Приложение за свързваемост

Версия 7

CONN–SUPP–00

Приложение за свързваемост

Версия 7

CONN–SUPP–00

Преди да използвате тази информация и продукта, за който тя се отнася, задължително прочетете общата информация със заглавие Приложение B, “Забележки” на страница 153.

Може да поръчате тези ръководства чрез представителството или офиса на IBM във вашата страна или като позвъните на телефон 1-800-879-2755 в САЩ или на телефон 1-800-IBM-4YOU в Канада.

Съдържание

Добре дошли в Приложението за свързваемост! v

Как е структурирана тази книга v
За кого е предназначена тази книга v
Други източници на информация vi

Глава 1. Свързване на DB2 за MVS/ESA в DRDA мрежа 1

DB2 за MVS/ESA 1
DB2 за MVS/ESA реализация 3
Настройка на рикуестър за приложения 6
Осигуряване на мрежова информация 7
Осигуряване на защита 16
Представяне на данни 21
Настройка на сървъра на приложения 21
Осигуряване на мрежова информация 22
Осигуряване на защита 27
Представяне на данни 33

Глава 2. Свързване на DB2 Universal Database за OS/390 в DRDA мрежа . 35

DB2 Universal Database за OS/390 35
DB2 Universal Database за OS/390 реализация 37
Допълнителни усъвършенствания на защитата . 40
Настройка на рикуестър за приложения 41
Осигуряване на мрежова информация 42
Осигуряване на защита 56
Представяне на данни 62
Настройка на сървъра на приложения 62
Осигуряване на мрежова информация 63
Осигуряване на защита 66
Осигуряване на мрежова защита 68
Защита на мениджъра на базата данни 70
Подсистема за защита 71
Представяне на данни 72

Глава 3. Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на SNA 73

DB2 Universal Database за AS/400 реализация 73
Настройка на рикуестър за приложения 73
Осигуряване на мрежова информация 74
Осигуряване на защита 79
Представяне на данни 81
Настройка на сървъра на приложения 82
Осигуряване на мрежова информация 83
Осигуряване на защита 83
Представяне на данни 86

Глава 4. Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на TCP/IP 89

Обобщение на информацията за DB2 Universal Database за AS/400 89
Съображения при настройка и използване на DB2 Universal Database за AS/400 DRDA TCP/IP сървър . 90
Съображения при настройка на DB2 Universal Database за AS/400 DRDA TCP/IP клиент 91
Съображения за защитата при използване на DRDA през TCP/IP 92

Глава 5. Допълнителни съображения при DB2 Universal Database за AS/400 и DB2 Universal Database 95

Глава 6. Свързване на DB2 за VSE & VM в DRDA мрежа 99

Преглед на DB2 за VM 99
Пример за комуникационен поток в рикуестър за приложения 101
Пример за комуникационни потоци на сървър на приложения 103
DB2 за VM реализация 105
Опции при предварителна обработка или изпълнение на приложение 105
Опции за стартиране на сървър на база данни 107
Настройка на рикуестър за приложения във VM обкръжение 108
Осигуряване на мрежова информация 109
Осигуряване на защита 115
Представяне на данни 119
Списък за активиране на DB2 за VM DRDA рикуестър за приложения 120
Настройка на сървър на приложения във VM обкръжение 121
Осигуряване на мрежова информация 121
Осигуряване на защита 123
Представяне на данни 126
Списък за активиране на DB2 за VM DRDA сървър на приложения 127
DB2 за VSE Преглед 128
Пример за комуникационни потоци на сървър на приложения 129
Ограничения 130
Параметри за стартиране на сървър на приложения 130
Параметърът RMTUSERS 130
Параметърът SYNCPNT 130
Настройка на сървър на приложения във VSE обкръжение 131
Осигуряване на мрежова информация 131
Осигуряване на защита 136
Представяне на данни 139
Списък за активиране на DB2 за VSE DRDA сървър на приложения 139

Приложение A. Най–разпространени проблеми при свързване 141
Най–чести проблеми в DB2 Connect 141
SQL0965 или SQL0969 141
SQL1338 по време на CONNECT 142
SQL1403N по време на CONNECT 142
SQL5043N 143
SQL30020 143
SQL30060 144
SQL30061 144
SQL30073 с код на връщане 119C при CONNECT 145
SQL30081N с код на връщане 1 145
SQL30081N с код на връщане 2 146
SQL30081N с код на връщане 9 147
SQL30081N с код на връщане 10 147
SQL30081N с код на връщане 20 148
SQL30081N с код на връщане 27 148
SQL30081N с код на връщане 79 148
SQL30081N със специфичен за протокола код за грешка 10032 149
Най–разпространени проблеми с DB2 UDB DRDA AS 149
Комуникационни грешки при CONNECT . . . 149
DRDA грешка при CONNECT 150
Грешка, че не е открита база данни при CONNECT 150
Грешка от защитата при CONNECT през APPC/SNA LU 6.2 150
Грешки при BIND 151

Приложение B. Забележки 153
Търговски марки 155

Индекс 157

Свързване с IBM 159
Информация за продукти 159

Добре дошли в Приложението за свързваемост!

В тази книга ще намерите допълнителна информация, която ще ви помогне при инсталиране и конфигуриране на различните разновидности DB2 релационни СУБД като DRDA рикуестъри или сървъри на приложения. Тази информация може да ви помогне да настроите:

- Сървъри IBM DB2 Universal Database (UDB) Версия 7, които работят като DRDA сървъри на приложения (AS).
- Рикуестъра за приложения IBM DB2 Connect Версия 7 (AR).
- Други DRDA продукти.

Информацията в тази книга се осигурява като допълнение към информацията в следните ръководства:

- *Бърз старт* за DB2 Universal Database Enterprise Edition Версия 7
- *Бърз старт* за DB2 Universal Database Extended – Enterprise Edition Версия 7
- *Бърз старт* за DB2 Connect Enterprise Edition Версия 7
- *Бърз старт* за DB2 Connect Personal Edition Версия 7.

За най–новата и най–актуална информация за хост продуктите (DB2 Universal Database за OS/390, DB2 Universal Database за AS/400 и DB2 за VSE и VM) трябва да се обърнете към документацията, която сте получили с тях.

Информация за конфигуриране на DB2 мениджър за синхронизация (SPM) за многосайтови обновявания потърсете в електронната публикация *Приложение за инсталиране и конфигуриране*.

Как е структурирана тази книга

Тази книга е структурирана както следва:

- Глава 1, “Свързване на DB2 за MVS/ESA в DRDA мрежа” на страница 1
- Глава 2, “Свързване на DB2 Universal Database за OS/390 в DRDA мрежа” на страница 35
- Глава 3, “Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на SNA” на страница 73
- Глава 4, “Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на TCP/IP” на страница 89
- Глава 5, “Допълнителни съображения при DB2 Universal Database за AS/400 и DB2 Universal Database” на страница 95
- Глава 6, “Свързване на DB2 за VSE & VM в DRDA мрежа” на страница 99
- Приложение A, “Най–разпространени проблеми при свързване” на страница 141
- Приложение B, “Забележки” на страница 153.

За кого е предназначена тази книга

Тази книга е предназначена за всеки, който има инсталиран DB2 Universal Database или DB2 Connect и иска да научи повече за свързваемостта в контекста на темите, представени в предишния раздел.

Други източници на информация

В този раздел са представени други източници на информация.

В World Wide Web

В World Wide Web можете да намерите най–новата информация за DB2 Connect, DB2 Universal Database и други софтуерни продукти на IBM. Сред тях са най–новите публикации, както и технически съвети и препоръки във вид на технически бележки. За да намерите тази информация в World Wide Web, изпълнете следните стъпки:

1. Задайте на вашия Web браузър следния URL:

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

2. Изберете “DB2 Universal Database”.
3. Например, потърсете “Technotes” с помощта на ключовата дума “DDCS”, “DRDA” или “Connect”.

Публикации за DRDA

Следните книги съдържат свързана информация и в това ръководство може да има препратки към тях.

Номер на форма	Заглавие
SC26–4783	*Ръководство за свързваемост на разпределена релационна база данни*
SC26–4773	*Ръководство за приложно програмиране за разпределена релационна база данни*
SC26–4782	*Ръководство за определяне на проблеми в разпределена релационна база данни*
SC26–4650	*Планиране за разпределена релационна база данни*
GC26–3195	*Ръководство за всеки мениджър на разпределена релационна база данни*
G321–5482	*Ниво 3 на архитектурата за управление на разпределени данни на IBM: Справочник*

Публикации за DRDA сървър

Сред публикациите за DRDA сървър са следните книги от библиотеките за DB2 Universal Database за AS/400, DB2 за OS/390 и DB2 за VSE и VM.

Номер на форма	Заглавие
SC41–5702	*Програмиране за AS/400 разпределена база данни (AS/400 Distributed Database Programming)*
SC41–9609	*Ръководство за програмиране за AS/400 SAA SQL/400 (AS/400 SAA Structured Query Language/400 Programmer's Guide)*

Номер на форма	Заглавие
SC41–9608	*Справочник за AS/400 SAA SQL/400 (AS/400 SAA Structured Query Language/400 Reference's Guide)*
GC21–8180	*Справочник за конфигуриране на AS/400 комуникации (AS/400 Communications Configuration Reference)*
SC26–8958	*DB2 Universal Database за OS/390 приложно програмиране и SQL справочник (DB2 Universal Database за OS/390 Application Programming and SQL Reference)*
SC26–8960	*Справочник за командите в DB2 Universal Database за OS/390 (DB2 Universal Database за OS/390 Command Reference)*
GC26–8970	*Справочник за инсталиране на DB2 Universal Database за OS/390 (DB2 Universal Database за OS/390 Installation Reference)*
SC26–8964	*DB2 Universal Database за OS/390 Справочник за отдалечени DRDA рикуестъри и сървъри*
SC26–8966	*SQL справочник за DB2 Universal Database за OS/390 (DB2 Universal Database за OS/390 SQL Reference)*
SC26–8957	*Ръководство за администриране на DB2 Universal Database за OS/390 (DB2 Universal Database за OS/390 Administration Guide)*
SC26–8967	*Ръководство и справочник за помощните програми в DB2 Universal Database за OS/390*
SH09–8087	*SQL справочник за DB2 за VSE и VM (DB2 за VSE и VM SQL Reference)*
SC26–3255	*IBM SQL справочник (IBM SQL Reference)*

Други свързани публикации

Номер на форма	Заглавие
SG24–2006	*Мигриране до DB2 Universal Database версия 5*
SG24–2213	*Въпроси за производителността на DB2 за OS/390 версия 5*
SG24–4893	*DB2 среща NT*
SG24–4894	*Универсално ръководство за свързваемост на DB2*
SG24–4693	*Начални умения със запомнени процедури в DB2*
SG24–2212	*DRDA поддръжка за TCP/IP в DB2 Universal Database за OS/390 версия 5.1 и DB2 Universal Database версия 5.0*
SC33–0814	*Ръководство за приложно програмиране за CICS за AIX*

Номер на форма	Заглавие
SC33–0931	*Ръководство за настройка и работа на CICS за AIX*
GC09–2829–00	*DB2 Connect Enterprise Edition за UNIX: Бърз старт*
GC09–2828–00	*DB2 Connect Enterprise Edition за OS/2 и Windows: Бърз старт*
GC09–2830–00	*DB2 Connect Personal Edition: Бърз старт*
GG24–4155	*Архитектура на разпределена релационна база данни: Използване на DDCS за AIX DRDA поддръжка с DB2 за MVS/ESA и DB2 Universal Database за AS/400*
GG24–4311	*Междуплатформена свързваемост и приложение на архитектурата на разпределена релационна база данни*
SC23–2443	*Обзор на семейството продукти Encina за AIX*

Глава 1. Свързване на DB2 за MVS/ESA в DRDA мрежа

DB2 за MVS/ESA е система за управление на IBM релационна база данни за системите MVS/XA и MVS/ESA. DB2 за MVS/ESA версия 2 подверсия 3 беше първото издание на DB2 за MVS/ESA, което може да поделя разпределени релационни данни с други DBMS, които поддържат DRDA протоколите. В тази глава е описано как DB2 за MVS/ESA осигурява поддръжка за разпределени релационни бази данни.Ако работите с DB2 Universal Database за OS/390 *не използвайте тази глава*: преминете направо към Глава 2, “Свързване на DB2 Universal Database за OS/390 в DRDA мрежа” на страница 35.

Информацията в тази глава основно се съсредоточава върху конфигурирането на DB2 за MVS/ESA за свързване:

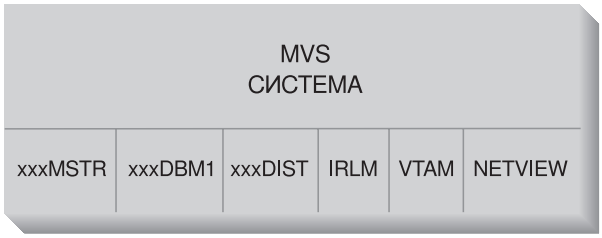
1. От DB2 Connect (вижте “Настройка на сървъра на приложения” на страница 21)
2. Към DB2 Universal Database сървъри (вижте “Настройка на рикуестър за приложения” на страница 6).

Информация за свързването на две DB2 за MVS/ESA системи или по–подробна информация, която описва как да дефинирате DRDA свързване към DB2 за MVS/ESA потърсете в изложението за свързване на разпределени бази данни в *Ръководство за администриране на IBM Database 2*.

С помощта на компонента AnyNet на VTAM версия 4 подверсия 2, можете да изпълнявате APPC през TCP/IP мрежа. Компонентът AnyNet се състои от AnyNet/MVS, който работи на хоста и AnyNet/2, който работи на работна станция и се изтегля от хоста. Всяко APPC приложение е достъпно за крайните потребители в TCP/IP мрежа без промяна в приложението. Като използва APPC през TCP/IP, приложна програма на MVS/ESA може да комуникира с друга APPC приложна програма, която работи с AnyNet APPC през TCP/IP на MVS/ESA, OS/2, AIX/6000, OS/400 или Windows. За повече информация вижте *Ръководство за VTAM AnyNet компонент за V4R2 на SNA през TCP/IP*.

DB2 за MVS/ESA

Фигура 1 на страница 2 показва MVS система, на която работи единично копие на DB2 за MVS/ESA. Освен това може да работят няколко копия на DB2 за MVS/ESA на една MVS система. За да се идентифицират копията на DB2 за MVS/ESA в рамките на дадена MVS система (или копия на DB2 за MVS/ESA в рамките на MVS/JES комплекс), на всяка DB2 система се присвоява *име на подсистема* – низ с дължина от един до четири символа, който е уникален в рамките на MVS/JES комплекса. В Фигура 1 на страница 2 името на DB2 за MVS/ESA подсистемата е *xxxx*. Три от имената на MVS адресните пространства са с префикс – името на DB2 за MVS/ESA подсистемата. Тези три адресни пространства образуват DB2 за MVS/ESA.



