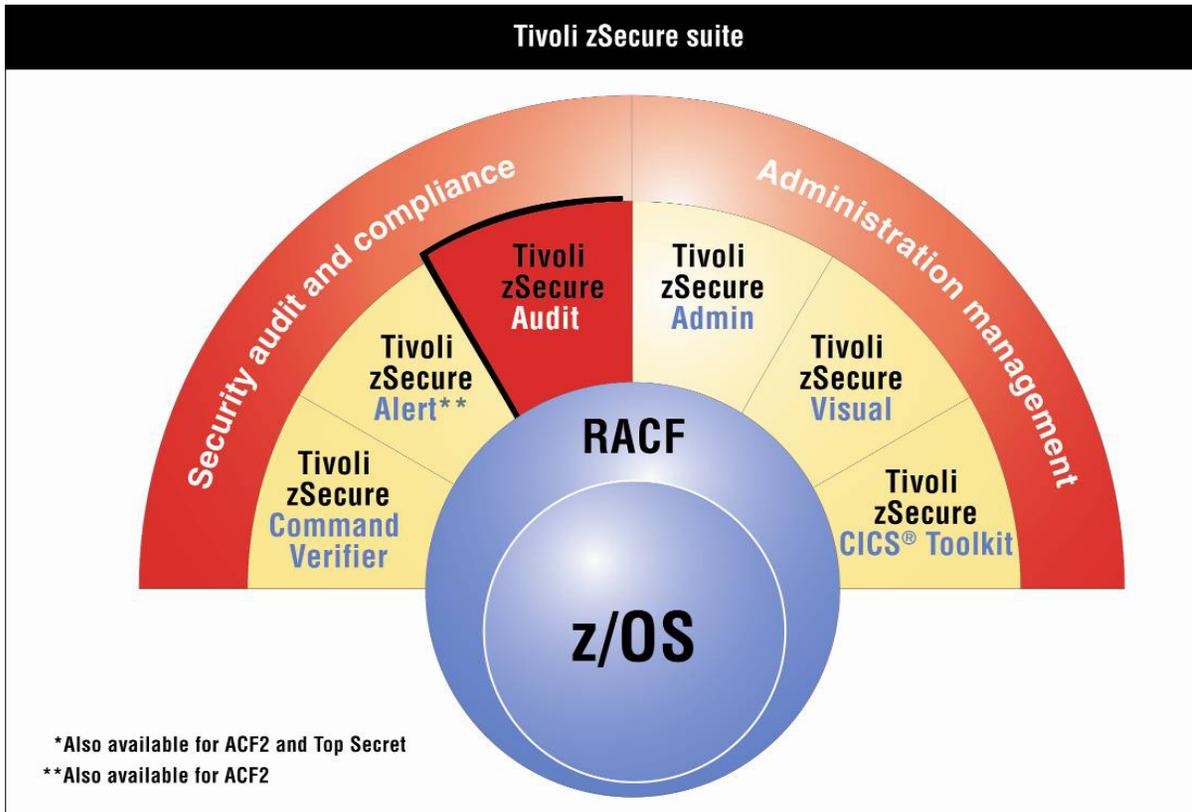
Additional information

Aspect	Value
Event :: subject	CRMQAP1
Event :: logrecordtype	SMF_PERMIT 1
Event :: command	PERMIT 'CERT001.** ACCESS(ALTER) CLASS(DATASET) GENERIC ID(CERT006)
Who :: originator	CRMQAP1

Investigate

IBM Tivoli zSecure Audit (z/OS)

- Détection des faiblesses
- Analyse automatique et visualisation des événements
- Permet de garantir la conformité et l'exhaustivité des audits



Fonctions:

