

Politique cohérente de sécurité des informations avec RACF

Spécifique SUPINFO

Jean-Pierre MARTI
IBM Certified Specialist RACF

Chapitre 1

Les Principes de Base de RACF

Vue générale

Présentation

- Schéma général
- La question envoyée à RACF
 - * QUI ?
 - * QUOI ?
 - * COMMENT ?
- Description des Objets RACF
- Relation entre RACF et le système d'exploitation
- Les pouvoirs
 - * Opérationnels
 - * Administratifs
 - * De contrôles

Schéma général

Sécurité - Protection de Ressources

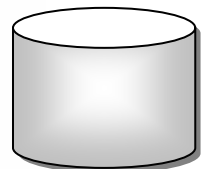
- Personne



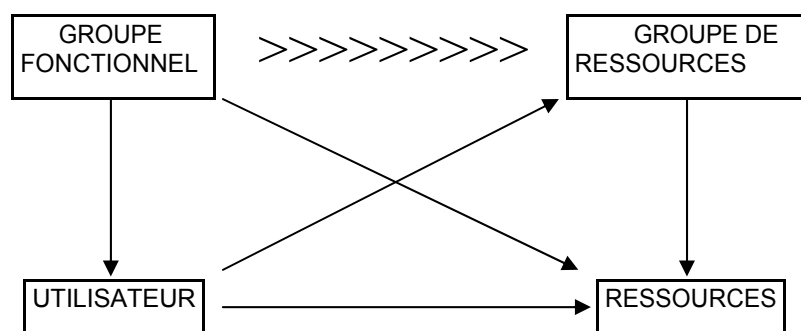
- Commodités



- Ressources



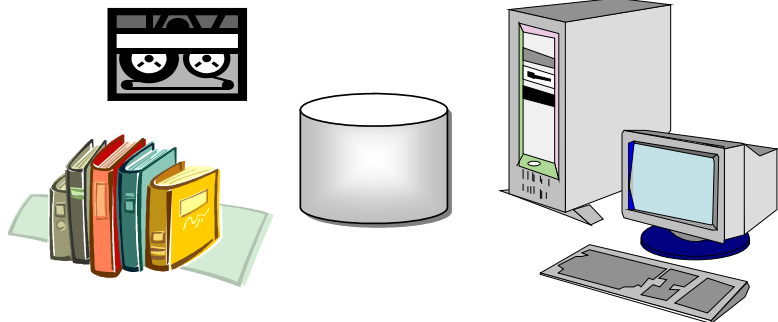
Relation USERS / RESSOURCES



La sécurité des données

La protection des données par :

- Destruction
- Modification
- Divulgence
- Utilisation



accidentelle ou intentionnelle

Relation USERS / RESSOURCES...

- En informatique tout est

RESSOURCE

- ✓ Temps
- ✓ Mémoire réelle ou virtuelle
- ✓ Opérations d'entrée/sortie
- ✓ Un programme
- ✓ Une portion de code dans un programme
- ✓ Une transaction
- ✓ Un fichier
- ✓ Une liste d'impression (sysout)
- ✓ Une commande opérateur, IDCAMS, DFDSS, ...
- ✓ Un noeud VTAM
- ✓ Etc ...

- Et, est accessible via un

GESTIONNAIRE

- Ce gestionnaire est tout indiqué pour opérer des contrôles de sécurité.

La question envoyée à RACF

Personnes et Ressources d'Information

Managers



Owners



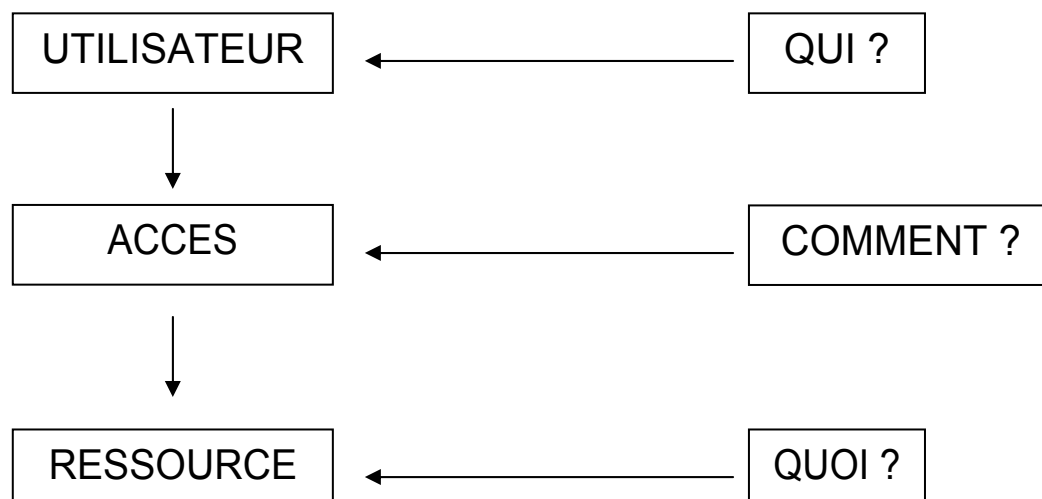
Prestataires de service



Users

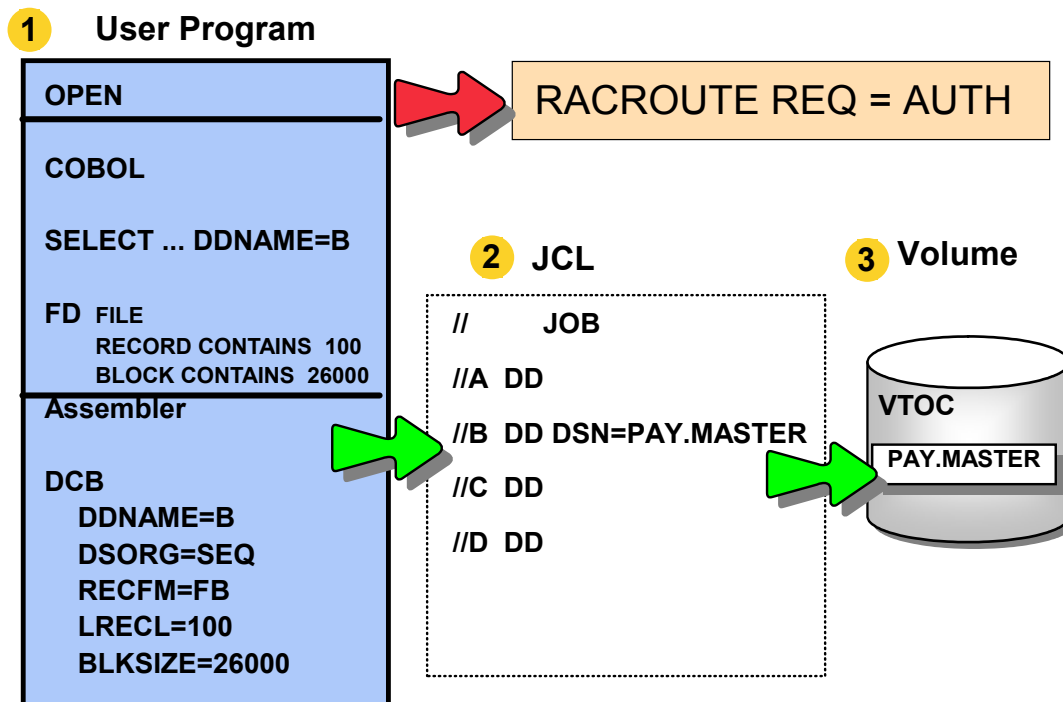


QUI, QUOI, COMMENT



La question envoyée à RACF

Open Processing



QUI, QUOI, COMMENT

- Pour opérer ce contrôle le gestionnaire de la ressource transmet à RACF :

1. L'identification de l'utilisateur : QUI
2. Le nom de la ressource visée : QUOI
3. Le type d'accès envisagé : COMMENT

- Exemple :

* QUI : USER1

* QUOI : nom d'un fichier

* COMMENT : une première indication est donnée dans OPEN à savoir

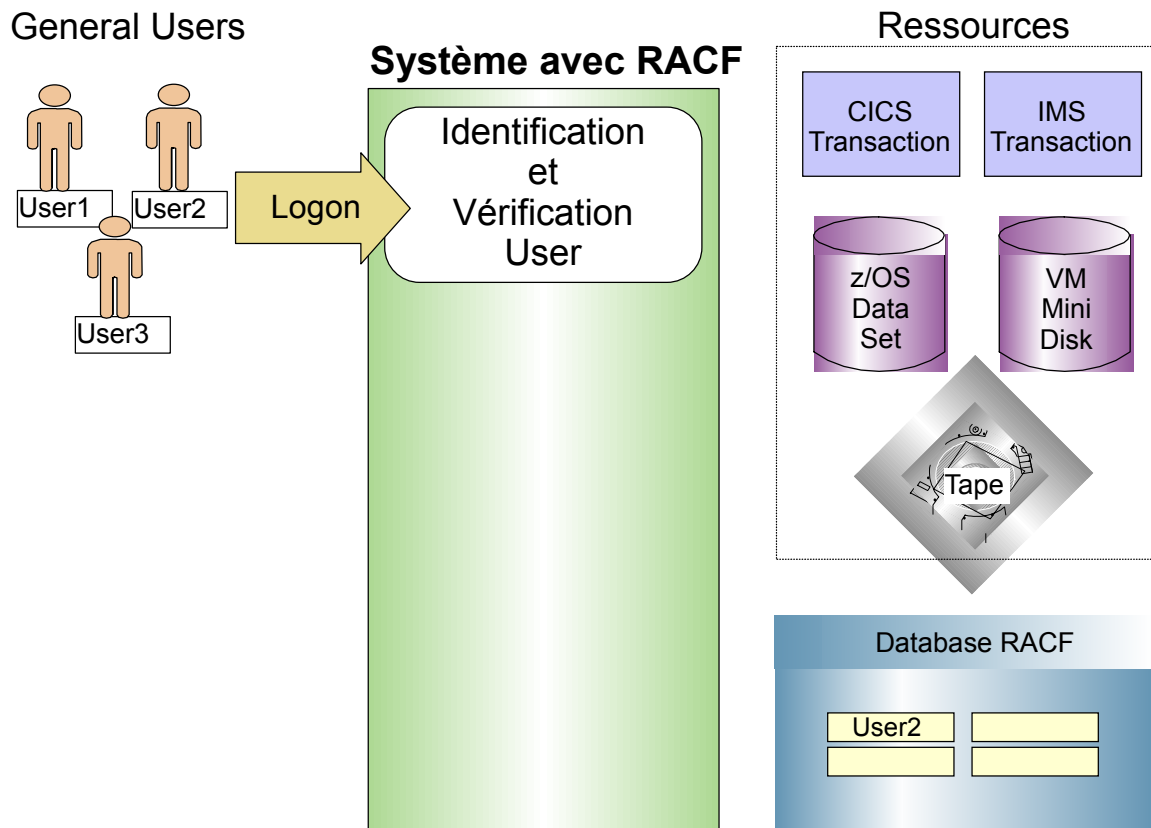
✓ INPUT = lire

✓ OUTPUT = écrire

✓ d'autre part, dans le JCL, le paramètre DISP, donne une seconde information : le traitement à faire en fin de step/job, éventuellement DELETE soit détruire.