Фигура 1. MVS адресни пространства, използвани от DB2 за MVS/ESA

Фигура 1 показва MVS адресните пространства, използвани при работата на разпределена база данни с DB2 за MVS/ESA. Тези адресни пространства работят заедно, за да позволят на потребителите на DB2 за MVS/ESA да имат достъп до локалните релационни бази данни и да комуникират с отдалечени DRDA системи. Целта на всяко адресно пространство е както следва:

xxxxMSTR
Адресно пространство за системни услуги за DB2 за MVS/ESA продукта, който отговаря за стартирането и спирането на DB2 за MVS/ESA и контролира локалния достъп до DB2 за MVS/ESA.

xxxxDBM1
Адресно пространство за базата данни, като отговаря за достъп до релационни бази данни, управлявани чрез DB2 за MVS/ESA. Това е мястото, където се изпълнява входа и изхода от ресурсите на базата данни от името на SQL приложните програми.

xxxxDIST
Частта от DB2 за MVS/ESA, която осигурява възможностите на разпределена база данни; също така известно като *Средство за разпределени данни* (DDF – DISTRIBUTED DATA FACILITY). Когато получи заявка за разпределена база данни, DDF я предава към *xxxx*DBM1, така че да се изпълнят необходимите входно/изходни операции към базата данни. В тази книга ще намерите подробно описание на DDF.

IRLM Мениджър за заключване, използван от DB2 за MVS/ESA, за да управлява достъпа до ресурсите на базата данни.

VTAM SNA комуникационен мениджър за MVS системата. DDF използва VTAM при комуникации с разпределена база данни от името на DB2 за MVS/ESA.

NETVIEW
Основният продукт за мрежово управление при MVS системи. Когато възникнат грешки при работа на разпределена база данни, DDF записва информацията за грешката (известна също като *предупреждение*) в базата данни NetView хардуерен монитор. Системните администратори могат да използват NetView, за да разгледат грешките, записани в базата данни на хардуерния монитор или да направят така, че при запис на предупреждения да се извикват автоматизирани процедури с команди.

Освен това NetView може да се използва за диагностика на VTAM комуникационни грешки. Допълнителна информация вижте в *Ръководство за определяне на проблеми в разпределена релационна база данни.*

Фигура 1 не показва никакви SQL приложни програми. Когато приложна програма използва DB2 за генериране на SQL оператори, приложната програма трябва да е прикрепена към DB2 за MVS/ESA по един от следните начини:

TSO Последователностите от задания и крайните потребители, които са влезли в TSO, се свързват към DB2 за MVS/ESA чрез средството за отдалечено свързване на ниво потребителски модел на TSO. Тази техника се използва при свързване на SPUFI и повечето QMF приложения към DB2 за MVS/ESA.

CICS/ESA
Когато CICS/ESA приложение изпрати SQL обръщения, CICS/ESA използва CICS интерфейса за отдалечено свързване, за да насочи SQL заявките към DB2 за MVS/ESA.

IMS/ESA
Транзакциите, които работят под управлението на IMS/ESA използват IMS интерфейса за отдалечено свързване, за да предадат SQL изрази за обработка от DB2 за MVS/ESA.

DDF Средството за разпределени данни отговаря за свързване на разпределени приложения към DB2 за MVS/ESA.

CAF Средството за отдалечено свързване на обръщения позволява на написани от потребителите подсистеми да се свързват директно към DB2 за MVS/ESA.

DB2 за MVS/ESA реализация

DRDA дефинира типове функции на системата за управление на базата данни. DB2 за MVS/ESA V2R3 поддържа отдалечена единица работа. При нея приложна програма, изпълнявана в една система, може да осъществи достъп до данни на отдалечена DBMS с помощта на SQL, осигурен от тази отдалечена DBMS. DB2 за MVS/ESA V3R1 поддържа разпределена единица работа. При нея приложна програма, изпълнявана в една система може да осъществи достъп до данни на няколко отдалечени DBMS с помощта на SQL, осигурен от отдалечените DBMS. Допълнителна информация за типовете разпределение, дефинирани от DRDA, потърсете в *DRDA Ръководство за свързваемост*.

Както е показано в Фигура 2 на страница 5, DB2 за MVS/ESA поддържа три конфигурации на свързвания към разпределени база данни с помощта на два метода за достъп:

[1] *Достъпът, насочен от системата* позволява на DB2 за MVS/ESA рикуестъра да се свърже към един или повече DB2 за MVS/ESA сървъри. Установеното свързване между DB2 за MVS/ESA рикуестъра и сървъра не се придържа към протоколите, дефинирани в DRDA и не може да се използва за свързване към DB2 за MVS/ESA на продукти, които не са DB2 за MVS/ESA. Този тип свързване се установява чрез кодиране в приложението на имена от три части или псевдоними.

[2] *Достъпът, насочван от приложение* позволява на DB2 за MVS/ESA, както и на не–DB2 за MVS/ESA рикуестър като DB2 Connect да се свързва към един или повече DB2 за MVS/ESA или не–DB2 за MVS/ESA сървъри на приложения като DB2 Universal Database и DB2 Universal Database за AS/400 с помощта на DRDA протоколи. Броят на сървърите на приложения, които могат да се свържат към рикуестъра в даден момент, зависи от версията на DB2 за MVS/ESA на рикуестъра. Ако рикуестърът е DB2 за MVS/ESA V2R3, тогава в даден момент може да е свързан само един сървър на приложения. Този тип свързване се установява чрез кодиране на SQL CONNECT оператори в приложението. Ако рикуестърът за приложения е DB2 за MVS/ESA V3R1, тогава в даден момент могат да се свързват един или повече сървъри на приложения.

[3] Достъп, насочван от приложение или от системата, може да се използва съвместно при установяване на свързвания.

Терминът *вторичен сървър* описва системи, действащи като сървъри на сървъри на приложения.

Ако всички системи в конфигурация поддържат двуфазов протокол за записване на промените, тогава се поддържа разпределена единица работа (многосайтово четене и многосайтово обновяване). Ако не всички системи поддържат този протокол, обновяванията в рамките на единица работа са или ограничени до отделен сайт, който не поддържа двуфазовия протокол за записване на промените, или до подмножество от сайтове, които го поддържат.

Фигура 2. DB2 за MVS/ESA разпределени свързвания

Таблица 1 на страница 6 сравнява типовете свързване при DB2 за MVS/ESA разпределена база данни.

Таблица 1. Сравнение на свързвания в DB2 за MVS/ESA разпределена база данни

[1] Достъп, насочван от системата	**[2] Достъп, насочван от приложения (като всички системи поддържат двуфазов протокол за записване на промените)**	**[3] Достъп, насочван от приложения и от система**
Всички участници трябва да са DB2 за MVS/ESA системи	Всеки две DRDA системи могат да се свързват една с друга	Рикуестър за приложения може да е всяка DRDA система; сървъри трябва да са DB2 за MVS/ESA системи
Може да се свързва директно към много участници	Може да се свързва директно към много участници	Рикуестърът за приложения се свързва директно към Сървър на приложения; Сървър на приложения от своя страна могат да се свързват към много DB2 за MVS/ESA вторични сървъри
Всяко SQL приложение може да има множество APPC сесии с всеки сървър	Всяко SQL приложение има една APPC сесия с всеки сървър	SQL приложение има една APPC сесия с всеки сървър; DB2 за MVS/ESA сървър на приложения може да установи много APPC сесии към всеки сървър за приложение
Има достъп както до локалните, така и до отдалечените ресурси в контекста на едно записване на промените	Има достъп както до локалните, така и до отдалечените ресурси в контекста на едно записване на промените	Рикуестър за приложения и Сървър на приложения имат достъп до локалните и отдалечени данни
По–ефективно при големи и много едновременни запитвания	По–ефективно при SQL оператори, които се изпълняват много малко пъти в контекста на едно записване на промените	Връзката рикуестър за приложения–Сървър на приложения се държи подобно на **[2]**; свързванията на вторичен сървър се държат подобно на **[1]**
Може да поддържа статичен или динамичен SQL, но сървърът динамично свързва статичния SQL при първото му изпълнение в контекста на записване на промените	Може да генерира статичен или динамичен SQL	Рикуестърът за приложения и Сървър на приложения могат да генерират статичен или динамичен SQL; вторичните сървъри поддържат статичен или динамичен SQL, но динамично свързват статичния SQL при първото му изпълнение в контекста на записване на промените
Ограничено до SQL операторите INSERT, DELETE и UPDATE и до операторите, които поддържат SELECT	Може да използва всички оператори, поддържани от системата, която ги изпълнява	Сървърите на приложения поддържат всеки SQL; вторичните сървъри поддържат само DML SQL (например CREATE или ALTER)

Настройка на рикуестър за приложения

DB2 за MVS/ESA реализира поддръжка на DRDA рикуестър за приложения, като неделима част от DB2 за MVS/ESA средството за разпределени данни (DDF – DISTRIBUTED DATA FACILITY). DDF може да се спре независимо от локалните средства за управление на DB2 за MVS/ESA база данни, но не може да работи при липса на поддръжка от страна на локалното управление на DB2 за MVS/ESA база данни.

Когато DB2 за MVS/ESA действа като рикуестър за приложения, може да свързва приложения, които работят на системата към отдалечена DB2 Universal Database, DB2 за MVS/ESA, DB2 Universal Database за OS/390, DB2 Universal Database за AS/400 и DB2 за VSE и VM сървъри на база данни, които изпълняват функцията на DRDA сървър на приложения.

За да осигурите достъп до разпределена база данни при DB2 за MVS/ESA Средство за обработка на заявки, трябва да направите следното:

- “Осигуряване на мрежова информация” на страница 7—Средство за обработка на заявки трябва да може да приема стойностите на RDB_NAME и да ги преобразува в SNA стойности NETID.LUNAME. DB2 за MVS/ESA използва *DB2 за MVS/ESA комуникационната база данни*, за да регистрира RDB_NAME и съответните мрежови параметри. Комуникационната база данни позволява на DB2 за MVS/ESA Средство за обработка на заявки да предава необходимата SNA информация на VTAM, когато се осъществяват заявки към разпределена база данни.
- “Осигуряване на защита” на страница 16— За да се приемат заявки за отдалечена база данни от Сървър на приложения, Средство за обработка на заявки трябва да осигурява информацията за защита, изисквана от сървъра. DB2 за MVS/ESAизползва комуникационната база данни и RACF, за да осигури необходимата информация за защита на мрежата.
- “Представяне на данни” на страница 21—Трябва да сте сигурни, че CCSID на рикуестъра за приложения е съвместим със сървъра на приложения.

Осигуряване на мрежова информация

Голяма част от обработките в среда на разпределена база данни изисква обмен на съобщения с други места във вашата мрежа. За да се изпълнят правилно тези обработки, трябва да направите следното:

1. Дефинирайте локалната система
2. Дефинирайте отдалечената система
3. Дефинирайте комуникациите
4. Определете RU размерите и стъпките

Дефиниране на локалната система

На всяка програма в мрежата се присвоява NETID и LU име, така че DB2 за MVS/ESA Средство за обработка на заявки трябва да има стойност NETID.LUNAME, когато се свързва към мрежата. Тъй като DB2 за MVS/ESA Средство за обработка на заявки е интегриран в локалната система за управление на DB2 за MVS/ESA база данни, Средство за обработка на заявки трябва също да има RDB_NAME. В DB2 за MVS/ESA изданията, DB2 за MVS/ESA използва RDB_NAME като име на *местоположение*.

Дефинирайте DB2 за MVS/ESA Средство за обработка на заявки да използва SNA мрежа, както следва:

1. Изберете LU име за вашата DB2 за MVS/ESA система. NETID за вашата DB2 за MVS/ESA система автоматично се получава от VTAM при стартирането на DDF.
2. Дефинирайте LU името и името на местоположение в DB2 за MVS/ESA *bootstrap data set* (BSDS). (DB2 за MVS/ESA ограничава името на местоположението до 16 символа.)
3. Създайте VTAM APPL дефиниция, за да регистрирате избраното LU име във VTAM.

Конфигуриране на DDF BSDS: DB2 за MVS/ESA прочита BSDS при стартирането, за да получи системните инсталационни параметри. Един от записите в BSDS се нарича *DDF запис*, защото съдържа информацията, използвана от DDF при свързване към VTAM. Тази информация се състои от следното:

- Името на местоположението за DB2 за MVS/ESA системата
- LU името за DB2 за MVS/ESA системата

- Паролата, използвана при свързване на DB2 за MVS/ESA система към VTAM

DDF BSDS информацията можете да доставите на DB2 за MVS/ESA по два начина:

- Използвайте DDF инсталационния панел DSNTIPR, когато за първи път инсталирате DB2 за MVS/ESA, за да осигурите необходимата DDF BSDS информация. Много от инсталационните параметри не се разглеждат тук, защото е по–важно да знаете как да свържете DB2 за MVS/ESA към VTAM. Фигура 3 показва как да използвате инсталационния панел, за да запишете името на местоположение SYDNEY, LU името LUDBD1 и паролата PSWDBD1 в DB2 за MVS/ESA BSDS.

```
 1 DDF STARTUP OPTION   ===> AUTO      NO (DDF не се стартира),
                                       AUTO (автоматично стартиране) или
                                       COMMAND (стартира се с команда)
 2 DB2 LOCATION NAME    ===> SYDNEY    Име, което другите DB2 използват при
                                       обръщение към тази DB2
 3 DB2 NETWORK LUNAME   ===> LUDBD1    име за обръщение от VTAM към тази DB2
 4 DB2 NETWORK PASSWORD ===> PSWDBD1   Парола за свързване към други DB2
 5 RLST ACCESS ERROR    ===> NOLIMIT   Реакция при грешка в отдал. RLST достъп
                                       NORUN     - Изобщо не се изпълнява
                                       1-5000000 - Лимит CPU сервизни единици
НАТИСНЕТЕ: ENTER за продължение END за край HELP за допълнителна информация
```

Фигура 3. DB2 за MVS/ESA инсталационен панел DSNTIPR

- Ако DB2 за MVS/ESA вече е инсталиран, можете да използвате помощната програма за промяна съдържанието на журнала (DSNJU003), за да обновите информацията в BSDS.

  Фигура 4 показва как да обновите BSDS с името на местоположение SYDNEY, LU името LUDBD1 и паролата 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
//*
```

Фигура 4. Примерна дефиниция на Bootstrap Data Set DDF

При стартиране на DDF (автоматично при стартиране на DB2 за MVS/ESA или с командата на DB2 за MVS/ESA START DDF) се създава връзка с VTAM, като се прехвърля LU името и парола към VTAM. VTAM разпознава DB2 за MVS/ESA системата като сравнява LU името и паролата (ако е необходима VTAM парола) със стойностите, дефинирани в оператора на DB2 за MVS/ESA VTAM APPL. VTAM паролата се използва, за да се провери дали DB2 за MVS/ESA има оторизация да използва определеното LU име на VTAM системата. VTAM паролата не се

прехвърля през мрежата и не се използва за свързване на други системи в мрежата към DB2 за MVS/ESA.

Ако VTAM не изисква парола, пропуснете ключовата дума PASSWORD= в помощната програма за промяна съдържанието на журнала. Липсата на ключовата дума посочва, че не е необходима VTAM парола.

Създаване на VTAM APPL дефиниция: След като дефинирате VTAM LU името и парола в DB2 за MVS/ESA, трябва да регистрирате тези стойности във VTAM. VTAM използва оператора APPL, за да дефинира локалните LU имена. Фигура 5 показва как да дефинирате LU името LUDBD1 във VTAM.

