IBM

Tivoli software

Tivoli Security : Suite zSecure

La Gestion Globale de la Sécurité

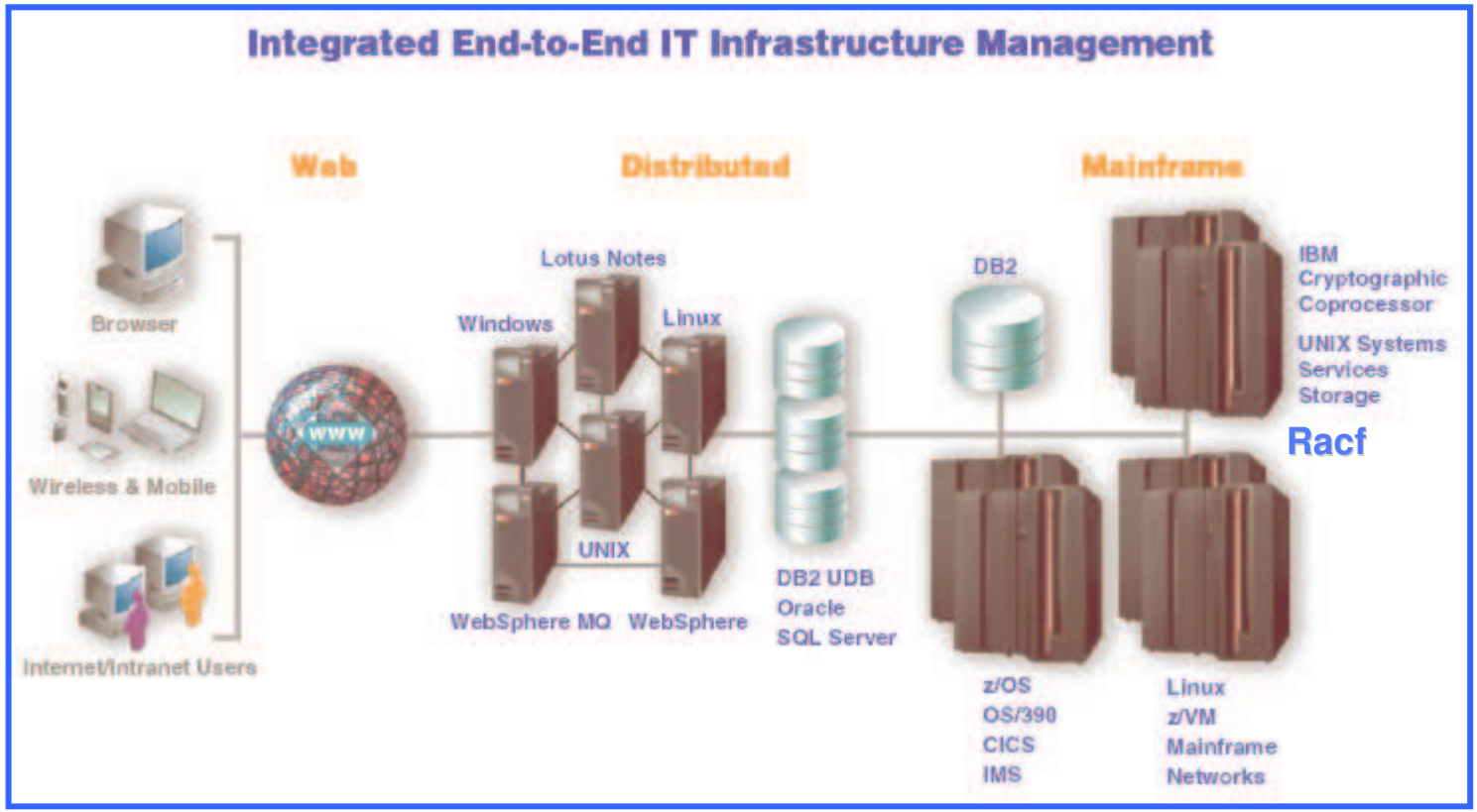
De bout en bout

francois.lebe@fr.ibm.com

© 2007 IBM Corporation

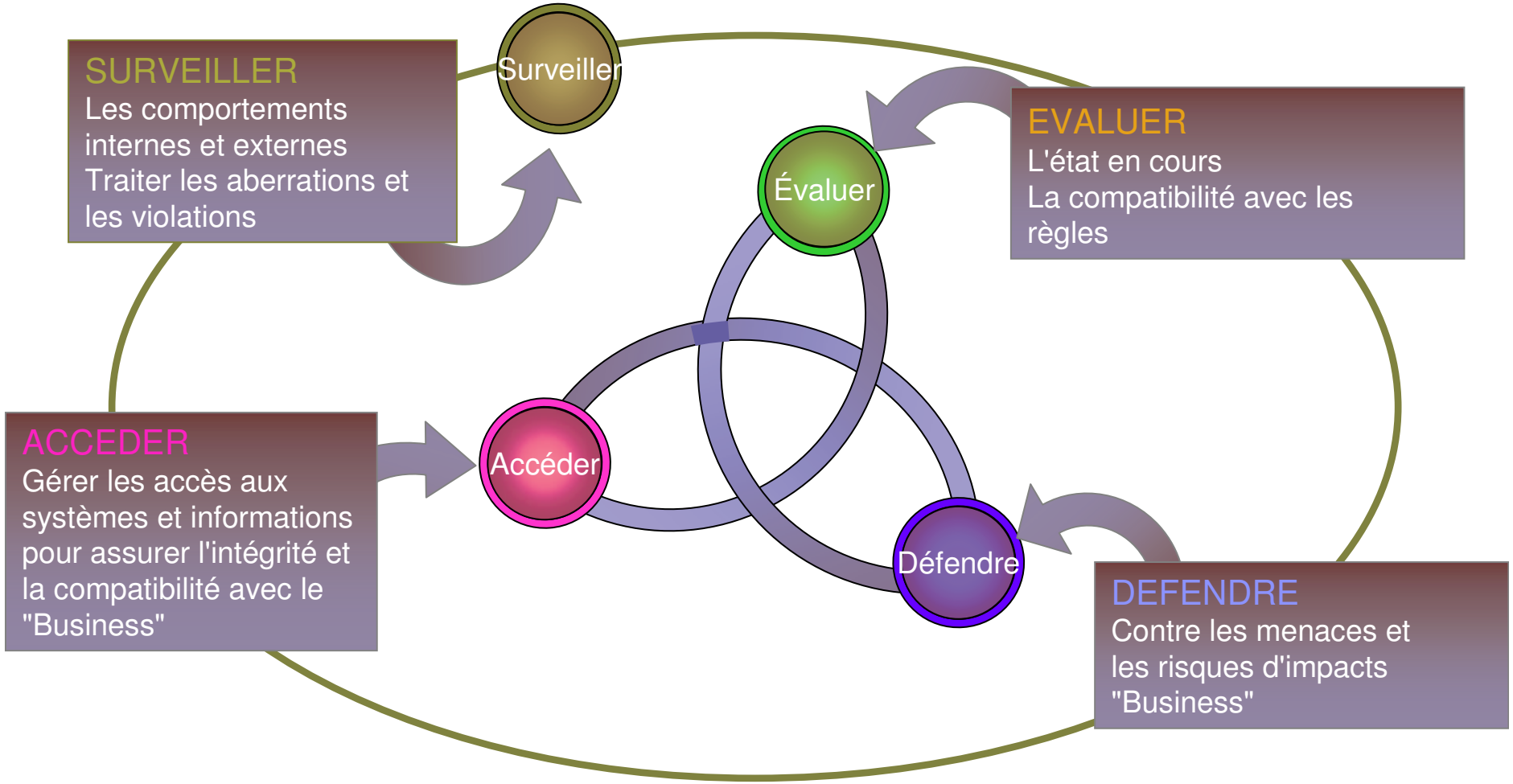
Sécurité du Système d'Information : De bout en bout