La question envoyée à RACF

Authentification User



QUI

- Un "USER" est un objet informatique qui fait des demandes de services à un système d'information

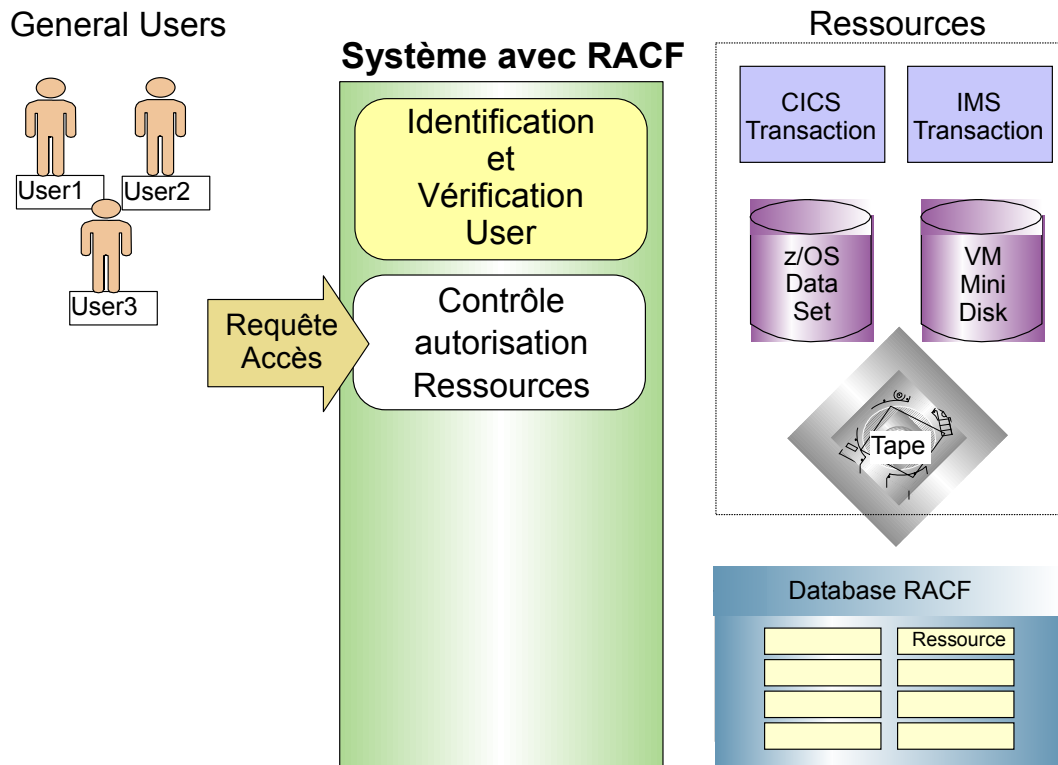
- Exemple :

- * Un utilisateur demandant l'accès à une ressource contrôlée par RACF sera identifié à RACF par un "USERID". Ce "USERID" est normalement contrôlé par RACF à son entrée dans le système :
 - ✓ TSO:LOGON
 - ✓ CICS, IMS, DB2, NETVIEW : SIGNON
 - ✓ BATCH : JES/JCL
 - ✓ "STARTED TASK"

- Un USERID fait toujours partie d'un Groupe
- Un "GROUP" est un ensemble logique de "USERS" qui ont un point commun tel que :
 - * Appartenance à un même service
 - * Appartenance à une même fonction
 - * Appartenance à une même catégorie et qui ont les mêmes besoins d'autorisation sur les mêmes ressources
- Un USERID peut faire partie de plusieurs Groupes
- Les USERIDs et GROUPLDs sont définis par des Profiles dans la Database RACF

La question envoyée à RACF

Contrôle Autorisation Ressources

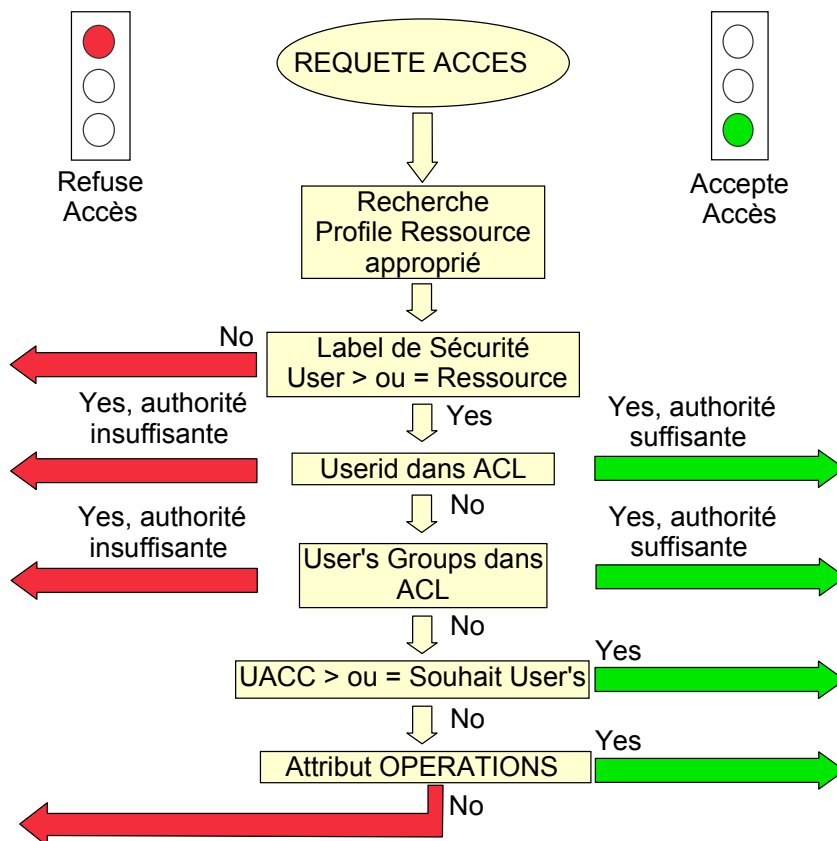


QUOI

- Des Ressources
 - ⊗ décrites par un Profile RACF dont le nom défini dans la DATABASE RACF est composé :
 - ✓ d'un nom de Classe RACF
 - ✓ et d'une entité

La question envoyée à RACF

Contrôle Autorisation Ressources



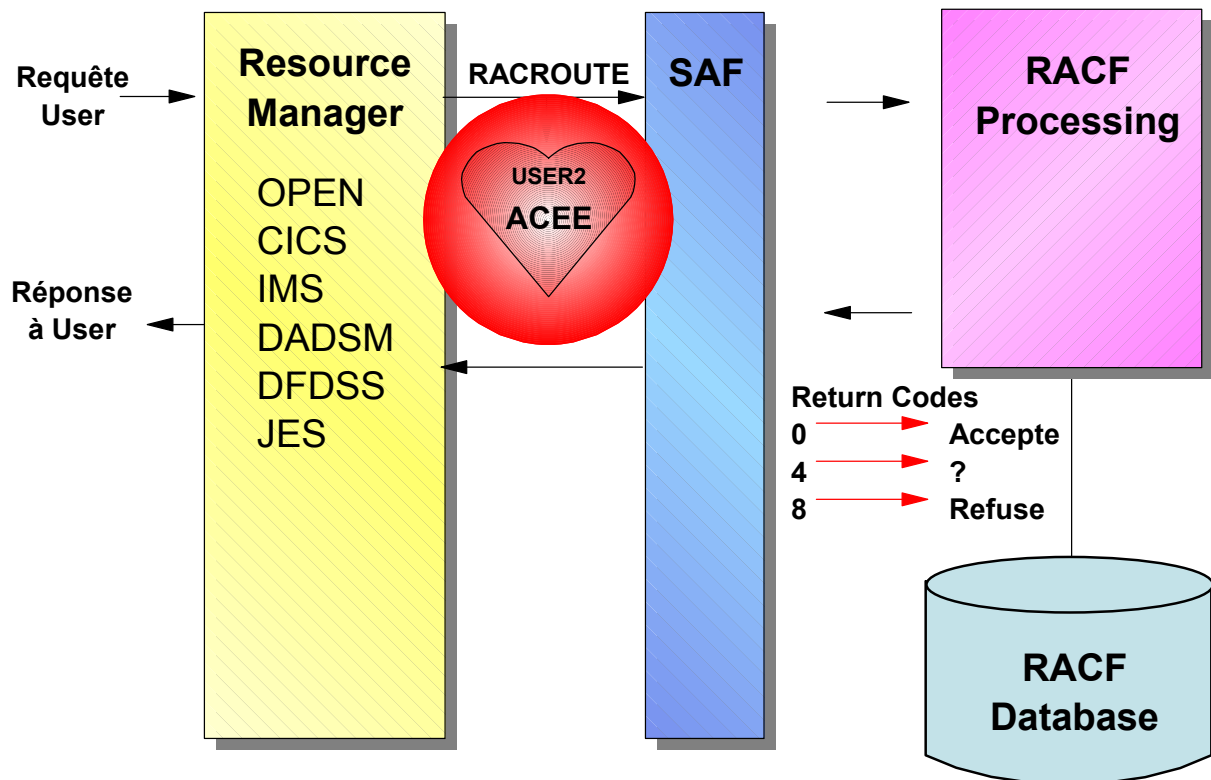
COMMENT

○ Le COMMENT peut être :

- ✓ ALTER
- ✓ CONTROL
- ✓ UPDATE
- ✓ READ
- ✓ EXEC (réservé à la bibliothèque invoquée à partir de la carte JOBLIB ou STEPLIB)
- ✓ NONE
- ✓ ou rien

Relation entre RACF & Système Exploitation

Resource Managers et RACF




- "Resource Manager"
 - * Fournira les paramètres de contrôle lors de l'appel à RACF
 - Soit via la macro RACROUTE d'appel à SAF (System Authorisation Facility)
 - Soit via les macros d'appel direct à RACF
 - ✓ RACDEF
 - ✓ RACHECK
 - ✓ Etc...
- Exemple de "Resource Manager"
 - * "Data Management"
 - OPEN, EOVS, SCRATCH, ...
 - CICS
 - IMS
 - TWS (ex OPC)
 - DB2
 - JES
 - etc...