```
DB2APPLS VBUILD TYPE=APPL
*
*--------------------------------------------------------------------*
*                                                                    *
*           APPL ДЕФИНИЦИЯ ЗА DB2 СИСТЕМАТА  SYDNEY                    *
*                                                                    *
*--------------------------------------------------------------------*
*
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
```

Фигура 5. Примерна DB2 за MVS/ESA APPL дефиниция

За оператора на VTAM APPL има много ключови думи. Значението на ключовите думи е представено подробно в *Ръководство за администриране на DB2*. Представените тук ключови думи са свързани с темите на тази книга. Ключовите думи, които са от значение за Фигура 5, са описани както следва:

LUDBD1

VTAM използва етикета на оператора APPL като LU име. В този случай LU името е LUDBD1. Синтаксисът на APPL не позволява да се остави място за пълната стойност NETID.LUNAME. Стойността NETID не се определя във VTAM оператора APPL, защото на всички VTAM приложения автоматично има се присвоява стойност NETID за VTAM системата.

AUTOSES=1

Броят на SNA сесиите победители, които се стартират автоматично, когато се генерира APPC заявка за промяна броя на сесиите – Change Number of Sessions (CNOS). Трябва да се въведе различна от нула стойност за AUTOSES, за да се информира DB2 за MVS/ESA при всяко неуспешно изпълнение на VTAM CNOS.

Не е необходимо автоматично да стартирате всички APPC сесии между всеки два участника в разпределена база данни. Ако стойността AUTOSES е по–малка от ограничението за сесии победители (DMINWNL), VTAM

забавя стартирането на останалите SNA сесии, докато те станат необходими за приложение в разпределена база данни.

DMINWNL=10

Броят на сесиите, за които тази DB2 за MVS/ESA система е победител. Параметърът DMINWNL се подразбира при обработка на CNOS, но може да се замени за всеки конкретен участник, като се добави ред в таблицата SYSIBM.SYSLUMODES в DB2 за MVS/ESA комуникационната база данни.

DMINWNR=10

Броят на сесиите, за които системата партньор е победител. Параметърът DMINWNR се подразбира при обработка на CNOS, но може да се замени за всеки конкретен участник, като се добави ред в таблицата SYSIBM.SYSLUMODES в DB2 за MVS/ESA комуникационната база данни.

DSESLIM=20

Общият брой на сесиите (победили или загубили сесии), които можете да установите между DB2 за MVS/ESA и друга разпределена система за специфичното име на групата в този режим. Параметърът DSESLIM е по подразбиране при обработка на CNOS, но може да се замени за всеки отделен участник, като се добави ред в таблицата SYSIBM.SYSLUMODES в DB2 за MVS/ESA комуникационната база данни.

Ако участникът не поддържа броя на сесиите, заявени от параметрите DSESLIM, DMINWNL или DMINWNR, обработката на CNOS определя нови стойности за тези параметри, които са приемливи за участника.

EAS=9999

Оценка за общия брой на сесиите, които тази VTAM LU изисква.

MODETAB=RDBMODES

Определя таблицата VTAM MODE, в която се намира всяко име на режим в DB2 за MVS/ESA.

PRTCT=PSWDBD1

Определя VTAM паролата, която да се използва при опитите да се свърже DB2 за MVS/ESA към VTAM. Ако е пропусната ключовата дума PRTCT, не се изисква парола и трябва да пропуснете ключовата дума PASSWORD= в DB2 за MVS/ESA помощната програма за промяна съдържанието на журнала.

SECACPT=ALREADYV

Определя най–високата стойност за защита на ниво SNA сесия, която се приема от тази DB2 за MVS/ESA система, когато приеме заявка към разпределена база данни от отдалечена система. Ключовата дума ALREADYV посочва, че тази DB2 за MVS/ESA система може да приеме три опции за защита на SNA сесия от други DRDA системи, които са изпратили заявка за данни от тази DB2 за MVS/ESA система:

- SECURITY=SAME (валидността на заявката вече е проверена и съдържа само потребителския идентификатор).
- SECURITY=PGM (заявката съдържа идентификатора и паролата на потребителя).
- SECURITY=NONE (заявката не съдържа никаква информация за защита). DB2 за MVS/ESA отхвърля DRDA заявките, които определят SECURITY=NONE.

Най–добре е винаги да определяте SECACPT=ALREADYV, защото нивото на защита на SNA сесията за всеки DB2 за MVS/ESA участник се взима от DB2 за MVS/ESA комуникационната база данни (колоната USERSECURITY на таблицата SYSIBM.SYSLUNAMES). SECACPT=ALREADYV ви дава

най–голяма гъвкавост при определянето на стойностите за USERSECURITY.

VERIFY=NONE
Определя нивото за защита на SNA сесия (валидност на LU на участник), изисквано от тази DB2 за MVS/ESA система. Стойността NONE посочва, че не е необходимо да се проверява валидността на LU на партньор.

DB2 за MVS/ESA не ограничава вашия избор за ключовата дума VERIFY. В несигурна мрежа се препоръчва използването на VERIFY=REQUIRED. Ако се използва VERIFY=REQUIRED, VTAM отхвърля партньорите, които не могат да изпълнят проверка на валидност на LU на партньора. Ако изберете VERIFY=OPTIONAL, VTAM проверява валидността на LU на партньора само за тези, които осигуряват поддръжка.

VPACING=2
Определя брояча за VTAM стъпката на 2.

SYNCLVL=SYNCPT
Посочва, че DB2 за MVS/ESA може да поддържа двуфазов протокол за записване на промените. VTAM използва тази информация, за да информира партньора, че е достъпен двуфазов протокол за записване на промените. При наличието на тази ключова дума DB2 за MVS/ESA автоматично използва двуфазов протокол за записване на промените, ако партньорът го поддържа.

ATNLOSS=ALL
Посочва, че DB2 за MVS/ESA трябва да се информира при всяко прекратяване на VTAM сесия. Така при необходимост DB2 за MVS/ESA изпълнява повторно синхронизиране на SNA.

DSESLIM, DMINWNL и DMINWNR ви позволяват да установите максималния брой VTAM сесии по подразбиране за всички партньори. При партньори, които имат специални изисквания по отношение на максималния брой сесии, може да се използва таблицата SYSIBM.SYSLUMODES, за да се замени стойността по подразбиране. Например може да предпочетете да определите такъв максимален брой VTAM сесии по подразбиране, който е подходящ за вашите OS/2 системи. За другите партньори можете да създадете редове в таблицата SYSIBM.SYSLUMODES, за да дефинирате съответния максимален брой сесии. Разгледайте следните примерни стойности:

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

Тези параметри позволяват на всеки партньор да създаде до четири сесии с DB2 за MVS/ESA, в които партньорът е победител за всяка от сесиите. Тъй като OS/2 създава LU 6.2 диалог с DB2 за MVS/ESA, като направи OS/2 победител за всички сесии, ще получите малко предимство в производителността. Ако OS/2 има достъпна сесия победител, не е необходимо да пита за позволение, за да стартира нов LU 6.2 диалог.

Дефиниране на отдалечени системи

Когато DB2 за MVS/ESA приложение заяви данни от отдалечена система, DB2 за MVS/ESA търси в таблиците на комуникационната база данни, за да намери информация за отдалечената система, като изпълнява и търсене на:

- LU името и TP името
- Информацията за защитата на мрежата, необходима за отдалечената страна
- Максималния брой сесии и имената на режимите, използвани при комуникация с отдалечената страна

Комуникационната база данни е група от SQL таблици, управлявани от DB2 за MVS/ESA системен администратор. Като DB2 за MVS/ESA системен администратор трябва да използвате SQL, за да вмъкнете редове в комуникационната база данни, за да опишете всеки потенциален DRDA партньор. Комуникационната база данни се състои от пет таблици:

1. **SYSIBM.SYSLOCATIONS**

   Тази таблица позволява на DB2 за MVS/ESA да определи LU името и TPN стойността за всяко RDB_NAME, избрано от DB2 за MVS/ESA приложение. Колоните са:

   LOCATION
   RDB_NAME на отдалечена система. DB2 за MVS/ESA ограничава стойността за RDB_NAME до 16 байта, което е с два байта по–късо от 18–байтовото ограничение, дефинирано в DRDA.

   LOCTYPE
   В момента не се използва; трябва да е празна.

   LINKNAME
   LU името на отдалечената система.

   LINKATTR
   TPN на отдалечената система. Ако отдалечената система е DB2 за MVS/ESA или използва DRDA стойността по подразбиране на TPN (X'07F6C4C2'[1]), може да се използва празен низ, за да се определи TPN, защото DB2 за MVS/ESA автоматично избира правилната стойност.

   Ако отдалечената система изисква TPN стойност, различна от стойността по подразбиране, трябва да я въведете тук.

2. **SYSIBM.SYSLUNAMES**

   Тази таблица дефинира мрежовите атрибути на отдалечените системи. Колоните са:

   LUNAME
   LU името на отдалечената система.

   SYSMODENAME
   VTAM името на режима на влизане в системата, използван при установяване на *междусистемен* диалог DB2 за MVS/ESA–до–DB2 за MVS/ESA за поддръжка на вторичен сървър DB2 за MVS/ESA (насочван от системата достъп). Ако тази колона е празна, IBMDB2LM трябва да се използва при диалог между DB2 за MVS/ESA системи

   USERSECURITY
   Опциите за приемане от страна на мрежовата защита, които се изискват от отдалечената система, когато тази DB2 за MVS/ESA система действа като сървър за отдалечената система (изисквания при *входяща защита*).

   ENCRYPTPSWDS
   Дали са закодирани паролите, обменяни с този партньор. Закодирани пароли се поддържат само от DB2 за MVS/ESA рикуестъри и сървъри.

---

[1] – тази TPN стойност *за сега* се отнася за DB2 за VM.

MODESELECT

Определя дали да се използва таблицата SYSIBM.SYSMODESELECT, за да се избере запис за VTAM режим за влизане (име на режим) на базата на крайния потребител и приложение, което прави заявката. Ако тази колона съдържа 'Y', таблицата SYSIBM.SYSMODESELECT се използва за получаване на името на режима за всяка изходяща заявка към разпределена база данни.

Ако MODESELECT съдържа нещо различно от 'Y', се използва името на режима IBMDB2LM при заявки с насочван от системата достъп, а името на режим IBMRDB се използва при DRDA заявките.

Колоната MODESELECT ви позволява да определите приоритети за заявките към разпределена база данни, като се определи VTAM клас на услуга (COS – class of service), асоцииран с името на режима.

USERNAMES

Необходимото ниво за проверка откъде идва и преобразуване на потребителски идентификатор. Освен това тази колона определя параметрите на защита, използвани от тази DB2 за MVS/ESA подсистема при заявка за данни от отдалечения участник (изисквания за *изходяща защита*). ИМЕНАТА НА ПОТРЕБИТЕЛИТЕ може да са със стойност I, O или B.

3. **SYSIBM.SYSLUMODES**

Тази таблица се използва за дефиниране на максималния брой на LU 6.2 сесии (CNOS ограничения) за всеки партньор. Колоните са:

LUNAME

LU името на отдалечената система.

MODENAME

Името на VTAM режима на влизане, чиито ограничения се определят. Ако колоната MODENAME е празна, по подразбиране се запълва с IBMDB2LM.

CONVLIMIT

Максималният брой активни сесии между локалната DB2 за MVS/ESA и отдалечената система за този режим на влизане. Тази стойност се използва, за да замени параметъра DSESLIM във VTAM оператора за дефиниране APPL за този режим на влизане, който определя максималния брой VTAM сесии по подразбиране за DB2 за MVS/ESA.

Стойността, избрана в CONVLIMIT, се използва при CNOS, за да се определят стойностите DMINWNR и DMINWNL на CONVLIMIT/2.

AUTO Дали обработката на CNOS и предварителното заделяне на сесии се инициира автоматично при стартирането на DDF или се отлага до първата препратка към LU името чрез този режим на влизане.

4. **SYSIBM.SYSMODESELECT**

Тази таблица ви позволява да определите различни имена на режими за отделните крайни потребители и DB2 за MVS/ESA приложения. Тъй като всяко име на VTAM режим може да има асоцииран клас на услуги (COS), можете да използвате тази таблица, за да присвоите приоритети при прехвърляне в мрежата за приложенията в разпределената база данни, на основата на комбинация от AUTHID, PLANNAME и LUNAME. Колоните са:

AUTHID

идентификатор за оторизация на DB2 за MVS/ESA потребител (потребителски идентификатор). По подразбиране е празно, като

показва, че определеното име на режим при влизане се прилага за всички идентификатори за оторизации.

PLANNAME
Името на плана, асоциирано с приложението, което заявява достъп до отдалечената база данни. По подразбиране е празно, като показва, че определеното име на режим при влизане се прилага за всички имена на план. Името на план, използвано за командата BIND PACKAGE е DSNBIND.

LUNAME
LU името, асоциирано с отдалечената база данни.

MODENAME
Името на VTAM режима на влизане, който да се използва, когато се насочва заявка на разпределена база данни към посочената отдалечена система. По подразбиране е празно, като посочва, че IBMDB2LM трябва да се използва при сесии с насочване на достъпа от системата, а IBMRDB трябва да се използва при DRDA сесии.

5. **SYSIBM.SYSUSERNAMES**

Тази таблица се използва за управление на имената на крайните потребители, като осигурява пароли, преобразуване на имена и проверка откъде идва. DB2 за MVS/ESA използва името на крайния потребител като идентификатор за оторизация. Повечето други продукти разглеждат това име като потребителски идентификатор.

С тази таблица можете да използвате преобразуване на името, за да определите да се използват различни стойности за SNA потребителския идентификатор и DB2 за MVS/ESA идентификатор за оторизация. Процесът за преобразуване на имената е позволен при заявки от отдалечена система (*изходящи* заявки) и за заявки, които идват от отдалечена система (*входящи* заявки). Ако паролите не са закодирани, тази таблица е източник за паролата на крайния потребител, когато се изпраща потребителски идентификатор и парола към отдалечената страна. Колоните са:

TYPE Описанието за това как се използва реда (дали е ред, описващ преобразуване на име за изходящи, входящи заявки или заявки за проверка откъде идва).

AUTHID
При преобразуване на изходящо име това е DB2 за MVS/ESA идентификатора за оторизация, който да се преобразува. При преобразуване на входящо име това е SNA потребителския идентификатор, който да се преобразува. И в двата случая празна стойност на AUTHID се отнася за всички идентификатори за оторизация или потребителски идентификатори.

LUNAME
LU името на отдалечената система, за която се отнася този ред. Ако е празно, стойността NEWAUTHID се прилага за всички системи.

NEWAUTHID
Новото име на крайния потребител (SNA потребителски идентификатор или DB2 за MVS/ESA идентификатор за оторизация). Ако е празно, означава, че не е необходимо да преобразувате идентификатора.

PASSWORD
Паролата, използвана на заделения диалог, ако паролите не са закодирани (ENCRYPTPSWDS = 'N' в SYSIBM.SYSLUNAMES). Ако паролите са закодирани, тази колона се игнорира.

Дефиниране на комуникациите

VTAM е Комуникационен мениджър за MVS системите. VTAM приема функции на LU 6.2 от DB2 за MVS/ESA и ги конвертира до потоци данни на LU 6.2, които можете да прехвърляте през мрежата. За да може VTAM да комуникира с приложенията партньори, дефинирани в DB2 за MVS/ESA комуникационната база данни, трябва да предоставите на VTAM следната информация:

- LU името за всеки сървър.

  При комуникации на DB2 за MVS/ESA с VTAM, DB2 за MVS/ESA може да предава само LU име (не NETID.LUNAME) на VTAM, за да определи желаното предназначение. Това LU име трябва да е уникално в рамките на LU имената, известни на локалната VTAM система, за да може VTAM да определи NETID и LU името от стойността за LU име, предадена от DB2 за MVS/ESA. Когато LU имената са уникални в рамките на SNA мрежата на предприятието, се опростява значително процеса на дефиниране на VTAM ресурсите. За съжаление това не винаги е възможно. Ако LU имената в рамките на вашите SNA мрежи не са уникални, трябва да използвате VTAM преобразуването на LU име, за да изградите правилната комбинация от NETID.LUNAME за LU името, което не е уникално. Този процес е описан в "Преобразуване имена на ресурси" в *Ръководство за мрежова реализация на VTAM*.

  Мястото и синтаксисът на VTAM дефинициите, използвани за дефиниране на отдалечени LU имена зависи от това как логически и физически е свързана отдалечената система към локалната VTAM система.
- Размерът на RU, размера на стъпката на пакета и класа на услугите за всяко име на режим. Създайте запис в таблицата с VTAM режимите за всяко име на режим, определено в комуникационната база данни. Освен това трябва да дефинирате IBMRDB и IBMDB2LM.
- VTAM и RACF профилите за алгоритъма за проверка валидността на LU, ако смятате да използвате проверка на валидността на LU на участника.

Определяне RU размерите и стъпките

Записите, които дефинирате във VTAM таблицата с режими, определят размерите на RU и броя стъпки. Неправилното дефиниране на тези стойности, може да има отрицателно влияние върху всички VTAM приложения.

След като изберете RU размерите, максималния брой сесии, и броя на стъпките, изключително важно е да се разгледа какво е влиянието на тези стойности върху съществуващата VTAM мрежа. Трябва да разгледате следните неща, когато инсталирате нова система на разпределена база данни:

- При VTAM CTC свързвания проверете, дали параметърът MAXBFRU е достатъчно голям, за да поеме RU размера плюс 29 байта, които VTAM добавя за заглавната част на SNA заявката и заглавната част на пакета за прехвърляне. MAXBFRU се измерва в единици от по 4K байта, така че MAXBFRU трябва да е поне 2, за да събере RU с размер 4K.
- При NCP свързвания се убедете, че MAXDATA е достатъчно голямо, за да поеме размера на RU плюс 29 байта. Ако определите размер на RU от 4K, MAXDATA трябва да е поне 4125.

  Ако определите NCP параметъра MAXBFRU, изберете стойност, която събира размера на RU плюс 29 байта. При NCP, параметърът MAXBFRU дефинира броя на входно/изходните буфери на VTAM, които могат да се използват за поемане на PIU. Ако изберете размер от 441 на IOBUF буфера, MAXBFRU=10 обработва правилно RU с размер 4K, защото 10*441 е повече от 4096+29.

- *DRDA Ръководство за свързваемост* описва как да оцените както е влиянието върху вашата разпределена база данни на VTAM IOBUF пула. Ако използвате прекалено много ресурси за IOBUF пула, производителността на VTAM се влошава за всички VTAM приложения.

Осигуряване на защита

Когато отдалечена система изпълнява обработки в разпределена база данни от името на SQL приложение, трябва да може да удовлетвори изискванията за защитата на Средство за обработка на заявки, Сървър на приложения и мрежата, която ги свързва. Тези изисквания спадат към една или повече от следните категории:

- Избиране на имена на крайни потребители
- Параметри за защита на мрежата
- Защита на мениджъра на базата данни
- Защита, прилагана от външна подсистема за защита
- Представяне на данни

Избиране имена на крайни потребители

При MVS системите на крайните потребители се присвояват *потребителски идентификатори* с дължина от 1 до 8 символа. Тази стойност трябва да е уникална в рамките на определената MVS система, но може да не е уникална в цялата SNA мрежа. Например може да има потребител с име JONES в NEWYORK системата и друг потребител с име JONES в DALLAS системата. Ако тези два потребителя са един и същи човек, няма да има конфликт. Обаче, ако JONES в DALLAS е различен от JONES в NEWYORK, SNA мрежата (а следователно и разпределените бази данни в рамките на мрежата) не могат да различат JONES в NEWYORK от JONES в DALLAS. Ако не коригирате тази ситуация, JONES в DALLAS може да използва правата, предоставени на JONES в NEWYORK системата.

За да отстрани конфликтите в имената, DB2 за MVS/ESA поддържа преобразуване на имената на крайните потребители. Когато приложение в DB2 за MVS/ESA Средство за обработка на заявки направи заявка към разпределена база данни, DB2 за MVS/ESA изпълнява преобразуване на името, ако комуникационната база данни посочи, че е необходимо *преобразуване на изходящо име*. Ако е избрано преобразуване на изходящо име, DB2 за MVS/ESA винаги налага да се изпраща парола с всяка изходяща заявка към разпределена база данни.

Преобразуването на изходящото име в DB2 за MVS/ESA се активира, като се настрои колоната USERNAMES в таблицата SYSIBM.SYSLUNAMES да е `'O'` или `'B'`. Ако USERNAMES е определено на `'O'`, преобразуването на името на крайния потребител се изпълнява за изходящите заявки. Ако USERNAMES е установено на `'B'`, преобразуването на името на крайния потребител се изпълнява както за входящите, така и за изходящите заявки.

Тъй като DB2 за MVS/ESA оторизацията зависи от потребителския идентификатор на крайния потребител и от потребителския идентификатор на DB2 за MVS/ESA плана, или собственика на пакета, процесът на преобразуване на името на крайния потребител се изпълнява за потребителския идентификатор на крайния потребител, потребителския идентификатор на собственика на плана и потребителския

идентификатор на собственика на пакета.[2]В процеса на преобразуване на имената се търси в таблицата SYSIBM.SYSUSERNAMES в следната последователност, за да се намери ред, който съответства на следните образци (TYPE.AUTHID.LUNAME):

1. O.AUTHID.LUNAME—Правило за преобразуване на специфичен краен потребител на специфичен партньор.
2. O.AUTHID.празно—Правило за преобразуване на специфичен краен потребител на произволен партньор.
3. O.празно.LUNAME—Правило за преобразуване на произволен краен потребител на специфичен партньор.

Ако не се намери съответен ред, DB2 за MVS/ESA отхвърля заявката към разпределената база данни. Ако редът се намери, стойността в колоната NEWAUTHID се използва като идентификатор за оторизация. (Празна стойност на NEWAUTHID показва, че трябва да се използва оригиналното име без преобразуване.)

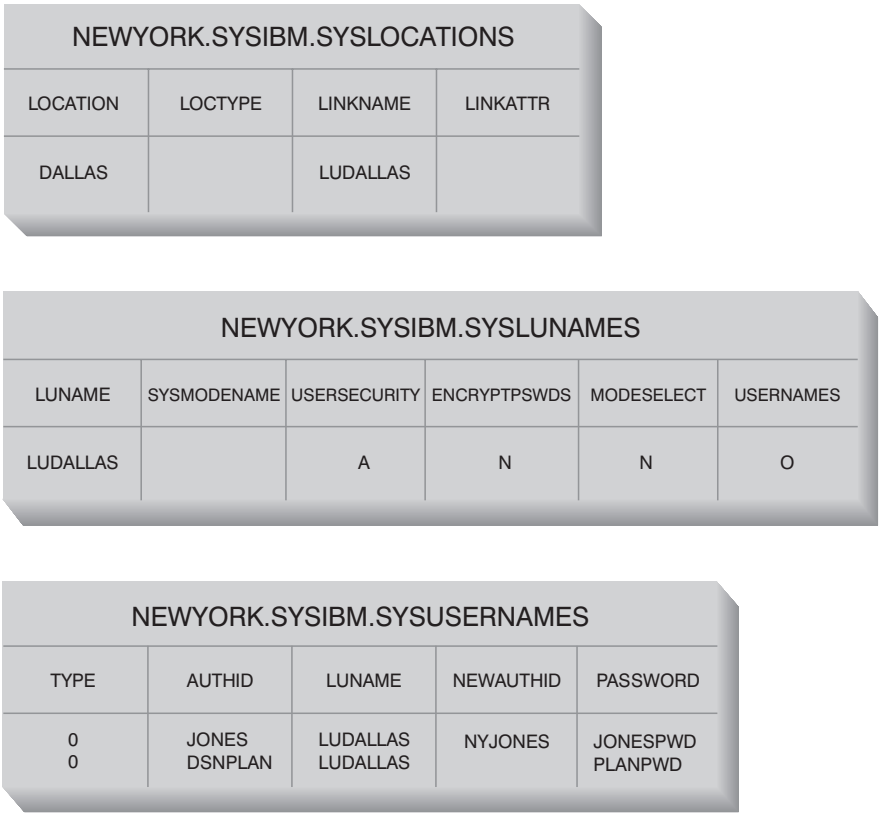
Разгледайте примера, представен по–рано. Искате да дадете на JONES в NEWYORK различно име (NYJONES), когато JONES изпълнява заявки към разпределената база данни в DALLAS. В примера приемаме, че приложението, използвано от JONES е собственост на DSNPLAN (собственик на DB2 за MVS/ESA план) и не е необходимо да преобразувате този потребителски идентификатор, когато се изпраща в DALLAS. Необходимите SQL оператори, с които да се определят правилата за преобразуване на имената в комуникационната база данни са показани в Фигура 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');
```