- **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"**



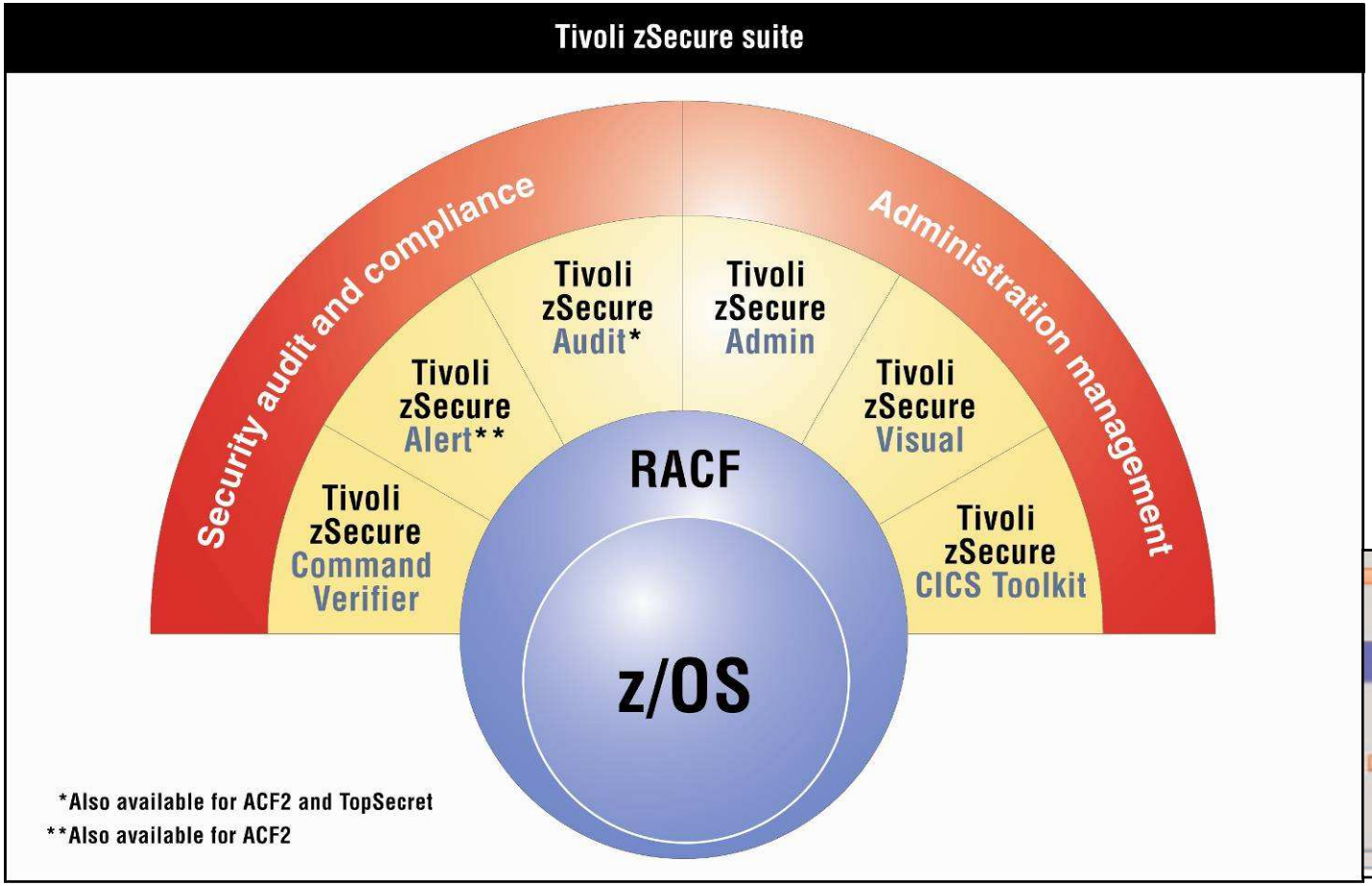
© 2007 IBM Corporation

La vision et la stratégie IBM concernant la sécurité



© 2007 IBM Corporation

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



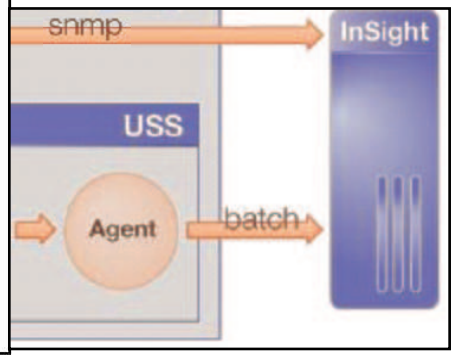
SURVEILLER

DEFENDRE

ACCEDER