Description des Objets RACF

Les profiles RACF

User ID	Owner	Password	Attributes	Security Classification	Groups	Segments	
						TSO	OMVS



Encrypted

Profile Name	Owner	UACC	Access List	Security Classification	Auditing
---------------------	--------------	-------------	--------------------	--------------------------------	-----------------

- Il existe des objets RACF décrits dans la BASE RACF appelés "PROFILES"
 - * USERS
 - * GROUPES
 - * RESSOURCES
- Définition des profiles RACF :
 - * Pour opérer ses contrôles RACF utilise sa Base de données dans laquelle il stocke les règles qui lui ont été fournies. Les enregistrements dans le fichier RACF s'appellent "PROFILES"
- Le fichier RACF contient 4 types de PROFILES
 - * User profile
 - * Group profile
 - * Dataset profile
 - * General Resource profile
- Les Fichiers RACF (appelés aussi Database RACF) sont à définir dans une Table RACF : ICHRDSNT
- Un Dataset profile protège les ressources fichiers (disques ou bandes) de l'environnement MVS
- Toute autre ressource est protégée par un General Resource profile

Les pouvoirs



- *Etablir Politique Sécurité*
- *Désigner Responsabilité*
- *Autorité de Délégation*
- *Ressources allouées*
- *Etc . . .*

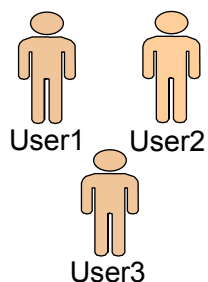
Présentation des Pouvoirs

- Pouvoir Opérationnel
 - * "Le Pouvoir d'accéder"
- Pouvoir Administratif
 - * "Le Pouvoir d'autoriser"
- Pouvoir de Contrôle
 - * Le Pouvoir de voir :
 - ✓ Qui accède ?
 - ✓ Qui autorise ?

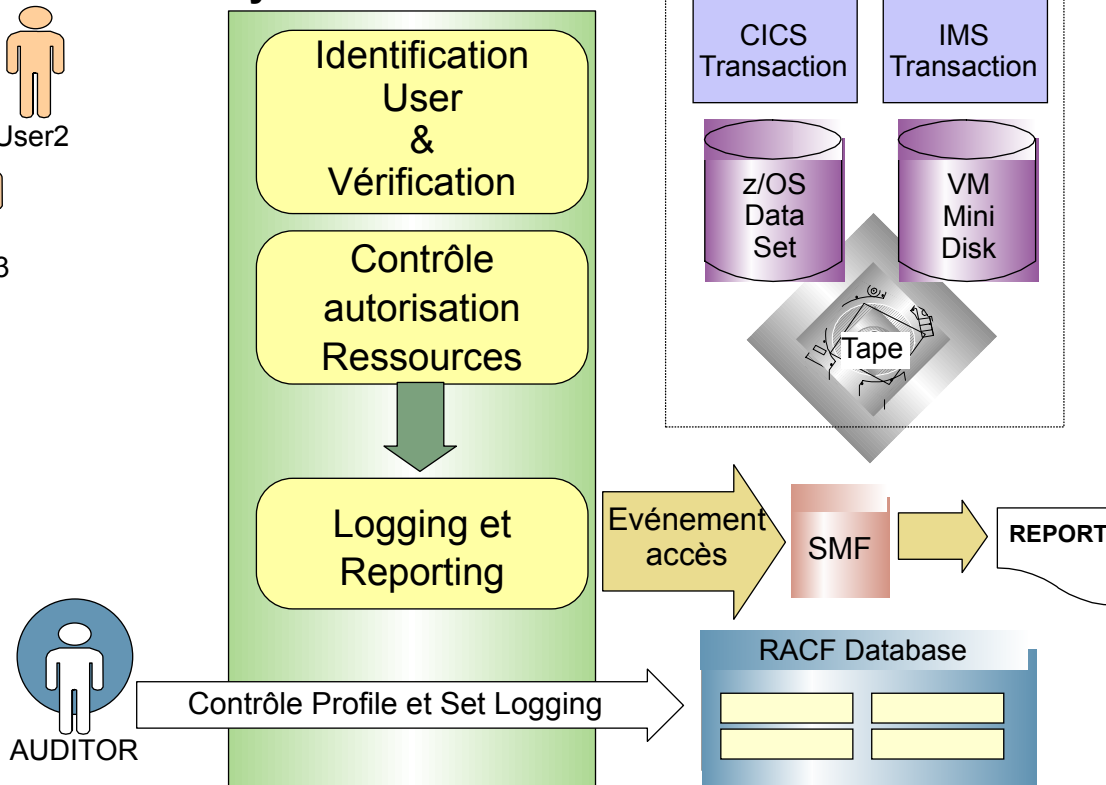
Les pouvoirs

Attribut AUDITOR

General Users



Système avec RACF



Contrôle

✓ **Le Pouvoir de Contrôle ou AUDITING**

C'est le pouvoir de contrôler que les pouvoirs OPERATIONNEL et d'ADMINISTRATION restent conformes aux besoins et aux tâches confiées

✓ **Les privilèges RACF le permettant sont :**

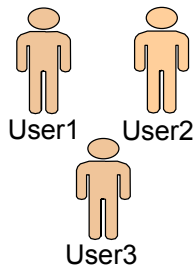
Les attributs AUDITOR ou GROUP- AUDITOR

Remarque : Des outils de contrôle sont fournis dans RACF pour assurer l'Auditing

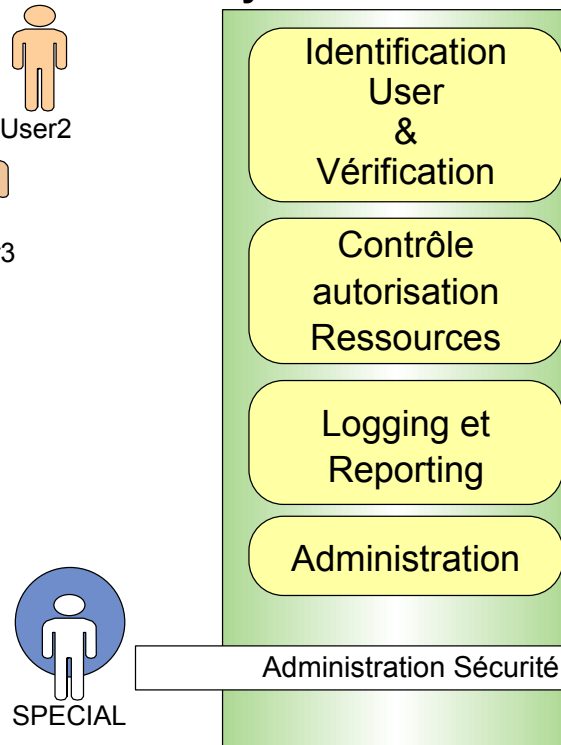
Les pouvoirs

Administration Sécurité

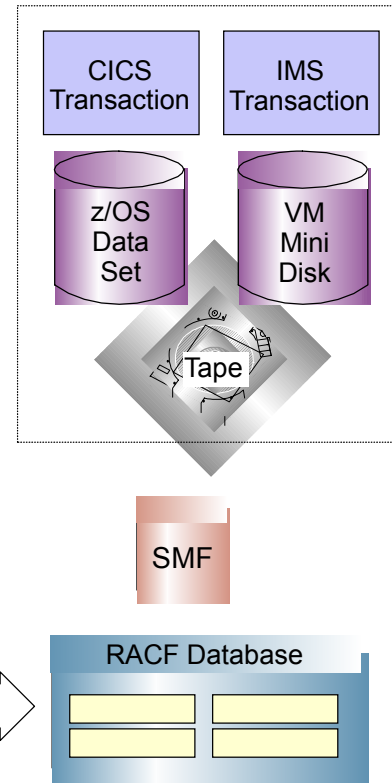
General Users



Système avec RACF



Ressources



Administration

○ Le Pouvoir d'Administration

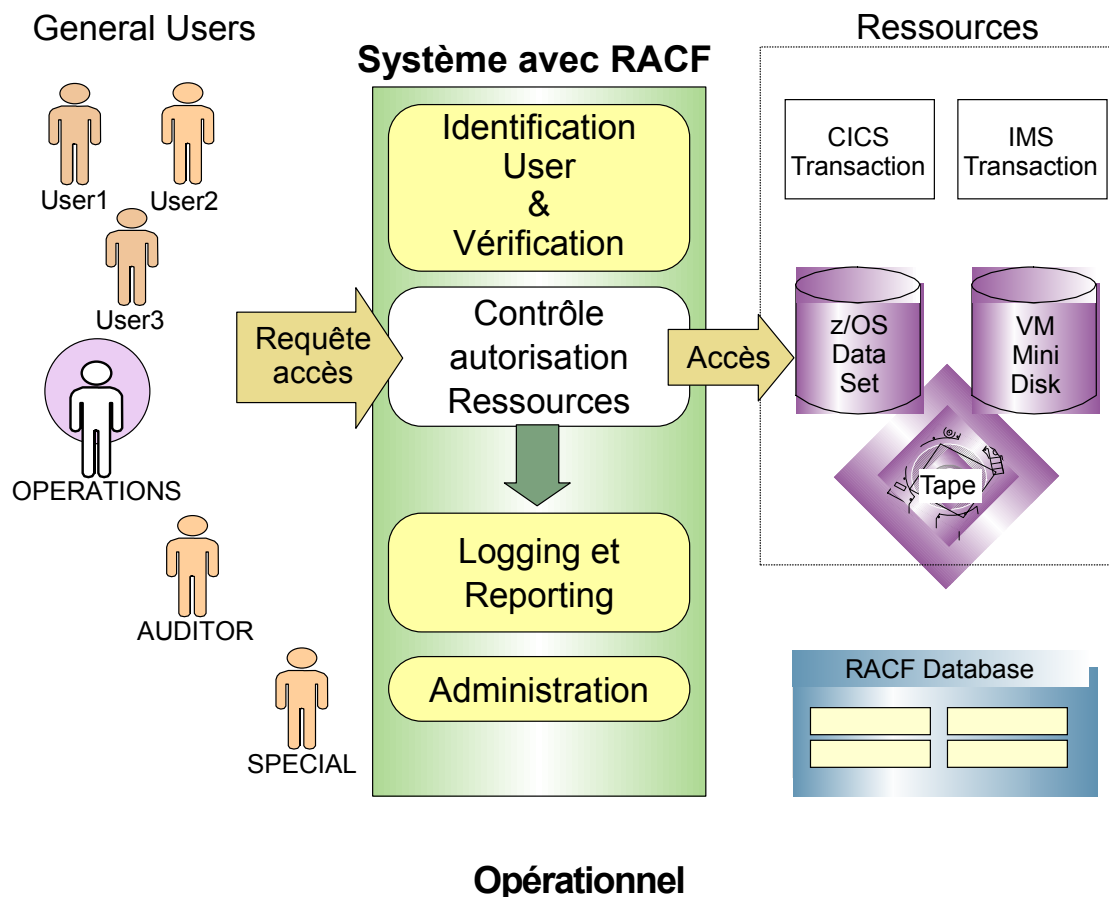
C'est le pouvoir de gérer des Profils RACF (Userids/Groupids/Ressources)