- "Audit Priority" pour mise en évidence des faiblesses
- Contrôle du status de RACF (Setropts, Autab, Global ...)
- Suivi des activités utilisateurs (Trusted, activité password...)
- "Verify" (conformités utilisateurs, groupes, fichiers, programmes...)
- Analyse les contenus des fichiers sensibles (Zaps & PTFs, membres modifiés, dupliqués...)
- Détecte les changements systèmes (paramètres IPL, SVC, PPT, consoles, SMF, classes...)
- Trace des événements (ressources, users, IP ... par records SMF)
- Si besoin, rapports sur mesures à l'aide d'un langage puissant
- Intégré avec Tivoli zSecure Admin
- Agent pour Tivoli Compliance Manager

```

Consul zSecure RACF Display Selection
Command ==>
Name      Summary  Records  Title
OVERVIEW  140869   140869   Audit concern overview by priority (higher priorities only)
DMS
DMSAUDIT
EXITS
DASDVOL
MOUNT
SENSAPP
SENSLINK
SENSLPA
SENSALL
SETROPTS
SETROPAU
ROUTER
AUTAB
RANGE
RACFDSN
RACFCLAS
GLOBAL
TEMPLATE
STARTED
STCTABLE
TRUSTUSR
AUTHSYS
AUTHUID0
AUTHGRP
SHRDUIDS
DMVSNUID
SHRDGIDS
DMVSNPID
PROTECT
PUNONE
PVOID
PWINNONE
PWIMLONG
PWEXPIRE
PHEXPIRE
PUNOCHG
PHNOCHG
PWAGESUM
PWAGESUM
PWAGEALL
PWAGENEV
PWAGE5YR
PWAGE4YR
PWAGE3YR
PWAGE2YR
PWAGE1YR
PWAGE0YR
PWAGE6MN
PWAGE5MN

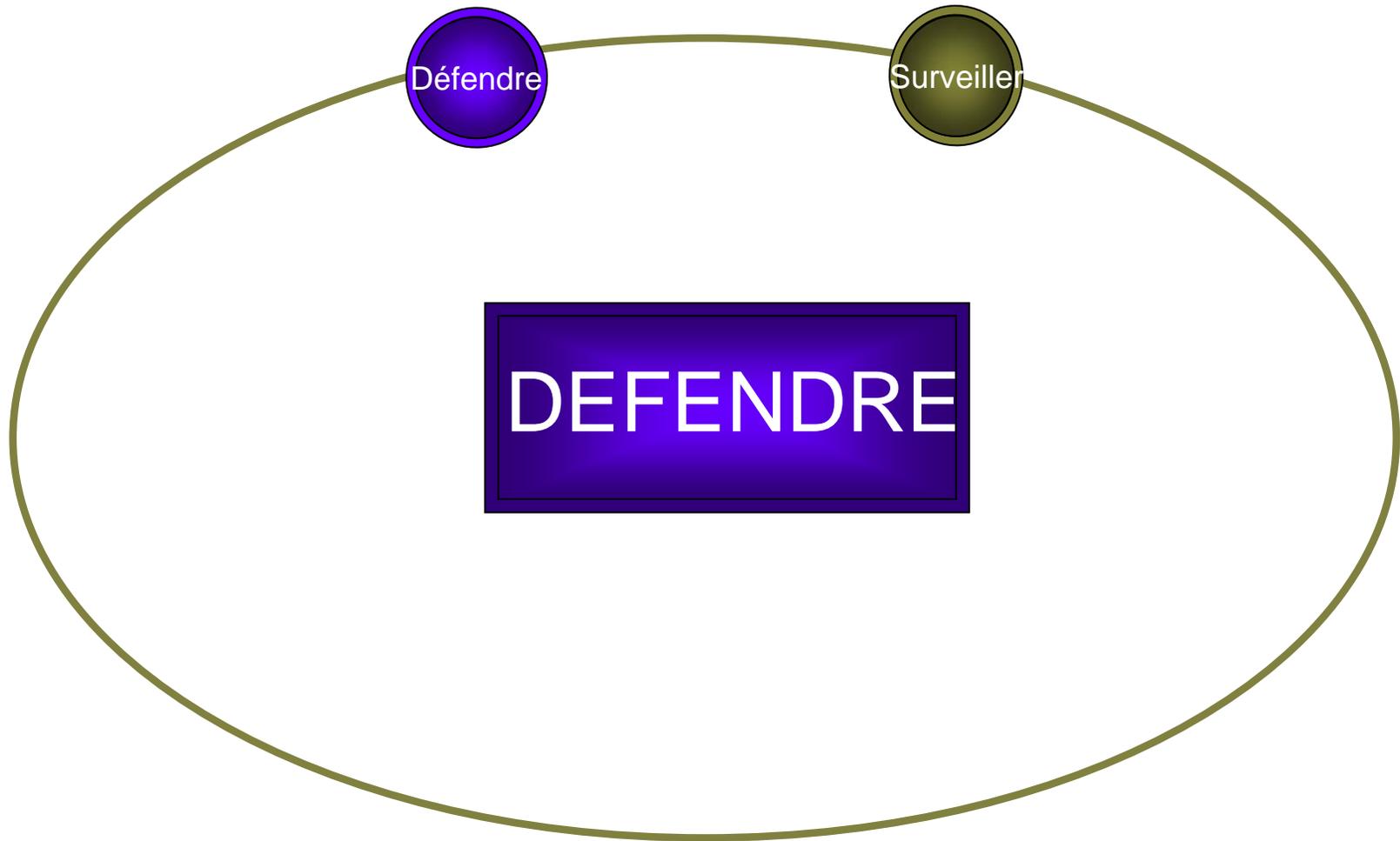
```

