VisualAge Pacbase 2.5

INTERFACE SYSTEMES DE SECURITE
MANUEL DE REFERENCE

DDSEC000151F

Remarque

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à la section "Remarques" de la page suivante.

En application de votre contrat de licence, vous pouvez consulter ou télécharger la documentation de VisualAge Pacbase, régulièrement mise à jour, à partir du site Web du Support Technique :
http://www.software.ibm.com/ad/vapacbase/support.htm

La section Catalogue dans la page d'accueil de la Documentation vous permet d'identifier la dernière édition disponible du présent document.

Première Edition (Mai 1996)

La présente édition s'applique à :

- VisualAge Pacbase Version 2.0
- VisualAge Pacbase Version 2.5

Vous pouvez nous adresser tout commentaire sur ce document (en indiquant sa référence) via le site Web de notre Support Technique à l'adresse suivante :
http://www.software.ibm.com/ad/vapacbase/support.htm
ou en nous adressant un courrier à :
IBM Paris Laboratory
Support VisualAge Pacbase
30, rue du Château des Rentiers
75640 PARIS Cedex 13
FRANCE

IBM pourra disposer comme elle l'entendra des informations contenues dans vos commentaires, sans aucune obligation de sa part.

REMARQUES

Ce document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM. Cela ne signifie pas qu'IBM ait l'intention de les annoncer dans tous les pays où la compagnie est présente.

Toute référence à un produit, logiciel ou service IBM n'implique pas que seul ce produit, logiciel ou service puisse être utilisé. Tout autre élément fonctionnellement équivalent peut être utilisé, s'il n'enfreint aucun droit d'IBM.

Il est de la responsabilité de l'utilisateur d'évaluer et de vérifier lui-même les installations et applications réalisées avec des produits, logiciels ou services non expressément référencés par IBM.

IBM peut détenir des brevets ou des demandes de brevet couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous donne aucun droit de licence sur ces brevets ou demandes de brevet. Si vous désirez recevoir des informations concernant l'acquisition de licences, veuillez en faire la demande par écrit à l'adresse suivante :

Intellectual Property and Licensing
International Business Machines Corporation
North Castle Drive, Armonk, New-York 10504-1785
USA

Les détenteurs de licences du présent produit souhaitant obtenir des informations sur celui-ci à des fins : (i) d'échange d'informations entre des programmes développés indépendamment et d'autres programmes (y compris celui-ci) et (ii) d'utilisation mutuelle des informations ainsi échangées doivent s'adresser à :

IBM Paris Laboratory
Département SMC
30, rue du Château des Rentiers
75640 PARIS Cedex 13
FRANCE

De telles informations peuvent être mises à la disposition du Client et seront soumises aux termes et conditions appropriés, y compris dans certains cas au paiement d'une redevance.

IBM peut modifier ce document, le produit qu'il décrit ou les deux.

MARQUES

IBM est une marque d'International Business Machines Corporation, Inc.
AIX, AS/400, CICS, CICS/MVS, CICS/VSE, COBOL/2, DB2, IMS, MQSeries, OS/2, PACBASE, RACF, RS/6000, SQL/DS, TeamConnection et VisualAge sont des marques d'International Business Machines Corporation, Inc. dans certains pays.

Java et toutes les marques et logos incluant Java sont des marques de Sun Microsystems, Inc. dans certains pays.
Microsoft, Windows, Windows NT et le logo Windows sont des marques de Microsoft Corporation dans certains pays.
UNIX est une marque enregistrée aux Etats-Unis et/ou dans d'autres pays et utilisée avec l'autorisation exclusive de la société X/Open Company Limited.

D'autres sociétés peuvent être propriétaires des autres marques, noms de produits ou logos qui pourraient apparaître dans ce document.

TABLE DES MATIERES

1. INTERFACE PACBASE - RACF OU TOPSECRET

1.1. INTRODUCTION

INTRODUCTION

Un système de sécurité assure les contrôles des codes utilisateur et de leur mot de passe ainsi que les autorisations d'accès.

L'Interface Systèmes de Sécurité a pour objet d'assurer la communication des contrôles entre le système de sécurité installé sur le site et PACBASE.

Concernant PACBASE et la Transaction de gestion des paramètres et de mise en production (xxEF), l'Interface de Sécurité effectue les tâches suivantes :

- En TP : récupération automatique du USERID du SIGN-ON CICS ou IMS qu'il affiche sur la grille de connexion de PACBASE ou de la transaction xxEF.

- Contrôle d'accès à la bibliothèque : au lieu d'être effectué par le système de sécurité, il est effectué par PACBASE.

- En batch : pour les procédures PACBASE comportant une entrée utilisateur (carte '*') lancées sous TSO, le code utilisateur et le mot de passe pourront ne plus être renseignés.