Фигура 6. SQL за преобразуване на изходящо име

Получените в резултат таблици на комуникационната база данни са показани в Фигура 7 на страница 18:

[2] Ако заявката се изпрати на DB2 за MVS/ESA сървър, преобразуването на имената се изпълнява за собственика на пакета и на плана. Към имената на собственика на пакета и плана никога няма асоциирана парола.



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

Фигура 7. Преобразуване на изходящи имена

Защита на мрежа

След като Средство за обработка на заявки избере имената на крайните потребители, които представляват отдалеченото приложение, Средство за обработка на заявки трябва да осигури необходимата за LU 6.2 информация за защита на мрежата. LU 6.2 осигурява три основни функции за защита на мрежата:

- Защита на ниво сесия, която се контролира от ключовата дума VERIFY на оператора VTAM APPL. Обърнете се към изложението след Фигура 5 на страница 9 за обяснение как да определите параметрите за защита на ниво сесия.
- Защита на ниво диалог, която се контролира от съдържанието на таблицата SYSIBM.SYSLUNAMES.
- Закодиране на данни, което се поддържа само за VTAM 3.4 и следващите версии на VTAM.

Тъй като Сървър на приложения е отговорен за управлението на ресурсите на базата данни, Сървър на приложения диктува кои функции за защита на мрежата да се изискват от Средство за обработка на заявки. Трябва да запишете изискванията за защита на ниво диалог за всеки Сървър на приложения в таблицата SYSIBM.SYSLUNAMES, като настроите колоната USERNAMES на таблицата SYSIBM.SYSLUNAMES да отразява изискванията на сървъра на приложенията.

Възможните опции за защита на SNA диалог са:

SECURITY=SAME

Също така е известно като вече проверена защита, защото към отдалечената система се изпраща само потребителският идентификатор на крайния потребител (не се изпраща парола). Използвайте това ниво на защита на диалог, когато колоната USERNAMES в SYSIBM.SYSLUNAMES не съдържа 'O' или 'B'.

Тъй като DB2 за MVS/ESA обвързва преобразуването на името на крайния потребител със защитата на изходящия диалог, няма да ви позволи да използвате SECURITY=SAME, когато е активирана функцията за преобразуване на името на крайния потребител.

SECURITY=PGM

В този случай към отдалечената система се изпращат идентификаторът и паролата на крайния потребител, за да се провери тяхната валидност. Използвайте тази опция на защита, когато колоната USERNAMES в таблицата SYSIBM.SYSLUNAMES съдържа 'O' или 'B'.

В зависимост от опциите, определени в таблицата SYSIBM.SYSLUNAMES, DB2 за MVS/ESA получава паролата на крайния потребител от два различни източника:

- Некодирани пароли се получават от колоната PASSWORD на таблицата SYSIBM.SYSUSERNAMES. DB2 за MVS/ESA извлича пароли от таблицата SYSIBM.SYSUSERNAMES, когато в колоната ENCRYPTPSWDS в таблицата SYSIBM.SYSLUNAMES не е въведено 'Y'. Получените от този източник пароли могат да се прехвърлят до всеки DRDA Сървър на приложения.

  Фигура 8 дефинира паролите за SMITH и JONES. Колоната LUNAME в примера съдържа празни места, така че тези пароли се използват за всяка отдалечена система, към която се SMITH или JONES се опитва да получи достъп.

```
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');
```

Фигура 8. Изпращане на пароли към отдалечени системи

- Закодираните пароли се изпращат на отдалечената система, когато колоната ENCRYPTPSWDS на SYSIBM.SYSLUNAMES съдържа 'Y'. Закодираните пароли се извличат от RACF (или продукт, еквивалентен на RACF) и могат да се интерпретират само от друга DB2 за MVS/ESA система. При комуникация със система, която не е DB2 за MVS/ESA, не определяйте ENCRYPTPSWDS да е 'Y'.

  DB2 за MVS/ESA търси в таблицата SYSIBM.SYSUSERNAMES, за да определи дали да се прехвърля потребителският идентификатор (стойността NEWAUTHID) към отдалечената система. Така преобразуваното име се използва за извличане на RACF паролата. Ако не искате да преобразувате имената, трябва да създадете редове в SYSIBM.SYSUSERNAMES, които да указват да се изпращат имената без преобразуване. Фигура 9 на страница 20 позволява заявките да се изпращат на LUDALLAS и LUNYC без преобразуване на името на крайния потребител (потребителски идентификатор).

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

Фигура 9. Изпращане на закодирани пароли към отдалечени системи

SECURITY=NONE
: Тази опция не се поддържа от DRDA, така че DB2 за MVS/ESA не обезпечава тази опция за защита.

Защита на мениджъра на базата данни

Един начин Средство за обработка на заявки да участва в защитата на разпределена база данни е чрез преобразуване на изходящите имена, както беше посочено по–горе в “Избиране имена на крайни потребители” на страница 16. Можете да използвате преобразуването на изходящите имена, за да управлявате достъпа до всеки Сървър на приложения на базата на самоличността на крайния потребител, който изпраща заявката и приложението, което я генерира. Други начини, чрез които DB2 за MVS/ESA Средство за обработка на заявки дава своя принос в защитата на разпределената система са:

Изграждане на отдалечени приложения
: Крайните потребители свързват отдалечените програми на Сървър на приложения с командата на DB2 за MVS/ESA BIND PACKAGE. DB2 за MVS/ESA *не* ограничава използването на командата BIND PACKAGE на рикуестъра. Но крайният потребител не може да използва отдалечен пакет, докато пакетът не се включи в план на DB2 за MVS/ESA. DB2 за MVS/ESA *наистина* ограничава използването на командата BIND PLAN. Краен потребител не може да добави отдалечен пакет към план, освен ако не са му предоставени правата BIND или BINDADD с помощта на оператора на DB2 за MVS/ESA GRANT.

  При свързване на пакет използвайте опцията ENABLE/DISABLE, за да определите дали пакетът да се използва от TSO, CICS/ESA, IMS/ESA или от отдалечена DB2 за MVS/ESA подсистема.