File Edit Edit Settings Menu Utilities Compilers Test Help

EDIT
Command =
d
001146
001147
001148
001149
001150
001151
001152
001153
001154
001155
001156
001157
001158
001159
001160
001161
001162
***** **

Event	Disc	SAF	auth	00-01	01-02	02-03	03-04	04-05	05-06	06-07	07-08	08-09	09-10	10-11	11-12	12-13	13-14	14-15	15-16	16-17	17-18	18-19	19-20	20-21	21-22	22-23	23-24	total	%
RACINIT	S			4926	4934	4733	3823	4370	10535	4211	2089	936	2904	2800	1099	2614	2520	2500	1317	1132	3189	1086	1071	5785	5474	8486	4250	86784	12
RACINIT	V			0	0	0	0	2	2	0	0	1	3	24	269	0	1	0	0	2	1	1	0	0	0	0	0	306	0
ACCESS	S	T		269	0	0	0	0	18	0	0	0	1758	9776	0	0	0	0	0	0	105	0	0	0	0	0	0	11926	1
ACCESS	S	O		0	0	0	0	0	0	1	3	63	75	8	9	0	94	3	6	8	4	0	0	0	0	0	0	274	0
ACCESS	S	N		2462	2849	3393	4167	4741	5406	3710	2578	2282	2165	4812	25295	2045	2635	2627	3079	3544	2305	1203	857	979	2360	1734	7498	94726	13
ACCESS	V	N		8	19	14	35	22	24	4	14	0	9	264	1016	13	7	6	6	8	5	10	1	1	5	8	51	1550	0
ADDVOL	S	N		0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	2	0
RENAME	S	N		33	14	16	7	3	5	10	3	16	19	17	15	7	9	7	9	14	12	8	5	4	16	6	17	272	0
DELETE	S	N		47	33	48	21	9	14	28	10	49	63	54	64	25	56	31	59	50	59	29	16	33	40	20	46	904	0
DEFINE	S	O		0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
DEFINE	S	N		0	0	0	0	0	0	0	0	1	0	0	0	0	0	2	0	6	0	0	0	0	0	0	0	9	0
DEFINE	V	N		0	0	6	0	0	18	6	0	0	0	6	0	0	0	1	0	0	0	0	19	0	0	0	0	56	0
ADDSD	S	S		0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0
ADDSD	V	N		0	0	0	12	0	0	0	3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	3	0	18	0
ADDGROUP	V	N		0	0	0	8	0	0	0	2	0	0	0	0	0	0	0	0	0	0	0	0	0	2	0	0	12	0
ADDUSER	S	N		0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	2	0
ADDUSER	V	N		0	4	4	3	1	2	0	1	0	0	0	0	0	0	0	0	2	0	0	0	0	0	0	1	18	0
ALTDSD	S	S		0	12	0	0	1	2	0	0	0	0	0	0	0	4	0	3	0	0	0	0	0	0	0	0	22	0
ALTDSD	V	N		0	0	0	41	0	123	41	0	0	0	41	0	0	0	0	0	0	0	0	0	0	0	0	0	246	0
ALTUSER	S	S		0	0	0	0	0	0	0	0	0	0	0	9	0	0	0	0	0	0	0	0	0	0	0	0	9	0