Afin d'assurer une standardisation du contrôle pour tous les systèmes de sécurité, PACBASE est interfacé non pas directement avec le système de sécurité, mais avec SAF (System Authorization Facility) par l'intermédiaire des macro-instructions RACROUTE pour RACF ou des macro-instructions TSS pour TOPSECRET.

1.2. MISE EN OEUVRE

MISE EN OEUVRE

MISE EN OEUVRE AU NIVEAU PACBASE

L'Interface Système de Sécurité PACBASE est une option payante de PACBASE. En tant que telle, son utilisation est contrôlée par la clé d'accès à PACBASE. De ce fait, la première opération à effectuer est de modifier cette clé.

Cette clé est fournie avec le produit lors de l'installation de l'interface PACBASE-RACF ou TOPSECRET.

La deuxième opération est de définir dans PACBASE le type de l'outil de sécurité utilisé (RACF ou TOPSECRET), et la classe (de ressources) RACF ou TOPSECRET sous laquelle vont être définies les ressources logiques PACBASE.

Vous pouvez réaliser ces deux opérations :

. en TP en accédant, via le code transaction xxEF (xx étant le radical de la base), à l'écran PK de 'Mise à jour des clés d'accès'. Pour une description complète de cet écran, référez-vous au Manuel d'Utilisation PACBASE, Chapitre "Gestion de la Base", Sous-chapitre "Mise à jour des clés d'accès".

. en batch via la procédure PARM. Dans le JCL de lancement de cette procédure, vous devez coder une ligne 'NK' pour modifier la clé d'accès, et une ligne 'NS' pour définir l'outil de sécurité et la classe. Pour la description complète des lignes 'NK' et 'NS', reportez-vous au Manuel d'Exploitation de PACBASE, Partie II "Procédures Batch", Chapitre "PARM: Mise à Jour des Paramètres Utilisateur", Sous-chapitre "Description des entrées et recommandations".

MISE EN OEUVRE AU NIVEAU DU SYSTEME DE SECURITE

1. Création d'une classe RACF ou d'une classe de ressources TOPSECRET

Une classe ou une classe de ressources se codifie sur quatre caractères et doit être identique sous le système de sécurité et PACBASE.

Création d'une classe RACF

Pour que RACF puisse assurer les contrôles dont il a la charge, toutes les ressources logiques PACBASE sont associées à une classe RACF, définie dans PACBASE via l'écran PK ou la procédure batch PARM, et sous RACF à l'aide de la macro RACF 'ICHERCDE', qui génère une entité placée dans le membre ICHRRCDE résidant dans la SYS1.LINKLIB.

Le paramètre "longueur maximale des ressources" comporte 4 caractères (1 pour le code autorisation, 3 pour la Bibliothèque).

PACBASE est interfacé non pas directement avec RACF, mais avec SAF, par l'intermédiaire des macros RACROUTE.

Pour la prise en compte des macros RACROUTE, la classe doit être codifiée à l'aide de la macro ICHRFRTB, qui génère une entrée dans la table 'RACF ROUTER' (membre ICHRFR01 qui réside dans la bibliothèque SYS1.LINKLIB).

Création d'une classe de ressources TOPSECRET

Pour que TOPSECRET puisse assurer les contrôles dont il a la charge, toutes les ressources logiques PACBASE sont associées à une classe de ressources TOPSECRET, définie dans PACBASE via l'écran PK ou la procédure batch PARM, et sous TOPSECRET en saisissant :

```
TSS ADD(RDT) RESCLASS(cccc) RESCODE(xx), avec

cccc : classe de ressources
xx : code hexadécimal indiquant le type de ressources.
```

2. Création des ressources

La création des ressources est à effectuer seulement si le choix des autorisations d'accès aux bibliothèques PACBASE par RACF ou TOPSECRET a été selectionné.

Cette classe doit contenir les ressources logiques PACBASE, c'est-à-dire les autorisations possibles pour chaque Bibliothèque, présentées sous la forme de couples (autorisation, Bibliothèque).

Pour RACF :

Les ressources sont créées par la procédure 'RDEFINE'.

Pour TOPSECRET :

Les ressources sont créées par la commande :

```
    TSS ADD(nom-dept) cccc(nbib) cccc(nbib) ..., avec

nom-dept = nom du département,
cccc = classe de ressources,
n = niveau d'autorisation,
bib = code Bibliothèque PACBASE.
```

EXEMPLE :

Soit une base comprenant deux Bibliothèques BI1 et BI2. Les ressources définies sous la classe seront, pour les autorisations au niveau Bibliothèque :

```
4BI1 3BI1 2BI1 1BI1 0BI1 4BI2 3BI2 2BI2 1BI2 0BI2
```

Remarque : il n'y a pas de distinction entre l'autorisation globale et l'autorisation par base car cette dernière n'existe pas dans l'Interface Système de Sécurité.