Изпълнение на отдалечени приложения
: За да може краен потребител на DB2 за MVS/ESA да изпълни отдалечено приложение, той трябва да има право да изпълни DB2 за MVS/ESA плана, свързан с това приложение. Собственикът на DB2 за MVS/ESA план автоматично има право да го изпълнява. На други крайни потребители може да се предоставят права за изпълнение на плана, като се използва операторът на DB2 за MVS/ESA GRANT EXECUTE. По този начин собственикът на приложение в разпределена база данни може да контролира използването на приложението на база на отделни потребители.

Подсистема за защита

Външната подсистема за защита на MVS системите се осигурява от RACF и други продукти, които предоставят интерфейс, съвместим с RACF. DB2 за MVS/ESA Средство за обработка на заявки няма директни обръщения към външната подсистема за защита, с изключение на поддръжката на закодирани пароли, описана в “Защита на мрежа” на страница 18. Обаче външната подсистема за защита се използва косвено от Средство за обработка на заявки при следните ситуации:

- Продуктът, който отговаря за отдалечено свързване на ниво потребителски модел на крайния потребител към DB2 за MVS/ESA, използва външната подсистема за защита, за да провери валидността на крайния потребител (потребителски идентификатор и парола). Това става преди крайният потребител да се свърже на ниво потребителски модел към DB2 за MVS/ESA. Както беше посочено по–горе, CICS/ESA, TSO и IMS/ESA са примери за продукти, които свързват крайни потребители към DB2 за MVS/ESA.
- Ако използвате защита на ниво SNA сесия (чрез ключовата дума VERIFY на оператора на DB2 за MVS/ESA VTAM APPL), VTAM се обръща към външната подсистема за защита за проверка на идентичността на отдалечената система.

Представяне на данни

DB2 за MVS/ESA се доставя, като по подразбиране при инсталирането идентификаторът на кодиран набор символи (CCSID) е 500. Тази стойност по подразбиране вероятно *няма* да е правилна за вашата инсталация.

При инсталирането на DB2 за MVS/ESA, трябва да определите така инсталационния идентификатор CCSID, че да съответства на идентификатора CCSID на символите, генерирани и изпратени към DB2 за MVS/ESA от входните устройства на вашата система. Този CCSID обикновено се определя от използвания национален език. Ако инсталационният CCSID не е правилен, при конвертирането на символите ще се получат неправилни резултати. В *DB2 Connect: Ръководство на потребителя* можете да видите списък с поддържаните идентификатори CCSID за всяка държава или национален език.

Трябва да се уверите, че вашата DB2 за MVS/ESA подсистема има възможността да конвертира от идентификатора CCSID на всеки сървър на приложения до инсталационния CCSID на вашата DB2 за MVS/ESA подсистема. DB2 за MVS/ESA осигурява таблици за конвертиране за най–разпространените комбинации от CCSID идентификатор на източник и приемник, но не и за всички възможни комбинации. Ако е необходимо, можете да добавите множество от таблици за конвертиране и процедури за конвертиране. Обърнете се към *Ръководството за администриране на DB2* за допълнителна информация за конвертирането на символи от DB2 за MVS/ESA.

Настройка на сървъра на приложения

Поддръжката на сървър на приложения в DB2 за MVS/ESA позволява на DB2 за MVS/ESA да действа като сървър за DRDA рикуестър на приложения. Средство за обработка на заявки, свързан към DB2 за MVS/ESA Сървър на приложения може да е:

- DB2 за MVS/ESA рикуестър
- DB2 Connect Версия 7, която може да работи на AIX, HP–UX, OS/2, SCO, Solaris, Linux, Windows 9x или Windows NT.
- DB2 Universal Database Enterprise Edition Версия 7 или DB2 Universal Database Extended – Enterprise Edition с активирана поддръжка на DB2 Connect.
- Рикуестър Distributed Database Connection Services (DDCS) Версия 2, който може да работи на AIX, HP–UX, OS/2, Solaris, Windows 3.1, Windows 3.11 for Workgroups, Windows 95 или Windows NT, както и на SCO, SGI или SINIX.
- OS/400 рикуестър
- DB2 за VM рикуестър
- Всеки друг продукт, който поддържа протоколите DRDA Средство за обработка на заявки

За всяко Средство за обработка на заявки, свързано към DB2 за MVS/ESA Сървър на приложения, DB2 за MVS/ESA Сървър на приложения поддържа достъп до база данни както следва:

- На Средство за обработка на заявки е разрешен достъп до таблиците, записани на DB2 за MVS/ESA сървъра на приложения. Средство за обработка на заявки трябва да създаде пакет на DB2 за MVS/ESA Сървър на приложения, преди да може да се изпълни приложението. DB2 за MVS/ESA Сървър на приложения използва пакета, за да намери SQL операторите на приложението по време на изпълнението.
- Средство за обработка на заявки може да информира DB2 за MVS/ESA Сървър на приложения, че достъпът трябва да е ограничен само до четене, ако DRDA връзката рикуестър–сървър не поддържа двуфазовия протокол за записване на промените. Например, DB2 за MVS/ESA V2R3 рикуестър със CICS front end ще информира DB2 за MVS/ESA сървъра на приложения, че не са позволени обновявания.
- Освен това на Средство за обработка на заявки може да е разрешен достъп до таблици, съхранени на други DB2 за MVS/ESA системи в мрежата с помощта на насочван от системата достъп. Насочваният от системата достъп позволява на средство за обработка на заявки да установи свързване към няколко бази данни в една единица работа.

Осигуряване на мрежова информация

За да може DB2 за MVS/ESA Сървър на приложения правилно да обработва заявки към разпределени бази данни, трябва да изпълните следните стъпки:

1. Да дефинирате сървъра на приложения на локалната Комуникационен мениджър.
2. Да дефинирате разположението на всеки потенциален вторичен сървър, така че DB2 за MVS/ESA сървърът на приложения да може да пренасочва SQL заявките към техните крайни местоположения.
3. Да осигурите необходимата защита.
4. Да осигурите представянето на данните.

Дефиниране на сървър на приложения

За да може Сървър на приложения да получава заявки към разпределени бази данни, трябва да е дефиниран в локалната Комуникационен мениджър и да има уникално име RDB_NAME. За да дефинирате Сървър на приложения, трябва да изпълните следните стъпки:

1. Изберете LU името и RDB_NAME, което ще се използва от DB2 за MVS/ESA Сървър на приложения. Записването на тези имена в DB2 за MVS/ESA и VTAM става по същия начин, както е описано в “Дефиниране на локалната система” на страница 7. Избраното от вас RDB_NAME за DB2 за MVS/ESA трябва да се достави на всички крайни потребители и Средство за обработка на заявки, които изискват свързваемост към Сървър на приложения.
2. Регистрирайте стойността NETID.LUNAME за DB2 за MVS/ESA Сървър на приложения с всеки Средство за обработка на заявки, който изисква достъп, така че Средство за обработка на заявки да може да насочва SNA заявките към DB2 за MVS/ESA сървъра. Това е така дори за случаите, при които Средство за обработка на заявки може да изпълни динамично мрежово маршрутизиране, тъй като Средство за обработка на заявки трябва да знае стойността NETID.LUNAME, преди да може да използва динамичното мрежово маршрутизиране.

3. Осигурете стойността по подразбиране за DRDA TPN (X'07F6C4C2') за всяко Средство за обработка на заявки, тъй като DB2 за MVS/ESA автоматично я използва.
4. Създайте запис във VTAM таблицата с режимите за всяко име на режим, което е заявено от Средство за обработка на заявки. Тези записи описват RU размерите, стъпката в размера на пакета и класа на услугите за всяко име на режим.
5. Дефинирайте максималния брой сесии за Средство за обработка на заявки, които могат да се свързват с DB2 за MVS/ESA Сървър на приложения. Операторът VTAM APPL дефинира максималния брой сесии по подразбиране за всички партньори. Ако искате да установите различна стойност по подразбиране за определен партньор, можете да използвате таблицата SYSIBM.SYSLUMODES на комуникационната база данни (CDB).

   Вижте “Определяне RU размерите и стъпките” на страница 15 за информация как да прегледате вашата VTAM мрежа.
6. Създайте записи в DB2 за MVS/ESA CDB, за да определите кои Средство за обработка на заявки могат да се свързват към DB2 за MVS/ESA Сървър на приложения. Двата основни подхода за дефиниране записите на CDB за Средство за обработка на заявки в мрежата са:
   a. Можете да вмъкнете ред в SYSIBM.SYSLUNAMES, който осигурява стойности по подразбиране, които да се използват за всяка LU, която не е специфично описана в CDB (редът по подразбиране съдържа празни полета в колоната LUNAME). Този подход ви позволява да дефинирате специфични атрибути за някои LU в мрежата, а да установите стойността по подразбиране за всички останали LU.

      Например можете да позволите на DALLAS системата (друга DB2 за MVS/ESA система), да изпраща вече проверени за валидност заявки към разпределени бази данни (LU 6.2 SECURITY=SAME), но да изисквате мениджър на базата данни системите да изпращат пароли. Освен това може да не искате да въвеждате запис в CDB за всяка мениджър на базата данни система, особено ако има голям брой такива системи. Фигура 10 показва как CDB може да се използва, за да се определи SECURITY=SAME за DALLAS системата, а да се наложи SECURITY=PGM за всички други системи, които изпращат заявки.

```
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', ' ');
```

Фигура 10. Установяване на стойности по подразбиране при свързване на рикуестър на приложения

   b. Можете да използвате CDB, за да проверява правата отделно за всеки Средство за обработка на заявки в мрежата, като настроите CDB по един от следните начини:
      - Не записвайте ред по подразбиране в SYSIBM.SYSLUNAMES. Ако няма ред по подразбиране (ред с празно име на LU), DB2 за MVS/ESA изисква по един ред в SYSIBM.SYSLUNAMES с името на LU за всеки рикуестър на приложения, който се опитва да се свърже. Ако CDB не съдържа съответния ред, Средство за обработка на заявки не разрешава достъпа.

- Запишете ред по подразбиране в SYSIBM.SYSLUNAMES, който да определи, че е необходима проверка откъде идва (колоната USERNAMES е установена на 'I' или 'B'). Така DB2 за MVS/ESA позволява достъп само на тези Средство за обработка на заявки и крайни потребители, които да дефинирани в таблицата SYSIBM.SYSUSERNAMES, както е описано в “Проверка откъде идва” на страница 27 . Може да предпочетете да използвате този подход, ако правилата за преобразуване на имената изискват ред с празно име LU в SYSIBM.SYSLUNAMES, но не искате DB2 за MVS/ESA да използва този ред, за да позволи неограничен достъп до DB2 за MVS/ESA Сървър на приложения.