○ Les privilèges RACF le permettant sont :

- ✓ les attributs :
 - SPECIAL ou
 - GROUP-SPECIAL ou
 - CLAUTH (classe(s) de ressource)
- ✓ les autorités groupe de connexion :
 - JOIN ou
 - CONNECT ou
 - CREATE
- ✓ OWNER

Les pouvoirs

Attribut OPERATIONS



○ Le Pouvoir d'Opérationnel

C'est le pouvoir d'agir en utilisant les ressources informatiques, elles-mêmes

○ Les privilèges RACF le permettant sont :

- ✓ les attributs :
 - OPERATIONS ou
 - GROUP-OPERATIONS
- ✓ le niveau d'accès dans la liste d'accès par userid/groupid :
 - ALTER/CONTROL/UPDATE/READ/EXECUTE
- ✓ l'autorité groupe de connexion :
 - USE ou (CREATE/CONNECT/JOIN) pour les accès par groupids
- ✓ les labels de sécurité :
 - SECLABEL/SECLEVEL/CATEGORY

Remarque : le niveau d'accès explicite NONE ou les attributs REVOKE ou GROUP-REVOKE sont des "privilèges" non-opérationnels

Chapitre 2

LES UTILISATEURS : Description et Administration

Présentation

Définir Users et Groups

- ✦ Types Users
 - Users Spéciaux
 - Users Généraux
- ✦ Groups RACF
 - Administration User
 - Administration Ressource
 - Administration Accès
 - Délégation
- ✦ Qui devrait Posséder les Profiles?
- ✦ Centralisé ou Décentralisé?

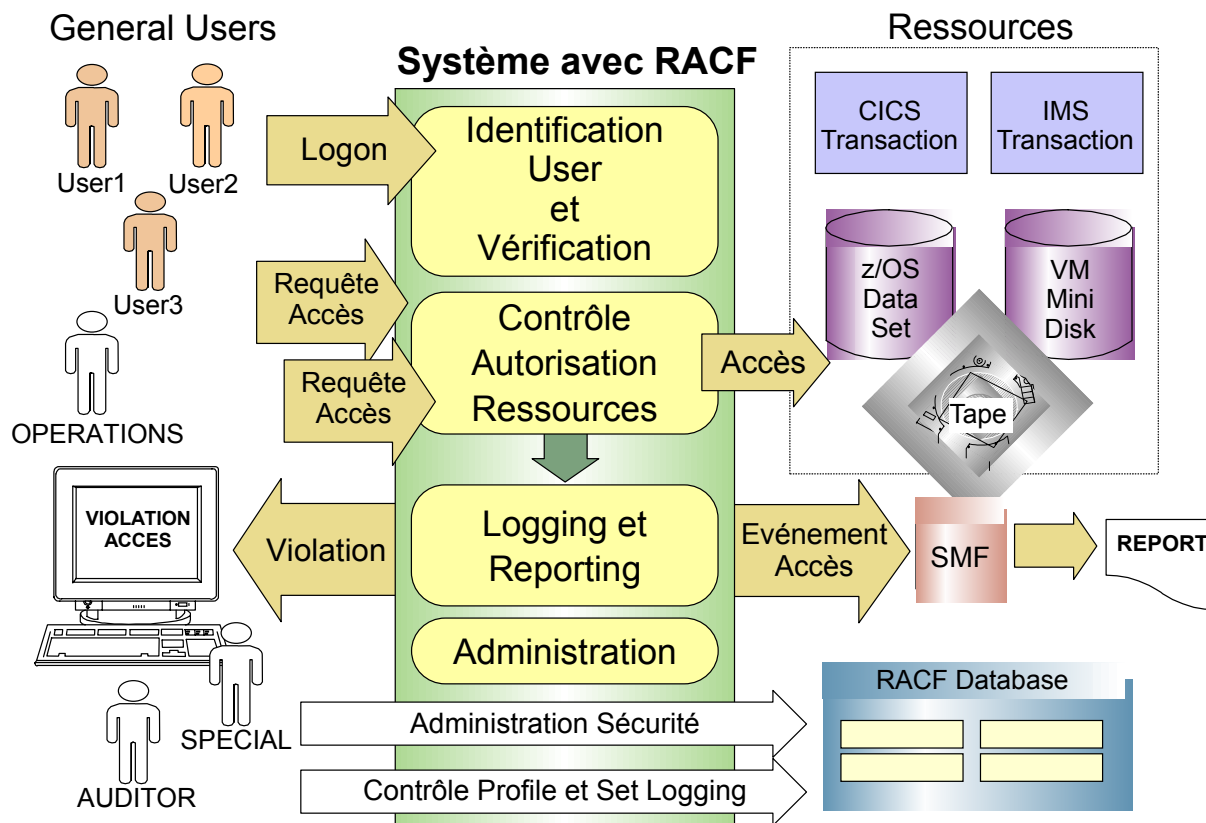


Présentation

- DESCRIPTION
 - Définition d'un utilisateur
 - ✓ USERID - Name - Password - Owner
 - Définition d'un Groupe
 - Définition des UTILISATEURS dans des GROUPES
 - ✓ Default Group - Connect Group - Pouvoirs dans les groupes
 - Notion de Segment
- ADMINISTRATION
 - Définition
 - Champ d'action de cette administration (SCOPE)
 - Résumé des Commandes
 - Exemple de définition d'un groupe fonctionnel d'utilisateurs

Description : USER/GROUP

Types Users

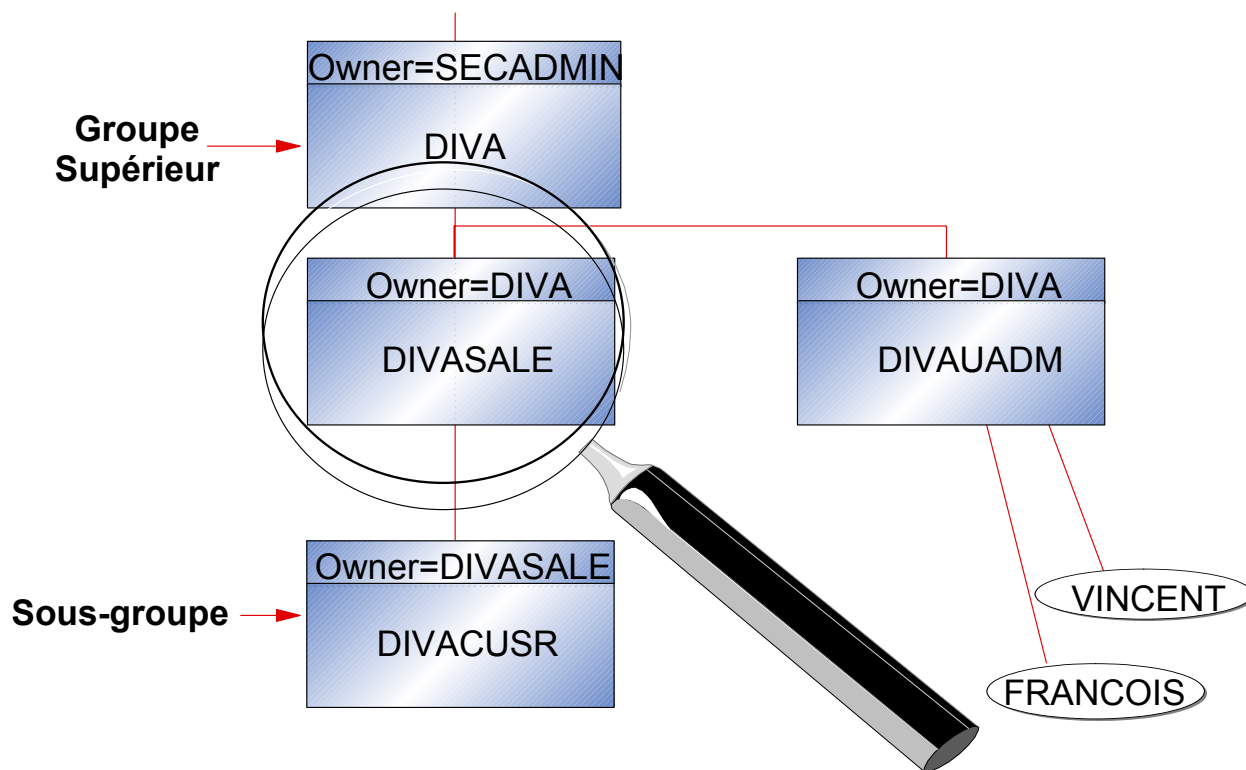


Définition d'un utilisateur

- Une personne qui demande des services à un système d'information
- Le service sera demandé via :
 - ✓ Un JOB batch
 - ✓ Une STARTED TASK
 - ✓ TSO
 - ✓ Une transaction CICS, IMS, DB2, ...