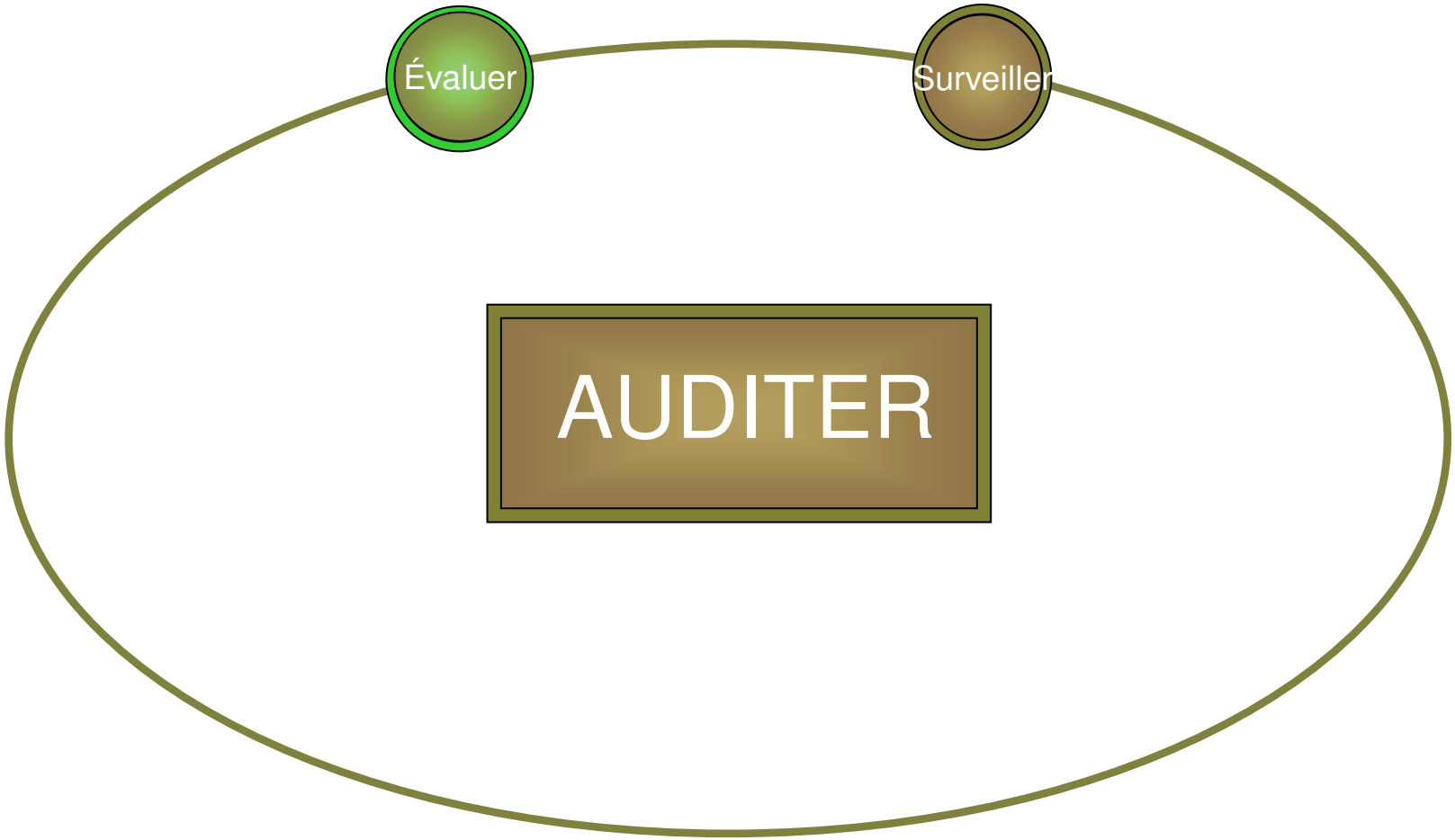
EVALUER

De bout en bout



© 2007 IBM Corporation

Audit de conformité & Audit des évènements

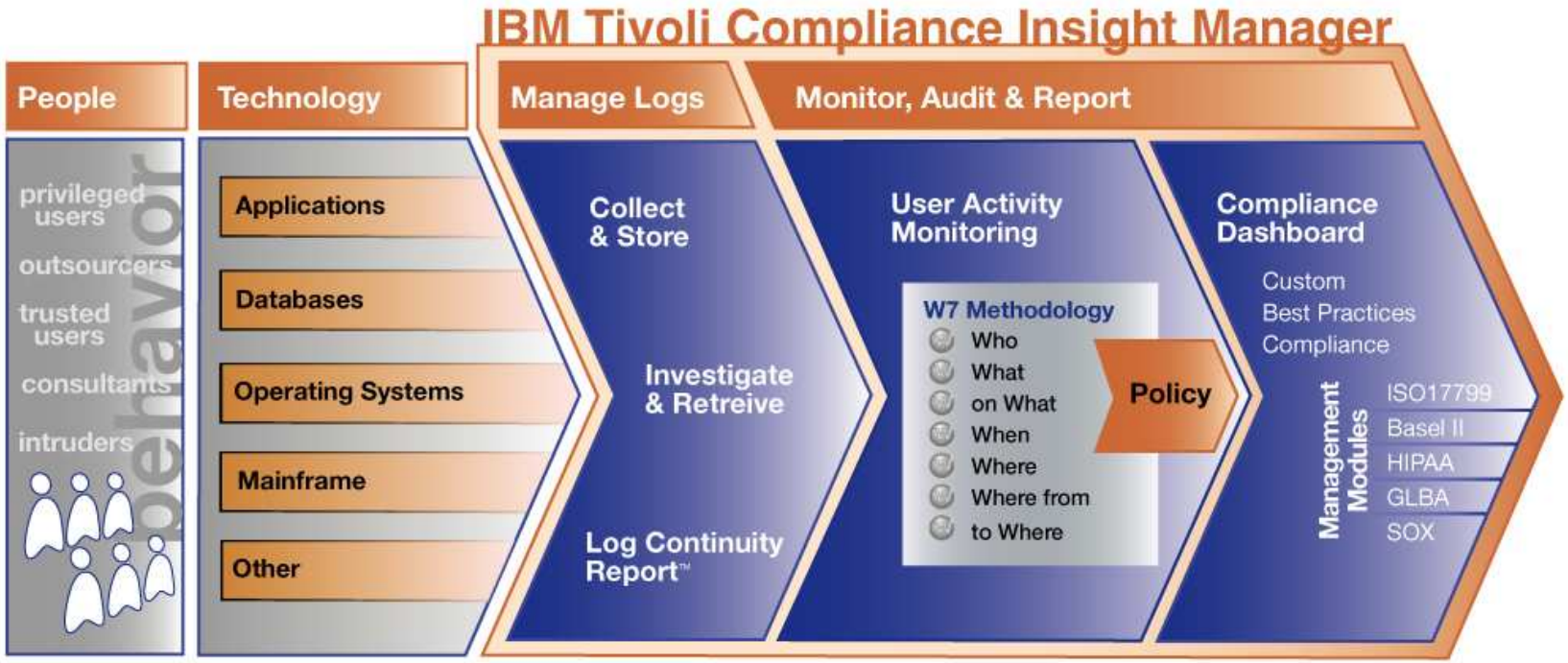


Connaître pour Défendre & Agir

© 2007 IBM Corporation

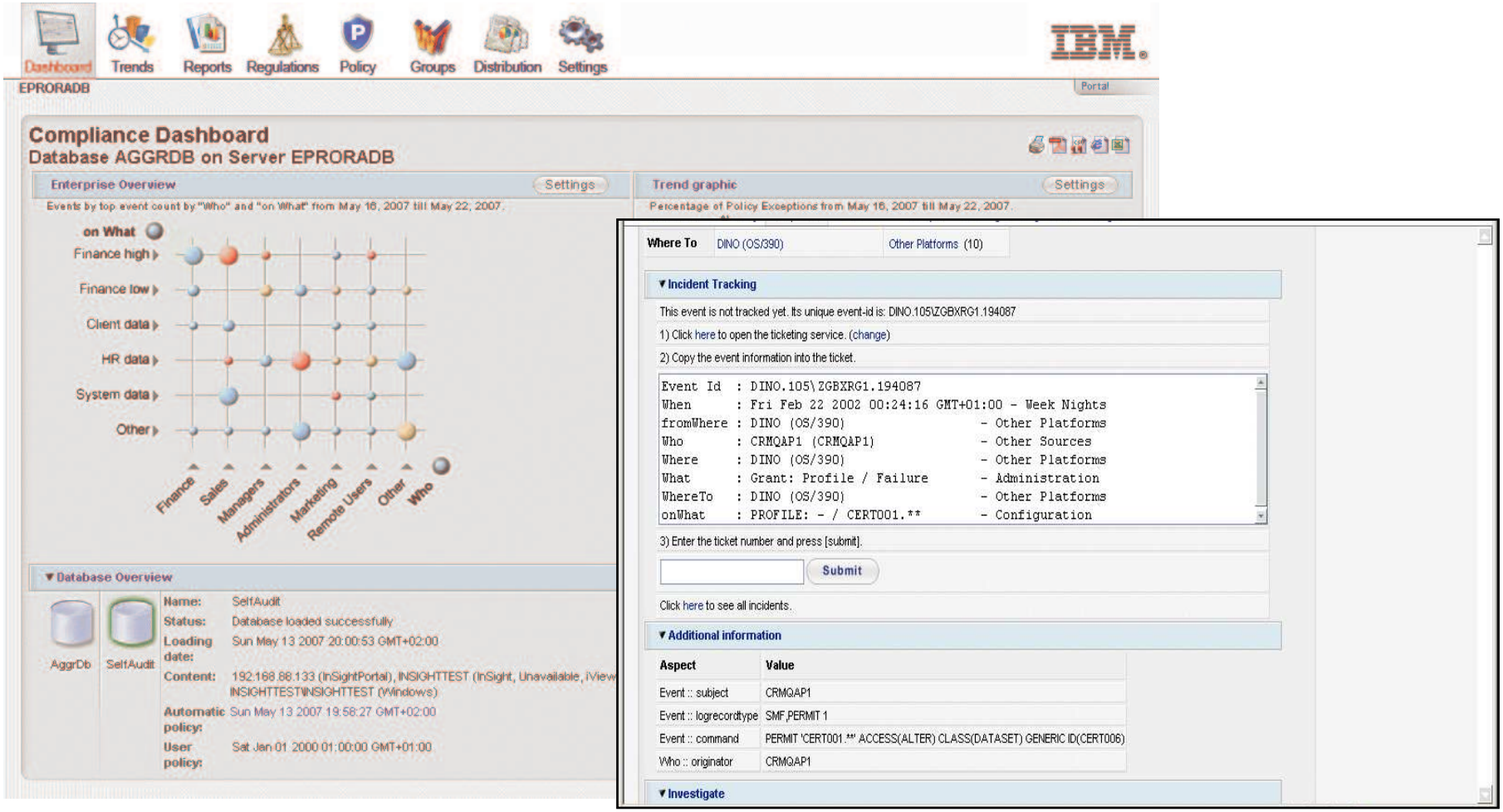
Audit global : Tivoli zSecure Compliance Insight Manager