Les ressources correspondant à l'autorisation générale sont définies à l'aide d'un code Bibliothèque spécial $$$:

$$ 3$$$ 2$$$ 1$$$ 0$$$

Le caractère '*' étant un caractère générique, sous le système de sécurité, l'Inter-Bibliothèque '***' est codée avec 3 caractères "livre sterling" (ou 3 "dièses" suivant le clavier).

Il existe trois autres codes Bibliothèque spéciaux :

. $B pour une autorisation aux procédures batch,
. $E pour une autorisation au module de Personnalisation,
. $P pour une autorisation à la procédure PARM de gestion des utilisateurs.

3. Définition des autorisations par utilisateur

La définition des utilisateurs autorisés à accéder à une ressource se fait :

Pour RACF à l'aide de la procédure 'PERMIT',

```
Pour TOPSECRET à l'aide de la commande :       TSS PERMIT(code-
utilisateur) cccc(bib) cccc(bib) ...
```

Les ressources et codes non déclarés sous le système de sécurité (RACF ou TOPSECRET) sont considérés comme interdits sous PACBASE.

MISE EN OEUVRE DES PROGRAMMES

Avec l'apparition de l'interface PACBASE-RACF ou PACBASE-TOPSECRET, de nouveaux programmes ou load-modules sont mis à la disposition de l'utilisateur.

Programmes ASSEMBLEUR

Pour RACF :

PACSECU8 est utilisé pour le batch et le TP.

Ce programme, qui est linké avec les paramètres RENT et REUS, doit être stocké dans une bibliothèque autorisée et introduit dans le membre LNKLSTxx de la bibliothèque SYS1.PARMLIB, pour éviter de concaténer cette bibliothèque dans les STEPLIB des JCL.
Ce programme doit être déclaré aussi dans la table ICHAUTAB, qui se trouve dans la bibliothèque SYS1.LPALIB, avec l'autorisation de RACFLIST SVC et RACFINIT SVC.

Pour TOPSECRET :

PACTSS est utilisé pour le batch sous MVS/CICS et pour le batch et TP sous MVS/IMS.
PACTSSC est utilisé pour le TP sous MVS/CICS.

Programmes COBOL

PACSECB pour le batch sous MVS/CICS et pour le batch et TP sous MVS/IMS.

xxSECT pour le TP sous MVS/CICS, où xx représente le radical de la base.

1.3. UTILISATION

UTILISATION DE PACBASE AVEC RACF OU TOPSECRET

L'interface effectue ses contrôles suivant trois indicateurs signalés au niveau de la procédure PARM :

- Indicateur d'utilisation du système de sécurité.

- Indicateur de contrôle de l'utilisateur.

  Pour RACF, il permet d'indiquer si l'utilisateur connecté sous CICS ou IMS pour le TP, ou TSO pour le batch, a le droit de se connecter à PACBASE avec un code utilisateur différent du sien. Cet indicateur n'est valable que si le système de sécurité est utilisé.

  Pour TOPSECRET, cet indicateur est forcé : il n'est pas possible de se connecter avec un code utilisateur différent du sien.

- Indicateur de contrôle des ressources (accès à la bibliothèque) par PACBASE ou par le système de sécurité. Cet indicateur n'est valable que si le système de sécurité est utilisé.

Ces indicateurs permettent de distinguer différents modes de gestion : gestion totale et stricte sous système de sécurité, gestion totale et souple sous système de sécurité et gestion sous PACBASE.

GESTION TOTALE ET STRICTE SOUS SYSTEME DE SECURITE

Le contrôle des utilisateurs et des accès à la bibliothèque est géré par l'interface de sécurité et un utilisateur ne peut se connecter qu'avec son propre code.

. Connexion TP : la grille de SIGN-ON PACBASE ou PARM est initialisée avec le code utilisateur signé sous CICS ou IMS. Ce code est récupéré dans l'IO-PCB sous IMS et par un ordre EXEC CICS ASSIGN USERID sous CICS (seulement valable à partir de la version CICS 1.7). La modification du code utilisateur est interdite.

. La zone mot de passe est verrouillée et non renseignée. Le curseur est positionné sur le code bibliothèque.

. Ecran GP (RACF uniquement) : comme RACF ne propage pas le user et le mot de passe CICS ou IMS, il faut les insérer sur la carte JOB. Le mot de passe n'étant pas transmis par le système, il faut que l'utilisateur le renseigne sur l'écran GP (zone qui n'est pas visible) la première fois qu'il fait SUB ou JOB.

Un message d'avertissement est affiché si la zone n'a pas déjà été renseignée.
A partir de la version RACF 1.9, il n'est plus obligatoire de renseigner le mot de passe en utilisant le fait qu'un utilisateur a le droit de lancer un job pour un autre utilisateur (surrogate user).