Description : USER / GROUP

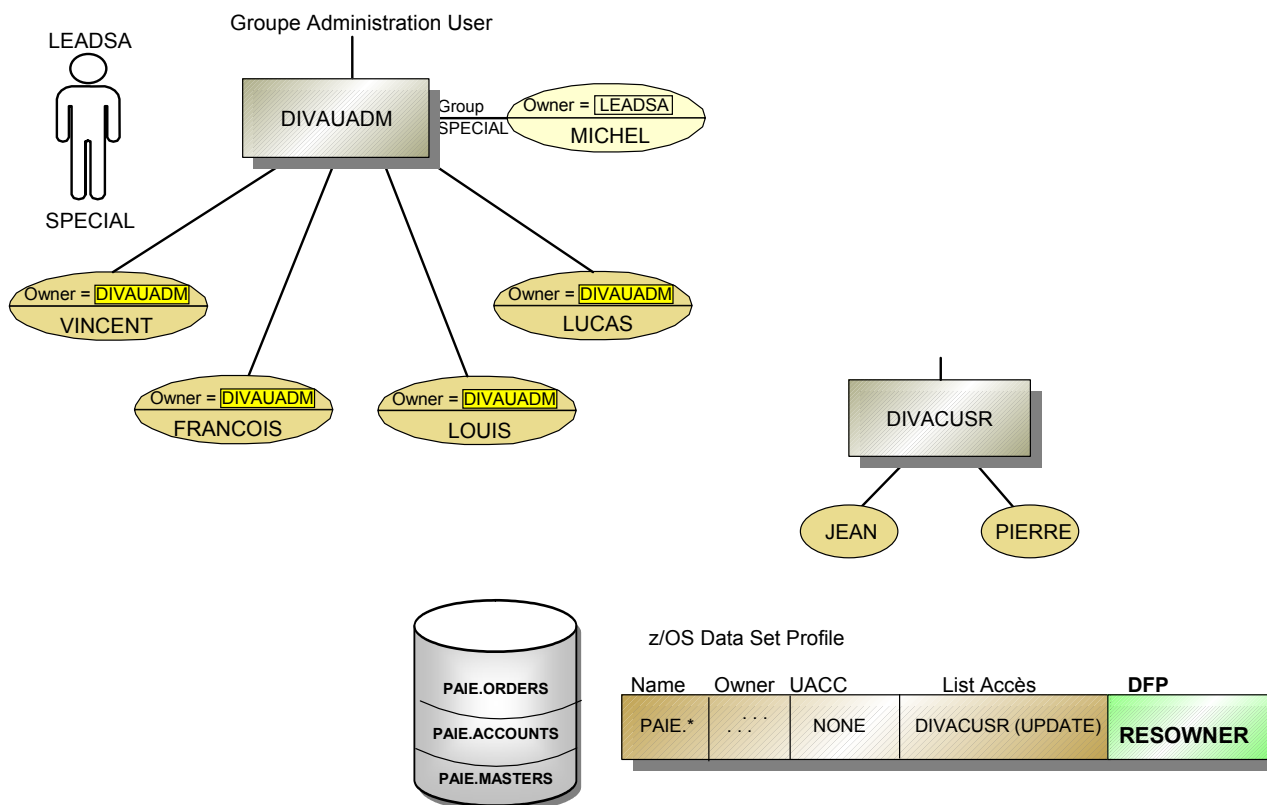
Group RACF



Définition d'un groupe

- Avec RACF un utilisateur travaille TOUJOURS dans le cadre d'un GROUPE.
- Ce qui permet de donner les autorisations au GROUPE plutôt qu'à l'utilisateur.
- Simplification de gestion des autorisations.
- Réalisation d'un cloisonnement entre les fonctions.
- La notion de GROUPE permet de définir un ensemble d'utilisateurs :
 - ✓ Ayant les mêmes besoins
 - ✓ Ayant la même appartenance
 - ✓ d'une même équipe

3 types de groupes



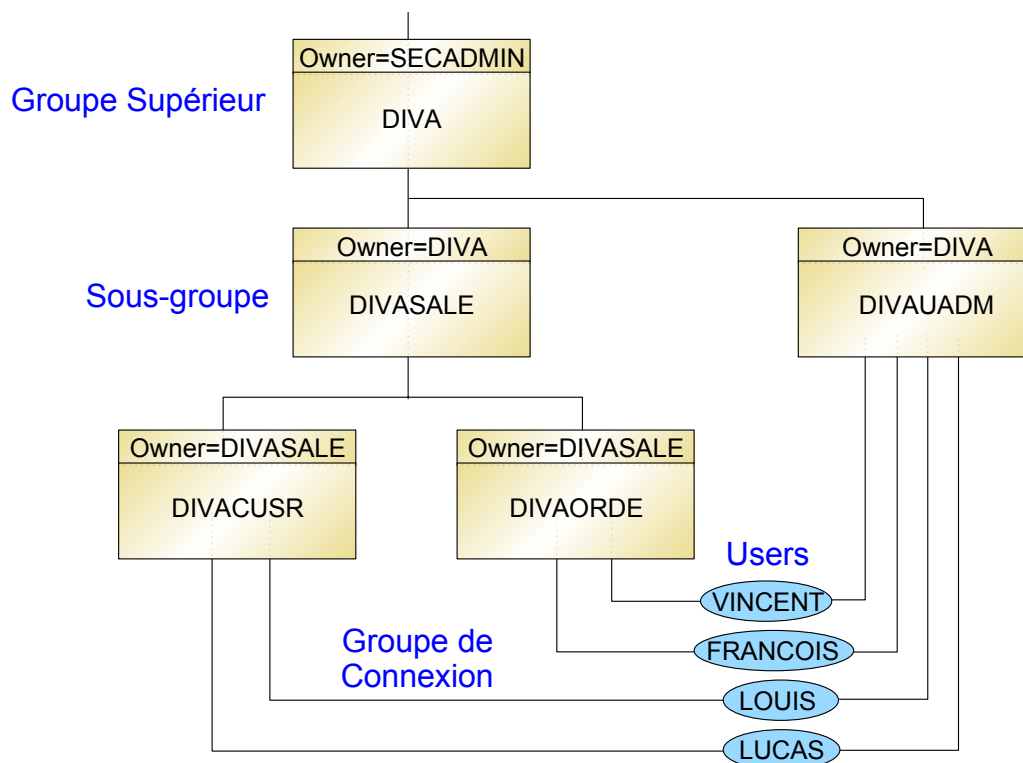
Définition d'un groupe...

1. Groupe fonctionnel rassemblant un ensemble d'utilisateurs ayant la même activité. (Une activité étant définie par le besoin du même niveau d'accès aux mêmes ressources)
2. Groupe de rattachement des fichiers à protéger (notion RACF : tout fichier, pour qu'il soit protégeable par RACF doit avoir comme HLQ soit un GROUPE soit un USERID.
 - Exemples :
 - ✓ Le groupe PAIE est obligatoire pour définir la protection de tous les fichiers ayant comme 1er qualifieur PAIE.
 - ✓ Le userid USER1 est obligatoire pour définir la protection de tous les fichiers ayant comme 1er qualifieur USER1.
3. Groupe de rattachement à un segment DFP afin de fournir les classes SMS à un fichier lors de son allocation (Classes par défaut)

Administration : USER/GROUP...

- Exemple de définition d'un groupe fonctionnel d'utilisateurs

Group RACF



- Les commandes RACF pour définir la structure ci-dessus :

- ✓ AG DIVAUADM SUPGROUP(DIVA) ...
- ✓ AG DIVAORDE SUPGROUP(DIVASALE)
- ✓ AG DIVACUSR SUPGROUP(DIVASALE)
- ✓ AU VINCENT DFLTGRP(DIVAUADM) AUTH(USE)
- ✓ AU FRANCOIS DFLTGRP(DIVAUADM) AUTH(USE)
- ✓ AU LOUIS DFLTGRP(DIVAUADM) AUTH(USE)
- ✓ AU LUCAS DFLTGRP(DIVAUADM) AUTH(USE)
- ✓ CO VINCENT GROUP(DIVAORDE) AUTH(JOIN)
- ✓ CO FRANCOIS GROUP(DIVAORDE) AUTH(JOIN)
- ✓ CO LOUIS GROUP(DIVACUSR) AUTH(USE)
- ✓ CO LUCAS GROUP(DIVACUSR) AUTH(USE)

Chapitre 3

LES RESSOURCES : **Description et Administration**

Définition d'une Ressource à RACF

○ Définition générale

- Une Ressource peut être n'importe quoi à partir du moment où l'on sait la nommer à RACF :
 - ✓ Ressources standards IBM
 - ✓ Ressources clients
- Une Ressource peut être :
 - ✓ Un fichier
 - ✓ Tout autre chose, qui sera appelé: "GENERAL RESSOURCE"
 - Volumes Bandes
 - Terminaux
 - Transactions
 - Programmes
 - Commandes MVS, JES, AMS, DFDSS, ...
 - Etc....

○ Définition d'une Ressource à RACF

- Nom d'une classe
 - ✓ DATASET, TERMINAL, TAPEVOL, DASDVOL, TCICSTRN, TIMS,
- Nom de l'objet ou d'une collection d'objets à l'intérieur d'une classe
- Le propriétaire (OWNER)

○ Cas particulier de définition des Fichiers

- Si le HLQ est un nom de userid : ce userid doit être défini à RACF
- Si le HLQ n'est pas un nom de userid : ce HLQ doit être défini à RACF comme Groupid
 - ✓ Recommandation :
 - Le Groupid HLQ doit être différent des Connects Groups ou du Default Group

Notion de Listes d'accès

- La définition des ressources comporte des autorisations d'accès
 - Implicite : UACC (Universel Access)
 - ✓ Comporte 1 entrée
 - ✓ S'applique aux utilisateurs non définis à RACF ou à ceux non définis explicitement dans la liste d'accès
 - Explicite : Liste d'accès
 - ✓ Comporte 0 ou n entrées
 - ✓ S'applique aux utilisateurs définis à RACF
- Liste d'accès
 - Liste d'accès standard
 - ✓ 1 entrée est définie par :
 - Un nom
 - Une intention d'accès
 - Liste d'accès conditionnel
 - ✓ 1 entrée est définie par :
 - Un nom
 - Une intention d'accès : niveau d'accès
 - Une condition : WHEN

Administration des Ressources

- Faire vivre les descriptions des ressources et de leurs listes définies dans le fichier RACF

- Champ d'action de cette administration
 - Cette administration pourra être :
 - ✓ Soit centralisée
 - ✓ Soit déléguée au niveau d'une fonction/application
 - ✓ Soit au niveau d'un utilisateur

- Résumé des commandes
 - ADDSD (AD), ALTDSD (ALD), DELDSD (DD), LISTDSD (LD)
 - RDEFINE (RDEF), RALTER (RALT), RDELETE (RDEL), RLIST (RL)
 - PERMIT (PE)

Administration des Ressources...

