Connectivité
Informations complémentaires

Version 7

SDB2-CONN-SU

Connectivité
Informations complémentaires

Version 7

SDB2-CONN-SU

Important

Avant d'utiliser le présent document et le produit associé, prenez connaissance des informations générales figurant à l'«Annexe B. Remarques» à la page 193.

LE PRESENT DOCUMENT EST LIVRE "EN L'ETAT". IBM DECLINE TOUTE RESPONSABILITE, EXPRESSE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE QUALITE MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessous ne vous sera pas applicable.

Ce document est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. Les informations qui y sont fournies sont susceptibles d'être modifiées avant que les produits décrits ne deviennent eux-mêmes disponibles. En outre, il peut contenir des informations ou des références concernant certains produits, logiciels ou services non annoncés dans ce pays. Cela ne signifie cependant pas qu'ils y seront annoncés.

Pour plus de détails, pour toute demande d'ordre technique, ou pour obtenir des exemplaires de documents IBM, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial.

Vous pouvez également consulter les serveurs Internet suivants :

- http://www.fr.ibm.com (serveur IBM en France)
- http://www.can.ibm.com (serveur IBM au Canada)
- http://www.ibm.com (serveur IBM aux Etats-Unis)

Compagnie IBM France
Direction Qualité
Tour Descartes
92066 Paris-La Défense Cedex 50

Table des matières

Avis aux lecteurs canadiens

Le présent document a été traduit en France. Voici les principales différences et particularités dont vous devez tenir compte.

Illustrations

Les illustrations sont fournies à titre d'exemple. Certaines peuvent contenir des données propres à la France.

Terminologie

La terminologie des titres IBM peut différer d'un pays à l'autre. Reportez-vous au tableau ci-dessous, au besoin.

IBM France	IBM Canada
ingénieur commercial	représentant
agence commerciale	succursale
ingénieur technico-commercial	informaticien
inspecteur	technicien du matériel

Claviers

Les lettres sont disposées différemment : le clavier français est de type AZERTY, et le clavier français-canadien de type QWERTY.

OS/2 et Windows - Paramètres canadiens

Au Canada, on utilise :

- les pages de codes 850 (multilingue) et 863 (français-canadien),
- le code pays 002,
- le code clavier CF.

Nomenclature

Les touches présentées dans le tableau d'équivalence suivant sont libellées différemment selon qu'il s'agit du clavier de la France, du clavier du Canada ou du clavier des États-Unis. Reportez-vous à ce tableau pour faire

correspondre les touches françaises figurant dans le présent document aux touches de votre clavier.

France	Canada	Etats-Unis
↖ (Pos1)	↖	Home
Fin	Fin	End
⇞ (PgAr)	⇞	PgUp
⇟ (PgAv)	⇟	PgDn
Inser	Inser	Ins
Suppr	Suppr	Del
Echap	Echap	Esc
Attn	Intrp	Break
Impr écran	ImpEc	PrtSc
Verr num	Num	Num Lock
Arrêt défil	Défil	Scroll Lock
⇪ (Verr maj)	FixMaj	Caps Lock
AltGr	AltCar	Alt (à droite)

Brevets

Il est possible qu'IBM détienne des brevets ou qu'elle ait déposé des demandes de brevets portant sur certains sujets abordés dans ce document. Le fait qu'IBM vous fournisse le présent document ne signifie pas qu'elle vous accorde un permis d'utilisation de ces brevets. Vous pouvez envoyer, par écrit, vos demandes de renseignements relatives aux permis d'utilisation au directeur général des relations commerciales d'IBM, 3600 Steeles Avenue East, Markham, Ontario, L3R 9Z7.

Assistance téléphonique

Si vous avez besoin d'assistance ou si vous voulez commander du matériel, des logiciels et des publications IBM, contactez IBM direct au 1 800 465-1234.

Préface

Le présent manuel fournit des informations complémentaires concernant l'installation et la configuration de différents produits SGBDR DB2, utilisés comme demandeurs ou serveurs d'applications DRDA. Ces informations permettent de configurer :

- les serveurs IBM DB2 Universal Database (UDB) Version 7, utilisés en tant que serveurs d'applications DRDA (AS)
- les demandeurs d'application IBM DB2 Connect Version 7 (AR)
- d'autres produits conformes à l'architecture DRDA

Le présent manuel constitue un complément d'information à celles contenues dans les manuels *Mise en route* suivants :

- DB2 Universal Database Enterprise Edition Version 7
- DB2 Universal Database Extended - Enterprise Edition Version 7
- DB2 Connect Enterprise Edition Version 7
- DB2 Connect Personal Edition Version 7

Les dernières informations relatives aux produits hôte (DB2 Universal Database for OS/390, DB2 Universal Database pour AS/400 et DB2 pour VSE & VM) figurent dans leur documentation respective.

Pour plus de détails sur la configuration du Gestionnaire de points de synchronisation DB2 (SPM) pour des mises à jour multisites, reportez-vous au manuel en ligne *Installation et configuration - Informations complémentaires*.

Structure du manuel

Le présent manuel se compose des chapitres suivants :

Utilisateurs concernés

Le présent manuel s'adresse aux personnes chargées de l'installation de DB2 Universal Database ou de DB2 Connect. Il leur permettra d'en savoir davantage sur les sujets répertoriés dans la section précédente.

Autres sources d'informations

Cette section énumère d'autres sources d'informations utiles.

Sur le World Wide Web

Vous pouvez trouver sur le Web les informations les plus récentes concernant DB2 Connect, DB2 Universal Database, et les autres logiciels IBM, notamment les dernières publications ainsi que des conseils et des remarques techniques sous la forme de Technotes. Pour trouver ces informations sur le Web, procédez comme suit:

1. Entrez dans votre navigateur Web l'adresse suivante:

   ```
   http://www.ibm.com/software/data/db2/library/
   ```

2. Sélectionnez "DB2 Universal Database".
3. Par exemple, repérez les remarques techniques (*Technotes*) en entrant un argument de recherche, par exemple, "DDCS", "DRDA" ou "Connect".

Publications DRDA connexes

Les ouvrages suivants contiennent des informations connexes et peuvent être cités comme références dans ce manuel.

Référence	Titre
SC26-4783	*Distributed Relational Database Architecture Connectivity Guide*
SC26-4773	*Distributed Relational Database Architecture Application Programming Guide*
SC26-4782	*Distributed Relational Database Architecture Problem Determination Guide*
SC26-4650	*Planning for Distributed Relational Database Architecture*
GC26-3195	*Distributed Relational Database Architecture Every Manager's Guide*

Référence	Titre
G321-5482	*IBM Distributed Data Management Architecture Level 3: Reference*

Publications serveur DRDA connexes

Les publications connexes ci-après concernent le serveur DRDA. Elles figurent dans les bibliothèques DB2 Universal Database pour AS/400, DB2 pour OS/390 et DB2 pour VSE & VM.

Référence	Titre
SC41-5702	*AS/400 Distributed Database Programming*
SC41-9609	*AS/400 SAA Structured Query Language/400 Programmer's Guide*
SC41-9608	*AS/400 SAA Structured Query Language/400 Reference*
GC21-8180	*AS/400 Communications Configuration Reference*
SC26-8958	*DB2 Universal Database for OS/390 Application Programming and SQL Reference*
SC26-8960	*DB2 Universal Database for OS/390 Command Reference*
GC26-8970	*DB2 Universal Database for OS/390 Installation Reference*
SC26-8964	*DB2 Universal Database for OS/390 Reference for Remote DRDA Requesters and Servers*
SC26-8966	*DB2 Universal Database for OS/390 SQL Reference*
SC26-8957	*DB2 Universal Database for OS/390 Administration*
SC26-8967	*DB2 Universal Database for OS/390 Utility Guide and Reference*
SH09-8087	*DB2 pour VSE & VM Guide SQL*
SC26-3255	*IBM SQL Reference*

Autres publications connexes

Référence	Titre
SG24-2006	*Migrating to DB2 Universal Database Version 5*
SG24-2213	*DB2 for OS/390 Version 5 Performance Topics*
SG24-4893	*DB2 Meets NT*
SG24-4894	*The Universal Connectivity Guide to DB2*
SG24-4693	*Getting Started with DB2 Stored Procedures*
SG24-2212	*DRDA Support for TCP/IP in DB2 Universal Database for OS/390 V5.1 and DB2 Universal Database V5.0*
SC33-0814	*CICS pour AIX Application Programming Guide*
SC33-0931	*CICS pour AIX Customization and Operation Guide*
GC11-1639	*DB2 Connect Enterprise Edition pour UNIX - Mise en route*
GC11-1640	*DB2 Connect Enterprise Edition pour OS/2 et Windows - Mise en route*
GC11-1647	*DB2 Connect Personal Edition - Mise en route*
GG24-4155	*Distributed Relational Database Architecture: Using DDCS for AIX DRDA support with DB2 pour MVS/ESA and DB2 Universal Database pour AS/400*
GG24-4311	*Distributed Relational Database Architecture Cross Platform Connectivity and Application*
SC23-2443	*Encina for AIX Product Family Overview*

Chapitre 1. Connexion de DB2 pour MVS/ESA au sein d'un réseau DRDA

DB2 pour MVS/ESA est le système de gestion de bases de données relationnelles IBM pour les systèmes MVS/XA et MVS/ESA. DB2 pour MVS/ESA version 2 édition 3 était la première édition de DB2 pour MVS/ESA en mesure de partager des données relationnelles réparties avec d'autres systèmes de gestion de bases de données prenant en charge des protocoles DRDA. Le présent chapitre décrit le mode de prise en charge par DB2 pour MVS/ESA des systèmes de gestion de bases de données relationnelles réparties. Si vous travaillez avec DB2 Universal Database for OS/390, *ignorez le présent chapitre*. Passez au «Chapitre 2. Connexion de DB2 Universal Database for OS/390 au sein d'un réseau DRDA» à la page 43.

Dans le présent chapitre, l'accent est mis principalement sur la configuration de DB2 pour MVS/ESA à des fins de connectivité :

1. depuis DB2 Connect (voir section «Configuration du serveur d'applications» à la page 27)
2. vers des serveurs DB2 Universal Database (voir section «Configuration du demandeur d'application» à la page 8).

Pour en savoir plus sur la connexion de deux systèmes DB2 pour MVS/ESA ou pour obtenir plus de détails sur la définition de connexions DRDA avec DB2 pour MVS/ESA, reportez-vous à la section relative à la connexion de systèmes de gestion de bases de données réparties dans le manuel *IBM Database 2 - Administration Guide*.

Grâce à la fonction AnyNet de VTAM version 4 édition 2, vous pouvez exécuter APPC sur un réseau TCP/IP. La fonction AnyNet se compose de AnyNet/MVS qui s'exécute sur un hôte et de AnyNet/2 qui s'exécute sur un poste de travail et qui est téléchargé à partir de l'hôte. N'importe quelle application APPC est accessible à un utilisateur final sur un réseau TCP/IP sans qu'aucune modification ne soit apportée à l'application. Dans le cas d'une utilisation d'APPC sur TCP/IP, un programme d'application sur MVS/ESA peut communiquer avec un autre programme d'application APPC s'exécutant avec AnyNet APPC sur TCP/IP sur MVS/ESA, OS/2, AIX/6000, OS/400 ou Windows. Pour plus de détails, reportez-vous au manuel *VTAM AnyNet Feature for V4R2 Guide to SNA over TCP/IP*.

DB2 pour MVS/ESA

La figure 1 illustre un système MVS exécutant une seule copie de DB2 pour MVS/ESA. Il est également possible d'en exécuter plusieurs sur un seul système MVS. Pour identifier les copies de DB2 pour MVS/ESA sur un système MVS déterminé (ou les copies de DB2 pour MVS/ESA sur un complexe MVS/JES), vous devez attribuer à chaque système DB2 un *nom de sous-système*, une chaîne de un à quatre caractères, unique dans un complexe MVS/JES. Dans la figure 1, le nom du sous-système DB2 pour MVS/ESA est *xxxx*. Trois noms d'espaces adresse MVS sont précédés du nom du sous-système DB2 pour MVS/ESA. Les espaces adresse forment le produit DB2 pour MVS/ESA.

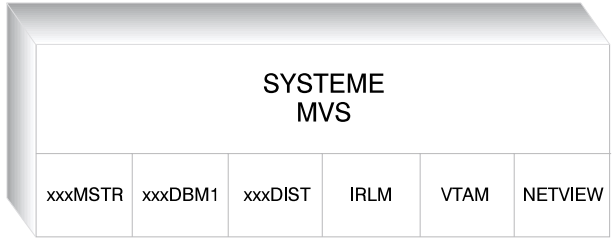

Figure 1. Espaces adresse MVS utilisés par DB2 pour MVS/ESA

La figure 1 illustre les espaces adresse MVS concernés par le traitement des bases de données réparties avec DB2 pour MVS/ESA. Ces espaces adresse permettent aux utilisateurs de DB2 pour MVS/ESA d'accéder à des bases de données relationnelles locales et de communiquer avec des systèmes DRDA éloignés. La fonction des espaces adresse est la suivante :

xxxxMSTR
Espace adresse des services système pour le produit DB2 pour MVS/ESA, chargé du démarrage et de l'arrêt de DB2 pour MVS/ESA, et du contrôle de l'accès local à DB2 pour MVS/ESA.

xxxxDBM1
Espace adresse des services base de données, responsable de l'accès aux bases de données relationnelles contrôlées par DB2 pour MVS/ESA. C'est là que sont exécutées les entrées et sorties aux ressources de base de données pour les programmes d'application SQL.

xxxxDIST
La partie de DB2 pour MVS/ESA qui fournit les fonctions de bases de données réparties, également appelée *Distributed Data Facility* (DDF).

Lors de la réception d'une demande de base de données répartie, DDF transmet la demande à *xxxx*DBM1, de sorte que puissent être exécutées les opérations d'entrée-sortie de base de données requises. Le présent manuel décrit DDF en détail.

IRLM Gestionnaire de verrous utilisé par DB2 pour MVS/ESA pour contrôler l'accès aux ressources de base de données.

VTAM
Gestionnaire de communications SNA pour le système MVS. DDF utilise VTAM pour l'exécution de communications de bases de données réparties au nom de DB2 pour MVS/ESA.

NETVIEW
Produit phare de la gestion de réseau sur les systèmes MVS. Lorsqu'une erreur se produit au cours du traitement d'une base de données répartie, DDF enregistre les informations relatives à l'erreur (également appelées *alertes*) dans la base de données du moniteur matériel NetView. Les administrateurs système peuvent utiliser NetView pour examiner les erreurs stockées dans la base de données du moniteur matériel ou fournir des procédures de commandes automatisées à utiliser chaque fois que sont enregistrées des conditions d'alerte.

NetView peut également permettre de détecter des erreurs de communication VTAM. Pour plus de détails, reportez-vous au manuel *Distributed Relational Database Architecture Problem Determination Guide*.

La figure 1 à la page 2 n'illustre pas de programmes d'application SQL. Lorsqu'un programme d'application utilise DB2 pour lancer des instructions SQL, il doit définir une liaison au produit DB2 pour MVS/ESA selon l'une des méthodes suivantes :

TSO Les travaux par lots et les utilisateurs finals connectés à TSO sont connectés à DB2 pour MVS/ESA via la fonction de définition de liaison de TSO. Il s'agit de la technique utilisée pour connecter SPUFI et la plupart des applications QMF à DB2 pour MVS/ESA.

CICS/ESA
Lorsqu'une application CICS/ESA émet des appels SQL, le produit CICS/ESA utilise l'interface de définition de liaison CICS pour acheminer les requêtes SQL vers DB2 pour MVS/ESA.

IMS/ESA
Les transactions qui s'exécutent sous le contrôle de IMS/ESA utilisent l'interface de définition de liaison IMS pour la transmission des instructions SQL à DB2 pour MVS/ESA pour traitement.

DDF DDF (Distributed Data Facility) est chargé de la connexion des applications réparties à DB2 pour MVS/ESA.

CAF La fonction de connexion d'appel (CAF) permet aux sous-systèmes écrits par l'utilisateur de se connecter directement à DB2 pour MVS/ESA.

Mise en oeuvre de DB2 pour MVS/ESA

DRDA définit les types de fonctions de système de gestion de bases de données réparties. DB2 pour MVS/ESA V2R3 prend en charge la fonction unité d'oeuvre éloignée. Avec l'unité d'oeuvre éloignée, un programme d'application s'exécutant sur un système peut accéder à des données au niveau d'un SGBD éloigné en utilisant le SQL fourni par ce dernier. DB2 pour MVS/ESA V3R1 prend en charge la fonction unité d'oeuvre répartie. Avec l'unité d'oeuvre répartie, un programme d'application s'exécutant sur un système peut accéder à des données au niveau de plusieurs SGBD éloignés en utilisant le SQL fourni par ces derniers. Pour en savoir plus sur les types de distribution définis par DRDA, reportez-vous au manuel *DRDA Connectivity Guide*.

Comme l'illustre la figure 2 à la page 6, DB2 pour MVS/ESA prend en charge trois configurations de connexions de bases de données réparties, selon deux méthodes d'accès :

[1] *L'accès défini par le système* permet à un demandeur DB2 pour MVS/ESA de se connecter à un ou plusieurs serveur(s) DB2 pour MVS/ESA. Cette connexion établie entre le demandeur DB2 pour MVS/ESA et le serveur n'adhère pas aux protocoles définis dans DRDA et ne peut pas être utilisée pour connecter des produits non DB2 pour MVS/ESA à DB2 pour MVS/ESA. L'établissement de ce type de connexion se fait par la codification, dans l'application, de noms ou d'alias composés de trois parties.

[2] *L'accès défini par l'application* permet à un demandeur DB2 pour MVS/ESA ou non DB2 pour MVS/ESA (par exemple, DB2 Connect) de se connecter à un ou plusieurs serveurs d'applications DB2 pour MVS/ESA ou non DB2 pour MVS/ESA (par exemple, DB2 Universal Database et DB2 Universal Database pour AS/400) en utilisant des protocoles DRDA. Le nombre de serveurs d'applications pouvant être simultanément connectés au demandeur d'application dépend du niveau de DB2 pour MVS/ESA de ce demandeur. Si le demandeur d'application est DB2 pour MVS/ESA version 2.3, un seul serveur d'applications peut être connecté à la fois. L'établissement de ce type de connexion se fait par la codification d'instructions SQL CONNECT dans l'application. Si le demandeur d'application est DB2 pour MVS/ESA V3R1, un ou plusieurs serveur(s) d'applications peuvent être connecté(s) simultanément.

[3] L'accès défini par l'application et l'accès défini par le système peuvent être utilisés conjointement pour établir des connexions.

Le terme *serveur secondaire* décrit des systèmesutilisé en tant que serveurs du serveur d'applications.

Si, dans une configuration, tous les systèmes prennent en charge la validation en deux phases, l'unité d'oeuvre répartie (lecture et mise à jour sur plusieurs sites) est prise en charge. Si la validation en deux phases n'est pas prise en charge par tous les systèmes, les mises à jour à l'intérieur d'une unité d'oeuvre sont limitées soit à un seul site ne prenant pas en charge la validation en deux phases, soit au sous-ensemble de sites prenant en charge la validation en deux phases.

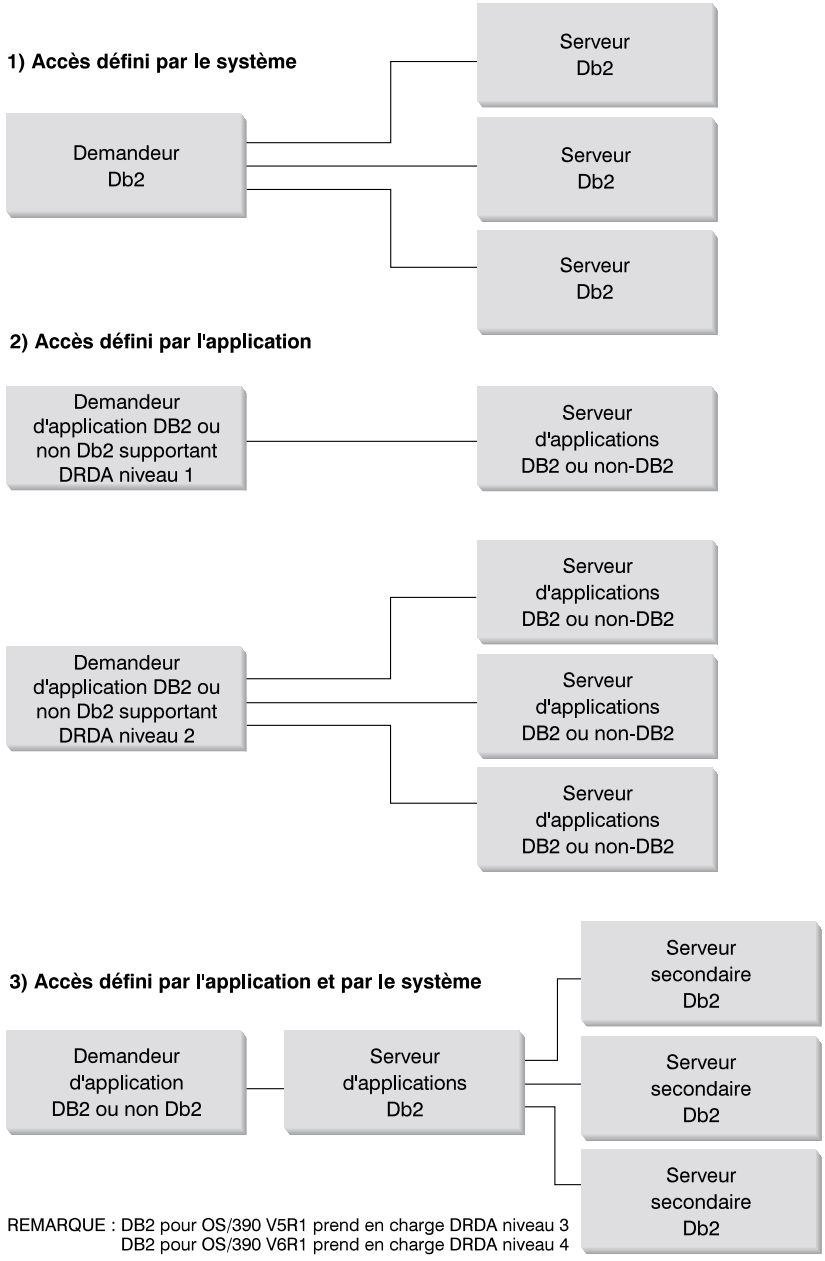

Figure 2. Connexions réparties de DB2 pour MVS/ESA

Le tableau 1 compare les types de connexion de bases de données réparties DB2 pour MVS/ESA.

Tableau 1. Comparaison de connexions de bases de données réparties DB2 pour MVS/ESA

[1] Accès défini par le système	**[2] Accès défini par l'application (l'ensemble des systèmes prenant en charge la validation en deux phases)**	**[3] Accès défini par l'application et accès défini par le système**
Tous les partenaires doivent être des systèmes DB2 pour MVS/ESA.	Permet d'interconnecter deux systèmes DRDA, quels qu'ils soient.	Le demandeur d'application peut être n'importe quel système DRDA ; les serveurs doivent être des systèmes DB2 pour MVS/ESA.
Permet une connexion directe à plusieurs partenaires.	Permet une connexion directe à plusieurs partenaires.	Le demandeur d'application se connecte directement aux serveurs d'applications ; les serveurs d'applications peuvent se connecter à plusieurs serveurs secondaires DB2 pour MVS/ESA.
Chaque application SQL peut avoir plusieurs conversations APPC avec chaque serveur.	Chaque application SQL a une conversation APPC avec chaque serveur.	L'application SQL a une conversation APPC avec chaque serveur ; le serveur d'applications DB2 pour MVS/ESA peut établir plusieurs conversations APPC avec chaque serveur pour l'application.
Permet d'accéder aux ressources locales et éloignées dans une seule portée de validation.	Permet d'accéder aux ressources locales et éloignées dans une seule portée de validation.	Le demandeur d'application et le serveur d'applications peuvent accéder aux données locales et éloignées
Plus efficace au niveau de requêtes volumineuses et de requêtes simultanées.	Plus efficace au niveau des instructions SQL exécutées très peu de fois dans une seule portée de validation.	La connexion demandeur d'application-serveur d'applications se comporte comme **[2]** ; les connexions de serveurs secondaires se comportent comme **[1]**.
Prise en charge du SQL statique ou dynamique mais le serveur définit dynamiquement l'accès au SQL statique lors de la première exécution dans une seule portée de validation.	Permet de lancer des instructions SQL statiques ou dynamiques.	Le demandeur d'application et le serveur d'applications peuvent lancer des instructions SQL statiques ou dynamiques ; les serveurs secondaires prennent en charge le SQL statique ou dynamique mais définissent dynamiquement l'accès au SQL statique lors de la première exécution dans une seule portée de validation.

Tableau 1. Comparaison de connexions de bases de données réparties DB2 pour MVS/ESA (suite)

[1] Accès défini par le système	[2] Accès défini par l'application (l'ensemble des systèmes prenant en charge la validation en deux phases)	[3] Accès défini par l'application et accès défini par le système
Limité aux instructions SQL INSERT, DELETE et UPDATE ainsi qu'aux instructions qui prennent en charge SELECT.	Peut utiliser toute instruction prise en charge par le système qui exécute l'instruction.	Les serveurs d'applications prennent en charge toute forme de SQL ; les serveurs secondaires ne prennent en charge que le SQL DML (par exemple, CREATE ou ALTER)

Configuration du demandeur d'application

DB2 pour MVS/ESA met en oeuvre le support de demandeur d'application DRDA en tant que partie intégrante de la fonction DDF (Distributed Data Facility) de DB2 pour MVS/ESA. La fonction DDF peut être arrêtée de façon indépendante à partir des fonctions de gestion de bases de données de DB2 pour MVS/ESA mais ne peut pas s'exécuter en l'absence du support de gestion de base de données locale de DB2 pour MVS/ESA.

Lorsque DB2 pour MVS/ESA agit en tant que demandeur d'application, il peut connecter des applications s'exécutant sur le système à des serveurs de bases de données éloignés DB2 Universal Database, DB2 pour MVS/ESA, DB2 Universal Database for OS/390, DB2 Universal Database pour AS/400 et DB2 pour VSE & VM, qui mettent en oeuvre la fonction de serveur d'applications DRDA.

Si vous souhaitez que le demandeur d'application DB2 pour MVS/ESA fournisse un accès à la base de données répartie, vous devez prendre en compte les informations suivantes :

- «Définition des données réseau» à la page 9 — Le demandeur d'application doit pouvoir accepter les valeurs RDB_NAME et les convertir en valeurs SNA NETID.LUNAME. DB2 pour MVS/ESA utilise la *base de données de communications DB2 pour MVS/ESA* pour enregistrer les valeurs RDB_NAME et leurs paramètres de réseau correspondants. La base de données de communications permet au demandeur d'application DB2 pour MVS/ESA de transmettre à VTAM les informations SNA requises lors de l'émission de demandes de bases de données réparties.
- «Définition de la sécurité» à la page 21 — Pour que les demandes de bases éloignées soient acceptées par le serveur d'applications, le demandeur d'application doit fournir les informations de sécurités requises par le serveur. DB2 pour MVS/ESA utilise la base de données de communications et RACF pour fournir les informations de sécurité relatives au réseau.

- «Représentation des données» à la page 27 — Vous devez vous assurer que le CCSID du demandeur d'application est compatible avec celui du serveur d'applications.

Définition des données réseau

La plupart des opérations de traitement exécutées dans un environnement de bases de données réparties nécessitent l'échange de messages avec d'autres sites du réseau. Pour que ces opérations s'exécutent correctement, vous devez effectuer les opérations suivantes :

1. Définition du système local.
2. Définition des systèmes éloignés.
3. Définition des communications.
4. Définition de la taille de RU et de la régulation.

Définition du système local

Chaque programme sur le réseau se voit attribuer un NETID et un nom de LU. Votre demandeur d'application DB2 pour MVS/ESA doit donc avoir une valeur NETID.LUNAME lors de sa connexion au réseau. Etant donné que le demandeur d'application DB2 pour MVS/ESA est intégré dans le système de gestion de la base de données DB2 pour MVS/ESA locale, il doit avoir un RDB_NAME. Dans les publications DB2 pour MVS/ESA, il est fait référence au nom RDB_NAME en tant que nom d'*emplacement*.

Définissez le demandeur d'application DB2 pour MVS/ESA pour le réseau SNA en procédant comme suit :

1. Sélectionnez un nom de LU pour votre système DB2 pour MVS/ESA. Le NETID de votre système DB2 pour MVS/ESA s'obtient automatiquement à partir de VTAM au démarrage de DDF.
2. Définissez le nom de LU et le nom d'emplacement dans le *fichier d'amorçage* (BSDS) DB2 pour MVS/ESA. (DB2 pour MVS/ESA limite le nom d'emplacement à 16 caractères).
3. Créez une définition APPL VTAM pour enregistrer le nom de LU sélectionné avec VTAM.

Configuration du fichier d'amorçage de DDF : DB2 pour MVS/ESA lit le fichier d'amorçage pendant le traitement du démarrage pour obtenir des paramètres d'installation du système. L'un des enregistrements stockés dans le fichier d'amorçage est appelé *enregistrement DDF*, parce qu'il contient les informations utilisées par la fonction DDF pour se connecter à VTAM. Ces informations sont les suivantes :

- nom de l'emplacement pour le système DB2 pour MVS/ESA
- nom de LU pour le système DB2 pour MVS/ESA
- mot de passe utilisé lors de la connexion du système DB2 pour MVS/ESA à VTAM

Vous pouvez fournir les informations du fichier d'amorçage de DDF à DB2 pour MVS/ESA de deux manières :

- Utilisez le panneau d'installation DDF DSNTIPR lors de la première installation de DB2 pour MVS/ESA pour fournir les informations du fichier d'amorçage de DDF requises. De nombreux paramètres d'installation ne sont pas développés ici car il est plus important de savoir connecter DB2 pour MVS/ESA à VTAM. La figure 3 explique comment utiliser le panneau d'installation pour enregistrer le nom d'emplacement SYDNEY, le nom de LU LUDBD1 et le mot de passe PSWDBD1 dans le fichier d'amorçage de DB2 pour MVS/ESA.

```
 1 DDF STARTUP OPTION   ===> AUTO      NO (DDF not startable),
                                       AUTO (automatic start up), or
                                       COMMAND (start by command)
 2 DB2 LOCATION NAME    ===> SYDNEY    The name other DB2s use to
                                       refer to this DB2
 3 DB2 NETWORK LUNAME   ===> LUDBD1    The name VTAM uses to refer to this DB2
 4 DB2 NETWORK PASSWORD ===> PSWDBD1   Password for connecting to other DB2s
 5 RLST ACCESS ERROR    ===> NOLIMIT   Action on non-local RLST access error
                                       NOLIMIT   - Run without limit
                                       NORUN     - Do not run at all
                                       1-5000000 - Limit in CPU service units
PRESS:  ENTER to continue   END to exit   HELP for more information
```

Figure 3. DB2 pour MVS/ESA - Panneau d'installation DSNTIPR

- Si DB2 pour MVS/ESA est déjà installé, vous pouvez utiliser l'utilitaire du journal des modifications (DSNJU003) pour la mise à jour des informations dans le fichier d'amorçage.

  La figure 4 à la page 11 montre comment mettre à jour le fichier d'amorçage avec le nom d'emplacement SYDNEY, le nom de LU LUDBD1 et le mot de passe PSWDBD1.

```
//SYSADMB JOB ,'DB2 2.3 JOB',CLASS=A
//*
//*        CHANGE LOG INVENTORY:
//*        UPDATE BSDS WITH
//*             - DB2 LOCATION NAME FOR SYDNEY
//*             - VTAM LUNAME (LUDBD1)
//*             - DB2/VTAM PASSWORD
//*
//DSNBSDS EXEC PGM=DSNJU003
//STEPLIB  DD  DISP=SHR,DSN=DSN230.DSNLOAD
//SYSUT1   DD  DISP=OLD,DSN=DSNC230.BSDS01
//SYSUT2   DD  DISP=OLD,DSN=DSNC230.BSDS02
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSIN    DD  *
 DDF    LOCATION=SYDNEY,LUNAME=LUDBD1,PASSWORD=PSWDBD1
//*
```

Figure 4. Exemple de définition du fichier d'amorçage de DDF

Lorsque DDF est lancé (soit automatiquement au démarrage de DB2 pour MVS/ESA, soit au moyen de la commande START DDF de DB2 pour MVS/ESA), il se connecte à VTAM, transmettant le nom de LU et le mot de passe à VTAM. VTAM reconnaît le système DB2 pour MVS/ESA en vérifiant le nom de LU et le mot de passe (si un mot de passe VTAM est requis) avec les valeurs définies dans l'instruction APPL VTAM DB2 pour MVS/ESA. Le mot de passe VTAM permet de vérifier que DB2 pour MVS/ESA est habilité à utiliser le nom de LU spécifié sur le système VTAM. Le mot de passe VTAM n'est pas transmis via le réseau et ne permet pas de connecter d'autres systèmes du réseau à DB2 pour MVS/ESA.

Si VTAM n'exige pas de mot de passe, ignorez le mot clé PASSWORD= dans l'inventaire du journal des modifications. L'absence de mot clé indique qu'aucun mot de passe VTAM n'est nécessaire.

Création d'une définition APPL VTAM : Après avoir défini le nom de LU VTAM et le mot de passe pour DB2 pour MVS/ESA, il vous faut enregistrer ces valeurs avec VTAM. VTAM utilise l'instruction APPL pour définir les noms de LU locales. La figure 5 à la page 12 illustre la définition du nom de LU LUDBD1 pour VTAM.

```
DB2APPLS VBUILD TYPE=APPL
*
*--------------------------------------------------------------------*
*                                                                    *
*           APPL DEFINITION FOR THE SYDNEY DB2 SYSTEM                *
*                                                                    *
*--------------------------------------------------------------------*
*
LUDBD1   APPL  APPC=YES,                                          X
              AUTH=(ACQ),                                         X
               AUTOSES=1,                                         X
               DMINWNL=10,                                        X
               DMINWNR=10,                                        X
               DSESLIM=20,                                        X
               EAS=9999,                                          X
               MODETAB=RDBMODES,                                  X
               PRTCT=PSWDBD1,                                     X
               SECACPT=ALREADYV,                                  X
               SRBEXIT=YES,                                       X
               VERIFY=NONE,                                       X
               VPACING=2,                                         X
               SYNCLVL=SYNCPT,                                    X
               ATNLOSS=ALL                                        X
```

Figure 5. Exemple de définition APPL pour DB2 pour MVS/ESA

Plusieurs mots clés sont disponibles dans l'instruction APPL VTAM. Vous trouverez des explications détaillées concernant la signification des mots clés dans le manuel *DB2 - Administration Guide*. Les seuls mots clés abordés ici sont ceux qui se rapportent aux rubriques du présent manuel. Les mots clés intéressants de la figure 5 sont décrits comme suit :

LUDBD1

VTAM utilise l'étiquette d'instruction APPL comme nom de LU. Dans ce cas, le nom de LU est LUDBD1. La syntaxe APPL ne prévoit pas de place pour une valeur NETID.LUNAME complète. La valeur de NETID n'est pas spécifiée dans l'instruction APPL VTAM car elle est automatiquement attribuée à toutes les applications VTAM pour le système VTAM.

AUTOSES=1

Nombre de sessions de vainqueur de conflit SNA qui démarrent automatiquement lors de l'émission d'une demande CNOS APPC (modification du nombre de sessions). Une valeur différente de zéro doit être fournie avec AUTOSES pour informer DB2 pour MVS/ESA chaque fois que le traitement de CNOS VTAM échoue.

II n'est pas nécessaire de démarrer automatiquement toutes les sessions APPC entre les deux partenaires de bases de données réparties concernés. Si la valeur de AUTOSES est inférieure au nombre maximal de vainqueurs de conflit (DMINWNL), VTAM diffère le

démarrage des sessions SNA restantes jusqu'à ce qu'elles soient requises par une application de base de données répartie.

DMINWNL=10
Nombre de sessions dans lesquelles ce système DB2 pour MVS/ESA est le vainqueur de conflit. Le paramètre DMINWNL est la valeur par défaut pour le traitement de CNOS, mais celle-ci peut être remplacée pour tout partenaire donné, par l'ajout d'une ligne à la table SYSIBM.SYSLUMODES dans la base de données de communications DB2 pour MVS/ESA.

DMINWNR=10
Nombre de sessions dans lesquelles le système partenaire est le vainqueur de conflit. Le paramètre DMINWNR est la valeur par défaut pour le traitement de CNOS, mais celle-ci peut être remplacée pour tout partenaire donné, par l'ajout d'une ligne à la table SYSIBM.SYSLUMODES dans la base de données de communications DB2 pour MVS/ESA.

DSESLIM=20
Nombre total de sessions (qui ont abouti ou non) que vous pouvez établir entre DB2 pour MVS/ESA et un autre système réparti pour un nom de groupe de mode donné. Le paramètre DSESLIM est la valeur par défaut pour le traitement de CNOS, mais celle-ci peut être remplacée par tout partenaire donné, par l'ajout d'une ligne à la table SYSIBM.SYSLUMODES dans la base de données de communications DB2 pour MVS/ESA.

Si le partenaire ne peut pas prendre en charge le nombre de sessions indiquées par les paramètres DSESLIM, DMINWNL ou DMINWNR, le processus CNOS négocie, pour ces paramètres, de nouvelles valeurs qui peuvent être acceptées par le partenaire.

EAS=9999
Estimation du nombre total de sessions requises par cette LU VTAM.

MODETAB=RDBMODES
Identifie la table MODE VTAM contenant chaque nom de mode DB2 pour MVS/ESA.

PRTCT=PSWDBD1
Identifie le mot de passe VTAM à utiliser lors d'une tentative de connexion de DB2 pour MVS/ESA à VTAM. Si vous omettez le mot clé PRTCT, aucun mot de passe n'est requis et vous devez omettre le mot clé PASSWORD= dans l'inventaire du journal des modifications de DB2 pour MVS/ESA.

SECACPT=ALREADYV
Identifie la valeur de sécurité de conversation SNA la plus élevée qui soit acceptée par ce système DB2 pour MVS/ESA lors de la réception

d'une demande de base de données répartie émanant d'un système éloigné. Le mot clé ALREADYV indique que ce système DB2 pour MVS/ESA peut accepter trois options de sécurité de session SNA issues d'autres systèmes DRDA demandant des données provenant de ce système DB2 pour MVS/ESA :

- SECURITY=SAME (demande qui a déjà été vérifiée et qui contient uniquement l'ID utilisateur du demandeur).
- SECURITY=PGM (demande contenant l'ID utilisateur et le mot de passe du demandeur).
- SECURITY=NONE (demande ne contenant aucune donnée de sécurité). DB2 pour MVS/ESA rejette les demandes DRDA spécifiant SECURITY=NONE.

Il est préférable de toujours spécifier SECACPT=ALREADYV car le niveau de sécurité des conversations SNA de chacun des partenaires DB2 pour MVS/ESA est issu de la base de données de communications DB2 pour MVS/ESA (colonne USERSECURITY de la table SYSIBM.SYSLUNAMES). SECACPT=ALREADYV vous offre la plus grande souplesse pour la sélection des valeurs de USERSECURITY.

VERIFY=NONE
Identifie le niveau de sécurité des sessions SNA (vérification de la LU partenaire) requis par ce système DB2 pour MVS/ESA. La valeur NONE indique que la vérification de la LU partenaire n'est pas requise.

DB2 pour MVS/ESA ne restreint pas votre choix pour le mot clé VERIFY. Dans le cas d'un réseau non sécurisé, VERIFY=REQUIRED est recommandé. VERIFY=REQUIRED permet à VTAM de rejeter les partenaires qui ne peuvent pas effectuer de vérification de LU partenaire. Si vous choisissez VERIFY=OPTIONAL, VTAM effectue la vérification de la LU partenaire uniquement pour les partenaires qui en fournissent le support.

VPACING=2
Attribue la valeur 2 pour la régulation de VTAM.

SYNCLVL=SYNCPT
Indique que DB2 pour MVS/ESA peut prendre en charge la validation en deux phases. VTAM utilise ces informations pour informer le partenaire que la validation en deux phases est disponible. Si ce mot clé est présent, DB2 pour MVS/ESA utilise automatiquement la validation en deux phases si cette dernière peut être prise en charge par le partenaire.

ATNLOSS=ALL

Indique que DB2 pour MVS/ESA doit être informé chaque fois que se termine une session VTAM. C'est la garantie que DB2 pour MVS/ESA exécute une resynchronisation SNA lorsque cela est requis.

DSESLIM, DMINWNL et DMINWNR vous permettent de définir un nombre maximal de sessions VTAM par défaut pour l'ensemble des partenaires. Pour les partenaires requérant un nombre maximal de sessions particulier, la table SYSIBM.SYSLUMODES peut être utilisée pour remplacer le nombre maximal de sessions par défaut. Vous pouvez par exemple vouloir spécifier un nombre maximal de sessions par défaut VTAM adapté à vos systèmes OS/2. Pour d'autres partenaires, vous pouvez, dans la table SYSIBM.SYSLUMODES, créer des lignes pour définir le nombre maximal de sessions voulu. Considérez ces exemples de valeurs :

```
DSESLIM=4,DMINWNL=0,DMINWNR=4
```

Ces paramètres permettent à chacun des partenaires de créer jusqu'à quatre sessions DB2 pour MVS/ESA, le partenaire étant le vainqueur de conflit dans chacune des sessions. Dans la mesure où OS/2 crée les conversations LU 6.2 avec DB2 pour MVS/ESA en faisant d'OS/2 le vainqueur de conflit dans les sessions, vous profitez d'un petit avantage au niveau de la performance. Si OS/2 a une session de vainqueur de conflit disponible, aucune permission n'est requise pour le démarrage d'une nouvelle conversation LU 6.2.

Définition des systèmes éloignés

Lorsqu'une application DB2 pour MVS/ESA demande des données issues d'un système éloigné, DB2 pour MVS/ESA recherche dans les tables de bases de données de communications des informations relatives au système éloigné. Ces recherches portent également sur :

- le nom de LU et le TPN
- les informations de sécurité réseau requises par le site éloigné
- le nombre maximal de sessions et les noms de mode utilisés pour la communication avec le site éloigné

La base de données de communications est un groupe de tables SQL géré par l'administrateur du système DB2 pour MVS/ESA. En tant qu'administrateur du système DB2 pour MVS/ESA, vous devez utiliser le SQL pour insérer des lignes dans la base de données de communications afin de décrire chaque partenaire DRDA potentiel. La base de données de communications se compose de cinq tables :

1. **SYSIBM.SYSLOCATIONS**

   Cette table permet à DB2 pour MVS/ESA de déterminer le nom de LU et la valeur de TPN pour chaque RDB_NAME sélectionné par une application DB2 pour MVS/ESA. Les colonnes sont les suivantes :

LOCATION
RDB_NAME du système éloigné. DB2 pour MVS/ESA limite la longueur de la valeur de RDB_NAME à 16 octets, ce qui représente 2 octets de moins par rapport à la limite de 18 octets définie dans DRDA.

LOCTYPE
Non utilisé actuellement ; doit rester en blanc.

LINKNAME
Nom de LU du système éloigné.

LINKATTR
TPN du système éloigné. Si le système éloigné est un système DB2 pour MVS/ESA ou s'il utilise la valeur TPN DRDA par défaut (X'07F6C4C2',[1]) ; une chaîne vide peut être indiquée pour spécifier le TPN car DB2 pour MVS/ESA choisit automatiquement la valeur correcte.

Si le système éloigné requiert une valeur de TPN différente de la valeur de TPN par défaut, vous devez mentionner cette valeur dans cette colonne.

2. **SYSIBM.SYSLUNAMES**

Cette table définit les attributs de réseau des systèmes éloignés. Les colonnes sont les suivantes :

LUNAME
Nom de LU du système éloigné.

SYSMODENAME
Nom de mode de connexion VTAM utilisé pour l'établissement de conversations *entre deux systèmes* DB2 pour MVS/ESA pour le support du serveur secondaire DB2 pour MVS/ESA (accès défini par le système). Une valeur à blanc dans cette colonne indique qu'il faut utiliser IBMDB2LM pour les conversations du système DB2 pour MVS/ESA.

USERSECURITY
Options d'acceptation de sécurité réseau requises quant au système éloigné lorsque ce système DB2 pour MVS/ESA fait office de serveur pour le système éloigné (conditions requises de *sécurité entrante*).

ENCRYPTPSWDS
Indique si les mots de passe échangés avec ce partenaire sont codés ou non. Les mots de passe codés sont uniquement pris en charge par les demandeurs et les serveurs DB2 pour MVS/ESA.

---

1. C'est cette valeur TPN qui s'applique *actuellement* à DB2 pour VM.

MODESELECT

Détermine si la table SYSIBM.SYSMODESELECT est utilisée ou non pour la sélection d'une entrée de mode de connexion VTAM (nom de mode) basée sur l'utilisateur final ou l'application qui émet la demande. Si cette colonne contient un 'Y', la table SYSIBM.SYSMODESELECT est utilisée pour obtenir le nom de mode pour chaque demande de base de données répartie sortante.

Si MODESELECT contient une autre valeur que 'Y', le nom de mode IBMDB2LM est utilisé pour les demandes d'accès défini par le système et le nom de mode IBMRDB est utilisé pour les demandes DRDA.

La colonne MODESELECT vous permet de donner la priorité aux demandes de base de données répartie en spécifiant une classe de service VTAM associée au nom de mode.

USERNAMES

Niveau d'identification du site émetteur et conversion de l'ID utilisateur requis. Cette colonne spécifie également les paramètres de sécurité utilisés par ce sous-système DB2 pour MVS/ESA lors de la demande de données émanant du partenaire éloigné (conditions requises de *sécurité sortante*). Cette colonne peut avoir pour valeur I, O, ou B.

3. **SYSIBM.SYSLUMODES**

Cette table permet de définir le nombre maximal de sessions LU 6.2 (limites CNOS) pour chaque système partenaire. Les colonnes sont les suivantes :

LUNAME

Nom de LU du système éloigné.

MODENAME

Nom du mode de connexion VTAM dont les limites sont spécifiées. Une valeur à blanc revient à indiquer IBMDB2LM.

CONVLIMIT

Nombre maximal de conversations actives entre le système local DB2 pour MVS/ESA et le système éloigné pour ce mode de connexion. Cette valeur permet de remplacer le paramètre DSESLIM dans l'instruction de définition APPL VTAM pour ce mode de connexion, qui fournit le nombre maximal de sessions VTAM par défaut pour DB2 pour MVS/ESA.

La valeur sélectionnée dans CONVLIMIT est utilisée pendant le processus CNOS afin de définir CONVLIMIT/2 pour DMINWNR et DMINWNL.

AUTO

Détermine si la pré-allocation de sessions et le traitement de CNOS sont initialisés automatiquement au démarrage de DDF ou reportés jusqu'à la première référence au nom de LU via ce mode de connexion.

4. **SYSIBM.SYSMODESELECT**

   Cette table vous permet de spécifier différents noms de mode pour des utilisateurs finals individuels et des applications DB2 pour MVS/ESA. Dans la mesure où une classe de service (COS) peut être associée à chaque nom de mode VTAM, vous pouvez utiliser cette table pour attribuer des priorités de transmission de réseau aux applications de base de données répartie, sur la base d'une combinaison de AUTHID, PLANNAME et LUNAME. Les colonnes sont les suivantes :

   AUTHID

   ID autorisation de l'utilisateur DB2 pour MVS/ESA. La valeur par défaut est à blanc, ce qui indique que le nom de mode de connexion spécifié s'applique à tous les ID autorisation.

   PLANNAME

   Nom de plan associé à l'application demandant l'accès à un système de bases de données éloignées. La valeur par défaut est à blanc, ce qui indique que le nom de mode de connexion spécifié s'applique à tous les noms de plan. Le nom de plan utilisé pour la commande BIND PACKAGE est DSNBIND.

   LUNAME

   Nom de LU associé au système de bases de données éloignées.

   MODENAME

   Nom de mode de connexion VTAM à utiliser lors de l'acheminement d'une demande de base de données répartie vers le système éloigné indiqué. Par défaut, cette valeur est à blanc, pour indiquer que l'on doit utiliser IBMDB2LM pour les conversations à accès défini par le système et IBMRDB pour les conversations DRDA.

5. **SYSIBM.SYSUSERNAMES**

   Cette table permet de gérer les noms d'utilisateurs finals via des mots de passe, des conversions de noms et des identifications de site émetteur. DB2 pour MVS/ESA utilise le nom de l'utilisateur comme ID autorisation. La plupart des autres produits utilisent ce nom comme ID utilisateur.

   Avec cette table, vous pouvez utiliser la conversion de nom pour imposer l'utilisation de valeurs différentes pour l'ID utilisateur SNA et l'ID autorisation DB2 pour MVS/ESA. Le processus de conversion de nom est autorisé pour les demandes destinées à un système éloigné (demandes *sortantes*) et pour les demandes émanant d'un système éloigné (demandes *entrantes*). Si les mots de passe ne sont pas codés, cette table est la source

du mot de passe de l'utilisateur final lorsque l'ID utilisateur et le mot de passe sont envoyés vers un site éloigné. Les colonnes sont les suivantes :

TYPE Description de l'utilisation de la ligne (qu'il s'agisse ou non d'une ligne décrivant les conversions de noms pour les demandes sortantes ou entrantes d'identification de site émetteur).

AUTHID
Pour la conversion de nom sortante, il s'agit de l'ID autorisation DB2 pour MVS/ESA à convertir. Pour la conversion de nom entrante, il s'agit de l'ID utilisateur SNA à convertir. Dans les deux cas, une valeur AUTHID à blanc s'applique à tous les ID autorisation ou utilisateurs.

LUNAME
Nom de LU du système éloigné auquel s'applique cette ligne. Si la valeur est à blanc, la valeur NEWAUTHID s'applique à tous les systèmes.

NEWAUTHID
Nouveau nom d'utilisateur final (ID utilisateur SNA ou ID autorisation DB2 pour MVS/ESA). Une valeur à blanc indique qu'il n'est pas nécessaire de convertir l'ID.

PASSWORD
Mot de passe utilisé pour la conversation d'allocation si les mots de passe ne sont pas codés (ENCRYPTPSWDS = 'N' dans SYSIBM.SYSLUNAMES). Si les mots de passe sont codés, ignorez cette colonne.

Paramétrage des communications

VTAM est le gestionnaire de communications des systèmes MVS. VTAM accepte les verbes LU 6.2 à partir de DB2 pour MVS/ESA et les convertit en flots de données LU 6.2 que vous pouvez transmettre sur le réseau. Pour permettre à VTAM de communiquer avec les applications partenaires définies dans les bases de données de communications DB2 pour MVS/ESA, vous devez fournir à VTAM les informations suivantes :

- Le nom de LU pour chaque serveur.

  Lorsque DB2 pour MVS/ESA communique avec VTAM, il est autorisé à ne transmettre qu'un seul nom de LU (pas NETID.LUNAME) à VTAM pour identifier la destination voulue. Ce nom de LU doit être unique parmi les noms de LU connus du système VTAM local, permettant ainsi à VTAM de déterminer les noms de NETID et de LU à partir du nom de LU transmis par DB2 pour MVS/ESA. Le fait que les noms de LU soient uniques sur le réseau SNA d'une entreprise simplifie grandement le processus de définition des ressources VTAM. Toutefois, cela n'est pas toujours possible. Si les noms de LU de vos réseaux SNA ne sont pas uniques, vous devez utiliser la conversion de nom de LU VTAM afin de créer la combinaison

NETID.LUNAME correcte pour un nom de LU qui n'est pas unique. Vous trouverez la description de cette procédure dans la section «Resource Name Translation» du manuel *VTAM Network Implementation Guide*.

L'emplacement et la syntaxe de ces définitions VTAM permettant de définir des noms de LU éloignée dépendent essentiellement du type de connexion physique et logique du système éloigné au système VTAM local.

- La taille de RU, la taille de la fenêtre de régulation et la classe de service pour chaque nom de mode. Créez une entrée dans la table de modes VTAM pour chaque nom de mode spécifié dans la base de données de communications. Vous devez également définir IBMRDB et IBMDB2LM.
- Les profils VTAM et RACF pour l'algorithme de vérification de la LU, si vous pensez utiliser la vérification de LU partenaire.

Définition de la taille de RU et de la régulation

Les entrées de table de modes VTAM que vous avez définies spécifient les tailles de RU et la régulation. Si ces valeurs ne sont pas mentionnées correctement, des effets indésirables peuvent se produire pour toutes les applications VTAM.

Une fois que vous avez choisi les tailles de RU, le nombre maximal de sessions et la régulation, il est très important d'évaluer l'impact que ces valeurs peuvent avoir sur le réseau VTAM existant. Lors de l'installation d'une nouvelle base de données répartie, vous devez tenir compte des éléments suivants :

- Dans le cas des connexions VTAM CTC, vérifiez que la valeur du paramètre MAXBFRU est suffisante pour gérer la taille de RU plus les 29 octets ajoutés par VTAM pour l'en-tête de demande et l'en-tête de transmission SNA. MAXBFRU se mesure en unités de 4 ko, il doit donc prendre une valeur minimale de 2 pour pouvoir gérer un RU de 4 ko.
- Dans le cas de connexions NCP, assurez-vous que la valeur du paramètre MAXDATA est suffisante pour gérer la taille de RU plus 29 octets. Si vous indiquez une taille de RU de 4 ko, MAXDATA doit prendre au moins la valeur 4125.

  Si vous indiquez le paramètre NCP MAXBFRU, sélectionnez une valeur pouvant gérer la taille de RU plus 29 octets. Dans la cas de NCP, le paramètre MAXBFRU définit le nombre de tampons d'E-S VTAM pouvant prendre en charge l'unité d'information acheminable (PIU). Si vous choisissez une taille de tampon IOBUF de 441, MAXBFRU=10 traite correctement une RU de 4 ko car 10*441 est supérieur à 4096+29.
- Le manuel *DRDA Connectivity Guide* indique comment évaluer l'impact de votre base de données répartie sur le pool IOBUF VTAM. Si une trop grande quantité de ressources de pool IOBUF est utilisée, les performances du système VTAM seront affectées pour toutes les applications VTAM.