. Procédures batch comportant une carte '*' : le code utilisateur et le mot de passe ne sont plus obligatoires, le système prendra automatiquement le code utilisateur signé sous TSO.

Ceci entraîne que le PASSWORD n'est plus présent dans les fichiers temporaires des chaînes batch, y compris dans GPRT car la propagation du USER et du PASSWORD est correctement assurée par le système de sécurité pour les jobs de compilation soumis par cette procédure.
Autre conséquence, les chaînes comportant des steps avec une carte '*' peuvent s'enchaîner sans intervention manuelle pour y préciser le mot de passe.
Ce procédé implique une restriction pour l'utilisateur de RACF : il ne peut indiquer plusieurs cartes '*' avec des codes utilisateurs différents du sien pour les procédures le permettant (telle GPRT).
Remarque : avec TOPSECRET, l'utilisateur ne peut de toutes façons jamais indiquer un code utilisateur différent du sien.

GESTION TOTALE ET SOUPLE SOUS SYSTEME DE SECURITE

Cette gestion n'est possible que sous RACF.

Les contrôles utilisateurs et d'accès à la bibliothèque sont gérés par l'interface de sécurité mais l'utilisateur peut se connecter avec un autre code que le sien.

. Connexion TP : identique à la gestion précédente, mais la zone comprenant le USER code est saisissable ainsi que la zone PASSWORD. L'utilisateur peut alors modifier ces deux zones, le mot de passe étant obligatoire. Dans le cas d'une modification, un contrôle est effectué par l'interface pour valider le code USER et le mot de passe par le système de sécurité.

. Ecran GP : identique à la gestion précédente. Si l'utilisateur a renseigné le mot de passe sur la grille de de connexion, il n'est pas nécessaire de le repréciser.

. Procédure batch comportant une carte étoile : comme pour le TP dans le cas où le code user est différent de TSO, le mot de passe doit être renseigné. Ceci permet donc de lancer des jobs avec plusieurs cartes '*' de codes user différents. Dans le cas de USER différents, les jobs lancés par GPRT comporteront les paramètres USER et PASSWORD. Même dans ce cas, les fichiers temporaires ne comportent pas le mot de passe, ce qui signifie qu'il n'est pas possible d'enchaîner des steps ayant une carte '*'. Le mot de passe doit être renseigné à chaque fois. Bien entendu, dans le cas où le USER est identique à celui de TSO, la gestion est identique à la précédente.

GESTION DES RESSOURCES SOUS PACBASE

Les contrôles utilisateur sont effectués suivant l'un des deux modes précédents pour RACF ou toujours suivant le mode 'Gestion totale et stricte' pour TOPSECRET mais les contrôles d'accès aux bibliothèques sont gérés par PACBASE. Les autorisations d'accès aux bibliothèques doivent être saisies sous PACBASE, sur l'écran PU, la zone mot de passe devient non saisissable.

REMARQUE

Les fonctionnalités suivantes ne sont plus disponibles avec l'Interface de sécurité :

- La commande +AG pour la procédure GPRT,
- La copie de JCL de l'écran GP vers un autre utilisateur.
- La modification du mot de passe sur la grille de connexion.

1.4. GESTION DES ERREURS (RACF SEULEMENT)

GESTION DES ERREURS SOUS RACF

Si une anomalie est détectée après identification de l'utisateur et déclaration des ressources demandées, un message d'erreur PACBASE s'affiche. A ce message est adjoint un code retour, composé d'un code retour SAF et d'un code correspondant à la nature de l'erreur.

L'utilisateur doit communiquer ce code retour à l'administrateur du système de sécurité qui l'analysera et proposera la solution appropriée.

Le code varie selon la nature de l'erreur :

'I': erreur sur le code utilisateur.

Macro instruction RACROUTE REQUEST=VERIFY permettant de contrôler le code utilisateur et le mot de passe.

'L': accès à la Bibliothèque renseignée impossible.

Macro instruction RACROUTE REQUEST=LIST, ENVIR=CREATE, utilisée pour construire une copie mémoire de tous les profiles de ressources pour la classe considérée.

'C': accès à la Bibliothèque renseignée impossible.

Macro instruction RACROUTE REQUEST=FASTAUTH, qui contrôle l'autorisation d'accès à la ressource.

'D': accès à la Bibliothèque renseignée impossible.

Macro instruction RACROUTE REQUEST=LIST, ENVIR=DELETE, utilisée pour détruire la copie mémoire construite par ENVIR = CREATE.

'P': mot de passe à blanc.