Audit en temps réel & Protection des bases (Protection & Actions immédiates)



IBM Tivoli zSecure Alert & Command Verifier

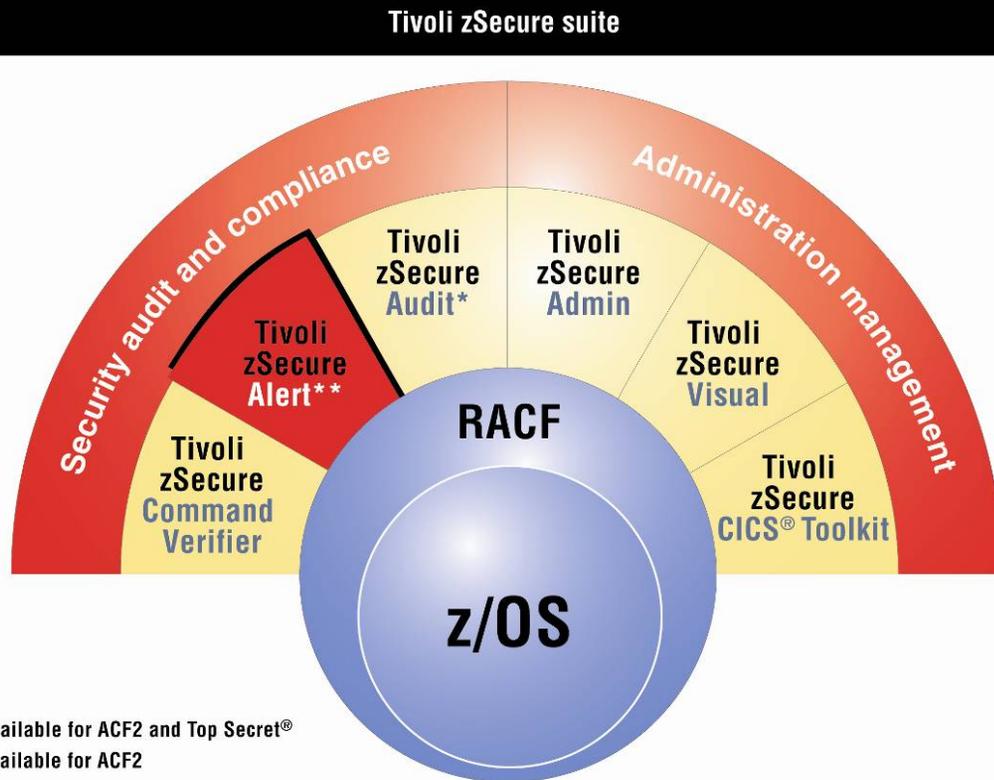
- Détection des impacts en temps réel
- Alertes externes en temps réel
- Protection des commandes non conformes

Fonctions Alert :

- Travailler en mode exception
- Externaliser immédiatement une menace
- Formats WTO, SNMP, SMTP
- Personnalisation sous ISPF
- Alertes standards pré définies
- Intégré avec zSecure Admin
- Source : WTO, SMF et extra records RACF
- Si besoin, ajout sur mesures à l'aide d'un langage puissant