Exemples de définition de Ressources

- ADDSD 'USER1*' UACC(NONE) OWNER(USER1)
- ADDSD 'USER1.**' UACC(NONE) OWNER(USER1)
- ADDSD 'USER1*.COBOL' UACC(NONE)
- ADDSD 'SYS1.MACLIB' GEN UACC(READ) OWNER(GSYS)
- ADDSD 'PAIE.PROD.*' UACC(NONE) OWNER(GPROD)

- RDEF TERMINAL TERM* UACC(NONE)
- RDEF TERMINAL TERM1 UACC(NONE) WHEN(DAYS(DAYS) TIME(11:2000)
- RDEF TERMINAL TERM2 UACC(NONE) WHEN(DAYS(DAYS) TIME(11:2000) TIMEZONE(W,3)

- RDEF OPERCMDS JES2.** UACC(NONE)
- RDEF TCICSTRN TR* UACC(NONE)
- RDEF GCICSTRN GTRN1 ADDMEM(TR03 CEDF CEDA) UACC(NONE)

Exemples de définition de Listes d'accès

- PE 'USER1.*' ID(USER2) ACC(READ)
- PE 'USER1.**' ID(USER2) ACC(READ)
- PE 'USER1ACOBOL' ID(USER2) ACC(READ)
- PE 'SYS1.MACLIB' GEN ID(USER2) ACC(UPDATE)
- PE 'PAIE.PROD.*' ID(GPROD) ACC(UPDATE) WHEN(PROGRAM(PROGPAIE))

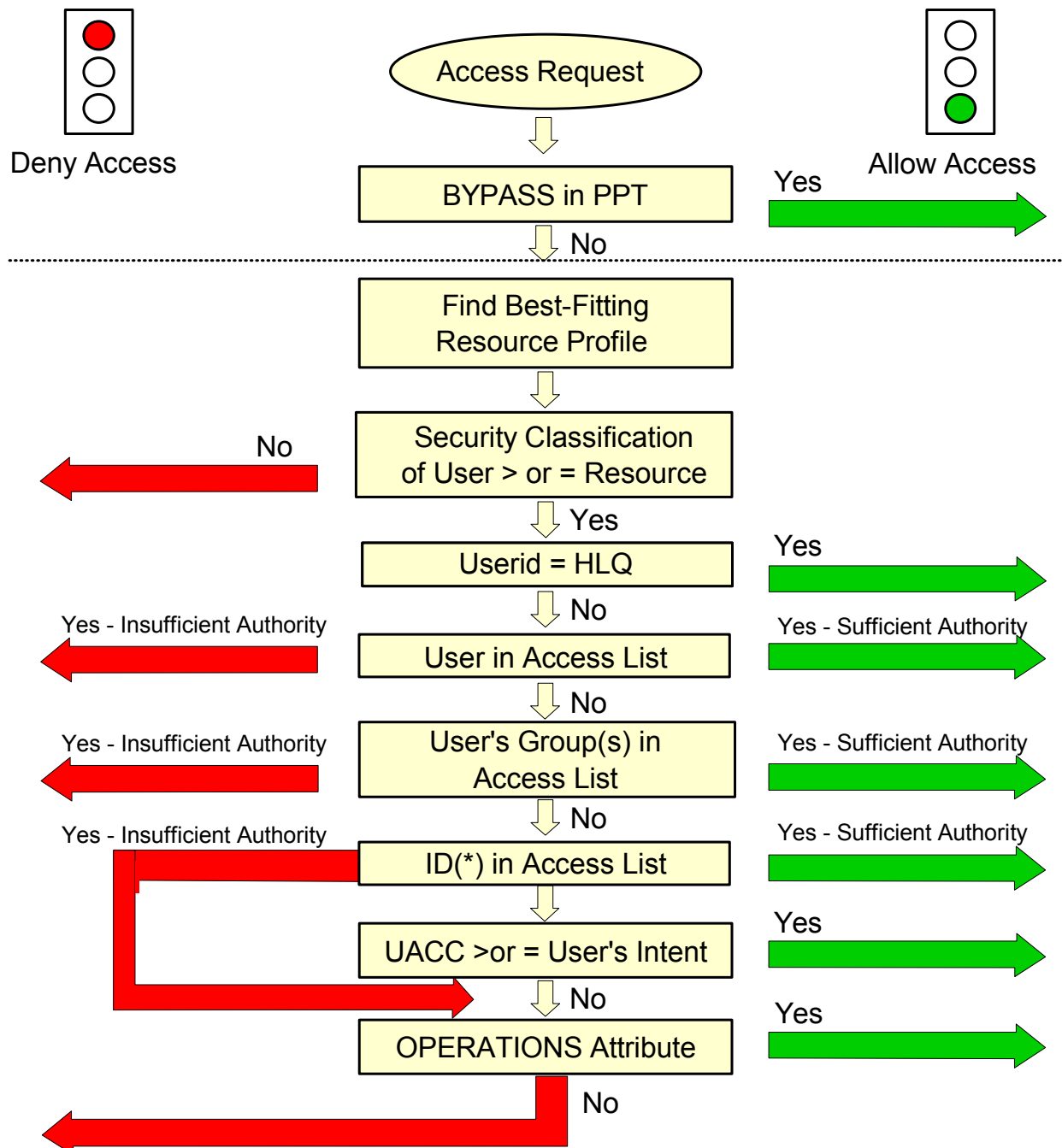
- PE CLASS(TERMINAL) TERM1 ID(USER2) ACC(USFR2)

- PE JES2.** CLASS(OPERCMDS) ID(USER2) ACC(READ) WHEN(JESINPUT(INTRDR))
- PE TR* CLASS(TCICSTRN) ID(GUSERS) ACC(READ)
- PE GTRN1* CLASS(GCICSTRN) ID(ADMCICS) ACC(READ)

Chapitre 4

RELATION entre UTILISATEURS et RESSOURCES

Contrôle d'autorisation simplifié à l'OPEN du Fichier





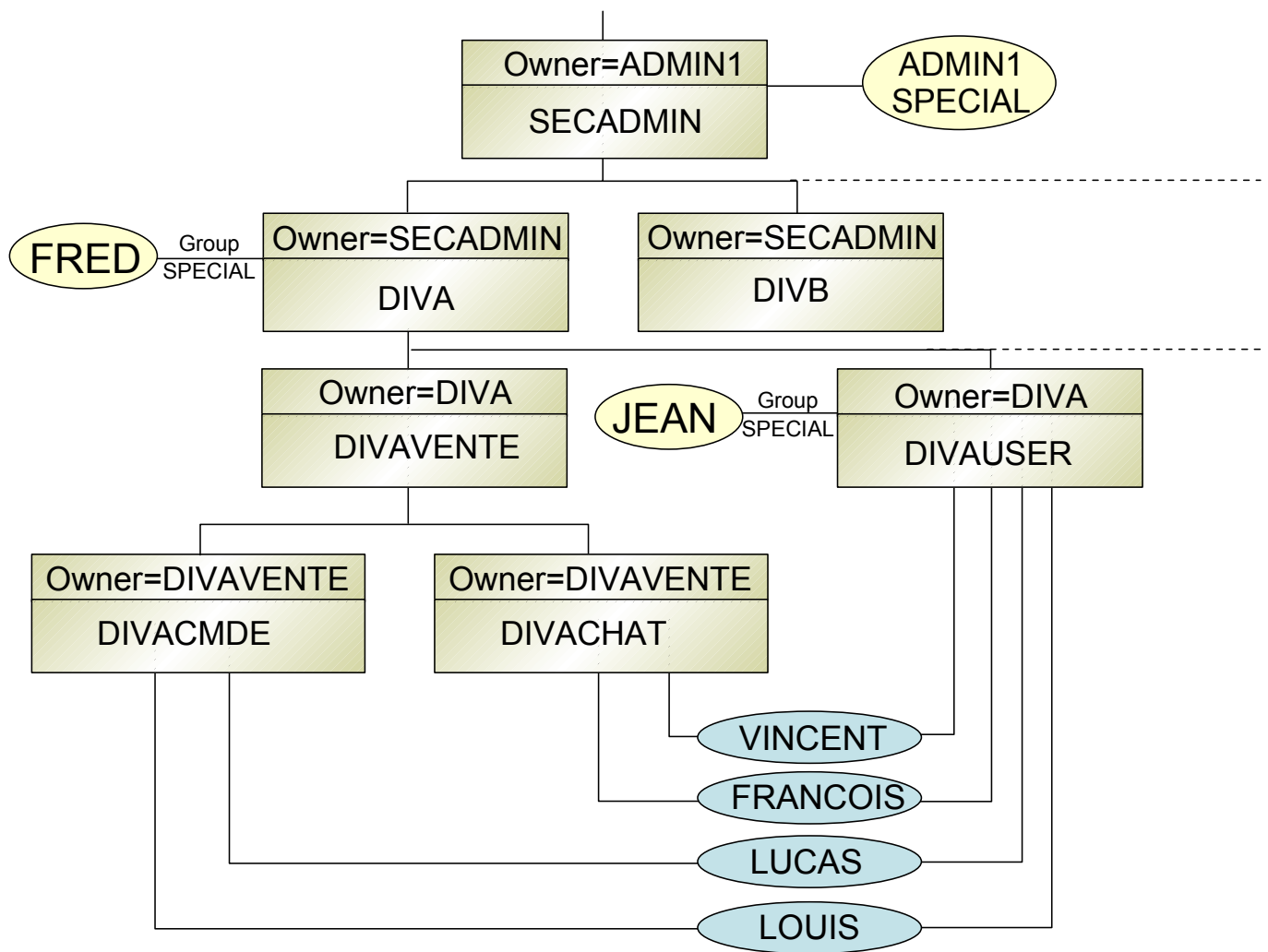
NOTES :