- **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)**



© 2007 IBM Corporation

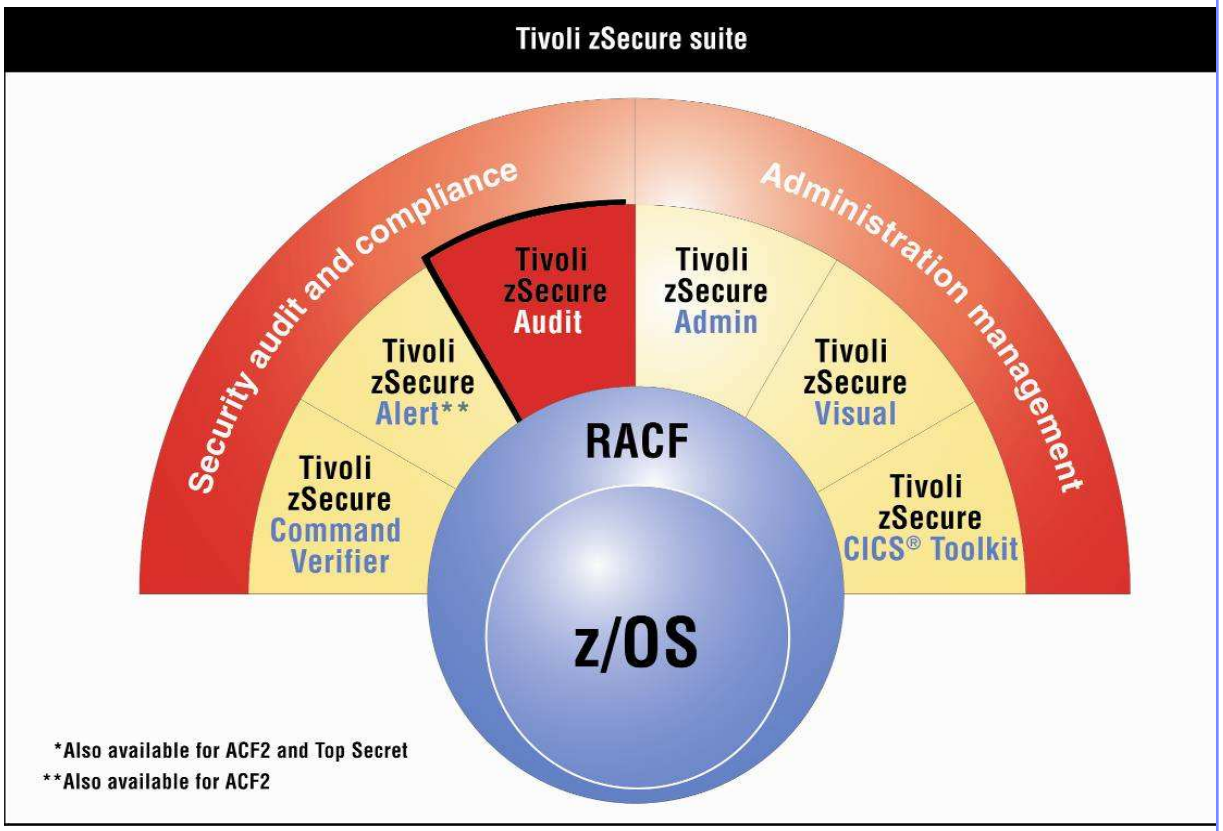
Audit global : Tivoli zSecure Compliance Insight Manager



© 2007 IBM Corporation

IBM Tivoli zSecure Audit (z/OS)

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



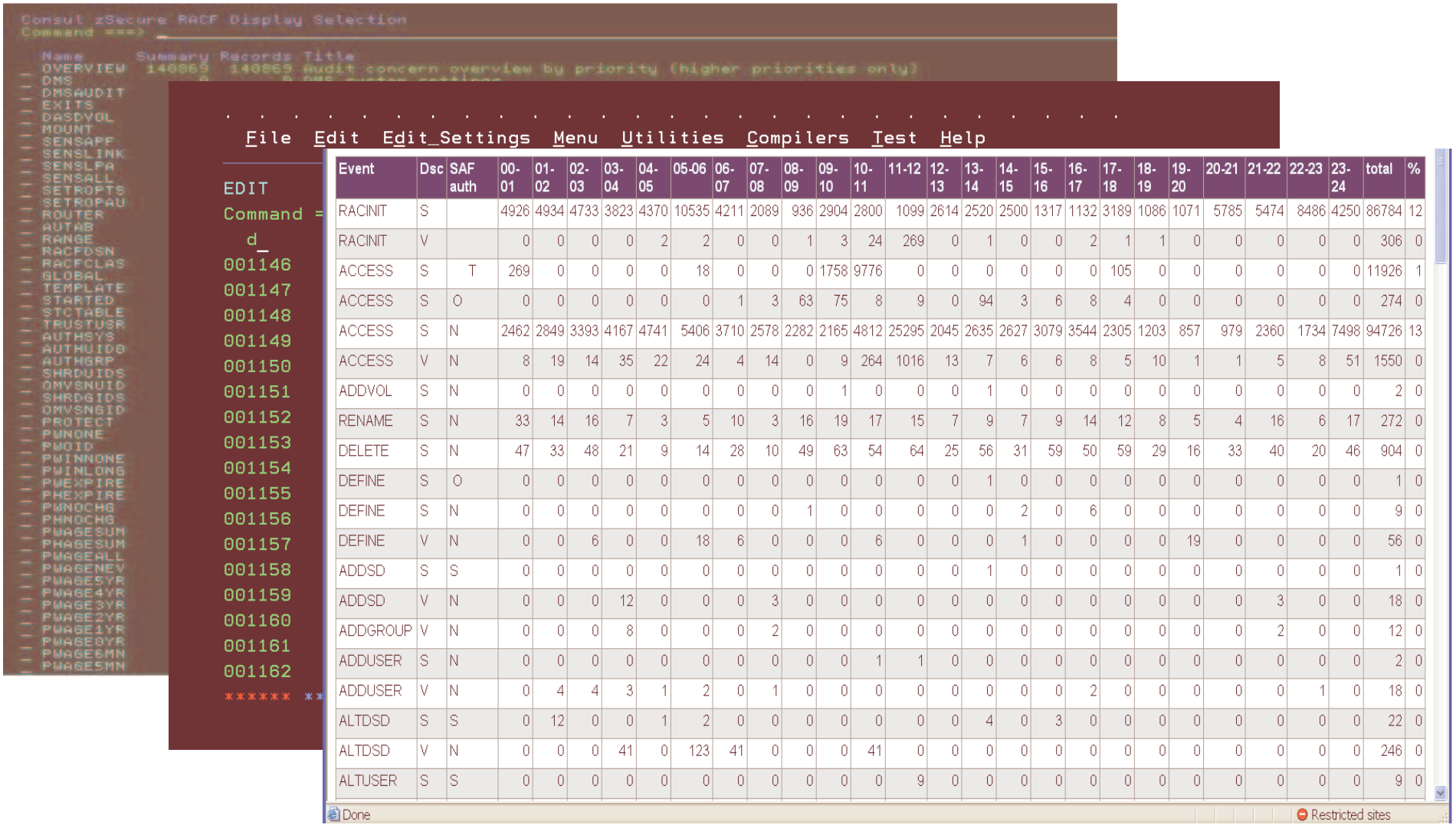
Fonctions:

- "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 évènements (ressources, users, IP … par records SMF)
- Si besoin, rapports sur mesure à l'aide d'un langage puissant
- Intégré avec Tivoli zSecure Admin
- Agent pour Tivoli Compliance Manager