  В Фигура 11 няма ред с празно поле в колоната LUNAME, така че DB2 за MVS/ESA отказва достъп на всяка LU, различна от LUDALLAS или 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', ' ');
```

Фигура 11. Идентифициране при свързвания на отделни рикуестъри за приложения

Дефиниране на вторични сървъри

DB2 за MVS/ESA не реализира сървър на база данни така, както е дефинирано в DRDA. Вместо това DB2 за MVS/ESA осигурява вторични сървъри, които осигуряват достъп до няколко DB2 за MVS/ESA системи в отделна единица работа с помощта на достъп, насочван от системата.

SQL разлики: SQL, който се поддържа при насочван от системата достъп, се различава значително от DRDA отдалечена единица работа:

- SQL операторът CONNECT не се използва за установяване на свързване към вторичен сървър. Вместо него достъпът до сървъра се осъществява, като се определят имената от три части на SQL обект. Например следният SQL оператор се насочва към сървъра с достъп, насочван от системата CHICAGO:

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

- Не са позволени SQL DDL оператори (например CREATE).
- Насочваният от системата достъп не поддържа отдалечено свързване (например BIND PACKAGE), така че не е необходимо да свързвате вашето приложение на сървър с достъп, насочван от системата, преди да се опитате да изпълните приложението.
- Към вторичния сървър могат да се изпращат статични или динамични SQL оператори, но всички оператори се генерират динамично. Това е така, защото вторичният сървър няма план или пакет със SQL операторите на приложението, така че не е възможно да избере предварително пътеките за достъп до база данни.
- Едно SQL приложение може едновременно да осъществи достъп до няколко вторични сървъри.
- Повече от една DB2 за MVS/ESA система може да е приемник за SQL обновявания в контекста на дадено записване на промените.
- Приложение може да използва няколко LU 6.2 диалога към вторичен сървър в контекста на едно записване на промените. Обикновено DB2 за MVS/ESA Сървър на приложения създава един LU 6.2 диалог за всяко SQL запитване,

което е само за четене. Така вторичният сървър може да предвиди FETCH заявките на SQL приложението и да изпрати набора за отговор, преди на практика да е заявен от приложението.

SQL имена на обекти: Когато DB2 за MVS/ESA Сървър на приложения получи SQL заявка, проверява името на SQL обекта, за да определи дали обектът се намира в мрежата. DB2 за MVS/ESA приема имена на SQL обекти от една, две или три части, като името приема една от следните форми:

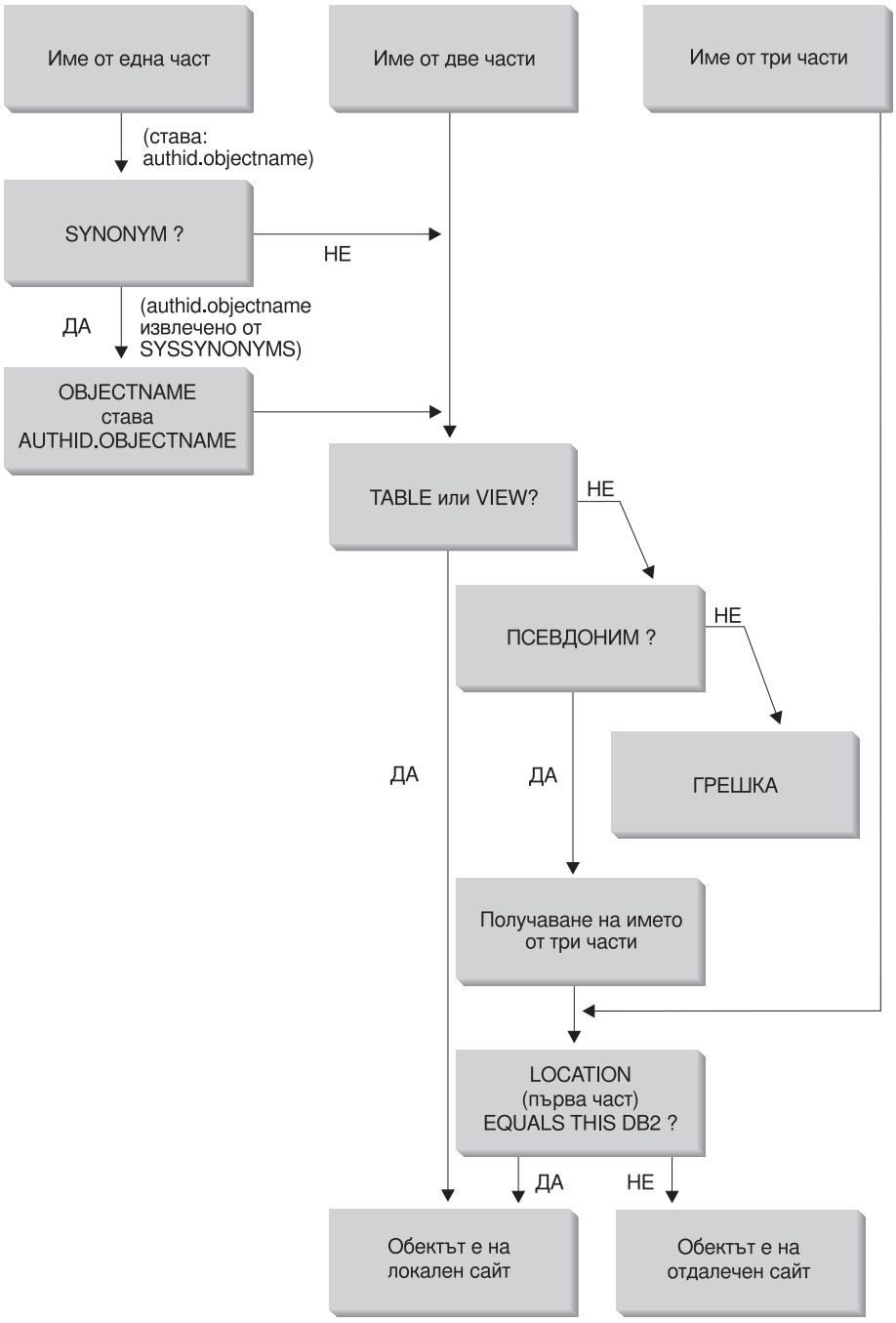
objectname определя името на DB2 за MVS/ESA таблица, производна таблица, синоним или псевдоним.

authid.objectname определя собственика на обекта и името на обекта.

location.authid.objectname определя системата–собственик, потребителя–собственик и името на обекта.

Ако името на мястото (първата част в име на обект от три части) съответства на RDB_NAME на локалната DB2 за MVS/ESA система, заявката определя локален DB2 за MVS/ESA обект.

Ако не съответства на RDB_NAME на локалната DB2 за MVS/ESA система, DB2 за MVS/ESA Сървър на приложения пренасочва заявката към системата, определена от името на местоположението с помощта на достъп, насочван от системата. Системата приемник трябва да е друга DB2 за MVS/ESA система, тъй като насочваният от системата достъп се поддържа само между DB2 за MVS/ESA системи. Насочваният от системата достъп не поддържа никакви функции за отдалечено свързване на приложения, така че не е необходимо да свързвате приложенията на сървъра, преди да ги използвате. Фигура 12 на страница 26 обобщава процеса, използван от DB2 за MVS/ESA за анализиране имената на SQL обектите.



Фигура 12. DB2 за MVS/ESA анализ на имена на SQL обекти

Дефиниране на сървър: Ако DB2 за MVS/ESA Сървър на приложения трябва да пренасочва SQL заявки, трябва да дефинирате всеки вторичен сървър в CDB и VTAM. По–голяма част от дефинирането е подобно на процеса, описан в “Дефиниране на отдалечени системи” на страница 11. За да свържете вторични сървъри, направете следното:

1. Запишете стойностите RDB_NAME и LU име за всеки сървър в CDB и VTAM. Стойността TPN, използвана при насочван от системата достъп е различна от DRDA стойността по подразбиране. Но тази разлика не е от значение, защото DB2 за MVS/ESA автоматично избира правилната стойност.

2. В SYSIBM.SYSLUNAMES дефинирайте изискванията към защитата за всеки вторичен сървър. Този процес е описан в “Осигуряване на защита” на страница 16.
3. Дефинирайте името на режима (или имената), използван между DB2 за MVS/ESA Сървър на приложения и вторичните сървъри и поставете тези имена на режими във VTAM таблицата с режимите. Името на режима по подразбиране е IBMDB2LM.
4. Дефинирайте максималния брой сесии за всеки вторичен сървър. Използва се същия процес за определяне на максималния брой сесии както описания в “Дефиниране на локалната система” на страница 7. Насочваният от системата достъп може да установи няколко диалога за всяко SQL приложение. Може да е необходимо да установите по–голям максимален брой сесии при свързвания с насочван от системата достъп, отколкото при DRDA свързвания. Вижте “Свързване на разпределени бази данни” в *Ръководство за администриране на DB2* за специфичните подробности за това как да изчислите броя на LU 6.2 сесиите, необходими за приложенията с достъп, насочван от системата.

Като собственик на ресурси в база данни, вторичният сървър управлява защитата в базата данни за SQL обектите, които се намират на сървъра. Обаче тази отговорност се поделя с DB2 за MVS/ESA Сървър на приложения, който прави заявката. Сървърът управлява достъпа до SQL обектите както следва:

- Вторичният сървър няма копие на DB2 за MVS/ESA плана, така че DB2 за MVS/ESA Сървър на приложения, който се обръща към него, трябва да провери дали крайният потребител има право да изпълни пакета на системата (Сървър на приложения).
- Статичните SQL оператори се изпълняват динамично на вторичния сървър, като се използват правата, предоставени от собственика на DB2 за MVS/ESA пакета на заявяващия DB2 за MVS/ESA Сървър на приложения.
- Динамичните SQL оператори се изпълняват с помощта на правата, предоставени на крайния потребител на Средство за обработка на заявки.

Осигуряване на защита

Когато Средство за обработка на заявки насочи заявка за разпределена база данни към DB2 за MVS/ESA Сървър на приложения, са включени следните съображения, свързани със защитата:

- Проверка откъде идва
- Избиране на имена на крайни потребители
- Параметри за защита на мрежата
- Защита на мениджъра на базата данни
- Защита, прилагана от външна подсистема за защита

Проверка откъде идва

Когато DB2 за MVS/ESA Сървър на приложения получи име на краен потребител от Средство за обработка на заявки, Сървър на приложения може да наложи ограничение върху имената на крайните потребители, получени от даден Средство за обработка на заявки. Това се постига чрез използването на проверката *откъде идва*. Проверката откъде идва позволява на Сървър на приложения да определи, че даден потребителски идентификатор може да се използва само от определени партньори. Например, Сървър на приложения може да ограничи JONES да “идва от” DALLAS. Ако друго Средство за обработка на заявки (различен от DALLAS) се опита да изпрати името JONES на Сървър на приложения, тогава Сървър на

приложения може да отхвърли заявката, защото името не идва от правилно местоположение в мрежата.

DB2 за MVS/ESA реализира проверка откъде идва като част от преобразуването на входящите имена на крайни потребители, описано в следващия раздел.

Избиране на имена на крайни потребители

Потребителският идентификатор, предаден от Средство за обработка на заявки може да не е уникален в рамките на цялата SNA мрежа. Може да е необходимо DB2 за MVS/ESA Сървър на приложения да изпълни преобразуване на входящите имена, за да създаде уникални имена на крайни потребители в рамките на SNA мрежата. Аналогично може да е необходимо DB2 за MVS/ESA Сървър на приложения да изпълни преобразуване на изходящите имена, за да осигури уникални имена на крайни потребители за вторичните сървъри, използвани в приложението (вижте “Осигуряване на защита” на страница 16 за информация относно преобразуването на изходящите имена на крайните потребители).

Преобразуването на входящите имена се активира, като в колоната USERNAMES на таблицата SYSIBM.SYSLUNAMES се въведе стойността `'I'` (inbound translation–входящо преобразуване) или `'B'` (both inbound and outbound translation – едновременно входящо и изходящо преобразуване). Когато е в сила преобразуване на входящи имена, DB2 за MVS/ESA конвертира потребителския идентификатор, изпратен от Средство за обработка на заявки и името на собственика на DB2 за MVS/ESA плана (ако Средство за обработка на заявки е друга DB2 за MVS/ESA система).

Ако Средство за обработка на заявки изпрати едновременно потребителски идентификатор и парола с помощта на APPC функцията ALLOCATE, се проверява тяхната валидност преди преобразуването на потребителския идентификатор. Колоната PASSWORD в SYSIBM.SYSUSERNAMES не се използва за проверка валидността на паролата. Вместо това потребителският идентификатор и паролата се представят на външната система за защита (RACF или еквивалентен на RACF продукт), за да се провери валидността.

Когато се проверява входящ потребителски идентификатор на функцията ALLOCATE, DB2 за MVS/ESA има оторизационни изходи, които можете да използвате, за да осигурите списък с вторични идентификатори AUTHID и да изпълните допълнителни проверки. За подробности вижте *Ръководство за администриране на DB2*.

При преобразуването на входящото име се търси ред в таблицата SYSIBM.SYSUSERNAMES, който трябва да отговаря на един от образците, показани в следния списък (TYPE.AUTHID.LUNAME):

1. I.AUTHID.LUNAME—Специфичен краен потребител от специфичен Средство за обработка на заявки
2. I.AUTHID.blank—Специфичен краен потребител от произволен Средство за обработка на заявки
3. I.blank.LUNAME—Произволен краен потребител от специфичен Средство за обработка на заявки

Достъпът са отказва, ако не се намери ред. Ако се намери ред, се позволява отдалечен достъп и името на крайния потребител се променя на стойността, осигурена в колоната NEWAUTHID, като празна стойност NEWAUTHID показва, че името не е променено. Всички DB2 за MVS/ESA проверки за оторизация за ресурси (например права за SQL таблица), изпълнени от DB2 за MVS/ESA, се изпълняват върху преобразуваните имена на потребители, вместо върху първоначалните.

Когато DB2 за MVS/ESA Сървър на приложения получи име на краен потребител от Средство за обработка на заявки, могат да се постигнат редица задачи с помощта на възможността на DB2 за MVS/ESA за преобразуване на входящите имена:

- Можете да промените името на крайния потребител, така че да стане уникално. Например, следните SQL оператори преобразуват името на крайния потребител JONES от рикуестъра за приложения NEWYORK (LUNAME LUNYC) до различно име (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', ' ');
```

- Можете да промените името на крайния потребител така, че група потребители да се представят с едно име. Например, може да искате да представите всички потребители от NEWYORK Средство за обработка на заявки (LUNAME LUNYC) с името на потребител NYUSER. Така можете да предоставите SQL права на името NYUSER и да контролирате SQL достъпа, който се предоставя на потребителите от 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', ' ');
```

- Можете да ограничите имената на крайните потребители, предавани от определен Средство за обработка на заявки. Това приложение на възможността за преобразуване имената на крайните потребители изпълнява проверката откъде идва, описана в “Проверка откъде идва” на страница 27. Например, следващите SQL оператори позволяват използването само на SMITH и JONES като имена на крайни потребители от Средство за обработка на заявки NEWYORK. На всяко друго име ще се откаже достъп, защото не е изброено в таблицата 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', ' ', ' ');
```

- Можете да ограничите различните Средство за обработка на заявки, на които е позволено свързване към DB2 за MVS/ESA Сървър на приложения. Това е още една функция на проверката откъде идва. Следващият пример приема всяко име на краен потребител, изпратено от Средство за обработка на заявки NEWYORK (LUNYC) или Средство за обработка на заявки CHICAGO (LUCHI). На всички други Средство за обработка на заявки се отказва достъп, тъй като в реда по подразбиране на SYSIBM.SYSLUNAMES е определено преобразуване на входящото име за всички входящи заявки.

```
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', ' ', ' ');
```

Осигуряване на мрежова защита

LU 6.2 осигурява три основни функции за защита на мрежата:

- Защита на ниво сесия
- Защита на ниво диалог
- Закодиране

“Защита на мрежа” на страница 18 представя как да се определи защита на ниво сесия и закодиране с DB2 за MVS/ESA. DB2 за MVS/ESA Сървър на приложения използва защита на ниво сесия и закодиране по абсолютно същия начин както DB2 за MVS/ESA Средство за обработка на заявки.

Остава само да се разгледа защитата на ниво SNA диалог. Някои аспекти на защитата на ниво диалог са уникални за DB2 за MVS/ESA Сървър на приложения. DB2 за MVS/ESA Сървър на приложения играе две отделни роли в защитата на мрежата:

- Като рикуестър към вторични сървъри DB2 за MVS/ESA Сървър на приложения отговаря за генерирането на APPC заявки, които съдържат параметрите за защита на ниво SNA диалог, необходими за вторичните сървъри. DB2 за MVS/ESA Сървър на приложения използва колоната USERNAMES на таблицата SYSIBM.SYSLUNAMES и таблицата SYSIBM.SYSUSERNAMES, за да дефинира изискванията за защитата на ниво SNA диалог за всеки вторичен сървър. Елементите на тези дефиниции са идентични с дефинициите в “Защита на мрежа” на страница 18.
- Като сървър за Средство за обработка на заявки, DB2 за MVS/ESA Сървър на приложения диктува на Средство за обработка на заявки изискванията за защита на ниво SNA диалог. DB2 за MVS/ESA използва колоната USERSECURITY от таблицата SYSIBM.SYSLUNAMES, за да определи защитата на диалог, изисквана от всеки Средство за обработка на заявки в мрежата. Следните стойности се използват в колоната USERSECURITY:

  C Показва, че DB2 за MVS/ESA изисква от Средство за обработка на заявки да изпрати потребителски идентификатор и парола (LU 6.2 SECURITY=PGM) с всяка заявка за разпределена база данни. Ако колоната ENCRYPTPSWDS в SYSIBM.SYSLUNAMES съдържа 'Y', DB2 за MVS/ESA приема, че паролата вече е в закодиран формат на RACF (това е възможно само за DB2 за MVS/ESA Средство за обработка на заявки). Ако колоната ENCRYPTPSWDS не съдържа 'Y', DB2 за MVS/ESA очаква паролата в стандартния формат LU 6.2 (EBCDIC представяне на символите). И в двата случая DB2 за MVS/ESA предава стойностите за потребителски идентификатор и парола за проверка на подсистемата за защита. Трябва да имате подсистема за защита, която осигурява проверка на APPC потребителски идентификатор и парола; например RACF има възможност да направи това. Ако подсистемата за защита отхвърли

двойката потребителски идентификатор–парола, се отказва достъпът до разпределената база данни.

Всички други стойности
Показва, че Средство за обработка на заявки може да изпрати или вече проверен потребителски идентификатор (LU 6.2 SECURITY=SAME), или потребителски идентификатор и парола (LU 6.2 SECURITY=PGM). Ако се изпратят потребителски идентификатор и парола, DB2 за MVS/ESA ги обработва, както е описано за стойността 'C' по–горе. Ако заявката съдържа само потребителски идентификатор, се генерира обръщение към подсистемата за защита, за да разпознае потребителя, освен ако не се използва таблицата SYSUSERNAMES за управление на входящи потребителски идентификатори.

Ако възникне нарушаване на защитата, LU 6.2 изисква от DB2 за MVS/ESA Сървър на приложения да върне SNA код на състояние за грешка в защитата ('080F6051'X) на Средство за обработка на заявки. Тъй като този код на състояние не описва причината за проблема, DB2 за MVS/ESA осигурява два метода за записване на причините за нарушаване защитата на разпределена система:

- Генерира се съобщение DSNL030I, което осигурява LUWID на рикуестъра и кода за причина на DB2 с описание за проблема. Освен това DSNL030I включва изпратения от отхвърлената заявка за приложение AUTHID, ако е известен.
- Предупреждение се записва в NETVIEW базата данни за следене на хардуера, което съдържа същата информация, както осигурената в съобщението DSNL030I.