2. INTERFACE PACTABLE - RACF OU TOPSECRET

2.1. INTRODUCTION

INTRODUCTION

Un système de sécurité assure les contrôles des codes utilisateur et de leur mot de passe ainsi que les autorisations d'accès.

L'Interface Systèmes de Sécurité a pour objet d'assurer la communication des contrôles entre le système de sécurité installé sur le site et PACTABLE.

Concernant PACTABLE et la Transaction de gestion des paramètres et de mise en production (xxEF), l'Interface de Sécurité effectue les tâches suivantes :

- En TP : récupération automatique du USERID du SIGN-ON CICS ou IMS qu'il affiche sur la grille de connexion de PACTABLE ou de la transaction xxEF.

- Contrôle d'accès à la bibliothèque : au lieu d'être effectué par le système de sécurité, il est effectué par PACTABLE.

- En batch : pour les procédures PACTABLE comportant une entrée utilisateur (carte '*') lancées sous TSO, le code utilisateur et le mot de passe pourront ne plus être renseignés.

Afin d'assurer une standardisation du contrôle pour tous les systèmes de sécurité, PACTABLE est interfacé non pas directement avec le système de sécurité, mais avec SAF (System Authorization Facility) par l'intermédiaire des macro-instructions RACROUTE pour RACF ou des macro-instructions TSS pour TOPSECRET.

2.2. MISE EN OEUVRE

MISE EN OEUVRE

1. Création d'une classe de ressources

Pour que le système de sécurité puisse assurer les contrôles dont il a la charge, chaque base PACTABLE doit être identifiée par une classe. La classe doit être créée sous PACTABLE par le gestionnaire des tables à l'aide de la transaction 'XX90' et :

. sous RACF à l'aide de la macro RACF 'ICHERCDE'.

. sous TOPSECRET à l'aide de la commande :

```
TSS RESCLASS(cccc) RESCODE(xx), avec
 cccc = classe de ressources
 xx = code héxadécimal identifiant la ressource.
```

Le nom d'une classe se codifie sur quatre caractères et doit être identique sous le système de sécurité et PACTABLE.

2. Création des ressources

La création des ressources n'est à effectuer que si celles-ci sont contrôlées par le système de sécurité.

Cette classe doit contenir les ressources logiques PACTABLE, c'est-à-dire les autorisations possibles pour chaque table jusqu'au niveau sous-schéma, sous-système. Ces autorisations doivent être présentées sous la forme d'un ensemble AUTORISATION, SOUS-SCHEMA, SOUS-SYSTEME, NUMERO DE TABLE.

La recherche des autorisations se fait dans l'ordre de rangement des éléments de cet ensemble. En cas d'absence de sous-schéma, de sous-système ou de No de table, les blancs sont remplacés par des '$'. En cas d'absence d'autorisation particulière pour une table, c'est le niveau global d'autorisation qui est pris en compte.

Pour RACF :

Les ressources sont créées par la procédure 'RDEFINE'.

Pour TOPSECRET :

Les ressources sont créées par la commande :

TSS ADD (nom-dept) cccc(nstable) cccc(nstable) ..., avec

nom-dept = nom du département,
n = numéro du sous-schéma,
s = numéro du sous-système,
table = code de la table.

EXEMPLE

Supposons que l'on veuille connaître les autorisations possibles pour la table suivante :

```
No DE SOUS-SCHEMA     No DE SOUS-SYSTEME     No DE TABLE
       1                     3                  Table

Les recherches se déroulent dans l'ordre suivant :

1         1  3  Table
2         $  3  Table
3         1  $  Table
4         $  $  Table
5         $  $  $$$$$$
```

Le caratère '*' est un caractère générique. Sur les sites dotés de RACF ou TOPSECRET, le code du gestionnaire des$$$$$$$'.

3. Définition des autorisations par utilisateur

La définition des utilisateurs autorisés à accéder à une ressource se fait :

. sous RACF à l'aide de la procédure RACF 'PERMIT',

. sous TOPSECRET à l'aide de la commande :

```
    TSS PERMIT (code-utilisateur) cccc(nstable), avec
     cccc = classe de ressources,
     n = code du sous-schéma,
     s = code du sous-système,
     table = code de la table.
```

Les ressources et codes non déclarés sous le système de sécurité sont considérés comme interdits sous PACTABLE.

EXPLOITATION DE L'INTERFACE PACTABLE / RACF OU TOPSECRET

Avec l'apparition de l'interface PACTABLE-RACF ou TOPSECRET, de nouveaux programmes ou load-modules sont mis à la disposition de l'utilisateur.

Programmes ASSEMBLEUR

Pour RACF :

PACSECU8 est utilisé pour le batch et le TP.