Fonctions Command Verifier :

- Contrôle du contenu (mots clefs)
- Politiques (Xfacility resource class)
- Délégation contrôlée



*Also available for ACF2 and Top Secret®

**Also available for ACF2

IBM Tivoli zSecure Alert & Command Verifier

Menu Options Info Commands Setup

Command ==)

Select the a
The followin

Id	Cate
1	User
7	Grou
2	Data
3	Gene
4	UNI)
5	RACF
6	Sys-
0	Othe

*****>

Specify S
Type Sub
80

Specify W
Prefix

Select al
/ E-mail
= Specif
Enter / t
- ISPF S

Alert: Global read specified on /etc/security/server.kdb

File Edit View Create Actions Help

Workspace Alert: Global read specified on /etc/security/server.kdb

New Memo Reply Forward Delete Folder Copy into

C2POLICE at PROD To: Joe.Security@consul.com
15/09/03 1:41 cc: Pete.Auditor@consul.com

Subject: Alert: Global read specified on /etc/security/server.kdb

Global read specified when altering file access

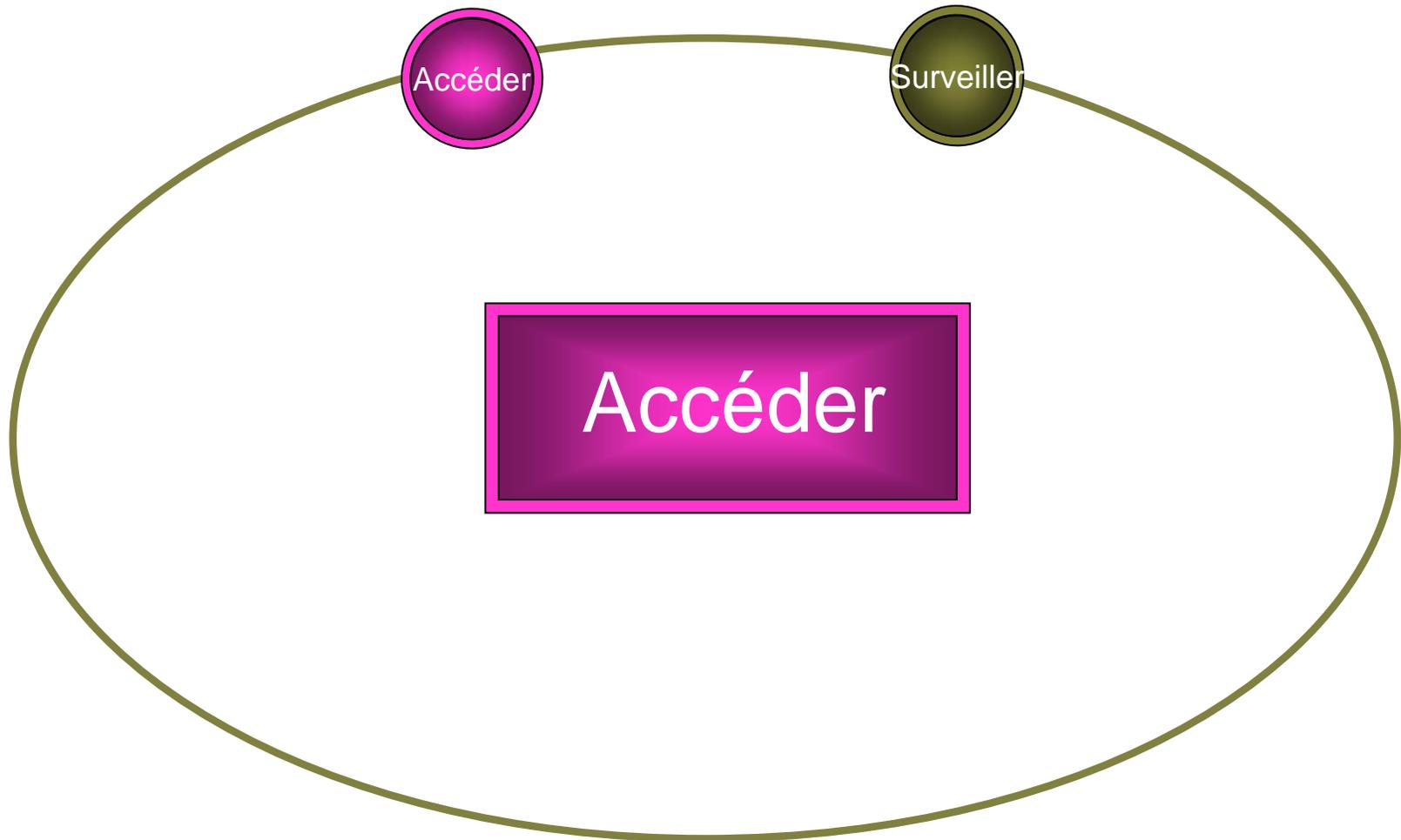
Alert id	1403
Date and time	Mon 15/09/03 1:40
Path	/etc/security/cert.arm
Old permissions	rw-----
New permissions	rw-r--r--
Result	Success
User	SPROG11 JOE TECHNICIAN
Job name	SPROG11
System ID	PROD