Définition de la sécurité

Lorsqu'un système éloigné exécute des opérations de traitement sur des bases de données réparties au nom d'une application SQL, il doit être capable de répondre aux critères de sécurité du demandeur d'application, du serveur d'applications et du réseau reliant ces derniers entre eux. Ces critères entrent dans une ou plusieurs des catégories suivantes :

- sélection des noms d'utilisateurs finals
- paramètres de sécurité réseau
- sécurité du gestionnaire de bases de données
- sécurité assurée par un sous-système de sécurité externe
- représentation des données

Sélection des noms d'utilisateurs finals

Dans les systèmes MVS, les utilisateurs finals sont identifiés par un *ID utilisateur* comportant de 1 à 8 caractères. Cet ID utilisateur doit être unique pour un système MVS particulier mais ne doit pas forcément l'être sur tout le réseau SNA. Par exemple, prenons le cas de deux utilisateurs s'appelant tous les deux JONES ; l'un se trouve sur le système NEWYORK et l'autre sur le système DALLAS. S'il s'agit d'une seule et même personne, il n'existe aucun risque de conflit. Cependant, si l'utilisateur JONES de DALLAS n'est pas le même que l'utilisateur JONES de NEWYORK, le réseau SNA (et, par conséquent, les systèmes de bases de données réparties de ce réseau) ne pourront pas faire la distinction entre ces deux utilisateurs. Si vous ne remédiez pas à cette situation, JONES de DALLAS pourra utiliser les droits de JONES de NEWYORK.

DB2 pour MVS/ESA fournit un support de conversion pour les noms d'utilisateurs finals afin d'éviter les conflits de dénomination. Lorsqu'une application au niveau du demandeur d'application DB2 pour MVS/ESA émet une demande de base de données répartie, DB2 pour MVS/ESA exécute la conversion du nom si la base de données de communications spécifie que la *conversion de nom sortante* est requise. Si la conversion de nom sortante est sélectionnée, DB2 pour MVS/ESA exige toujours qu'un mot de passe soit envoyé avec chaque demande de base de données répartie sortante.

Pour activer la conversion de nom sortante dans DB2 pour MVS/ESA, vous devez définir 'O' ou 'B' pour la colonne USERNAMES de la table SYSIBM.SYSLUNAMES. Si 'O' est défini pour USERNAMES, la conversion du nom d'utilisateur final s'effectue pour les demandes sortantes. Si 'B' est défini pour USERNAMES, la conversion du nom d'utilisateur final s'effectue pour les demandes sortantes et entrantes.

Etant donné que l'autorisation DB2 pour MVS/ESA dépend à la fois de l'ID utilisateur de l'utilisateur final et de l'ID utilisateur du propriétaire du module ou du plan DB2 Universal Database for OS/390, le processus de conversion

du nom d'utilisateur final s'opère pour l'ID utilisateur de l'utilisateur final, l'ID utilisateur du propriétaire du plan et l'ID utilisateur du propriétaire du module.[2] Le processus de conversion de nom recherche dans la table SYSIBM.SYSUSERNAMES, dans la séquence suivante, une ligne qui corresponde à l'un des modèles (TYPE.AUTHID.LUNAME) suivants :

1. O.AUTHID.LUNAME— Règle de conversion pour un utilisateur final particulier vers un système partenaire particulier.
2. O.AUTHID.espace— Règle de conversion pour un utilisateur final particulier vers n'importe quel système partenaire.
3. O.espace.LUNAME— Règle de conversion pour n'importe quel utilisateur vers un système partenaire particulier.

S'il n'existe aucune ligne correspondante, DB2 pour MVS/ESA rejette la demande de base de données répartie. S'il existe une ligne correspondante, la valeur de la colonne NEWAUTHID est utilisée comme ID autorisation. (Une valeur NEWAUTHID à blanc indique que le nom original est utilisé sans conversion).

Reportez-vous à l'exemple déjà évoqué. Vous souhaitez attribuer à JONES de NEWYORK un nom différent (NYJONES) lorsque JONES envoie des demandes de bases de données réparties à DALLAS. Dans l'exemple, imaginez que l'application utilisée par JONES appartienne à DSNPLAN (propriétaire du plan DB2 pour MVS/ESA) et qu'il ne soit pas nécessaire de convertir cet ID utilisateur lors de son envoi à DALLAS. Les instructions SQL requises pour la fourniture des règles de conversion des noms dans les bases de données de communications sont illustrées à la figure 6.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', 'O');
INSERT INTO SYSIBM.SYSLOCATIONS
     (LOCATION, LOCTYPE, LINKNAME, LINKATTR)
  VALUES ('DALLAS', ' ', 'LUDALLAS', '');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'JONES', 'LUDALLAS', 'NYJONES', 'JONESPWD');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'DSNPLAN', 'LUDALLAS', ' ', 'PLANPWD');
```

Figure 6. SQL pour conversion de nom sortante

2. Si la demande est envoyée à un serveur DB2 pour MVS/ESA, la conversion de nom s'opère également pour le propriétaire du module et pour celui du plan. Aucun mot de passe n'est jamais associé aux noms de propriétaires de module et de plan.

Les tables de bases de données qui en résultent sont illustrées à la figure 7 :

NEWYORK.SYSIBM.SYSLOCATIONS

LOCATION	LOCTYPE	LINKNAME	LINKATTR
DALLAS		LUDALLAS	

NEWYORK.SYSIBM.SYSLUNAMES

LUNAME	SYSMODENAME	USERSECURITY	ENCRYPTPSWDS	MODESELECT	USERNAMES
LUDALLAS		A	N	N	O

NEWYORK.SYSIBM.SYSUSERNAMES

TYPE	AUTHID	LUNAME	NEWAUTHID	PASSWORD
0 0	JONES DSNPLAN	LUDALLAS LUDALLAS	NYJONES	JONESPWD PLANPWD

Figure 7. Conversion de nom sortante

Sécurité réseau

Une fois que le demandeur d'application a sélectionné les noms d'utilisateurs finals pour représenter l'application éloignée, il doit fournir les données de sécurité réseau LU 6.2 requises. Il existe trois principales fonctions de sécurité réseau pour les unités logiques LU 6.2 :

- Sécurité au niveau de la session, définie par le mot clé VERIFY dans l'instruction APPL VTAM. Reportez-vous aux commentaires de la figure 5 à la page 12, pour connaître la procédure à suivre pour la définition des options de sécurité au niveau de la session.
- Sécurité au niveau de la conversation, définie par le contenu de la table SYSIBM.SYSLUNAMES.

- Cryptage des données, pris en charge uniquement pour VTAM 3.4 et les éditions ultérieures de VTAM.

Dans la mesure où le serveur d'applications est chargé de la gestion des ressources de bases de données, il détermine quelles sont les fonctions de sécurité réseau requises pour le demandeur d'application. Vous devez enregistrer les conditions de sécurité requises au niveau de la conversation de chaque serveur d'applications dans la table SYSIBM.SYSLUNAMES en définissant la colonne USERNAMES de cette table de manière à ce qu'elle reflète les conditions requises par le serveur d'applications.

Les options possibles pour les conversations SNA sont les suivantes :

SECURITY=SAME

Egalement connue sous le nom de sécurité déjà vérifiée, cette option suppose que seul l'ID utilisateur de l'utilisateur final est transmis au système éloigné (aucun mot de passe n'est transmis). Utilisez ce niveau de sécurité de conversation lorsque la colonne USERNAMES dans SYSIBM.SYSLUNAMES ne contient ni 'O' ni 'B'.

Dans la mesure où DB2 pour MVS/ESA lie la conversion de nom d'utilisateur final à la sécurité de la conversation sortante, vous n'êtes pas autorisé à utiliser SECURITY=SAME lorsque la conversion de nom d'utilisateur final sortante est activée.

SECURITY=PGM

Cette option déclenche l'envoi de l'ID utilisateur final et du mot de passe au système éloigné pour validation. Utilisez cette option de sécurité lorsque la colonne USERNAMES de la table SYSIBM.SYSLUNAMES contient 'O' ou 'B'.

En fonction des options définies dans la table SYSIBM.SYSLUNAMES, DB2 pour MVS/ESA obtient le mot de passe de l'utilisateur final de deux sources différentes :

- Les mots de passe non codés proviennent de la colonne PASSWORD de la table SYSIBM.SYSUSERNAMES. DB2 pour MVS/ESA extrait les mots de passe de la table SYSIBM.SYSUSERNAMES lorsque la colonne ENCRYPTPSWDS de la table SYSIBM.SYSLUNAMES n'a pas pour valeur 'Y'. Les mots de passe obtenus par ce biais peuvent être transmis à n'importe quel serveur d'application DRDA.

  La figure 8 à la page 25 définit les mots de passe pour SMITH et JONES. La colonne LUNAME de l'exemple contient des valeurs à blanc, par conséquent ces mots de passe sont utilisés pour n'importe quelle tentative d'accès à un système éloigné de la part de SMITH ou de JONES.

```
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'JONES', ' ', ' ', 'JONESPWD');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'SMITH', ' ', ' ', 'SMITHPWD');
```

Figure 8. Envoi de mots de passe sur des sites éloignés

- Les mots de passe codés sont envoyés sur le site éloigné lorsque la colonne ENCRYPTPSWDS de la table SYSIBM.SYSLUNAMES contient 'Y'. Les mots de passe codés sont extraits de RACF (ou d'un produit équivalent), et ne peuvent être interprétés que par un autre système DB2 pour MVS/ESA. En cas de communication avec un système autre que DB2 pour MVS/ESA, n'indiquez pas 'Y' dans ENCRYPTPSWDS.

  DB2 pour MVS/ESA recherche dans la table SYSIBM.SYSUSERNAMES l'ID utilisateur (valeur NEWAUTHID) à transmettre au système éloigné. Ce nom converti permet l'extraction du mot de passe RACF. Si vous ne souhaitez pas convertir les noms, vous devez créer des lignes dans la table SYSIBM.SYSUSERNAMES qui déclenchent l'envoi des noms sans conversion. La figure 9 permet l'envoi de demandes à LUDALLAS et à LUNYC sans conversion du nom d'utilisateur final (ID utilisateur).

```
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('O', ' ', 'LUDALLAS', ' ', ' ');
```

Figure 9. Envoi de mots de passe codés sur des sites éloignés

SECURITY=NONE

Cette option n'est pas prise en charge par DRDA ; DB2 pour MVS/ESA ne prévoit donc rien pour cette option de sécurité.

Sécurité du gestionnaire de bases de données

La conversion de nom sortante constitue, pour le demandeur d'application, l'un des moyens de participer à la sécurité d'une base de données répartie, comme indiqué à la section «Sélection des noms d'utilisateurs finals» à la page 21. Vous pouvez utiliser la fonction de conversion du nom sortante pour contrôler l'accès à chaque serveur d'applications, sur la base de l'identité de l'utilisateur final et de l'application effectuant la demande. Les autres moyens

permettant au demandeur d'application DB2 pour MVS/ESA de contribuer à la sécurité des systèmes répartis sont les suivants :

Définition des accès aux applications éloignées

Les utilisateurs finals définissent les accès aux applications éloignées au niveau du serveur d'applications via la commande BIND PACKAGE de DB2 pour MVS/ESA. DB2 pour MVS/ESA *ne limite pas* l'utilisation de la commande BIND PACKAGE au niveau du demandeur. Toutefois, un utilisateur final ne peut pas utiliser de module éloigné si celui-ci ne fait pas partie d'un plan DB2 pour MVS/ESA. DB2 pour MVS/ESA *limite* l'utilisation de la commande BIND PLAN. Un utilisateur final ne peut pas ajouter le module éloigné à un plan, à moins de bénéficier du privilège BIND ou BINDADD avec l'instruction GRANT de DB2 pour MVS/ESA.

Lors de la définition de l'accès à un module, utilisez l'option ENABLE/DISABLE pour spécifier si le module doit être utilisé par TSO, CICS/ESA, IMS/ESA ou par un sous-système DB2 pour MVS/ESA éloigné.

Exécution d'applications éloignées

Pour exécuter une application éloignée, l'utilisateur final DB2 pour MVS/ESA doit disposer des droits d'exécution du plan DB2 pour MVS/ESA associé à cette application. Le propriétaire du plan DB2 pour MVS/ESA dispose automatiquement des droits d'exécution du plan. Les autres utilisateurs finals peuvent également se voir accorder les droits d'exécution du module à l'aide de l'instruction GRANT EXECUTE de DB2 pour MVS/ESA. Le propriétaire de l'application de base de données répartie peut alors contrôler l'utilisation de l'application à raison d'un utilisateur à la fois.

Sous-système de sécurité

Le sous-système de sécurité externe sur les systèmes MVS est fourni par RACF ou des produits équivalents qui offrent une interface compatible avec RACF. Le demandeur d'application DB2 pour MVS/ESA n'a pas d'appels directs avec le sous-système de sécurité externe, exception faite du support de mot de passe codé dont vous trouverez la description dans la section «Sécurité réseau» à la page 23. Toutefois, le sous-système de sécurité externe est utilisé indirectement au niveau du demandeur d'application, dans les situations suivantes :

- Le produit permettant de connecter l'utilisateur final à DB2 pour MVS/ESA utilise le sous-système de sécurité externe pour valider l'identité de l'utilisateur final (ID utilisateur et mot de passe). Cela se produit avant que l'utilisateur final ne se connecte à DB2 pour MVS/ESA. Comme déjà mentionné, CICS/ESA, TSO et IMS/ESA sont des exemples de produits qui permettent de connecter les utilisateurs finals à DB2 pour MVS/ESA.

- Si vous utilisez la sécurité au niveau de la session SNA (via le mot clé VERIFY dans l'instruction APPL VTAM de DB2 pour MVS/ESA), le sous-système de sécurité externe est appelé pour valider l'identité du système éloigné.

Représentation des données

DB2 pour MVS/ESA est livré avec un ID de jeu de caractères codés d'installation par défaut est 500. Cette valeur par défaut n'est probablement *pas* correcte pour votre installation.

Lors de l'installation de DB2 pour MVS/ESA, vous devez définir le CCSID d'installation en fonction du CCSID des caractères générés et transmis à DB2 pour MVS/ESA par les unités d'entrée au niveau de votre site. Ce CCSID est généralement déterminé par la langue nationale utilisée. Si le CCSID d'installation n'est pas correct, la conversion des caractères produira des résultats erronés. Pour connaître la liste des CCSID pris en charge pour chaque pays ou langue nationale, reportez-vous au manuel *DB2 Connect User's Guide*.

Vous devez vous assurer que votre sous-système DB2 pour MVS/ESA dispose de la fonction de conversion de chaque CCSID du serveur d'applications en CCSID d'installation du sous-système DB2 pour MVS/ESA. DB2 pour MVS/ESA fournit les tables de conversion pour les combinaisons de CCSID source et cible les plus répandues, mais pas pour toutes les combinaisons possibles. Vous pouvez compléter l'ensemble de tables et de routines de conversion disponibles, si nécessaire. Pour en savoir plus sur la conversion de caractères DB2 pour MVS/ESA, reportez-vous au manuel *DB2 Administration Guide*.

Configuration du serveur d'applications

Le support de serveur d'applications de DB2 pour MVS/ESA lui permet d'assurer une fonction serveur pour les demandeurs d'application DRDA. Le demandeur d'application connecté à un serveur d'applications DB2 pour MVS/ESA peut être :

- un demandeur DB2 pour MVS/ESA
- DB2 Connect Version 7 pouvant s'exécuter sous AIX, HP-UX, OS/2, SCO, Solaris, Linux, Windows 9x ou Windows NT
- DB2 Universal Database Enterprise Edition Version 7 ou DB2 Universal Database Extended - Enterprise Edition avec utilisation du support DB2 Connect
- un demandeur DDCS version 2 pouvant s'exécuter sous AIX, HP-UX, OS/2, Solaris, Windows 3.1, Windows 3.11 pour Workgroups, Windows 95 ou Windows NT ainsi que sous SCO, SGI ou SINIX
- un demandeur OS/400

- un demandeur DB2 pour VM
- tout autre produit prenant en charge les protocoles pour demandeur d'application DRDA

Pour n'importe quel demandeur d'application connecté à un serveur d'applications DB2 pour MVS/ESA, ce dernier prend en charge l'accès à la base de données, comme suit :

- Le demandeur d'application est autorisé à accéder aux tables stockées au niveau du serveur d'applications DB2 pour MVS/ESA. Le demandeur d'application doit créer un module au niveau du serveur d'applications DB2 pour MVS/ESA pour que l'application puisse s'exécuter. Le serveur d'applications DB2 pour MVS/ESA utilise le module pour localiser les instructions SQL de l'application au moment de l'exécution.
- Le demandeur d'application peut informer le serveur d'applications DB2 pour MVS/ESA que l'accès doit être restreint aux activités en lecture seulement si la connexion serveur-demandeur DRDA ne prend pas en charge le processus de validation en deux phases. Par exemple, un demandeur V2R3 DB2 pour MVS/ESA avec un récepteur CICS informera le serveur d'applications DB2 pour MVS/ESA que les mises à jour ne sont pas autorisées.
- Le demandeur d'application peut aussi se voir accorder l'autorisation d'accéder aux tables stockées au niveau d'autres systèmes DB2 pour MVS/ESA sur le réseau utilisant l'accès défini par le système. L'accès défini par le système permet au demandeur d'application d'établir des connexions à plusieurs systèmes de bases de données dans une seule unité d'oeuvre.

Définition des données réseau

Pour que le serveur d'applications DB2 pour MVS/ESA puisse correctement traiter les demandes de bases de données réparties, vous devez procéder comme suit :

1. Définissez le serveur d'applications sur le gestionnaire de communications local.
2. Définissez chaque destination de serveur secondaire potentiel pour permettre au serveur d'applications DB2 pour MVS/ESA de réacheminer les demandes SQL vers leur destination finale.
3. Définissez la sécurité nécessaire.
4. Prévoyez la représentation des données.

Définition du serveur d'applications

Pour que le serveur d'applications puisse recevoir des demandes de bases de données réparties, il doit être défini sur le gestionnaire de communications local et avoir une valeur RDB_NAME unique. Vous devez effectuer les opérations suivantes pour définir correctement le serveur d'applications :

1. Sélectionnez le nom de LU et le RDB_NAME devant être utilisés par le serveur d'applications DB2 pour MVS/ESA. Le procédé d'enregistrement de ces noms dans DB2 pour MVS/ESA et VTAM est identique à celui décrit à la section «Définition du système local» à la page 9. Le RDB_NAME choisi pour DB2 pour MVS/ESA doit être fourni à l'ensemble des utilisateurs finals et des demandeurs d'application pour lesquels la connectivité au serveur d'applications est nécessaire.
2. Enregistrez la valeur NETID.LUNAME pour le serveur d'applications DB2 pour MVS/ESA avec chaque demandeur d'application requérant l'accès, de sorte que le demandeur d'application puisse acheminer les demandes SNA vers le serveur DB2 pour MVS/ESA. Il en est ainsi même dans les cas où le demandeur d'application est en mesure d'exécuter un routage de réseau dynamique, car le demandeur d'application doit connaître le NETID.LUNAME avant que le routage de réseau dynamique puisse être utilisé.
3. Fournissez le TPN par défaut de DRDA (X'07F6C4C2') pour chaque demandeur d'application car DB2 pour MVS/ESA utilise cette valeur automatiquement.
4. Créez une entrée dans la table de modes VTAM pour chaque nom de mode demandé par un demandeur d'application. Ces entrées décrivent les tailles de RU, la taille de la fenêtre de régulation et la classe de service pour chaque nom de mode.
5. Définissez le nombre maximal de sessions pour les demandeurs d'application qui se connectent au serveur d'applications DB2 pour MVS/ESA. L'instruction VTAM APPL définit le nombre maximal de sessions par défaut pour tous les systèmes partenaires. Si vous voulez définir des valeurs par défaut uniques pour un partenaire donné, vous pouvez utiliser la table SYSIBM.SYSLUMODES de la base de données de communications (CDB).

   Reportez-vous à la section «Définition de la taille de RU et de la régulation» à la page 20, pour savoir comment visualiser votre réseau VTAM.
6. Créez des entrées dans la base de données de communications de DB2 pour MVS/ESA afin d'identifier les demandeur d'applications autorisés à se connecter au serveur d'applications DB2 pour MVS/ESA. Deux approches de base permettent de définir des entrées de base de données de communications pour les demandeurs d'application sur le réseau :
   a. Vous pouvez insérer une ligne dans la table SYSIBM.SYSLUNAMES qui fournit les valeurs par défaut à utiliser pour toute LU ne faisant

pas l'objet d'une description particulière dans la base de données de communication (la ligne par défaut contient une valeur à blanc dans la colonne LUNAME). Cette approche vous permet de définir des attributs particuliers pour certaines des LU de votre réseau, tout en définissant des valeurs par défaut pour toutes les autres LU.

Par exemple, vous pouvez permettre au système DALLAS (autre système DB2 pour MVS/ESA) d'envoyer des demandes de bases de données réparties déjà vérifiées (LU 6.2 SECURITY=SAME), tout en demandant aux gestionnaires de bases de données d'envoyer des mots de passe. Par ailleurs, vous pouvez ne pas vouloir enregistrer d'entrées dans la base de données de communication de chaque gestionnaire de bases de données, en particulier si ces derniers sont nombreux. La figure 10 montre comment la base de données de communications peut servir à spécifier SECURITY=SAME pour le système DALLAS, tout en imposant SECURITY=PGM pour tous les autres demandeurs.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES (' ', ' ', 'C', 'N', 'N', ' ');
```

Figure 10. Définition de valeurs par défaut pour les connexions de demandeurs d'application

b. Vous pouvez utiliser la base de données de communications pour accorder des droits à chaque demandeur d'application individuellement sur le réseau, selon l'une des deux méthodes suivantes :

   - N'enregistrez pas de ligne par défaut dans la table SYSIBM.SYSLUNAMES. En l'absence de ligne par défaut (ligne contenant un nom de LU à blanc), DB2 pour MVS/ESA requiert une ligne dans la table SYSIBM.SYSLUNAMES contenant le nom de LU de chaque demandeur d'application essayant de se connecter. Si la base de données de communications ne contient pas de ligne correspondante, le demandeur d'application se voit refuser l'accès.
   - Enregistrez une ligne par défaut dans la table SYSIBM.SYSLUNAMES indiquant que l'identification du site émetteur est requise (colonne USERNAMES ayant pour valeur 'I' ou 'B'). Du coup, DB2 pour MVS/ESA limite l'accès aux seuls demandeur d'application et aux utilisateurs finals identifiés dans la table SYSIBM.SYSUSERNAMES, comme décrit dans la section «Identification du site émetteur» à la page 35. Il se peut que vous souhaitiez utiliser cette approche si les règles de conversion de nom que vous utilisez requièrent une ligne contenant un nom de LU à

blanc dans la table SYSIBM.SYSLUNAMES, mais que vous ne voulez pas que DB2 pour MVS/ESA utilise cette ligne pour permettre un accès non restreint au serveur d'applications DB2 pour MVS/ESA.

Dans la figure 11, aucune ligne ne contient de valeur à blanc dans la colonne LUNAME, par conséquent DB2 pour MVS/ESA refuse l'accès à toute LU autre que LUDALLAS ou LUNYC.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', ' ');
```

Figure 11. Identification de connexions de demandeurs d'application individuelles

Définition de serveurs secondaires

DB2 pour MVS/ESA ne met pas en oeuvre de serveur de bases de données comme défini dans DRDA. En revanche, DB2 pour MVS/ESA fournit des serveurs secondaires permettant l'accès à plusieurs systèmes DB2 pour MVS/ESA dans une seule unité d'oeuvre, via l'accès défini par le système.

Différences de SQL : Le SQL pris en charge par l'accès défini par le système diffère de manière significative de l'unité d'oeuvre éloignée DRDA :

- L'instruction SQL CONNECT n'est pas utilisée pour établir une connexion avec un serveur secondaire. En revanche, il est possible d'accéder au serveur en spécifiant des noms d'objets SQL composés de trois parties. Par exemple, l'instruction SQL suivante est acheminée vers le serveur à accès défini par le système, CHICAGO :

  ```
  SELECT * FROM CHICAGO.USER.TABLE;
  ```

- Les instructions SQL DDL (par exemple, CREATE) ne sont pas autorisées.
- L'accès défini par le système ne prend pas en charge la définition d'accès éloigné (par exemple, BIND PACKAGE). Par conséquent, vous n'êtes pas tenu de définir un accès à votre application au niveau du serveur d'accès défini par le système avant de tenter d'exécuter l'application.
- Les instructions SQL transmises à un serveur secondaire peuvent être statiques ou dynamiques mais toutes les instructions sont émises dynamiquement. Cela se produit parce que le serveur secondaire n'a pas de plan ou de module contenant les instructions SQL de l'application. Par conséquent, le serveur ne peut pas choisir à l'avance les chemins d'accès aux bases de données.
- Une application SQL unique peut accéder à plusieurs serveurs secondaires en même temps.

- Plusieurs systèmes DB2 pour MVS/ESA peuvent être la cible de mises à jour SQL, pour une portée de validation déterminée.
- Une application peut utiliser plusieurs conversations LU 6.2 vers un serveur secondaire dans le cadre d'une seule validation. Le serveur d'applications DB2 pour MVS/ESA crée généralement une conversation LU 6.2 pour chaque requête SQL en lecture uniquement. Ceci permet au serveur secondaire d'anticiper les demandes FETCH de l'application SQL et de transmettre l'ensemble des réponses avant que celles-ci ne soient demandées par l'application.

Noms d'objets SQL : Lorsque le serveur d'applications DB2 pour MVS/ESA reçoit une requête SQL, il examine le nom d'objet SQL afin de déterminer l'emplacement de l'objet sur le réseau. DB2 pour MVS/ESA accepte des noms d'objets SQL monopartites, bipartites ou tripartites, sous l'une des formes suivantes :

nomobj indique le nom d'une table, d'une vue, d'un synonyme ou d'un alias DB2 pour MVS/ESA

idaut.nomobj indique le propriétaire et le nom de l'objet

emplacement.idaut.nomobj indique le système propriétaire, l'utilisateur propriétaire ainsi que le nom de l'objet

Si le nom d'emplacement (première partie du nom d'objet tripartite) correspond au RDB_NAME du système DB2 pour MVS/ESA local, la demande identifie un objet DB2 pour MVS/ESA local.

Si le nom d'emplacement ne correspond pas au RDB_NAME du système DB2 pour MVS/ESA local, le serveur d'applications DB2 pour MVS/ESA réachemine la demande vers le système identifié par le nom d'emplacement à l'aide de l'accès défini par le système. Le système cible doit être un autre système DB2 pour MVS/ESA car l'accès défini par le système est pris en charge uniquement entre les systèmes DB2 pour MVS/ESA. L'accès défini par le système ne prend en charge aucune fonction de définition d'accès éloigné. Par conséquent, l'application ne doit pas obligatoirement être liée au serveur avant son exécution. La figure 12 à la page 33 résume le procédé utilisé par DB2 pour MVS/ESA pour résoudre les noms d'objet SQL.

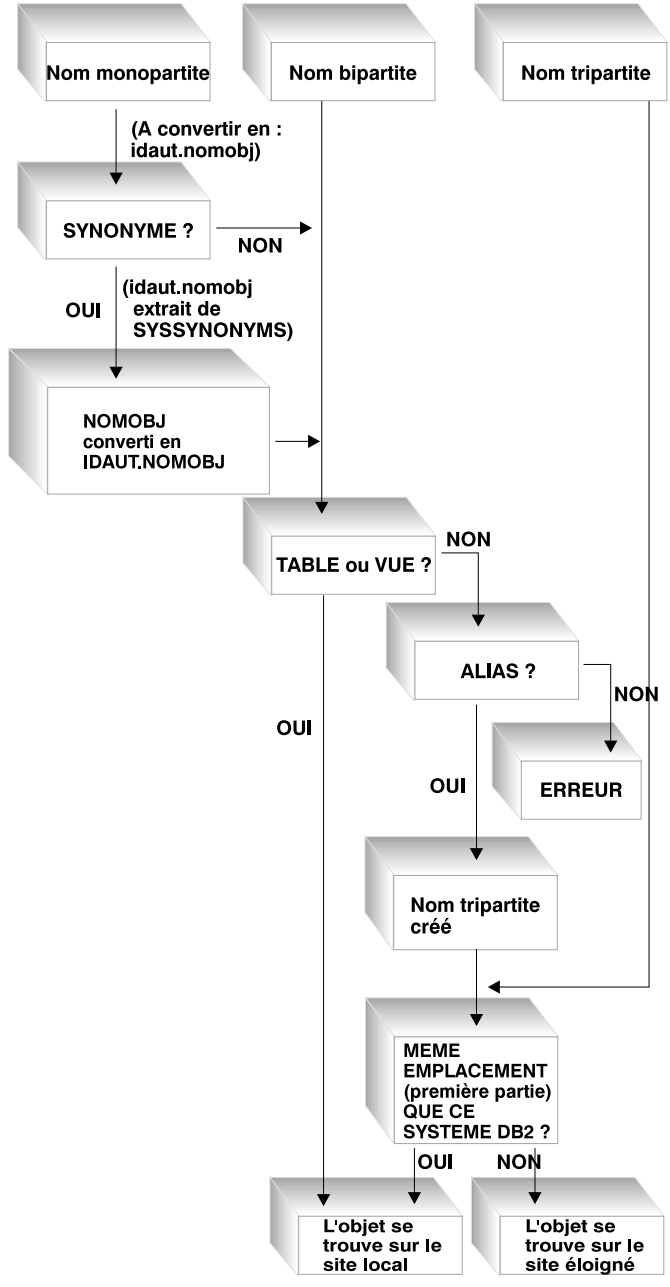

Figure 12. Résolution de noms d'objets SQL DB2 pour MVS/ESA

Définition du serveur : Si le serveur d'applications DB2 pour MVS/ESA doit réacheminer les requêtes SQL, vous devez définir chaque serveur secondaire dans la base de données de communications et VTAM. Le processus de définition est en grande partie identique au processus décrit à la section «Définition des systèmes éloignés» à la page 15. Pour connecter des serveurs secondaires, procédez comme suit :

1. Enregistrez les valeurs correspondant au RDB_NAME et au nom de LU pour chaque serveur dans la base de données de communications et dans VTAM. La valeur de TPN utilisée par l'accès défini par le système est différente de la valeur par défaut de DRDA. Toutefois, cette différence n'est pas importante car DB2 pour MVS/ESA choisit automatiquement la valeur correcte.
2. Définissez, dans la table SYSIBM.SYSLUNAMES, les conditions requises pour la sécurité de chaque serveur secondaire. Vous trouverez la description de ce processus à la section «Définition de la sécurité» à la page 21.
3. Définissez le nom de mode (ou les noms) utilisé entre le serveur d'applications DB2 pour MVS/ESA et les serveurs secondaires et placez ces noms de mode dans la table de modes VTAM. Le nom de mode par défaut est IBMDB2LM.
4. Définissez le nombre maximal de sessions pour chaque serveur secondaire. Le processus utilisé pour établir le nombre maximal de sessions est identique à celui décrit à la section «Définition du système local» à la page 9. Toutefois, l'accès défini par le système peut établir plusieurs conversations pour chaque application SQL. Il se peut que vous ayez besoin d'établir un nombre maximal de sessions supérieur pour les connexions d'accès défini par le système par rapport au nombre de sessions associé aux connexions DRDA.Reportez-vous à la section «Connexion de systèmes de bases de données réparties» dans le manuel *DB2 - Guide de l'administrateur,* pour en savoir plus sur le calcul du nombre de sessions LU 6.2 requises par les applications d'accès défini par le système.

En tant que propriétaire des ressources de base de données, le serveur secondaire contrôle la sécurité de base de données pour les objets SQL résidant au niveau du serveur. Toutefois, cette responsabilité est partagée par le serveur d'applications DB2 pour MVS/ESA qui émet la demande. Le serveur contrôle l'accès aux objets SQL, comme suit :

- Le serveur secondaire n'a pas de copie du plan DB2 pour MVS/ESA. Par conséquent, il revient au serveur d'applications DB2 pour MVS/ESA de vérifier que l'utilisateur final est autorisé à exécuter le module au niveau du système demandeur (le serveur d'applications).

- Les instructions SQL statiques sont exécutées dynamiquement au niveau du serveur secondaire grâce aux privilèges accordés au propriétaire du module DB2 pour MVS/ESA, au niveau du serveur d'applications demandeur DB2 pour MVS/ESA.
- Les instructions SQL dynamiques sont exécutées grâce aux privilèges accordés à l'utilisateur final, au niveau du demandeur d'application.

Définition de la sécurité

Lorsqu'un demandeur d'application achemine une demande de base de données répartie vers le serveur d'application, DB2 pour MVS/ESA, les critères de sécurité suivants peuvent être pris en compte :

- identification du site émetteur
- sélection des noms d'utilisateurs finals
- paramètres de sécurité réseau
- sécurité du gestionnaire de bases de données
- sécurité assurée par un sous-système de sécurité externe

Identification du site émetteur

Lorsqu'un serveur d'applications DB2 pour MVS/ESA reçoit un nom d'utilisateur final du demandeur d'application, il peut limiter les noms d'utilisateurs reçus d'un demandeur d'application donné. Cela est rendu possible par l'utilisation de *l'identification du site émetteur*. L'identification du site émetteur permet au serveur d'applications d'indiquer que seuls des partenaires donnés sont autorisés à utiliser un ID utilisateur donné. Par exemple, le serveur d'applications peut limiter JONES à «identification du site émetteur» DALLAS. Si un autre demandeur d'application (différent de DALLAS) tente d'envoyer le nom JONES au serveur d'applications, ce dernier peut rejeter la demande car le nom ne provient pas de l'emplacement réseau correct.

DB2 pour MVS/ESA exécute l'identification du site émetteur comme faisant partie de la fonction de conversion sortante du nom d'utilisateur final, dont vous trouverez la description à la section suivante.

Sélection des noms d'utilisateurs finals

Il se peut que l'ID utilisateur transmis par le demandeur d'application ne soit pas unique dans l'ensemble du réseau SNA. Il se peut que le serveur d'applications DB2 pour MVS/ESA ait besoin d'exécuter une conversion de nom entrante pour créer des noms d'utilisateurs finals uniques sur le réseau SNA. De la même manière, le serveur d'applications DB2 pour MVS/ESA peut avoir besoin d'effectuer une conversion de nom entrante pour fournir un nom d'utilisateur final unique aux serveurs secondaires impliqués dans l'application (pour plus de détails concernant la conversion entrante de nom d'utilisateur final, reportez-vous à «Définition de la sécurité» à la page 21).

La conversion de nom entrante est activée lorsque la colonne USERNAMES de la table SYSIBM.SYSLUNAMES a pour valeur 'I' (conversion entrante) ou 'B' (conversion entrante et sortante). Lorsque la conversion de nom entrante est active, DB2 pour MVS/ESA convertit l'ID utilisateur envoyé par le demandeur d'application et le nom du propriétaire du plan DB2 pour MVS/ESA (si le demandeur d'application est un autre système DB2 pour MVS/ESA).

Si le demandeur d'application envoie un ID utilisateur et un mot de passe dans le verbe APPC ALLOCATE, ceux-ci sont validés avant la conversion de l'ID utilisateur. La colonne PASSWORD dans la table SYSIBM.SYSUSERNAMES n'est pas utilisée pour la validation du mot de passe. En revanche, l'ID utilisateur et le mot de passe sont présentés au système de sécurité externe (RACF ou produit équivalent) pour validation.

Lorsque l'ID utilisateur entrant dans le verbe ALLOCATE est vérifié, DB2 pour MVS/ESA dispose de sorties d'autorisation qui vous permettent de fournir une liste d'AUTHID secondaires et d'exécuter des contrôles de sécurité supplémentaires. Pour plus de détails, reportez-vous au manuel *DB2 Administration Guide*.

Le processus de conversion de nom entrante recherche, dans la table SYSIBM.SYSUSERNAMES, une ligne qui doit correspondre à l'un des modèles ci-après (TYPE.AUTHID.LUNAME) :

1. I.AUTHID.LUNAME—Utilisateur final particulier issu d'un demandeur d'application particulier
2. I.AUTHID.espace— Utilisateur final particulier issu de n'importe quel demandeur d'application
3. I.espace.LUNAME—N'importe quel utilisateur final issu d'un demandeur d'application particulier

Si aucune ligne n'est trouvée, l'accès éloigné est refusé. Si une ligne est trouvée, l'accès éloigné est autorisé et le nom de l'utilisateur final est modifié pour prendre la valeur contenue dans la colonne NEWAUTHID (une valeur NEWAUTHID à blanc indique que le nom reste inchangé). Toutes les vérifications d'autorisation de ressources DB2 pour MVS/ESA (par exemple, privilèges de tables SQL) effectuées par DB2 pour MVS/ESA sont exécutées sur les noms d'utilisateurs finals convertis plutôt que sur les noms d'utilisateurs originaux.

Lorsqu'un serveur d'applications DB2 pour MVS/ESA reçoit un nom d'utilisateur final du demandeur d'application, plusieurs objectifs peuvent être atteints par le biais de la fonction de conversion de nom entrante DB2 pour MVS/ESA :

- Vous pouvez modifier un nom d'utilisateur final pour le rendre unique. Par exemple, les instructions SQL suivantes convertissent le nom d'utilisateur final JONES du demandeur d'application NEWYORK (LUNAME LUNYC) en un nom différent (NYJONES).

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'JONES', 'LUNYC', 'NYJONES', ' ');
```

- Vous pouvez modifier le nom de l'utilisateur final pour que, dans un groupe, tous les utilisateurs soient représentés par un nom unique. Par exemple, vous pouvez représenter tous les utilisateurs du demandeur d'application NEWYORK (LUNAME LUNYC) par le nom d'utilisateur NYUSER. Cela vous permet d'octroyer des privilèges SQL au nom NYUSER et de contrôler l'accès SQL accordé aux utilisateurs de NEWYORK.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', ' ', 'LUNYC', 'NYUSER', ' ');
```

- Vous pouvez limiter le nombre de noms d'utilisateurs finals transmis par un demandeur d'application donné. Le fait d'utiliser la fonction de conversion de nom d'utilisateur final permet d'exécuter l'identification du site émetteur décrite à la section «Identification du site émetteur» à la page 35. Par exemple, les instructions SQL qui suivent n'autorisent comme utilisateurs finals provenant de l'demandeur d'application NETWORK que SMITH et JONES. Tout autre nom se voit refuser l'accès car il n'est pas mentionné dans la table SYSIBM.SYSUSERNAMES.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'SMITH', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'JONES', 'LUNYC', ' ', ' ');
```

- Vous pouvez limiter le nombre de demandeurs d'application autorisés à se connecter au serveur d'applications DB2 pour MVS/ESA. Il s'agit là d'une

autre fonction d'identification du site émetteur. Dans l'exemple qui suit, n'importe quel nom d'utilisateur final envoyé par le demandeur d'application NEWYORK (LUNYC) ou CHICAGO (LUCHI) est accepté. Les autres demandeurs d'application se voient refuser l'accès car la ligne par défaut SYSIBM.SYSLUNAMES indique la conversion de nom entrante pour toutes les demandes entrantes.

```
INSERT INTO SYSIBM.SYSLUNAMES
     (LUNAME, SYSMODENAME, USERSECURITY, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES (' ', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.SYSUSERNAMES
     (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('I', ' ', 'LUCHI', ' ', ' ');
```

Définition de la sécurité réseau

Il existe dans LU 6.2 trois niveaux importants de sécurité :

- la sécurité au niveau des sessions
- la sécurité au niveau des conversations
- le cryptage

La section «Sécurité réseau» à la page 23, traite de la définition de la sécurité au niveau des sessions et du cryptage avec DB2 pour MVS/ESA. Le serveur d'applications DB2 pour MVS/ESA utilise la sécurité au niveau des sessions et le cryptage exactement de la même manière que le demandeur d'application DB2 pour MVS/ESA.

Le seul critère de sécurité réseau restant est la sécurité au niveau des conversations SNA. Certains aspects relatifs à la sécurité au niveau des conversations sont uniques pour un serveur d'applications DB2 pour MVS/ESA. Le serveur d'applications DB2 pour MVS/ESA joue deux rôles distincts dans la sécurité réseau :

- En tant que demandeur auprès de serveurs secondaires, le serveur d'applications DB2 pour MVS/ESA est chargé d'émettre des demandes APPC contenant les paramètres de sécurité de niveau conversations SNA requis par les serveurs secondaires. Le serveur d'applications DB2 pour MVS/ESA utilise la colonne USERNAMES des tables SYSIBM.SYSLUNAMES et SYSIBM.SYSUSERNAMES pour définir les conditions requises pour la sécurité de niveau conversations SNA pour chaque serveur secondaire. Les explications détaillées de ces définitions sont identiques à celles contenues dans la section «Sécurité réseau» à la page 23.
- En tant que serveur pour le demandeur d'application, le serveur d'applications DB2 pour MVS/ESA dicte les conditions requises pour la

sécurité de niveau conversations SNA pour le demandeur d'application. DB2 pour MVS/ESA utilise la colonne USERSECURITY de la table SYSIBM.SYSLUNAMES pour déterminer la sécurité des conversations requises à partir de chaque demandeur d'application sur le réseau. Les valeurs suivantes sont utilisées dans la colonne USERSECURITY :

C Cette valeur indique que DB2 pour MVS/ESA requiert que le demandeur d'application envoie un ID utilisateur et un mot de passe (LU 6.2 SECURITY=PGM) avec chaque demande de base de données distribuée. Si la colonne ENCRYPTPSWDS de la table SYSIBM.SYSLUNAMES contient un 'Y', DB2 pour MVS/ESA suppose que le mot de passe est dans un format codé RACF (possible uniquement dans le cas d'un demandeur d'application DB2 pour MVS/ESA). Si la colonne ENCRYPTPSWDS ne contient pas de 'Y', DB2 pour MVS/ESA s'attend à trouver le mot de passe dans le format LU 6.2 standard (représentation de caractères EBCDIC). Dans les deux cas, DB2 pour MVS/ESA transmet les valeurs correspondant à l'ID utilisateur et au mot de passe au sous-système de sécurité pour validation. Il vous faut un sous-système de sécurité en mesure de vérifier le mot de passe et l'ID utilisateur APPC ; par exemple, RACF a une fonction de vérification des mots de passe et des ID utilisateurs APPC. Si le sous-système de sécurité rejette le couple ID-mot de passe, l'accès à la base de données répartie est refusé.

Toute autre valeur
Indique que le demandeur d'application est autorisé à envoyer un ID utilisateur déjà vérifié (LU 6.2 SECURITY=SAME) ou un ID utilisateur et un mot de passe (LU 6.2 SECURITY=PGM). Si un ID utilisateur et un mot de passe sont envoyés, DB2 pour MVS/ESA les traite de la façon décrite précédemment pour la valeur 'C'. Si la demande contient uniquement un ID utilisateur, le sous-système de sécurité est appelé pour authentifier l'utilisateur à moins que la table SYSUSERNAMES ne soit utilisée pour la gestion des ID utilisateur entrants.

En cas de violation de la sécurité, la LU 6.2 exige du serveur d'applications DB2 pour MVS/ESA qu'il renvoie un code de détection d'arrêt anormal SNA ('080F6051'X) au demandeur d'application. Dans la mesure où ce code de détection ne décrit pas la cause de l'arrêt anormal, DB2 pour MVS/ESA propose deux méthodes permettant d'enregistrer la cause des violations de sécurité répartie :

- Un message DSNL030I est émis, qui fournit la LUWID du demandeur ainsi qu'un code anomalie DB2 décrivant l'arrêt anormal. DSNL030I comprend également le AUTHID, si celui-ci est connu, envoyé à partir de la demande d'application qui a été rejetée.

- Une alerte est enregistrée dans la base de données du moniteur matériel NETVIEW, qui contient les mêmes informations que celles contenues dans le message DSNL030I.

Sécurité du gestionnaire de bases de données

En tant que propriétaire des ressources de base de données, le serveur d'applications DB2 pour MVS/ESA contrôle les fonctions de sécurité de base de données pour les objets SQL résidant sur le serveur d'applications DB2 pour MVS/ESA. L'accès aux objets gérés par DB2 pour MVS/ESA est régi par des privilèges octroyés aux utilisateurs par l'administrateur de DB2 pour MVS/ESA ou les propriétaires des objets individuels. Les deux classes d'objets de base contrôlées par le serveur d'applications DB2 pour MVS/ESA sont les suivantes :

- **Modules**—Les utilisateurs individuels sont autorisés à créer, remplacer et exécuter les modules par le biais de l'instruction GRANT de DB2 pour MVS/ESA. Lorsqu'un utilisateur final est propriétaire d'un module, il peut automatiquement l'exécuter ou le remplacer. Les autres utilisateurs, quant à eux, doivent se voir accorder le droit d'exécution du module au niveau du serveur d'applications DB2 pour MVS/ESA, à l'aide de l'instruction GRANT. Le droit USE peut être accordé à des utilisateurs finals individuels ou à PUBLIC, ce qui permet à la totalité des utilisateurs finals d'exécuter le module.

  Lorsqu'une application est liée à DB2 pour MVS/ESA, le module contient les instructions SQL contenues dans le programme de l'application. Ces instructions sont classées comme suit :

  SQL statique
  : L'instruction SQL et les objets SQL désignés par cette dernière sont connus au moment où l'application est liée à DB2 pour MVS/ESA. Le créateur du module doit disposer des droits appropriés pour exécuter chaque instruction SQL statique du module.

    Lorsqu'un utilisateur final dispose des droits d'exécution d'un module, il dispose automatiquement des droits lui permettant d'exécuter chaque instruction SQL statique contenue dans le module. Les utilisateurs finals n'ont donc pas besoin d'utiliser les privilèges d'accès aux tables DB2 pour MVS/ESA si le module qu'ils exécutent contient uniquement des instructions SQL statiques.

  SQL dynamique
  : Décrit une instruction SQL qui n'est pas connue tant que le programme n'est pas exécuté. En d'autres termes, l'instruction SQL est créée par le programme et liée dynamiquement à DB2 pour MVS/ESA à l'aide de l'instruction SQL PREPARE. Lorsqu'un utilisateur final exécute une instruction SQL dynamique, il doit disposer des privilèges d'accès aux tables nécessaires à l'exécution de l'instruction SQL. Dans la mesure où l'instruction SQL est

inconnue lors de la création du plan ou du module, le propriétaire du module n'accorde pas automatiquement à l'utilisateur final les droits requis.

- **Objets SQL**—Il s'agit de tables, de vues, de synonymes ou d'alias. Les utilisateurs DB2 pour MVS/ESA peuvent se voir accorder plusieurs niveaux de droits pour créer, supprimer, modifier ou lire des objets SQL individuels. Ces droits sont requis pour définir l'accès des instructions SQL statiques ou exécuter les instructions SQL dynamiques.

Lors de la création d'un module, l'option DISABLE/ENABLE vous permet de contrôler quels sont les types de connexion DB2 pour MVS/ESA en mesure d'exécuter le module. Vous pouvez utiliser les routines de sortie d'exit de sécurité RACF et DB2 pour MVS/ESA afin de permettre, de manière sélective, aux utilisateurs finals d'utiliser DDF. Vous pouvez utiliser RLF pour définir les limites de temps de traitement pour les définitions d'accès éloigné et les exécutions de SQL dynamiques.

Prenons pour exemple un module DB2 pour MVS/ESA appelé MYPKG, et appartenant à JOE. JOE peut permettre à SAL d'exécuter le module à l'aide de l'instruction GRANT USE de DB2 Universal Database for OS/390. Lorsque SAL exécute le module, il se produit ce qui suit :

- DB2 pour MVS/ESA vérifie que SAL dispose des droits USE pour le module.
- SAL peut exécuter chaque instruction SQL statique dans le module parce que JOE dispose des privilèges d'accès aux objets SQL pour la création du module.
- Si le module a des instructions SQL dynamiques, SAL doit disposer de ses propres droits d'accès aux tables. Par exemple, SAL ne peut pas exécuter SELECT * FROM JOE.TABLE5 tant qu'elle ne dispose pas des droits d'accès en lecture à JOE.TABLE5.

Sous-système de sécurité

L'utilisation par le serveur d'applications DB2 pour MVS/ESA du sous-système de sécurité (RACF ou produit équivalent) dépend de la façon dont vous définissez la fonction de conversion de nom entrante dans la table SYSIBM.SYSLUNAMES :

- Si vous indiquez 'I' ou 'B' pour la colonne USERNAMES, la fonction de conversion de nom entrante est active et DB2 pour MVS/ESA suppose que l'administrateur de DB2 pour MVS/ESA utilise la conversion de nom entrante pour exécuter une partie de la mise en place de la sécurité système. Le sous-système de sécurité externe est appelé uniquement si le demandeur d'application envoie une demande contenant à la fois l'ID utilisateur et le mot de passe (SECURITY=PGM). Il vous faut un sous-système de sécurité en mesure de vérifier le mot de passe et l'ID

utilisateur APPC ; par exemple, RACF a une fonction de vérification des mots de passe et des ID utilisateurs APPC.

Si la demande émanant du demandeur d'application contient uniquement un ID utilisateur (SECURITY=SAME), le système de sécurité externe n'est en aucun cas appelé car les règles de conversion de nom entrante déterminent les utilisateurs qui sont autorisés à se connecter au serveur d'applications DB2 pour MVS/ESA.

- Si vous indiquez une valeur autre que 'I' ou 'B' pour la colonne USERNAMES, le sous-système de sécurité est vérifié comme suit :
  - Lors de la réception d'une demande de base de données répartie émanant du demandeur d'application, DB2 pour MVS/ESA appelle le système de sécurité externe pour valider l'ID de l'utilisateur final (et le mot de passe, le cas échéant).
  - Le système de sécurité externe est appelé pour vérifier que l'utilisateur final est autorisé à se connecter au sous-système DB2 pour MVS/ESA.
- Dans les deux cas, une sortie d'autorisation est émise pour fournir une liste d'ID autorisation secondaire. Pour plus de détails, reportez-vous au manuel *DB2 Administration Guide*.

Représentation des données

Vous devez vous assurer que votre sous-système DB2 pour MVS/ESA dispose de la fonction de conversion du CCSID du demandeur d'application en CCSID d'installation du sous-système DB2 pour MVS/ESA. Reportez-vous à la section «Représentation des données» à la page 27, pour plus de détails.

Chapitre 2. Connexion de DB2 Universal Database for OS/390 au sein d'un réseau DRDA

DB2 Universal Database for OS/390 est le système de gestion de bases de données relationnelles IBM pour les systèmes OS/390. Le présent chapitre ne concerne pas les éditions précédentes. Reportez-vous au «Chapitre 1. Connexion de DB2 pour MVS/ESA au sein d'un réseau DRDA» à la page 1.

Le présent chapitre explique comment connecter des demandeurs d'application DRDA (tels que DB2 Connect) à un serveur d'applications DB2 Universal Database for OS/390 version 5, et comment configurer des demandeurs d'application DB2 Universal Database for OS/390 pour communiquer avec des serveurs d'applications DRSDA tels que DB2 Universal Database version 5 sur d'autres systèmes.

Dans ce chapitre, l'accent est mis principalement sur d'autres types de systèmes DRDA à DB2 Universal Database for OS/390 via des connexions SNA. Cependant, DB2 Universal Database for OS/390 version 5 fournit également un support pour les communications de bases de données à l'aide de connexions TCP/IP natives (sans AnyNet), ainsi que des informations sur l'utilisation de TCP/IP. Pour plus de détails sur la configuration et l'utilisation des connexions TCP/IP, reportez-vous aux manuels *DB2 for OS/390 Version 5 Installation Guide* et *DRDA Support for TCPIP with DB2 for OS/390 Version 5 and DB2 Universal Database Universal Database*.

Pour en savoir plus sur la connexion de deux systèmes DB2 pour OS/390 ou pour obtenir plus de détails sur la définition de connexions DRDA à DB2 pour OS/390, reportez-vous à la section relative à la connexion de systèmes de bases de données réparties dans le manuel *DB2 for OS/390 Administration Guide*.

Remarques :

1. Grâce à la fonction AnyNet de VTAM version 4 édition 2, vous pouvez exécuter APPC sur un réseau TCP/IP. Toutefois, nous recommandons aux utilisateurs de DB2 pour OS/390 V5.1 d'utiliser le support TCP/IP natif plutôt que la fonction AnyNet APPC sur TCP/IP.
2. Le présent chapitre ne contient aucune information sur l'utilisation de DCE.

DB2 Universal Database for OS/390

La figure 13 montre un système OS/390 exécutant une seule copie de DB2 Universal Database for OS/390. Il est également possible d'exécuter plusieurs copies de DB2 pour OS/390 sur un seul système. Pour distinguer les différentes copies de DB2 pour OS/390 sur un système donné (ou des copies de DB2 pour OS/390 dans un ensemble JES), un *nom de sous-système*, composé de un à quatre caractères et unique au sein de l'ensemble JES, est attribué à chaque système DB2. Dans la figure 13, le nom de sous-système de DB2 Universal Database for OS/390 est *xxxx*. Trois des espaces adresse OS/390 sont précédés du nom de sous-système DB2 pour OS/390. Ils constituent le produit DB2 pour OS/390.

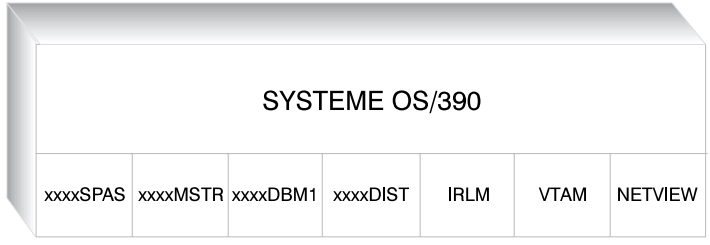

Figure 13. Espaces adresse OS/390 utilisés par DB2 pour OS/390

La figure 13 illustre les espaces adresses OS/390 impliqués dans le traitement des bases de données réparties avec DB2 pour OS/390. Ces espaces adresse permettent aux utilisateurs de DB2 pour OS/390 d'accéder à des bases de données relationnelles locales et de communiquer avec des systèmes DRDA éloignés. La fonction des espaces adresse est la suivante :

xxxxSPAS
Espace adresse destiné aux procédures mémorisées DB2.

xxxxMSTR
Espace adresse des services système pour le produit DB2 pour OS/390, chargé du démarrage et de l'arrêt de DB2 pour OS/390, ainsi que du contrôle de l'accès en local à DB2 pour OS/390.

xxxxDBM1
Espace adresse des services base de données, qui contrôle l'accès aux bases de données relationnelles gérées par DB2 pour OS/390. C'est là que sont exécutées les entrées et sorties aux ressources de base de données pour les programmes d'application SQL.

xxxxDIST
La partie de DB2 Universal Database for OS/390 qui fournit les fonctions de bases de données réparties, également appelée *Distributed Data Facility* (DDF). Lors de la réception d'une demande de base de données répartie, DDF transmet la demande à *xxxx*DBM1, de sorte que puissent être exécutées les opérations d'entrée-sortie de base de données requises.

IRLM Gestionnaire de verrous utilisé par DB2 pour OS/390 pour contrôler l'accès aux ressources de bases de données.

VTAM
Serveur de communications IBM pour les fonctions SNA OS/390 (VTAM). DDF utilise SNA ou TCP/IP pour l'exécution de communications de bases de données réparties au nom de DB2 pour OS/390. La figure ne représente aucun espace adresse pour TCP/IP.