Ce programme, qui est linké avec les paramètres RENT et REUS, doit être stocké dans une bibliothèque autorisée et introduit dans le membre LNKLSTxx de la bibliothèque SYS1.PARMLIB, pour éviter de concaténer cette bibliothèque dans les STEPLIB des JCL.
Ce programme doit être déclaré aussi dans la table ICHAUTAB, qui se trouve dans la bibliothèque SYS1.LPALIB, avec l'autorisation de RACFLIST SVC et RACFINIT SVC.

Pour TOPSECRET :

PACTSS est utilisé pour le batch sous MVS/CICS et pour le batch et TP sous MVS/IMS.
PACTSSC est utilisé pour le TP sous MVS/CICS.

Programmes COBOL

PACSECB pour le batch sous MVS/CICS et pour le batch et TP sous MVS/IMS.

xxSECT pour le TP sous MVS/CICS, où xx représente le radical de la base.

2.3. UTILISATION

IMPLANTATION DE L'INTERFACE PACTABLE/RACF OU TOPSECRET

L'acquisition de l'interface PACTABLE / RACF ou TOPSECRET implique une modification des paramètres de la base. La transaction 'XX90', où 'XX' représente le radical de la base, permet au gestionnaire des tables de les mettre à jour en précisant le type de système de sécurité ('R' pour RACF ou 'S' pour TOPSECRET), ainsi que la classe d'identification de la base PACTABLE et deux indicateurs :

- Indicateur de contrôle de l'utilisateur.

  Pour RACF, il permet d'indiquer si l'utilisateur connecté sous CICS ou IMS pour le TP ou TSO pour le batch, a le droit de se connecter à PACTABLE avec un code utilisateur différent du sien. Cet indicateur n'est valable que si le système de sécurité est utilisé.

  Pour TOPSECRET, cet indicateur est forcé car un utilisateur ne peut pas se connecter avec un code différent du sien.

- Indicateur de contrôle des ressources (accès aux tables) par PACTABLE ou par le système de sécurité. Cet indicateur n'est valable que si le système de sécurité est utilisé.

Ces indicateurs permettent de distinguer deux modes de gestion différents : gestion totale et stricte sous système de sécurité ou gestion totale et stricte sous système de sécurité.

GESTION TOTALE ET STRICTE SOUS SYSTEME DE SECURITE

Le contrôle des utilisateurs et des accès à la table est géré par l'interface de sécurité et un utilisateur ne peut se connecter qu'avec son propre code.

. Connexion TP : la grille de SIGN-ON PACTABLE est initialisée avec le code utilisateur signé sous CICS ou IMS. Ce code est récupéré dans l'IO-PCB sous IMS et par un ordre EXEC CICS ASSIGN USERID sous CICS (seulement valable à partir de la version CICS 1.7). La modification du code utilisateur est interdite.

. La zone mot de passe est verrouillée et non renseignée. Le curseur est positionné sur le code bibliothèque.

. RACF uniquement : Ecrans LJ,LE : comme RACF ne propage pas le user et le mot de passe CICS ou IMS, il faut les insérer sur la carte JOB. Le mot de passe n'étant pas transmis par le système, il faut que l'utilisateur le renseigne sur les écrans LJ ou LE (zone qui n'est pas visible) la première fois qu'il fait SUB ou JOB.

Un message d'avertissement est affiché si la zone n'a pas déjà été renseignée.
A partir de la version RACF 1.9, il n'est plus obligatoire de renseigner le mot de passe en utilisant le fait qu'un utilisateur a le droit de lancer un job pour un autre utilisateur (surrogate user).

. Procédures batch comportant une carte d'identification : le code utilisateur et le mot de passe ne sont plus obligatoires, le système prendra automatiquement le code utilisateur signé sous TSO. Ceci entraîne que le PASSWORD n'est plus présent dans les fichiers temporaires des chaînes batch.

Pour RACF uniquement : Autre conséquence, les chaînes comportant des steps avec une carte '*' peuvent s'enchaîner sans intervention manuelle pour y préciser le mot de passe.
Ce procédé implique une restriction, l'utilisateur ne peut indiquer plusieurs cartes '*' avec des codes utilisateurs différents du sien pour les procédures le permettant.
Note : avec TOPSECRET, l'utilisateur ne peut de toutes façons jamais indiquer un code utilisateur différent du sien.

GESTION TOTALE ET SOUPLE SOUS SYSTEME DE SECURITE

Cette gestion n'est possible que sous RACF.

Les contrôles utilisateurs et d'accès à la table sont gérés par l'interface de sécurité mais l'utilisateur peut se connecter avec un autre code que le sien.

. Connexion TP : identique à la gestion précédente, mais la zone comprenant le USER code est saisissable ainsi que la zone PASSWORD. L'utilisateur peut alors modifier ces deux zones, le mot de passe étant obligatoire. Dans le cas d'une modification, un contrôle est effectué par l'interface pour valider le code USER et le mot de passe par le système de sécurité.