© 2007 IBM Corporation

IBM Tivoli zSecure Audit

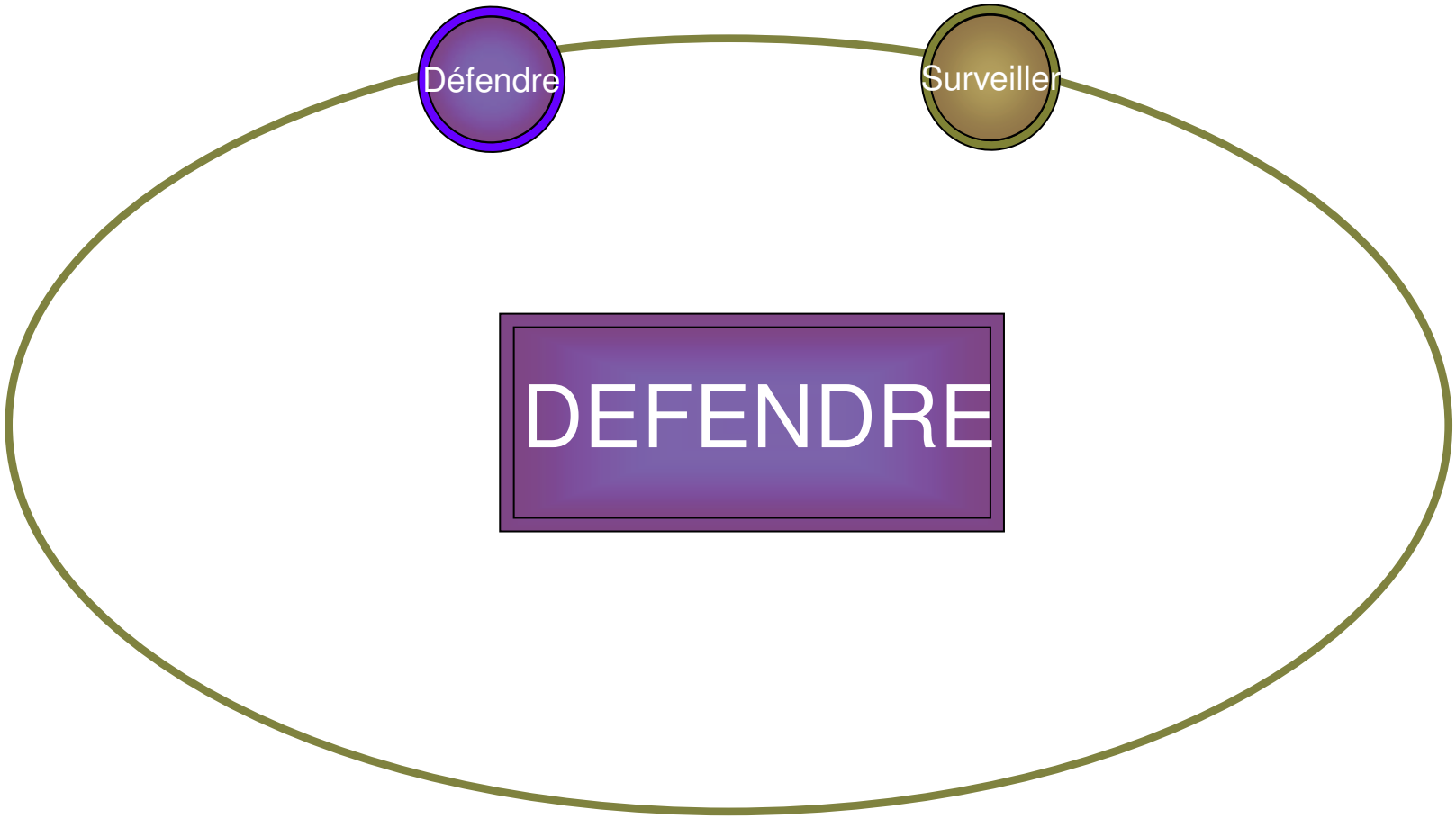
En XML



Event	Dsc	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	3	0	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	1	0	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

© 2007 IBM Corporation

Audit en temps réel & Protection des bases

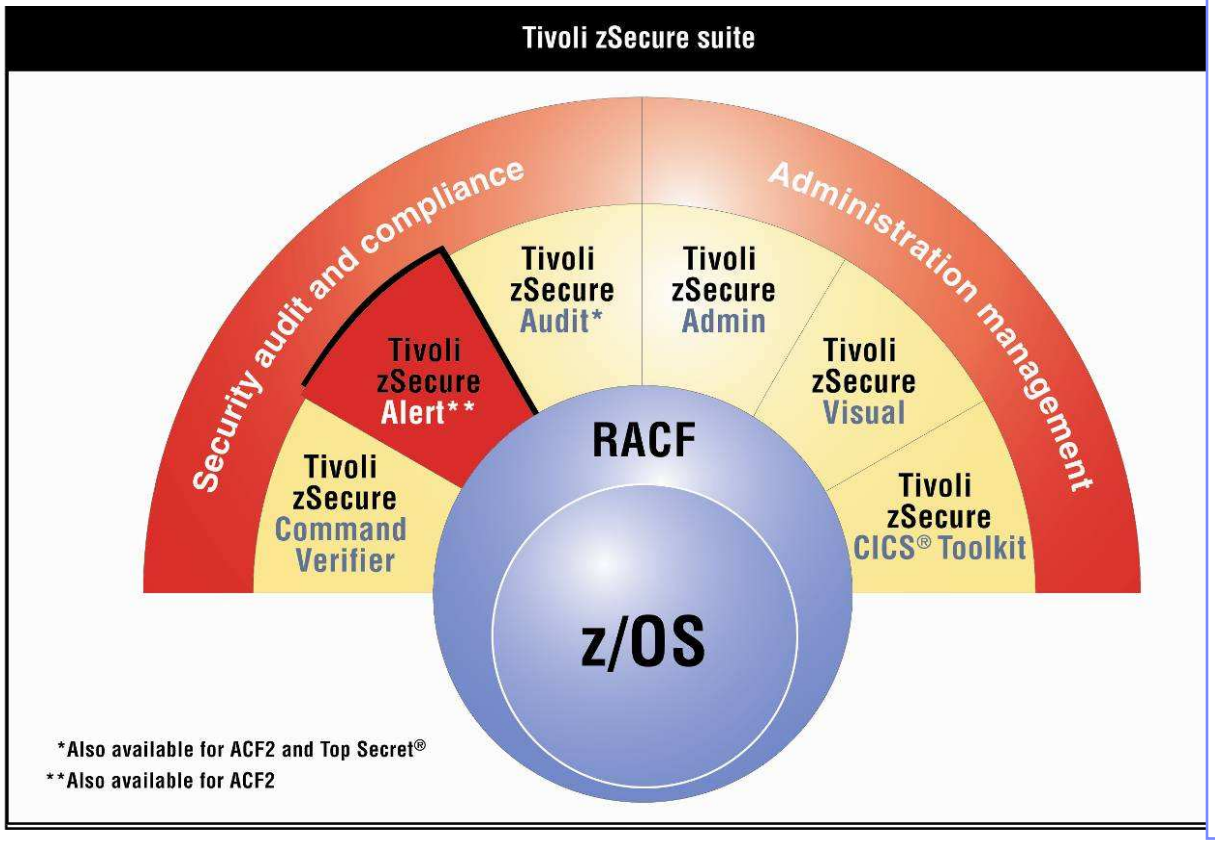


Protection & Actions immédiates

© 2007 IBM Corporation

IBM Tivoli zSecure Alert & Command Verifier

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



Fonctions Alert :