NETVIEW
Produit phare de la gestion de réseau sur les systèmes OS/390. Lorsqu'une erreur se produit au cours du traitement d'une base de données répartie, DDF enregistre les informations relatives à l'erreur (également appelées *alertes*) dans la base de données du moniteur matériel NetView. Les administrateurs système peuvent utiliser NetView pour examiner les erreurs stockées dans la base de données du moniteur matériel ou fournir des procédures de commandes automatisées à utiliser chaque fois que sont enregistrées des conditions d'alerte.

NetView peut également permettre de détecter des erreurs de communication VTAM. Pour plus de détails, reportez-vous au manuel *Distributed Relational Database Architecture Problem Determination Guide*.

La figure 13 à la page 44 n'illustre pas de programmes d'application SQL. Lorsqu'un programme d'application utilise DB2 pour lancer des instructions SQL, il doit définir une liaison au produit DB2 pour OS/390 selon l'une des méthodes suivantes :

TSO Les travaux par lots et utilisateurs finals connectés à TSO sont connectés à DB2 pour OS/390 via la fonction de définition de liaison de TSO. Il s'agit de la technique utilisée pour connecter SPUFI et la plupart des applications QMF à DB2 Universal Database for OS/390.

CICS/ESA
Lorsqu'une application CICS/ESA émet des appels SQL, le produit CICS/ESA utilise l'interface de définition de liaison CICS pour acheminer les requêtes SQL vers DB2 pour OS/390.

IMS/ESA
Les transactions qui s'exécutent sous le contrôle de IMS/ESA utilisent

l'interface de définition de liaison IMS pour la transmission des instructions SQL à DB2 pour OS/390 pour traitement.

DDF DDF (Distributed Data Facility) est chargé de la connexion des applications réparties à DB2 pour OS/390.

CAF La fonction de connexion d'appels (CAF) permet aux sous-systèmes écrits par l'utilisateur de se connecter directement à DB2 pour OS/390.

Mise en oeuvre de DB2 pour OS/390

DRDA définit les types de fonctions de système de gestion de bases de données réparties. DB2 Universal Database for OS/390 prend en charge la fonction unité d'oeuvre éloignée. Avec l'unité d'oeuvre éloignée, un programme d'application s'exécutant sur un système peut accéder aux données d'un système de gestion de bases de données réparties à l'aide du SQL fournir par ce dernier.

DB2 Universal Database for OS/390 prend également en charge l'unité d'oeuvre répartie. Avec l'unité d'oeuvre répartie, un programme d'application s'exécutant sur un système peut accéder à des données au niveau de plusieurs SGBD éloignés en utilisant le SQL fourni par ces derniers. Pour en savoir plus sur les types de distribution définis par DRDA, reportez-vous au manuel *DRDA Connectivity Guide*.

Comme le montre la figure 14 à la page 48, DB2 Universal Database for OS/390 prend en charge trois configurations de connexions de bases de données réparties, selon deux méthodes d'accès :

[1] *L'accès défini par le système* (on parle également de *protocole privé de DB2 UDB pour OS/390*) permet à un demandeur DB2 UDB pour OS/390 de se connecter à un ou plusieurs serveurs DB2 UDB pour OS/390. Cette connexion établie entre le demandeur DB2 UDB pour OS/390 et le serveur n'adhère pas aux protocoles définis dans DRDA et ne peut pas être utilisée pour connecter des produits non DB2 UDB pour OS/390 à DB2 pour OS/390. L'établissement de ce type de connexion se fait par la codification, dans l'application, de noms ou d'alias composés de trois parties.

[2] *L'accès défini par l'application* permet à un demandeur DB2 Universal Database for OS/390 ou non DB2 Universal Database for OS/390 (par exemple, DB2 Connect) de se connecter à un ou plusieurs serveurs d'applications DB2 Universal Database for OS/390 ou non DB2 Universal Database for OS/390 (par exemple, DB2 Universal Database et DB2 Universal Database pour AS/400) via des protocoles DRDA. Le nombre de serveurs d'applications pouvant être simultanément connectés au demandeur d'application dépend du niveau de DB2 UDB pour OS/390 du demandeur d'application. Si le demandeur d'application est DB2 pour

MVS/ESA version 2.3, un seul serveur d'applications peut être connecté à la fois. L'établissement de ce type de connexion se fait par la codification d'instructions SQL CONNECT dans l'application. Si le demandeur d'application est DB2 pour MVS/ESA version 3.1 ou suivante, un ou plusieurs serveur(s) d'applications peuvent être connecté(s) simultanément.

[3] L'accès défini par l'application et l'accès défini par le système peuvent être utilisés conjointement pour établir des connexions. Vous ne pouvez pas vous connecter en utilisant DRDA et la mémoire contrôlée par le système dans la même unité d'exécution.

Le terme *serveur secondaire* décrit des systèmes utilisés en tant que serveurs du serveur d'applications.

Si, dans une configuration, tous les systèmes prennent en charge la validation en deux phases, l'unité d'oeuvre répartie (lecture et mise à jour sur plusieurs sites) est prise en charge. Si la validation en deux phases n'est pas prise en charge par tous les systèmes, les mises à jour à l'intérieur d'une unité d'oeuvre sont limitées soit à un seul site ne prenant pas en charge la validation en deux phases, soit au sous-ensemble de sites prenant en charge la validation en deux phases.

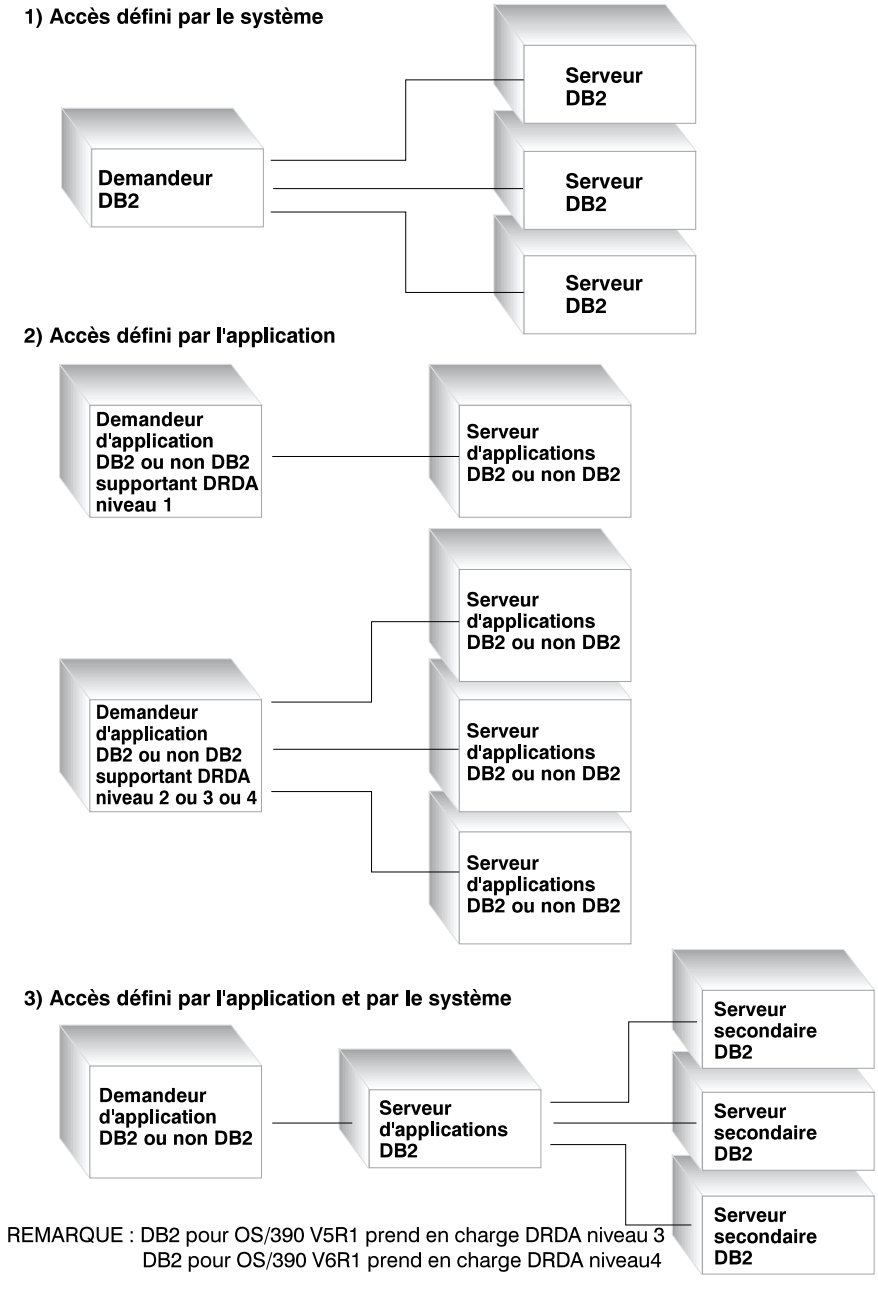

Figure 14. Connexions réparties de DB2 Universal Database for OS/390

Le tableau 2 compare les types de connexion de bases de données réparties DB2 Universal Database for OS/390.

Tableau 2. Comparaison de connexions de bases de données réparties DB2 Universal Database for OS/390

[1] Accès défini par le système	**[2] Accès défini par l'application (l'ensemble des systèmes prenant en charge la validation en deux phases)**	**[3] Accès défini par l'application et accès défini par le système**
Tous les partenaires doivent être des systèmes DB2 Universal Database for OS/390.	Permet d'interconnecter deux systèmes DRDA, quels qu'ils soient.	Le demandeur d'application peut être n'importe quel système DRDA ; les serveurs doivent être des systèmes DB2 Universal Database for OS/390.
Permet une connexion directe à plusieurs partenaires.	Permet une connexion directe à plusieurs partenaires.	Le demandeur d'application se connecte directement aux serveurs d'applications ; les serveurs d'applications peuvent se connecter à plusieurs serveurs secondaires DB2 Universal Database for OS/390.
Chaque application SQL peut avoir plusieurs conversations avec chaque serveur.	Chaque application SQL a une conversation avec chaque serveur.	L'application SQL a une conversation avec chaque serveur ; le serveur d'applications DB2 Universal Database for OS/390 peut établir plusieurs conversations avec chaque serveur pour l'application.
Permet d'accéder aux ressources locales et éloignées dans une seule portée de validation.	Permet d'accéder aux ressources locales et éloignées dans une seule portée de validation.	Le demandeur d'application et le serveur d'applications peuvent accéder aux données locales et éloignées
Plus efficace au niveau de requêtes volumineuses et de requêtes simultanées.	Plus efficace au niveau des instructions SQL exécutées très peu de fois dans une seule portée de validation.	La connexion demandeur d'application-serveur d'applications se comporte comme **[2]** ; les connexions de serveurs secondaires se comportent comme **[1]**.
Prise en charge du SQL statique ou dynamique mais le serveur définit dynamiquement l'accès au SQL statique lors de la première exécution dans une seule portée de validation.	Permet de lancer des instructions SQL statiques ou dynamiques.	Le demandeur d'application et le serveur d'applications peuvent lancer des instructions SQL statiques ou dynamiques ; les serveurs secondaires prennent en charge le SQL statique ou dynamique mais définissent dynamiquement l'accès au SQL statique lors de la première exécution dans une seule portée de validation.

Tableau 2. Comparaison de connexions de bases de données réparties DB2 Universal Database for OS/390 (suite)

[1] Accès défini par le système	[2] Accès défini par l'application (l'ensemble des systèmes prenant en charge la validation en deux phases)	[3] Accès défini par l'application et accès défini par le système
Limité aux instructions SQL INSERT, DELETE et UPDATE ainsi qu'aux instructions qui prennent en charge SELECT.	Peut utiliser toute instruction prise en charge par le système qui exécute l'instruction.	Les serveurs d'applications prennent en charge toute forme de SQL ; les serveurs secondaires ne prennent en charge que le SQL DML (par exemple, CREATE ou ALTER)

Fonctions supplémentaires de sécurité

Codes de sécurité étendue

Avant la version 5.1 de DB2 Universal Database for OS/390, les demandes de connexion avec ID utilisateur et mot de passe pouvaient ne pas aboutir et générer `SQL30082`, code raison 0, mais sans explication de l'échec.

La version 5.1 de DB2 Universal Database for OS/390 apporte une amélioration : la prise en charge de codes de sécurité étendue. Celle-ci permet d'obtenir des diagnostics supplémentaires, tels que `(MOT DE PASSE PERIME)`, en plus du code raison.

Pour pouvoir bénéficier de cette amélioration, vous devez affecter la valeur `YES` au paramètre d'installation `ZPARM` de DB2 Universal Database for OS/390 pour une sécurité étendue. Pour définir la valeur `EXTSEC=YES`, utilisez l'écran d'installation DSN6SYSP de DB2 Universal Database for OS/390 ou l'écran DDF 1 (DSNTIPR). La valeur défaut est `EXTSEC=NO`. Si un mot de passe a expiré, les applications PC, UNIX, Apple Macintosh et Web utilisant DB2 Connect recevront un message d'erreur SQL01404.

Sécurité TCP/IP déjà vérifiée

Pour fournir un support pour l'option de sécurité `AUTHENTICATION=CLIENT` de DB2 Universal Database, utilisez l'écran d'installation de DB2 Universal Database for OS/390 DSNTIP4 (ou l'écran DDF 2) et affectez la valeur `YES` au paramètre de sécurité TCP/IP déjà vérifiée.

Sécurité des applications PC ODBC et Java

Les applications ODBC et Java sur postes de travail utilisent des instructions SQL dynamiques, ce qui peut affecter la sécurité pour certaines installations. DB2 Universal Database for OS/390 inclut une nouvelle option de définition d'accès, `DYNAMICRULES (BIND)`, qui permet l'exécution de ce langage sous le contrôle du propriétaire ou du programme de définition d'accès. Pour la procédure de définition de DYNAMICRULES via DB2 Connect, reportez-vous au manuel *Command Reference*.

DB2 Universal Database et DB2 Connect version 5 fournissent un nouveau paramètre de configuration CLI/ODBC, CURRENTPACKAGESET, figurant dans le fichier de configuration DB2CLI.INI. Vous devez associer à ce paramètre un nom de schéma disposant des privilèges appropriés. Une instruction SQL SET CURRENT PACKAGESET schema sera alors automatiquement émise après chaque connexion à l'application.

Utilisez le gestionnaire ODBC pour mettre à jour le fichier DB2CLI.INI. Pour plus de détails, reportez-vous au manuel *Installation et configuration - Informations complémentaires*.

Prise en charge de la modification de mot de passe

Si une instruction SQL CONNECT renvoie un message signalant que le mot de passe associé à l'ID utilisateur a expiré, avec DB2 Connect, Version 5.2 et plus, vous pouvez désormais modifier le mot de passe sans avoir à vous connecter à TSO. Via DRDA, DB2 Universal Database for OS/390 peut changer le mot de passe à votre place.

L'utilisateur doit fournir l'ancien mot de passe ainsi que le nouveau mot de passe et le mot de passe de vérification. Si DCS est l'option de sécurité indiquée sur le serveur DB2 Connect Enterprise Edition, une demande de modification du mot de passe est envoyée au serveur de bases de données DB2 Universal Database for OS/390. S'il s'agit de SERVER, le mot de passe du serveur DB2 Connect est modifié.

Avantage supplémentaire, il n'est plus obligatoire de définir le LU de manière distincte. Pour plus de détails, reportez-vous au manuel *Mise en route* consacré à DB2 Connect Enterprise Edition.

Configuration du demandeur d'application

DB2 Universal Database for OS/390 met en oeuvre le support de demandeur d'application DRDA en tant que partie intégrante de la fonction DDF (Distributed Data Facility) de DB2 pour MVS/ESA. La fonction DDF peut être arrêtée de façon indépendante à partir des fonctions de gestion de bases de données de DB2 Universal Database for OS/390 mais ne peut pas s'exécuter en l'absence du support de gestion de base de données locale de DB2 Universal Database for OS/390.

Lorsque DB2 Universal Database for OS/390 agit en tant que demandeur d'application, il peut connecter des applications s'exécutant sur le système à des serveurs de bases de données éloignés DB2 Universal Database, DB2 pour MVS/ESA, DB2 Universal Database for OS/390, DB2 Universal Database pour AS/400 et DB2 pour VSE & VM, qui mettent en oeuvre la fonction de serveur d'applications DRDA.

Si vous souhaitez que le demandeur d'application DB2 Universal Database for OS/390 fournisse un accès à la base de données répartie, vous devez prendre en compte les informations suivantes :

- «Définition des données réseau» — Le demandeur d'application doit pouvoir accepter les valeurs RDB_NAME et les convertir en valeurs SNA NETID.LUNAME ou en valeurs d'adresse TCP/IP. DB2 Universal Database for OS/390 utilise la *base de données de communications DB2 Universal Database for OS/390* (CDB) pour enregistrer les valeurs RDB_NAME et leurs paramètres de réseau correspondants. La CDB permet au demandeur d'application DB2 Universal Database for OS/390 de transmettre les informations requises au serveur de communications lors de l'émission de demandes de bases de données réparties sur des connexions SNA ou TCP/IP.
- «Définition de la sécurité» à la page 70— Pour que les demandes de bases éloignées soient acceptées par le serveur d'applications, le demandeur d'application doit fournir les informations de sécurités requises par le serveur. DB2 Universal Database for OS/390 utilise la base de données de communications, DCE, RACF ou un autre sous-système de sécurité
- «Représentation des données» à la page 78 — Vous devez vous assurer que le CCSID du demandeur d'application est compatible avec celui du serveur d'applications.

Définition des données réseau

La plupart des opérations de traitement exécutées dans un environnement de bases de données réparties nécessitent l'échange de messages avec d'autres sites du réseau. Pour que cela s'effectue correctement, vous devez procéder aux opérations suivantes :

1. Définition du système local.
2. Définition des systèmes éloignés.
3. Définition des communications (pour les connexions SNA ou TCP/IP).
4. Définition de la taille de RU et de la régulation (pour les connexions SNA uniquement).

Reportez-vous aux sections «Définition du système local (SNA)» ou «Définition du système local (TCP/IP)» à la page 59.

Définition du système local (SNA)

Chaque programme sur le réseau SNA se voit attribuer un NETID et un nom de LU. Votre demandeur d'application DB2 Universal Database for OS/390 doit donc avoir une valeur NETID.LUNAME (attribuée via VTAM) lors de sa connexion au réseau. Parce que le demandeur d'application DB2 Universal Database for OS/390 est intégré dans le système de gestion de la base de données DB2 Universal Database for OS/390 locale, il doit également avoir un nom RDB_NAME. Dans les publications DB2 Universal Database for OS/390, il est fait référence au nom RDB_NAME en tant que nom d'*emplacement*.

Définissez le demandeur d'application DB2 Universal Database for OS/390 pour le réseau SNA en procédant comme suit :

1. Sélectionnez un nom de LU pour votre système DB2 Universal Database for OS/390. Le NETID de votre système DB2 Universal Database for OS/390 s'obtient automatiquement à partir de VTAM au démarrage de DDF.
2. Définissez le nom de LU et le nom d'emplacement dans le *fichier d'amorçage* (BSDS) DB2 pour MVS/ESA. (DB2 Universal Database for OS/390 limite le nom d'emplacement à 16 caractères.)
3. Créez une définition APPL VTAM pour enregistrer le nom de LU sélectionné avec VTAM.
4. Vérifiez que les fonctions de sécurité étendue sont activées (YES). Reportez-vous à la section «Fonctions supplémentaires de sécurité» à la page 50.

Configuration du fichier d'amorçage de DDF : DB2 Universal Database for OS/390 lit le fichier d'amorçage pendant le traitement du démarrage pour obtenir des paramètres d'installation du système. L'un des enregistrements stockés dans le fichier d'amorçage est appelé *enregistrement DDF*, parce qu'il contient les informations utilisées par la fonction DDF pour se connecter à VTAM. Ces informations sont les suivantes :

- Nom de l'emplacement pour le système DB2 Universal Database for OS/390
- Nom de LU pour le système DB2 Universal Database for OS/390
- Mot de passe utilisé lors de la connexion du système DB2 Universal Database for OS/390 à VTAM

Vous pouvez fournir les informations du fichier d'amorçage de DDF à DB2 Universal Database for OS/390 de deux manières :

- Utilisez le panneau d'installation DDF DSNTIPR lors de la première installation de DB2 Universal Database for OS/390 pour fournir les informations du fichier d'amorçage de DDF requises. De nombreux paramètres d'installation ne sont pas développés ici car il est plus important de savoir connecter DB2 Universal Database for OS/390 à VTAM. La figure 15 à la page 54 explique comment utiliser le panneau d'installation pour enregistrer le nom d'emplacement NEW_YORK3, le nom de LU NYM2DB2 et le mot de passe PSWDBD1 dans le fichier d'amorçage de DB2 Universal Database for OS/390.

```
                            DISTRIBUTED DATA FACILITY                      =
==> _

 Enter data below:

  1 DDF STARTUP OPTION   ===> AUTO      NO, AUTO, or COMMAND
  2 DB2 LOCATION NAME    ===> NEW_YORK3         The name other DB2s use to
                                         refer to this DB2
  3 DB2 NETWORK LUNAME   ===> NYM2DB2   The name VTAM uses to refer to this DB2
  4 DB2 NETWORK PASSWORD ===> PSWDBD1   Password for DB2's VTAM application
  5 RLST ACCESS ERROR    ===> NOLIMIT   NOLIMIT, NORUN, or 1-5000000
  6 RESYNC INTERVAL      ===> 3         Minutes between resynchronization period
  7 DDF THREADS          ===> ACTIVE    (ACTIVE or INACTIVE) Status of a
                                        database access thread that commits or
                                        rolls back and holds no database locks
                                        or cursors
  8 DB2 GENERIC LUNAME   ===>           Generic VTAM LU name for this DB2
                                        subsystem or data sharing group
  9 IDLE THREAD TIMEOUT  ===> 120       0 or seconds until dormant server ACTIVE
                                        thread will be terminated (0-9999)
 10 EXTENDED SECURITY    ===> YES       Allow change password and descriptive
                                        security error codes.  YES or NO.
 PRESS:  ENTER to continue   RETURN to exit   HELP for more information
```

Figure 15. DB2 Universal Database for OS/390 - Panneau d'installation DSNTIPR

- Si DB2 Universal Database for OS/390 est déjà installé, vous pouvez utiliser l'inventaire du journal des modifications (DSNJU003) pour la mise à jour des informations dans le fichier d'amorçage

  La figure 16 montre comment mettre à jour le fichier d'amorçage avec le nom d'emplacement NEW_YORK3, le nom de LU NYM2DB2 et le mot de passe PSWDBD1.

```
//SYSADMB JOB ,'DB2 5.1 JOB',CLASS=A
//*
//*        CHANGE LOG INVENTORY:
//*        UPDATE BSDS WITH
//*             - DB2 LOCATION NAME FOR NEW_YORK3
//*             - VTAM LUNAME (NYM2DB2)
//*             - DB2/VTAM PASSWORD
//*
//DSNBSDS EXEC PGM=DSNJU003
//STEPLIB  DD  DISP=SHR,DSN=DSN510.DSNLOAD
//SYSUT1   DD  DISP=OLD,DSN=DSNC510.BSDS01
//SYSUT2   DD  DISP=OLD,DSN=DSNC510.BSDS02
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSIN    DD  *
 DDF    LOCATION=NEW_YORK3,LUNAME=NYM2DB2,PASSWORD=PSWDBD1
//*
```

Figure 16. Exemple de définition du fichier d'amorçage de DDF (pour VTAM)

Lorsque DDF est lancé (soit automatiquement au démarrage de DB2 Universal Database for OS/390, soit au moyen de la commande START DDF de DB2 Universal Database for OS/390), il se connecte à VTAM, transmettant le nom de LU et le mot de passe à VTAM. VTAM reconnaît le système DB2 Universal Database for OS/390 en vérifiant le nom de LU et le mot de passe (si un mot de passe VTAM est requis) avec les valeurs définies dans l'instruction APPL VTAM. Le mot de passe VTAM permet de vérifier que DB2 Universal Database for OS/390 est habilité à utiliser le nom de LU spécifié sur le système VTAM. Le mot de passe VTAM n'est pas transmis via le réseau et ne permet pas de connecter d'autres systèmes du réseau à DB2 Universal Database for OS/390.

Si VTAM n'exige pas de mot de passe, ignorez le mot clé PASSWORD= dans l'inventaire du journal des modifications. L'absence de mot clé indique qu'aucun mot de passe VTAM n'est nécessaire.

Création d'une définition APPL VTAM : Après avoir défini le nom de LU VTAM et le mot de passe pour DB2 Universal Database for OS/390, il vous faut enregistrer ces valeurs avec VTAM. VTAM utilise l'instruction APPL pour définir les noms de LU locales. La figure 17, illustre la définition de nom de LU NYM2DB2 pour VTAM.

```
 DB2APPLS VBUILD TYPE=APPL
 *
 *--------------------------------------------------------------------*
 *                                                                    *
 *           APPL DEFINITION FOR THE NEW_YORK3 DB2 SYSTEM             *
 *                                                                    *
 *--------------------------------------------------------------------*
 *
NYM2DB2  APPL   APPC=YES,                                          X
                AUTH=(ACQ),                                        X
                AUTOSES=1,                                         X
                DMINWNL=10,                                        X
                DMINWNR=10,                                        X
                DSESLIM=20,                                        X
                EAS=9999,                                          X
                MODETAB=RDBMODES,                                  X
                PRTCT=PSWDBD1,                                     X
                SECACPT=ALREADYV,                                  X
                SRBEXIT=YES,                                       X
                VERIFY=NONE,                                       X
                VPACING=2,                                         X
                SYNCLVL=SYNCPT,                                    X
                ATNLOSS=ALL                                        X
```

Figure 17. Exemple de définition APPL VTAM pour DB2 Universal Database for OS/390

Plusieurs mots clés sont disponibles dans l'instruction APPL VTAM. Vous trouverez des explications détaillées concernant la signification des mots clés

dans le manuel *DB2 for OS/390 Administration Guide*. Les seuls mots clés abordés ici sont ceux qui se rapportent aux rubriques du présent manuel. Les mots clés intéressants de la figure 17 à la page 55 sont décrits comme suit :

NYM2DB2
VTAM utilise l'étiquette d'instruction APPL comme nom de LU. Dans ce cas, le nom de LU est NYM2DB2. La syntaxe APPL ne prévoit pas de place pour une valeur NETID.LUNAME complète. La valeur de NETID n'est pas spécifiée dans l'instruction APPL VTAM car elle est automatiquement attribuée à toutes les applications VTAM pour le système VTAM.

AUTOSES=1
Nombre de sessions de vainqueur de conflit SNA qui démarrent automatiquement lors de l'émission d'une demande CNOS APPC (modification du nombre de sessions). Une valeur différente de zéro doit être fournie avec AUTOSES pour informer DB2 Universal Database for OS/390 chaque fois que le traitement de CNOS VTAM échoue.

II n'est pas nécessaire de démarrer automatiquement toutes les sessions APPC entre les deux partenaires de bases de données réparties concernés. Si la valeur de AUTOSES est inférieure au nombre maximal de vainqueurs de conflit (DMINWNL), VTAM diffère le démarrage des sessions SNA restantes jusqu'à ce qu'elles soient requises par une application de base de données répartie.

DMINWNL=10
Nombre de sessions dans lesquelles ce système DB2 Universal Database for OS/390 est le vainqueur de conflit. Le paramètre DMINWNL est la valeur par défaut pour le traitement de CNOS, mais elle peut être remplacée pour tout partenaire donné, en ajoutant une ligne à la table SYSIBM.LUMODES dans la base de données de communications DB2 Universal Database for OS/390.

DMINWNR=10
Nombre de sessions dans lesquelles le système partenaire est le vainqueur de conflit. Le paramètre DMINWNR est la valeur par défaut pour le traitement de CNOS, mais elle peut être remplacée pour tout partenaire donné, en ajoutant une ligne à la table SYSIBM.LUMODES dans la base de données de communications DB2 Universal Database for OS/390.

DSESLIM=20
Nombre total de sessions (qui ont abouti ou non) que vous pouvez établir entre DB2 Universal Database for OS/390 et un autre système réparti pour un nom de groupe de mode donné. Le paramètre DSESLIM est la valeur par défaut pour le traitement de CNOS, mais elle peut être remplacée pour tout partenaire donné en ajoutant une

ligne à la table SYSIBM.LUMODES dans la base de données de communications DB2 Universal Database for OS/390.

Si le partenaire ne peut pas prendre en charge le nombre de sessions indiquées par les paramètres DSESLIM, DMINWNL ou DMINWNR, le processus CNOS négocie, pour ces paramètres, de nouvelles valeurs qui peuvent être acceptées par le partenaire.

EAS=9999
Estimation du nombre total de sessions requises par cette LU VTAM.

MODETAB=RDBMODES
Identifie la table MODE VTAM contenant chaque nom de mode DB2 Universal Database for OS/390.

PRTCT=PSWDBD1
Identifie le mot de passe VTAM à utiliser lors d'une tentative de connexion de DB2 Universal Database for OS/390 à VTAM. Si vous omettez le mot clé PRTCT, aucun mot de passe n'est requis et vous devez omettre le mot clé PASSWORD= dans l'inventaire du journal des modifications de DB2 Universal Database for OS/390.

SECACPT=ALREADYV
Identifie la valeur de sécurité de conversation SNA la plus élevée qui soit acceptée par ce système DB2 Universal Database for OS/390 lors de la réception d'une demande de base de données répartie émanant d'un système éloigné. Le mot clé ALREADYV indique que ce système DB2 Universal Database for OS/390 peut accepter trois options de sécurité de session SNA issues d'autres systèmes DRDA demandant des données provenant de ce système DB2 Universal Database for OS/390 :

- SECURITY=SAME (demande qui a déjà été vérifiée et qui contient uniquement l'ID utilisateur du demandeur).
- SECURITY=PGM (demande contenant le mot de passe du demandeur ou un PassTicket).
- SECURITY=NONE (demande ne contenant aucune donnée de sécurité). DB2 Universal Database for OS/390 rejette les demandes DRDA spécifiant SECURITY=NONE.

Il est préférable de toujours spécifier SECACPT=ALREADYV, car le niveau de sécurité des conversations SNA de chaque partenaire DB2 Universal Database for OS/390 est issu de la base de données de communications DB2 Universal Database for OS/390 (colonne USERSECURITY de la table SYSIBM.LUNAMES). SECACPT=ALREADYV vous offre la plus grande souplesse pour la sélection des valeurs de USERSECURITY.

VERIFY=NONE

Identifie le niveau de sécurité des sessions SNA (vérification de la LU partenaire) requis par ce système DB2 Universal Database for OS/390. La valeur NONE indique que la vérification de la LU partenaire n'est pas requise.

DB2 Universal Database for OS/390 ne restreint pas votre choix pour le mot clé VERIFY. Dans le cas d'un réseau non sécurisé, VERIFY=REQUIRED est recommandé. VERIFY=REQUIRED permet à VTAM de rejeter les partenaires qui ne peuvent pas effectuer de vérification de LU partenaire. Si vous choisissez VERIFY=OPTIONAL, VTAM effectue la vérification de la LU partenaire uniquement pour les partenaires qui en fournissent le support.

VPACING=2

Attribue la valeur 2 pour la régulation de VTAM.

SYNCLVL=SYNCPT

Indique que DB2 Universal Database for OS/390 peut prendre en charge la validation en deux phases. VTAM utilise ces informations pour informer le partenaire que la validation en deux phases est disponible. Si ce mot clé est présent, DB2 Universal Database for OS/390 utilise automatiquement la validation en deux phases si cette dernière peut être prise en charge par le partenaire.

ATNLOSS=ALL

Indique que DB2 Universal Database for OS/390 doit être informé chaque fois que se termine une session VTAM. C'est la garantie que DB2 Universal Database for OS/390 exécute une resynchronisation SNA lorsque cela est requis.

DSESLIM, DMINWNL et DMINWNR vous permettent de définir un nombre maximal de sessions VTAM par défaut pour l'ensemble des partenaires. Pour les partenaires requérant un nombre maximal de sessions particulier, la table SYSIBM.LUMODES peut être utilisée pour remplacer le nombre maximal de sessions par défaut. Vous pouvez par exemple vouloir spécifier un nombre maximal de sessions par défaut VTAM adapté à vos systèmes OS/2. Pour d'autres partenaires, vous pouvez, dans la table SYSIBM.LUMODES, créer des lignes pour définir le nombre maximal de sessions voulu. Considérez ces exemples de valeurs :

```
DSESLIM=4,DMINWNL=0,DMINWNR=4
```

Ces paramètres permettent à chacun des partenaires de créer jusqu'à quatre sessions avec DB2 Universal Database for OS/390, le partenaire étant le vainqueur de conflit dans chacune des sessions. Parce qu'OS/2 crée les conversations LU 6.2 avec DB2 Universal Database for OS/390 en faisant d'OS/2 le vainqueur de conflit dans les sessions, vous profitez d'un petit

avantage au niveau de la performance. Si OS/2 a une session de vainqueur de conflit disponible, aucune permission n'est requise pour le démarrage d'une nouvelle conversation LU 6.2.

Définition du système local (TCP/IP)

Pour plus de commodité, la présente section contient des informations extraites du manuel *DB2 Connect Enterprise Edition pour OS/2 et Windows - Mise en route*. Pour des informations plus détaillées, reportez-vous aux manuels *DB2 Universal Database for OS/390 Installation Reference* et *DRDA Support for TCP/IP with DB2 Universal Database for OS/390 and DB2 Universal Database*.

Les étapes nécessaires à la définition des communications TCP/IP avec DB2 Universal Database for OS/390 sont les suivantes :

1. Les communications TCP/IP doivent être activées sur DB2 Universal Database for OS/390 et le système partenaire.
2. Deux numéros de port TCP/IP appropriés doivent être affectés par votre administrateur réseau. Par défaut, DB2 Universal Database for OS/390 utilise le numéro de port 446 pour les connexions de base de données et le numéro de port 5001 pour les demandes de resynchronisation (validation en deux phases).
3. Le serveur d'applications éloignées ou le demandeur d'application doit utiliser les mêmes numéros de port (ou noms de service) que DB2 Universal Database for OS/390.
4. Vérifiez que l'option de sécurité TCP/IP "already verified" (déjà vérifié) a la valeur `YES`. Reportez-vous à la section «Fonctions supplémentaires de sécurité» à la page 50.
5. Le fichier d'amorçage de DB2 Universal Database for OS/390 doit comprendre des paramètres supplémentaires. La figure 18 à la page 60 présente les paramètres supplémentaires requis pour activer les communications TCP/IP.

```
//SYSADMB JOB ,'DB2 5.1 JOB',CLASS=A
//*
//*        CHANGE LOG INVENTORY:
//*        UPDATE BSDS WITH
//*             - DB2 LOCATION NAME FOR NEW_YORK3
//*             - VTAM LUNAME (NYM2DB2)
//*             - DB2/VTAM PASSWORD
//*
//*             - GENERIC LU NAME
//*             - TCP/IP PORT FOR DATABASE CONNECTIONS
//*             - TCP/IP PORT FOR RESYNCH OPERATIONS
//*
//DSNBSDS EXEC PGM=DSNJU003
//STEPLIB  DD  DISP=SHR,DSN=DSN510.DSNLOAD
//SYSUT1   DD  DISP=OLD,DSN=DSNC510.BSDS01
//SYSUT2   DD  DISP=OLD,DSN=DSNC510.BSDS02
//SYSPRINT DD  SYSOUT=*
//SYSUDUMP DD  SYSOUT=*
//SYSIN    DD  *
 DDF    LOCATION=NEW_YORK3,LUNAME=NTYM2DB2,PASSWORD=PSWDBD1,
        GENERICLU=name,PORT=446,RESPORT=5001
/*
//*
```

Figure 18. Exemple de définition de fichier d'amorçage de DDF (pour TCP/IP)

Définition des systèmes éloignés

Lorsqu'une application DB2 Universal Database for OS/390 demande des données issues d'un système éloigné, elle effectue une recherche dans les tables de bases de données de communications pour trouver des informations relatives au système éloigné. La base de données de communications (CDB) est un groupe de tables SQL géré par l'administrateur du système DB2 Universal Database for OS/390. En tant qu'administrateur du système DB2 Universal Database for OS/390, vous pouvez utiliser SQL pour insérer des lignes dans la base de données de communications pour décrire chaque partenaire DRDA potentiel. Vous trouverez une description complète de la base de données de communications et de son utilisation dans les manuels *DB2 Universal Database for OS/390 SQL Reference* et *DB2 Universal Database for OS/390 Installation Guide*.

Les informations suivantes sont recherchées dans la base de données de communications :

- Le nom de LU et le TPN (pour les connexions SNA)
- L'adresse TCP/IP (requise uniquement pour les connexions SNA TCP/IP sortantes)
- Les informations de sécurité réseau requises par le site éloigné
- Le nombre maximal de sessions et les noms de mode utilisés pour la communication avec le site éloigné (connexion SNA)

Peuplement de la base de données de communications : Aucune mise à jour de la base de données de communications n'est requise si vous n'utilisez que les connexions de bases de données TCP/IP entrantes ; ainsi, si vous souhaitez n'utiliser DB2 Universal Database for OS/390 qu'en tant que serveur TCP/IP, il n'est pas nécessaire de peupler la base de données de communications et les valeurs par défaut peuvent être utilisées. Toutefois, si vous utilisez les connexions SNA entrantes, vous devez laisser au moins une ligne à blanc dans SYSIBM.LUNAMES. Par exemple, pour permettre aux demandes de connexion de bases de données SNA d'être acceptées par n'importe quelle LU DB2 Connect en entrée, utilisez une commande SQL comme celle-ci :

```
INSERT INTO SYSIBM.LUNAMES (LUNAME) VALUES ('        ')
```

Lorsque vous utilisez DB2 Universal Database for OS/390 comme demandeur, la base de données de communications doit toujours être mise à jour. Vous devez insérer des lignes dans la table SYSIBM.LOCATIONS ainsi que dans la table SYSIBM.LUNAMES (pour les connexions SNA) ou SYSIBM.IPNAMES (pour les connexions TCP/IP).

En outre, si vous souhaitez contrôler les besoins de sécurité entrante ou la conversion d'id utilisateur entrant pour les connexions SNA, il se peut que d'autre mises à jour soient requises dans la base de données de communications soient requises. Des exemples supplémentaires sont fournis comme indiqué ci-après. La section «Définition de la sécurité» à la page 70, indique comment définir la sécurité utilisateur lors de la configuration d'un demandeur d'application et la section «Définition de la sécurité» à la page 83, décrit la configuration d'un serveur d'applications.

Le manuel *DB2 Universal Database for OS/390 Administration Guide* décrit en décrit en détail les conditions requises pour la mise à jour des tables de bases de données de communications. Après avoir rempli la base de données de communications, vous pouvez écrire des requêtes permettant d'accéder aux données présentes sur des systèmes éloignés. Le manuel *DB2 Universal Database for OS/390 Installation Reference* fournit également des informations sur la mise à jour des bases de données de communications.

Gestion des demandes par la base de données de communications : Lors de l'envoi d'une demande, DB2 Universal Database for OS/390 utilise la colonne LINKNAME de la table du catalogue SYSIBM.LOCATIONS pour déterminer le protocole de réseau à utiliser pour la connexion de base de données sortante. Pour recevoir des demandes VTAM, vous devez sélectionner un nom LUNAME dans le panneau d'installation DSNTIPR de DB2 Universal Database for OS/390. Pour recevoir des demandes TCP/IP, vous devez sélectionner un port DRDA et un port de resynchronisation dans le panneau d'installation DSNTIP5 de DB2 Universal Database for OS/390.

TCP/IP utilise le numéro de port du serveur pour transmettre des demandes du réseau au sous-système DB2 approprié.

Si la valeur de la colonne LINKNAME se trouve dans la table SYSIBM.IPNAMES, TCP/IP est utilisé pour les connexions DRDA. Si la valeur se trouve dans la table SYSIBM.LUNAMES, SNA est utilisé. Si le même nom se trouve à la fois dans SYSIBM.LUNAMES et dans SYSIBM.IPNAMES, TCP/IP est utilisé pour la connexion à l'emplacement.

Remarque : Un demandeur ne peut pas se connecter à un emplacement donné en utilisant à la fois les protocoles SNA et TCP/IP. Par exemple, si la table SYSIBM.LOCATIONS indique LU1 comme LINKNAME et si LU1 est défini à la fois dans la table SYSIBM.IPNAMES et dans la table SYSIBM.LUNAMES, TCP/IP est le seul protocole utilisé pour la connexion à LU1 à partir de ce demandeur.

Tables de bases de données de communications : La base de données de communications est constituée des tables suivantes :

1. **SYSIBM.LOCATIONS**

   Cette table permet à DB2 Universal Database for OS/390 de déterminer les informations d'adresse SNA ou TCP/IP requises pour l'accès à chaque nom RDB_NAME sélectionné par une application DB2 Universal Database for OS/390 *pour les demandes sortantes*. Les colonnes sont les suivantes :

   LOCATION
   RDB_NAME du système éloigné. DB2 Universal Database for OS/390 limite la longueur de la valeur de RDB_NAME à 16 octets, ce qui représente 2 octets de moins par rapport à la limite de 18 octets définie dans DRDA.

   LINKNAME
   Nom de LU ou attributs TCP/IP du système éloigné.

   PORT Nom de port TCP/IP ou informations relatives au nom de service (le nom de port par défaut pour DRDA est 446).

   TPN Nom du programme transactionnel APPC du système éloigné. Si le système éloigné est un système DB2 Universal Database for OS/390 ou utilise la valeur de TPN DRDA par défaut (X'07F6C4C2'), une chaîne de caractères vide peut être utilisée pour spécifier le TPN car DB2 Universal Database for OS/390 choisit automatiquement la valeur appropriée.

   Si le système éloigné requiert une valeur de TPN différente de la valeur de TPN par défaut, vous devez mentionner cette valeur dans cette colonne.

2. **SYSIBM.LUNAMES**

   Cette table définit les attributs de réseau des systèmes éloignés utilisant les connexions SNA. Les colonnes sont les suivantes :

   LUNAME
   Nom de LU du système éloigné.

   SYSMODENAME
   Nom de mode de connexion VTAM utilisé pour l'établissement de conversations *entre deux systèmes* DB2 Universal Database for OS/390 pour le *support de serveur secondaire* de DB2 Universal Database for OS/390 (accès défini par le système). Une valeur à blanc dans cette colonne indique qu'il faut utiliser IBMDB2LM pour les conversations du système DB2 Universal Database for OS/390.

   SECURITY_IN
   Options d'acceptation de sécurité réseau requises quant au système éloigné lorsque ce système DB2 Universal Database for OS/390 fait office de serveur pour le système éloigné (conditions requises de *sécurité entrante*). Les valeurs peuvent être les suivantes :

   - **V** pour "verify" (vérifié). Une demande de connexion entrante doit comprendre l'un des éléments suivants : un ID utilisateur et un mot de passe, un ID utilisateur et un PassTicket RACF ou un ticket de sécurité DCE.
   - **A** pour "already verified" (déjà vérifié). Une demande ne requiert pas de mot de passe, bien qu'un contrôle de mot de passe soit effectué si elle est envoyée. Avec cette option, une demande de connexion entrante est acceptée si elle comprend l'un des éléments suivants : un ID utilisateur, un ID utilisateur et un mot de passe, un ID utilisateur et un PassTicket RACF ou un ticket de sécurité DCE.

     Si la colonne USERNAMES contient 'I' ou 'B', RACF n'est pas appelé pour valider les demandes de connexion entrantes ne contenant qu'un ID utilisateur.

   SECURITY_OUT
   Options d'acceptation de sécurité réseau requises du système éloigné lorsque ce système DB2 Universal Database for OS/390 agit en tant que demandeur (conditions requises de *sécurité sortante*). Les valeurs peuvent être les suivantes :

   - **A** pour "already verified" (déjà vérifié). Les demandes de connexion sortantes contiennent un ID autorisation, mais pas de mot de passe. L'ID autorisation utilisé pour une demande de connexion sortante est l'ID autorisation de l'utilisateur DB2 ou un ID converti, selon la valeur de la colonne USERNAMES.

- **R** pour ″RACF PassTicket″ (PassTicket RACF). Les demandes de connexion sortantes contiennent un ID utilisateur et un PassTicket RACF. Le nom de LU du serveur est utilisé comme nom d'application du PassTicket RACF.

  L'ID autorisation utilisé pour une demande de connexion sortante est l'ID autorisation de l'utilisateur DB2 ou un ID converti, selon la valeur de la colonne USERNAMES.
- **P** pour ″password″ (mot de passe). Les demandes de connexion sortantes contiennent un ID autorisation et un mot de passe. Le mot de passe est obtenu à partir de la table SYSIBM.USERNAMES ou de RACF, selon la valeur indiquée dans la colonne ENCRYPTPWDS.

  La colonne USERNAMES doit spécifier 'B' ou 'O'.

ENCRYPTPSWDS
Indique si les mots de passe échangés avec ce partenaire sont codés ou non. Les mots de passe codés sont uniquement pris en charge par les demandeurs et les serveurs DB2 Universal Database for OS/390.

MODESELECT
Détermine si la table SYSIBM.MODESELECT est utilisée ou non pour la sélection d'une entrée de mode de connexion VTAM (nom de mode) basée sur la demande émise par l'utilisateur final ou l'application qui émet la demande. Si cette colonne contient un 'Y', la table SYSIBM.MODESELECT est utilisée pour obtenir le nom de mode pour chaque demande de base de données répartie sortante.

Si MODESELECT contient une autre valeur que 'Y', le nom de mode IBMDB2LM est utilisé pour les demandes d'accès défini par le système et le nom de mode IBMRDB est utilisé pour les demandes DRDA.

La colonne MODESELECT vous permet de donner la priorité aux demandes de base de données répartie en spécifiant une classe de service VTAM associée au nom de mode.

USERNAMES
Niveau d'identification du site émetteur et conversion de l'ID utilisateur requis. Cette colonne spécifie également les paramètres de sécurité utilisés par ce sous-système DB2 Universal Database for OS/390 lors de la demande de données émanant du partenaire éloigné (conditions requises de *sécurité sortante*). Cette colonne peut avoir pour valeur I, O, ou B (entrants seulement, sortants seulement ou les deux).

GENERIC
Indique si DB2 Universal Database for OS/390 doit utiliser son nom de LU réel ou générique.

3. **SYSIBM.LUMODES**

Cette table permet de définir le nombre maximal de sessions LU 6.2 (limites CNOS) pour les systèmes partenaires utilisant les connexions APPC (SNA). Les colonnes sont les suivantes :

LUNAME
Nom de LU du système éloigné.

MODENAME
Nom du mode de connexion VTAM dont les limites sont spécifiées. Une valeur à blanc revient à indiquer IBMDB2LM.

CONVLIMIT
Nombre maximal de conversations actives entre le système DB2 Universal Database for OS/390 local et le système éloigné pour ce mode de connexion. Cette valeur permet de remplacer le paramètre DSESLIM dans l'instruction de définition APPL VTAM pour ce mode de connexion, qui définit le nombre maximal de sessions VTAM par défaut pour DB2 Universal Database for OS/390.

La valeur sélectionnée dans CONVLIMIT est utilisée pendant le processus CNOS afin de définir CONVLIMIT/2 pour DMINWNR et DMINWNL.

4. **SYSIBM.MODESELECT**

Cette table vous permet de spécifier différents noms de mode pour des utilisateurs finals individuels et des applications DB2 Universal Database for OS/390. Elle est utilisée uniquement pour les connexions SNA. Dans la mesure où une classe de service (COS) peut être associée à chaque nom de mode VTAM, vous pouvez utiliser cette table pour attribuer des priorités de transmission de réseau aux applications de base de données répartie, sur la base d'une combinaison de AUTHID, PLANNAME et LUNAME. Les colonnes sont les suivantes :

AUTHID
ID autorisation de l'utilisateur DB2 Universal Database for OS/390. La valeur par défaut est à blanc, ce qui indique que le nom de mode de connexion spécifié s'applique à tous les ID autorisation.

PLANNAME
Nom de plan associé à l'application demandant l'accès à un système de bases de données éloignées. La valeur par défaut est à blanc, ce qui indique que le nom de mode de connexion spécifié

s'applique à tous les noms de plan. Le nom de plan utilisé pour la commande BIND PACKAGE est DSNBIND.

LUNAME
Nom de LU associé au système de bases de données éloignées.

MODENAME
Nom de mode de connexion VTAM à utiliser lors de l'acheminement d'une demande de base de données répartie vers le système éloigné indiqué. Par défaut, cette valeur est à blanc, pour indiquer que l'on doit utiliser IBMDB2LM pour les conversations à accès défini par le système et IBMRDB pour les conversations DRDA.

5. **SYSIBM.USERNAMES**

Cette table permet de gérer les noms d'utilisateurs finals via des mots de passe, des conversions de noms et des identifications de site émetteur. DB2 Universal Database for OS/390 utilise le nom de l'utilisateur comme ID autorisation. La plupart des autres produits utilisent ce nom comme ID utilisateur.

Avec cette table, vous pouvez utiliser la conversion de nom pour faire en sorte que différentes valeurs soient utilisées pour les connexions d'ID utilisateur et l'ID autorisation DB2 Universal Database for OS/390. Le processus de conversion de nom est autorisé pour les demandes destinées à un système éloigné (demandes *sortantes*) et pour les demandes émanant d'un système éloigné (demandes *entrantes*). Si les mots de passe ne sont pas codés, cette table est la source du mot de passe de l'utilisateur final lorsque l'ID utilisateur et le mot de passe sont envoyés vers un site éloigné. Les colonnes sont les suivantes :

TYPE Description de l'utilisation de la ligne (qu'il s'agisse ou non d'une ligne décrivant les conversions de noms pour les demandes sortantes ou entrantes d'identification de site émetteur).

I signifie connexions entrantes, **O** signifie connexions sortantes.

Utilisez ″O″ pour les connexions TCP/IP (la conversion d'ID et l'identification de site émetteur sortantes ne sont pas effectuées pour les demandes TCP/IP).

AUTHID
Pour la conversion de nom sortante, il s'agit de l'ID autorisation DB2 Universal Database for OS/390 à convertir. Pour la conversion de nom entrante, il s'agit de l'ID utilisateur SNA à convertir. Dans les deux cas, une valeur AUTHID à blanc s'applique à tous les ID autorisation ou utilisateurs.

LINKNAME
Identifie les emplacements de réseaux VTAM ou TCP/IP associés à

cette ligne. Une valeur à blanc dans cette colonne indique que cette règle de conversion de nom s'applique à n'importe quel partenaire TCP/IP ou SNA.

Si une valeur LINKNAME est spécifiée, l'une des instructions suivantes ou les deux doivent être vraies :

- Une ligne existe dans SYSIBM.LUNAMES, dont le nom de LUNAME correspond à la valeur spécifiée dans la colonne LINKNAME de la table SYSIBM.USERNAMES. Cette ligne indique le site VTAM associé à cette règle de conversion de nom.
- Une ligne existe dans SYSIBM.IPNAMES dont le nom LINKNAME correspond à la valeur indiquée dans la colonne SYSIBM.USERNAMES LINKNAME. Cette ligne indique l'hôte TCP/IP associé à cette règle de conversion de nom.

  La conversion de nom et l'identification du site émetteur entrantes ne sont pas effectuées pour les clients TCP/IP.

NEWAUTHID
Nouveau nom d'utilisateur final (ID utilisateur SNA ou ID autorisation DB2 Universal Database for OS/390). Une valeur à blanc indique qu'il n'est pas nécessaire de convertir l'ID.

PASSWORD
Mot de passe utilisé pour la conversation d'allocation si les mots de passe ne sont pas codés (ENCRYPTPSWDS = 'N' dans SYSIBM.LUNAMES). Si les mots de passe sont codés, ignorez cette colonne.

6. **SYSIBM.IPNAMES**

Cette table est utilisée pour les noeuds TCP/IP.

LINKNAME
La valeur spécifiée dans cette colonne doit correspondre à la valeur spécifiée dans la colonne LINKNAME de SYSIBM.LOCATIONS.

SECURITY_OUT
Cette colonne définit l'option de sécurité DRDA utilisée lorsque des applications SQL DB2 locales se connectent à un serveur éloigné associé à cet hôte TCP/IP :

- **A** pour ″already verified″ (déjà vérifié). Les demandes de connexion sortantes contiennent un ID autorisation, mais pas de mot de passe. L'ID autorisation utilisé pour une demande de connexion sortante est l'ID autorisation de l'utilisateur DB2 ou un ID converti, selon la valeur de la colonne USERNAMES.
- **R** pour ″RACF PassTicket″ (PassTicket RACF). Les demandes de connexion sortantes contiennent un ID utilisateur et un

PassTicket RACF. La valeur spécifiée dans la colonne LINKNAME est utilisée comme nom d'application PassTicket RACF pour le serveur éloigné.

L'ID autorisation utilisé pour une demande de connexion sortante est l'ID autorisation de l'utilisateur DB2 ou un ID converti, selon la valeur de la colonne USERNAMES.

- **P** pour "password" (mot de passe). Les demandes de connexion sortantes contiennent un ID autorisation et un mot de passe. Le mot de passe provient de la table SYSIBM.USERNAMES.

  La colonne USERNAMES doit spécifier "O."

USERNAMES

Cette colonne contrôle la conversion d'ID autorisation sortante. Cette opération est effectuée lorsqu'un ID autorisation est envoyé par DB2 à un serveur éloigné.

- **O** signifie qu'un ID sortant fait l'objet d'une conversion. Des lignes de la table SYSIBM.USERNAMES sont utilisées pour effectuer la conversion d'ID.

  Aucune conversion ou identification du site émetteur n'est effectuée pour les ID entrants.
- Une valeur à blanc signifie qu'aucune conversion n'est effectuée.

IPADDR

Cette colonne contient l'adresse IP ou le nom de domaine d'un hôte TCP/IP éloigné. La colonne IPADDR doit être spécifiée comme suit :

- Si la colonne IPADDR contient une chaîne de caractères justifiée à gauche et contenant quatre valeurs numériques délimitées par des points décimaux, DB2 considère que la valeur est une adresse IP en notation décimale avec points. Par exemple, la chaîne '123.456.78.91' sera interprétée comme une adresse IP en notation décimale avec points.
- Toutes les autres valeurs sont interprétées en tant que nom de domaine TCP/IP, pouvant être résolu par l'appel "gethostbyname". Les noms de domaine TCP/IP ne tiennent pas compte des majuscules et des minuscules.

Paramétrage des communications (SNA)

VTAM est le gestionnaire de communications des systèmes OS/390. VTAM accepte les verbes LU 6.2 de DB2 Universal Database for OS/390 et les convertit en flots de données LU 6.2 que vous pouvez transmettre sur le réseau. Pour permettre à VTAM de communiquer avec les applications partenaires définies dans les bases de données de communications DB2 Universal Database for OS/390, vous devez fournir à VTAM les informations suivantes :

- Le nom de LU pour chaque serveur.