Защита на мениджъра на базата данни

Като собственик на ресурси в база данни, DB2 за MVS/ESA Сървър на приложения контролира функциите за защита на SQL обектите, които се намират на DB2 за MVS/ESA Сървър на приложения. Достъпът до управляваните от DB2 за MVS/ESA обекти се контролира от правата, които се предоставят на потребителите от администратора на DB2 за MVS/ESA или от собствениците на отделните обекти. Двата основни класа обекти, които се управляват от DB2 за MVS/ESA Сървър на приложения, са:

- **Пакети**—Отделните крайните потребители имат право да създават да заменят и да изпълняват пакети с помощта на оператора на DB2 за MVS/ESA GRANT. Когато краен потребител е собственик на пакет, той може да изпълнява или да заменя пакета. На другите крайни потребители трябва специално да им е предоставено правото да изпълняват пакета на DB2 за MVS/ESA Сървър на приложения с оператора GRANT. Възможността USE може да се предостави на отделни крайни потребители или на PUBLIC, което означава, че всички крайни потребители могат да изпълняват пакета.

  При свързване на приложение към DB2 за MVS/ESA пакетът съдържа SQL операторите, които се намират в приложната програма. Тези SQL оператори са класифицирани като:

  Статичен SQL
  Статичен SQL означава, че SQL операторът и SQL обектите, които се съдържат в израза са известни в момента, когато приложението се свързва с DB2 за MVS/ESA. Този, който създава пакета, трябва да има право да изпълнява всеки от статичните SQL оператори, които се съдържат в пакета.

  Когато крайни потребители получат право да изпълняват пакет, те автоматично имат право да изпълняват всеки от статичните SQL оператори, които се съдържат в него. Затова не е необходима никаква

таблица на DB2 за MVS/ESA с права на достъп за крайните потребители, ако пакетът съдържа само статични SQL оператори.

Динамичен SQL

Динамичният SQL описва SQL израз, който не е известен, преди изпълнението на програмата. С други думи, SQL изразът се изгражда от програмата и динамично се свързва с DB2 за MVS/ESA с помощта на оператора SQL PREPARE. Когато краен потребител изпълнява динамичен SQL оператор, потребителят трябва да има таблицата с права на достъп, необходима за изпълнението на SQL израза. Тъй като SQL изразът не е известен при създаването на плана или пакета, крайният потребител не може автоматично да получи необходимите права като собственик на пакета.

- **SQL обекти**— Това са таблици, производни таблици, синоними или псевдоними. На потребителите на DB2 за MVS/ESA може да се предоставят различни нива с права на достъп, за да създават, изтриват, променят или четат отделни SQL обекти. Тези права са необходими, за да се свържат статични SQL изрази или да се изпълнят динамични SQL изрази.

Когато създавате пакет, опцията DISABLE/ENABLE ви позволява да контролирате кои типове DB2 за MVS/ESA свързване могат да стартират пакета. Можете да използвате RACF и DB2 за MVS/ESA процедури за изход при защита, за да можете избирателно да разрешавате на крайни потребители да използват DDF. С помощта на RLF можете да определите ограничения върху процесорното време за отдалечени свързвания и изпълнение на динамичен SQL.

Да разгледаме пакета на DB2 за MVS/ESA с име MYPKG, чийто собственик е JOE. JOE може да позволи на SAL да изпълни пакета с помощта на DB2 за MVS/ESA оператора GRANT USE. Когато SAL изпълни пакета, възниква следното:

- DB2 за MVS/ESA проверява дали на SAL е предоставено право за използване USE за пакета.
- SAL може да използва всеки статичен SQL израз в пакета, защото JOE е имал необходимите права за SQL обекти, за да създаде пакета.
- Ако пакетът има динамични SQL изрази, SAL трябва да има своя собствена SQL таблица с права на достъп. Например, SAL не може да използва SELECT * FROM JOE.TABLE5, освен ако на нея не е предоставен достъп за четене до JOE.TABLE5.

Подсистема за защита

Използването на подсистема за защита (RACF или еквивалентна на RACF) от DB2 за MVS/ESA Сървър на приложения зависи от това как дефинирате функцията за преобразуване на входящите имена в таблицата SYSIBM.SYSLUNAMES:

- Ако определите 'I' или 'B' за колоната USERNAMES, преобразуването на входящи имена е активно и DB2 за MVS/ESA приема, че администраторът на DB2 за MVS/ESA използва тази функция, за да изпълни част от действията при защитата на системата. Външната подсистема за защита се извиква, само ако Средство за обработка на заявки изпрати заявка, която съдържа едновременно потребителски идентификатор и парола (SECURITY=PGM). Трябва да имате подсистема за защита, която осигурява проверка на APPC потребителски идентификатор и парола; например RACF има възможност да направи това.

  Ако заявката от Средство за обработка на заявки съдържа само потребителски идентификатор (SECURITY=SAME), изобщо няма да има обръщение към външната подсистема за защита, защото правилата за преобразуване на входящите имена определят кои потребители могат да се свързват към DB2 за MVS/ESA Сървър на приложения.

- Ако определите нещо различно от 'I' или 'B' за колоната USERNAMES, се изпълняват следните проверки от подсистемата за защита:
  - — Когато Средство за обработка на заявки получи заявка на разпределена база данни, DB2 за MVS/ESA се обръща към външната подсистема за защита, за да провери валидността на потребителския идентификатор на крайния потребител (и паролата, ако е осигурена).
  - — Външната подсистема за защита се извиква да провери дали крайният потребител има право да се свързва към DB2 за MVS/ESA подсистемата.
- И в двата случай се осигурява изход при оторизацията, за да се осигури списък с вторични идентификатори за оторизация. За повече информация вижте *Ръководство за администриране на DB2*.

Представяне на данни

Трябва да се уверите, че вашата DB2 за MVS/ESA подсистема има възможността да конвертира от идентификатора CCSID на всеки сървър на приложения до инсталационния CCSID на вашата DB2 за MVS/ESA подсистема. За допълнителна информация се обърнете към “Представяне на данни” на страница 21.

Глава 2. Свързване на DB2 Universal Database за OS/390 в DRDA мрежа

DB2 Universal Database за OS/390 е система за управление на IBM релационна база данни за системите OS/390. В тази глава не са разгледани предишни версии. Вижте Глава 1, “Свързване на DB2 за MVS/ESA в DRDA мрежа” на страница 1.

Тази глава описва как да свържете DRDA рикуестъри за приложения (като DB2 Connect) към DB2 Universal Database за OS/390 сървър на приложения и как да настроите DB2 Universal Database за OS/390 рикуестъри за приложения да комуникират с DRDA сървъри на приложения като DB2 Universal Database на други системи.

Информацията в тази глава основно се съсредоточава върху свързването на различните от DRDA системи към DB2 Universal Database за OS/390 чрез SNA мрежови връзки. DB2 Universal Database за OS/390 версия 5 въведе поддръжка за комуникации с бази данни чрез собствени TCP/IP връзки (без да се използва AnyNet), така че са включени също така и някои съображения за TCP/IP свързвания. За по–подробна информация за настройка и използване на TCP/IP връзки се обърнете към *Ръководство за инсталиране на DB2 Universal Database за OS/390* и *DRDA поддръжка на TCPIP с DB2 Universal Database за OS/390 и DB2 Universal Database*.

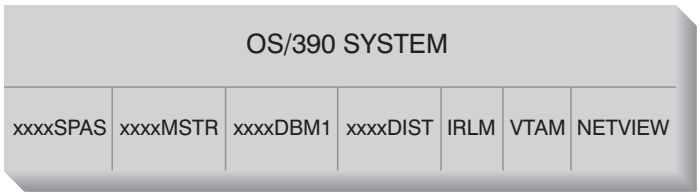
Допълнителна информация за свързването на две DB2 Universal Database за OS/390 системи или по–подробна информация, която описва как да дефинирате DRDA свързване към DB2 Universal Database за OS/390 потърсете в изложението за свързване на разпределени бази данни в *Ръководство за администриране на DB2 Universal Database за OS/390*.

Забележки:

1. С помощта на компонента AnyNet на VTAM версия 4 подверсия 2, можете да изпълнявате APPC през TCP/IP мрежа. Но потребителите на DB2 Universal Database за OS/390 версия 5.1 се насърчават да използват собствената TCP/IP поддръжка вместо компонента AnyNet APPC през TCP/IP.
2. Тази глава не съдържа никаква информация за използването на DCE.

DB2 Universal Database за OS/390

Фигура 13 на страница 36 показва OS/390 система, на която работи единично копие на DB2 Universal Database за OS/390. Освен това може да работят няколко копия на DB2 Universal Database за OS/390 на една система. За да се идентифицират копията на DB2 Universal Database за OS/390 в рамките на дадена система (или копия на DB2 Universal Database за OS/390 в рамките на JES комплекс), на всяка DB2 система се присвоява *име на подсистема* – низ с дължина от една до четири символа, който е уникален в рамките на JES комплекса. В Фигура 13 на страница 36 името на DB2 Universal Database за OS/390 подсистемата е *xxxx*. Три от имената на OS/390 адресните пространства са с префикс – името на DB2 Universal Database за OS/390 подсистемата. Тези три адресни пространства образуват DB2 Universal Database за OS/390.



Фигура 13. OS/390 адресни пространства, използвани от DB2 Universal Database за OS/390

Фигура 13 показва OS/390 адресните пространства, използвани при работата на разпределена база данни с DB2 Universal Database за OS/390. Тези адресни пространства работят заедно, за да позволят на потребителите на DB2 Universal Database за OS/390 да имат достъп до локалните релационни бази данни и да комуникират с отдалечени DRDA системи. Целта на всяко адресно пространство е както следва:

xxxxSPAS
Адресно пространство на DB2 запомнени процедури.

xxxxMSTR
Адресно пространство за системни услуги за DB2 Universal Database за OS/390 продукта, който отговаря за стартирането и спирането на DB2 Universal Database за OS/390 и контролира локалния достъп до DB2 Universal Database за OS/390.

xxxxDBM1
Адресно пространство за базата данни, като отговаря за достъп до релационни бази данни, управлявани чрез DB2 Universal Database за OS/390. Това е мястото, където се изпълнява входа и изхода от ресурсите на базата данни от името на SQL приложните програми.

xxxxDIST
Частта от DB2 Universal Database за OS/390, която осигурява възможностите на разпределена база данни; също така известно като *Средство за разпределени данни* (DDF – DISTRIBUTED DATA FACILITY). При получаване на заявка за разпределена база данни DDF я предава към *xxxx*DBM1, така че да се изпълнят необходимите входно/изходни операции към базата данни.

IRLM Мениджър за заключване, използван от DB2 Universal Database за OS/390, за да управлява достъпа до ресурсите на базата данни.

VTAM IBM Комуникационен сървър за OS/390 SNA функции (VTAM). DDF може да използва SNA или TCP/IP при комуникации с разпределена база данни от името на DB2 Universal Database за OS/390. В тази диаграма не е показано никакво адресно пространство за TCP/IP.

NETVIEW
Основният продукт за мрежово управление при OS/390 системи. Когато възникнат грешки при работа на разпределена база данни, DDF записва информацията за грешката (известна също като *предупреждение*) в базата данни NetView хардуерен монитор. Системните администратори могат да използват NetView, за да разгледат грешките, записани в базата данни на хардуерния монитор или да направят така, че при запис на предупреждения да се извикват автоматизирани процедури с команди.

Освен това NetView може да се използва за диагностика на VTAM комуникационни грешки. Допълнителна информация вижте в *Ръководство за определяне на проблеми в разпределена релационна база данни*.

Фигура 13 не показва никакви SQL приложни програми. Когато приложна програма използва DB2 за генериране на SQL оператори, тя трябва да е прикрепена към DB2 Universal Database за OS/390 по един от следните начини:

TSO Последователностите от задания и крайните потребители, които са влезли в TSO, се свързват към DB2 Universal Database за OS/390 чрез средството за отдалечено свързване на ниво потребителски модел на TSO. Тази техника се използва при свързване на SPUFI и повечето QMF приложения към DB2 Universal Database за OS/390.

CICS/ESA
Когато CICS/ESA приложение изпрати SQL обръщение, CICS/ESA използва CICS интерфейса за отдалечено свързване, за да насочи SQL заявките към DB2 Universal Database за OS/390.

IMS/ESA
Транзакциите, които работят под управлението на IMS/ESA, използват IMS интерфейса за отдалечено свързване, за да предадат SQL изрази за обработка от DB2 Universal Database за OS/390.

DDF Средството за разпределени данни отговаря за свързване на разпределени приложения към DB2 Universal Database за OS/390.

CAF Средството за отдалечено свързване на обръщения позволява на написани от потребителите подсистеми да се свързват директно към DB2 Universal Database за OS/390.

DB2 Universal Database за OS/390 реализация

DRDA дефинира типове функции на системата за управление на базата данни. DB2 Universal Database за OS/390 поддържа отдалечена единица работа. При нея приложна програма, изпълнявана в една система, може да осъществи достъп до данни на отдалечена DBMS с помощта на SQL, осигурен от тази отдалечена DBMS.

DB2 Universal Database за OS/390 също поддържа разпределена единица работа. При нея приложна програма, изпълнявана в една система, може да осъществи достъп до данни на няколко отдалечени DBMS с помощта на SQL, осигурен от отдалечените DBMS. Допълнителна информация за типовете разпределение, дефинирани от DRDA потърсете в *DRDA Ръководство за свързваемост*.

Както е показано в Фигура 14 на страница 39, DB2 Universal Database за OS/390 поддържа три конфигурации на свързвания към разпределени база данни с помощта да два метода за достъп:

[1] *Достъпът, насочен от системата* (също така известен като използване на *DB2 Universal Database за OS/390 частен протокол*), позволява на DB2 Universal Database за OS/390 рикуестъра да се свърже към един или повече DB2 Universal Database за OS/390 сървъри. Установеното свързване между DB2 Universal Database за OS/390 рикуестъра и сървъра не се придържа към протоколите, дефинирани в DRDA и не може да се използва за свързване към DB2 Universal Database за OS/390 на продукти, които не са DB2 Universal Database за OS/390. Този тип свързване се установява чрез кодиране в приложението на имена от три части или псевдоними.