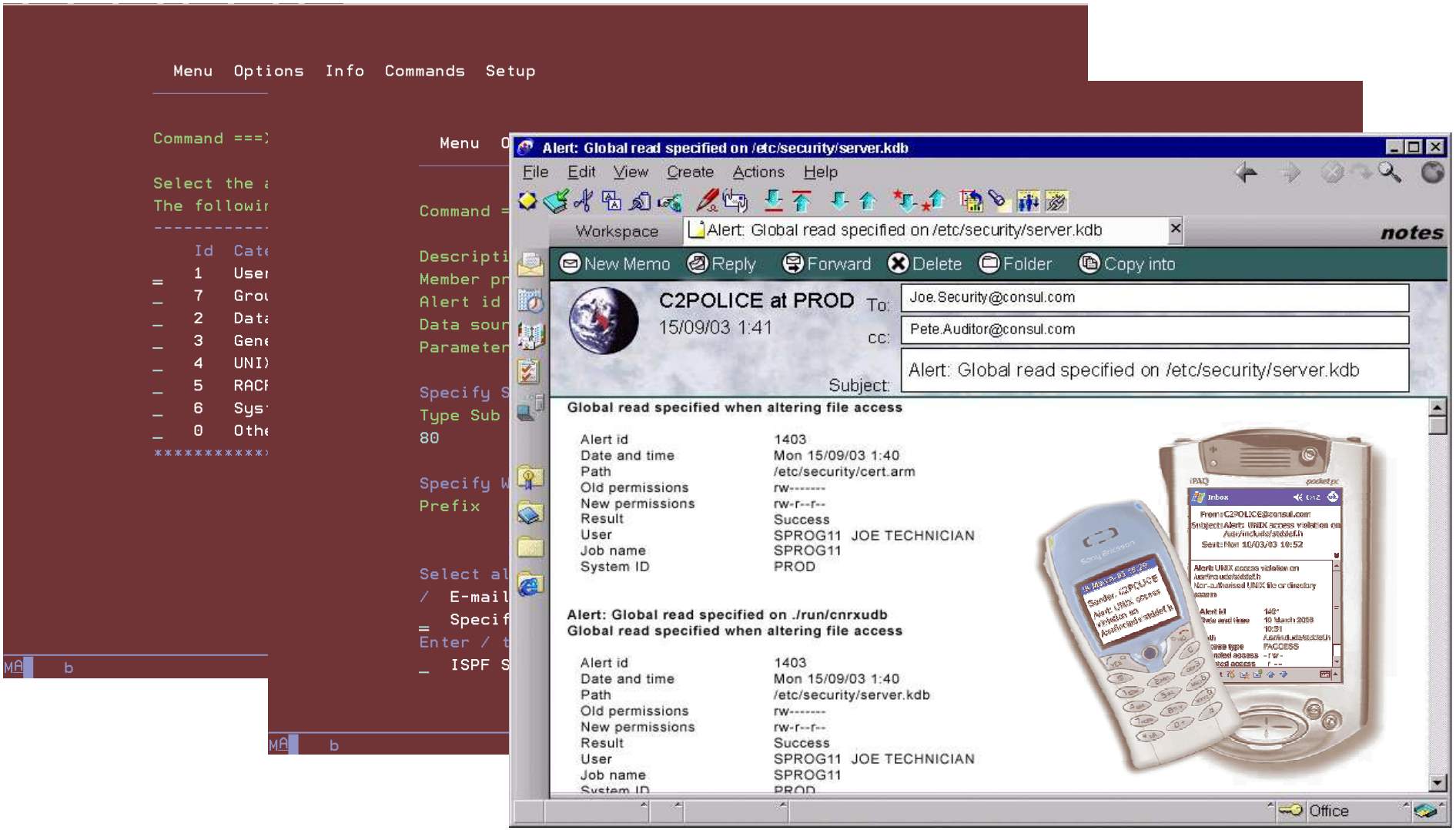
- Travailler en mode exception
- Externaliser immédiatement une menace
- Formats WTO, SNMP, SMTP
- Personnalisation sous ISPF
- Alertes standards pré définies
- Intégré avec zSecure Admin
- Source : WTO, SMF et extra records RACF
- Si besoin, ajout sur mesure à l'aide d'un langage puissant

Fonctions Command Verifier :