  Lorsque DB2 Universal Database for OS/390 communique avec VTAM, il est autorisé à ne transmettre qu'un seul nom de LU (pas NETID.LUNAME) à VTAM pour identifier la destination voulue. Ce nom de LU doit être unique parmi les noms de LU connus du système VTAM local, permettant ainsi à VTAM de déterminer les noms de NETID et de LU à partir du nom de LU transmis par DB2 Universal Database for OS/390. Le fait que les noms de LU soient uniques sur le réseau SNA d'une entreprise simplifie grandement le processus de définition des ressources VTAM. Toutefois, cela n'est pas toujours possible. Si les noms de LU de vos réseaux SNA ne sont pas uniques, vous devez utiliser la conversion de nom de LU VTAM afin de créer la combinaison NETID.LUNAME correcte pour un nom de LU qui n'est pas unique. Vous trouverez la description de cette procédure dans la section «Resource Name Translation» du manuel *VTAM Network Implementation Guide*.

  L'emplacement et la syntaxe de ces définitions VTAM permettant de définir des noms de LU éloignée dépendent essentiellement du type de connexion physique et logique du système éloigné au système VTAM local.
- La taille de RU, la taille de la fenêtre de régulation et la classe de service pour chaque nom de mode. Créez une entrée dans la table de modes VTAM pour chaque nom de mode spécifié dans la base de données de communications. Vous devez également définir IBMRDB et IBMDB2LM.
- Les profils VTAM et RACF pour l'algorithme de vérification de la LU, si vous pensez utiliser la vérification de LU partenaire.

Définition de la taille de RU et de la régulation : Les entrées de table de modes VTAM que vous avez définies spécifient les tailles de RU et la régulation. Si ces valeurs ne sont pas mentionnées correctement, des effets indésirables peuvent se produire pour toutes les applications VTAM.

Une fois que vous avez choisi les tailles de RU, le nombre maximal de sessions et la régulation, il est très important d'évaluer l'impact que ces valeurs peuvent avoir sur le réseau VTAM existant. Lors de l'installation d'une nouvelle base de données répartie, vous devez tenir compte des éléments suivants :

- Dans le cas des connexions VTAM CTC, vérifiez que la valeur du paramètre MAXBFRU est suffisante pour gérer la taille de RU plus les

29 octets ajoutés par VTAM pour l'en-tête de demande et l'en-tête de transmission SNA. Le paramètre MAXBFRU est indiqué par unités de 4 ko ; ce paramètre doit donc prendre une valeur minimale de 2 pour pouvoir gérer une RU de 4 ko.

- Dans le cas de connexions NCP, assurez-vous que la valeur du paramètre MAXDATA est suffisante pour gérer la taille de RU plus 29 octets. Si vous indiquez une taille de RU de 4 ko, MAXDATA doit prendre au moins la valeur 4125.

  Si vous indiquez le paramètre NCP MAXBFRU, sélectionnez une valeur pouvant gérer la taille de RU plus 29 octets. Dans la cas de NCP, le paramètre MAXBFRU définit le nombre de tampons d'E-S VTAM pouvant prendre en charge l'unité d'information acheminable (PIU). Si vous choisissez une taille de tampon IOBUF de 441, MAXBFRU=10 traite correctement une RU de 4 ko car 10*441 est supérieur à 4096+29.
- Le manuel *DRDA Connectivity Guide* indique comment évaluer l'impact de votre base de données répartie sur le pool IOBUF VTAM. Si une trop grande quantité de ressources de pool IOBUF est utilisée, les performances du système VTAM seront affectées pour toutes les applications VTAM.

Définition des communications (TCP/IP)

Reportez-vous à la section «Définition du système local (TCP/IP)» à la page 59.

Définition de la sécurité

Lorsqu'un système éloigné exécute des opérations de traitement sur des bases de données réparties au nom d'une application SQL, il doit être capable de répondre aux critères de sécurité du demandeur d'application, du serveur d'applications et du réseau reliant ces derniers entre eux. Ces critères entrent dans une ou plusieurs des catégories suivantes :

- Sélection des noms d'utilisateurs finals
- Paramètres de sécurité réseau
- Sécurité du gestionnaire de bases de données
- Sécurité assurée par un sous-système de sécurité externe
- Représentation des données

Sélection des noms d'utilisateurs finals

Dans les systèmes OS/390, les utilisateurs finals sont identifiés par un *ID utilisateur* comportant de 1 à 8 caractères. Cet ID utilisateur doit être unique pour un système OS/390 donné, mais ne doit pas forcément l'être sur tout le réseau. Par exemple, prenons le cas de deux utilisateurs s'appelant tous les deux JONES ; l'un se trouve sur le système NEWYORK et l'autre sur le système DALLAS. S'il s'agit d'une seule et même personne, il n'existe aucun risque de conflit. Cependant, si l'utilisateur JONES de DALLAS n'est pas le même que l'utilisateur JONES de NEWYORK, le réseau SNA (et, par conséquent, les systèmes de bases de données réparties de ce réseau) ne

pourront pas faire la distinction entre ces deux utilisateurs. Si vous ne remédiez pas à cette situation, JONES de DALLAS pourra utiliser les droits de JONES de NEWYORK.

DB2 Universal Database for OS/390 fournit un support de conversion pour les noms d'utilisateurs finals afin d'éviter les conflits de dénomination. Lorsqu'une application au niveau du demandeur d'application DB2 Universal Database for OS/390 émet une demande de base de données répartie, DB2 Universal Database for OS/390 exécute la conversion du nom si la base de données de communications spécifie que la *conversion de nom sortante* est requise. Si la conversion de nom sortante est sélectionnée, DB2 Universal Database for OS/390 exige toujours qu'un mot de passe soit envoyé avec chaque demande de base de données répartie sortante.

Pour activer la conversion de nom sortante dans DB2 Universal Database for OS/390, vous devez définir ″O″ ou ″B″ pour la colonne USERNAMES de la table SYSIBM.LUNAMES ou SYSIBM.IPNAMES. Si 'O' est défini pour USERNAMES, la conversion du nom d'utilisateur final s'effectue pour les demandes sortantes. Si 'B' est défini pour USERNAMES, la conversion du nom d'utilisateur final s'effectue pour les demandes sortantes et entrantes.

Etant donné que l'autorisation DB2 Universal Database for OS/390 dépend à la fois de l'ID utilisateur de l'utilisateur final et de l'ID utilisateur du propriétaire du module ou du plan DB2 Universal Database for OS/390, le processus de conversion du nom d'utilisateur final s'opère pour l'ID utilisateur de l'utilisateur final, l'ID utilisateur du propriétaire du plan et l'ID utilisateur du propriétaire du module.[3] Le processus de conversion de nom recherche dans la table SYSIBM.USERNAMES, dans la séquence suivante, une ligne qui corresponde à l'un des modèles (TYPE.AUTHID.LINKNAME) suivants :

1. O.AUTHID.LINKNAME— Règle de conversion pour un utilisateur final particulier vers un système partenaire particulier.
2. O.AUTHID.espace— Règle de conversion pour un utilisateur final particulier vers n'importe quel système partenaire.
3. O.espace.LINKNAME— Règle de conversion pour n'importe quel utilisateur vers un système partenaire particulier.

S'il n'existe aucune ligne correspondante, DB2 Universal Database for OS/390 rejette la demande de base de données répartie. S'il existe une ligne

3. Si la demande est envoyée à un serveur DB2 Universal Database for OS/390, la conversion de nom s'opère également pour le propriétaire du module et pour celui du plan. Aucun mot de passe n'est jamais associé aux noms de propriétaires de module et de plan.

correspondante, la valeur de la colonne NEWAUTHID est utilisée comme ID autorisation. (Une valeur NEWAUTHID à blanc indique que le nom original est utilisé sans conversion).

Reportez-vous à l'exemple déjà évoqué. Vous souhaitez attribuer à JONES de NEWYORK un nom différent (NYJONES) lorsque JONES envoie des demandes de bases de données réparties à DALLAS. Dans l'exemple, imaginez que l'application utilisée par JONES appartienne à DSNPLAN (propriétaire du plan DB2 Universal Database for OS/390) et qu'il ne soit pas nécessaire de convertir cet ID utilisateur lors de son envoi à DALLAS. Les instructions SQL requises pour la fourniture des règles de conversion des noms dans les bases de données de communications sont illustrées à la figure 19.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_OUT, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', 'O');
INSERT INTO SYSIBM.LOCATIONS
     (LOCATION, LINKNAME, LINKATTR)
  VALUES ('DALLAS', 'LUDALLAS', '');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'JONES', 'LUDALLAS', 'NYJONES', 'JONESPWD');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'DSNPLAN', 'LUDALLAS', ' ', 'PLANPWD');
```

Figure 19. SQL pour conversion de nom sortante (SNA)

Les tables de bases de données de communications qui en résultent sont illustrées à la figure 20 à la page 73.

NEWYORK.SYSIBM.LOCATIONS

LOCATION	LINKNAME	PORT	TPN
DALLAS	LUDALLAS		

NEWYORK.SYSIBM.LUNAMES

LUNAME	SYSMODENAME	SECURITY-IN	SECURITY-OUT	ENCRYPTPSWDS	MODESELECT	USERNAMES
LUDALLAS			A	N	N	O

NEWYORK.SYSIBM.USERNAMES

TYPE	AUTHID	LINKNAME	NEWAUTHID	PASSWORD
0 0	JONES DSNPLAN	LUDALLAS LUDALLAS	NYJONES	JONESPWD PLANPWD

Figure 20. Conversion de nom sortante

La figure 21 présente un exemple plus simple indiquant comment se connecter à un serveur d'applications DRDA DB2 Universal Database à l'aide d'une connexion SNA.

```
  INSERT INTO SYSIBM.LUNAMES (LUNAME,
                              SECURITY_OUT,
                              ENCRYPTPSWDS,
                              USERNAMES)
                       VALUES ('NYX1GW01','P','N','O');
INSERT INTO SYSIBM.LOCATIONS (LOCATION,LINKNAME,TPN)
                             VALUES('TASG6',
                                    'NYX1GW01','NYSERVER');
INSERT INTO SYSIBM.USERNAMES (TYPE,AUTHID,LINKNAME,NEWAUTHID,PASSWORD)
       VALUES ('O','      ','NYX1GW01','SVTDBM6','SG6JOHN');
```

Figure 21. SQL pour conversion de nom sortante (exemple simple pour SNA)

La figure 22 présente un exemple simple indiquant comment se connecter à un serveur d'applications DRDA DB2 Universal Database à l'aide d'une connexion TCP/IP.

```
-- DB2 for Solaris1 - UNIX
   DELETE FROM SYSIBM.IPNAMES WHERE LINKNAME = 'SOLARIS1' ;
   INSERT INTO SYSIBM.IPNAMES ( LINKNAME
                              , SECURITY_OUT
                              , USERNAMES
                                , IBMREQD
                              , IPADDR)
                        VALUES ( 'SOLARIS1'
                              , 'P'
                              , 'O'
                                , 'N'
                              , '9.21.45.4')
                              ;
   INSERT INTO SYSIBM.LOCATIONS ( LOCATION
                                , LINKNAME
                                , IBMREQD
                                , PORT
                                , TPN)
                          VALUES ( 'TCPDB1'
                                , 'SOLARIS1'
                                , 'N'
                                , '30088'
                                , '')
                                ;
   INSERT INTO SYSIBM.USERNAMES ( TYPE
                                , AUTHID
                                , LINKNAME
                                , NEWAUTHID
                                , PASSWORD
                                , IBMREQD)
                          VALUES ( 'O'
                                , ''
                                , 'SOLARIS1'
                                , 'svtdbm5'
                                , 'svt5dbm'
                                , 'N')
                                ;
```

Figure 22. SQL pour conversion de nom sortante (exemple simple pour TCP/IP)

Sécurité réseau

Une fois que le demandeur d'application a sélectionné les noms d'utilisateurs finals pour représenter l'application éloignée, il doit fournir les données de sécurité réseau LU requises.

Pour les connexions SNA, la LU 6.2 offre trois grandes fonctions de sécurité réseau :

- Sécurité au niveau de la session, définie par le mot clé VERIFY dans l'instruction APPL VTAM. Reportez-vous aux commentaires de la figure 17 à la page 55, pour connaître la procédure à suivre pour la définition des options de sécurité au niveau de la session.
- Sécurité au niveau de la conversation, définie par le contenu de la table SYSIBM.LUNAMES.
- Cryptage des données, pris en charge uniquement pour VTAM 3.4 et les éditions ultérieures de VTAM.

Dans la mesure où le serveur d'applications est chargé de la gestion des ressources de bases de données, il détermine quelles sont les fonctions de sécurité réseau requises pour le demandeur d'application. Vous devez enregistrer les conditions de sécurité requises au niveau de la conversation de chaque serveur d'applications dans la table SYSIBM.LUNAMES ou SYSIBM.IPNAMES en définissant la colonne USERNAMES de manière à ce qu'elle reflète les conditions requises par le serveur d'applications.

Les options possibles pour les conversations SNA sont les suivantes :

SECURITY=SAME

Egalement connue sous le nom de sécurité déjà vérifiée, cette option suppose que seul l'ID utilisateur de l'utilisateur final est transmis au système éloigné (aucun mot de passe n'est transmis). Utilisez ce niveau de sécurité de conversation lorsque la colonne USERNAMES dans SYSIBM.LUNAMES ne contient ni 'O' ni 'B'.

Dans la mesure où DB2 Universal Database for OS/390 lie la conversion de nom d'utilisateur final à la sécurité de la conversation sortante, vous n'êtes pas autorisé à utiliser SECURITY=SAME lorsque la conversion de nom d'utilisateur final sortante est activée.

SECURITY=PGM

Cette option déclenche l'envoi de l'ID utilisateur final et du mot de passe au système éloigné pour validation. Utilisez cette option de sécurité lorsque la colonne USERNAMES de la table SYSIBM.LUNAMES contient 'O' ou 'B'.

En fonction des options définies dans la table SYSIBM.LUNAMES, DB2 Universal Database for OS/390 obtient le mot de passe de l'utilisateur final de deux sources différentes :

- Les mots de passe non codés proviennent de la colonne PASSWORD de la table SYSIBM.USERNAMES. DB2 Universal Database for OS/390 extrait les mots de passe de la table SYSIBM.USERNAMES lorsque la colonne ENCRYPTPSWDS de la

table SYSIBM.LUNAMES n'a pas pour valeur 'Y'. Les mots de passe obtenus par ce biais peuvent être transmis à n'importe quel serveur d'application DRDA.

La figure 23 définit les mots de passe pour SMITH et JONES. La colonne LUNAME de l'exemple contient des valeurs à blanc, par conséquent ces mots de passe sont utilisés pour toute tentative d'accès à un système éloigné de la part de SMITH ou de JONES.

```
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'JONES', ' ', ' ', 'JONESPWD');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', 'SMITH', ' ', ' ', 'SMITHPWD');
```

Figure 23. Envoi de mots de passe sur des sites éloignés (SNA)

- Les mots de passe codés sont envoyés sur le site éloigné lorsque la colonne ENCRYPTPSWDS de la table SYSIBM.LUNAMES contient 'Y'. Les mots de passe codés sont extraits de RACF (ou d'un produit équivalent), et ne peuvent être interprétés que par un autre système DB2 Universal Database for OS/390. En cas de communication avec un système autre que DB2 Universal Database for OS/390, n'indiquez pas ″Y″ dans ENCRYPTPSWDS.

  DB2 Universal Database for OS/390 recherche dans la table SYSIBM.USERNAMES l'ID utilisateur (valeur NEWAUTHID) à transmettre au système éloigné. Ce nom converti permet l'extraction du mot de passe RACF. Si vous ne souhaitez pas convertir les noms, vous devez créer des lignes dans la table SYSIBM.USERNAMES qui déclenchent l'envoi des noms sans conversion. La figure 24 permet l'envoi de demandes à LUDALLAS et à LUNYC sans conversion du nom d'utilisateur final (ID utilisateur).

```
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('O', ' ', 'LUDALLAS', ' ', ' ');
```

Figure 24. Envoi de mots de passe codés sur des sites éloignés (SNA)

SECURITY=NONE

Cette option n'est pas prise en charge par DRDA ; DB2 Universal Database for OS/390 ne prévoit donc rien pour cette option de sécurité.

Sécurité du gestionnaire de bases de données

La conversion de nom sortante constitue, pour le demandeur d'application, l'un des moyens de participer à la sécurité d'une base de données répartie, comme indiqué à la section «Sélection des noms d'utilisateurs finals» à la page 70. Vous pouvez utiliser la fonction de conversion du nom sortante pour contrôler l'accès à chaque serveur d'applications, sur la base de l'identité de l'utilisateur final et de l'application effectuant la demande. Les autres moyens permettant au serveur d'applications DB2 Universal Database for OS/390 de contribuer à la sécurité des systèmes répartis sont les suivants :

Définition des accès aux applications éloignées

Les utilisateurs finals définissent les accès aux applications éloignées au niveau du serveur d'applications via la commande BIND PACKAGE de DB2 Universal Database for OS/390. DB2 Universal Database for OS/390 *ne limite pas* l'utilisation de la commande BIND PACKAGE au niveau du demandeur. Toutefois, un utilisateur final ne peut pas utiliser de module éloigné si celui-ci ne fait pas partie d'un plan DB2 Universal Database for OS/390. DB2 Universal Database for OS/390 *limite* l'utilisation de la commande BIND PLAN. Un utilisateur final ne peut pas ajouter le module éloigné à un plan, à moins de bénéficier du privilège BIND ou BINDADD avec l'instruction GRANT de DB2 Universal Database for OS/390.

Lors de la définition de l'accès à un module, utilisez l'option ENABLE/DISABLE pour spécifier si le module doit être utilisé par TSO, CICS/ESA, IMS/ESA ou par un sous-système DB2 Universal Database for OS/390 éloigné.

Exécution d'applications éloignées

Pour exécuter une application éloignée, l'utilisateur final DB2 Universal Database for OS/390 doit disposer des droits d'exécution du plan DB2 Universal Database for OS/390 associé à cette application. Le propriétaire du plan DB2 Universal Database for OS/390 dispose automatiquement des droits d'exécution du plan. Les autres utilisateurs finals peuvent également se voir accorder les droits d'exécution du module à l'aide de l'instruction GRANT EXECUTE de DB2 Universal Database for OS/390. Le propriétaire de l'application de base de données répartie peut alors contrôler l'utilisation de l'application à raison d'un utilisateur à la fois.

Sous-système de sécurité

Le sous-système de sécurité externe sur les systèmes OS/390 est généralement fourni par RACF ou par un autre produit offrant une interface compatible

avec RACF. Le demandeur d'application DB2 Universal Database for OS/390 n'a pas d'appels directs avec le sous-système de sécurité externe, exception faite du support de mot de passe codé dont vous trouverez la description dans la section «Sécurité réseau» à la page 74. Toutefois, le sous-système de sécurité externe est utilisé indirectement au niveau du demandeur d'application, dans les situations suivantes :

- Le produit permettant de connecter l'utilisateur final à DB2 Universal Database for OS/390 utilise le sous-système de sécurité externe pour valider l'identité de l'utilisateur final (ID utilisateur et mot de passe). Cela se produit avant que l'utilisateur final ne se connecte à DB2 Universal Database for OS/390. Comme déjà mentionné, CICS/ESA, TSO et IMS/ESA sont des exemples de produits qui permettent de connecter les utilisateurs finals à DB2 Universal Database for OS/390.
- Si vous utilisez la sécurité au niveau de la session SNA (via le mot clé VERIFY dans l'instruction APPL VTAM de DB2 Universal Database for OS/390), le sous-système de sécurité externe est appelé pour valider l'identité du système éloigné.

Représentation des données

DB2 Universal Database for OS/390 est livré avec un ID de jeu de caractères codés d'installation dont la valeur par défaut est 500. Cette valeur par défaut n'est probablement *pas* correcte pour votre installation.

Lors de l'installation de DB2 Universal Database for OS/390, vous devez définir le CCSID d'installation en fonction du CCSID des caractères générés et transmis à DB2 Universal Database for OS/390 par les unités d'entrée au niveau de votre site. Ce CCSID est généralement déterminé par la langue nationale utilisée. Si le CCSID d'installation n'est pas correct, la conversion des caractères produira des résultats erronés. Pour connaître la liste des CCSID pris en charge pour chaque pays ou langue nationale, reportez-vous au manuel *DB2 Connect User's Guide*.

Vous devez vous assurer que votre sous-système DB2 Universal Database for OS/390 dispose de la fonction de conversion de chaque CCSID du serveur d'applications en CCSID d'installation du sous-système DB2 Universal Database for OS/390. DB2 Universal Database for OS/390 fournit les tables de conversion pour les combinaisons de CCSID source et cible les plus répandues, mais pas pour toutes les combinaisons possibles. Vous pouvez compléter l'ensemble de tables et de routines de conversion disponibles, si nécessaire. Pour en savoir plus sur la conversion de caractères DB2 pour MVS/ESA, reportez-vous au manuel *DB2 Universal Database for OS/390 Administration Guide*.

Configuration du serveur d'applications

Le support de serveur d'applications de DB2 Universal Database for OS/390 lui permet d'assurer une fonction serveur pour les demandeurs d'application DRDA. Le demandeur d'application connecté à un serveur d'applications DB2 Universal Database for OS/390 peut être :

- un demandeur DB2 Universal Database for OS/390
- DB2 Connect
- DB2 Universal Database Enterprise Edition Version 7 ou DB2 Universal Database Extended - Enterprise Edition avec utilisation du support DB2 Connect
- un demandeur DB2 version 2 pouvant s'exécuter sous AIX, HP-UX, OS/2, Solaris, Windows 3.1, Windows 3.11 pour Workgroups, Windows 95, ou Windows NT ainsi que sous Macintosh, SCO, SGI ou SINIX. DDCS multi-utilisateur version 2.3, DDCS mono-utilisateur version 2.3 et DDCS pour Windows version 2.4 offrent cette fonction
- un demandeur OS/400
- un demandeur DB2 pour VM
- tout produit prenant en charge les protocoles pour demandeur d'application DRDA

Pour n'importe quel demandeur d'application connecté à un serveur d'applications DB2 Universal Database for OS/390, ce dernier prend en charge l'accès à la base de données, comme suit :

- Le demandeur d'application est autorisé à accéder aux tables stockées au niveau du serveur d'applications DB2 Universal Database for OS/390. Le demandeur d'application doit créer un module au niveau du serveur d'applications DB2 Universal Database for OS/390 pour que l'application puisse s'exécuter. Le serveur d'applications DB2 Universal Database for OS/390 utilise le module pour localiser les instructions SQL de l'application au moment de l'exécution.
- Le demandeur d'application peut informer le serveur d'applications DB2 Universal Database for OS/390 que l'accès doit être restreint aux activités en lecture seulement si la connexion serveur-demandeur DRDA ne prend pas en charge le processus de validation en deux phases. Par exemple, un demandeur DDCS V2R3 avec un récepteur CICS informera le serveur d'applications DB2 Universal Database for OS/390 que les mises à jour ne sont pas autorisées.
- Le demandeur d'application peut aussi se voir accorder l'autorisation d'accéder aux tables stockées au niveau d'autres systèmes DB2 Universal Database for OS/390 sur le réseau utilisant l'accès défini par le système. L'accès défini par le système permet au demandeur d'application d'établir des connexions à plusieurs systèmes de bases de données dans une seule unité d'oeuvre.

Définition des données réseau

Pour que le serveur d'applications DB2 Universal Database for OS/390 puisse correctement traiter les demandes de bases de données réparties, vous devez procéder comme suit :

1. Définissez le serveur d'applications sur le gestionnaire de communications local.
2. Définissez chaque destination de serveur secondaire potentiel pour permettre au serveur d'applications DB2 Universal Database for OS/390 de réacheminer les demandes SQL vers leur destination finale.
3. Définissez la sécurité nécessaire.
4. Prévoyez la représentation des données.

Définition du serveur d'applications (SNA)

Pour que le serveur d'applications puisse recevoir des demandes de bases de données réparties, il doit être défini sur le gestionnaire de communications local et avoir une valeur RDB_NAME unique. La présente section traite des connexions SNA. Vous devez effectuer les opérations suivantes pour définir correctement le serveur d'applications :

1. Sélectionnez le nom de LU et le RDB_NAME devant être utilisés par le serveur d'applications DB2 Universal Database for OS/390. Le procédé d'enregistrement de ces noms dans DB2 Universal Database for OS/390 et VTAM est identique à celui décrit à la section «Définition du système local (SNA)» à la page 52. Le RDB_NAME choisi pour DB2 Universal Database for OS/390 doit être fourni à l'ensemble des utilisateurs finals et des demandeurs d'application pour lesquels la connectivité au serveur d'applications est nécessaire.
2. Enregistrez la valeur NETID.LUNAME pour le serveur d'applications DB2 Universal Database for OS/390 avec chaque demandeur d'application requérant l'accès, de sorte que le demandeur d'application puisse acheminer les demandes SNA vers le serveur DB2 Universal Database for OS/390. Il en est ainsi même dans les cas où le demandeur d'application est en mesure d'exécuter un routage de réseau dynamique, car le demandeur d'application doit connaître le NETID.LUNAME avant que le routage de réseau dynamique puisse être utilisé.
3. Fournissez le TPN par défaut de DRDA (X'07F6C4C2') pour chaque demandeur d'application car DB2 Universal Database for OS/390 utilise cette valeur automatiquement.
4. Créez une entrée dans la table de modes VTAM pour chaque nom de mode demandé par un demandeur d'application. Ces entrées décrivent les tailles de RU, la taille de la fenêtre de régulation et la classe de service pour chaque nom de mode.
5. Définissez le nombre maximal de sessions pour les demandeurs d'application qui se connectent au serveur d'applications DB2 Universal Database for OS/390. L'instruction VTAM APPL définit le nombre

maximal de sessions par défaut pour tous les systèmes partenaires. Si vous voulez définir des valeurs par défaut uniques pour un partenaire donné, vous pouvez utiliser la table SYSIBM.LUMODES de la base de données de communications (CDB).

Reportez-vous à la section «Définition de la taille de RU et de la régulation » à la page 69, pour savoir comment visualiser votre réseau VTAM.

6. Créez des entrées dans la base de données de communications DB2 Universal Database for OS/390 afin d'identifier les demandeurs d'application autorisés à se connecter au serveur d'applications DB2 Universal Database for OS/390. Deux approches de base permettent de définir des entrées de base de données de communications pour les demandeurs d'application sur le réseau :

   a. Vous pouvez insérer une ligne dans la table SYSIBM.LUNAMES qui fournit les valeurs par défaut à utiliser pour toute LU ne faisant pas l'objet d'une description particulière dans la base de données de communications (la ligne par défaut contient une valeur à blanc dans la colonne LUNAME). Cette approche vous permet de définir des attributs particuliers pour certaines des LU de votre réseau, tout en définissant des valeurs par défaut pour toutes les autres LU.

      Par exemple, vous pouvez permettre au système DALLAS (autre système DB2 Universal Database for OS/390) d'envoyer des demandes de bases de données réparties déjà vérifiées (LU 6.2 SECURITY=SAME), tout en demandant aux gestionnaires de bases de données d'envoyer des mots de passe. Par ailleurs, vous pouvez ne pas vouloir enregistrer d'entrées dans la base de données de communication de chaque gestionnaire de bases de données, en particulier si ces derniers sont nombreux. La figure 25, illustre comment utiliser la base de données de communications pour spécifier SECURITY=SAME pour le système DALLAS tout en appliquant SECURITY=PGM pour tous les autres demandeurs.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES (' ', ' ', 'C', 'N', 'N', ' ');
```

Figure 25. Définition de valeurs par défaut pour les connexions de demandeurs d'application (SNA)

b. Vous pouvez utiliser la base de données de communications pour accorder des droits à chaque demandeur d'application individuellement sur le réseau, selon l'une des deux méthodes suivantes :

   - N'enregistrez pas de ligne par défaut dans la table SYSIBM.LUNAMES. En l'absence de ligne par défaut (ligne contenant un nom de LU à blanc), DB2 Universal Database for OS/390 requiert une ligne dans la table SYSIBM.LUNAMES contenant le nom de LU de chaque demandeur d'application essayant de se connecter. Si la base de données de communications ne contient pas de ligne correspondante, le demandeur d'application se voit refuser l'accès.
   - Enregistrez une ligne par défaut dans la table SYSIBM.LUNAMES indiquant que l'identification du site émetteur est requise (colonne USERNAMES ayant pour valeur 'I' ou 'B'). Il en résulte que DB2 Universal Database for OS/390 limite l'accès aux demandeurs d'application et utilisateurs finals identifiés dans la table SYSIBM.USERNAMES, comme décrit dans la section «Identification du site émetteur» à la page 83. Il se peut que vous souhaitiez utiliser cette approche si les règles de conversion de nom que vous utilisez requièrent une ligne contenant un nom de LU à blanc dans la table SYSIBM.LUNAMES, mais vous ne voulez pas que DB2 Universal Database for OS/390 utilise cette ligne pour permettre un accès non restreint au serveur d'applications DB2 Universal Database for OS/390.

   Dans la figure 26, aucune ligne ne contient de valeur à blanc dans la colonne LUNAME, par conséquent DB2 Universal Database for OS/390 refuse l'accès à toute LU autre que LUDALLAS ou LUNYC.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', ' ');
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', ' ');
```

Figure 26. Identification de connexions de demandeurs d'application individuelles (SNA)

Définition du serveur d'applications (TCP/IP)

Pour que le serveur d'applications puisse recevoir des demandes de bases de données réparties sur des connexions TCP/IP, il doit être défini sur le sous-système TCP/IP local et avoir une valeur RDB_NAME unique. En outre, le fichier d'amorçage de DB2 Universal Database for OS/390 doit comprendre les paramètres nécessaires, et il se peut que vous deviez effectuer des mises à jour dans la base de données de communications de DB2 Universal Database for OS/390.

1. Pour obtenir des informations sur la configuration de TCP/IP sur le serveur d'applications, reportez-vous au manuel *DB2 for OS/390 Installation Reference*. La configuration du demandeur d'application est décrite dans les manuels *DB2 Connect Enterprise Edition pour OS/2 et Windows - Mise en route* et *DB2 Connect Personal Edition - Mise en route*.
2. Un exemple de définition de fichier d'amorçage est présenté à la figure 18 à la page 60.
3. Aucune mise à jour de la base de données de communications n'est requise si vous n'utilisez que les connexions de bases de données entrantes ; ainsi, si vous souhaitez n'utiliser DB2 Universal Database for OS/390 qu'en tant que serveur, il n'est pas nécessaire de remplir la base de données de communications et les valeurs par défaut peuvent être utilisées. Vous trouverez ci-après un exemple simple de mise à jour de SYSIBM.IPNAMES.

   Si vous souhaitez autoriser les demandes de connexion de base de données entrantes pour les noeuds TCP/IP, vous pouvez utiliser une commande SQL comme celle-ci pour mettre à jour cette table :

   ```
   INSERT INTO SYSIBM.IPNAMES (LINKNAME) VALUES('        ')
   ```

Définition de la sécurité

Lorsqu'un demandeur d'application achemine une demande portant sur une base de données répartie vers le serveur d'applications DB2 Universal Database for OS/390, les critères de sécurité suivants peuvent être pris en compte :

- Identification du site émetteur
- Sélection des noms d'utilisateurs finals
- Paramètres de sécurité réseau
- Sécurité du gestionnaire de bases de données
- Sécurité assurée par un sous-système de sécurité externe

Identification du site émetteur

Lorsqu'un serveur d'applications DB2 Universal Database for OS/390 reçoit un nom d'utilisateur final du demandeur d'application, il peut limiter les noms d'utilisateurs reçus d'un demandeur d'application donné. Cela est rendu possible par l'utilisation de *l'identification du site émetteur*. L'identification du site émetteur permet au serveur d'applications d'indiquer que seuls des partenaires donnés sont autorisés à utiliser un ID utilisateur donné. Par exemple, le serveur d'applications peut limiter JONES à «identification du site émetteur» DALLAS. Si un autre demandeur d'application (différent de DALLAS) tente d'envoyer le nom JONES au serveur d'applications, ce dernier peut rejeter la demande car le nom ne provient pas de l'emplacement réseau correct.

DB2 Universal Database for OS/390 exécute l'identification du site émetteur dans le cadre de la conversion sortante de nom d'utilisateur final, dont vous trouverez la description à la section suivante.

Remarque : L'identification de site entrant et de site émetteur n'est pas effectuée pour les demandes entrantes TCP/IP.

Sélection des noms d'utilisateurs finals

Il se peut que l'ID utilisateur transmis par le demandeur d'application ne soit pas unique dans l'ensemble du réseau SNA. Il se peut que le serveur d'applications DB2 Universal Database for OS/390 ait besoin d'exécuter une conversion de nom entrante pour créer des noms d'utilisateurs finals uniques sur le réseau SNA. De la même manière, le serveur d'applications DB2 Universal Database for OS/390 peut avoir besoin d'effectuer une conversion de nom entrante pour fournir un nom d'utilisateur final unique aux serveurs secondaires impliqués dans l'application (pour plus de détails concernant la conversion entrante de nom d'utilisateur final, reportez-vous à la section «Définition de la sécurité» à la page 70).

La conversion de nom entrante est activée lorsque la définition de la colonne USERNAMES de la table SYSIBM.LUNAMES ou SYSIBM.IPNAMES a pour valeur 'I' (conversion entrante) ou 'B' (conversion entrante et sortante). Lorsque la conversion de nom entrante est active, DB2 Universal Database for OS/390 convertit l'ID utilisateur envoyé par le demandeur d'application et le nom du propriétaire du plan DB2 Universal Database for OS/390 (si le demandeur d'application est un autre système DB2 Universal Database for OS/390).

Si le demandeur d'application envoie un ID utilisateur et un mot de passe dans le verbe APPC ALLOCATE, ceux-ci sont validés avant la conversion de l'ID utilisateur. La colonne PASSWORD dans la table SYSIBM.USERNAMES n'est pas utilisée pour la validation du mot de passe. En revanche, l'ID utilisateur et le mot de passe sont présentés au système de sécurité externe (RACF ou produit équivalent) pour validation.

Lorsque l'ID utilisateur entrant dans le verbe ALLOCATE est vérifié, DB2 Universal Database for OS/390 dispose de sorties d'autorisation qui vous permettent de fournir une liste d'AUTHID secondaires et d'exécuter des contrôles de sécurité supplémentaires. Pour plus de détails, reportez-vous au manuel *DB2 Universal Database for OS/390 Administration Guide*.

Le processus de conversion de nom entrante recherche dans la table SYSIBM.USERNAMES une ligne qui doit correspondre à l'un des modèles illustrés ci-après (TYPE.AUTHID.LINKNAME).

1. I.AUTHID.LINKNAME— Utilisateur final particulier issu d'un demandeur d'application particulier

2. I.AUTHID.espace— Utilisateur final particulier issu de n'importe quel demandeur d'application
3. I.espace.LINKNAME— N'importe quel utilisateur final issu d'un demandeur d'application particulier

Si aucune ligne n'est trouvée, l'accès éloigné est refusé. Si une ligne est trouvée, l'accès éloigné est autorisé et le nom de l'utilisateur final est modifié pour prendre la valeur contenue dans la colonne NEWAUTHID (une valeur NEWAUTHID à blanc indique que le nom reste inchangé). Toutes les vérifications d'autorisation de ressources DB2 Universal Database for OS/390 (par exemple, privilèges de tables SQL) effectuées par DB2 Universal Database for OS/390 sont exécutées sur les noms d'utilisateurs finals convertis plutôt que sur les noms d'utilisateurs originaux.

Lorsqu'un serveur d'applications DB2 Universal Database for OS/390 reçoit un nom d'utilisateur final du demandeur d'application, plusieurs objectifs peuvent être atteints par le biais de la fonction de conversion de nom entrante de DB2 Universal Database for OS/390 :

- Vous pouvez modifier un nom d'utilisateur final pour le rendre unique. Par exemple, les instructions SQL suivantes convertissent le nom d'utilisateur final JONES du demandeur d'application NEWYORK (LUNAME LUNYC) en un nom différent (NYJONES).

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'JONES', 'LUNYC', 'NYJONES', ' ');
```

- Vous pouvez modifier le nom de l'utilisateur final pour que, dans un groupe, tous les utilisateurs soient représentés par un nom unique. Par exemple, vous pouvez représenter tous les utilisateurs du demandeur d'application NEWYORK (LUNAME LUNYC) par le nom d'utilisateur NYUSER. Cela vous permet d'octroyer des privilèges SQL au nom NYUSER et de contrôler l'accès SQL accordé aux utilisateurs de NEWYORK.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
  VALUES ('I', ' ', 'LUNYC', 'NYUSER', ' ');
```

- Vous pouvez limiter le nombre de noms d'utilisateurs finals transmis par un demandeur d'application donné. Le fait d'utiliser la fonction de conversion de nom d'utilisateur final permet d'exécuter l'identification du site émetteur décrite à la section «Identification du site émetteur» à la page 83. Par exemple, les instructions SQL qui suivent admettent

uniquement SMITH et JONES comme noms d'utilisateurs finals du demandeur d'application NEWYORK. Tout autre nom se voit refuser l'accès car il n'est pas mentionné dans la table SYSIBM.USERNAMES.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'SMITH', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('I', 'JONES', 'LUNYC', ' ', ' ');
```

- Vous pouvez restreindre le nombre de demandeurs d'application autorisés à se connecter au serveur d'applications DB2 Universal Database for OS/390. Il s'agit là d'une autre fonction d'identification du site émetteur. Dans l'exemple qui suit, n'importe quel nom d'utilisateur final envoyé par le demandeur d'application NEWYORK (LUNYC) ou CHICAGO (LUCHI) est accepté. D'autres demandeurs d'application se voient refuser l'accès car la ligne par défaut SYSIBM.LUNAMES indique la conversion de nom entrante pour toutes les demandes entrantes.

```
INSERT INTO SYSIBM.LUNAMES
     (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
              MODESELECT, USERNAMES)
VALUES (' ', ' ', 'A', 'N', 'N', 'I');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('I', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.USERNAMES
     (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('I', ' ', 'LUCHI', ' ', ' ');
```

Définition de la sécurité réseau

Pour les connexions SNA, la LU 6.2 offre trois grandes fonctions de sécurité réseau :

- Sécurité au niveau des sessions
- Sécurité au niveau des conversations
- Cryptage

La section «Sécurité réseau» à la page 74, traite de la définition de la sécurité au niveau des sessions et du cryptage avec DB2 Universal Database for OS/390. Le serveur d'applications DB2 Universal Database for OS/390 utilise la sécurité au niveau des sessions et le cryptage exactement de la même manière que le demandeur d'application DB2 Universal Database for OS/390.

Le seul critère de sécurité réseau restant est la sécurité au niveau des conversations SNA. Certains aspects relatifs à la sécurité au niveau des conversations sont uniques pour un serveur d'applications DB2 Universal

Database for OS/390. Le serveur d'applications DB2 Universal Database for OS/390 joue deux rôles distincts dans la sécurité réseau :

- En tant que demandeur auprès de serveurs secondaires, le serveur d'applications DB2 Universal Database for OS/390 est chargé d'émettre des demandes APPC contenant les paramètres de sécurité de niveau conversations SNA requis par les serveurs secondaires. Le serveur d'applications DB2 Universal Database for OS/390 utilise la colonne USERNAMES des tables SYSIBM.LUNAMES et SYSIBM.USERNAMES pour définir les conditions requises pour la sécurité de niveau conversations SNA pour chaque serveur secondaire. Les explications détaillées de ces définitions sont identiques à celles contenues dans la section «Sécurité réseau» à la page 74.
- En tant que serveur pour le demandeur d'application, le serveur d'applications DB2 Universal Database for OS/390 dicte les conditions requises pour la sécurité de niveau conversations SNA pour le demandeur d'application. DB2 Universal Database for OS/390 utilise la colonne USERSECURITY de la table SYSIBM.LUNAMES pour déterminer la sécurité des conversations requises à partir de chaque demandeur d'application sur le réseau. Les valeurs suivantes sont utilisées dans la colonne USERSECURITY :

  C Cette valeur indique que DB2 Universal Database for OS/390 demande au demandeur d'application d'envoyer un ID utilisateur et un mot de passe (LU 6.2 SECURITY=PGM) avec chaque demande portant sur une base de données distribuée. Si la colonne ENCRYPTPSWDS de la table SYSIBM.LUNAMES contient un 'Y', DB2 Universal Database for OS/390 suppose que le mot de passe est dans un format codé RACF (possible uniquement dans le cas d'un demandeur d'application DB2 Universal Database for OS/390). Si la colonne ENCRYPTPSWDS ne contient pas de 'Y', DB2 Universal Database for OS/390 s'attend à trouver le mot de passe dans le format LU 6.2 standard (représentation de caractères EBCDIC). Dans les deux cas, DB2 Universal Database for OS/390 transmet les valeurs correspondant à l'ID utilisateur et au mot de passe au sous-système de sécurité pour validation. Il vous faut un sous-système de sécurité en mesure de vérifier le mot de passe et l'ID utilisateur APPC ; par exemple, RACF a une fonction de vérification des mots de passe et des ID utilisateurs APPC. Si le sous-système de sécurité rejette le couple ID-mot de passe, l'accès à la base de données répartie est refusé.

  Toute autre valeur
  Indique que le demandeur d'application est autorisé à envoyer un ID utilisateur déjà vérifié (LU 6.2 SECURITY=SAME) ou un ID utilisateur et un mot de passe (LU 6.2 SECURITY=PGM). Si un ID utilisateur et un mot de passe sont envoyés, DB2 Universal

Database for OS/390 les traite de la façon décrite précédemment pour la valeur 'C'. Si la demande contient uniquement un ID utilisateur, le sous-système de sécurité est appelé pour authentifier l'utilisateur à moins que la table SYSUSERNAMES ne soit utilisée pour la gestion des ID utilisateur entrants.

En cas de violation de la sécurité, la LU 6.2 exige du serveur d'applications DB2 Universal Database for OS/390 qu'il renvoie un code de détection d'arrêt anormal SNA ('080F6051'X) au demandeur d'application. Dans la mesure où ce code de détection ne décrit pas la cause de l'arrêt anormal, DB2 Universal Database for OS/390 propose deux méthodes permettant d'enregistrer la cause des violations de sécurité répartie :

- Un message DSNL030I est émis, qui fournit la LUWID du demandeur ainsi qu'un code anomalie DB2 décrivant l'arrêt anormal. DSNL030I comprend également le AUTHID, si celui-ci est connu, envoyé à partir de la demande d'application qui a été rejetée.
- Une alerte est enregistrée dans la base de données du moniteur matériel NETVIEW, qui contient les mêmes informations que celles contenues dans le message DSNL030I.

Sécurité du gestionnaire de bases de données

En tant que propriétaire des ressources de base de données, le serveur d'applications DB2 Universal Database for OS/390 contrôle les fonctions de sécurité de base de données pour les objets SQL résidant sur le serveur d'applications DB2 Universal Database for OS/390. L'accès aux objets gérés par DB2 Universal Database for OS/390 est régi par des privilèges octroyés aux utilisateurs par l'administrateur de DB2 Universal Database for OS/390 ou les propriétaires des objets individuels. Les deux classes d'objets de base contrôlées par le serveur d'applications DB2 Universal Database for OS/390 sont les suivantes :

- **Modules**— Les utilisateurs individuels sont autorisés à créer, remplacer et exécuter les modules par le biais de l'instruction GRANT de DB2 Universal Database for OS/390. Lorsqu'un utilisateur final est propriétaire d'un module, il peut automatiquement l'exécuter ou le remplacer. Les autres utilisateurs, quant à eux, doivent se faire accorder spécifiquement le droit d'exécution du module au niveau du serveur d'applications DB2 Universal Database for OS/390, à l'aide de l'instruction GRANT. Les droits USE peuvent être octroyés à des utilisateurs finals ou à PUBLIC, ce qui permet à la totalité des utilisateurs d'exécuter le module.

  Lorsqu'une application est liée à DB2 Universal Database for OS/390, le module contient les instructions SQL contenues dans le programme de l'application. Ces instructions sont classées comme suit :

  SQL statique
  L'instruction SQL et les objets SQL désignés par cette dernière sont connus au moment où l'application est liée à DB2 Universal

Database for OS/390. Le créateur du module doit disposer des droits appropriés pour exécuter chaque instruction SQL statique du module.

Lorsqu'un utilisateur final dispose des droits d'exécution d'un module, il dispose automatiquement des droits lui permettant d'exécuter chaque instruction SQL statique contenue dans le module. Les utilisateurs finals n'ont donc pas besoin d'utiliser les privilèges d'accès aux tables DB2 Universal Database for OS/390 si le module qu'ils exécutent contient uniquement des instructions SQL statiques.

SQL dynamique
Décrit une instruction SQL qui n'est pas connue tant que le programme n'est pas exécuté. En d'autres termes, l'instruction SQL est créée par le programme et liée dynamiquement à DB2 Universal Database for OS/390 à l'aide de l'instruction SQL PREPARE. Lorsqu'un utilisateur final exécute une instruction SQL dynamique, il doit disposer des privilèges d'accès aux tables nécessaires à l'exécution de l'instruction SQL. Dans la mesure où l'instruction SQL est inconnue lors de la création du plan ou du module, le propriétaire du module n'accorde pas automatiquement à l'utilisateur final les droits requis.

- **Objets SQL**— Il s'agit de tables, de vues, de synonymes ou d'alias. Les utilisateurs DB2 Universal Database for OS/390 peuvent se voir accorder plusieurs niveaux de droits pour créer, supprimer, modifier ou lire des objets SQL individuels. Ces droits sont requis pour définir l'accès des instructions SQL statiques ou exécuter les instructions SQL dynamiques.

Lors de la création d'un module, l'option DISABLE/ENABLE vous permet de contrôler les types de connexion DB2 Universal Database for OS/390 en mesure d'exécuter le module. Vous pouvez utiliser les routines d'exit de sécurité RACF et DB2 Universal Database for OS/390 afin de permettre, de manière sélective, aux utilisateurs finals d'utiliser DDF. Vous pouvez utiliser RLF pour définir les limites de temps de traitement pour les définitions d'accès éloigné et les exécutions de SQL dynamiques.

Prenons pour exemple un module DB2 Universal Database for OS/390 appelé MYPKG, et appartenant à JOE. JOE peut permettre à SAL d'exécuter le module à l'aide de l'instruction GRANT USE de DB2 Universal Database for OS/390. Lorsque SAL exécute le module, il se produit ce qui suit :

- DB2 Universal Database for OS/390 vérifie que SAL dispose des droits USE pour le module.
- SAL peut exécuter chaque instruction SQL statique dans le module parce que JOE dispose des privilèges d'accès aux objets SQL pour la création du module.

- Si le module a des instructions SQL dynamiques, SAL doit disposer de ses propres droits d'accès aux tables. Par exemple, SAL ne peut pas exécuter SELECT * FROM JOE.TABLE5 tant qu'elle ne dispose pas des droits d'accès en lecture à JOE.TABLE5.

Sous-système de sécurité

L'utilisation par le serveur d'applications DB2 Universal Database for OS/390 du sous-système de sécurité (RACF ou produit équivalent) dépend de la façon dont vous définissez la fonction de conversion de nom entrante dans la table SYSIBM.LUNAMES :

- Si vous indiquez 'I' ou 'B' pour la colonne USERNAMES, la fonction de conversion de nom entrante est active et DB2 Universal Database for OS/390 suppose que l'administrateur de DB2 Universal Database for OS/390 utilise la conversion de nom entrante pour exécuter une partie de la mise en place de la sécurité. Le sous-système de sécurité externe est appelé uniquement si le demandeur d'application envoie une demande contenant à la fois l'ID utilisateur et le mot de passe (SECURITY=PGM). Il vous faut un sous-système de sécurité en mesure de vérifier le mot de passe et l'ID utilisateur APPC ; par exemple, RACF a une fonction de vérification des mots de passe et des ID utilisateurs APPC.

  Si la demande émanant du demandeur d'application contient uniquement un ID utilisateur (SECURITY=SAME), le système de sécurité externe n'est en aucun cas appelé car les règles de conversion de nom entrante déterminent les utilisateurs qui sont autorisés à se connecter au serveur d'applications DB2 Universal Database for OS/390.
- Si vous indiquez une valeur autre que 'I' ou 'B' pour la colonne USERNAMES, le sous-système de sécurité est vérifié comme suit :
  - Lors de la réception d'une demande de base de données répartie émanant du demandeur d'application, DB2 Universal Database for OS/390 appelle le système de sécurité externe pour valider l'ID de l'utilisateur final (et le mot de passe, le cas échéant).
  - Le système de sécurité externe est appelé pour vérifier que l'utilisateur final est autorisé à se connecter au sous-système DB2 Universal Database for OS/390.
- Dans les deux cas, une sortie d'autorisation est émise pour fournir une liste d'ID autorisation secondaire. Pour plus de détails, reportez-vous au manuel *DB2 Universal Database for OS/390 Administration Guide*.

Représentation des données

Vous devez vous assurer que votre sous-système DB2 Universal Database for OS/390 dispose de la fonction de conversion du CCSID du demandeur d'application en CCSID d'installation du sous-système DB2 Universal Database for OS/390. Reportez-vous à la section «Représentation des données» à la page 78, pour plus de détails.

Chapitre 3. Connexion de DB2 Universal Database pour AS/400 au sein d'un réseau DRDA via SNA

L'OS/400 inclut DB2 Universal Database pour AS/400, le système de gestion de bases de données relationnelles IBM pour les systèmes AS/400.

Le présent chapitre explique la procédure à suivre pour configurer un système AS/400 en vue de sa connexion :

1. depuis des postes de travail DB2 Connect (voir section «Configuration du serveur d'applications» à la page 105), et
2. vers un serveur DB2 Universal Database (voir section «Configuration du demandeur d'application» à la page 94).

Pour plus de détails sur la connexion de deux systèmes AS/400, reportez-vous au manuel *AS/400 Distributed Database Programming*.

DB2 Universal Database pour AS/400 version 4.2 permet désormais de prendre en charge les communications DRDA via TCP/IP. La principale source d'informations sur ce sujet est, là aussi, le manuel *AS/400 Distributed Database Programming*, et, pour un récapitulatif des étapes requises, le «Chapitre 4. Connexion de DB2 Universal Database pour AS/400 au sein d'un réseau DRDA via TCP/IP» à la page 113. Les principes sont les mêmes que ceux décrits dans le présent chapitre, mais les opérations de configuration du réseau sont beaucoup plus simples.

Mise en oeuvre de DB2 Universal Database pour AS/400

Le présent chapitre décrit le mode de prise en charge des systèmes de gestion de bases de données réparties par le système DB2 Universal Database pour AS/400. Le logiciel sous licence OS/400 2.1.1 prenait déjà en charge les unités d'oeuvre éloignées DRDA. OS/400 3.1 prend en charge, en plus, l'unité d'oeuvre répartie DRDA. Cette prise en charge faisant partie intégrante du système d'exploitation OS/400, vous n'avez pas à installer les logiciels sous licence Query Manager et SQL Development Kit de DB2 Universal Database pour AS/400 pour utiliser le support DRDA ou exécuter des programmes contenant des instructions SQL imbriquées.

Configuration du demandeur d'application

La prise en charge des demandeurs d'application DRDA par le système AS/400 fait partie intégrante du système d'exploitation OS/400. Par conséquent, il suffit que ce dernier soit actif pour que cette prise en charge soit assurée. Cela s'applique également à la prise en charge du serveur d'applications dans DB2 Universal Database pour AS/400.

Lorsque DB2 Universal Database pour AS/400 joue le rôle de demandeur d'application, il peut se connecter à tout serveur d'applications prenant en charge le protocole DRDA. Si vous souhaitez que DB2 Universal Database pour AS/400 fournisse un accès à la base de données répartie, vous devez prendre en compte les informations suivantes :

- définition des données réseau
- mise en place d'un système de sécurité
- représentation des données

Définition des données réseau

Le demandeur d'application doit être capable d'accepter un nom de base de données relationnelle et de le convertir en paramètres de réseau. Le système AS/400 utilise le répertoire des bases de données relationnelles pour enregistrer le nom des bases de données relationnelles ainsi que les paramètres réseau correspondants. Ce répertoire permet au demandeur d'application AS/400 de transmettre les données réseau nécessaires à l'établissement de communications dans un réseau de base de données répartie.

La plupart des opérations de traitement exécutées dans un environnement de bases de données réparties nécessitent l'échange de messages avec d'autres sites du réseau. Pour que ces opérations s'exécutent correctement en environnement SNA, vous devez :

- définir le système local pour DB2 Universal Database pour AS/400
- définir le système éloigné pour DB2 Universal Database pour AS/400
- définir les communications pour DB2 Universal Database pour AS/400

Définition du système local pour DB2 Universal Database pour AS/400

Le répertoire des bases de données relationnelles de chaque demandeur d'application doit comporter une entrée correspondant à la base de données relationnelle locale ainsi qu'une entrée pour chaque base de données relationnelle éloignée auquel accède le demandeur d'application. Sur le réseau de base de données répartie, tout système AS/400 qui joue le rôle uniquement de serveur d'applications doit disposer, dans son répertoire de bases de données relationnelles, d'une entrée correspondant à la base de données

relationnelle locale. Pour plus de détails sur le répertoire des bases de données relationnelles, reportez-vous au manuel *AS/400 Distributed Database Programming*.

Pour définir le système local, nommez la base de données locale en ajoutant, dans le répertoire des bases de données relationnelles, une entrée correspondant à un un nom d'emplacement éloigné avec la valeur *LOCAL. Cette opération s'effectue à l'aide de la commande ADDRDBDIRE. L'exemple suivant utilise la commande ADDRDBDIRE, où ROCHESTERDB désigne la base de données du demandeur d'application :

```
ADDRDBDIRE RDB(ROCHESTERDB) RMTLOCNAME(*LOCAL)
```

Pour plus de détails sur le répertoire des bases de données relationnelles, reportez-vous au manuel *AS/400 Distributed Database Programming*.

Remarque : Dans les versions les plus récentes d'OS/400, le nom de la base de données relationnelle locale est créé automatiquement s'il n'existe pas au moment requis. Le nom utilisé est le nom de système figurant dans les attributs réseau.

Définition du système éloigné pour DB2 Universal Database pour AS/400

Le répertoire des bases de données relationnelles de chaque serveur d'applications du réseau de base de données répartie doit comporter une entrée locale ainsi qu'une entrée pour chaque base de données éloignée de chaque demandeur d'application. Pour créer ces entrées, procédez comme suit :

- Définissez les bases de données éloignées pour la base de données locale en ajoutant une entrée correspondant à chacune d'entre elles dans le répertoire des bases de données relationnelles, à l'aide de la commande `ADDRDBDIRE` ou `WRKRDBDIRE`. Pour les communications SNA, les informations que vous pouvez indiquer sont les suivantes :
  - nom de la base de données éloignée
  - nom de l'emplacement éloigné sur lequel réside la base de données
  - nom de l'emplacement local
  - nom du mode utilisé pour l'établissement des communications
  - ID éloigné réseau
  - nom de l'unité utilisée pour les communications
  - nom du programme de transaction de la base de données éloignée

  Dans la plupart des cas, il suffit d'indiquer le nom de la base de données éloignée et le nom d'emplacement éloigné[4] de la base de données. Lorsque

4. Sous OS/400, le «nom d'emplacement» correspond à «nom de LU» en VTAM, et le «nom d'emplacement éloigné», à «nom de LU éloignée ou de partenaire».

seul le nom de l'emplacement éloigné est spécifié, les valeurs par défaut sont utilisées pour les autres paramètres. Le système sélectionne une description d'unité en fonction du nom d'emplacement éloigné.