Alert: Global read specified on /run/cnruxdb

Global read specified when altering file access

Alert id	1403
Date and time	Mon 15/09/03 1:40
Path	/etc/security/server.kdb
Old permissions	rw-----
New permissions	rw-r--r--
Result	Success
User	SPROG11 JOE TECHNICIAN
Job name	SPROG11
System ID	PROD

Administration RACF (partenariat zSecure Audit & Alert)

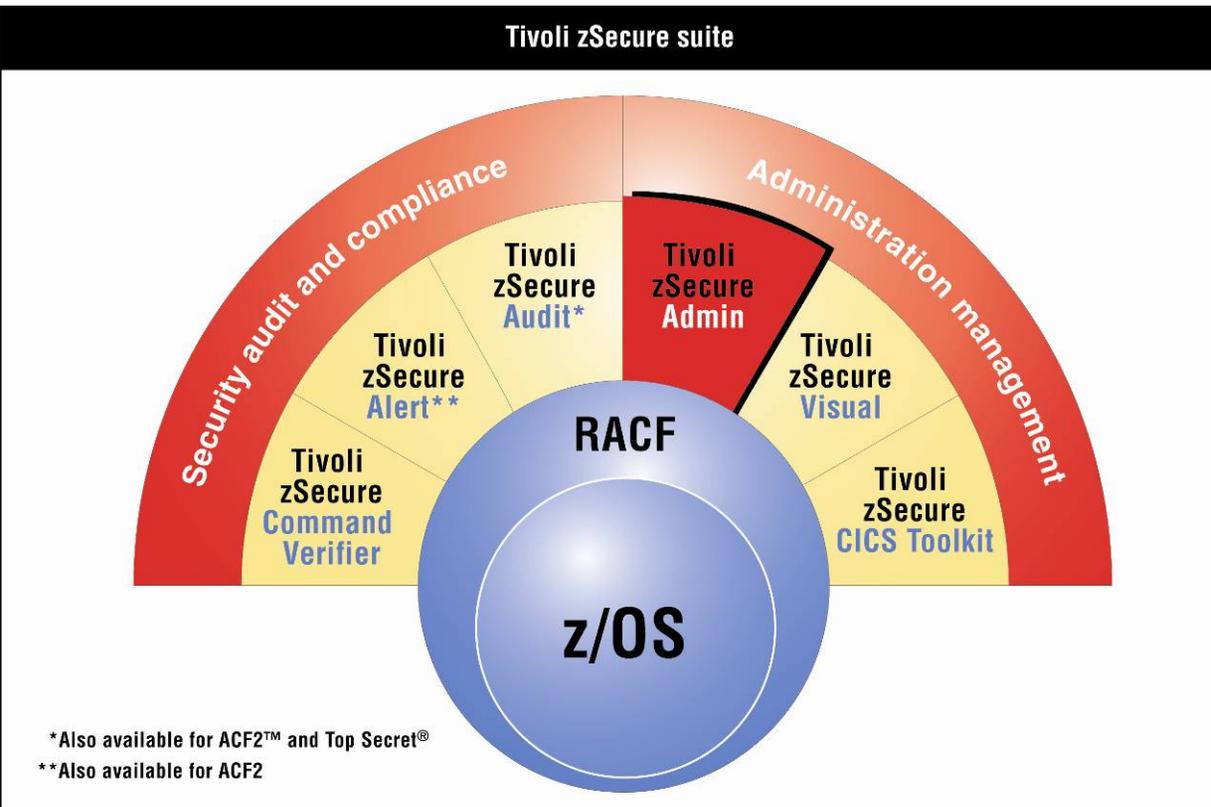


IBM Tivoli zSecure Admin

- Administration complète de RACF
- Gestion simplifiée et efficiente
- Démarches guidées et automatisées
- En "live" mais sous contrôle

Fonctions:

- Respecte RACF
- Interface ISPF standard
- PF1 : help !
- Accès direct aux bases RACF
- Intègre les données "système"
- Exécution des ordres contrôlée
- Filtres (gestion par exceptions)
- "Mass update" (tout l'utilisateur)
- Clonage
- Délégation
- Complet (USS, Certificat...)
- Rapports par défauts
- Gestion de l'état actuel ...
- Pour ajout/modification
- Quick Admin & Helpdesk
- Access Check rapide
- TRES Rapide !