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

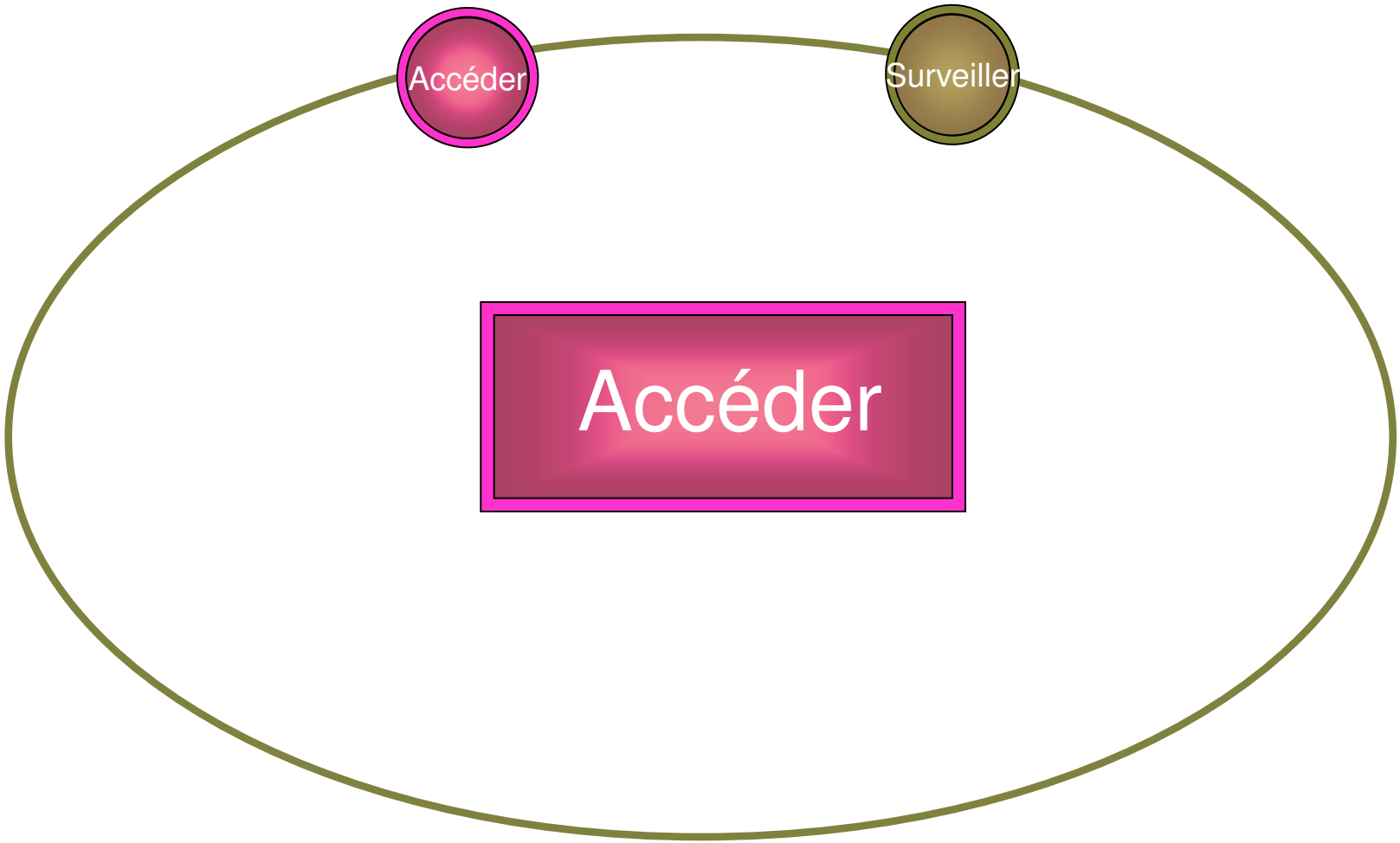
© 2007 IBM Corporation

IBM Tivoli zSecure Alert & Command Verifier



© 2007 IBM Corporation

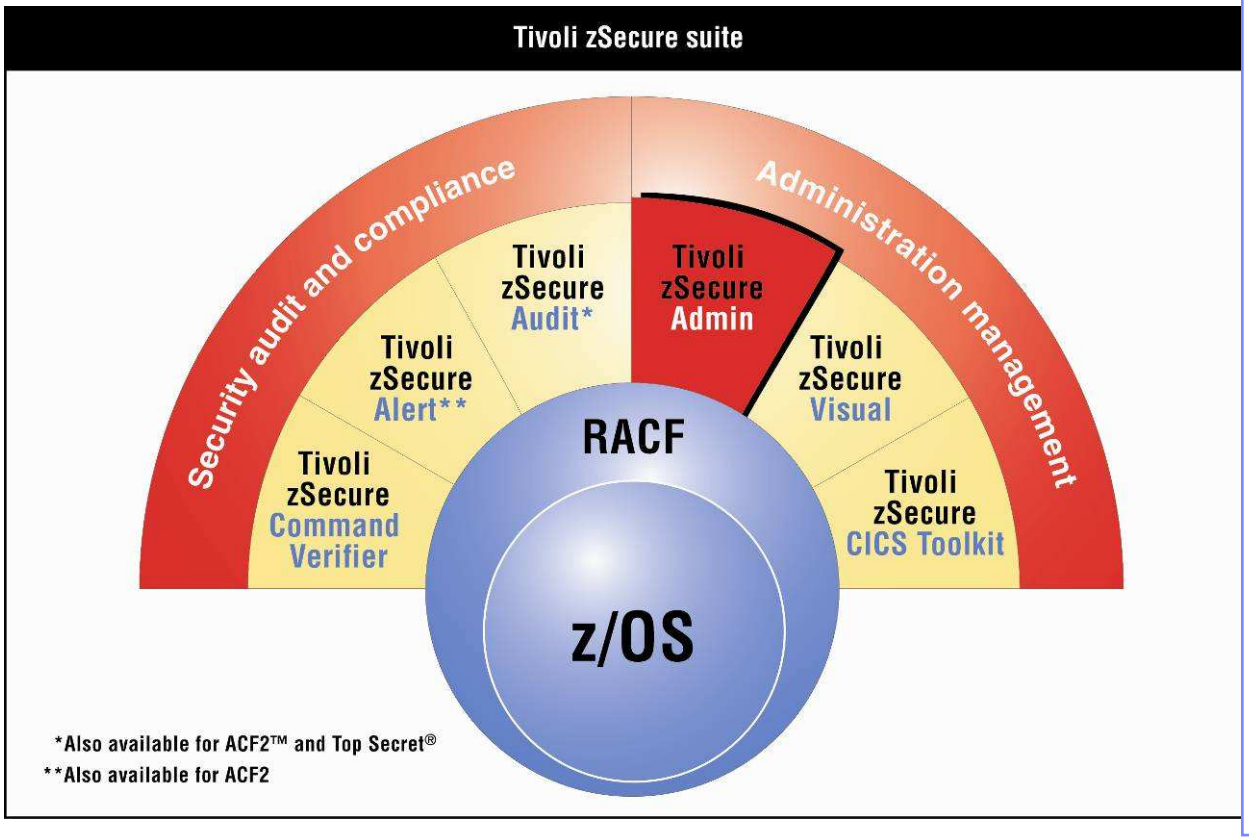
Administration RACF (partenariat zSecure Audit & Alert)



© 2007 IBM Corporation

IBM Tivoli zSecure Admin

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

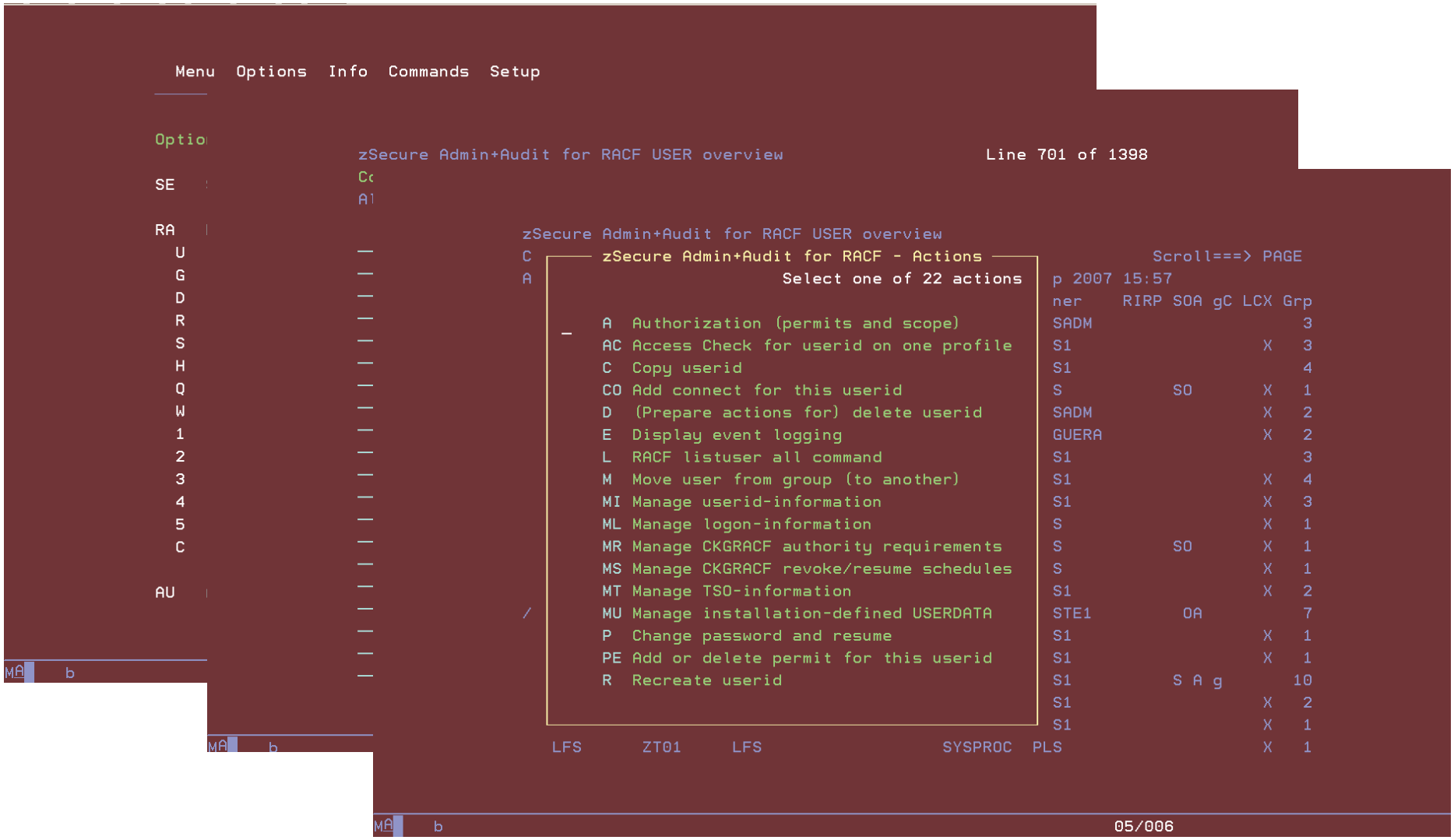


Fonctions:

- 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 !