Si plusieurs descriptions d'unités contiennent le même nom d'emplacement éloigné et qu'une description spécifique est requise, les valeurs indiquées pour le nom d'emplacement local et l'ID éloigné réseau dans l'entrée du répertoire des bases de données relationnelles doivent concorder avec celles figurant dans la description d'unité. La sélection de descriptions d'unités pouvant s'avérer complexe lorsque plusieurs d'entre elles utilisent le même nom d'emplacement éloigné, essayez d'utiliser des noms distincts dans chacune d'elles afin de limiter les risques de confusion. Par défaut, le nom du programme de transaction de la base de données éloignée est celui associé par défaut à DRDA, c'est à dire X'07F6C4C2'.

Les paramètres de communication indiqués dans le répertoire des bases de données relationnelles sont utilisés pour établir une conversation avec le système éloigné.

Pour les connexions TCP/IP (prises en charge dans DB2 Universal Database pour AS/400 version 4.2), seuls le nom de la base de données éloignée, et l'adresse et le port IP associé sont requis. Reportez-vous au manuel «Chapitre 4. Connexion de DB2 Universal Database pour AS/400 au sein d'un réseau DRDA via TCP/IP» à la page 113.

Paramétrage des communications SNA

La présente section décrit comment configurer les communications sur l'AS/400 à l'aide de l'architecture APPN. Le système AS/400 permet également la configuration de communications APPC avancées, mais celles-ci n'offrent pas de support pour l'acheminement des données sur réseau. Une base de données répartie AS/400 peut toutefois fonctionner avec ces deux types de configuration. Pour plus de détails sur les configurations APPC, reportez-vous au manuel *OS/400 Communications Configuration*.

La fonction AnyNet de l'AS/400 permet à des applications APPC de s'exécuter sur un réseau TCP/IP (Transmission Control Protocol/Internet Protocol). Les exemples fournis dans les sections qui suivent incluent DDM (gestion de fichiers éloignés), SNA Distribution Services (services de distribution SNA), Alerts (fonction d'alerte) et 5250 Display Station Pass-Through (fonction passe-système 5250). La configuration de certains paramètres supplémentaires suffit à exécuter ces applications sans modification sur un réseau TCP/IP. Pour indiquer la prise en charge de AnyNet, affectez la valeur *ANYNW au paramètre LINKTYPE de la commande CRTCTLAPPC.

Pour plus de détails sur APPC sur TCP/IP, reportez-vous aux manuels *OS/400 Communications Configuration* et *OS/400 TCP/IP Configuration and Reference*. Le support TCP/IP en natif pour les communications DRDA est fourni dans DB2 Universal Database pour AS/400 version 4.2. Pour plus de détails, reportez-vous au «Chapitre 4. Connexion de DB2 Universal Database pour AS/400 au sein d'un réseau DRDA via TCP/IP» à la page 113.

APPN comporte une fonction de mise en réseau qui permet à l'AS/400 de se connecter à un réseau de systèmes et de le contrôler sans avoir à utiliser le support de mise en réseau traditionnellement fourni par un grand système. Les étapes suivantes vous permettent de configurer un AS/400 pour le support APPN :

1. Définition des attributs de réseau à l'aide de la commande CHGNETA (Modifier les attributs réseau)

   Les attributs de réseau à définir sont les suivants :

   - nom du système local
   - nom du système au sein du réseau APPN
   - ID local du réseau
   - type de noeud
   - nom des serveurs de réseau utilisés par le système AS/400 (si l'AS/400 est un noeud d'extrémité)
   - points de contrôle du réseau (si l'AS/400 est un noeud d'extrémité)

2. Création de la description de la ligne de communication

   La description de la ligne de communication décrit la liaison physique ainsi que le protocole de liaison de données à utiliser entre l'AS/400 et le réseau. Pour la créer, utilisez les commandes suivantes :

   - CRTLINETH (Créer une ligne Ethernet)
   - CRTLINSDLC (Créer une ligne SDLC)
   - CRTLINTRN (Créer une ligne en anneau à jeton)
   - CRTLINX25 (Créer une ligne X.25)

3. Création de descriptions de contrôleur

   Les descriptions de contrôleur décrivent les systèmes adjacents du réseau. Pour indiquer que le support APPN doit être utilisé, spécifiez APPN(*YES) lors de leur création. Les commandes nécessaires à la création des descriptions de contrôleur sont les suivantes :

   - CRTCTLAPPC (Créer un contrôleur APPC),
   - CRTCTLHOST (Créer un contrôleur hôte SNA).

   Si la valeur *YES est affectée au paramètre AUTOCRTCTL dans une description de ligne en anneau à jeton ou Ethernet, une description de

contrôleur est créée automatiquement lorsque le système reçoit une demande de démarrage de session sur une ligne en anneau à jeton ou Ethernet.

4. Création d'une description de classe de service

   Utilisez la description de classe de service pour sélectionner les voies de communication (encore appelées routes ou groupes de transmission) et déterminer la priorité de transmission. Cinq descriptions de classe de service sont fournies par le système :

   #CONNECT
   Classe de service par défaut.

   #BATCH
   Classe de service pour les travaux par lots.

   #BATCHSC
   Semblable à la classe de service BATCH, à la différence qu'une sécurité de liaison de données correspondant au moins à un réseau à commutation de paquets est nécessaire. Dans les réseaux de ce type, les données n'empruntent pas toujours la même voie.

   #INTER
   Classe de service configurée pour les communications interactives.

   #INTERSC
   Semblable à la classe de service INTER, à la différence qu'une sécurité de liaison de données correspondant au moins à un réseau à commutation de paquets est nécessaire.

   Pour créer d'autres descriptions de classe de service, utilisez la commande CRTCOSD.

5. Création d'une description de mode

   La description de mode fournit les caractéristiques des sessions ainsi que le nombre de sessions susceptibles d'être utilisées pour négocier les valeurs autorisées entre l'emplacement local et l'emplacement éloigné. Elle pointe également vers la classe de service utilisée pour la conversation. Plusieurs modes prédéfinis sont livrés avec le système :

   BLANK
   Nom du mode par défaut spécifié dans les attributs réseau à la livraison du système.

   #BATCH
   Mode configuré pour les travaux traités par lots.

   #BATCHSC
   Semblable à BATCH, à la différence qu'une sécurité de liaison de données correspondant au moins à un réseau à commutation de paquets est nécessaire pour la classe de service associée.

#INTER
Mode configuré pour les communications interactives.

#INTERSC
Semblable à INTER, à la différence qu'une sécurité de liaison de données correspondant au moins à un réseau à commutation de paquets est nécessaire pour la classe de service associée.

IBMRDB
Mode configuré pour les communications DRDA.

Pour créer d'autres descriptions de mode, utilisez la commande CRTMODD.

6. Création de descriptions d'unité

   La description d'unité fournit les caractéristiques de la connexion physique entre le système local et le système éloigné. Vous n'avez pas à créer manuellement des descriptions d'unité si l'AS/400 s'exécute avec APPN et en tant qu'unité logique (LU) indépendante. Le système AS/400 crée automatiquement la description d'unité et l'associe à la description de contrôleur appropriée lors de l'établissement de la session. Si l'AS/400 est une LU dépendante, vous devez créer manuellement les descriptions d'unité à l'aide de la commande CRTDEVAPPC. Spécifiez la valeur `APPN(*YES)` dans la description d'unité pour indiquer qu'APPN est utilisé.

7. Création de listes d'emplacements APPN

   Si vous devez ajouter d'autres emplacements locaux (appelés *LU* dans d'autres systèmes) ou définir des caractéristiques spéciales pour des emplacements APPN éloignés, vous devez créer des listes d'emplacements APPN. Le nom d'emplacement local correspond au nom de point de contrôle spécifié dans les attributs réseau. Si vous avez besoin d'emplacements supplémentaires pour l'AS/400, une liste d'emplacements locaux APPN doit être créée. Par exemple, si un emplacement éloigné n'appartient pas au même réseau que celui dont fait partie l'emplacement local, vous devez définir des caractéristiques particulières pour cet emplacement éloigné. Cela suppose la création d'une liste d'emplacements éloignés APPN. La commande CRTCFGL (Créer une liste de configuration) vous permet de définir des listes d'emplacements.

8. Activation des communications.

   Vous pouvez activer les descriptions de communication à l'aide de la commande VRYCFG (Changer l'état de configuration) ou WRKCFGSTS (Gérer l'état de la configuration). Si les descriptions de ligne sont activées, les contrôleurs et les unités appropriés connectés à celles-ci sont aussi activés. La commande WRKCFGSTS permet également de visualiser l'état de chaque connexion.

9. Taille de RU et régulation

   La taille de RU et la régulation sont déterminées en fonction des valeurs spécifiées dans la description de mode. Lors de la création de cette dernière, des valeurs par défaut sont proposées pour ces deux paramètres. Il s'agit d'estimations AS/400 convenant à la plupart des environnements comportant une base de données répartie. Si la valeur par défaut est acceptée pour la taille de RU, le système AS/400 détermine la valeur la plus appropriée à utiliser. Lorsque l'AS/400 communique avec un autre système prenant en charge la régulation adaptative, la valeur spécifiée pour la régulation ne constitue qu'une valeur de départ. La régulation est ajustée par chaque système, en fonction de sa capacité à gérer les données qu'il reçoit. Dans le cas de systèmes ne prenant pas en charge la régulation adaptative, la valeur de la régulation est négociée au démarrage de la session et reste la même pour toute la durée de cette dernière. Pour plus de détails, reportez-vous au manuel *OS/400 Communications Configuration*.

Remarques :

1. La description de contrôleur correspond aux macros d'unité physique NCP/VTAM (Network Control Program and Virtual Telecommunications Access Method).
2. La description d'unité correspond à la macro d'unité logique NCP/VTAM. Elle contient des informations comparables à celles qui sont consignées dans le profil de LU partenaire sous Communications Manager/2 1.1.
3. La description de mode correspond aux tables de modes NCP/VTAM et au profil Mode service de transmission sous Communications Manager.

Pour plus de détails sur la configuration du support de mise en réseau et la gestion des listes d'emplacements, reportez-vous aux manuels *OS/400 Communications Configuration* et *APPN Support*. Pour consulter des exemples illustrant l'utilisation des commandes CL pour la définition des configurations système, reportez-vous au manuel *AS/400 Distributed Database Programming*.

Définition de la sécurité

Lorsqu'un système éloigné exécute des opérations de traitement sur des bases de données réparties en lieu et place d'une application SQL, il doit être capable de répondre aux critères de sécurité du demandeur d'application, du serveur d'applications et du réseau reliant ces derniers entre eux. Ces critères entrent dans une ou plusieurs des catégories suivantes :

- sélection des noms d'utilisateurs finals
- paramètres de sécurité réseau
- sécurité du gestionnaire de bases de données
- sécurité imposée par la sécurité AS/400

Sélection des noms d'utilisateurs finals

Sur les systèmes AS/400, un ID utilisateur de 1 à 10 caractères est affecté à chaque utilisateur final. Cet identificateur doit être distinct pour chacun d'eux au sein d'un même système, mais pas nécessairement au sein du réseau. Il s'agit de l'ID utilisateur transmis au système éloigné lors de l'établissement d'une connexion entre deux bases de données. Pour éviter les conflits entre les ID utilisateur définis sur les différents systèmes du réseau, il est fréquent qu'ils fassent l'objet d'une conversion sortante, avant d'être transmis sur le réseau. Toutefois, le système AS/400 n'offre aucune fonction de conversion sortante permettant la résolution des conflits potentiels sur le serveur. Ces conflits doivent être résolus au niveau du serveur d'applications, sauf si vous utilisez les clauses supplémentaires USER et USING avec l'instruction AS/400 SQL CONNECT. USER est un ID utilisateur reconnu sur le serveur d'applications et USING est le mot de passe correspondant.

Sécurité réseau

Une fois que le demandeur d'application a sélectionné les noms d'utilisateurs finals pour représenter l'application éloignée, il doit fournir les données de sécurité réseau LU 6.2 requises. Il existe trois principales fonctions de sécurité réseau pour les unités logiques LU 6.2 :

- Sécurité au niveau des sessions, définie par le mot clé LOCPWD de la commande CRTDEVAPPC.
- Sécurité au niveau des conversations, définie par le système d'exploitation OS/400.
- Cryptage, non pris en charge par le système d'exploitation OS/400.

La sécurité assurée au niveau des sessions s'effectue par le biais d'une vérification de LU à LU. Une clé est associée à chaque LU et doit concorder avec la clé de la LU éloignée. Vous en spécifiez la valeur à l'aide du mot clé LOCPWD de la commande CRTDEVAPPC.

Dans la mesure où le serveur d'applications est chargé de la gestion des ressources de bases de données, il détermine les fonctions de sécurité réseau requises pour le demandeur d'application. Il revient à l'administrateur de la sécurité AS/400 de vérifier que les contraintes de sécurité imposées par chaque serveur d'applications ne dépassent pas les fonctions prises en charge par le demandeur d'application AS/400.

Les options de sécurité possibles pour les conversations SNA sont les suivantes :

SECURITY=SAME

Cette option est également connue sous le nom de "sécurité déjà vérifiée". Elle suppose que seul l'ID utilisateur d'une application soit transmis au système éloigné. Aucun mot de passe n'est transmis. Dans

les versions antérieures à la version 2.2.0 de l'AS/400, ce niveau de sécurité était le seul qui soit pris en charge par un demandeur d'application AS/400.

SECURITY=PGM
Cette option entraîne la transmission à la fois de l'ID utilisateur et du mot de passe d'un utilisateur au système éloigné pour authentification. Dans les versions antérieures à la version 2.2.0 de l'AS/400, cette option de sécurité n'était pas prise en charge par un demandeur d'application AS/400.

SECURITY=NONE
Cette option n'est pas prise en charge lorsque l'AS/400 est un demandeur d'application.

Sécurité du gestionnaire de bases de données

L'AS/400 ne dispose pas d'un sous-système de sécurité externe. Toutes les procédures de sécurité sont gérées par la fonction de sécurité du système d'exploitation OS/400, comme le décrit la section suivante («Sécurité système»).

Sécurité système

Le système d'exploitation OS/400 assure le contrôle des accès à tous les objets du système (programmes, modules, tables, vues, collections, etc.).

Le demandeur d'application contrôle les accès aux seuls objets résidant sur celui-ci. La sécurité des objets résidant sur le serveur d'applications est assurée par ce dernier, en fonction de l'ID utilisateur qui lui est transmis par le demandeur d'application. Cet ID utilisateur est associé à l'utilisateur du demandeur d'application AS/400 ou à l'ID utilisateur indiqué dans la clause USER de l'instruction SQL CONNECT (par exemple, CONNECT TO nom-bdd USER id-utilisateur USING mot-de-passe).

La sécurité des objets peut être modifiée à l'aide des commandes CL de gestion des droits sur les objets ou des instructions SQL GRANT et REVOKE. Vous disposez notamment des deux commandes CL suivantes : GRTOBJAUT (Octroyer droits sur un objet) et RVKOBJAUT (Révoquer droits sur un objet). Ces commandes peuvent être utilisées pour tout objet du système. Les instructions GRANT et REVOKE, en revanche, ne s'appliquent qu'aux objets SQL : tables, vues et modules. Par conséquent, si vous devez modifier les droits d'accès à d'autres objets (programmes ou collections, par exemple), utilisez les commandes GRTOBJAUT et RVKOBJAUT.

Affectation et révocation de droits : Utilisez la commande suivante sur un système AS/400 pour octroyer à l'utilisateur UTIL1 les droits *USE sur le programme PGMA :

```
GRTOBJAUT OBJ(PGMA) OBJTYPE(*PGM) USER(UTIL1) AUT(*USE)
```

La commande permettant de révoquer ces mêmes droits est la suivante :

```
RVKOBJAUT OBJ(PGMA) OBJTYPE(*PGM) USER(UTIL1) AUT(*USE)
```

*PGM indique que l'objet est le type programme. *SQLPKG, *LIB et *FILE sont utilisés respectivement pour un module, une collection et une table.

Les commandes GRTOBJAUT et RVKOBJAUT peuvent également être utilisées pour empêcher les utilisateurs de créer des programmes et des modules. En cas de révocation du droit sur une quelconque commande CRTSQLxxx (où xxx = RPG, C, CBL, FTN ou PLI), l'utilisateur perd la possibilité de créer des programmes. Si la révocation porte sur la commande CRTSQLPKG, il devient impossible à l'utilisateur de créer des modules à partir du demandeur d'application ou sur le serveur d'applications.

Par exemple, entrez la commande suivante sur le système AS/400 pour octroyer à l'utilisateur UTIL1 le droit *USE sur la commande CRTSQLPKG :

```
GRTOBJAUT OBJ(CRTSQLPKG) OBJTYPE(*CMD) USER(UTIL1) AUT(*USE)
```

Cette commande permet à l'utilisateur d'exécuter la commande crtsqlpkg sur le demandeur d'application. Sur le serveur d'applications, elle lui permet créer des modules.

La commande permettant de révoquer le même droit est la suivante :

```
RVKOBJAUT OBJ(CRTSQLPKG) OBJTYPE(*CMD) USER(UTIL1) AUT(*USE)
```

Affectation des droits par défaut : Lorsque des objets sont créés, les utilisateurs se voient octroyer des droits d'accès par défaut à ces derniers : le créateur d'une table, d'une vue ou d'un programme dispose de tous les droits sur ces objets, tandis que les autres utilisateurs se voient octroyer les mêmes droits que ceux dont ils disposent sur la bibliothèque ou la collection dans laquelle ces objets sont créés.

Pour plus de détails sur la sécurité système, reportez-vous au manuel *AS/400 Security - Reference*.

Représentation des données

Les produits prenant en charge l'architecture DRDA effectuent automatiquement les opérations de conversion requises sur le système récepteur. Il est toutefois nécessaire que le CCSID (ID de jeu de caractères codés) du demandeur d'application soit reconnu par le système récepteur.

Sur un demandeur d'application, prêtez attention au CCSID associé aux éléments suivants :

- Travail demandeur

La fonction de support de gestion de travaux OS/400 affecte au CCSID d'un travail la valeur du CCSID figurant dans le profil utilisateur. Si cette valeur est *SYSVAL, la fonction de support de gestion extrait le CCSID à partir de la valeur système QCCSID (fixée initialement à 65535). Si 65535 est affecté au CCSID de travaux portant sur la connexion à partir de DB2 Universal Database, les tentatives de connexion n'aboutissent pas. Modifier la valeur système QCCSID aurait une incidence sur l'ensemble du système. Il est donc recommandé de modifier le CCSID du profil utilisateur pour le travail qui est à l'origine du travail de serveur, en affectant à cet CCSID la valeur appropriée (par exemple, 37 pour l'anglais américain). En règle générale, il est judicieux d'utiliser le CCSID de l'AS/400 auquel vous vous connectez.

Le CCSID d'un travail peut être modifié à l'aide de la commande CHGJOB (Modifier un travail). Si la modification doit également porter sur les travaux suivants, utilisez la commande CHGUSRPRF (Modifier un profil utilisateur) pour modifier la valeur du CCSID dans le profil utilisateur. Pour connaître le CCSID en cours pour un travail, utilisez dans un programme CL la commande RTVJOBA (Extraire attributs du travail). En mode interactif, exécutez pour ce faire la commande WRKJOB (Gérer un travail), puis sélectionnez l'option 2 (Attributs de définition).

- Fichiers physiques de base de données

  Par défaut, le CCSID d'un fichier physique de base de données est le même que celui attribué par défaut au travail lors de sa création (et qui peut être différent du CCSID en cours). Ceci ne s'applique pas si un CCSID a été explicitement indiqué dans la commande CRTPF (Créer un fichier physique) ou CRTSRCPF (Créer un fichier source). Avant DB2 pour l'AS/400 V3R1, le CCSID du travail représentait la valeur par défaut, soit 65535, inadapté pour l'architecture DRDA. Le CCSID de travail par défaut n'est plus 65535 et est donc approprié pour les fichiers physiques auxquels l'accès s'effectue via DRDA.

  Vous pouvez utiliser la commande DSPFD (Afficher description fichier) pour visualiser le CCSID d'un fichier ou la commande DSPFFD (Afficher description des zones) pour connaître le CCSID des zones d'un fichier.

  Utilisez la commande CHGPF (Modifier un fichier physique) pour modifier le CCSID d'un fichier physique. Les fichiers physiques ne sont pas nécessairement modifiables si une ou plusieurs des conditions suivantes sont remplies :

  – Les fichiers logiques sont définis à partir des fichiers physiques. Dans ce cas, vous devrez peut-être effectuer les opérations suivantes :

    1. Sauvegardez les fichiers logiques et physiques ainsi que leurs chemins d'accès respectifs.
    2. Imprimez la liste des droits sur les fichiers logiques (DSPOBJAUT).
    3. Supprimez les fichiers logiques.

4. Modifiez les fichiers physiques.
5. Restaurez les fichiers physiques et logiques ainsi que leurs chemins d'accès sur les fichiers physiques modifiés.
6. Redéfinissez les droits sur les fichiers logiques (Cf. liste imprimée).

– Un CCSID est explicitement affecté aux fichiers ou aux zones. Pour modifier un fichier pour lequel le CCSID est défini au niveau des zones, créez un nouveau fichier physique et copiez les données dans ce dernier à l'aide de la commande CPYF (Copier un fichier) associée au paramètre FMTOPT(*MAP).
– Les formats d'enregistrement sont partagés dans une version de l'OS/400 antérieure à la V3R1.

Configuration du serveur d'applications

Le support pour serveur d'applications disponible sur le système AS/400 lui permet de jouer le rôle d'un serveur pour les demandeurs d'application DRDA. Le demandeur d'application connecté à un serveur d'applications DB2 Universal Database pour AS/400 peut être n'importe quel client prenant en charge les protocoles DRDA.

Le demandeur d'application est autorisé à accéder aux tables stockées en local sur le serveur d'applications DB2 Universal Database pour AS/400. Il doit créer un module sur ce dernier avant qu'une instruction SQL ne puisse être exécutée. Le serveur d'applications DB2 Universal Database pour AS/400 utilise le module contenant les instructions SQL de l'application au moment de l'exécution du programme.

Définition des données réseau

Pour pouvoir traiter les demandes de base de données répartie sur le serveur d'applications AS/400, vous devez définir le nom de la base de données du serveur d'applications dans le répertoire des bases de données relationnelles. Pour les communications SNA, vous devez définir le système de serveur d'applications, ainsi que les tailles de RU et la régulation. Pour les communication TCP/IP prises en charge depuis DB2 Universal Database pour AS/400 version 4.2, reportez-vous au «Chapitre 4. Connexion de DB2 Universal Database pour AS/400 au sein d'un réseau DRDA via TCP/IP» à la page 113.

Définition du nom de la base de données du serveur d'applications

L'identification de la base de données du serveur d'applications (sur ce dernier) s'effectue de la même façon que pour la base de données du demandeur d'application (sur celui-ci). A l'aide de la commande ADDRDBDIRE (Ajouter poste répertoire RDB), indiquez *LOCAL comme nom d'emplacement éloigné.

Définition du serveur d'applications sur le réseau

Pour un accès via SNA, la définition du serveur d'applications sur le réseau est identique à la définition du demandeur d'application sur le réseau. Vous devez créer des descriptions appropriées de ligne, de contrôleurs, d'unités et de mode afin de définir à la fois le serveur d'applications et le demandeur d'application émetteur des demandes. Pour plus de détails sur la définition du serveur d'application, reportez-vous aux sections «Définition du système local pour DB2 Universal Database pour AS/400» à la page 94, et «Définition du système éloigné pour DB2 Universal Database pour AS/400» à la page 95. Consultez également le manuel *AS/400 Distributed Database Programming*.

Le programme de transaction utilisé pour démarrer une base de données du serveur d'applications AS/400 porte le nom DRDA par défaut X'07F6C4C2'. Ce nom de programme de transaction est défini dans le système AS/400 pour démarrer le serveur d'applications. Le port est le paramètre correspondant pour les connexions TCP/IP (lorsque DB2/400 prend en charge ce protocole). DB2/400 utilise toujours en tant que serveur le port identifié 446 DRDA.

Définition de la taille de RU et de la régulation

Vous devez passer en revue les définitions réseau pour déterminer si le réseau de bases de données réparties affecte le réseau existant. Les points à prendre en compte sont les mêmes pour le serveur d'applications et le demandeur d'application.

Définition de la sécurité

Lorsqu'un demandeur d'application achemine une requête portant sur une base de données répartie vers le serveur d'applications AS/400, les critères de sécurité suivants peuvent être pris en compte :

- sélection des noms d'utilisateurs finals
- paramètres de sécurité réseau
- sécurité du gestionnaire de bases de données
- sécurité AS/400

Sélection des noms d'utilisateurs finals

Le demandeur d'application transmet un ID utilisateur au serveur d'applications pour permettre le contrôle des droits d'accès. Le travail exécuté sur le serveur d'applications AS/400 emploie cet ID utilisateur ou, dans certaines circonstances, un ID utilisateur par défaut.

Le serveur d'applications AS/400 n'assure pas de conversion d'ID utilisateur entrante pour résoudre les conflits éventuels entre les ID utilisateur qui ne sont pas uniques au sein du réseau, ni pour regrouper plusieurs utilisateurs sous un même identificateur. Chaque ID utilisateur envoyé par un demandeur d'application doit être reconnu sur le serveur d'applications. Une technique de regroupement des requêtes entrantes sous un même ID utilisateur, avec perte partielle de sécurité, consiste à spécifier un ID utilisateur par défaut dans une

entrée du sous-système de communication qui gère les demandes de démarrage de travaux éloignés. Reportez-vous aux descriptions des commandes ADDCMNE et CHGCMNE dans le manuel *AS/400 CL Reference*.

Sécurité réseau SNA

Il existe trois principales fonctions de sécurité réseau pour les unités logiques LU 6.2 :

- sécurité au niveau des sessions
- sécurité au niveau des conversations
- cryptage (non pris en charge par le système AS/400)

Le serveur d'applications DB2 Universal Database pour AS/400 utilise la sécurité au niveau des sessions, exactement comme le demandeur d'application DB2 Universal Database pour AS/400.

Le serveur d'applications contrôle les niveaux de sécurité SNA utilisés pour les conversations. Le paramètre SECURELOC de la description d'unité APPC ou la valeur de sécurité indiquée dans la liste d'emplacements éloignés APPN détermine les éléments acceptés en provenance du demandeur d'application lors d'une conversation.

Les options possibles pour les conversations SNA sont les suivantes :

SECURITY=SAME
: Egalement connue sous le nom de "sécurité déjà vérifiée", cette option implique que seul l'ID utilisateur est requis par le serveur d'applications. Aucun mot de passe n'est transmis. Utilisez ce niveau de sécurité sur le serveur d'applications en attribuant la valeur *YES au paramètre SECURELOC dans la description d'unité APPC ou au paramètre d'emplacement protégé dans la liste d'emplacements éloignés APPN.

SECURITY=PGM
: Cette option implique qu'à la fois l'ID utilisateur et le mot de passe sont requis par le serveur d'applications. Utilisez ce niveau de sécurité sur le serveur d'applications en attribuant la valeur *NONE au paramètre SECURELOC dans la description d'unité APPC ou la valeur *NO au paramètre d'emplacement protégé.

SECURITY=NONE
: Aucun ID utilisateur ni mot de passe n'est requis par le serveur d'applications. La conversation peut s'effectuer à l'aide d'un profil utilisateur par défaut sur le serveur d'applications. Pour utiliser cette option, indiquez un profil utilisateur par défaut dans le répertoire des communications du sous-système et attribuez la valeur *NO au paramètre SECURELOC ou au paramètre d'emplacement protégé.

Les services SNADS nécessitent la définition d'un ID utilisateur par défaut. Ils doivent donc disposer de leur propre sous-système si vous n'utilisez pas d'ID utilisateur par défaut pour les applications DRDA.

Reportez-vous à la section «Sélection des noms d'utilisateurs finals» à la page 106, pour connaître l'une des techniques de regroupement des demandes de démarrage de travaux entrantes sous un même ID utilisateur. Cette technique n'entraîne pas la vérification de l'ID utilisateur transmis par le demandeur d'application. Le démarrage du travail sur le serveur d'applications s'effectue sous l'ID utilisateur par défaut et l'utilisateur qui a demandé la connexion à partir du serveur d'application peut accéder à ce dernier même si son ID utilisateur dispose de droits restreints. Pour que cela soit possible, le serveur d'applications doit être défini comme un emplacement non protégé, un ID utilisateur par défaut doit être spécifié dans le répertoire de communications du sous-système AS/400 et le demandeur d'application doit être configuré pour transmettre uniquement un ID utilisateur lors du traitement de la connexion. Si un mot de passe est transmis, l'ID utilisateur qui l'accompagne est utilisé à la place de l'ID utilisateur par défaut.

Les entrées du répertoire de communications du sous-système AS/400 se distinguent en fonction de l'unité et du nom de mode utilisés pour démarrer la conversation. Si vous affectez un ID utilisateur par défaut distinct aux différentes combinaisons unité/mode, les utilisateurs peuvent être regroupés en fonction du mode de communication avec le serveur d'applications.

Le système AS/400 offre également une fonction de sécurité réseau utilisée uniquement pour la gestion des bases de données et des fichiers répartis. Il existe un attribut réseau pour l'accès à ces types de systèmes qui entraîne le rejet de toutes les tentatives d'accès ou bien qui autorise un contrôle objet-par-objet de la sécurité par le système.

Sécurité réseau TCP/IP

DB2 Universal Database pour AS/400 version 4.2 comporte une nouvelle commande appelée CRTDDMTCPA. Elle vous permet d'indiquer si un serveur accepte ou non les demandes de connexion TCP/IP sans mot de passe.

Sécurité du gestionnaire de bases de données

Toutes les procédures de sécurité sont gérées par la fonction de sécurité du système d'exploitation OS/400.

Sécurité système

L'AS/400 ne dispose pas d'un sous-système de sécurité externe. La gestion de la sécurité est assurée dans son ensemble par la fonction de sécurité de l'OS/400, qui fait partie intégrante du système d'exploitation. Ce dernier contrôle les droits d'accès sur tous les objets présents sur le système (programmes, modules, tables, vues et collections).

Le serveur d'applications contrôle les accès aux objets résidant sur ce dernier. Ce contrôle s'effectue en fonction de l'ID utilisateur qui démarre le travail sur le serveur d'applications. La section «Sélection des noms d'utilisateurs finals» à la page 106, décrit comment cet ID utilisateur est déterminé.

La sécurité des accès aux objets peut être gérée à l'aide des commandes CL de gestion des droits sur les objets et des instructions SQL GRANT et REVOKE. Il s'agit des commandes CL GRTOBJAUT (Octroyer droits sur un objet) et RVKOBJAUT (Révoquer droits sur un objet), que vous pouvez utiliser pour tout objet résidant sur le système. Les instructions GRANT et REVOKE, en revanche, ne s'appliquent qu'aux objets SQL : tables, vues et modules. Par conséquent, si vous devez modifier les droits d'accès à d'autres objets que ces derniers (à des programmes ou des collections, par exemple), utilisez les commandes GRTOBJAUT et RVKOBJAUT.

Lorsque des objets sont créés sur le système, les utilisateurs se voient octroyer des droits d'accès par défaut à ces derniers : le créateur d'une table, d'une vue ou d'un module reçoit tous les droits sur cet objet, tandis que le public (c'est-à-dire tous les autres ID utilisateur) se voit octroyer les mêmes droits que ceux dont il dispose sur la collection ou la bibliothèque dans laquelle l'objet est créé.

Les droits sur les objets auxquels font référence les instructions statiques ou dynamiques d'un module sont vérifiés au moment de l'exécution de ce module. Si le créateur du module ne dispose pas d'un droit d'accès aux objets référencés, des messages d'avertissement sont renvoyés lorsque le module est créé. Au moment de l'exécution, l'utilisateur qui exécute le module prend les mêmes droits d'accès que le créateur du module. Si ce dernier est autorisé à accéder à une table mais que l'utilisateur qui exécute le module ne l'est pas, il reçoit le même droit que le créateur du module sur la table et peut donc utiliser cette dernière.

Pour plus de détails sur la sécurité système, reportez-vous au manuel *AS/400 Security - Reference*.

Représentation des données

Les produits prenant en charge l'architecture DRDA effectuent automatiquement les opérations de conversion requises sur le serveur d'applications. Pour que cela soit possible, il est toutefois nécessaire que le CCSID du serveur d'applications soit convertible par le demandeur d'application.

Sur un serveur d'applications, prêtez attention au CCSID associé aux éléments suivants :

- Travail serveur dans le sous-système de communication

Le CCSID du travail serveur doit être compatible avec le demandeur d'application. Il est établi en fonction du profil de l'utilisateur qui a émis la demande de connexion. La fonction de support de gestion de travaux OS/400 affecte au CCSID d'un travail la valeur figurant dans le profil utilisateur. Si ce dernier n'en contient pas, la valeur système est utilisée comme CCSID (QCCSID) (fixée initialement à 65535).

Avant de soumettre une demande à DB2 Universal Database pour AS/400, vous devez ouvrir une session et, à l'aide de la commande CHGUSRPRF (Modifier un profil utilisateur), attribuer une valeur de CCSID admise au profil utilisateur du travail qui sera utilisé pour les demandes DRDA.

- Collections SQL

  Une collection SQL est constituée d'un objet bibliothèque OS/400, d'un journal, d'un récepteur de journal et, facultativement, d'un dictionnaire de données IDDU si la clause WITH DATA DICTIONARY est spécifiée dans l'instruction CREATE COLLECTION. Les fichiers physiques et logiques utilisés pour certains de ces objets prennent par défaut le CCSID du travail au moment de la création de ce dernier. Si vous interrogez le dictionnaire de données ou le catalogue à partir d'un demandeur d'application ne prenant pas en charge le CCSID de ces fichiers, vous risquez d'obtenir des données non affichables ou déformées. Il est possible également que le demandeur d'application émette un message indiquant que le CCSID n'est pas pris en charge. Pour remédier à cela, vous devez créer une nouvelle collection SQL avec un CCSID de travail acceptable par d'autres systèmes.

  Le CCSID d'un travail peut être modifié à l'aide de la commande CHGJOB (Modifier un travail). Si la modification doit également porter sur les travaux suivants, utilisez la commande CHGUSRPRF (Modifier un profil utilisateur) pour modifier le CCSID défini dans le profil utilisateur. Dans un programme CL, utilisez la commande RTVJOBA (Extraire attributs du travail) pour connaître le CCSID du travail en cours. En mode interactif, exécutez pour ce faire la commande WRKJOB (Gérer un travail), puis sélectionnez l'option 2 (Attributs de définition).

- Tables SQL et autres fichiers DB2 Universal Database pour AS/400 accessibles via DRDA

  Une table SQL correspond à un fichier physique DB2 Universal Database pour AS/400 contenu dans une bibliothèque portant le même nom que la collection. Les colonnes d'une table correspondent également aux définitions des zones d'un fichier physique. Le CCSID de la table ou des colonnes de cette dernière peut être incompatible avec le demandeur d'application. Pour modifier cette valeur, reportez-vous à la section «Représentation des données» à la page 103, qui explique comment modifier les fichiers physiques de base de données. Dans les versions antérieures à OS/400 3.1, les incompatibilités de CCSID étaient principalement liées à l'affectation par défaut du CCSID 65535 à de nombreux fichiers ou tables

SQL. Dans la version 3.1 et suivantes, les CCSID de ces fichiers sont modifiés automatiquement, de sorte qu'une valeur plus appropriée leur soit affectée.

Chapitre 4. Connexion de DB2 Universal Database pour AS/400 au sein d'un réseau DRDA via TCP/IP

Le présent chapitre contient un résumé des informations fournies dans le manuel *AS/400 Distributed Database Programming*, expliquant comment configurer un système AS/400 :

- en tant que demandeur d'application DRDA utilisant des communications TCP/IP sortantes ;
- en tant que serveur d'applications DRDA utilisant des communications TCP/IP entrantes.

Les principes sont les mêmes que ceux décrits au «Chapitre 3. Connexion de DB2 Universal Database pour AS/400 au sein d'un réseau DRDA via SNA» à la page 93, mais les opérations de configuration du réseau sont beaucoup plus simples.

Remarques :

1. Pour les communications DRDA via TCP/IP, le numéro de port par défaut associé aux connexions des bases de données est 446.
2. La mise en oeuvre de DB2 Universal Database pour AS/400 version 4 édition 2 ne permet pas d'appliquer la validation en deux phases (unité d'oeuvre répartie) à des communications TCP/IP.

Récapitulatif des informations DB2 Universal Database pour AS/400

Voici la liste des sections contenues dans le manuel *AS/400 Distributed Database Programming*, à lire et auxquelles vous référer :

- Chapitre 1. Distributed Relational Database and the AS/400 System (les bases de données relationnelles réparties et l'AS/400) :
  - Distributed relational Database Processing (Traitement des bases de données relationnelles réparties)
  - DRDA and CDRA Support (Support DRDA et CDRA)
- Chapitre 3. Communications for an AS/400 Distributed Relational Database (Les communications d'une base de données relationnelle répartie AS/400) :
  - Configuring a Communications Network using TCP/IP (Configuration d'un réseau de communications via TCP/IP)
- Chapitre 4. Security for an AS/400 Distributed Relational Database (La sécurité d'une base de données relationnelle répartie AS/400) :
  - DRDA Security using TCP/IP (La sécurité DRDA via TCP/IP)

- Chapitre 5. Setting Up an AS/400 Distributed Relational Database (Configuration d'une base de données relationnelle répartie AS/400) :
  - Work Management for DRDA Use with TCP/IP (Gestion du travail pour l'utilisation de DRDA avec TCP/IP)
  - Setting up the TCP/IP Server (Configuration du serveur TCP/IP)
- Chapitre 6. Distributed Relational Database Administration and Operation Tasks (Administration et fonctionnement d'une base de données relationnelle répartie) :
  - Managing a TCP/IP Server (Gestion d'un serveur TCP/IP)
- Chapitre 8. Distributed Relational Database Performance (Les performances d'une base de données relationnelle répartie) :
  - Factors that Affect Blocking for DRDA (Facteurs affectant le groupage lié à DRDA)
- Chapitre 9. Handling Distributed Relational Database Problems (Traitement des problèmes des bases de données relationnelles réparties) :
  - Handling Connection Request Failures for TCP/IP (Résolution des échecs de demandes de connexion à TCP/IP)
  - Starting a Service Job for a TCP/IP Server (Lancement d'un travail de maintenance pour un serveur TCP/IP)
- Annexe B. Cross-Platform Access Using DRDA (Accès inter-plateforme via DRDA).

Par ailleurs, vous devez connaître :

- le numéro de port et le nom hôte TCP/IP associés au serveur et au demandeur ;
- le CCSID et la page de codes associés au serveur et au demandeur ;
- l'ID utilisateur et le mot de passe requis lors de l'établissement des connexions aux bases de données.

Remarques sur la configuration et l'utilisation du serveur TCP/IP DRDA DB2 Universal Database pour AS/400

Lors de la configuration du serveur TCP/IP DRDA DB2 Universal Database pour AS/400, il faut vérifier avant toute chose que le serveur a bien été démarré. La commande CL permettant de lancer le serveur DRDA (également appelé serveur DDM) est la suivante :

```
STRTCPSVR SERVER(*DDM)
```

Le serveur DRDA peut également être lancé à l'aide de la commande TCP/IP Server (STRTCPSVR) utilisée seule ou avec la valeur *ALL affectée au paramètre SERVER. Le serveur DRDA démarrera automatiquement lors du lancement de TCP/IP si la commande CL suivante a été émise :

```
CHGDDMTCPA AUTOSTART(*YES)
```

La commande CL suivante permet de vérifier que le démarrage du serveur a abouti :

```
WRKUSRJOB USER(QUSER) STATUS(*ACTIVE)
```

Cette commande affiche une liste de travaux. Si vous la faites défiler d'environ une page, vous verrez apparaître deux lignes contenant les informations suivantes :

```
__   QRWTLSTN    QUSER       BATCH    ACTIVE
__   QRWTSRVR    QUSER       PJ       ACTIVE
```

(Il peut y avoir plusieurs occurrences de la ligne QRWTSRVR, selon le nombre de travaux de prédémarrage du serveur PRESTART actifs.)

Si la ligne QRWTLSTN s'affiche, cela signifie que le travail à l'écoute des demandes de connexions DRDA et DDM est actif. Ce travail répartit l'activité entre les travaux QRWTSRVR à mesure de la réception des demandes de connexion.

L'autre mode de vérification du démarrage du serveur DRDA consiste à émettre la commande STRTCPSVR SERVER(*DDM) et à rechercher le message 'DDM TCP/IP server already active' dans le résultat obtenu.

Le nom du travail de pré-démarrage utilisé pour une connexion particulière peut être obtenu en lançant une commande DSPLOG semblable à la suivante :

```
DSPLOG PERIOD(('15:55'))
```

où l'heure indiquée est antérieure à celle de l'établissement de la connexion. Vous obtenez ainsi une liste des entrées de l'historique, que vous pouvez faire défiler. Recherchez une entrée semblable à la suivante, qui contiendra le nom du travail serveur :

```
DDM job 039554/QUSER/QRWTSRVR servicing user SRR on 03/30/98 at 15:57:38.
```

Ce nom de travail est utile pour consulter le journal associé aux travaux actifs. Il permet également de démarrer une activité de surveillance sur des travaux encore actifs à des fins d'identification d'incident ou de visualisation des messages provenant de l'optimiseur de requêtes. Voici un exemple de

commande CL permettant de lancer une activité de surveillance en utilisant les informations mentionnées précédemment :

```
STRSRVJOB 039554/QUSER/QRWTSRVR
```

Pour faire passer le travail faisant l'objet de la surveillance en mode débogage, exécutez la commande STRDBG :

```
STRDBG UPDPROD(*YES)
```

Dans certaines circonstances, le serveur DRDA sauvegarde l'historique des travaux de pré-démarrage avant de recycler le travail et d'effacer le journal. Cela se produit lorsqu'une panne grave est détectée ou que le travail a pris fin pendant l'exécution du service (via la commande STRSRVJOB).

Pour trouver l'historique des travaux sauvegardé à l'issue du travail, lancez la commande suivante :

```
WRKJOB id-utilisateur/QPRTJOB
```

où id-utilisateur est l'ID utilisateur qui a permis d'établir la connexion (SRR dans l'exemple ci-dessus).

Vous obtenez ainsi une liste de travaux à partir de laquelle il est possible d'en sélectionner un, ou une option de menu associée à un travail unique. Sélectionnez l'option 4, 'Work with spooled files' pour rechercher l'historique des travaux sauvegardé. Il s'agit du fichier QPJOBLOG lorsqu'il existe plusieurs fichiers placés en file d'attente. L'option 5 permet d'afficher le fichier historique des travaux.

Exemple de messages émanant de l'optimiseur de requêtes susceptibles d'apparaître dans l'historique des travaux d'un serveur, lorsqu'un travail a été exécuté en mode débogage :

```
     CPI4329    Information   00    03/30/98   16:14:57   QQQIMPLE
               QSYS        3911     QSQOPEN      QSYS         09C4
  Message . . . . :   Arrival sequence access was used for file TBL2.
  Cause . . . . . :   Arrival sequence access was used to select
    records from member TBL2 of file TBL2 in library SR. If file TBL2
    in library SR is a logical file then member TBL2 of physical file
    TBL2 in library SR is the actual file from which records are
    being selected. A file name of *N for the file indicates it is a
    temporary file. Recovery  . . . :   The use of an access path may
    improve the performance of the query if record selection is
    specified. If an access path does not exist, you may want to
    create one whose left-most key fields match fields in the record
    selection.  Matching more key fields in the access path with
    fields in the record selection will result in improved
    performance. Generally, to force the use of an existing access
    path, specify order by fields that match the left-most key fields
    of that access path. For more information refer to the DB2 for
    AS/400 SQL Programming book.
```

Remarques sur la configuration du client TCP/IP DRDA DB2 Universal Database pour AS/400

En dehors des considérations de sécurité traitées dans la section suivante, lorsque vous utilisez DB2 Universal Database pour AS/400 en tant que demandeur d'application via TCP/IP, vous devez essentiellement veiller à ajouter, dans le répertoire RDB, une entrée correspondant au serveur d'applications éloigné. Cette opération est similaire à celle décrite dans le chapitre précédent consacré aux communications SNA. Toutefois, au lieu des paramètres APPC tels que le nom de LU éloignée et le nom du programme transactionnel, vous devez utiliser deux paramètres TCP/IP : nom ou adresse IP de l'hôte éloigné et numéro de port ou nom de service. La deuxième partie du paramètre définissant l'emplacement éloigné peut être *SNA (valeur par défaut) ou *IP (valeur indiquant que la connexion s'établira via TCP/IP).

Remarques sur la sécurité lors de l'utilisation de l'architecture DRDA sur TCP/IP

DRDA sur TCP/IP en natif n'utilise pas les services et principes de sécurité des communications de l'OS/400, tels que les périphériques de communications, les modes, les attributs d'emplacement sécurisé et les niveaux de sécurité des conversations associés aux communications APPC. La configuration de la sécurité de TCP/IP s'effectue donc de manière assez différente.

Il existe deux types de mécanismes de sécurité pris en charge par la mise en oeuvre DB2/400 actuelle de DRDA sur TCP/IP :

1. ID utilisateur seulement
2. ID utilisateur avec mot de passe

Dans le cas d'un serveur d'applications DB2 Universal Database pour AS/400, le mode de sécurité par défaut consiste en l'ID utilisateur avec mot de passe. Lors de l'installation du système, vous devez donc fournir pour les demandes de connexion TCP/IP entrantes un mot de passe avec l'ID utilisateur sous lequel le travail serveur doit s'exécuter. La commande CHGDDMTCPA permet d'autoriser l'absence de mot de passe. Pour effectuer cette modification, entrez CHGDDMTCPA PWDRQD(*NO). Vous devez avoir le droit *IOSYSCFG pour utiliser cette commande.

Dans le cas d'un demandeur d'application DB2 Universal Database pour AS/400 (ou client), vous avez le choix entre deux méthodes pour envoyer un mot de passe avec l'ID utilisateur lors des demandes de connexion TCP/IP. En leur absence, seul un ID utilisateur sera envoyé.

La première méthode d'envoi d'un mot de passe consiste à utiliser la forme USER/USING de l'instruction SQL CONNECT, en respectant la syntaxe suivante :

```
CONNECT TO nom-bdd USER id-utilisateur USING 'mot-de-passe'
```

où les mots en minuscules représentent les paramètres de connexion appropriés. Dans un programme utilisant des instructions SQL imbriquées, les valeurs affectées à l'ID utilisateur et au mot de passe peuvent être contenues dans des variables associées à l'hôte.

La seconde méthode consiste à utiliser une entrée d'autorisation serveur. Une liste d'autorisations serveur est associé à chaque profil utilisateur existant sur le système. Par défaut, cette liste est vide mais vous pouvez y ajouter des entrées par la commande ADDSVRAUTE. Lors d'une tentative de connexion DRDA sur TCP/IP, DB2 Universal Database pour AS/400 vérifie si cette liste contient le profil utilisateur sous lequel le travail client s'exécute. Si le nom de la base de données contenu dans l'instruction CONNECT est identique au nom SERVER dans une entrée autorisation, le paramètre USRID correspondant figurant dans l'entrée est utilisé en tant qu'ID utilisateur de connexion ; par ailleurs, s'il existe également un paramètre PASSWORD dans cette entrée, cette valeur est également envoyée dans la demande de connexion.

Pour que le mot de passe soit sauvegardé par la commande ADDSVRAUTE, le paramètre système QRETSVRSEC doit être défini par la valeur '1', la valeur par défaut étant '0'. Pour procéder à la modification, entrez :

```
CHGSYSVAL QRETSVRSEC VALUE('1')
```

La syntaxe de la commande ADDSVRAUTE est la suivante :

```
ADDSVRAUTE USRPRF(profil-util) SERVER(nom-bdd) USRID(id-utilisateur) PASSWORD(mot-de-passe)
```

Le paramètre USRPRF spécifie le profil utilisateur sous lequel le travail demandeur d'application s'exécute. Le paramètre SERVER indique le nom de la base de données relationnelle éloignée, le paramètre USRID, le profil utilisateur sous lequel le travail serveur s'exécutera, et le paramètre PASSWORD, le mot de passe associé au profil utilisateur existant sur le serveur.

Remarque : Dans le paramètre SERVER, il est essentiel d'indiquer le nom de la base de données relationnelle en majuscules.

Si vous omettez le paramètre USRPRF, le profil utilisateur permettant d'exécuter la commande ADDSVRAUTE sera adopté par défaut ; si vous omettez le paramètre USRID, le profil utilisateur permettant d'exécuter la commande USRPRF sera utilisé par défaut. Si vous omettez le paramètre PASSWORD ou que la valeur QRETSVRSEC est 0, l'entrée ne contiendra

aucun mot de passe et, lors d'une tentative de connexion utilisant l'entrée, le mécanisme de sécurité sera l'ID utilisateur seulement.

Une entrée autorisation serveur peut être supprimée par la commande RMVSVRAUTE, et modifiée par la commande CHGSVRAUTE. Pour une description détaillée de ces commandes, reportez-vous au manuel "AS/400 Command Reference".

Si une entrée autorisation serveur existe pour une base de données relationnelle et que la forme USER/USING de l'instruction CONNECT est utilisée, c'est cette dernière qui est employée en priorité.

Chapitre 5. Informations complémentaires sur les opérations SQL

Le présent chapitre fournit des informations supplémentaires sur les opérations SQL entre DB2 Universal Database pour AS/400 et DB2 Common Server version 2 ou DB2 Universal Database version 5. Il fournit également des informations sur les opérations SQL entre DB2 Universal Database pour AS/400 et DB2 pour OS/2 mais, en règle générale, ces indications s'appliquent également à DB2 Common Server version 2 et DB2 Universal Database version 5 sur d'autres plateformes, comme suit :

1. Sur l'AS/400, les noms de table sont qualifiés par une collection (ou par un nom de bibliothèque) et ils résident dans la base de données DB2 Universal Database pour AS/400 (une par système AS/400). Cependant, sur le PC, une table est qualifiée par l'ID utilisateur qui l'a créée et elle réside dans une base de données particulière (ou dans plusieurs, dans le cas de DB2 pour OS/2).
   a. Cela implique que toute requête envoyée de DB2 pour OS/2 (via DB2 Connect) vers DB2 Universal Database pour AS/400 mentionne l'ID utilisateur du travail cible (qui s'effectue sur l'AS/400) en tant que nom (par défaut) de la collection, si celui-ci ne figure pas dans le nom de la table recherchée. Soyez donc attentif, faute de quoi la table ne pourra être localisée.
   b. Cela implique également que toute requête émise par DB2 Universal Database pour AS/400 vers DB2 pour OS/2 doit être associée à un qualifiant de table implicite, si celui-ci n'est pas explicité dans la requête (au format "qualifiant.nom-table"). Le qualifiant de table pour OS/2 (indiqué en tant que collection ou bibliothèque par le demandeur d'application AS/400) prend par défaut l'ID de l'utilisateur à l'origine de la requête. Là encore, vous devez être attentif, faute de quoi la table ne pourra être localisée.
   c. Vous pouvez attribuer un ID utilisateur commun aux bases de données et tables DB2 pour OS/2 que vous créez. En effet, contrairement à DB2 Universal Database pour AS/400, DB2 pour OS/2 ne comporte pas de collections physiques, mais simplement un qualifiant de table, correspondant à l'ID de l'utilisateur qui crée la base de données.
2. DB2 Connect (ou DDCS) est requis si DB2 pour OS/2 s'exécute comme client utilisant le protocole DRDA ; il ne l'est pas lorsqu'il sert uniquement de serveur.

3. Il est important de configurer DB2 Connect correctement, comme suit :
   a. Assurez-vous que vous disposez des niveaux d'édition les plus récents de DB2 pour OS/2 et de DB2 Connect ; sinon, appliquez les PTF disponibles appropriées.
   b. Suivez les procédures d'installation et de configuration décrites dans les manuels correspondants.
4. Avec APPC, veillez à configurer les communications en conséquence ; un contrôleur et une unité doivent être créés pour le PC si DB2 pour OS/2 sert de demandeur d'application ou de serveur d'applications. De plus, quel que soit le protocole de communication utilisé, le répertoire de bases de données relationnelles doit comporter une entrée pour chaque base de données DB2 pour OS/2 à laquelle un AS/400 peut se connecter.

   Pour configurer les communications APPC, procédez comme suit :
   a. Vous pouvez créer manuellement les descriptions de contrôleur et d'unité, ou bien laisser le système les créer si vous disposez d'un réseau en anneau à jeton et que la valeur *YES est indiquée au paramètre de description de ligne AUTOCRTCLT. Utilisez la commande WRKLIND (Gérer descriptions de lignes), option 2 (Modifier) pour consulter la description de ligne. Localisez le paramètre AUTOCRTCLT (Création automatique de contrôleurs) et notez la valeur qui lui est attribuée.

      Si votre système crée automatiquement les contrôleurs, vous pouvez lancer la création des descriptions de contrôleur requises. Pour ce faire, ouvrez le dossier CM/2 à partir d'OS/2, puis cliquez sur Start Communications et exécutez Subsystem Management. Notez les détails relatifs au sous-système SNA, puis aux liaisons logiques. Ouvrez la fenêtre correspondant à celles-ci afin d'activer la liaison au système sur lequel vous souhaitez créer la description de contrôleur. La description d'unité y sera automatiquement créée, ultérieurement.
   b. Sur l'AS/400, l'unité et le contrôleur associés au PC doivent être actifs pour que la liaison entre les deux systèmes puisse être établie. Si la valeur *NO est affectée au paramètre SWTDSC dans la description de contrôleur, l'état des contrôleurs actifs ne change pas. Par ailleurs, vous pouvez affecter la valeur *YES au paramètre ONLINE. Ainsi, le contrôleur sera activé à l'issue de l'IPL. (Dans ce cas, vous devrez peut-être également attribuer la valeur *YES au paramètre ONLINE également dans la description d'unité.) Pour que vous puissiez modifier des paramètres de description de contrôleur, celle-ci doit être hors fonction et la valeur *USER doit être définie pour le paramètre CTLOWN (propriétaire de contrôleur).
   c. Pour ajouter une entrée au répertoire de bases de données relationnelles pour chaque base de données DB2 pour OS/2 à laquelle un AS/400 peut se connecter, utilisez la commande ADDRDBDIRE, en indiquant le nom de la base de données DB2 pour OS/2 en tant que

nom de base de données relationnelle, et le nom du poste de travail en tant que nom d'emplacement éloigné.