. Ecran LJ,LE : identique à la gestion précédente. Si l'utilisateur a renseigné le mot de passe sur la grille de de connexion, il n'est pas nécessaire de le repréciser.

. Procédure batch comportant une carte d'identification : comme pour le TP dans le cas où le code user est différent de TSO, le mot de passe doit être renseigné. Ceci permet donc de lancer des jobs avec plusieurs cartes '*' de codes user différents.

Les fichiers temporaires ne comportent pas le mot de passe, ce qui signifie qu'il n'est pas possible d'enchaîner des steps ayant une carte d'identification. Le mot de passe doit être renseigné à chaque fois. Bien entendu, dans le cas où le USER est identique à celui de TSO, la gestion est identique à la précédente.

Le champ TYPE de la transaction XX90 peut donc prendre deux valeurs : "blanc" ou "P". "P" représente le contrôle des ressources par PACTABLE et non par le système de sécurité.

La zone BLOC prend la valeur "blanc" ou "N". "N" indique que l'utilisateur ne peut se servir d'un autre code que le sien.

2.4. GESTION DES ERREURS (RACF SEULEMENT)

GESTION DES ERREURS SOUS RACF

Si une anomalie est détectée après identification de l'utisateur et déclaration des ressources demandées, un message d'erreur PACBASE s'affiche. A ce message est adjoint un code retour, composé d'un code retour SAF et d'un code correspondant à la nature de l'erreur.

L'utilisateur doit communiquer ce code retour à l'administrateur du système de sécurité qui l'analysera et proposera la solution appropriée.

Le code varie selon la nature de l'erreur :

'I': erreur sur le code utilisateur.

Macro instruction RACROUTE REQUEST=VERIFY permettant de contrôler le code utilisateur et le mot de passe.

'L': accès à la Bibliothèque renseignée impossible.

Macro instruction RACROUTE REQUEST=LIST, ENVIR=CREATE, utilisée pour construire une copie mémoire de tous les profiles de ressources pour la classe considérée.

'C': accès à la Bibliothèque renseignée impossible.

Macro instruction RACROUTE REQUEST=FASTAUTH, qui contrôle l'autorisation d'accès à la ressource.

'D': accès à la Bibliothèque renseignée impossible.

Macro instruction RACROUTE REQUEST=LIST, ENVIR=DELETE, utilisée pour détruire la copie mémoire construite par ENVIR = CREATE.

'P': mot de passe à blanc.

3. INTERFACE DSMS - RACF OU TOPSECRET

3.1. INTRODUCTION

INTRODUCTION

Un système de sécurité assure les contrôles des codes utilisateur et de leur mot de passe.

L'Interface Systèmes de Sécurité a pour objet d'assurer la communication des contrôles entre le système de sécurité installé sur le site et DSMS.

Concernant DSMS, l'Interface de Sécurité effectue les tâches suivantes :

- En TP : récupération automatique du USERID du SIGN-ON CICS ou IMS qu'il affiche sur la grille de connexion.

- En batch : pour les procédures DSMS comportant une entrée utilisateur (carte '*') lancées sous TSO, le code utilisateur et le mot de passe pourront ne plus être renseignés.

Afin d'assurer une standardisation du contrôle pour tous les systèmes de sécurité, DSMS est interfacé non pas directement avec le système de sécurité, mais avec SAF (System Authorization Facility) par l'intermédiaire des macro-instructions RACROUTE pour RACF ou des macro-instructions TSS pour TOPSECRET.

3.2. MISE EN OEUVRE

MISE EN OEUVRE

MISE EN OEUVRE DES PROGRAMMES

Avec l'apparition de l'interface DSMS-RACF ou DSMS-TOPSECRET, de nouveaux programmes ou load-modules sont mis à la disposition de l'utilisateur.

Programmes ASSEMBLEUR

Pour RACF :

PACSECU8 est utilisé pour le batch et le TP.

Ce programme, qui est linké avec les paramètres RENT et REUS, doit être stocké dans une bibliothèque autorisée et introduit dans le membre LNKLSTxx de la bibliothèque SYS1.PARMLIB, pour éviter de concaténer cette bibliothèque dans les STEPLIB des JCL.
Ce programme doit être déclaré aussi dans la table ICHAUTAB, qui se trouve dans la bibliothèque SYS1.LPALIB, avec l'autorisation de RACFLIST SVC et RACFINIT SVC.

Pour TOPSECRET :

PACTSS est utilisé pour le batch sous MVS/CICS et pour le batch et TP sous MVS/IMS.
PACTSSC est utilisé pour le TP sous MVS/CICS.

Programmes COBOL

PACSECB pour le batch sous MVS/CICS et pour le batch et TP sous MVS/IMS.

xxSECT pour le TP sous MVS/CICS, où xx représente le radical de la base.