Chapitre 7

ADMINISTRATION et DELEGATION

Champ de contrôle d'un attribut de délégation

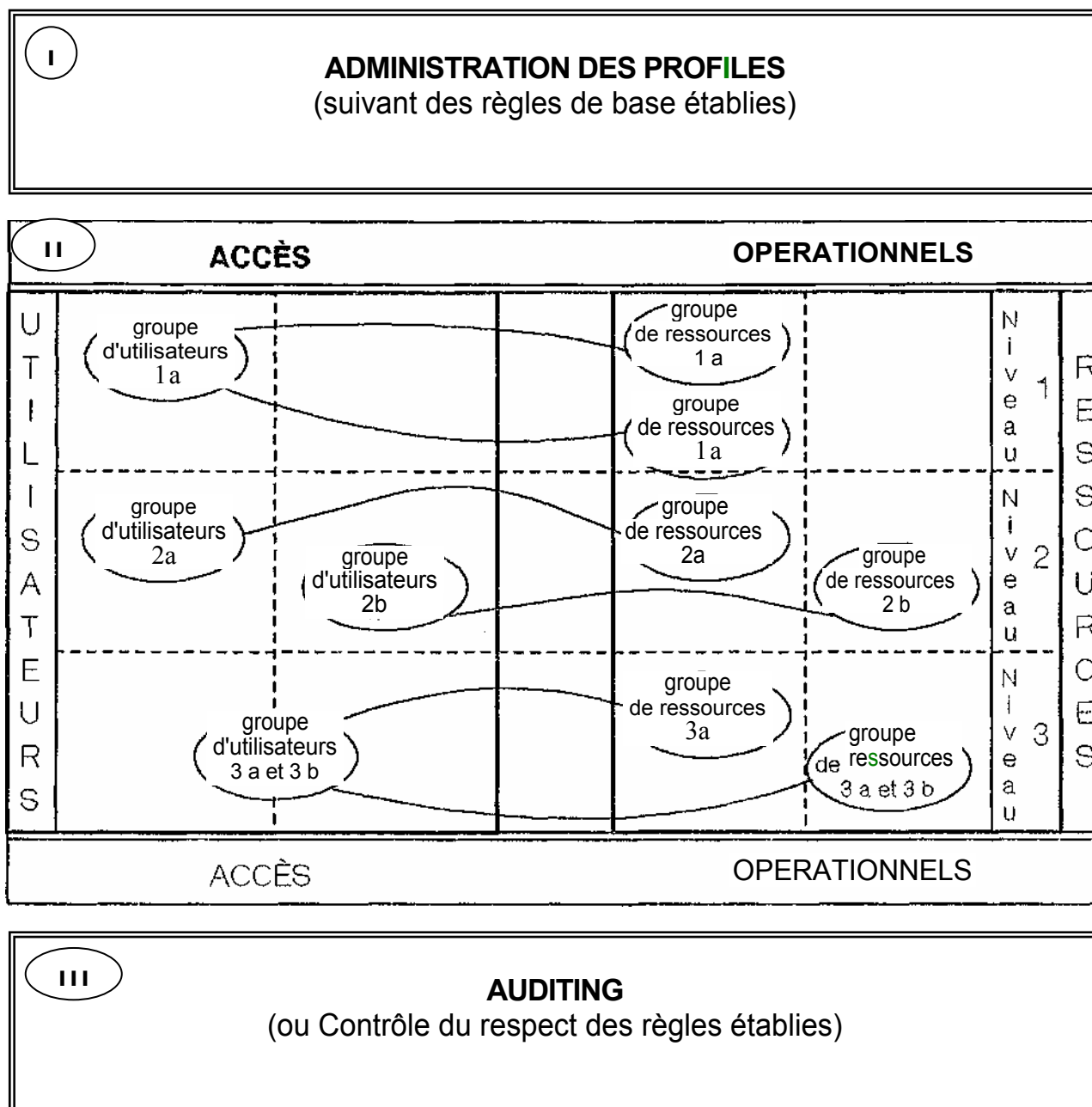
Attribut : GROUP-SPECIAL



Chapitre 8

LOGGING et AUDITING

1 - Séparation des pouvoirs



2 - L'Auditeur : son rôle et ses outils de contrôle

- L'Auditeur des données informatiques a pour charge :
 - ☆ de contrôler que
 - l'accès aux ressources
 - et l'administration des profilesest conforme par
 - un **logging** sélectif
 - et un **checking** systématique ou aléatoire
 - ☆ et, éventuellement, de fournir au management ou aux propriétaires de ressources des informations (**reporting**)
 - sur les violations d'accès aux systèmes ou aux ressources
 - sur les userids, leurs privilèges, leurs changements
 - sur les ressources, les accès effectués, les protections en place effectivement, leurs changements
- L'Auditeur central dispose :
 - ☆ d'un attribut privilégié : AUDITOR
 - pour mettre en place, dans la database RACF, les options de logging
 - et consulter tout profile de la database RACF
 - ☆ et d'outils de contrôle:
 - le RACF Report Writer (RACFRW)
 - le Data Security Monitor (DSMON)
 - l'utilitaire IRRUT100 / ICHUT100
 - les commandes RACF (la commande SR, particulièrement)

Remarque : l'attribut GROUP-AUDITOR permet à un auditeur de groupes d'assurer le contrôle des profiles se trouvant dans son champ de contrôle (portée groupes)

3 - Le Logging

○ Logging système : Logging automatique

- ☆ RVARV
- ☆ SETROPTS
- ☆ RACINIT
 - LOGON
 - JOB
- ☆ des accès garantis aux fichiers par l'opérateur à la console lors d'un traitement en "FAILSOFT PROCESSING"

○ Logging utilisateur : Logging sous contrôle d'options activées par la Cde RACF : SETROPTS

- ☆ LOGOPTIONS(
 - ALWAYS(class-name),
 - NEVER(class-name),
 - SUCCESSES(class-name),
 - FAILURES(class-name),
 - DEFAULT(class-name))
 - Chaque classe ne pouvant avoir qu'un niveau d'audit, les niveaux d'audit sont traités dans l'ordre suivant :
 1. ALWAYS
 2. NEVER
 3. SUCCESSES
 4. FAILURES
 5. DEFAULT
- ☆ SAUDIT / NOSAUDIT
- ☆ SECLEVELAUDIT(security-level) / NOSECLEVELAUDIT
- ☆ OPERAUDIT / NOOPERAUDIT
- ☆ CMDVIOL / NOCMDVIOL
- ☆ AUDIT(class-name/*) / NOAUDIT(class-name/*)

3 - Le Logging...

- L'Auditeur, grâce à son attribut privilégié (AUDITOR ou GROUP-AUDITOR) peut mettre en place, modifier, rafraîchir en mémoire les options de logging :

Commandes RACF	Options de Logging	Commentaires	Attributs RACF nécessaires
SETROPTS (SETR)	AUDIT(classe,...)	logging des profils modifiés	AUDITOR
	SAUDIT	logging de l'activité des userids ayant SPECIAL ou GROUP-SPECIAL	
	OPERAUDIT	logging de l'activité des userids ayant OPERATIONS ou GROUP-OPERATIONS	
	CMDVIOL	logging des commandes RACF ayant échoué par insuffisance d'autorisation	
	SECLABELAUDIT (seclabel)	logging des accès sur les ressources de ce Seclabel	
	LOGOPTIONS (ALWAYS/NEVER/SUCCESS/FAILURES/DEFAULT (classe,...))	logging sur la base de la classe de ressources	
	REFRESH RACLIST/GENLIST (classe,...)	rafraîchissement en mémoire commune de profils discrets ou uniquement génériques	AUDITOR ou SPECIAL ou CLAUTH (...)
	REFRESH GENERIC	rafraîchissement en mémoire de profils génériques (classe DATASET)	SPECIAL ou AUDITOR ou GROUP-AUDITOR/-SPECIAL et profils dans la portée
ALU	UAUDIT	logging de l'activité d'un userid spécifique	AUDITOR ou GROUP-AUDITOR pour un userid ou une ressource dans le champ de contrôle (portée)
ALD ou RALT	GLOBALAUDIT (ALL/FAILURES/SUCCESS/NONE (niveau d'accès),...)	logging d'accès aux ressources suivant : - le type d'accès (réussi ou non) - et le niveau d'accès	

Remarque : la commande : SETR LIST permet de lister les options globales RACF.
Elle peut être lancée par un userid ayant l'un des attributs :
SPECIAL / AUDITOR / GROUP-SPECIAL / GROUP-AUDITOR

3 - Le Logging...

- Le Logging se fait dans les fichiers SMF et des enregistrements spécifiques SMF/RACF sont créés :

Enregistrement SMF / RACF	Cas de création des enregistrements	Contenu des enregistrements
81	<ul style="list-style-type: none"> ● à l'initialisation de RACF 	<ul style="list-style-type: none"> ● date et heure ● identification du processeur ● nom de chaque fichier RACF ● options globales de RACF
80	<ul style="list-style-type: none"> ● lors d'un accès non autorisés au système (mauvais password, mauvais groupe ou terminal non autorisé) ● lors d'un accès autorisé ou non autorisé à une ressource protégée par RACF ● lors d'une modification autorisée ou non autorisée de profile RACF ● lors de l'utilisation des commandes RACF : SETR et RVAR 	<ul style="list-style-type: none"> ● date et heure ● identification du processeur ● code événement <ul style="list-style-type: none"> • accès au système • accès à une ressource protégée par RACF • utilisation d'une commande RACF ● userid ● groupid ● autorité utilisée pour accès à la ressource ou exécution de la commande ● raison du logging ● terminal ● jobname
83	<ul style="list-style-type: none"> ● lorsqu'un changement de SECLABEL affecte des fichiers protégés catalogués par les commandes RACF: AD ou ALD ou DD 	<ul style="list-style-type: none"> ● date et heure ● identification du processeur ● commande RACF (AD, ALD, DD) ● liste des fichiers catalogués affectés par SECLABEL changé

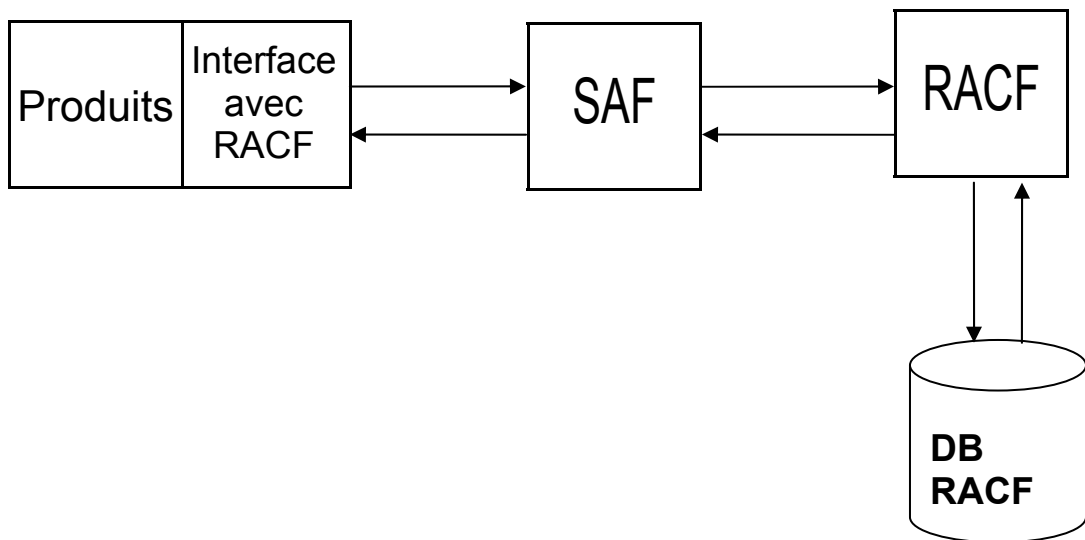
- Remarque :

☆ les commandes suivantes ne donnent pas lieu à logging LG, LU, LD, RL, SR, LDIR, SRDIR, LF, SRFILE