5. La valeur de CCSID appropriée est requise pour les tables (fichiers physiques) sur l'AS/400 utilisé par DB2 pour OS/2. Vous pouvez visualiser la valeur de CCSID à l'aide de la commande DSPFD, et la modifier pour les fichiers physiques, à l'aide de la commande CHGPF. Pour que la connexion aboutisse, vous devrez peut-être modifier, en plus, l'un des éléments suivants : le CCSID du travail, le CCSID du profil utilisateur employé ou le CCSID du système (valeur QCCSID) si la valeur par défaut, 65535, est affectée. En règle générale, il est préférable d'apporter cette modification dans le profil utilisateur sous lequel le travail de serveur sera exécuté.
6. Pour pouvoir utiliser DB2 Connect avec un serveur AS/400, vous devez créer des modules SQL sur l'AS/400 pour les programmes d'applications et les utilitaires DB2 Connect.
   a. Vous pouvez utiliser la commande DB2 PREP pour traiter le fichier source d'un programme d'application comportant des instructions SQL. Ce traitement génère un fichier source modifié contenant des appels de langage hôte qui correspondent aux instructions SQL. Il crée également, par défaut, un module SQL dans la base de données à laquelle vous êtes connecté.
   b. Pour définir les accès des utilitaires DB2 Connect à tout serveur DB2 AS/400, procédez comme suit :

      1)
      ```
      CONNECT TO nom-bdd-éloignée
      ```

      2)
      ```
      BIND chemin@DDCS400.LST BLOCKING ALL SQLERROR CONTINUE
               MESSAGES DDCS400.MGS GRANT PUBLIC
      ```

      Remplacez `chemin` dans `chemin@DDCS400.LST` par le chemin par défaut, `C:\SQLLIB\BND\`, ou par votre emplacement local si le chemin par défaut n'a pas été indiqué lors de l'installation.

      Remarque : La PTF SF23624 est requise pour la version 3 édition 1 de l'OS/400. En effet, elle permet d'éviter la génération du code d'erreur SQL de type -901 à partir de la base de données DB2 Universal Database pour AS/400, au niveau du troisième fichier de liens (*.bnd) dans la liste.

      3)
      ```
      CONNECT RESET
      ```

7. Pour permettre la transmission d'instructions SQL interactives de DB2 Universal Database pour AS/400 à DB2 pour OS/2, procédez comme suit :
   a. Utilisez les attributs de session NAMING(*SQL), DATFMT(*ISO) et TIMFMT(*ISO). D'autres formats que *ISO peuvent être utilisés mais pas tous les formats et la valeur attribuée au format de date (DATFMT) doit également être indiquée au format d'heure (TIMFMT).
   b. Notez la correspondance entre les COLLECTIONS sur l'AS/400 et le qualifieur de table (ID de l'utilisateur ayant créé la table) pour DB2 pour OS/2. Reportez-vous à l'étape 1 ci-avant pour d'autres détails sur les opérations SQL.
   c. Lors de la toute première session interactive, vous DEVEZ également indiquer COMMIT(*CS) pour le contrôle de validation, puis (1) RELEASE ALL, (2) COMMIT et (3) CONNECT TO nomrdb (celui d'une base de données particulière). A ce stade, vous pouvez également associer la valeur PUBLIC au droit d'exécution du module QSQL400.QSQL0200 (GRANT EXECUTE ON PACKAGE QSQL400.QSQL0200 TO PUBLIC) (ou associer ce droit à des utilisateurs particuliers). Ainsi, d'autres personnes pourront utiliser ce module SQL pour transmettre des instructions SQL en interactif.
8. Pour tout programme créé sur un AS/400 qui accède à une base de données DB2 pour OS/2, veillez à utiliser les commandes DB2 pour OS/2 suivantes :
   a.
   ```
   GRANT ALL PRIVILEGES ON TABLE nom-table TO utilisateur
   ```
   b.
   ```
   GRANT EXECUTE ON PACKAGE nom-module (généralement,
     le nom du programme AS/400) TO utilisateur
   ```

   Vous pouvez, si vous le souhaitez, indiquer "PUBLIC" à la place de *utilisateur*.
9. Lors du développement d'applications AS/400 utilisant DB2 pour OS/2 (version 2.1.1 ou antérieure), le message SQL5057 était généré suite à la commande CRTSQLxxx pour indiquer la création d'un module SQL sur le PC, même lorsque ce module n'était pas réellement créé. Désormais, cette erreur ne se produit plus dans DB2 pour OS/2.

   Par ailleurs, dans les versions précédentes de DB2 pour OS/2, aucun module SQL n'était créé pour les programmes OS/400 dont la zone de texte de la description de membre source contenait des données.
10. Dans DB2 pour OS/2, les procédures mémorisées en langage C ne peuvent pas utiliser les paramètres argc et argv, c'est-à-dire qu'elles ne peuvent pas être de type *principal()*, tandis que les procédures mémorisées sur l'AS/400 doivent utiliser ces paramètres. (Reportez-vous aux exemples de procédures mémorisées DB2 pour OS/2 dans le

sous-répertoire \SQLLIB\SAMPLES ; recherchez les fichiers OUTSRV.SQC et OUTCLI.SQC dans le sous-répertoire C.)

11. Indiquez en MAJUSCULES les noms des procédures mémorisées dans DB2 pour OS/2 et appelées par un AS/400, (qui utilise des majuscules pour ces noms). Cela signifie que tout nom de procédure indiqué en minuscules, même correctement, ne sera pas trouvé (pour l'AS/400, ces noms sont toujours en majuscules).
12. Si vous n'appliquez pas la PTF appropriée pour les instructions SQL imbriquées, une instruction CALL d'un AS/400 vers DB2 pour OS/2 ne peut aboutir que si vous indiquez le nom de la procédure dans une variable hôte (CALL:nom-procédure-hôte(...)). La PTF requise pour la V3R7 est SF35932, et pour la V3R2, SF36535.
13. Les procédures mémorisées sur l'AS/400 ne peuvent pas inclure une instruction COMMIT si elles sont créées pour être exécutées dans le même groupe d'activation que le programme appelant (méthode de création correcte). Aussi, bien que sur DB2 pour OS/2, une procédure mémorisée puisse inclure une instruction COMMIT, le concepteur de l'application doit tenir compte du fait que DB2 Universal Database pour AS/400 ne sera pas informé de l'exécution de l'instruction COMMIT.

Chapitre 6. Connexion de DB2 pour VSE et VM au sein d'un réseau DRDA

SQL/DS (DB2 pour VM) version 3 édition 5 fournit un support de serveur d'applications d'unité d'oeuvre éloignée DRDA et de demandeur d'application DRDA pour les systèmes VM. SQL/DS (DB2 pour VSE) version 3.5 permet de prendre en charge un serveur d'applications d'unité d'oeuvre éloignée DRDA pour les systèmes VSE.

En outre, DB2 pour VSE et VM version 5.1 permet de prendre en charge un serveur d'applications d'unité d'oeuvre répartie DRDA pour les systèmes VM et VSE. Le présent chapitre met principalement l'accent sur la connexion DB2 pour VSM et VM à d'autres types de systèmes DRDA éloignés. Pour de plus amples informations sur la connexion de deux systèmes DB2 pour VSE et VM, reportez-vous aux manuels suivants :

- *VM/ESA Connectivity Planning, Administration and Operation*
- *DB2 for VM System Administration*
- *DB2 for VSE System Administration*

Présentation de DB2 pour VM

Chaque système de gestion de bases de données DB2 pour VM peut gérer une ou plusieurs bases de données (une à la fois) et est identifié par le nom de la base de données en cours de traitement. Ce nom de base de données relationnelle est unique dans un ensemble de réseaux SNA interconnectés.

Les différents composants DRDA et VM concernés par le traitement d'une base de données répartie sont décrits ci-après. Ces composants permettent aux systèmes de gestion de bases de données DB2 pour VM d'accéder à des bases relationnelles locales et de communiquer avec des systèmes DRDA éloignés dans le réseau SNA.

AVS Le support APPC/VTAM (AVS) est un composant de VM qui permet aux applications d'accéder au réseau SNA. Il fournit la fonction de LU telle qu'elle est définie par SNA. Une LU est appelée *passerelle* en environnement VM. AVS s'exécute dans un système de contrôle de groupe telle qu'une application VTAM. Il convertit les appels de macros APPC/VM en appels de macros APPC/VTAM et inversement. APPC/VM utilise AVS pour acheminer et convertir les flots de données. Grâce à AVS, les requêtes DB2 pour VM sont acheminées entre le système VM local et les emplacements SNA éloignés. AVS doit

être utilisé chaque fois que des applications ou des bases de données DB2 pour VM communiquent avec des bases de données ou des applications d'un autre type.

Au niveau du demandeur d'application, l'utilisateur doit être autorisé à se connecter via la passerelle AVS avant tout envoi de requête. Dans le cas du serveur d'applications, la passerelle AVS en réception doit être également autorisée à se connecter à un serveur DB2 pour VM avant de pouvoir prendre en compte les requêtes des utilisateurs. L'autorisation est obtenue en fournissant les instructions de contrôle de répertoire IUCV appropriées à la machine utilisateur, à la machine de la base de données et aux machines AVS émettrices et réceptrices. Pour les détails sur la procédure à suivre, reportez-vous au manuel *VM/ESA Connectivity Planning, Administration, and Operation.*

APPC/VM
APPC/VM est une API de niveau assembleur qui fournit un sous-ensemble de la fonction LU 6.2 tel qu'il est défini par SNA. En termes pratiques, elle fournit les instructions LU 6.2 qui permettent aux applications DB2 pour VM de se connecter à des systèmes de gestion de bases de données locaux et éloignés et de s'exécuter dans ces systèmes. Les instructions LU 6.2 prises en charge par APPC/VM sont indiquées dans le manuel *VM/ESA CP Programming Services.*

Répertoire de communication
Le répertoire de communications est un fichier CMS NAMES qui joue un rôle spécifique dans l'établissement des conversations APPC entre un demandeur d'application VM local et un serveur d'applications. Le répertoire fournit les informations nécessaires à l'acheminement et à l'établissement d'une conversation APPC avec un serveur cible. Ces informations sont le nom de LU, le nom de programme transactionnel, la sécurité, le nom de mode, l'ID utilisateur, le mot de passe et le nom de la base de données.

DB2 pour VM utilise la marque COMDIR :dbname pour associer le nom RDB_NAME aux données de routage correspondantes.

Ce fichier spécial et sa fonction de communication sont décrits dans le manuel VM/ESA *Connectivity Planning, Administration, and Operation.*

CRR CRR (récupération coordonnée des ressources) est une fonction de VM qui coordonne la validation ou la restitution des mises à jour de ressources protégées. Les programmes d'application répartis, associés à CRR, utilisent des conversations protégées pour assurer l'intégrité des ressources de transactions réparties.

CRR Recovery Server
Le serveur de récupération CRR est un composant de la fonction CRR fonctionnant sur sa propre machine virtuelle. Il est chargé de la fonction de journalisation des points de synchronisation et de la fonction de resynchronisation.

GCS Le système de contrôle de groupe est un composant comprenant les éléments suivants :

- un segment partagé s'exécutant dans une machine virtuelle
- un superviseur VM reliant plusieurs machines virtuelles dans un groupe et qui contrôlera leur fonctionnement
- une interface entre les programmes suivants :
  - VTAM (méthode d'accès virtuelle en télétraitement)
  - AVS (support APPC/VTAM)
  - RSCS (sous-système de communication à distance)
  - CP (programme de contrôle)

  GCS supervise l'exécution des applications VTAM telles que AVS dans un environnement VM. Les machines virtuelles s'exécutant sous la supervision de GCS n'utilisent pas CMS.

Adaptateur de ressources
L'adaptateur de ressources est une partie du programme logique DB2 pour VM qui réside dans votre machine virtuelle et qui permet à votre application de demander l'accès à un serveur DB2 pour VM. La fonction demandeur d'application DRDA est intégrée à l'adaptateur de ressources.

TSAF La fonction transparente d'accès est un composant de VM qui fournit un support de communication entre des systèmes VM interconnectés. Un groupe TSAF admet jusqu'à huit systèmes VM, qui peuvent être considérés comme analogues, pour la connexion à un réseau local VM (ou à un grand réseau). Chaque système VM participant doit disposer d'une machine virtuelle TSAF en cours de fonctionnement. Dans un groupe TSAF, tous les ID utilisateur et les ID ressource sont uniques.

DB2 pour VM utilise TSAF pour acheminer les requêtes portant sur des bases de données réparties vers d'autres machines DB2 pour VM au sein d'un groupe TSAF. Si le système VM local ne dispose pas de machine virtuelle AVS, DB2 pour VM utilise TSAF pour l'acheminement des requêtes DRDA vers un système VM ne disposant pas d'une machine virtuelle AVS. AVS permet de faire suivre les requêtes vers d'autres groupes TSAF et des systèmes autres que DB2 pour VM.

Un groupe TSAF est considéré comme une ou plusieurs unités logiques dans un réseau SNA. L'accès aux ressources définies comme

globales dans le groupe TSAF peut être effectué via des programmes APPC éloignés résidant en un point quelconque du groupe.

En principe, un groupe TSAF s'exécute en mode autonome, indépendamment de VTAM et du réseau SNA. Cependant, il peut coopérer avec AVS et VTAM pour rendre ses ressources globales accessibles par les programmes APPC éloignés résidant en un point quelconque du réseau SNA. Pour cela, vous devez disposer d'une machine AVS et d'une machine VTAM s'exécutant sur un ou plusieurs membres TSAF. La fonction TSAF est décrite dans le manuel VM/ESA *Connectivity Planning, Administration, and Operation.*

VTAM

La méthode d'accès virtuelle en télétraitement (VTAM) fournit le support de communication de réseau pour la connectivité. DB2 pour VM utilise les fonctions VTAM via AVS pour acheminer les connexions et les requêtes vers les systèmes DRDA éloignés. La fonction VTAM est utilisée *uniquement* pour les demandes éloignées d'accès au réseau SNA.

***IDENT**

AVS et TSAF utilisent le nom de programme transactionnel (TPN) pour acheminer les requêtes entre les systèmes VM qui sont connectés via TSAF et AVS. Il peut s'agir d'un nom de programme transactionnel enregistré sous SNA ou d'un nom alphanumérique correct. VM considère le nom de programme transactionnel comme un ID ressource. Pour accéder aux systèmes DRDA éloignés, le serveur DB2 pour VM utilise le service système VM IDENTIFY (*IDENT) pour se définir comme gestionnaire d'un ID ressource global (TPN). Une fois que le serveur est identifié comme ressource globale, TSAF et AVS peuvent acheminer les requêtes DRDA vers le serveur DB2 pour VM si le nom de programme transactionnel reçu correspond à l'ID ressource.

Communications du demandeur d'application - exemple

L'exemple suivant illustre le rôle joué par chaque composant dans l'établissement des communications entre un demandeur d'application VM et un serveur DRDA éloigné. La figure 27 à la page 131, illustre comment un demandeur d'application se connecte à AVS et utilise VTAM pour accéder au réseau SNA. Les ressources éloignées ne sont pas acheminées vers le serveur d'applications DB2 pour VM local.

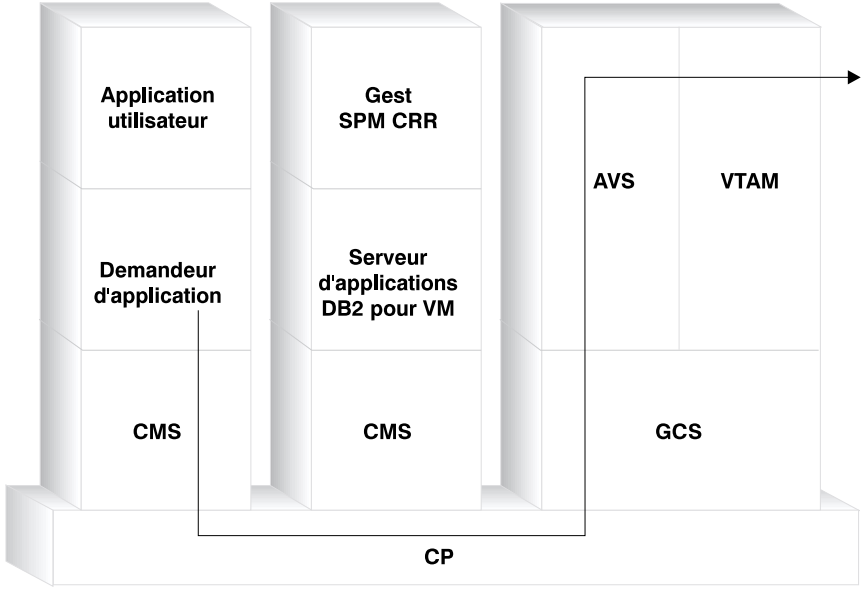

Figure 27. Demande d'accès à une ressource éloignée

Supposez qu'un demandeur d'application DB2 pour VM s'exécutant dans un groupe TSAF doive accéder à des données éloignées gérées par un serveur d'applications DRDA. Par définition, cela implique qu'une machine TSAF fonctionne sur l'hôte VM local où se trouve le demandeur d'application. En outre un composant AVS et une machine VTAM s'exécutent sur un système VM dans ce groupe TSAF. AVS et VTAM peuvent également résider sur le même système que le demandeur et le serveur d'applications.

Une fois la machine VTAM démarrée, elle définit une passerelle AVS locale vers le réseau SNA et active une ou plusieurs sessions qui seront utilisées ultérieurement pour l'établissement des conversations.

Une fois la machine AVS démarrée, elle négocie le nombre maximal de sessions pouvant être ouvertes entre la passerelle AVS locale et les LU partenaires potentielles.

Le serveur d'applications peut être actif ou inactif. L'opérateur peut le démarrer avant de traiter les requêtes à partir d'un demandeur d'application du même type ou de type différent.

Le demandeur d'application émet une instruction APPC/VM CONNECT pour établir une conversation de type LU 6.2 avec le serveur d'applications. La fonction CONNECT utilise le répertoire de communications CMS pour remplacer le nom de la base de données relationnelle par les noms de LU et de programme transactionnel appropriés comprenant l'adresse du serveur d'applications dans le réseau SNA. Le répertoire de communications CMS détermine également le niveau de sécurité de la conversation et les anneaux de sécurité, tels que l'ID utilisateur et le mot de passe pour accéder au site éloigné dans le cadre de la gestion des autorisations. Si vous utilisez le paramètre SECURITY=PGM, le demandeur d'application doit transférer l'ID utilisateur et le mot de passe au serveur d'applications. Vous pouvez indiquer l'ID utilisateur et le mot de passe dans le répertoire de communications CMS ou dans l'enregistrement APPCPASS défini dans le répertoire CP de l'utilisateur du demandeur d'application. Si vous utilisez le paramètre SECURITY=SAME, seul l'ID connexion VM du demandeur d'application est envoyé au serveur d'applications et aucun autre mot de passe n'est requis.

Par exemple, si vous utilisez le paramètre SECURITY=SAME, l'hôte vérifie si une machine AVS s'exécute en local. Si ce n'est pas le cas, l'hôte établit une connexion entre le demandeur d'application et la machine TSAF locale. La machine TSAF locale interroge les autres machines du groupe TSAF pour la machine AVS, puis se connecte à cette dernière.

Le composant AVS du groupe TSAF convertit la demande de connexion APPC/VM en un appel de fonction APPC/VTAM équivalent. AVS utilise ensuite une session existante ou alloue une nouvelle session entre sa passerelle (LU) et la LU éloignée. AVS établit ensuite une conversation avec la LU éloignée, puis transmet le nom de LU, le nom de p utilisateur. Si la LU éloignée est également un système VM, la session et la conversation sont gérées par le composant AVS s'exécutant sur ce système.

Communications du serveur d'applications - exemple

L'exemple suivant illustre le rôle joué par chaque composant dans l'établissement des communications entre un demandeur d'application éloigné et un serveur DRDA DB2 pour VM local. La figure 28 à la page 133 illustre comment VTAM achemine la connexion entrante vers la passerelle AVS spécifique, puis vers le serveur d'applications.

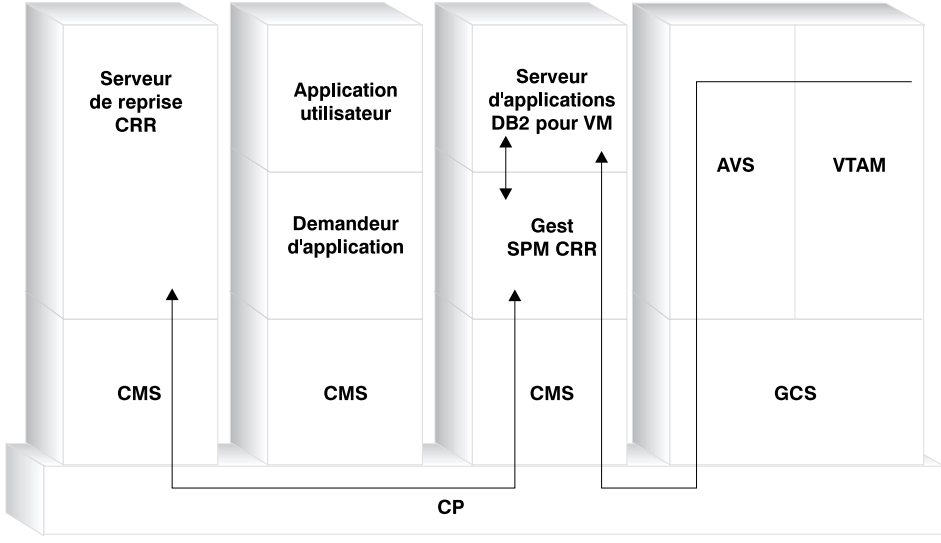

Figure 28. Accès à une ressource éloignée

Supposons qu'un serveur d'applications DB2 pour VM fonctionne dans un groupe TSAF. Par définition, cela implique qu'une machine TSAF fonctionne sur l'hôte VM local où se trouve le serveur d'applications. En outre un composant AVS et une machine VTAM s'exécutent sur un système VM dans ce groupe TSAF. AVS et VTAM peuvent également résider sur le même système que le demandeur et le serveur d'applications.

Une fois la machine VTAM démarrée, elle définit une passerelle AVS locale vers le réseau SNA et active une ou plusieurs sessions qui seront utilisées ultérieurement pour l'établissement des conversations.

Une fois la machine AVS démarrée, elle négocie le nombre maximal de sessions pouvant être ouvertes entre la passerelle AVS locale et les LU partenaires potentielles.

Le serveur d'applications peut être actif ou inactif. L'opérateur peut le démarrer avant de traiter les requêtes à partir d'un demandeur d'application du même type ou de type différent. Une fois le serveur d'applications démarré, il utilise le service *IDENT pour enregistrer l'ID ressource qu'il gère avec le système VM hôte. Chaque enregistrement crée une entrée dans une table de ressource interne maintenue par le système VM.

Une fois que le composant AVS local a établi la session avec sa LU partenaire, il accepte la conversation et transmet le TPN, l'ID utilisateur et le mot de passe à l'hôte VM pour validation. VM recherche alors le nom de programme transactionnel dans sa propre table de ressources internes. Cette table contient une entrée pour chaque ID ressource enregistré via le service système *IDENT. Si la recherche TPN aboutit, VM valide l'ID utilisateur et le mot de passe dans son répertoire, RACF ou un produit de sécurité similaire. Si la validation aboutit, AVS établit une connexion au serveur d'applications et lui transmet l'ID utilisateur dans le cadre des autorisations d'accès à la base de données.

Si la recherche dans la table n'aboutit pas, AVS suppose que le nom de programme transactionnel réside sur un autre système VM du groupe TSAF et établit une connexion à la machine TSAF locale, lui transmet l'ID utilisateur, le mot de passe et le nom de programme transactionnel. La machine TSAF interroge les autres machines du groupe TSAF. Si l'une de ces machines décèle la présence du nom de programme transactionnel dans sa table de ressource, la machine TSAF locale se connecte à la machine TSAF éloignée et lui transmet l'ID utilisateur et le mot de passe à vérifier avec son répertoire VM. Si la validation aboutit, la machine TSAF éloignée se connecte au serveur d'applications et lui transmet l'ID utilisateur en guise d'autorisation d'accès à la base de données.

Si le demandeur d'application souhaite bénéficier du support d'unité d'oeuvre répartie DRDA, il établit une conversation protégée (SYNCLEVEL=SYNCPT) avec le serveur d'applications DB2 pour VM. Avant d'afficher la fenêtre de connexion de DB2 pour VM, CMS crée une unité d'oeuvre CMS pour la conversation protégée sur la machine DB2 pour VM. DB2 pour VM utilise alors cette unité d'oeuvre CMS à chaque fois qu'il exécute un travail pour le demandeur. Lorsque DB2 pour VM commence à exécuter ce travail, il enregistre cette unité d'oeuvre CMS auprès du gestionnaire de point de synchronisation. Ensuite, lorsque DB2 reçoit une indication de validation (COMMIT) ou d'annulation (ROLLBACK) sur la conversation protégée, il demande au gestionnaire du point de synchronisation CRR de valider ou d'annuler l'unité d'oeuvre. Le gestionnaire du point de synchronisation CRR exécute ensuite la validation ou l'annulation, en demandant au serveur de récupération CRR d'effectuer une journalisation du point de synchronisation si nécessaire.

En fonction de la complexité du routage de la connexion, la conversation APPC entre le demandeur d'application et le serveur d'applications peut nécessiter l'utilisation de systèmes supplémentaires. Toutefois, toutes les connexions intermédiaires sont gérées par VM et sont transparentes pour le demandeur d'application ou l'application de l'utilisateur. L'interface APPC/VM permet aux serveurs d'applications DB2 pour VM de communiquer avec les programmes APPC se trouvant dans :

- le même système VM

- un système VM différent
- un système VM dans un réseau SNA où s'exécutent AVS et VTAM
- un système VM dans un groupe TSAF où s'exécutent AVS et VTAM
- un système autre que VM dans un réseau SNA prenant en charge le protocole LU 6.2
- un système non IBM dans un réseau SNA prenant en charge le protocole LU 6.2

Mise en oeuvre de DB2 pour VM

Comme illustré à la figure 29 à la page 136, une application VM doit s'exécuter via un demandeur d'application DB2 pour VM (adaptateur de ressources) pour accéder à toute base de données du serveur d'applications DB2 pour VM ou DRDA. Une base de données du serveur d'applications DB2 pour VM peut recevoir des requêtes SQL provenant de n'importe quel demandeur d'application DB2 pour VM ou DRDA.

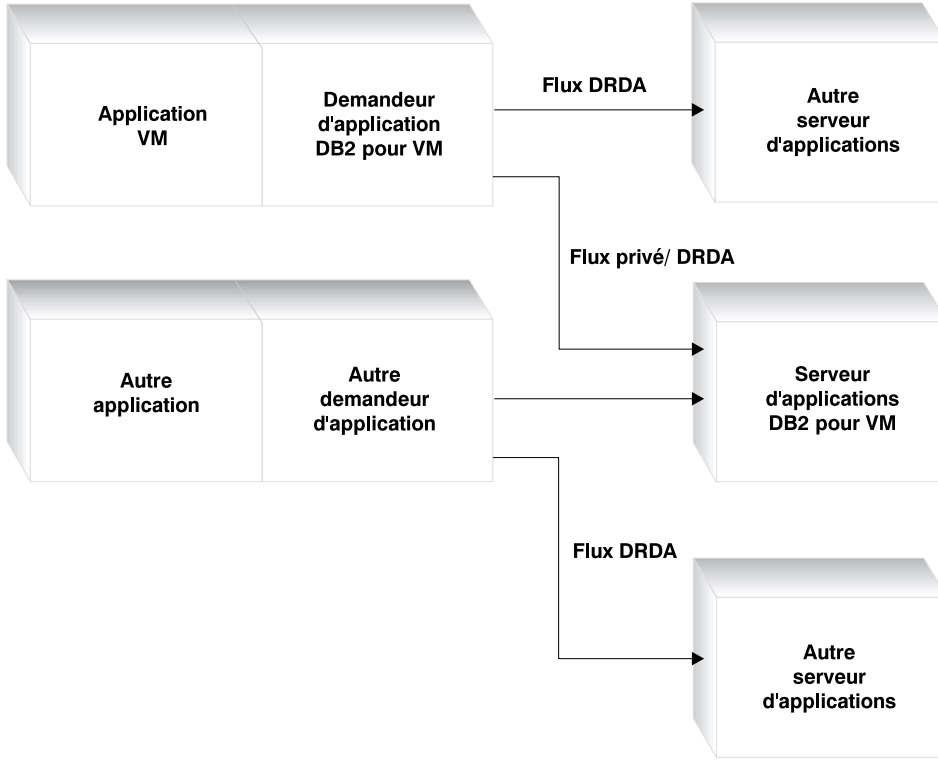

Figure 29. Demandeur d'application et serveur d'applications pour DB2 pour VM

Options de précompilation ou d'exécution d'une application

DB2 pour VM prend en charge trois options de traitement de la commande SQLINIT qui permettent à l'utilisateur et à l'administrateur de base de données d'activer le support de bases de données réparties. L'utilisateur peut indiquer l'une des options SQLINIT suivantes avant la précompilation ou l'exécution de l'application :

PROTOCOL(SQLDS)

Nécessite l'utilisation du protocole SQLDS privé. Il s'agit de l'option par défaut. Elle peut être utilisée entre un demandeur d'application DB2 pour VM application et un serveur, dans un environnement local ou éloigné. Le serveur d'applications DB2 pour VM suppose que le demandeur utilise les mêmes CCSID (ID de jeu de caractères codés)

que le serveur. Les valeurs par défaut des CCSID[5] définies par le demandeur via SQLINIT ne sont pas prises en charge et aucun identificateur d'unité logique de travail (LUWID) LU 6.2 n'est associé à la conversation. Si vous utilisez uniquement les systèmes DB2 pour VM, et le même CCSID par défaut partout, il s'agit de l'option la plus efficace.

PROTOCOL(AUTO)

Demande au demandeur d'application DB2 pour VM d'identifier si le serveur d'applications appartient à un système équivalent ou à un système de type différent. Il choisit alors automatiquement un protocole SQLDS privé pour un système du même type ou un protocole DRDA pour un système de type différent. Il peut être utilisé entre des systèmes de même type (locaux ou éloignés) et des systèmes de type différent. Si le serveur d'applications n'a pas été défini avec le paramètre PROTOCOL=SQLDS, le demandeur d'application et le serveur peuvent avoir des valeurs par défaut de CCSID différentes. Les requêtes et les réponses sont converties en conséquence. L'option AUTO est recommandée dans les cas suivants :

- si vous devez accéder à tous les types de systèmes ;
- si les valeurs par défaut du CCSID sont différentes pour le demandeur et le serveur (et que l'option du paramètre PROTOCOL n'a pas la valeur SQLDS) ;
- si vous souhaitez que l'identificateur d'unité logique de travail (LUWID) LU 6.2 soit associée à chaque conversation de manière à pouvoir effectuer facilement la trace d'une tâche jusqu'à son site d'origine. Cette option est très utile lorsque vous devez gérer un grand nombre de systèmes DB2 pour VM sur votre réseau de bases de données réparties.

PROTOCOL(DRDA)

Oblige le demandeur d'application DB2 pour VM à utiliser uniquement le protocole DRDA pour communiquer avec le serveur d'applications. Vous pouvez utiliser cette option entre des systèmes de même type (locaux ou éloignés) et des systèmes de type différent. Si le serveur d'applications est un système du même type, le protocole DRDA est utilisé entre les deux systèmes DB2 pour VM. Le demandeur d'application et le serveur d'applications peuvent avoir des CCSID par défaut différents. Les requêtes et les réponses sont converties en conséquence. Vous pouvez utiliser cette option pour la communication entre deux systèmes DB2 pour VM afin de tester des applications spécifiques où l'utilisation du protocole DRDA peut

5. Dans DB2 pour VM, le demandeur d'application et le serveur d'applications spécifient les valeurs par défaut des CCSID en indiquant une option CHARNAME, pour SQLINIT et SQLSTART respectivement. Le nom CHARNAME est un nom symbolique qui est mis en correspondance en interne avec les CCSID appropriés.

fournir un meilleur rendement en raison de l'utilisation d'une taille de tampon plus grande pour l'envoi et la réception de données.

Le tableau 3 compare les caractéristiques fonctionnelles des options de traitement SQLINIT du demandeur d'application DB2 for VM.

Tableau 3. Comparaison des options de traitement SQLINIT du demandeur d'application DB2 pour VM

[SQLDS]	**[AUTO]**	**[DRDA]**
Les deux partenaires doivent être des systèmes DB2 pour VM.	Connexion à tout système DRDA	Connexion à tout système DRDA
Possibilité de communiquer avec un partenaire en local via TSAF ou AVS/VTAM	Possibilité de communiquer avec un système DB2 pour VM en local ou avec un système DB2 pour VM éloigné via TSAF ou AVS. Dans le cas d'un système d'un autre type, la communication doit s'effectuer via AVS.	Possibilité de communiquer avec un système DB2 pour VM en local ou avec un système DB2 pour VM éloigné via TSAF ou AVS. Dans le cas d'un système d'un autre type, la communication doit s'effectuer via AVS.
Prise en charge de SQL statique, dynamique et dynamique étendu	Prise en charge de SQL statique, dynamique et dynamique étendu	Prise en charge de SQL statique, dynamique et dynamique étendu [6]
Les CCSID définis par SQLINIT pour le demandeur d'application sont ignorés par le serveur d'applications DB2 pour VM.	Les CCSID définis par SQLINIT pour le demandeur d'application sont reconnus par le serveur d'applications DB2 pour VM et sont convertis correctement.	Les CCSID définis par SQLINIT pour le demandeur d'application sont reconnus par le serveur d'applications DB2 pour VM et sont convertis correctement.
Taille de bloc fixe de 8 ko ; l'appel OPEN ne renvoie aucune ligne ; le demandeur d'application doit émettre explicitement une demande de fermeture de curseur.	DB2 pour VM à DB2 pour VM : méthode SQLDS ; autres types de connexion : méthode DRDA	Taille de bloc variable de 1 ko à 32 ko ; groupage plus compact des données ; l'appel OPEN renvoie un bloc de lignes ; le serveur d'applications peut fermer implicitement le curseur, évitant au demandeur d'application d'envoyer un appel CLOSE.
Possibilité d'utilisation du curseur INSERT et des PUT pour insérer un bloc de lignes à la fois en utilisant la taille de bloc de 8 ko	DB2 pour VM à DB2 pour VM : méthode SQLDS ; autres types de connexion : méthode DRDA	Les PUT sont transformés en insertions de lignes normales et sont envoyés à raison d'une ligne à la fois.

6. Le langage SQL dynamique étendu est pris en charge avec les flux DRDA qui les convertit en instructions statiques ou dynamiques. Toutefois, il existe certaines restrictions.

Tableau 3. Comparaison des options de traitement SQLINIT du demandeur d'application DB2 pour VM (suite)

Toutes les commandes uniques de DB2 pour VM sont prises en charge.	DB2 pour VM à DB2 pour VM : méthode SQLDS ; autres types de connexion : méthode DRDA	Les commandes opérateur DB2 pour VM, certaines instructions DB2 pour VM et certaines commandes ISQL et DBSU ne sont pas prises en charge (Voir le manuel *DB2 for VSE and VM SQL Reference*).
LUWID n'est pas pris en charge.	LUWID est pris en charge.	LUWID est pris en charge.

Options de démarrage du serveur de bases de données

Cette section décrit différentes options permettant de démarrer le serveur de bases de données.

Paramètre PROTOCOL

L'administrateur de la base de données peut indiquer l'une des options suivantes avec le paramètre `PROTOCOL` lors du démarrage du serveur.

SQLDS

Option par défaut, recommandée si le serveur d'applications ne doit offrir un support que pour les demandeurs d'application DB2 pour VM ou pour la demande d'application DB2 pour VSE bénéficiant du partage d'invité VSE. Le serveur d'applications utilise uniquement le flux privé (SQLDS).

Le serveur d'applications est dépendant de l'option de traitement sélectionnée par le demandeur d'application. Si le paramètre PROTOCOL(SQLDS) est indiqué pour un demandeur DB2 pour VM, le traitement effectué sur le serveur DB2 pour VM se poursuit normalement avec les flux privés. Si le paramètre PROTOCOL(AUTO) est indiqué pour un demandeur DB2 pour VM, le serveur DB2 pour VM indique au demandeur d'utiliser un flux privé. Aucune information de CCSID n'est échangée entre le demandeur d'application et le serveur d'applications. Ce dernier suppose que les CCSID du demandeur d'application sont identiques aux siens. Si le paramètre PROTOCOL(DRDA) est indiqué pour un demandeur DB2 pour VM, la conversation prend fin. Si un demandeur d'application autre que DB2 pour VSE et VM tente d'accéder au serveur DB2 pour VM, la conversation prend fin.

AUTO

Option recommandée si le serveur d'applications doit fournir un support pour le protocole privé et le protocole DRDA. Lorsque les paramètres PROTOCOL(SQLDS) ou PROTOCOL(AUTO) sont indiqués pour les demandeurs d'application, ces derniers communiquent dans un flux privé. Dans le cas d'un demandeur

d'application pour lequel l'option SQLDS est indiquée, aucune information de CCSID n'est échangée et le serveur d'applications suppose que les CCSID du demandeur d'application sont identiques aux siens. Lorsque l'option AUTO est indiquée pour un demandeur, les informations relatives au CCSID sont échangées et la conversion de CCSID pour les requêtes et les réponses est effectuée de manière appropriée. Le flux DRDA est requis par des demandeurs autres que DB2 pour VM, ou par n'importe quel demandeur DB2 pour VM spécifiant PROTOCOL(DRDA).

Paramètre SYNCPNT
Ce paramètre indique si un gestionnaire de points de synchronisation (SPM) va être utilisé pour coordonner l'activité de lecture et d'écriture multisite de l'unité d'oeuvre répartie DRDA-2.

Si Y est spécifié, le serveur utilise si possible un gestionnaire de points de synchronisation pour coordonner les activités de resynchronisation et de validation en deux phases. Si N est spécifié, le serveur d'applications n'utilise pas de SPM pour exécuter les validations en deux phases et il est limité aux unités d'oeuvre réparties à lecture multisite et à écriture monosite ; il peut constituer ce site unique. Si Y est spécifié, mais que le serveur d'applications ne trouve aucun gestionnaire de points de synchronisation disponible, le serveur fonctionne comme si N avait été indiqué.

La valeur par défaut est SYNCPNT=Y lorsque PROTOCOL=AUTO. Lorsque PROTOCOL=SQLDS, la valeur du paramètre SYNCPNT est N.

Configuration du demandeur d'application dans un environnement VM

DB2 pour VM met en oeuvre le support du demandeur d'application DRDA en tant que partie intégrante de l'adaptateur de ressources résidant sur la machine virtuelle de l'utilisateur final avec l'application. Vous pouvez utiliser le support du demandeur d'application même si la machine virtuelle du gestionnaire de bases de données locales n'est pas active. Vous pouvez activer le support du demandeur d'application DRDA en exécutant SQLINIT EXEC avec l'option PROTOCOL (AUTO) ou PROTOCOL (DRDA) (reportez-vous à la section «Options de précompilation ou d'exécution d'une application» à la page 136).

Lorsque DB2 pour VM est utilisé comme demandeur d'application, il peut se connecter à un serveur d'applications DB2 pour VM ou à tout autre serveur prenant en charge l'architecture DRDA. Si vous souhaitez que le demandeur d'application DB2 pour VM fournisse un accès à la base de données répartie, vous devez prendre en compte les informations suivantes :

- «Définition des données réseau» à la page 141. Le demandeur d'application doit pouvoir accepter les valeurs RDB_NAME et les convertir en valeurs NETID.LUNAME. DB2 pour VM utilise le répertoire de communications

CMS pour cataloguer les valeurs RDB_NAME et les paramètres réseau correspondants. Le répertoire de communications permet au demandeur d'application de transmettre les informations SNA requises à VTAM lors de l'émission de demandes portant sur une base de données répartie.

- «Définition de la sécurité» à la page 149. Si vous souhaitez que le serveur d'applications accepte les demandes portant sur une base de données éloignée, le demandeur d'application doit fournir les informations de sécurité requises par le serveur d'applications. DB2 pour VM utilise le répertoire de communications et le répertoire CP au niveau du demandeur d'application, ou le répertoire CP ou RACF éventuellement au niveau du serveur d'applications afin de fournir les informations de sécurité de réseau lors de l'émission de demandes portant sur une base de données répartie.
- «Représentation des données» à la page 154. Le CCSID du demandeur d'application doit être compatible avec celui du serveur d'applications.

Définition des données réseau

La plupart des opérations de traitement exécutées dans un environnement de bases de données réparties nécessitent l'échange de messages avec d'autres sites du réseau. Pour effectuer ce processus correctement, procédez par étapes dans l'ordre suivant :

1. Définition du système local.
2. Définition des systèmes éloignés.
3. Définition des sous-systèmes de communication
4. Définition de la taille de RU et de la régulation
5. Préparation du demandeur d'application DB2 pour VM

Définition du système local

Le demandeur d'application DB2 pour VM et le serveur d'applications DB2 pour VM sont indépendants l'un de l'autre. Le demandeur d'application DB2 pour VM achemine les demandes de connexion directement vers des serveurs d'applications locaux ou éloignés. Cependant, il ne se définit pas lui-même comme la cible des demandes de connexion entrantes. Seul le serveur d'applications DB2 pour VM peut accepter (ou rejeter) les demandes de connexion entrantes. Par conséquent, le demandeur d'application DB2 pour VM n'identifie pas les valeurs RDB_NAME et TPN pour lui-même, contrairement à DB2 Universal Database for OS/390.

Définissez le demandeur d'application DB2 pour VM sur le réseau SNA, en procédant comme suit :

1. Définissez les noms de passerelle AVS en utilisant les instructions de définition APPL VTAM.

   Des noms de passerelle doivent être définis par le demandeur d'application (des noms de LU par exemple) pour l'acheminement des demandes sortantes dans le réseau. La figure 30 à la page 142, en présente

un exemple. Ces instructions figurent sur la machine virtuelle VTAM. Lorsque VTAM est démarré, les passerelles sont identifiées sur le réseau mais ne sont pas activées tant que la machine virtuelle AVS n'est pas démarrée. Chaque machine virtuelle AVS peut définir plusieurs passerelles sur un système hôte VM.

```
                VBUILD  TYPE=APPL
************************************************************
*                                                          *
*     Gateway Definition for Toronto DB2 for VM System     *
*                                                          *
************************************************************
TORGATE  APPL  APPC=YES,                                   X
               AUTHEXIT=YES,                               X
               AUTOSES=1,                                  X
               DMINWNL=10,                                 X
               DMINWNR=10,                                 X
               DSESLIM=20,                                 X
               EAS=9999,                                   X
               MAXPVT=100K,                                X
               MODETAB=RDBMODES,                           X
               PARSESS=YES,                                X
               SECACPT=ALREADYV,                           X
               SYNCLVL=SYNCPT,                             X
               VPACING=2
```

Figure 30. Exemple de définition de passerelle AVS

La liste suivante décrit les mots clés d'instruction APPL VTAM qui sont applicables aux rubriques du présent manuel. (L'instruction APPL VTAM prend en charge de nombreux autres mots clés non indiqués ici).

TORGATE
VTAM utilise l'étiquette d'instruction APPL comme nom (LU) de passerelle. Dans la figure 30, la passerelle TORGATE est définie. Le NETID n'est pas indiqué dans l'instruction APPL VTAM. Il est automatiquement affecté à toutes les applications VTAM du système VTAM.

AUTOSES=1
La passerelle TORGATE spécifie qu'une session de vainqueur de conflit SNA démarre automatiquement lorsque vous lancez une commande APPC de modification du nombre de sessions (CNOS). Vous devez indiquer une valeur différente de zéro au paramètre AUTOSES pour AVS si vous voulez être averti de chaque échec de la commande CNOS. II n'est pas nécessaire de démarrer automatiquement toutes les sessions APPC entre les deux partenaires de bases de données réparties concernés. Si la valeur de AUTOSES est inférieure au nombre maximal de vainqueurs de

conflit (DMINWNL), VTAM diffère le démarrage des sessions restantes jusqu'à ce qu'elles soient demandées par l'application de base de données répartie.

DMINWNL=10
La passerelle TORGATE indique que ce système DB2 pour VM est le vainqueur de conflit sur 10 sessions au minimum. Le traitement CNOS utilise le paramètre DMINWNL comme valeur par défaut, mais cette valeur peut être remplacée à tout moment pour tout partenaire donné, si vous émettez une commande AGW CNOS à partir de la machine virtuelle AVS.

DMINWNR=10
La passerelle TORGATE indique que ce système partenaire est le vainqueur de conflit sur 10 sessions au minimum. Le traitement CNOS utilise le paramètre DMINWNR comme valeur par défaut, mais cette valeur peut être remplacée à tout moment pour tout partenaire donné, si vous émettez une commande AGW CNOS à partir de la machine virtuelle AVS.

DSESLIM=20
Le nombre total de sessions (qui ont abouti ou non) admises entre la passerelle TORGATE et tous les systèmes répartis partenaires pour un nom de groupe de mode donné est égal à 20. Le traitement CNOS utilise le paramètre DSESLIM comme valeur par défaut, mais cette valeur peut être remplacée à tout moment pour tout partenaire donné, si vous émettez une commande AGW CNOS à partir de la machine virtuelle AVS. Si le partenaire ne peut pas prendre en charge le nombre de sessions indiquées par les paramètres DSESLIM, DMINWNL ou DMINWNR, le processus CNOS négocie, pour ces paramètres, de nouvelles valeurs qui peuvent être acceptées par le partenaire.

EAS=9999
Estimation du nombre total de sessions requises par cette LU VTAM.

MODETAB=RDBMODES
Le nom de la table de modes VTAM est RDBMODES. Cette table contient tous les noms de mode qui peuvent être utilisés par cette passerelle pour la communication avec d'autres partenaires de bases de données réparties.

SECACPT=ALREADYV
Il s'agit du paramètre de sécurité identifiant le niveau de sécurité de conversation le plus élevé pouvant être pris en charge par cette passerelle lorsqu'il est présenté avec une demande de base de données répartie à partir d'un partenaire éloigné. Il est

recommandé d'utiliser l'option SECACPT=ALREADYV. Cette option prend en charge les niveaux de sécurité suivants :

- SECURITY=NONE, demande ne contenant aucune donnée de sécurité. DB2 pour VM rejette les demandes DRDA utilisant ce niveau de sécurité.
- SECURITY=PGM, demande contenant l'ID utilisateur et le mot de passe du demandeur. DB2 pour VM accepte les demandes DRDA utilisant ce niveau de sécurité.
- SECURITY=SAME indique une demande qui a déjà été vérifiée et qui contient uniquement l'ID utilisateur du demandeur.

SYNCLVL=SYNCPT

Le paramètre SYNCLVL spécifie le niveau du support de synchronisation pour AVS. La valeur SYNCPT indique que les niveaux de synchronisation NONE, CONFIRM et SYNCPT sont pris en charge. Si cette passerelle AVS doit être utilisée pour les activités des unités d'oeuvre réparties DRDA-2 sur un serveur DB2 pour VM, spécifiez la valeur SYNCPT. S'il ne doit PAS y avoir d'activités des unités d'oeuvre réparties, spécifiez la valeur CONFIRM (indique que NONE et CONFIRM sont pris en charge, mais pas SYNCPT).

VERIFY=NONE

Identifie le niveau de la sécurité de session SNA (vérification de la LU partenaire) requis par ce système DB2 pour VM. La valeur NONE indique que la vérification de la LU partenaire n'est pas requise.

DB2 pour VM ne limite pas votre choix au mot clé VERIFY, mais la version VTAM que vous exécutez peut influencer ce choix. Dans un réseau non sécurisé, DB2 pour VM recommande l'utilisation du paramètre VERIFY=REQUIRED. Si vous choisissez VERIFY=OPTIONAL, VTAM effectue la vérification de la LU partenaire uniquement pour les partenaires qui en fournissent le support. VERIFY=REQUIRED permet à VTAM de rejeter les partenaires qui ne peuvent pas effectuer de vérification de LU partenaire.

VPACING=2

Ce paramètre permet de définir la régulation utilisée entre la LU partenaire et cette passerelle. La régulation de session est très importante pour les systèmes de bases de données réparties.

2. Activez la passerelle.

   L'activation de la passerelle s'effectue à partir de la machine virtuelle AVS fonctionnant sur le même hôte (ou d'autres hôtes du même groupe TSAF) comme demandeur d'application DB2 pour VM. Indiquez une commande ACTIVATE GATEWAY GLOBAL dans le profil de la machine AVS ou

lancez cette commande en mode interactif à partir de la console d'une machine AVS pour activer automatiquement la passerelle à chaque démarrage du système AVS.

3. Utilisez la commande AGW CNOS pour négocier le nombre de sessions entre la passerelle et chacune de ses LU partenaires.

   Assurez-vous que la valeur MAXCONN indiquée dans le répertoire CP de la machine sur laquelle se trouve la passerelle AVS est suffisamment élevée pour la prise en charge du nombre total de sessions requises.

   Lancez la commande AGW DEACTIVE GATEWAY à partir de la machine virtuelle AVS pour désactiver la passerelle. La définition de la passerelle est conservée. La passerelle peut être réactivée à tout moment à l'aide de la commande AGW ACTIVATE GATEWAY GLOBAL.

   Reportez-vous au manuel *VM/ESA Connectivity Planning, Administration and Operation* pour les formats des commandes AVS.

4. Vérifiez que le NETID VTAM est défini dans le gestionnaire de bases de données DB2 POUR VM lors de l'installation.

   Le NETID de l'hôte (ou des autres hôtes du même groupe TSAF) où réside le demandeur d'application est fourni par VTAM dès que la demande parvient au réseau. Le NETID est stocké dans le NETID SNA du fichier CMS et réside sur le disque de production DB2 pour VM auquel a accès le demandeur d'application. Le demandeur d'application utilise le NETID pour générer le LUWID qui se transmet au cours de chaque conversation.

Définition des systèmes éloignés

Pour définir les systèmes éloignés, enregistrez les noms de LU qui activent VTAM pour localiser la destination de réseau désirée. Lors du démarrage d'AVS, ce dernier identifie globalement les noms de passerelle (noms de LU) disponibles pour l'acheminement des demandes SQL dans le réseau VTAM. Le nom de passerelle doit être unique dans un ensemble de noms de LU reconnus par le système VTAM local, afin que les demandes entrantes et sortantes soient acheminées vers le nom de LU approprié. Ceci constitue le meilleur moyen de s'assurer que le nom de la passerelle est vraiment unique sur le réseau. En outre, le processus de définition de ressource VTAM en est simplifié.

Lorsqu'une application DB2 pour VM demande des données à un système éloigné, DB2 pour VM recherche dans le répertoire de communications CMS les informations suivantes relatives à ce système :

- nom de la passerelle (nom de LU locale)
- nom de LU éloignée
- nom de programme transactionnel éloigné (TPN)
- niveau de sécurité de conversation requis par le serveur d'applications

- ID utilisateur permettant d'identifier le demandeur d'application au niveau du serveur d'applications
- mot de passe autorisant le demandeur d'application à accéder au serveur d'applications
- nom de mode décrivant les caractéristiques de session à utiliser pour communiquer avec le serveur d'applications
- RDB_NAME

Le répertoire de communications CMS est un fichier CMS de type NAMES, qui est créé et géré par un administrateur système DB2 pour VM. Vous pouvez, comme l'administrateur, créer ce fichier sous XEDIT et ajouter les entrées que vous souhaitez pour identifier chaque partenaire DRDA potentiel. Chaque entrée du répertoire est composée d'un ensemble de marques et des valeurs qui leurs sont associées. La figure 31 présente un exemple d'entrée. Lorsqu'une recherche est effectuée, la clé de recherche est comparée à la valeur de la marque :dbname pour chaque entrée du fichier, jusqu'à ce qu'une correspondance soit trouvée ou jusqu'à la fin du fichier. Dans l'exemple de la figure 31, le responsable des ventes à Toronto veut créer un rapport de ventes mensuel pour la succursale de Montréal en accédant à distance à la base de données MONTREAL_SALES.

```
  SCOMDIR  NAMES    A1  V 132  Trunc=132 Size=10 Line=1 Col=1 Alt=8
====>
00001  :nick.MTLSALES
00002                 :tpn.SALES
00003                 :luname.TORGATE MTLGATE
00004                 :modename.BATCH
00005                 :security.PGM
00006                 :userid.SALESMGR
00007                 :password.GREATMTH
00008                 :dbname.MONTREAL_SALES
00009
```

Figure 31. Exemple d'entrée dans un répertoire de communications CMS

La marque :tpn identifie le nom du programme transactionnel qui active le serveur d'applications. La première partie de la marque :luname identifie la passerelle AVS (LU locale) utilisée pour l'accès au réseau SNA. La seconde représente le nom de LU éloignée. La marque :modename identifie le mode VTAM qui définit les caractéristiques des sessions allouées entre les LU locales et éloignées. La taille de RU, la régulation et la classe de service (COS) sont des exemples de ces caractéristiques. La marque :security indique le niveau de sécurité à utiliser pour la conversation lors de la connexion du demandeur d'application au serveur d'applications.

Le répertoire de communications CMS se trouve sur un disque système public accessible à tous les demandeurs d'application d'un système VM donné. Tout programme ou produit nécessitant l'accès éloigné via VTAM peut utiliser le répertoire de communications CMS.

Vous pouvez accéder aux deux niveaux du répertoire de communications CMS : système et utilisateur. Par exemple, vous pouvez créer un répertoire sur un disque système public, accessible à tous les demandeurs d'application d'un système VM donné. Vous pouvez également créer votre propre répertoire utilisateur pour remplacer les entrées existantes ou ajouter de nouvelles entrées qui n'apparaissent pas dans le répertoire système. La recherche est effectuée d'abord dans le répertoire utilisateur. En cas d'échec, elle se poursuit dans le répertoire système qui est une extension du répertoire utilisateur ; les recherches y sont effectuées uniquement lorsque les valeurs n'ont pas été trouvées dans le répertoire utilisateur.

Chacun de ces répertoires est identifié auprès de l'application et activé par la commande CMS SET COMDIR. Par exemple, vous pouvez utiliser la séquence de commandes suivante pour identifier les répertoires système et utilisateur (sur les disques S et A, respectivement), mais choisir d'activer uniquement le répertoire système pour les recherches :

```
SET COMDIR FILE SYSTEM SCOMDIR NAMES S

SET COMDIR FILE USER UCOMDIR NAMES A

SET COMDIR OFF USER
```

Le répertoire de communications CMS est décrit en détails dans le manuel *VM/ESA Connectivity Planning, Administration and Operation*. La commande CMS SET COMDIR est décrite dans le manuel *VM/ESA CMS Command Reference*.