*Also available for ACF2™ and Top Secret®

**Also available for ACF2



IBM Tivoli zSecure Admin

```

Menu  Options  Info  Commands  Setup
-----
Comm:  Menu  Options  Info  Commands  Setup          StartPanel
_ f
Show  Menu  Options  Info  Commands  Setup          StartPanel
Class
Resol
-----
Ownec
Insta
1  Profiles          Any profiles fitting mask/qualifier with their data sets
2  Non redundant     Data set profiles different from less specific profiles
3  Redundant         All data set profiles, mark if non-redundant (as in 2)
4  Permit/scope     User/group on access list, or access by any means
5  Out of group     Group data sets accessible to users outside the group
6  Non default      Data sets with more in access list than 'owner has alter'
7  Match            Find profiles that cover a data set or resource
8  Group tree       Group tree display
9  USERDATA        Display and action on profiles with USERDATA
A  Tapevol          Tapevol profile overview
B  RACFvars         RACF variable profiles
C  APPL             Application profiles
D  JES/328X        JES/328X definitions and log data sets
E  SDSF            SDSF command and display authorities
F  JES2            Access to JES2 resources
G  Compare users    Compare access and/or connect

Option ==>

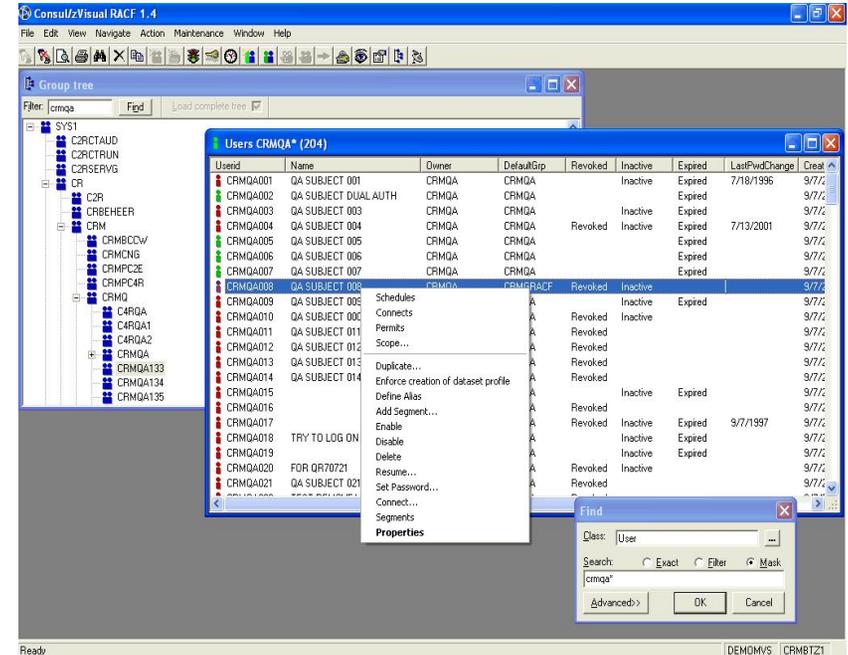
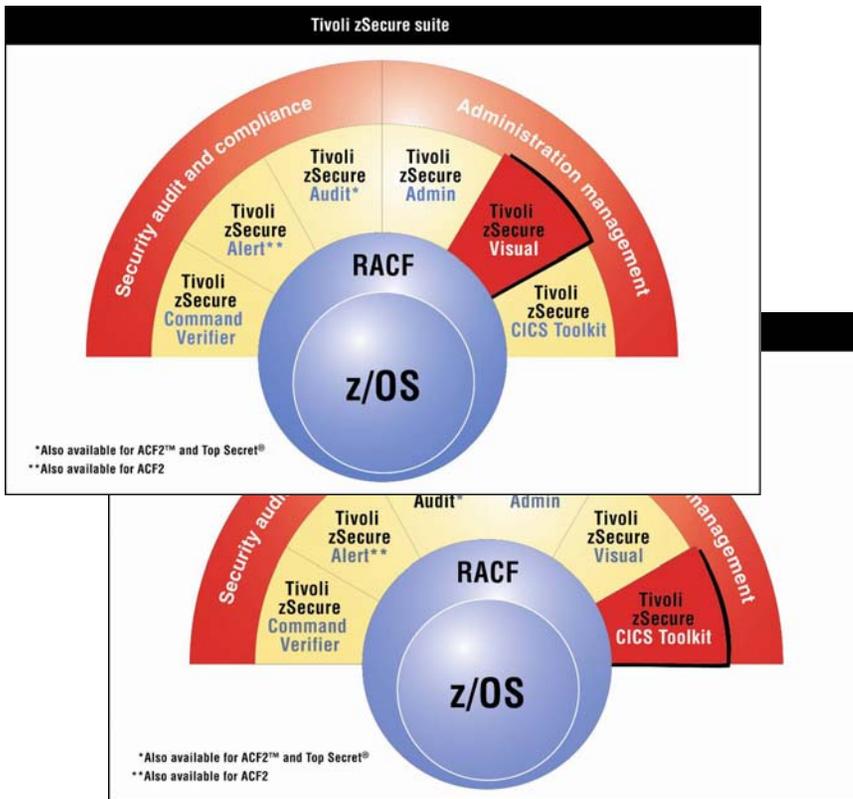
```



IBM Tivoli zSecure Visual & IBM Tivoli zSecure CICS Toolkit

RACF sous Windows !

Interface de sécurité sous CICS !



Fonctions :

- API Applications-RACF
- Délégation (écrans personnalisés)
- Effectuent les contrôles d'accès
- Interface industrialisée





Tivoli



Session 11 : Système Z

La Gestion Globale de la Sécurité au niveau du Système
d'Information, de bout en bout

Questions ?

François Lèbe
Michael Cable

francois.lebe@fr.ibm.com
michael.cable@be.ibm.com

1^{er} et 2 octobre 2007