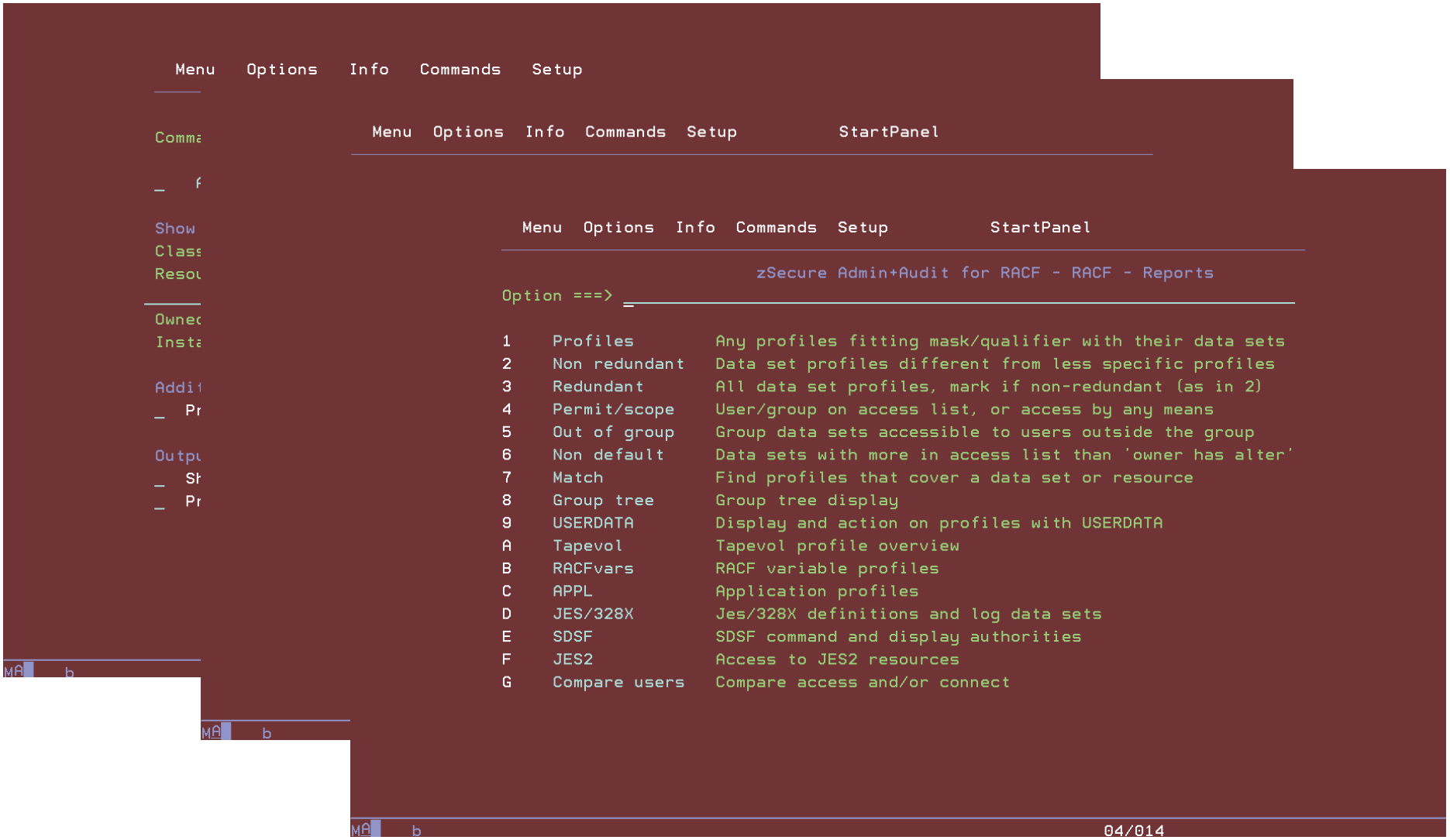
© 2007 IBM Corporation

IBM Tivoli zSecure Admin



© 2007 IBM Corporation

IBM Tivoli zSecure Admin

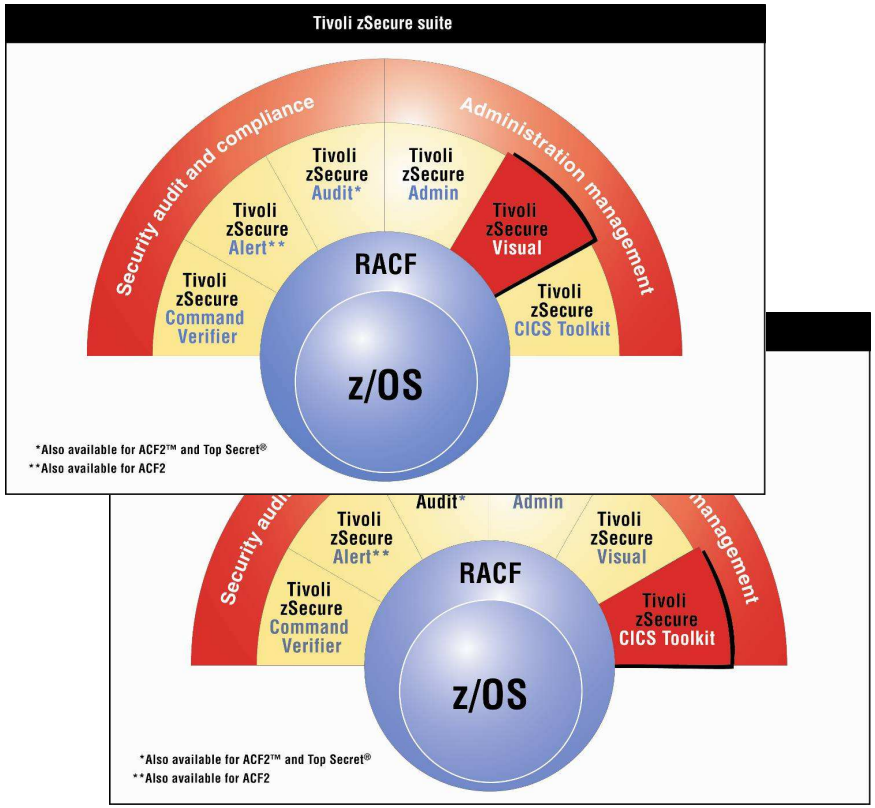


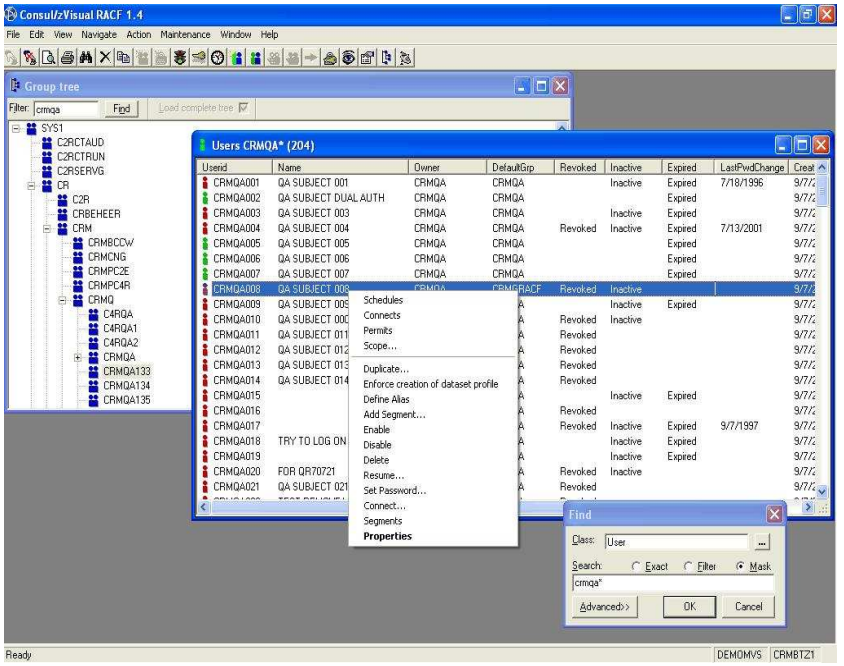
© 2007 IBM Corporation

IBM Tivoli zSecure Visual & IBM Tivoli zSecure CICS Toolkit

RACF sous Windows !

Interface de sécurité sous CICS !

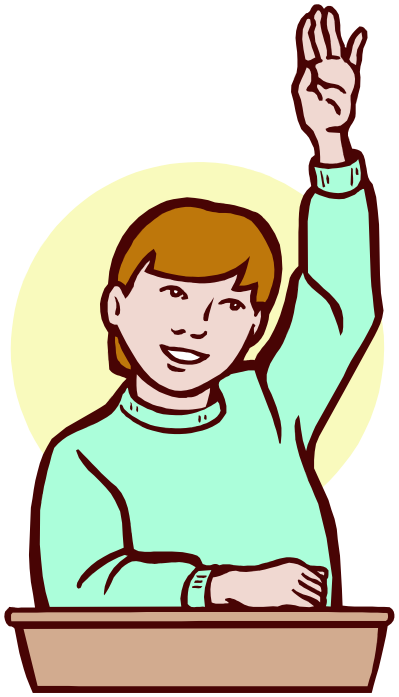




Fonctions :

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

© 2007 IBM Corporation



Questions?

© 2007 IBM Corporation