Définition du sous-système de communication

Dans l'environnement VM, la gestion des communications est effectuée par un ensemble de composants. Ces composants auquel il est fait appel pour les communications de systèmes autres que DRDA sont APPC/VM, le répertoire de communications CMS, TSAF, AVS et VTAM.

APPC/VM est l'API de niveau assembleur de la LU 6.2 que le demandeur d'application DB2 pour VM utilise pour demander des services de communication. Le répertoire de communications CMS fournit les informations d'acheminement et de sécurité du système partenaire réparti. AVS active la passerelle et convertit les flux APPC/VM sortants en flux APPC/VTAM, et les flux APPC/VTAM entrants en flux APPC/VM.

APPC/VM, TSAF et AVS utilisent le répertoire de communications CMS, VTAM et *IDENT pour acheminer les demandes en direction du partenaire DRDA approprié.

Pour permettre à VTAM de communiquer avec les applications partenaires identifiées dans le répertoire de communications CMS, vous devez fournir les informations suivantes :

1. Définissez le nom de LU de chaque demandeur d'application et serveur d'applications pour VTAM. L'emplacement et la syntaxe de ces définitions dépend du type de connexion physique et logique du système éloigné au système VTAM.
2. Créez une entrée dans la table de modes VTAM pour chaque nom de mode indiqué dans le répertoire de communications CMS. Ces entrées décrivent la taille de RU, la taille de la fenêtre de régulation et la classe de service pour un nom de mode donné.
3. Si vous envisagez d'utiliser la vérification de LU partenaire (sécurité de la session), indiquez les profils VTAM et RACF (ou équivalents) pour l' algorithme de vérification.

Remarques sur le nombre maximal de sessions AVS : Lorsqu'un demandeur d'application utilise AVS pour communiquer avec un serveur d'applications éloigné, une connexion est lancée automatiquement. Si cette connexion supplémentaire entraîne le dépassement du nombre maximal de sessions admises, AVS place cette connexion en attente jusqu'à ce qu'une session devienne disponible. Lorsqu'une session devient disponible, AVS attribue la session à la connexion en attente et l'application utilisateur reprend le contrôle des opérations. Pour éviter cette situation, augmentez le nombre maximal de sessions pour permettre l'établissement de connexions supplémentaires en cas d'accroissement des demandes. Assurez-vous également que la valeur MAXCONN indiquée dans le répertoire CP de la machine AVS est suffisamment élevée pour la prise en charge d'un grand nombre de sessions pour les connexions APPC/VM.

Définition de la taille de RU et de la régulation

Les entrées que vous définissez dans la table de modes VTAM indiquent la taille de RU et la régulation. Si ces valeurs ne sont pas mentionnées correctement, des effets indésirables peuvent se produire pour toutes les applications VTAM.

Une fois que vous avez choisi la taille de RU, le nombre maximal de sessions et la régulation, évaluez l'impact que ces valeurs peuvent avoir sur votre réseau SNA. Lors de l'installation d'une nouvelle base de données, vous devez tenir compte des éléments suivants :

- Dans le cas des connexions VTAM CTC, vérifiez que la valeur du paramètre MAXBFRU est suffisante pour gérer la taille de RU plus les

29 octets ajoutés par VTAM pour l'en-tête de demande et l'en-tête de transmission SNA. Le paramètre MAXBFRU est indiqué par unités de 4 ko ; ce paramètre doit donc prendre une valeur minimale de 2 pour pouvoir gérer une RU de 4 ko.

- Dans le cas de connexions NCP, assurez-vous que la valeur du paramètre MAXDATA est suffisante pour gérer la taille de la RU plus 29 octets. Si vous indiquez une taille de RU de 4 ko, MAXDATA doit prendre au moins la valeur 4125.

  Si vous indiquez le paramètre NCP MAXBFRU, sélectionnez une valeur correspondant à la valeur de RU plus 29 octets. Dans la cas de NCP, le paramètre MAXBFRU définit le nombre de tampons d'E-S VTAM pouvant prendre en charge l'unité d'information acheminable (PIU). Si vous choisissez une taille de tampon IOBUF de 441, MAXBFRU=10 traite correctement une RU de 4 ko car 10*441 est supérieur à 4096+29.
- Le manuel *DRDA Connectivity Guide* indique comment évaluer l'impact de votre base de données répartie sur le pool IOBUF VTAM. Si une trop grande quantité de ressources de pool IOBUF est utilisée, les performances du système VTAM seront affectées pour toutes les applications VTAM.

Préparation du demandeur d'application DB2 pour VM

Le demandeur d'application DB2 pour VM peut ne pas disposer du support DRDA. Suivez la procédure suivante pour préparer le demandeur d'application DB2 pour VM aux communications DRDA :

1. L'exec ARISDBMA vous permet d'installer le support DRDA :
   - Entrez "ARISDBMA DRDA(ARAS=Y)", si vous installez le support pour le demandeur et le serveur.
   - Entrez "ARISDBMA DRDA(AR=Y)", si vous installez le support pour le demandeur uniquement.

   Reportez-vous au manuel *DB2 for VM System Administration* pour plus de détails.
2. Après avoir exécuté ARISDBMA, reconstruisez la bibliothèque ARISQLLD LOADLIB de DB2 pour VM. Reportez-vous au chapitre *Using a DRDA Environment* du manuel *DB2 for VM System Administration* pour plus de détails.

Définition de la sécurité

Lorsqu'un système éloigné exécute des opérations de traitement sur des bases de données réparties au nom d'une application SQL, il doit être capable de répondre aux critères de sécurité du demandeur d'application, du serveur d'applications et du réseau reliant ces derniers entre eux. Ces critères entrent dans une ou plusieurs des catégories suivantes :

- sélection des noms d'utilisateurs finals
- paramètres de sécurité réseau

- sécurité du gestionnaire de bases de données
- sécurité assurée par un sous-système de sécurité externe

Sélection des noms d'utilisateurs finals

Dans SQL et LU 6.2, les utilisateurs sont identifiés par un ID utilisateur comportant de 1 à 8 caractères. Cette valeur doit être unique pour un système d'exploitation particulier mais ne l'est pas forcément sur tout le réseau SNA. Par exemple, prenons le cas de deux utilisateurs s'appelant tous les deux JONES ; l'un se trouve sur le système TORONTO et l'autre sur le système MONTREAL. S'il s'agit d'une seule et même personne, il n'existe aucun risque de conflit. Cependant, si l'utilisateur JONES de TORONTO n'est pas le même que JONES de MONTREAL, le réseau SNA (et, par conséquent, les systèmes de bases de données réparties de ce réseau) ne pourront pas faire la distinction entre ces deux utilisateurs. Par conséquent, JONES de TORONTO pourra utiliser les droits de JONES de MONTREAL et inversement, à moins que vous n'en décidiez autrement.

DB2 pour VM fournit un support de conversion pour les noms d'utilisateurs finals afin d'éviter les conflits de dénomination. Cependant, le système n'effectue pas la conversion des ID utilisateur. Si la conversion doit être effectuée par le système, vous devez vous assurer que la conversion entrante est assurée correctement au niveau du serveur d'applications.

La *conversion sortante* s'effectue à l'aide du répertoire de communications CMS. Le répertoire de communications CMS doit comporter une entrée `:security.PGM`. Si tel est le cas, les valeurs correspondantes des marques :userid et :password sont acheminées sur le site éloigné (serveur d'applications) dans la demande de connexion.

Lorsque vous créez l'entrée indiquée à la figure 32 à la page 151, l'utilisateur dont l'ID est JONES sur le système local (TORONTO) est mappé avec l'ID JONEST lorsqu'il se connecte au serveur d'applications MONTREAL_SALES_DB sur le système MONTREAL. L'ambiguïté au niveau des ID utilisateur est alors levée.

```
  UCOMDIR  NAMES    A1  V 132  Trunc=132 Size=10 Line=1 Col=1 Alt=8
====>
00001  :nick.MTLSALES
00002                 :tpn.SALES
00003                 :luname.TORLU MTLGATE
00004                 :modename.BATCH
00005                 :security.PGM
00006                 :userid.JONEST
00007                 :password.JONESPW
00008                 :dbname.MONTREAL_SALES_DB
00009
```

Figure 32. Conversion de nom sortante

Sécurité réseau

Une fois que le demandeur d'application a sélectionné le nom d'utilisateur final qui le représente sur le site éloigné, il doit fournir les données de sécurité réseau LU 6.2 requises. Il existe trois grandes fonctions de sécurité réseau pour les unités logiques LU 6.2 :

- La sécurité au niveau de la session est indiquée à l'aide du paramètre VERIFY dans l'instruction APPL VTAM.
- La sécurité au niveau des conversations est indiquée dans le répertoire de communications CMS.
- Le cryptage.

Dans la mesure où le serveur d'applications est chargé de la gestion des ressources de bases de données, il détermine les fonctions de sécurité réseau que le demandeur d'application doit fournir. Vous devez enregistrer les besoins de sécurité du serveur d'applications dans le répertoire de communications du demandeur d'application en définissant la valeur appropriée pour la marque :security.

Les options de sécurité au niveau des conversations prises en charge par DRDA sont les suivantes :

SECURITY=SAME

Egalement connue sous le nom de sécurité déjà vérifiée, cette option suppose que seul l'ID de l'utilisateur (ID connexion) final est transmis au système éloigné. Le mot de passe n'est pas transmis. Ce niveau de sécurité des conversations est utilisé lorsque `:security.SAME` est spécifié dans le répertoire de communications du demandeur d'application pour ce serveur. Lorsque cette option est utilisée, la conversion de nom d'utilisateur final sortante n'est pas effectuée. L'ID utilisateur envoyé au site DRDA éloigné correspond à l'ID connexion de l'utilisateur de CMS. La marque :userid du répertoire de communications CMS est ignorée pour :security.SAME.

SECURITY=PGM

Cette option déclenche l'envoi de l'ID utilisateur final et du mot de passe au système éloigné (serveur d'applications) pour validation. Cette option de sécurité est utilisée lorsque `:security.PGM` est spécifié dans l'entrée du répertoire de communications CMS du demandeur d'application. Lorsque cette option est utilisée, la conversion de nom d'utilisateur final sortante est effectuée.

DB2 pour VM ne prend pas en charge le cryptage du mot de passe. Le mot de passe peut être spécifié dans la marque `:password`, ou peut être stocké dans l'entrée du répertoire CP de l'utilisateur final à l'aide d'une instruction APPCPASS. L'utilisation de l'instruction APPCPASS est recommandée si vous voulez accroître le niveau de sécurité pour votre mot de passe. Si le mot de passe n'est pas spécifié dans l'entrée du répertoire de communications CMS, une instruction APPCPASS est recherchée dans l'entrée du répertoire système (VM) de l'utilisateur.

Instruction APPCPASS : VM fournit l'instruction APPCPASS pour optimiser la sécurité de l'ID utilisateur et du mot de passe utilisés par le demandeur d'application pour se connecter à un serveur d'applications. L'instruction APPCPASS offre une grande souplesse d'utilisation ; vous pouvez l'utiliser de différentes façons pour le stockage des données de sécurité :

- **ID utilisateur et mot de passe :** Dans ce cas, les marques :userid et :password du répertoire de communications CMS doivent être en blanc.
- **ID utilisateur uniquement :** Dans ce cas, la marque :userid du répertoire de communications CMS doit être en blanc et vous devez indiquer la marque :password pour le mot de passe utilisateur.
- **Mot de passe uniquement :** Dans ce cas, la marque :password du répertoire de communications CMS doit être en blanc et vous devez indiquer la marque :userid pour l'ID utilisateur.

La figure 33 à la page 153 illustre un exemple où l'ID utilisateur est stocké dans le répertoire de communications de l'utilisateur et le mot de passe dans l'entrée du répertoire VM de l'utilisateur. Dans l'entrée du répertoire de communications, l'ID utilisateur MTLSOU est indiqué, mais aucun mot de passe n'est mentionné. Le mot de passe est stocké dans l'entrée du répertoire VM de l'utilisateur.

```
  UCOMDIR  NAMES    A1  V 132  Trunc=132 Size=8  Line=1 Col=1 Alt=8
====>
00001  :nick.MTLSALES
00002                 :tpn.SALES
00003                 :luname.TORGATE MTLGATE
00004                 :modename.BATCH
00005                 :security.PGM
00006                 :userid.MTLSOU
00007                 :password.
00008                 :dbname.MONTREAL_SALES_DB
00009
```

Figure 33. Exemple d'entrée de répertoire de communications sans indication de mot de passe

Lorsque APPC/VM établit la connexion entre le demandeur d'application et le serveur d'applications en utilisant la conversation SECURITY=PGM, il lit les valeurs des marques :userid et :password et les transmet au serveur d'applications. Si l'une ou l'autre de ces marques est en blanc, le système recherche les informations manquantes dans l'entrée du répertoire VM de l'utilisateur. Dans ce cas, l'instruction APPCPASS doit figurer dans l'entrée de répertoire VM comme indiqué ci-après.

```
APPCPASS TORGATE MTLGATE MTLSOU Q6VBN8XP
```

Cette instruction indique à APPC/VM que l'utilisateur (demandeur d'application) demandant la connexion via la passerelle AVS locale TORGATE, la LU partenaire MTLGATE et l'ID utilisateur MTLSOU doit envoyer le mot de passe Q6VBN8XP au serveur d'applications. Ces deux éléments permettent d'identifier l'utilisateur au niveau du serveur d'applications.

Le placement de l'instruction APPCPASS dans le répertoire VM n'incombe pas à l'utilisateur final. Ce dernier doit demander au programmeur des systèmes VM d'effectuer cette tâche.

Pour de plus amples informations sur la sécurité au niveau des conversations et sur l'instruction APPCPASS, reportez-vous au manuel *VM/ESA Connectivity Planning, Administration, and Operation*.

Sécurité du gestionnaire de bases de données

Dans le cadre de la sécurité globale de la base de données répartie, le demandeur d'application peut jouer un rôle important en contrôlant les utilisateurs finals qui sont autorisés à effectuer des demandes de bases de données réparties. Dans DB2 pour VM, le demandeur d'application peut contribuer à la sécurité de la base de données répartie de trois façons différentes :

Conversion de nom d'utilisateur sortante

Vous pouvez utiliser la fonction de conversion de nom d'utilisateur sortante pour contrôler l'accès à un serveur d'applications particulier, en fonction de l'identité de l'utilisateur final effectuant la demande.

DB2 pour VM tente de convertir le nom de l'utilisateur final avant l'envoi de la demande au site éloigné. Toutefois, le meilleur moyen est de faire en sorte que le serveur d'applications effectue l'identification du site émetteur et la conversion entrante, car les utilisateurs de demandeur d'application VM peuvent remplacer la conversion sortante par leur répertoire de communications utilisateur CMS.

Précompilation d'une application

Les utilisateurs finals précompilent les applications éloignées vers un serveur d'applications particulier en utilisant la commande SQLPREP EXEC de DB2 pour VM ou la commande RELOAD PACKAGE de l'utilitaire de service de base de données (DBSU). DB2 pour VM ne se limite pas à ces fonctions. Lorsqu'un utilisateur final effectue la précompilation d'une application, il devient propriétaire du module issu de cette précompilation.

Exécution d'une application

Pour exécuter une application éloignée, l'utilisateur final DB2 pour VM doit disposer de droits sur le site éloigné (serveur d'applications) pour effectuer des opérations sur le module éloigné associé à l'application donnée. Le créateur (propriétaire) du module est automatiquement autorisé à l'exécuter. Les autres utilisateurs finals peuvent également se voir accorder les droits d'exécution du module à l'aide de l'instruction GRANT EXECUTE de DB2 pour VM. Le propriétaire de l'application de base de données répartie peut alors contrôler l'utilisation de l'application à raison d'un utilisateur à la fois.

Sous-système de sécurité

Le sous-système de sécurité externe sur les systèmes VM est assuré par RACF ou des produits équivalents qui fournissent une interface compatible avec RACF. Le demandeur d'application DB2 pour VM n'est pas directement en relation avec le système de sécurité externe. Ce dernier n'est pas utilisé pour fournir des mots de passe pour la sécurité au niveau des conversations. Si vous choisissez d'utiliser la sécurité au niveau des sessions, le sous-système de sécurité externe est appelé par VTAM pour valider l'identité du nom de LU éloignée lors de la vérification de la LU partenaire.

Représentation des données

Les valeurs par défaut appropriées de CHARNAME et du CCSID doivent être définies pour le demandeur d'application. En indiquant des valeurs correctes, vous assurez l'intégrité de la représentation des données alphanumériques et réduisez le temps système associé à la conversion de CCSID.

Par exemple, si votre demandeur d'application DB2 pour VM est généré avec la page de codes 37 et le jeu de caractères 697 (CP/CS 37/697) pour l'anglais (Etats-Unis), le demandeur d'application doit affecter par défaut à

CHARNAME la valeur ENGLISH. En effet, CP/CS 37/697 correspond au CCSID 37, qui lui-même correspond à la valeur ENGLISH pour CHARNAME.

La valeur par défaut de CHARNAME pour un système migré ou récemment installé est INTERNATIONAL et le CCSID est 500. Ces valeurs ne sont probablement *pas* correctes pour votre installation. Pour afficher les valeurs des CCSID par défaut en cours, utilisez la commande suivante :

```
SQLINIT QUERY
```

La valeur de CCSID appropriée pour le demandeur d'application peut être l'une des valeurs non prises en charge par les tables de conversion au niveau du serveur d'applications. Dans ce cas, vous pouvez établir la connexion en procédant de la manière suivante :

- Faites en sorte que le serveur d'applications mette à jour sa table de conversion de CCSID pour la prise en charge de la conversion entre le CCSID par défaut du demandeur d'application et le CCSID par défaut du serveur d'applications (pour plus de détails sur l'ajout de support de conversion de CCSID, reportez-vous aux manuels relatifs au serveur d'applications).
- Remplacez le CCSID par défaut du demandeur d'application en indiquant une valeur prise en charge par le serveur d'applications. Des problèmes d'intégrité des données peuvent en découler. Vous devez tenir compte des conséquences que cela peut entraîner. Par exemple :

  Un demandeur d'application utilise un contrôleur défini avec CP/CS 37/697. Le serveur d'applications ne prend pas en charge la conversion à partir du CCSID 37, mais du CCSID 285 (il s'agit de la valeur UK-ENGLISH pour CHARNAME pour SQL/DS).

  Si vous indiquez pour le demandeur d'application la valeur UK-ENGLISH pour CHARNAME (et un CCSID de 285), l'intégrité des données ne sera pas conservée. Par exemple, lorsque le symbole de la livre sterling (£) est demandé par le serveur d'applications, le demandeur d'application affiche le symbole du dollar ($). D'autres caractères peuvent également être différents.

  Pour modifier la valeur de CCSID d'un demandeur d'application DB2 pour VM, vous devez indiquer le paramètre CHARNAME du fichier SQLINIT EXEC. Reportez-vous au manuel *DB2 for VM System Administration* pour de plus amples informations.

La valeur de CCSID appropriée pour le demandeur d'application doit être prise en charge par les tables de conversion au niveau du demandeur d'application. Dans ce cas, vous pouvez établir la connexion en procédant de la manière suivante :

- Mettez à jour la table de conversion utilisée par le demandeur d'application pour la prise en charge de la conversion entre le CCSID par défaut du serveur d'applications et le CCSID par défaut du demandeur d'application. Reportez-vous au manuel *DB2 for VM System Administration* pour savoir comment mettre à jour la table système SYSTEM.SYSSTRINGS. Cette table permet de créer le fichier CMS ARISSTR MACRO, qui est utilisé par le demandeur d'application pour le support de conversion CCSID.
- Assurez-vous que le CCSID par défaut du serveur d'applications est modifié. Cette opération ne doit être exécutée qu'en cas de nécessité, en fonction de l'utilisation que vous comptez faire du CCSID par défaut du serveur d'applications. Le CCSID par défaut du serveur d'applications concerne tous les demandeurs d'application auquel il est connecté, le terminal opérateur utilisé avec le serveur d'applications et les données stockées dans les tables sur le serveur d'applications.

Liste de contrôle d'activation du demandeur d'application DRDA DB2 pour VM

La liste de contrôle ci-après récapitule les étapes nécessaires à l'activation d'un demandeur d'application DRDA pour les communications DRDA, en supposant que votre système VM soit installé, que ACF/VTAM soit utilisé comme méthode d'accès en télétraitement et que les définitions VTAM requises pour communiquer avec les systèmes éloignés telles que les définitions NCP soient complètes.

1. Définissez la passerelle AVS locale pour VTAM
2. Installez le support DRDA dans le demandeur d'application DB2 pour VM en utilisant la commande ARISDBMA.
3. Configurez un répertoire de communications CMS et ajoutez toutes les instructions APPCPASS nécessaires au répertoire VM de la machine VM de l'application. Utilisez la commande SET COMDIR CMS pour activer le répertoire de communications.
4. Démarrez VTAM et AVS pour que les applications VM puissent communiquer à distance via le réseau SNA.
5. Lancez la commande SQLINIT et indiquez aux paramètres DBNAME, PROTOCOL et CHARNAME respectivement la base de données par défaut ainsi que le protocole et les valeurs de CCSID à utiliser.
6. Préparez les applications sur le serveur éloigné.

Configuration du serveur d'applications dans un environnement VM

Le support du serveur d'applications dans DB2 pour VM permet à ce dernier de jouer le rôle de serveur pour les demandeurs d'application DRDA. Le demandeur d'application connecté à un serveur d'applications DB2 pour VM peut être :

- un demandeur DB2 pour VM
- un demandeur DB2 Universal Database for OS/390
- un demandeur OS/400
- un demandeur DB2 pour AIX
- tout demandeur d'application de la famille DB2, y compris DB2 CONNECT, ou n'importe quel autre produit supportant les protocoles de demandeur d'application DRDA

Quel que soit le demandeur d'application connecté à un serveur d'applications DB2 pour VM, ce dernier permet au demandeur d'application d'accéder aux objets de base de données (tels que les tables) stockés en local sur le serveur d'applications DB2 pour VM. Le demandeur d'application doit créer un module contenant les instructions SQL de l'application sur le serveur d'applications avant l'établissement de la connexion.

Pour que le serveur d'applications DB2 pour VM puisse traiter les demandes de bases de données réparties, vous devez effectuer les opérations ci-après :

1. Définir le serveur d'applications sur le sous-système de communications local.
2. Définir la sécurité nécessaire.
3. Prévoir la représentation des données.

Définition des données réseau

Définition du serveur d'applications

Pour que le serveur d'applications puisse recevoir des demandes de bases de données réparties, vous devez le définir sur le sous-système de communications local et affecter une valeur unique à RDB_NAME.

Procédez par étapes dans l'ordre suivant pour définir le serveur d'applications :

1. Définissez le serveur d'applications DB2 pour VM sur le réseau SNA. Après avoir sélectionné le nom de passerelle et la valeur de RDB_NAME pour le serveur d'applications DB2 pour VM, suivez les procédures décrites à la section «Définition des données réseau» à la page 141. La valeur de RDB_NAME choisie pour DB2 pour VM doit être fournie à tous les utilisateurs (demandeurs d'application) pouvant demander une connexion au serveur d'applications DB2 pour VM.

Le NETID est défini pour VTAM en tant que paramètre de lancement et toutes les demandes réparties à partir du demandeur d'application sont acheminées correctement. Le serveur d'applications DB2 pour VM ne définit pas le NETID.

Le serveur d'applications DB2 pour VM ne détermine pas non plus la passerelle à utiliser pour l'acheminement des demandes réparties entrantes provenant du demandeur d'application. Ce processus est toujours contrôlé par le demandeur d'application. Dans le cas d'un demandeur d'application DB2 pour VM, le répertoire de communications CMS indique le nom de la passerelle à l'aide des marques :luname et :tpn.

Pour que le serveur d'applications DB2 pour VM prenne en charge l'activité d'unité d'oeuvre répartie, le demandeur d'application doit sélectionner une passerelle AVS définie sur VTAM à l'aide du paramètre SYNCLVL=SYNCPT. Vérifiez que la passerelle AVS a été définie pour prendre en charge les unités d'oeuvre réparties.

2. Créez un serveur de récupération CRR utilisé pour gérer l'activité des unités d'oeuvre réparties pour les serveurs d'applications DB2 pour VM sur ce système VM. Pour ce faire, suivez les étapes permettant un chargement après installation des serveurs IBM et des pools de fichiers décrits dans le manuel *VM/ESA Installation Guide*. Cela inclut la définition d'un serveur CRR (VMSERVR) et d'un pool de fichiers CRR (VMSYSR). Lorsque vous démarrez le serveur de reprise CRR, vérifiez que vous avez spécifié un nom LUNAME correspondant au nom d'une passerelle AVS pour laquelle SYNCLVL=SYNCPT a été indiqué.
3. Assurez-vous que le répertoire CP de la machine du serveur d'applications contient bien une instruction IUCV *IDENT. Elle permet d'identifier le serveur en tant que ressource globale.
4. Créez une entrée dans la table de noms de mode VTAM pour chaque nom de mode demandé par le demandeur d'application. Ces entrées décrivent les caractéristiques de la session, telles que la taille de RU, la régulation et la classe de service pour un nom de mode donné.
5. Définissez le nombre maximal de sessions pour les demandeurs d'application qui se connectent au serveur d'applications de DB2 pour VM. L'instruction APPL VTAM définit le nombre maximal de sessions par défaut pour tous les systèmes partenaires. Pour définir des valeurs par défaut propres à un partenaire, utilisez la commande AGW CNOS à partir de la machine virtuelle AVS se trouvant sur le site du serveur d'applications. (Le nombre maximal de sessions est le plus souvent demandé par le demandeur d'application.)

   Une fois que vous avez choisi la taille de RU, le nombre maximal de sessions et la régulation, évaluez l'impact que ces valeurs peuvent avoir sur le pool IOBUF VTAM.

Mappage d'un nom de serveur sur un ID ressource (RESID) : L'ID ressource (RESID) correspond au nom de programme transactionnel sous VM. Dans l'environnement VM, il est généralement défini sous forme alphanumérique en 8 octets au plus. En principe, l'ID ressource défini doit être identique au nom du serveur, dans le but de faciliter la gestion du système. La figure 34 présente un exemple de fichier RESID NAMES. Reportez-vous à la figure 33 à la page 153, pour consulter l'entrée du

```
  RESID  NAMES    A1  V 132  Trunc=132 Size=4  Line=1 Col=1 Alt=3
====>
00001  :nick.MTLTPN
00002                 :dbname.MONTREAL_SALES_DB
00003                 :resid.SALES
00004
```

Figure 34. Exemple de fichier RESID NAMES

répertoire de communications définissant ce nom dbname et l'ID ressource (en tant que TPN). Si le nom du serveur d'applications ne peut pas être identique à l'ID ressource (RESID), le serveur d'applications DB2 pour VM utilise le fichier RESID NAMES pour établir le mappage. Le mappage est nécessaire dans les cas suivants :

- Vous utilisez un ID ressource différent du nom du serveur.
- Vous utilisez un nom dont la taille est supérieure à 8 octets.
- Vous utilisez un ID ressource d'une valeur hexadécimale de 4 octets, comme le TPN DRDA par défaut X'07F6C4C2'

Lors de l'installation, la valeur par défaut doit utiliser le nom du serveur indiqué dans le fichier SQLDBINS EXEC comme ID ressource. Pour créer une entrée de mappage dans le fichier RESID NAMES, indiquez le paramètre RESID dans SQLDBINS.

Lorsque vous démarrez la base de données en utilisant SQLSTART DB(nom_serveur), DB2 pour VM consulte l'ID ressource correspondant et informe VM qu'il s'agit de la ressource à contrôler. S'il ne trouve pas l'entrée dans le fichier RESID NAMES, DB2 pour VM suppose que l'ID ressource est identique au nom du serveur et le signale à VM. Pour de plus amples informations, reportez-vous au manuel *DB2 for VM System Administration.*

Préparation et démarrage du serveur d'applications DB2 pour VM

Le serveur d'applications DB2 pour VM peut ne pas disposer du support DRDA. Procédez comme suit pour préparer le serveur d'applications DB2 pour VM aux communications DRDA :

1. L'exec ARISDBMA vous permet d'installer le support DRDA :
   - Entrez "ARISDBMA DRDA(ARAS=Y)", si vous installez le support pour le demandeur et le serveur.
   - Entrez "ARISDBMA DRDA(AS=Y)", si vous installez le support pour le serveur uniquement.

   Reportez-vous au manuel *VM/ESA System Administration* pour plus de détails.
2. Après avoir exécuté ARISDBMA, reconstruisez la bibliothèque ARISQLLD LOADLIB de DB2 pour VM. Reportez-vous au chapitre *Using a DRDA Environment* du manuel *DB2 for VM System Administration* pour plus de détails.

Définition de la sécurité

Lorsqu'un demandeur d'application achemine une demande portant sur une base de données répartie vers le serveur d'applications DB2 pour VM, les critères de sécurité suivants peuvent être pris en compte :

- conversion de nom d'utilisateur final entrante
- paramètres de sécurité réseau
- sécurité du gestionnaire de bases de données
- sécurité assurée par un sous-système de sécurité externe

Noms d'utilisateurs finals

Dans SQL et LU 6.2, les utilisateurs finals sont identifiés par un ID utilisateur comportant 1 à 8 octets. Cet ID utilisateur doit être unique pour un système d'exploitation particulier mais ne doit pas forcément l'être sur tout le réseau SNA. Pour éviter les conflits de dénomination, DB2 pour VM peut facultativement utiliser la fonction de conversion d'ID utilisateur fournie par AVS, mais uniquement dans les conditions suivantes :

- Le demandeur d'application DB2 pour VM doit s'exécuter en environnement VM/ESA.
- Les demandes de connexion entrantes doivent être acheminées via une passerelle AVS.
- Le demandeur d'application partenaire doit utiliser la conversation SECURITY=SAME, également appelée *already verified* (déjà vérifié) en terminologie SNA.

Si une connexion est acheminée sur un serveur via AVS et que l'option SECURITY=SAME est utilisée, l'ID utilisateur AVS doit être converti. La commande AGW ADD USERID lancée à partir de la machine AVS doit

fournir un niveau de sécurité suffisant pour permettre la connexion d'utilisateurs d'une LU éloignée ou d'une passerelle AVS spécifique. Un mappage doit être disponible pour toutes les LU et les ID utilisateur entrants se connectant avec l'option SECURITY=SAME L'utilisation de cette commande est très souple ; vous pouvez accepter tous les ID utilisateur d'une LU particulière ou de toutes les LU éloignées. Vous pouvez aussi accepter un ensemble d'ID utilisateur spécifiques d'une LU spécifique.

Si vous utilisez la commande AGW ADD USERID pour autoriser les ID utilisateur entrants (déjà vérifiés) sur la machine AVS locale, aucune validation n'est effectuée par l'hôte. Cela signifie que l'ID autorisé n'existe pas forcément sur l'hôte mais que la connexion est acceptée.

Il existe deux méthodes pour modifier l'autorisation accordée à l'ID utilisateur AVS :

- Arrêtez AVS en utilisant la commande AGW STOP. L'autorisation accordée à l'ID utilisateur est entièrement annulée.
- Supprimez l'ID utilisateur en utilisant la commande AGW DELETE USERID.

Par exemple, l'utilisation d'ID utilisateur identiques sur des sites différents permet d'illustrer la façon dont la fonction de conversion AVS permet de résoudre les conflits de dénomination. Prenez le cas d'un utilisateur dont l'ID est JONES et résidant sur le système Toronto, et d'un autre ayant un ID identique mais localisé sur le système Montréal. Si l'utilisateur JONES de Montréal veut accéder aux données se trouvant sur le système Toronto, les actions suivantes au niveau de ce dernier empêchent tout conflit de dénomination et permettent d'éviter que JONES de Montréal ne dispose des droits accordés à JONES sur le système Toronto.

1. L'opérateur AVS doit utiliser la commande AGW ADD USERID pour convertir l'ID de l'utilisateur de Montréal en ID utilisateur local. Par exemple, si l'opérateur AVS émet une commande `AGW ADD USERID MTLGATE JONES MONTJON`, l'utilisateur de Montréal est identifié par MONTJON sur le système Toronto. Si tous les utilisateurs de Montréal peuvent se connecter (via une commande LU MTLGATE à distance) et qu'ils sont identifiés en local par leurs ID utilisateur éloignés, l'opérateur doit émettre la commande `AGW ADD USERID MTLGATE * =`. Ces commandes AVS peuvent également être ajoutées au profil AVS pour être exécutées automatiquement lors du lancement d'AVS.
2. L'administrateur de la base doit utiliser la commande GRANT de DB2 pour VM pour octroyer un ensemble de privilèges spécifiquement à l'ID utilisateur converti, MONTJON en l'occurrence.

Ces opérations peuvent également être effectuées sur le système Montréal de sorte que JONES de Toronto n'utilise pas les droits accordés à JONES de Montréal, lors de l'accès au système Montréal.

Pour plus de détails sur les commandes AVS qui prennent en charge la conversion d'ID utilisateur, reportez-vous au manuel *VM/ESA Connectivity Planning, Administration and Operation*.

Sécurité réseau

LU 6.2 offre trois fonctions principales de sécurité réseau :

- sécurité au niveau des sessions
- sécurité au niveau des conversations
- cryptage

Reportez-vous à la section «Sécurité réseau» à la page 151, pour savoir comment spécifier la sécurité au niveau des sessions pour DB2 pour VM. La sécurité au niveau des sessions avec le serveur d'applications DB2 pour VM fonctionne sur le même principe qu'avec le demandeur d'application DB2 pour VM.

Le demandeur d'application envoie un ID utilisateur qui a déjà été vérifié (SECURITY=SAME) ou un ID utilisateur et un mot de passe (SECURITY=PGM). Si un utilisateur et un mot de passe sont envoyés, ils sont validés sur l'hôte du serveur d'applications par CP, RACF ou un programme équivalent avec le répertoire VM. Si la validation n'aboutit pas, la demande de connexion est rejetée, sinon elle est acceptée. Si la demande contient uniquement un ID utilisateur, DB2 pour VM l'accepte sans valider cet ID.

Remarque : DB2 pour VM n'offre pas de fonction de cryptage car VM/ESA ne prend pas en charge le cryptage.

Sécurité du gestionnaire de bases de données

Le serveur d'applications DB2 pour VM vérifie si l'ID utilisateur fourni par VM dispose des droits CONNECT pour accéder à la base de données, puis rejette la connexion si l'ID utilisateur ne dispose pas de ces droits.

En tant que propriétaire des ressources de base de données, le serveur d'applications DB2 pour VM contrôle les fonctions de sécurité de base de données pour les objets SQL résidant sur le serveur d'applications DB2 pour VM. L'accès aux objets gérés par DB2 pour VM est contrôlé via un ensemble de privilèges qui sont accordés aux utilisateurs par l'administrateur système DB2 pour VM ou le propriétaire de l'objet particulier. Le serveur d'applications DB2 for VM contrôle deux classes d'objets :

- **Modules :** Les utilisateurs finals individuels sont autorisés à créer, remplacer et exécuter les modules avec l'instruction GRANT de DB2 pour

VM. Lorsqu'un utilisateur final crée un module, il dispose automatiquement des droits nécessaires pour son exécution ou son remplacement. Les autres utilisateurs finals peuvent se voir octroyer de manière spécifique les droits d'exécution du module au niveau du serveur d'applications DB2 pour VM, à l'aide de l'instruction GRANT EXECUTE. Le privilège RUN peut être accordé à des utilisateurs finals ou à PUBLIC, ce qui permet à tous les utilisateurs finals d'exécuter le module.

Lorsqu'une application est précompilée sur DB2 pour VM, le module contient les instructions SQL contenues dans le programme d'application. Ces instructions sont classées comme suit :

- **SQL statique :** Signifie que l'instruction SQL et les objets SQL désignés par cette dernière sont connus au moment de la précompilation de l'application. Le créateur du module doit disposer des droits appropriés pour exécuter chaque instruction SQL statique du module.

  Lorsqu'un utilisateur final dispose des droits d'exécution d'un module, il dispose automatiquement des droits lui permettant d'exécuter chaque instruction SQL statique contenue dans le module. Les utilisateurs finals n'ont donc pas besoin d'utiliser les privilèges d'accès aux tables DB2 pour VM si le module contient uniquement des instructions SQL statiques.
- **SQL dynamique :** Ce terme décrit une instruction SQL qui n'est pas connue tant que le module n'est pas exécuté. L'instruction SQL est créée par le programme et est précompilée de manière dynamique sur DB2 pour VM à l'aide de l'instruction SQL PREPARE ou EXECUTE IMMEDIATE. Lorsqu'un utilisateur final exécute une instruction SQL dynamique, il doit disposer des privilèges d'accès aux tables nécessaires à l'exécution de l'instruction SQL. Etant donné que l'instruction SQL est inconnue lors de la création du module, le propriétaire du module n'accorde pas automatiquement à l'utilisateur final les droits requis.

- **Objets SQL :** Il peut s'agir de tables, de vues ou de synonymes. Les utilisateurs DB2 pour VM peuvent se voir accorder plusieurs niveaux de droits pour créer, supprimer, modifier ou lire des objets SQL individuels. Ces droits sont requis pour la précompilation des instructions SQL statiques ou l'exécution d'instructions SQL dynamiques.

Sous-système de sécurité

L'utilisation de ce sous-système par le serveur d'applications DB2 pour VM est facultative. Si le serveur d'applications doit identifier le nom de LU du demandeur d'application, VTAM appelle le sous-système de sécurité pour effectuer l'échange de vérification de LU partenaire. La décision d'effectuer une vérification de LU partenaire dépend de la valeur indiquée au paramètre VERIFY de l'instruction APPL VTAM pour la passerelle qui est utilisée par le serveur d'applications DB2 pour VM pour recevoir les demandes entrantes portant sur les bases de données réparties.

Le sous-système de sécurité peut également être appelé par CP pour valider l'ID utilisateur et le mot de passe envoyés par le demandeur d'application. Si RACF est utilisé comme sous-système de sécurité et que vous ne disposez pas d'un profil système RACF, la validation est effectuée par RACF. Si vous disposez d'un profil système RACF, par exemple RACFPROF, utilisez les instructions suivantes pour demander cette validation à RACF :

```
RALTER VMXEVENT RACFPROF DELMEM (APPCPWVL/NOCTL

RALTER VMXEVENT RACFPROF ADDMEM (APPCPWVL/CTL

SETEVENT REFRESH RACFPROF
```

Représentation des données

Vous devez affecter à CHARNAME et au CCSID une valeur par défaut appropriée pour votre installation. L'utilisation de valeurs correctes vous permet d'assurer l'intégrité de la représentation des données alphanumériques et de réduire le temps système associé à la conversion de CCSID.

Par exemple, si votre serveur d'applications DB2 pour VM est accessible aux utilisateurs locaux dont les contrôleurs de terminal sont générés avec la page de codes 37 et le jeu de caractères 697 (CP/CS 37/697) pour l'anglais (Etats-Unis), le serveur d'applications doit affecter par défaut à CHARNAME la valeur ENGLISH. En effet, CP/CS 37/697 correspond au CCSID 37, qui lui-même correspond à la valeur ENGLISH pour CHARNAME.

Pour éviter des conversions de CCSID inutiles, faites en sorte que la valeur par défaut du serveur d'applications soit identique à la valeur par défaut des demandeurs d'application qui ont le plus souvent accès à votre serveur d'applications.

Vous trouverez ci-après un cas où ces deux objectifs peuvent être contradictoires.

- Un serveur d'applications dispose de moins de cinq demandeurs d'application en local (pour les demandeurs d'application VM, le paramètre de protocole doit prendre la valeur SQL/DS), mais plusieurs demandeurs d'application (environ 100) peuvent accéder au serveur d'applications via le protocole DRDA. Les contrôleurs des demandeurs d'application locaux sont définis à l'aide de CP/CS 37/697. Les demandeurs d'application éloignés utilisent le CCSID 285.

  Si la valeur par défaut de CHARNAME pour le serveur d'applications est ENGLISH, l'intégrité des données est assurée pour les demandeurs d'application locaux mais elle génère du temps système supplémentaire pour la conversion du CCSID de tous les demandeurs d'application éloignés.

  Lorsque la valeur par défaut de CHARNAME est UK-ENGLISH, aucun temps système supplémentaire n'est généré pour la conversion du CCSID

de tous les demandeurs d'application éloignés, mais l'intégrité des données n'est pas assurée pour les demandeurs d'application locaux. Par exemple, le symbole de la livre sterling est remplacé par celui du dollar.

Pour afficher le CCSID en cours du système, interrogez la table SYSTEM.SYSOPTIONS. Le CCSID par défaut du serveur d'applications prend généralement la valeur CCSIDMIXED. Si cette valeur est égale à zéro, le CCSID par défaut du système prend la valeur CCSIDSBCS. Les valeurs de CHARNAME, CCSIDSBCS, CCSIDMIXED et CCSIDGRAPHIC de cette table sont remplacées par les valeurs utilisées comme valeurs système par défaut chaque fois que la base de données est démarrée. Les valeurs se trouvant dans cette table ne sont pas toujours les valeurs par défaut du système. Il se peut qu'un utilisateur disposant des droits d'administrateur de bases de données les modifie, bien que ce ne soit pas conseillé. Pour modifier la valeur par défaut du CCSID d'un serveur d'applications, vous devez indiquer le paramètre CHARNAME dans le fichier SQLSTART EXEC lors du prochain démarrage du serveur d'applications. Reportez-vous au manuel *VM/ESA System Administration* pour de plus amples informations.

Si la base de données a été récemment installée pour le serveur d'applications, la valeur par défaut du paramètre CHARNAME est INTERNATIONAL et le CCSID par défaut est 500. Ces valeurs ne sont probablement *pas* correctes pour votre système. La valeur par défaut de CHARNAME pour un système migré est ENGLISH, et le CCSID par défaut est 37.

Liste de contrôle d'activation du serveur d'applications DRDA DB2 pour VM

La liste de contrôle ci-après récapitule les étapes nécessaires à l'activation d'un serveur d'applications DRDA pour les communications DRDA, en supposant que votre système VM est installé, que ACF/VTAM est utilisé comme méthode d'accès en télétraitement et que les définitions VTAM requises pour communiquer avec les systèmes éloignés, telles que les définitions NCP, sont complètes.

1. Définissez la passerelle AVS locale pour VTAM.
2. Créez un serveur de reprise CRR. Vérifiez que le nom de LUNAME spécifié par le serveur de reprise CRR correspond au nom d'une passerelle AVS pouvant traiter les conversations SYNCLVL=SYNCPNT.
3. Installez le support DRDA dans le serveur d'applications DB2 pour VM en utilisant la commande ARISDBMA.
4. Ajoutez une instruction IUCV *IDENT au répertoire CP de la machine serveur VM de sorte qu'elle puisse s'identifier en tant que ressource globale.
5. Définissez les ID utilisateur local et les mots de passe pour CP qui seront utilisés par les demandeurs d'application éloignés. Si nécessaire, mappez

les ID utilisateur éloignés avec les ID utilisateur VM locaux en utilisant la commande AVS AGW ADD USERID.

6. Créez une entrée dans la table de noms de mode VTAM pour chaque mode demandé par un demandeur d'application.
7. Démarrez VTAM et AVS pour que les applications VM puissent communiquer à distance via le réseau SNA.
8. Définissez le nombre maximal de sessions pour tous les systèmes partenaires sur lesquels résident les demandeurs d'application.
9. Démarrez le serveur d'applications DB2 pour VM avec les paramètres DBNAME, PROTOCOL et SYNCPNT. Une fois le gestionnaire de bases de données démarré, vérifiez qu'il s'est identifié comme une ressource GLOBAL.
10. Préparez des applications sur le serveur d'applications DB2 pour VM.

Présentation de DB2 pour VSE

Dans l'environnement d'exploitation VSE/ESA, DB2 pour VSE offre la fonction de serveur d'applications dans un environnement DRDA. La fonction de demandeur d'application n'est pas fournie. La présente section décrit les différents composants DB2 pour VSE et les composants VSE concernés par le traitement de la base de données répartie. Ces composants permettent au système de gestion de bases de données DB2 pour VSE de communiquer avec des demandeurs d'application DRDA éloignés dans un réseau SNA.

CICS(ISC)
Le composant de communication intersystème CICS offre les fonctions de LU 6.2 SNA (APPC) au serveur d'applications DB2 pour VSE.

CICS(SPM)
Le composant de gestion de points de synchronisation CICS fait partie intégrante du support de l'unité d'oeuvre répartie DRDA de DB2 pour VSE. Il agit en tant que participant du point de synchronisation et est chargé de coordonner l'activité de validation en deux phases sur un système VSE/ESA.

CICS(TRUE)
L'exit utilisateur CICS est une interface utilisée par la transaction AXE pour communiquer avec le gestionnaire de points de synchronisation CICS.

ACF/VTAM
CICS(ISC) utilise VTAM pour VSE pour établir les accès des sessions de LU à LU avec des systèmes éloignés ou en définir les accès. DB2 pour VSE utilise les conversations de base de type LU 6.2 sur ces sessions pour communiquer avec les demandeurs d'application DRDA éloignés.

AXE La transaction APPC-XPCC-Exchange est une transaction CICS activée par le demandeur d'application DRDA éloigné. Elle permet d'acheminer les flux de données DRDA entre le demandeur d'application éloigné et le serveur d'applications DB2 pour VSE, à l'aide du support LU 6.2 CICS et des fonctions VSE XPCC.

Répertoire DBNAME
Le répertoire DBNAME (nom de la base de données) mappe une demande entrante pour l'allocation d'une conversation avec un serveur d'applications prédéfini identifié par le nom de programme transactionnel entrant. Reportez-vous au manuel *SQL/DS System Administration Guide for VSE* pour plus de détails.

XPCC La communication interpartition est une interface de macro VSE permettant d'effectuer un transfert de données entre des partitions VSE.

Communications du serveur d'applications - exemple

La figure 35, illustre le rôle joué par chaque composant lors de l'établissement des communications entre le serveur d'applications DB2 pour VSE et le demandeur d'application éloigné.

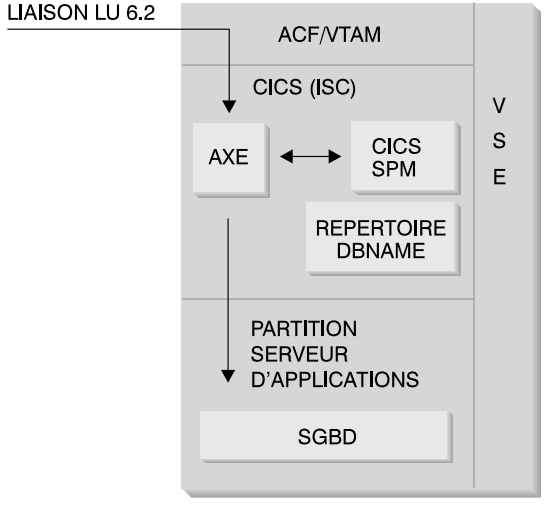

Figure 35. Méthode d'accès au serveur d'applications

Le demandeur d'application émet une instruction APPC ALLOCATE comportant un nom de LU et un nom de programme transactionnel spécifiques pour établir une conversation de type LU 6.2 avec le serveur

d'applications. Le nom de LU permet de diriger la demande ALLOCATE via VTAM vers CICS. Lorsqu'il reçoit l'instruction ALLOCATE, le programme CICS vérifie qu'une transaction AXE est définie avec ce nom de programme transactionnel et émet une demande d'ouverture de session CICS. Si le niveau de sécurité de la conversation pour la connexion CICS est VERIFY, l'ID utilisateur et le mot de passe doivent être transmis par le demandeur d'application et sont utilisés pour l'ouverture de session. Ils doivent figurer dans la table des autorisations d'ouverture de session CICS (DFHSNT) pour que la connexion soit acceptée. Si le niveau de sécurité est IDENTIFY, seul l'ID utilisateur est requis et CICS laisse au système éloigné le soin de contrôler les droits d'accès. Si l'authentification aboutit, CICS démarre la transaction AXE pour l'acheminement des demandes et assure la médiation entre le demandeur d'application et le serveur d'applications. Pour le nom de programme transactionnel utilisé par le demandeur d'application, une entrée doit être définie dans le répertoire DBNAME de DB2 pour VSE afin de désigner un serveur DB2 pour VSE actif dans le système VSE.

Si le demandeur d'application souhaite bénéficier du support d'unité d'oeuvre répartie, il spécifie la valeur SYNCPT pour le paramètre SYNCLVL dans l'instruction APPC ALLOCATE. Une fois la transaction AXE démarrée, elle interroge CICS pour déterminer le niveau de synchronisation de la conversation. S'il s'agit du niveau SYNCPT, elle procède comme suit :

- Si nécessaire, la transaction AXE active le support TRUE de façon à pouvoir communiquer avec le gestionnaire de points de synchronisation CICS.
- Elle enregistre l'unité d'oeuvre logique auprès du gestionnaire de points de synchronisation CICS.

Limitations

A la différence de DB2 pour VM, le serveur d'applications DB2 pour VSE accepte les flux de données DRDA en provenance de demandeurs d'application éloignés. Les protocoles privés ne sont pas pris en charge. Par conséquent, les demandeurs d'application VM ne peuvent pas accéder à un serveur VSE lorsque le paramètre PROTOCOL=SQLDS est défini.

Le serveur DRDA DB2 pour VSE ne peut pas acheminer les demandes issues de demandeurs d'application éloignés vers un serveur DB2 pour VM à l'aide de la fonction de partage d'hôtes VSE. Ces demandes doivent être directement transmises au serveur DRDA DB2 pour VM.

Paramètres de démarrage du serveur d'applications

Paramètre RMTUSERS

L'administrateur de bases de données peut spécifier le paramètre RMTUSERS au démarrage du serveur d'applications pour définir le nombre maximal de demandeurs d'application éloignés autorisés à se connecter au serveur. La

valeur indiquée est assimilable à celle du paramètre MAXCONN définie dans le répertoire VM sur le serveur de bases de données DB2 pour VM. Elle permet d'équilibrer la charge de travail entre les opérations de traitement locales et éloignées.

Lorsque la valeur du paramètre RMTUSERS est supérieure au nombre d'agents DB2 pour VSE disponibles (défini par NCUSER), certains utilisateurs éloignés doivent attendre qu'un agent DB2 pour VSE se libère pour traiter leur demande. En principe, un agent DB2 pour VSE est réaffecté à un utilisateur en attente à la fin d'une unité d'oeuvre logique (LUW). Toutefois, le serveur d'applications DB2 pour VSE prend en charge les accès privilégiés, qui permettent à un utilisateur éloigné de conserver un agent DB2 pour VSE pour l'exécution de plusieurs LUW jusqu'à la fin de la conversation.

Paramètre SYNCPNT

Ce paramètre indique si un gestionnaire de points de synchronisation (SPM) va être utilisé pour coordonner l'activité de lecture et d'écriture multisite de l'unité d'oeuvre répartie DRDA-2.

Si Y est spécifié, le serveur utilise si possible un gestionnaire de points de synchronisation pour coordonner les activités de resynchronisation et de validation en deux phases. Si N est spécifié, le serveur d'applications n'utilise pas de SPM pour exécuter les validations en deux phases et il est limité aux unités d'oeuvre réparties à lecture multisite et à écriture monosite ; il peut constituer ce site unique. Si Y est spécifié, mais que le serveur d'applications ne trouve aucun gestionnaire de points de synchronisation disponible, le serveur fonctionne comme si N avait été indiqué.

La valeur par défaut est SYNCPNT=Y lorsque RMTUSERS est supérieur à zéro. Lorsque RMTUSERS=0, le paramètre SYNCPNT a pour valeur N.

Configuration du serveur d'applications dans un environnement VSE

Le support du serveur d'applications DB2 pour VSE permet à DB2 pour VSE de jouer le rôle de serveur pour les demandeurs d'application DRDA. Les demandeurs d'application susceptibles d'être connectés à un serveur d'applications DB2 pour VSE sont les suivants :

- un demandeur DB2 pour VM
- un demandeur DB2 Universal Database for OS/390
- un demandeur DB2
- un demandeur OS/400
- tout demandeur d'application de la famille DB2, y compris DB2 CONNECT, ou n'importe quel autre produit supportant les protocoles de demandeur d'application DRDA

Définition des données réseau

Les deux opérations suivantes sont nécessaires à l'établissement d'une connexion réseau avec le serveur d'applications VSE :

1. Etablissement de sessions CICS de type LU 6.2 avec les systèmes éloignés
2. Définition du serveur d'applications

Etablissement de sessions CICS de type LU 6.2

Le serveur d'applications DB2 pour VSE utilise des liaisons CICS de type LU 6.2 pour communiquer avec le demandeur d'application. La partition CICS utilisée doit donc disposer de liaisons LU 6.2 avec les systèmes éloignés sur lesquels s'exécutent les demandeurs d'application. Le manuel *CICS/VSE Intercommunications Guide* contient des informations détaillées sur la manière de définir et d'établir des liaisons CICS de type LU 6.2 avec des systèmes éloignés.

Installation de CICS et définition des ressources pour les communications de type LU 6.2 :

1. Installation des modules requis pour ISC.

   Vous devez inclure les modules suivants dans votre système à l'aide d'une table d'initialisation du système (SIT) ou des paramètres de substitution pour l'initialisation :

   - Les programmes d'interface EXEC (indiquez EXEC=YES ou spécifiez la valeur par défaut).
   - Les programmes intersystèmes de communication (indiquez ISC=YES).
   - Le programme de contrôle de terminal généré par DFHSG PROGRAM=TCP. Vous devez disposer d'une version avec les paramètres ACCMETH=VTAM, CHNASSY=YES et VTAMDEV=LUTYPE6.
2. Installez le module Restart Resynchronization Support de CICS

   Si ce module CICS n'a pas été activé lors de l'installation du système CICS, vous devez mettre à jour les tables CICS suivantes pour activer la fonction de resynchronisation de redémarrage de CICS :

```
DFHJCT    Journal Control Table

          A journal used for the CICS system log must be
          defined in the DFHJCT specifying JFILEID=SYSTEM in a
          DFHJCT TYPE=ENTRY macro.

DFHPCT    Program Control Table

          To generate the DFHPCT entry to use the CICS Restart
          Resynchronization capability, enter:

              DFHPCT TYPE=GROUP,FN=RMI
```

```
DFHPPT    Processing Program Table

          To generate the DFHPPT entry to use the CICS Restart
          Resynchronization capability, enter:

              DFHPPT TYPE=GROUP,FN=RMI

DFHSIT    System Initialization Table.

          The DFHSIT macro must include the JCT parameter.
          Specify JCT=YES or JCT=(jj<,....>)  where jj is the
          SUFFIX parameter value specified in th DFHJCT
          TYPE=INITIAL macro defining the CICS system log
          journal data set.
```

3. Définissez CICS sur VTAM pour VSE.

   Pour prendre en charge les connexions LU 6.2, CICS doit être défini sur VTAM pour VSE en tant que noeud principal d'applications. Le nom de noeud principal d'applications qui est codé dans l'instruction APPL VTAM est l'ID APPL de la partition CICS indiquée dans la table SIT par le paramètre APPLID. Il s'agit du nom de LU utilisé par VTAM (et par conséquent, par les partenaires de communication CICS) pour identifier le système CICS.