Chapitre 9

Relation avec les autres produits

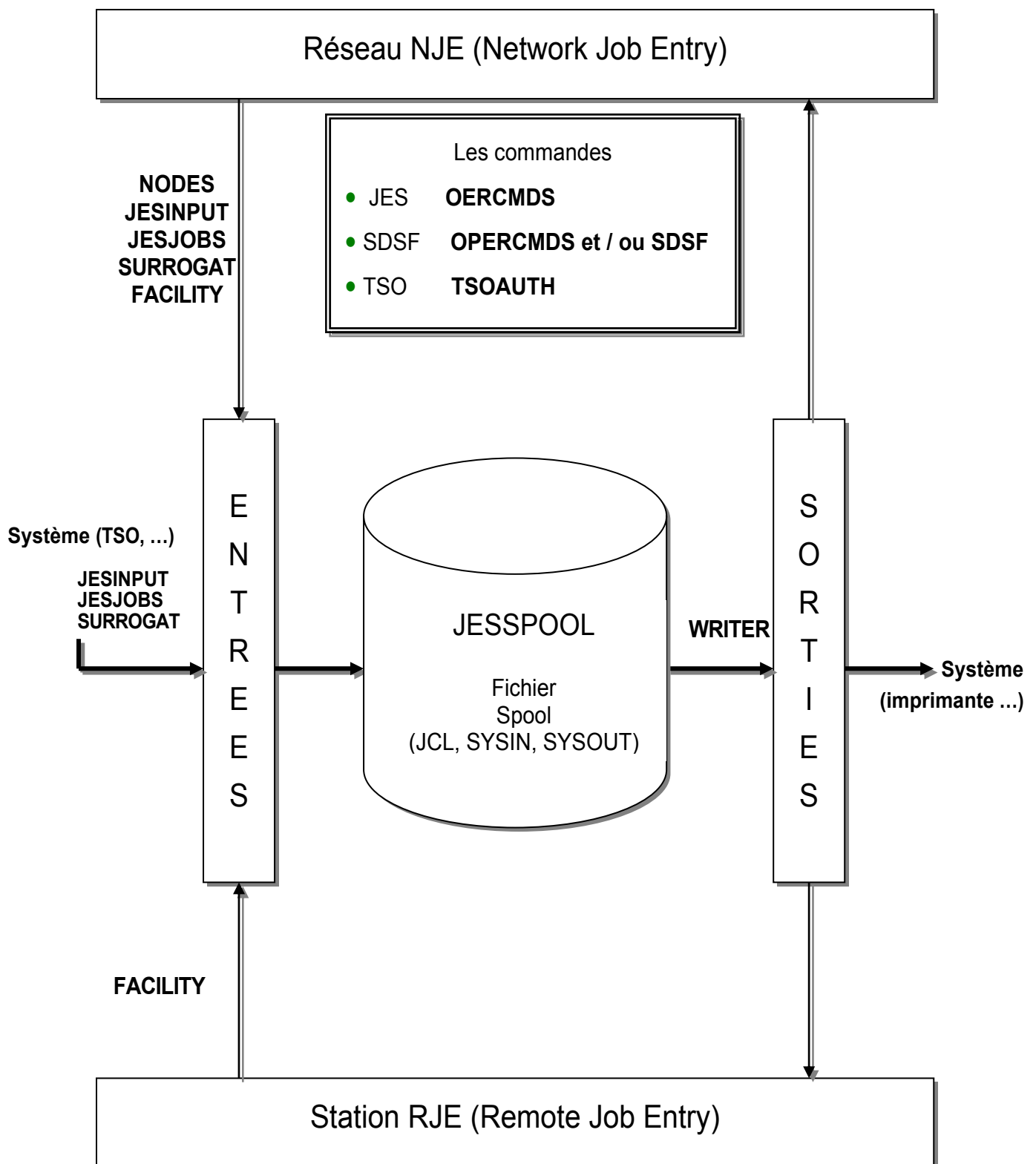
Schéma de principe



Définitions

- Produits avec interface implicite :
 - ☆ Rien à définir dans le produit
 - ☆ Définir dans RACF :
 - Les ressources à protéger et les autorisations
 - Les classes de ressources à contrôler
- Produits avec interface explicite :
 - ☆ Définir dans le produit : des paramètres, éventuellement des exits
 - ☆ Définir dans RACF :
 - Les ressources à protéger et les autorisations, en relation avec les paramètres définis dans le produit
 - Les classes de ressources à contrôler

1 – Vue générale



CONCLUSION

Concernant le produit à sécuriser

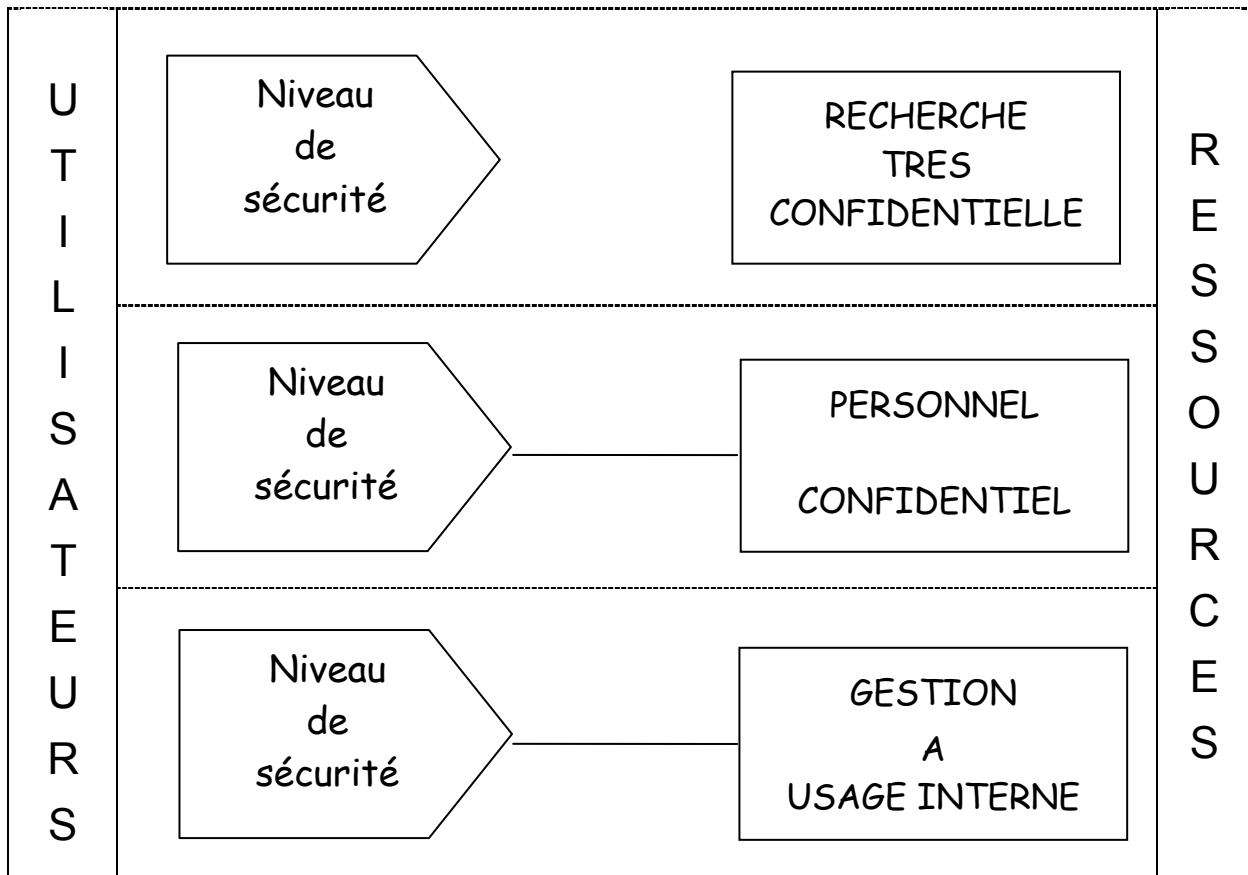
- Lire la documentation relative au produit pour s'assurer :
 - ☆ qu'il y a bien l'interface avec RACF
 - ☆ s'il y a des tables ou exit ou options à activer

- Dans RACF :
 - ☆ Définir les profils des différentes Ressources utilisées par le produit, en utilisant UACC = NONE
 - ☆ Définir les listes d'accès sur les Ressources
 - ☆ Activer les Classes de Ressources RACF utilisées par le produit

Chapitre 10

Extension des Contrôles : Les Labels de Sécurité

" Multi Level Security "



- Un même système informatique gère des ressources de différents **niveaux de sensibilité**.
- c'est à dire qu'un système est "multi level security".
- **L'isolation**
 - ☆ qui était hardware (autant de machines que de niveaux de sensibilités des ressources).
 - ☆ sera Software : le label de sécurité.

DAC - MAC

- Compte tenu de la grande quantité de ressources informatiques sous contrôle d'un système, on voudrait éviter qu'un Utilisateur autorisé d'accès sur une ressource d'un certain niveau de sécurité ne cède, on line, une telle ressource à un autre utilisateur non autorisé d'accès
- **Discretionary Accès Control**
 - ☆ Or, le contrôle par les listes d'accès des ressources ne le permet pas. En effet, un utilisateur autorisé, en READ, sur un fichier peut envoyer ce fichier à un autre utilisateur, non autorisé. Le contrôle par listes d'accès est à la discrétion de l'utilisateur autorisé.
- **Mandatory Access Control**
 - ☆ Pour empêcher, on line, un utilisateur, autorisé d'accès sur une ressource, de donner cette ressource à un utilisateur non autorisé, il existe un autre type de contrôle d'accès, basé sur les Labels de Sécurité associés :
 - au userid demandant l'accès au système
 - et aux ressources informatiques du système.

Norme

- Depuis quelques années, le Département de la Défense des Etats-Unis a établi :
 - ☆ pour des systèmes informatiques (Trusted Computer Base)
 - ☆ des niveaux de sécurité, reconnus de plus en plus :

					A1	Niveau de sécurité le plus élevé
					B3	
				B2		
			B1			
		C2				
	C1					
D						Niveau de sécurité le moins élevé

- A partir de RACF 1.9, un système informatique peut atteindre le niveau B1 de sécurité, ce qui implique l'obligation
 - ☆ de produits programmes garantis ("trusted")
 - ☆ de configurations systèmes et unités sûres
 - ☆ pour les userids et les ressources d'avoir des labels de sécurité
 - ☆ d'identification et authentification par RACF de tout user
 - ☆ de contrôle d'accès aux ressources à la fois MAC et DAC
 - ☆ d'auditing spécifique
- Aux Etats-Unis, il existe un organisme, le National Computer Security Center pour tester et garantir le niveau de sécurité des produits programmes.

Ainsi, à partir de RACF 1.9, MVS 313, TSO/E 2.2, VTAM 3.3, PSF 1.3, DFP 3.1 ont été développés en collaboration avec le NCSC pour garantir un système informatique au niveau de sécurité B1

Classe SECLABEL

- Un label de sécurité (SECLABEL) est l'association
 - ☆ d'un niveau de sécurité (SECLEVEL) spécifique
 - ☆ avec un ensemble (de zéro ou plusieurs) catégorie(s) (CATEGORY)
- Les seclabels permettront d'éviter la déclassification des informations