3.3. UTILISATION

UTILISATION DE DSMS AVEC RACF OU TOPSECRET

L'interface effectue ses contrôles suivant les indicateurs signalés au niveau de la procédure DRST :

- Indicateur d'utilisation du système de sécurité.

- Indicateur de contrôle de l'utilisateur.

  Pour RACF, il permet d'indiquer si l'utilisateur connecté sous CICS ou IMS pour le TP, ou TSO pour le batch, a le droit de se connecter à DSMS avec un code utilisateur différent du sien. Cet indicateur n'est valable que si le système de sécurité est utilisé.

  Pour TOPSECRET, cet indicateur est forcé : il n'est pas possible de se connecter avec un code utilisateur différent du sien.

Ces indicateurs permettent de distinguer différents modes de gestion : gestion totale et stricte sous système de sécurité, gestion totale et souple sous système de sécurité et gestion sous DSMS.

GESTION TOTALE ET STRICTE SOUS SYSTEME DE SECURITE

Le contrôle des utilisateurs est géré par l'interface de sécurité et un utilisateur ne peut se connecter qu'avec son propre code.

. Connexion TP : la grille de SIGN-ON DSMS est initialisée avec le code utilisateur signé sous CICS ou IMS. Ce code est récupéré dans l'IO-PCB sous IMS et par un ordre EXEC CICS ASSIGN USERID sous CICS (seulement valable à partir de la version CICS 1.7). La modification du code utilisateur est interdite.

. La zone mot de passe est verrouillée et non renseignée. Le curseur est positionné sur le code bibliothèque.

. Ecran LVQ (RACF uniquement) : comme RACF ne propage pas le user et le mot de passe CICS ou IMS, il faut les insérer sur la carte JOB. Le mot de passe étant lu par DSMS dans la table TUD, il doit donc être identique à celui déclaré dans CICS ou IMS.

. Procédures batch comportant une carte '*' : le code utilisateur et le mot de passe ne sont plus obligatoires, le système prendra automatiquement le code utilisateur signé sous TSO.

Ceci entraîne que le PASSWORD n'est plus présent dans les fichiers temporaires des chaînes batch, y compris dans DPRT car la propagation du USER et du PASSWORD est correctement assurée par le système de sécurité.
Autre conséquence, les chaînes comportant des steps avec une carte '*' peuvent s'enchaîner sans intervention manuelle pour y préciser le mot de passe.
Ce procédé implique une restriction pour l'utilisateur de RACF : il ne peut indiquer plusieurs cartes '*' avec des codes utilisateurs différents du sien pour les procédures le permettant (telle GPRT).
Remarque : avec TOPSECRET, cela n'est jamais possible.

GESTION TOTALE ET SOUPLE SOUS SYSTEME DE SECURITE

Cette gestion n'est possible que sous RACF.

Les contrôles utilisateurs sont gérés par l'interface de sécurité mais l'utilisateur peut se connecter avec un autre code que le sien.

. Connexion TP : identique à la gestion précédente, mais la zone comprenant le USER code est saisissable ainsi que la zone PASSWORD. L'utilisateur peut alors modifier ces deux zones, le mot de passe étant obligatoire. Dans le cas d'une modification, un contrôle est effectué par l'interface pour valider le code USER et le mot de passe par le système de sécurité.

. Ecran LVQ : identique à la gestion précédente.

. Procédure batch comportant une carte étoile : comme pour le TP dans le cas où le code user est différent de TSO, le mot de passe doit être renseigné.

Ceci permet donc de lancer des jobs avec plusieurs cartes '*' de codes user différents.
Dans le cas de USER différents, les jobs lancés par DPRT comporteront les paramètres USER et PASSWORD.
Même dans ce cas, les fichiers temporaires ne comportent pas le mot de passe, ce qui signifie qu'il n'est pas possible d'enchaîner des steps ayant une carte '*'. Le mot de passe doit être renseigné à chaque fois.
Bien entendu, dans le cas où le USER est identique à celui de TSO, la gestion est identique à la précédente.

3.4. GESTION DES ERREURS (RACF SEULEMENT)

GESTION DES ERREURS SOUS RACF

Si une anomalie est détectée après identification de l'utisateur, un message d'erreur DSMS s'affiche. A ce message est adjoint un code retour, composé d'un code retour SAF et d'un code correspondant à la nature de l'erreur.

L'utilisateur doit communiquer ce code retour à l'administrateur du système de sécurité qui l'analysera et proposera la solution appropriée.

Le code varie selon la nature de l'erreur :

'I': erreur sur le code utilisateur.

Macro instruction RACROUTE REQUEST=VERIFY
permettant de contrôler le code utilisateur et le mot de passe.

'P': mot de passe à blanc.