   Reportez-vous à la figure 36.

```
                 VBUILD  TYPE=APPL
*************************************************************************
*                                                                       *
*    LU Definition for Toronto VSE SQL/DS System                        *
*                                                                       *
*************************************************************************
VSEGATE  APPL  ACBNAME=VSEGATE,
               AUTH=(ACQ,SPO,VPACE),
               APPC=NO,
               SONSCIP=YES,
ESA=30
               MODTAB=RDBMODES,
               PARSESS=YES,
               VPACING=0
```

Figure 36. Exemple de définition APPL VTAM pour CICS

AUTH=(ACQ,SPO,VPACE)
ACQ permet à CICS de disposer de sessions LU 6.2.

SPO permet à CICS d'émettre une commande MODIFY vtamname USERVAR.

VPACE permet de réguler le flux de données intersystèmes.

ESA=30
Indique le nombre d'unités adressables du réseau pour lesquelles

CICS peut établir des sessions. Ce nombre doit inclure le nombre total de sessions parallèles pour ce système CICS.

PARSESS=YES
Indique le support de session parallèle LUTYPE6.

SONSCIP=YES
Indique le support de notification d'interruption de session (SON). Dans certains cas, ce support permet de récupérer une session défectueuse sans intervention de l'opérateur.

APPC=NO
Nécessaire pour permettre à CICS d'utiliser les macro-instructions VTAM. CICS n'émet pas de macro-instructions APPCCMD.

Remarque : SYNCLVL=SYNCPT n'est pas requis car APPC=NO est spécifié. CICS gère toutes les activités au niveau du point de synchronisation pour les unités d'oeuvre réparties.

4. Définissez des liaisons avec les systèmes éloignés à l'aide du protocole LU 6.2.
   a. Définissez toutes les LU éloignées sur CICS.

      Définissez toutes les LU éloignées en utilisant la commande CEDA DEFINE CONNECTION pour la définition des ressources en ligne (RDO) :

      - Spécifiez le nom de LU éloignée au paramètre NETNAME.
      - Spécifiez PROTOCOL=APPC pour vérifier que les protocoles LU 6.2 sont utilisés.
      - Spécifiez AUTOCONNECT=YES et INSERVICE=YES de sorte que la connexion, une fois installée, soit mise en service automatiquement et que les sessions soient acquises automatiquement.
      - Spécifiez le niveau de sécurité des conversations en utilisant le paramètre ATTACHSEC. ATTACHSEC=IDENTIFY est le niveau minimal de sécurité requis par DRDA.
      - Spécifiez le niveau de sécurité des sessions en utilisant le paramètre BINDPASSWORD. Par défaut, aucune sécurité n'est définie au niveau des sessions.

      Pour plus de détails sur la sécurité au niveau des conversations et des sessions, reportez-vous à la section «Définition de la sécurité» à la page 176.

b. Définissez les groupes de sessions LU 6.2 avec le système éloigné.

   Pour chaque connexion définie précédemment, définissez des groupes de sessions parallèles pour chaque liaison à la LU éloignée, en utilisant la commande CEDA DEFINE SESSIONS :

   - Spécifiez le nom de la connexion (définie ci-dessus) dans le paramètre CONNECTION.
   - Spécifiez l'entrée de la table de modes d'ouverture de session VTAM au paramètre MODENAME.
   - Utilisez le paramètre MAXIMUM pour spécifier :
     - Le nombre maximal de sessions
     - Le nombre maximal de sessions à prendre en charge en tant que vainqueurs de conflit

     Spécifiez les valeurs utilisées par le logiciel de communications du demandeur d'application DRDA, par exemple, IBM Communications Server pour OS/2.

   Sachez que le fait de définir des valeurs supérieures pour SENDSize et RECEIVESize peut améliorer la vitesse de transmission des données, mais rendra nécessaire une plus grande quantité de mémoire virtuelle sur le réseau. La taille prise en charge par toutes les couches du réseau SNA est égale à 4 ko. Lors de la configuration du serveur DRDA, vous devez donc attribuer à la taille des tampons d'émission et de réception la valeur de 4 ko. Lorsque des connexions peuvent être établies à partir d'utilisateurs éloignés, définissez ces paramètres pour déterminer la valeur optimale.

c. Définissez les ID utilisateur et les mots de passe pour l'accès à CICS.

   Définissez tous les utilisateurs de la table d'ouverture de session CICS (DFHSNT). Vous pouvez vérifier la validité d'un ID utilisateur en effectuant une connexion CESN à un terminal CICS. La connexion effectuée en local doit aboutir.

d. Définissez les modules de chargement (phases) pour CICS à l'aide de la commande CEDA DEFINE PROGRAM :

   1) ARICAXED - Transaction AXE
   2) ARICDIRD - Répertoire DBNAME et routine de recherche
   3) ARICDAXD - Gestionnaire des transactions DAXP et DAXT
   4) ARICDEBD - Gestionnaire d'activation du support CICS TRUE
   5) ARICDRAD - CICS TRUE
   6) ARICDR2 - Bloc de contrôle DR2DFLT

   Pour chacun de ces éléments, l'option LANGUAGE=ASSEMBLER doit être spécifiée.

e. Pour chaque TPN spécifié par le demandeur d'application, définissez une transaction AXE à l'aide de la commande CEDA DEFINE TRANSACTION :
   - Utilisez le paramètre TRANSACTION pour spécifier le TPN ;
   - Spécifiez PROGRAM=ARICAXED pour indiquer la phase ;
   - Utilisez le paramètre XTRANID pour spécifier un deuxième nom de transaction hexadécimal.

   Définissez également les transactions DAXP et DAXT, en spécifiant PROGRAM=ARICDAXD.

Exemples de définitions : Reportez-vous au manuel *DRDA Connectivity Guide* pour consulter les exemples de définitions.

Définition du serveur d'applications

1. Mettez à jour le répertoire DBNAME de DB2 pour VSE.

   Ajoutez une entrée au répertoire DBNAME pour chaque transaction définie précédemment, en utilisant la commande CEDA DEFINE TRANSACTION. Lorsque des sessions LU 6.2 sont établies, un demandeur d'application éloigné peut démarrer une conversation avec un serveur d'applications DB2 pour VSE. Pour ce faire, il alloue une conversation de type LU 6.2 au serveur d'applications, en indiquant un nom de programme transactionnel (TPN). Ce nom doit être un ID transaction CICS de la transaction AXE chargée d'acheminer les demandes en provenance ou en direction du serveur DB2 pour VSE. Le nom de programme transactionnel doit se trouver dans le répertoire DBNAME de DB2 pour VSE mappé avec le serveur DB2 pour VSE pour être accessible à partir du demandeur d'application. L'administrateur de bases de données DB2 pour VSE se charge de mettre à jour le répertoire DBNAME et d'informer les utilisateurs éloignés du mappage du nom de programme transactionnel avec le serveur.

   Le nom de programme transactionnel et le nom de serveur qui lui est associé (nom de la base de données tel qu'il est défini dans le répertoire DBNAME) doivent être identifiés au niveau du demandeur d'application :
   - Le demandeur d'application utilise le programme transactionnel pour lancer la transaction du routeur AXE.
   - Le demandeur d'application indique le nom de serveur dans le flux DRDA initial comme nom de base de données cible. L'utilisateur du serveur DB2 pour VSE utilise ce nom de serveur pour vérifier que le demandeur d'application accède au serveur approprié. Si le nom du serveur ne correspond pas, le demandeur d'application se voit refuser l'accès au serveur et il met fin à la conversation.
2. Utilisez la procédure ARISBDID pour créer et assembler le répertoire DBNAME (membre ARISDIRD.A).

Pour plus de détails, reportez-vous au manuel *DB2 for VSE System Administration.*

Préparation et démarrage du serveur d'applications DB2 pour VSE

1. La transaction AXE conserve un journal des erreurs qui est dans une file d'attente de stockage temporaire CICS appelé ARIAXELG. Le journal des erreurs contient des messages d'erreur utiles dans lesquels sont consignés les incidents de communication et les fins anormales de sessions DRDA. Définissez ce journal comme «récupérable» à l'aide de TST CICS.
2. Exécutez la procédure ARIS342D pour installer le support serveur d'applications DRDA.
3. Si nécessaire, exécutez la transaction DAXP pour spécifier le mot de passe et la langue par défaut qui seront utilisées lorsque le support TRUE de CICS sera activé pour un serveur donné. Reportez-vous au manuel *DB2 for VSE Operation* pour plus de détails.
4. Démarrez DB2 pour VSE en utilisant les paramètres DBNAME, RMTUSERS et SYNCPNT :
   - Le nom de base de données utilisé (DBNAME) doit être défini dans le répertoire DBNAME.
   - La valeur du paramètre RMTUSERS doit être différente de zéro.
   - Spécifiez SYNCPNT=Y pour activer le support d'unité d'oeuvre répartie.
5. Tous les utilisateurs éloignés doivent disposer de droits accordés par DB2 pour VSE, avec des niveaux différents. Reportez-vous au manuel *DB2 for VSE Database Administration* pour plus de détails.

Identification des incidents :

- Si le demandeur d'application réussit à trouver sa session CICS partenaire avec un nom de programme transactionnel correct (ce nom est défini dans le répertoire DBNAME), une transaction AXE est démarrée. Le nombre d'utilisations du programme ARICAXED est augmenté d'une unité (la vérification peut être effectuée à l'aide de la commande CEMT I PR(ARICAXED)).
- Pour vérifier qu'un ID utilisateur éloigné est établi dans la table d'ouverture de session CICS, effectuez une connexion locale à l'aide de la transaction CESN avec l'ID et le mot de passe de l'utilisateur éloigné. La connexion effectuée en local doit aboutir.
- Lorsque le serveur DB2 pour VSE est actif et qu'une application effectue une activité

d'unité d'oeuvre répartie DRDA-2 pour la première fois, le support TRUE sur un serveur s'active automatiquement. Consultez le message ARI0187I, qui indique que le support TRUE a été activé. Toutefois, si le message ARI0190E s'affiche, indiquant qu'une erreur s'est produite lors de l'activation de TRUE, consultez les éventuels messages d'erreur précédents sur la console.

- Si votre programme d'application DRDA reçoit le code de détection X'08063426' ou X'FFFE0101', cela peut indiquer que CICS ne dispose pas de suffisamment de sessions. CICS peut manquer de sessions si toutes les sessions sont utilisées ou sont en attente de déconnexion, mais la déconnexion n'a pas abouti. CICS peut manquer de sessions s'il existe beaucoup de transactions entrantes simultanées de courte durée. Dans ce cas, augmentez le nombre de sessions spécifiées au paramètre CEDA DEFINE SESSIONS MAXIMUM pour prendre en compte les sessions dont la déconnexion est programmée, mais non encore effectuée.

Définition de la sécurité

Le serveur d'applications DB2 pour VSE dépend de CICS pour la sécurité des communications intersystèmes. CICS offre différents systèmes de sécurité :

- Sécurité au moment de la définition d'accès

  Mise en oeuvre CICS de la vérification LU-LU du niveau de session LU 6.2 SNA. La mise en oeuvre de la sécurité au moment de la définition d'accès est facultative dans l'architecture LU 6.2. En ce qui concerne le serveur d'applications, elle peut être activée en indiquant un BINDPASSWORD dans la commande CEDA DEFINE CONNECTION lors de la définition de la connexion avec le demandeur d'application. Sur le demandeur d'application, la LU partenaire qui sert le demandeur d'application doit également prendre en charge la sécurité au moment de la définition d'accès et utilise le même mot de passe pour la vérification de la LU partenaire.

  Vous pouvez utiliser ce type de sécurité pour empêcher aux systèmes éloignés ne disposant pas des droits requis, d'établir des sessions avec CICS.

- Sécurité de la liaison

  La sécurité de la liaison peut être utilisée pour restreindre les connexions d'un système éloigné (et de son demandeur d'application DRDA résident) à un ensemble de transactions AXE donné.

Par exemple, vous pouvez définir deux transactions AXE : AXE2 avec la clé de sécurité 2 et AXE3 avec la clé de sécurité 3. Une sécurité opérateur de 3 peut être attribuée aux demandeurs d'application d'un système éloigné (par exemple, à l'aide du paramètre OPERSECURITY dans la commande CEDA DEFINE SESSION), ce qui leur permet de se connecter uniquement à AXE3. Cette transaction risque de ne pas disposer d'accès privilégiés au serveur lorsque AXE2 dispose de ces privilèges. Reportez-vous au manuel *DB2 for VSE System Administration* pour consulter une description de l'accès privilégié au serveur d'applications par des demandeurs d'application éloignés.

Reportez-vous au manuel *CICS Intercommunication Guide* pour connaître la manière d'activer la sécurité de la liaison.

- Sécurité utilisateur

  Mise en oeuvre CICS de la sécurité au niveau des conversations LU 6.2 SNA permettant la vérification de l'utilisateur final.

  La sécurité utilisateur valide l'ID utilisateur avec la table d'ouverture de session CICS (DFHSNT) avant d'accepter une demande de démarrage d'une conversation. Par exemple, les demandeurs d'application DRDA non définis dans la table d'ouverture de session CICS ne sont pas admis à se connecter à une transaction AXE pour démarrer une conversation avec le serveur DB2 pour VSE. Le niveau de sécurité utilisateur d'un système éloigné peut être sélectionné dans la commande CEDA DEFINE CONNECTION au moyen du paramètre ATTACHSEC. Les trois niveaux de sécurité de connexion sont les suivants :

  – LOCAL. Non pris en charge par DRDA.
  – IDENTIFY. Correspond à l'option SECURITY=SAME (ou "déjà vérifié") dans LU 6.2. Avec ce niveau de sécurité, CICS laisse au système éloigné la responsabilité de vérifier ses utilisateurs avant de les autoriser à attribuer une conversation au serveur DB2 pour VSE. Seul l'ID utilisateur est requis pour le processus de connexion CICS. Toutefois, si le mot de passe est transmis, CICS l'utilise pour la connexion.
  – VERIFY. Correspond à l'option SECURITY=PGM dans LU 6.2. Lorsque ce niveau de sécurité est sélectionné, CICS s'attend à ce que le système éloigné envoie l'ID utilisateur et le mot de passe lors de l'allocation de la conversation et rejette la connexion si le mot de passe n'est pas indiqué.
- Cryptage obligatoire pour le niveau de session LU 6.2 SNA. Non pris en charge.

Dans la mesure où le serveur d'applications est responsable de la gestion des ressources de bases de données, il détermine les fonctions de sécurité réseau que le demandeur d'application doit fournir. Par exemple, avec un demandeur d'application DB2 pour VM, vous devez enregistrer les besoins en matière de sécurité au niveau des conversations du serveur d'applications dans le répertoire de communications du demandeur d'application en

spécifiant la valeur appropriée dans la marque :security (voir la figure 37).

```
:nick.VSE1     :tpn.TOR3
               :luname.TORGATE VSEGATE
               :modename.IBMRDB
               :security.PGM
               :userid.SALESMGR
               :password.PROFIT
               :dbname.TORONTO3



Où :   TOR3    - ID transaction mappé dans la base de données TORONTO3.
       TORGATE - Passerelle VM/APPC.
       VSEGATE - ID application de la partition CICS/VSE utilisée
                 comme passerelle de TORONTO3.
       SALESMGR/PROFIT - USERID/PASSWORD défini dans le DFHSNT de
                         VSEGATE, et admis pour TORONTO3
       TORONTO3 - Nom spécifié au paramètre de démarrage DBNAME lorsque le
                  serveur d'applications DB2 pour VSE a été démarré (ou que
                  le nom de la base de données par défaut a été déterminé par le
                  répertoire DBNAME si DBNAME a été ignoré lors du démarrage).
```

Figure 37. Exemple d'entrée de répertoire de communications CMS

Sécurité du gestionnaire de bases de données

La conversion d'ID utilisateur n'est pas prise en charge par le serveur d'applications VSE. CICS utilise l'ID utilisateur transmis directement à partir du demandeur.

Après avoir été démarrée par le demandeur d'application, la transaction AXE extrait l'ID utilisateur de CICS et le transfère au serveur DB2 pour VSE. Pour définir le niveau de droit utilisateur requis sur les ressources de bases de données, vous devez mettre à jour l'ID utilisateur dans le catalogue DB2 pour VSE SYSTEM.SYSUSERAUTH.

Le serveur d'applications DB2 pour VSE vérifie si l'ID utilisateur fourni par CICS dispose des droits CONNECT pour accéder à la base de données, et refuse la connexion si ce n'est pas le cas.

En tant que propriétaire des ressources de base de données, le serveur d'applications DB2 pour VSE contrôle les fonctions de sécurité de base de données pour les objets SQL résidant sur le serveur d'applications DB2 pour VSE. L'accès aux objets gérés par DB2 pour VSE est contrôlé via un ensemble de privilèges qui sont accordés aux utilisateurs par l'administrateur système DB2 pour VSE ou le propriétaire de l'objet donné. Le serveur d'applications DB2 pour VSE contrôle deux classes d'objets :

- **Modules :** Les utilisateurs finals individuels sont autorisés à créer, remplacer et exécuter les modules avec l'instruction GRANT de DB2 pour VSE. Lorsqu'un utilisateur final crée un module, il dispose

automatiquement des droits nécessaires pour son exécution ou son remplacement. Les autres utilisateurs finals se voient attribuer de manière spécifique le droit d'exécution du module EXECUTE au niveau du serveur d'applications DB2 pour VSE, à l'aide de l'instruction GRANT EXECUTE. Le privilège RUN peut être accordé à des utilisateurs finals ou à PUBLIC de manière à permettre à tous les utilisateurs finals d'exécuter le module.

Lorsqu'une application est précompilée sur DB2 pour VSE, le module comporte les instructions SQL contenues dans le programme d'application. Ces instructions sont classées comme suit :

- **SQL statique :** Signifie que l'instruction SQL et les objets SQL désignés par cette dernière sont connus au moment de la précompilation de l'application. Le créateur du module doit disposer des droits appropriés pour exécuter chaque instruction SQL statique du module.

  Lorsqu'un utilisateur final dispose des droits d'exécution d'un module, il dispose automatiquement des droits lui permettant d'exécuter chaque instruction SQL statique contenue dans le module. Les utilisateurs finals n'ont donc pas besoin d'utiliser les privilèges d'accès aux tables DB2 pour VSE si le module contient uniquement des instructions SQL statiques.
- **SQL dynamique :** Ce terme décrit une instruction SQL qui n'est pas connue tant que le module n'est pas exécuté. L'instruction SQL est créée par le programme et est précompilée de manière dynamique sur DB2 pour VSE à l'aide de l'instruction SQL PREPARE ou EXECUTE IMMEDIATE. Lorsqu'un utilisateur final exécute une instruction SQL dynamique, il doit disposer des privilèges d'accès aux tables nécessaires à l'exécution de l'instruction SQL. Etant donné que l'instruction SQL est inconnue lors de la création du module, le propriétaire du module n'accorde pas automatiquement à l'utilisateur final les droits requis.

• **Objets SQL :** Il peut s'agir de tables, de vues ou de synonymes. Les utilisateurs DB2 pour VSE peuvent se voir accorder plusieurs niveaux de droits pour créer, supprimer, modifier ou lire des objets SQL individuels. Ce droit est requis pour la précompilation des instructions SQL statiques ou l'exécution d'instructions SQL dynamiques.

Représentation des données

Reportez-vous à la section «Représentation des données» à la page 164.

Liste de contrôle d'activation du serveur d'applications DRDA DB2 pour VSE

La liste de contrôle ci-après récapitule les étapes nécessaires à l'activation d'un serveur d'applications DRDA, en supposant que votre système VSE est installé, que ACF/VTAM est utilisé comme méthode d'accès en télétraitement et que les définitions VTAM requises pour communiquer avec les systèmes éloignés, telles que les définitions NCP, sont complètes.

1. Installez le support ISC et le module Restart Resynchronization Support de CICS.
2. Définissez CICS sur VTAM pour VSE.
3. Assemblez la table VTAM LOGMODE comportant l'entrée IBMRDB.
4. Assemblez la table d'ouverture de session comportant tous les ID utilisateur éloignés et mots de passes définis.
5. Démarrez CICS en indiquant les informations SIT appropriées :
   - ISC=YES
   - TST=YES, ARIAXELG défini comme RECOVERABLE dans le DFHTST et assemblé
   - APPLID=nom de LU (comme défini dans l'instruction APPL VTAM)
6. Définissez les systèmes éloignés pour CICS (RDO peut être utilisé) :
   - CEDA DEF CONNECTION
   - CEDA DEF SESSION
   - CEDA DEF PROGRAM
   - CEDA DEF TRANSACTION

   Toutes les définitions relatives à ces instructions doivent figurer sous un groupe appelé IBMG, par exemple. Installez ce groupe à l'aide de CEDA INSTALL GROUP(IBMG).
7. Mettez à jour le répertoire DBNAME (ARISDIRD.A) :
   - Définissez dans CICS tous les noms de programme transactionnel figurant dans ce répertoire. Les noms de programme transactionnel non définis pour CICS ne peuvent pas être utilisés.
   - Définissez chaque serveur d'applications DRDA DB2 pour VSE dans le répertoire en lui attribuant un nom de programme transactionnel correct.
8. Exécutez la procédure ARISBDID pour assembler le répertoire DBNAME mis à jour.
9. Préparez le serveur DB2 pour VSE :
   - Exécutez la procédure ARIS342D pour installer le support DRDA.
   - Si des applications DB2 pour VSE en ligne (par exemple, ISQL) sont exécutées à partir de la partition CICS, accordez le droit de planification à l'ID application (APPLID) CICS indiqué dans la table SIT CICS.
   - Accordez des droits à tous les utilisateurs éloignés.
10. Si nécessaire, exécutez la transaction CICS DAXP.
11. Démarrez DB2 pour VSE en utilisant le paramètre RMTUSERS approprié et, éventuellement, les paramètres DBNAME et SYNCPNT.
12. Préparez les applications sur le serveur d'applications DRDA VSE.

Annexe A. Incidents de connexion les plus fréquents

La présente annexe répertorie les symptômes les plus fréquents liés aux incidents de connexion se produisant sur le poste de travail DB2 Connect DB2 UDB lors de l'utilisation de DB2 Connect et du serveur d'applications DRDA DB2 UDB :

- «Incidents DB2 Connect les plus fréquents», et
- «Incidents les plus fréquents avec le serveur d'applications DRDA DB2 UDB» à la page 190.

Ces informations ont pour but de vous aider dans le processus de résolution des incidents. Reportez-vous également aux manuels *Guide des messages*, *Troubleshooting Guide* et *DB2 Connect User's Guide*.

Incidents DB2 Connect les plus fréquents

Cette section répertorie les symptômes les plus communs des incidents de connexion se produisant lors de l'utilisation de DB2 Connect. Pour chaque cas, vous trouverez :

- Un numéro de message accompagné du code retour (ou code retour spécifique d'un protocole) correspondant. Chacun de ces couples comporte un en-tête distinct ; ces en-têtes sont classés par numéro de message, puis par code retour.
- Un `symptôme`, fourni en règle générale sous la forme d'un exemple de message.
- Une suggestion de `solution`, indiquant l'origine probable de l'erreur. Dans certains cas, plusieurs solutions sont proposées.

Remarques :

1. Pour obtenir les informations les plus récentes sur les niveaux de correction de logiciel recommandés, reportez-vous au manuel `Mise en route` consacré à votre produit, ainsi qu'aux dernières remarques d'édition publiées.
2. Pour les couples message/code retour propres aux communications APPC, un code de détection est éventuellement renvoyé. Désormais, toutes les informations concernant ce type de code associé à un message particulier doivent être obtenues du sous-système SNA.

   Parfois, vous pouvez consulter les codes de détection SNA par le biais des journaux système. Cela dépend du sous-système SNA utilisé. Dans certaines solutions, vous devrez recréer l'incident avec une trace SNA active afin d'obtenir les informations concernant le code de détection.

3. Le terme `passerelle` fait référence à DB2 Connect Enterprise Edition.

SQL0965 ou SQL0969

Symptôme

Les messages SQL0965 et SQL0969 peuvent être émis avec différents codes retour provenant de DB2 Universal Database pour AS/400, DB2 Universal Database for OS/390, DB2 pour MVS/ESA et DB2 pour VM &VSE.

Lorsque vous recevez l'un de ces messages, recherchez le code SQL initial dans la documentation sur le serveur de base de données émettant le message.

Solution

Le code SQL reçu de la base de données hôte ne peut pas être converti. Remédiez à l'incident en vous fondant sur le code d'erreur, puis relancez la commande qui a échoué.

SQL1338 lors de l'exécution d'une instruction SQL CONNECT

Symptôme / Origine

Le nom de destination symbolique n'a pas été défini ou ne l'a pas été correctement.

Par exemple, cela peut se produire lorsqu'un noeud APPC est utilisé et que le nom de destination symbolique spécifié dans le répertoire de noeuds DB2 ne correspond à aucune entrée CPI-C dans la configuration du sous-système local de communications APPC.

Cela peut également être dû à l'existence de plusieurs piles SNA sur le poste. Vous devrez éventuellement vérifier dans les paramètres PATH et LIBPATH que la pile à utiliser apparaît en première position.

Solutions

1. Vérifiez que le nom de profil des informations de configuration CPI-C associées spécifié dans le répertoire de noeuuds DB2 correspond à la configuration SNA (avec distinction entre les majuscules et les minuscules).
2. Vous devrez éventuellement vérifier dans les paramètres PATH et LIBPATH que la pile à utiliser apparaît en première position.

SQL1403N lors de l'exécution d'une instruction SQL CONNECT

Symptôme

SQL1403N Le nom d'utilisateur et/ou le mot de passe sont incorrects.

Solution

1. L'authentification de l'utilisateur sur le poste DB2 Connect a échoué. Déterminez si l'utilisateur peut être authentifié sur ce poste.

   Si tel est le cas, assurez-vous que le mot de passe correct est indiqué dans l'instruction CONNECT, et modifiez-le si nécessaire.

   Si tel n'est pas le cas, l'entrée du répertoire de bases de données système a probablement été cataloguée de manière incorrecte avec le type d'authentification SERVER (il s'agit de la valeur par défaut, si le paramètre AUTHENTICATION n'a pas été défini explicitement). Vous pouvez alors la recataloguer en indiquant la valeur DCS ou CLIENT pour le type d'authentification.
2. Le mot de passe ne doit pas être envoyé à la base de données cible du serveur. Si l'entrée du répertoire des bases de données système a été catalogué avec le type d'authentification DCS, un mot de passe doit être transmis de DB2 Client à la base de données cible du serveur. Sur certaines plateformes, telle qu'AIX, le mot de passe ne peut être obtenu que s'il a été indiqué dans l'instruction CONNECT.

SQL5043N

Symptôme

Le démarrage du support d'un ou de plusieurs protocoles a échoué. Toutefois, la fonction du gestionnaire de bases de données a pu être démarrée.

Le protocole TCP/IP n'est peut-être pas opérationnel sur la passerelle DB2 Connect. Une connexion client peut avoir abouti auparavant.

Si `diaglevel = 4`, le journal de diagnostic (`db2diag.log`) peut contenir une entrée semblable :

```
   1997-05-30-14.09.55.321092   Instance:svtdbm5   Node:000
PID:10296(db2tcpcm)   Appid:none
common_communication  sqlcctcpconnmgr_child   Probe:46
DIA3205E Socket address "30090" configured in the TCP/IP
services file and
required by the TCP/IP server support is being used by another
process.
```

Solution

Cet avertissement signale que DB2 Connect, agissant en tant passerelle pour des clients éloignés, a des difficultés à traiter un, voire plusieurs protocoles de communications client. Il peut s'agir de TCP/IP, APPC, etc. ; en principe, le message indique que l'un des protocoles de communications définis dans DB2 Connect n'est pas configuré correctement.

Fréquemment, cet incident est dû à l'absence de définition de la variable de profil DB2COMM, ou à sa définition incorrecte. En règle générale, il résulte

d'une disparité entre la variable DB2COMM et les noms définis dans la configuration du gestionnaire de bases de données (par exemple, svcename, nname ou tpname).

Un des scénarios possibles est le suivant : une connexion précédente a abouti, puis vous avez reçu un message d'erreur SQL5043 alors que la configuration n'a pas été modifiée. Cela peut se produire avec le protocole TCP/IP, lorsque le système éloigné met fin de façon anormale à la connexion pour une raison quelconque. Dans ce cas, une connexion peut toujours sembler exister sur le client et vous pourrez peut-être rétablir la connexion sans autre intervention en émettant les commandes mentionnées ci-après.

Il est cependant probable qu'un des clients connectés à la passerelle détient toujours un pointeur sur le port TCP/IP. Sur chaque poste client connecté à la passerelle, lancez :

1. db2 terminate
2. db2stop

SQL30020

Symptôme

SQL30020N L'exécution a échoué en raison d'une erreur de protocole de répartition qui affectera l'exécution des commandes et des instructions SQL suivantes.

Solutions

Prenez contact avec votre support technique.

Recherchez un cliché ffdc (pid.000) dans le répertoire db2dump. Ensuite, formatez ce fichier avec la commande `db2fdump` et recherchez le terme ″ERROR″ dans le résultat obtenu. Un message de fin anormale MVS ABEND y figure peut-être. Si tel est le cas, consultez les messages VMS à la console pour plus de détails et recherchez le code de fin anormale dans le manuel consacré aux codes et messages MVS.

SQL30060

Symptôme

SQL30060N L'″<id-autorisation>″ ne dispose pas du privilège permettant d'exécuter l'opération ″<opération>″.

Solution

Lors de la connexion à DB2 pour MVS ou DB2 pour OS/390, les tables de la base de données de communications n'ont pas été mises à jour correctement. Reportez-vous aux manuels :

- `DB2 Connect - Mise en route`

SQL30061

Symptôme

Le nom ou l'alias de base de données est introuvable sur le serveur de bases de données hôte ou AS/400.

Solution

Un nom de base de données serveur incorrect peut avoir été indiqué dans l'entrée du répertoire DCS. Dans ce cas, SQLCODE -30061 est renvoyé à l'application.

Vérifiez le noeud, la base de données DB2 et les entrées du répertoire DCS. La valeur indiquée dans la zone du nom de base de données cible figurant dans l'entrée du répertoire DCS doit être identique au nom de la base de données résidant sur la plateforme. Ainsi, pour une base de données DB2 Universal Database for OS/390, le nom à utiliser doit être le même que celui indiqué dans la zone "LOCATION=nomempl" du fichier d'amorçage (BSDS), nom également fourni dans le message DSNL004I (LOCATION=emplacement) lors du démarrage de la fonction DDF (Distributed Data Facility).

Le manuel Mise en route de DB2 Connect correspondant à votre plateforme contient des exemples de mise à jour des catalogues DB2. Reportez-vous à la section "Mise à jour des répertoires DB2" de chaque chapitre décrivant la configuration SNA, ou au chapitre "Configuration des bases de données hôte ou AS/400 pour DB2 Connect", ou à la section "Configuration de TCP/IP".

Les commandes pouvant être utilisées avec un noeud APPC ou APPN sont les suivantes :

```
db2 catalog appc node <nom-noeud> remote <nom-dest-symb> security program
db2 catalog dcs database <nom-local> as <nom-bdd-réelle>
db2 catalog database <nom-local> as <alias> at node <nom-noeud>
            authentication dcs
```

Les commandes pouvant être utilisées avec un noeud TCP/IP sont les suivantes :

```
db2 catalog tcpip node <nom-noeud> remote <nom-ou-adresse-hôte>
            server <num-port_ou_nom-service>
db2 catalog dcs database <nom-local> as <nom-bdd-réelle>
db2 catalog database <nom-local> as <alias> at node <nom-noeud>
            authentication dcs
```

Pour vous connecter à la base de données, lancez ensuite la commande suivante :

```
db2 connect to <alias> user <nom-utilisateur> using <mot-de-passe>
```

SQL30073 avec code retour 119C lors de l'exécution d'une instruction SQL CONNECT

Symptôme

Le message SQL30073 a été envoyé avec un code retour 119C. Cela se produit lorsque la base de données cible du serveur ne prend pas en charge la page de codes utilisée par le client DB2 (via DB2 Connect). La page de codes est dérivée de la configuration de l'environnement d'exploitation dans lequel s'exécute le client DB2.

Pour plus de détails, reportez-vous au manuel *Administration Guide*.

Solution

En règle générale, vous pouvez remédier à cet incident en installant une PTF sur le système de bases de données serveur. Prenez contact avec le support technique approprié pour obtenir et appliquer toute PTF éventuellement conseillée pour supprimer ce symptôme.

Comme solution temporaire, l'utilisateur peut remplacer la page de codes par défaut en définissant la variable d'environnement DB2CODEPAGE. Pour ce faire, vérifiez l'environnement local ou adoptez la valeur 850.

Sur les plateformes UNIX, l'utilisateur peut éventuellement adopter une page de codes différente en définissant la variable d'environnement LANG par une autre valeur.

SQL30081N avec code retour 1

Symptôme

Le symptôme est constitué du message suivant accompagné d'un code de détection SNA :

```
  db2 connect to <nom-bdd> user <id-utilisateur>
  Enter password for <id-utilisateur>:
SQL30081N  Erreur de communication détectée.
   Protocole de communication
: "APPC".
   API de communication : "CPI-C".
   Emplacement en erreur
: "".
   Fonction de communication ayant détecté l'erreur
:
 "cmallc".
  Codes d'erreur spécifiques du protocole : "1", "*", "0x10030021".
   SQLSTATE=08001
```

Solution(s)

Dans le présent exemple, le code de détection est 10030021.

Les codes de détection les plus fréquents associés à ce message d'erreur et la solution recommandée dans chaque cas sont les suivants :

1. `SQL30081N avec code retour 1 et code de détection SNA 0877002C`

   Spécification d'un nom de réseau incorrect.

2. `SQL30081N avec code retour 1 et code de détection SNA ffff0003`

   Spécification d'une adresse MAC incorrecte ou liaison SNA non active.

3. `SQL30081N avec code retour 1 et code de détection SNA 10030021`

   Inadéquation du type de LU.

4. `SQL30081N avec code retour 1 et code de détection SNA 084B6031`

   Définition par la valeur 0 de MAXDBAT dans le paramètre DSNZPARM (sur un hôte DB2 pour MVS ou DB2 pour OS/390).

Autres suggestions :

1. Lors de la création du profil de la LU locale, définissez celle-ci en tant que LU par défaut. Par exemple, dans la liste des fonctions de CM/2, procédez comme suit :
   - Cochez la case 'Use this local LU as your default local LU alias', ou
   - Définissez la variable de profil ou d'environnement `APPCLLU` sur le système passerelle DB2 Connect Enterprise Edition par le nom de LU locale. Pour ce faire, vous pouvez modifier le fichier CONFIG.SYS, sous OS/2, ou utiliser le Panneau de configuration, sous Windows NT.
2. Vérifiez que le protocole SNA est opérationnel sur la passerelle DB2 Connect.
3. En cas d'utilisation de DB2 pour MVS ou de DB2 pour OS/390, vérifiez que l'espace adresse DDF (Distributed Data Facility) est démarré et que DB2 est opérationnel.

SQL30081N avec code retour 2

Symptôme

Le message SQL30081N est envoyé avec un code retour 2 et un code de détection SNA 08120022.

Solution

Le paramètre NUMILU sur NCP (extrémité hôte de la liaison) est peut-être défini par la valeur par défaut (0). Vérifiez-le, et, le cas échéant, changez cette valeur avant d'effectuer une nouvelle tentative après validation de la modification.

SQL30081N avec code retour 9

Symptôme

Vous recevez le message suivant (le code de détection SNA n'est pas indispensable dans ce cas) :

```
   db2 connect to <nom-bdd> user <id-utilisateur>
SQL30081N  Erreur de communication détectée.
   Protocole de communication : "APPC".
   API de communication : "CPI-C".
   Emplacement en erreur : "".
   Fonction de communication ayant détecté l'erreur :  "cmsend".
   Codes d'erreur spécifiques du protocole : "9", "*", "0x10086021".
   SQLSTATE=08001
```

Solution

L'origine de l'incident est la suivante : le nom du programme transactionnel (TPNAME) n'a pas été défini correctement sur le système DB2 Connect. Par exemple, vous avez modifié votre configuration SNA mais vous ne l'avez pas encore vérifiée sur la passerelle DB2 Connect. Pour de plus amples renseignements, consultez les manuels *DB2 Connect Enterprise Edition pour OS/2 et Windows - Mise en route* ou *DB2 Connect Personal Edition - Mise en route*.

SQL30081N avec code retour 10

Symptôme

Vous recevez le message suivant (le code de détection SNA n'est pas indispensable dans ce cas) :

```
SQL30081N  Erreur de communication détectée.
   Protocole de communication : "APPC".
   API de communication : "CPI-C".
   Emplacement en erreur : "".
   Fonction de communication ayant détecté l'erreur : "cmrcv".
   Codes d'erreur spécifiques du protocole : "10", "*", "*".
   SQLSTATE=08001
```

Solution

Vérifiez que DB2 est installé correctement.

Si vous utilisez la passerelle DB2 Connect pour OS/2, le message suivant peut s'afficher si le nom TP est mal défini :

```
   Codes d'erreur spécifiques du protocole : "10", "*", "0x084C0000".
   SQLSTATE=08001
```

Par exemple, dans ce cas, sous CM/2, il doit être défini comme suit :

```
Transaction program name        = 'nompt' (défini par l'utilisateur)
OS/2 program path and file name = notused
```

et (sur l'écran de configuration CM/2 suivant)

```
Presentation type - background
Operation type - Queued, operator preloaded
```

SQL30081N avec code retour 20

Symptôme

```
SQL30081N  Erreur de communication détectée.
Protocole de communication : "APPC".
API de communication : "CPI-C".
Emplacement en erreur : "".
Fonction de communication ayant détecté l'erreur : "xcstp".
Codes d'erreur spécifiques du protocole : "20", "*", "*".
SQLSTATE=08001
```

Solution

Vérifiez que le sous-système SNA est opérationnel sur le système DB2 Connect.

SQL30081N avec code retour 27

Symptôme

Le message SQL30081N est envoyé avec un code retour 27 et un code de détection SNA 800Axxxx.

Solution

La taille de l'unité d'information acheminable (PIU) VTAM est trop grande.

SQL30081N avec code retour 79

Symptôme

```
SQL30081N  Erreur de communication détectée.
Protocole de communication : "TCP/IP".
API de communication : "SOCKETS".
Emplacement en erreur : "".
Fonction de communication ayant détecté l'erreur : "connect".
Codes d'erreur spécifiques du protocole : "79", "*", "*".
SQLSTATE=08001
```

Solution(s)

Cette erreur peut se produire lorsqu'un client éloigné n'a pas réussi à se connecter à une passerelle DB2 Connect ou lors de la connexion à un hôte à partir d'une passerelle DB2 Connect.

1. La variable profil `DB2COMM` peut avoir été définie de façon incorrecte sur la passerelle DB2 Connect. Vérifiez-le. Par exemple, la commande `db2set`

db2comm=tcpip doit apparaître dans le fichier sqllib/db2profile lors de l'exécution de DB2 Extended Enterprise Edition sous AIX.

2. Il peut avoir une disparité entre le nom de service ou numéro de port TCP/IP indiqué sur le client DB2 et celui spécifié sur la passerelle DB2 Connect. Vérifiez les entrées correspondantes dans les fichiers services TCP/IP résidant sur les deux postes.
3. Vérifiez que DB2 est opérationnel sur la passerelle DB2 Connect. Définissez le paramètre de configuration du gestionnaire de bases de données diaglevel par la valeur 4, en lançant la commande suivante :

   ```
   db2 update dbm cfg using diaglevel 4
   ```

   Après avoir arrêté puis redémarré DB2, vérifiez dans le fichier db2diag.log que le démarrage des communications DB2 TCP/IP a bien abouti. Il doit apparaître un résultat semblable à ceci :

   ```
   1998-02-03-12.41.04.861119   Instance:svtdbm2   Node:00
   PID:86496(db2sysc)   Appid:none
   common_communication  sqlcctcp_start_listen   Probe:80
   DIA3000I "TCPIP" protocol support was successfully started.
   ```

SQL30081N avec un code erreur spécifique du protocole 10032

Symptôme

```
SQL30081N  Erreur de communication détectée.
Protocole de communication : "TCP/IP".
API de communication : "SOCKETS".
Emplacement en erreur : "9.21.85.159".
Fonction de communication ayant détecté l'erreur :  "send".
Codes d'erreur spécifiques du protocole : "10032",    "*", "*".
SQLSTATE=08001
```

Solution

Vous pouvez recevoir ce message d'erreur lors d'une tentative de déconnexion d'un poste sur lequel des communications TC/IP ont déjà échoué. Remédiez à l'incident sur le sous-système TCP/IP.

Sur la plupart des postes, il suffit de redémarrer le protocole TCP/IP sur le poste pour résoudre le problème. Parfois, il faut relancer la totalité du poste.

Incidents les plus fréquents avec le serveur d'applications DRDA DB2 UDB

Cette section répertorie les incidents les plus fréquents se produisant lors de l'utilisation du serveur d'applications DRDA DB2 UDB.

Erreurs de communication lors de l'exécution d'une instruction SQL CONNECT

Vérifiez que les éléments suivants sont définis correctement sur l'extrémité (poste) DB2 UDB.

APPC/SNA LU 6.2

1. Configuration SNA

   Vérifiez que le nom du programme transactionnel est défini, si nécessaire.

   Vérifiez également que le niveau de sécurité SAME est activé pour la LU du demandeur d'application, s'il doit être utilisé à partir du demandeur d'application DRDA.
2. Paramètre TPNAME de configuration du gestionnaire de bases de données
3. Variable d'environnement DB2COMM définie pour inclure APPC

Vérifiez que la commande db2start aboutit sans émettre d'avertissement.

TCP/IP

1. Fichier Services
2. Paramètre SVCENAME de configuration du gestionnaire de bases de données
3. Variable d'environnement DB2COMM définie pour inclure TCPIP. Vérifiez que la commande db2start aboutit sans émettre d'avertissement.

Erreur DRDA lors de l'exécution d'une instruction SQL CONNECT

APPC/SNA LU 6.2

Si vous utilisez SNA Server pour AIX, vérifiez que le nom de groupe de l'exécutable "/sqllib/adm/db2sysc" est spécifié dans la zone "Trusted group names" du profil "SNA System Defaults" de la configuration SNA.

TCP/IP

Si le demandeur d'application DRDA est DB2 pour OS/390, vérifiez que les PTF suivantes ont été appliquées : APAR PQ05771/PTF UQ06843 et APAR PQ07537/PTF UQ09146.

Erreur Base de données introuvable lors de l'exécution d'une instruction SQL CONNECT

Vérifiez que le demandeur d'application DRDA est configuré avec l'alias de la base de données cible DB2 UDB.

Erreur de sécurité lors de l'exécution d'une instruction SQL CONNECT sur APPC/SNA LU 6.2

Il existe des éléments spécifiques à prendre en compte lors de la définition du paramètre AUTHENTICATION dans la configuration du gestionnaire de bases de données DB2 UDB, si la connexion établie à partir d'un demandeur d'application DRDA s'effectue sur APPC/SNA LU 6.2. Si une erreur de sécurité se produit, vérifiez que ce paramètre de configuration est défini correctement, comme suit :

1. Client

Avec cette valeur, les connexions dotées du niveau de sécurité SAME et PROGRAM aboutiront.

2. Serveur

   Avec cette valeur, seules aboutiront les connexions dotées du niveau de sécurité PROGRAM établies vers le serveur d'applications DRDA DB2 UDB sous AIX avec SNA Server et sous OS/2 avec CS/2 version 4 (SPM étant configuré).

3. DCS

   L'option AUTHENTICATION DCS peut maintenant être utilisée avec le serveur d'applications DRDA DB2 UDB Version 7 pour l'établissement de connexions APPC par des clients DRDA utilisant le niveau de sécurité SAME (aucun mot de passe requis), tout en appliquant le type d'authentification SERVER (exigeant un mot de passe) pour les demandes de tous les autres clients.

   Avec cette valeur, les configurations suivantes sont admises :

   a. Serveur d'applications DRDA DB2 UDB sous AIX avec SNA Server et sous OS/2 avec CS/2 V4 (SPM étant configuré) :

      ```
      Security SAME
      ```

   b. Serveur d'applications DRDA DB2 UDB sous OS/2 avec CM/2 1.11, Windows NT et Sun Solaris :

      ```
      Security SAME ou PROGRAM
      ```

Ces différences sont dues au fait que certains sous-systèmes de communication ne soumettent pas de mot de passe entrant à DB2 UDB.

Erreurs lors de l'exécution d'une instruction SQL BIND

Vous pouvez recevoir un message SQLCA avec un code SQL 4930 si une option BIND spécifiée par le serveur d'applications DRDA n'est pas prise en charge. La zone SQLERRMC affiche des informations sur l'option BIND à l'origine de l'incident.

Annexe B. Remarques

Le présent document peut contenir des informations ou des références concernant certains produits, logiciels ou services IBM non annoncés dans ce pays. Pour plus de détails, référez-vous aux documents d'annonce disponibles dans votre pays, ou adressez-vous à votre partenaire commercial IBM. 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 brevets couvrant les produits mentionnés dans le présent document. La remise de ce document ne vous 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 :

IBM EMEA Director of Licensing
IBM Europe Middle-East Africa
Tour Descartes
La Défense 5
2, avenue Gambetta
92066 Paris-La Défense Cedex 50
France

Pour le Canada, veuillez adresser votre courrier à :

IBM Director of Commercial Relations
IBM Canada Ltd
3600 Steeles Avenue East
Markham, Ontario
L3R 9Z7
Canada

Les informations sur les licences concernant les produits utilisant un jeu de caractères double octet peuvent être obtenues par écrit à l'adresse suivante :

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japon

Le paragraphe suivant ne s'applique ni au Royaume-Uni, ni dans aucun pays dans lequel il serait contraire aux lois locales : LE PRESENT DOCUMENT EST LIVRE «EN L'ETAT». IBM DECLINE TOUTE RESPONSABILITE, EXPRESSE OU IMPLICITE, RELATIVE AUX INFORMATIONS QUI Y SONT CONTENUES, Y COMPRIS EN CE QUI CONCERNE LES GARANTIES DE QUALITE MARCHANDE OU D'ADAPTATION A VOS BESOINS. Certaines juridictions n'autorisent pas l'exclusion des garanties implicites, auquel cas l'exclusion ci-dessus ne vous sera pas applicable.

Le présent document peut contenir des inexactitudes ou des coquilles. Il est mis à jour périodiquement. Chaque nouvelle édition inclut les mises à jour. IBM peut modifier sans préavis les produits et logiciels décrits dans ce document.

Les références à des sites Web non IBM sont fournies à titre d'information uniquement et n'impliquent en aucun cas une adhésion aux données qu'ils contiennent. Les éléments figurant sur ces sites Web ne font pas partie des éléments du présent produit IBM et l'utilisation de ces sites relève de votre seule responsabilité.

IBM pourra utiliser ou diffuser, de toute manière qu'elle jugera appropriée et sans aucune obligation de sa part, tout ou partie des informations qui lui seront fournies.

Les licenciés souhaitant obtenir des informations permettant : (i) l'échange des données entre des logiciels créés de façon indépendante et d'autres logiciels (dont celui-ci), et (ii) l'utilisation mutuelle des données ainsi échangées, doivent adresser leur demande à :

IBM Canada Limited
Office of the Lab Director
1150 Eglinton Ave. East
North York, Ontario
M3C 1H7
CANADA

Ces informations peuvent être soumises à des conditions particulières prévoyant notamment le paiement d'une redevance.

Le logiciel sous licence décrit dans ce document et tous les éléments sous licence disponibles s'y rapportant sont fournis par IBM conformément aux termes du Contrat sur les produits et services IBM, des Conditions internationales d'utilisation des logiciels IBM ou de tout autre accord équivalent.

Les données de performance indiquées dans ce document ont été déterminées dans un environnement contrôlé. Par conséquent, les résultats peuvent varier de manière significative selon l'environnement d'exploitation utilisé. Certaines mesures évaluées sur des systèmes en cours de développement ne sont pas garanties sur tous les systèmes disponibles. En outre, elles peuvent résulter d'extrapolations. Les résultats peuvent donc varier. Il incombe aux utilisateurs de ce document de vérifier si ces données sont applicables à leur environnement d'exploitation.

Les informations concernant des produits non IBM ont été obtenues auprès des fournisseurs de ces produits, par l'intermédiaire d'annonces publiques ou via d'autres sources disponibles. IBM n'a pas testé ces produits et ne peut confirmer l'exactitude de leurs performances ni leur compatibilité. Elle ne peut recevoir aucune réclamation concernant des produits non IBM. Toute question concernant les performances de produits non IBM doit être adressée aux fournisseurs de ces produits.

Toute instruction relative aux intentions d'IBM pour ses opérations à venir est susceptible d'être modifiée ou annulée sans préavis, et doit être considérée uniquement comme un objectif.

Ce document peut contenir des exemples de données et des rapports utilisés couramment dans l'environnement professionnel. Ces exemples mentionnent des noms fictifs de personnes, de sociétés, de marques ou de produits à des fins illustratives ou explicatives uniquement. Toute ressemblance avec des noms de personnes, de sociétés ou des données réelles serait purement fortuite.

LICENCE DE COPYRIGHT :

Le présent logiciel peut contenir des exemples de programmes d'application en langage source destinés à illustrer les techniques de programmation sur différentes plateformes d'exploitation. Vous avez le droit de copier, de modifier et de distribuer ces exemples de programmes sous quelque forme que ce soit et sans paiement d'aucune redevance à IBM, à des fins de développement, d'utilisation, de vente ou de distribution de programmes d'application conformes aux interfaces de programmation des plateformes pour lesquelles ils ont été écrits ou aux interfaces de programmation IBM. Ces exemples de programmes n'ont pas été rigoureusement testés dans toutes les conditions. Par conséquent, IBM ne peut garantir expressément ou implicitement la fiabilité, la maintenabilité ou le fonctionnement de ces programmes.

Toute copie totale ou partielle de ces programmes exemples et des oeuvres qui en sont dérivées doit comprendre une notice de copyright, libellée comme suit :

© (nom de votre société) (année). Des segments de code sont dérivés des Programmes exemples d'IBM Corp. © Copyright IBM Corp. _indiquez l'année ou les années_. All rights reserved.

Marques

Les termes qui suivent, accompagnés d'un astérisque (*) dans le document, sont des marques d'International Business Machines Corporation dans certains pays.

ACF/VTAM
AISPO
AIX
AIX/6000
AIXwindows
AnyNet
APPN
AS/400
BookManager
CICS
C Set++
C/370
DATABASE 2
DataHub
DataJoiner
DataPropagator
DataRefresher
DB2
DB2 Connect
DB2 Extenders
DB2 OLAP Server
DB2 Universal Database
Distributed Relational Database Architecture
DRDA
eNetwork
Extended Services
FFST
First Failure Support Technology
IBM
IMS
IMS/ESA
LAN DistanceMVS
MVS/ESA
MVS/XA
Net.Data
OS/2
OS/390
OS/400
PowerPC
QBIC
QMF
RACF
RISC System/6000
RS/6000
S/370
SP
SQL/DS
SQL/400
System/370
System/390
SystemView
VisualAge
VM/ESA
VSE/ESA
VTAM
WebExplorer
WIN-OS/2

Les termes qui suivent sont des marques d'autres sociétés :

Microsoft, Windows et Windows NT sont des marques de Microsoft Corporation dans certains pays.

Java, ou toutes les marques et logos incluant Java, et Solaris sont des marques de Sun Microsystems, Inc.

Tivoli et NetView sont des marques de Tivoli Systems Inc. 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 sont propriétaires des autres marques, noms de produits ou logos accompagnés de deux astérisques (**) qui pourraient apparaître dans ce document.

Index

E

F

G

I

L

M

N

O

P

R

S

T

U

V

W

X

Comment prendre contact avec IBM

Si votre question est d'ordre technique, étudiez tout d'abord les solutions présentées dans le manuel *Troubleshooting Guide* avant de prendre contact avec le Service clients DB2. Ce manuel indique les informations susceptibles d'aider le Service clients à mieux répondre à vos besoins.

Pour obtenir des informations ou commander des produits DB2 avant de prendre contact avec le Service clients DB2 Universal Database, prenez contact avec votre partenaire commercial IBM.

Aux États-Unis, composez l'un des numéros suivants :

- 1-800-237-5511 pour obtenir le Service clients,
- 1-888-426-4343 pour connaître les options de service disponibles.

Infos produit

Aux États-Unis, composez l'un des numéros ci-après.

- Pour commander des produits ou obtenir des informations générales, composez le 1-800-IBM-CALL (1-800-426-2255) ou 1-800-3IBM-OS2 (1-800-342-6672).
- Pour commander des manuels, composez le 1-800-879-2755.

http://www.ibm.com/software/data/
Les pages DB2 World Wide Web fournissent des informations sur DB2, des descriptions de produit, les programmes de formation et d'autres informations.

http://www.ibm.com/software/data/db2/library/
DB2 Product and Service Technical Library permet d'accéder à des forums Q&A (questions/réponses), d'obtenir des correctifs et les dernières informations techniques sur DB2.

Remarque : (Il est possible que ces informations ne soient disponibles qu'en anglais.)

http://www.elink.ibmlink.ibm.com/pbl/pbl/
Le site Web de commande internationale de manuels fournit les informations correspondantes.

http://www.ibm.com/education/certify/
Le programme Professional Certification Program du site Web IBM fournit des informations sur les tests de certification concernant différents produits IBM, dont DB2.

ftp.software.ibm.com
Établissez une connexion anonyme. Des démonstrations, des correctifs, des informations et des outils associés à DB2 ou à des produits connexes sont disponibles dans le répertoire /ps/products/db2.

comp.databases.ibm-db2, bit.listserv.db2-l
Ces newsgroups sont accessibles à tous ceux qui souhaitent partager leurs expériences sur les produits DB2.

Sur Compuserve : GO IBMDB2
Exécutez cette commande pour accéder aux forums IBM DB2. Tous les produits DB2 sont pris en charge sur ces forums.

En dehors des Etats-Unis, pour savoir comment prendre contact avec IBM, consultez l'annexe A du manuel *IBM Software Support Handbook*. Pour accéder à ce document, allez sur le site Web : http://www.ibm.com/support/, puis effectuez une recherche sur le mot clé «handbook».

Remarque : Dans certains pays, les distributeurs agréés peuvent contacter leur centre d'assistance au lieu de prendre contact avec le centre de support IBM.

Référence: SDB2-CONN-SU