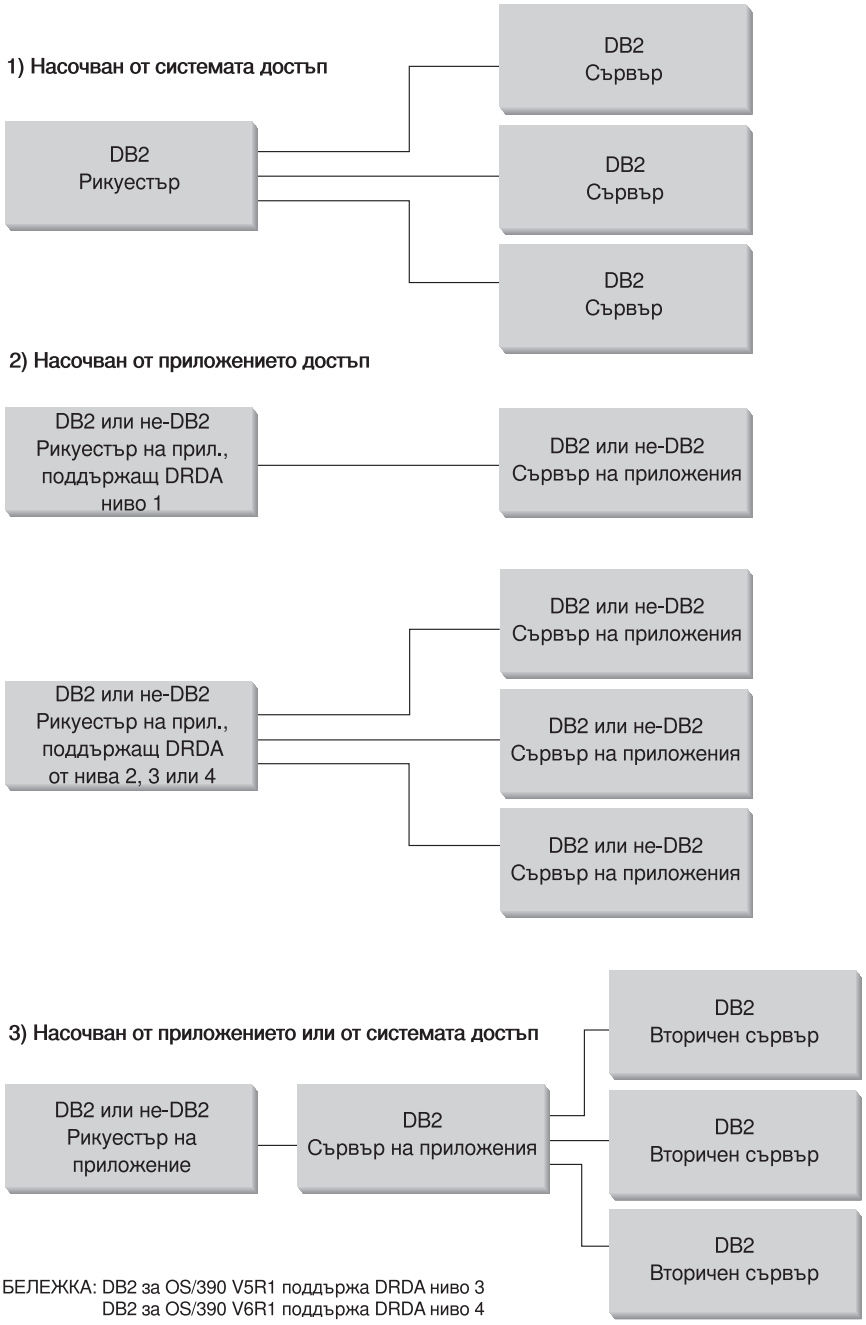
[2] *Достъпът, насочван от приложение* позволява на DB2 Universal Database за OS/390, както и на не–DB2 Universal Database за OS/390 рикуестър като DB2 Connect да се свързва към един или повече DB2 Universal Database за OS/390 или не–DB2 Universal Database за OS/390 сървъри на приложения като DB2 Universal Database и DB2 Universal Database за AS/400 с помощта на DRDA протоколи. Броят на сървърите на приложения, които могат да се свържат към рикуестъра в даден момент, зависи от версията на DB2 Universal Database за

OS/390 на рикуестъра. Ако рикуестърът е DB2 за MVS/ESA V2R3, тогава в даден момент може да е свързан само един сървър на приложения. Този тип свързване се установява чрез кодиране на SQL CONNECT оператори в приложението. Ако рикуестърът за приложения е DB2 за MVS/ESA V3R1 или следваща версия, тогава в даден момент могат да се свързват един или повече сървъри на приложения.

[3] Достъп, насочван от приложение или от системата, може да се използва съвместно при установяване на свързвания. Не можете при свързване в една и съща нишка да използвате DRDA и системно насочено съхранение.

Терминът *вторичен сървър* описва системи, действащи като сървъри на сървъри на приложения.

Ако всички системи в конфигурация поддържат двуфазов протокол за записване на промените, тогава се поддържа разпределена единица работа (многосайтово четене и многосайтово обновяване). Ако не всички системи поддържат този протокол, обновяванията в рамките на единица работа са или ограничени до отделен сайт, който не поддържа двуфазовия протокол за записване на промените, или до подмножество от сайтове, които го поддържат.



Фигура 14. DB2 Universal Database за OS/390 разпределени свързвания

Таблица 2 на страница 40 сравнява типовете свързване при DB2 Universal Database за OS/390 разпределена база данни.

Таблица 2. Сравнение на свързвания в DB2 Universal Database за OS/390 разпределена база данни

[1] Достъп, насочван от системата	**[2] Достъп, насочван от приложения (като всички системи поддържат двуфазов протокол за записване на промените)**	**[3] Достъп, насочван от приложения и от система**
Всички участници трябва да са DB2 Universal Database за OS/390 системи	Всеки две DRDA системи могат да се свързват една с друга	Рикуестър за приложения може да е всяка DRDA система; сървъри трябва да са DB2 Universal Database за OS/390 системи
Може да се свързва директно към много участници	Може да се свързва директно към много участници	Рикуестърът за приложения се свързва директно към Сървър на приложения; Сървър на приложения от своя страна могат да се свързват към много DB2 Universal Database за OS/390 вторични сървъри
Всяко SQL приложение може да има множество диалози с всеки сървър	Всяко SQL приложение има един диалог с всеки сървър	SQL приложение има по един диалог с всеки сървър; DB2 Universal Database за OS/390 сървър на приложения може да установи много диалози към всеки сървър за приложение
Има достъп както до локалните, така и до отдалечените ресурси в контекста на едно записване на промените	Има достъп както до локалните, така и до отдалечените ресурси в контекста на едно записване на промените	Рикуестър за приложения и Сървър на приложения имат достъп до локалните и отдалечени данни
По–ефективно при големи и много едновременни запитвания	По–ефективно при SQL оператори, които се изпълняват много малко пъти в контекста на едно записване на промените	Връзката рикуестър за приложения–Сървър на приложения се държи подобно на **[2]**; свързванията на вторичен сървър се държат подобно на **[1]**
Може да поддържа статичен или динамичен SQL, но сървърът динамично свързва статичния SQL при първото му изпълнение в контекста на записване на промените	Може да генерира статичен или динамичен SQL	Рикуестърът за приложения и Сървър на приложения могат да генерират статичен или динамичен SQL; вторичните сървъри поддържат статичен или динамичен SQL, но динамично свързват статичния SQL при първото му изпълнение в контекста на записване на промените
Ограничава се до SQL операторите INSERT, DELETE и UPDATE и до операторите, които поддържат SELECT	Може да използва всички оператори, поддържани от системата, която ги изпълнява	Сървърите на приложения поддържат всеки SQL; вторичните сървъри поддържат само DML SQL (например CREATE или ALTER)

Допълнителни усъвършенствания на защитата

Кодове за разширена защита

До версия 5.1 на DB2 Universal Database за OS/390 заявките за свързване, които съдържаха идентификатор или парола на потребителя, можеха да приключат неуспешно с код за причина 0 `SQL30082`, но без никакви други признаци за това какво може да е неправилно.

Във версия 5.1 на DB2 Universal Database за OS/390 беше въведено подобрението, което осигурява поддръжка на кодове за разширена защита. Ако се използва разширена защита, освен кода за причина се осигурява и допълнителна диагностична информация, като `(PASSWORD EXPIRED)`.

За да се възползвате от това, трябва да въведете стойност `ДА` за инсталационния параметър на DB2 Universal Database за OS/390 за разширена защита `ZPARM`.

Използвайте инсталационния панел на DB2 Universal Database за OS/390 DSN6SYSP, за да определите EXTSEC=YES. Освен това можете да използвате и DDF панел 1 (DSNTIPR). Стойността по подразбиране е EXTSEC=NO. Ако паролата е с изтекъл срок, PC, UNIX, Apple Macintosh и Web приложенията, които използват DB2 Connect, ще получат съобщение за грешка SQL01404.

TCP/IP защита – вече проверена

Ако искате да осигурите поддръжка за опцията за защита на DB2 Universal Database AUTHENTICATION=CLIENT, използвайте инсталационния панел на DB2 Universal Database за OS/390 DSNTIP4 (DDF панел 2), за да определите стойност ДА за параметъра, който указва дали вече е проверена TCP/IP защитата.

Настолен ODBC и защита на Java приложения

ODBC за работните станции и Java приложенията използват динамичен SQL. Това може да доведе до проблеми със защитата при някои инсталации. DB2 Universal Database за OS/390 въвежда нова опция за свързване DYNAMICRULES(BIND), която позволява изпълнението на динамичен SQL под оторизацията на собственика или на този, който е изпълнил свързването. Обърнете се към *Справочник на командите*, за да видите как DYNAMICRULES може да се определи чрез DB2 Connect.

DB2 Universal Database и DB2 Connect осигуряват нов CLI/ODBC конфигурационен параметър CURRENTPACKAGESET в конфигурационния файл DB2CLI.INI. Той трябва да съдържа името на схемата, която има съответните права на достъп. След всяко свързване към приложението автоматично ще се генерира SQL оператор SET CURRENT PACKAGESET схема.

Използвайте ODBC мениджъра, за да обновите DB2CLI.INI. Вижте *Приложение за инсталиране и конфигуриране* за допълнителна информация.

Поддръжка на промяна на парола

Ако оператор SQL CONNECT върне съобщение, което посочва, че е изтекъл срокът на валидност на паролата за потребителския идентификатор, при DB2 Connect версия 5.2 и следваща е възможно да се промени паролата, без да се преминава към TSO. С помощта на DRDA DB2 Universal Database за OS/390 може да смени паролата вместо вас.

Потребителят трябва да въведе старата парола, новата парола и да въведе повторно парола за проверка. Ако в DB2 Connect Enterprise Edition сървъра е определена защита DCS, тогава заявка за промяна на паролата се изпраща на DB2 Universal Database за OS/390 сървъра на базата данни. Ако е определена защита SERVER, тогава се променя паролата на DB2 Connect сървъра.

Допълнително предимство е, че не се изисква отделна дефиниция на LU. За допълнителна информация се обърнете към ръководството за DB2 Connect Enterprise Edition *Бърз старт*.

Настройка на рикуестър за приложения

DB2 Universal Database за OS/390 реализира поддръжка на DRDA рикуестър за приложения, като неделима част от DB2 Universal Database за OS/390 средството за разпределени данни (DDF – DISTRIBUTED DATA FACILITY). DDF може да се спре независимо от локалните средства за управление на DB2 Universal Database за OS/390 база данни, но не може да работи при липса на поддръжка от страна на локалното управление на DB2 Universal Database за OS/390 база данни.

Когато DB2 Universal Database за OS/390 действа като рикуестър за приложения, може да свързва приложения, които работят на системата към отдалечена DB2 Universal Database, DB2 за MVS/ESA, DB2 Universal Database за OS/390, DB2 Universal Database за AS/400 и DB2 за VSE и VM сървъри на база данни, които изпълняват функцията на DRDA сървър на приложения.

За да осигурите достъп до разпределена база данни при DB2 Universal Database за OS/390 Средство за обработка на заявки, трябва да направите следното:

- "Осигуряване на мрежова информация"—Средство за обработка на заявки трябва да може да приема стойностите на RDB_NAME и да ги преобразува в SNA стойности NETID.LUNAME или TCP/IP адрес. DB2 Universal Database за OS/390 използва *DB2 Universal Database за OS/390 комуникационната база данни* (CDB), за да регистрира RDB_NAME и съответните мрежови параметри. Комуникационната база данни позволява на DB2 Universal Database за OS/390 Средство за обработка на заявки да предава необходимата информация на комуникационния сървър, когато се осъществяват заявки към разпределена база данни през SNA или TCP/IP връзки.
- "Осигуряване на защита" на страница 56— За да се приемат заявки за отдалечена база данни от Сървър на приложения, Средство за обработка на заявки трябва да осигурява информацията за защита, изисквана от сървъра. DB2 Universal Database за OS/390 използва CDB и DCE, RACF или други подсистеми за защита, за да осигури необходимата информация за защита на мрежата.
- "Представяне на данни" на страница 62—Трябва да сте сигурни, че CCSID на рикуестъра на приложения е съвместим със сървъра на приложения.

Осигуряване на мрежова информация

Голяма част от обработките в среда на разпределена база данни изисква обмен на съобщения с други системи във вашата мрежа. За да се изпълнят правилно тези обработки, трябва да направите следното:

1. Дефинирайте локалната система
2. Дефинирайте отдалечената система
3. Дефинирайте комуникациите (за SNA или TCP/IP връзки)
4. Определете RU размерите и стъпките (само за SNA свързвания)

Вижте "Дефиниране на локалната система (SNA)" или "Дефиниране на локалната система (TCP/IP)" на страница 47.

Дефиниране на локалната система (SNA)

На всяка програма в SNA мрежата се присвоява NETID и LU име, така че DB2 Universal Database за OS/390 Средство за обработка на заявки трябва да има стойност NETID.LUNAME (присвоена чрез VTAM), когато се свързва към мрежата. Тъй като DB2 Universal Database за OS/390 Средство за обработка на заявки е интегриран в локалната система за управление на DB2 Universal Database за OS/390 база данни, Средство за обработка на заявки трябва също да има RDB_NAME. В DB2 Universal Database за OS/390 изданията, DB2 Universal Database за OS/390 използва RDB_NAME като име на *местоположение*.

Дефинирайте DB2 Universal Database за OS/390 Средство за обработка на заявки да използва SNA мрежа, както следва:

1. Изберете LU име за вашата DB2 Universal Database за OS/390 система. NETID за вашата DB2 Universal Database за OS/390 система автоматично се получава от VTAM при стартирането на DDF.

2. Дефинирайте LU името и името на местоположение в DB2 Universal Database за OS/390 *bootstrap data set* (BSDS). (DB2 Universal Database за OS/390 ограничава името на местоположението до 16 символа.)
3. Създайте VTAM APPL дефиниция, за да регистрирате избраното LU име във VTAM.
4. Уверете се, че параметърът за разширена защита е установен на YES. Вижте “Допълнителни усъвършенствания на защитата” на страница 40.

Конфигуриране на DDF BSDS: DB2 Universal Database за OS/390 прочита BSDS при стартирането, за да получи системните инсталационни параметри. Един от записите в BSDS се нарича *DDF запис*, защото съдържа информацията, използвана от DDF при свързване към VTAM. Тази информация се състои от следното:

- Името на местоположението за DB2 Universal Database за OS/390 системата
- LU името за DB2 Universal Database за OS/390 системата
- Паролата, използвана при свързване на DB2 Universal Database за OS/390 система към VTAM

По два начина можете да доставите DDF BSDS информацията на DB2 Universal Database за OS/390:

- Използвайте DDF инсталационния панел DSNTIPR, когато за първи път инсталирате DB2 Universal Database за OS/390, за да осигурите необходимата DDF BSDS информация. Много от инсталационните параметри не се разглеждат тук, защото е по–важно да знаете как да свържете DB2 Universal Database за OS/390 към VTAM. Фигура 15 показва как да използвате инсталационния панел, за да запишете името на местоположение NEW_YORK3, LU името NYM2DB2 и паролата PSWDBD1 в DB2 Universal Database за OS/390 BSDS.

```
                            DISTRIBUTED DATA FACILITY                      =
==> _

 Въведете данните отдолу:

  1 DDF STARTUP OPTION   ===> AUTO      NO, AUTO или COMMAND
  2 DB2 LOCATION NAME    ===> NEW_YORK3         Име, което другите DB2 използват
                                                при обръщение към тази DB2
  3 DB2 NETWORK LUNAME   ===> NYM2DB2   име за DB2 обръщение, използвано от VTAM
  4 DB2 NETWORK PASSWORD ===> PSWDBD1   Парола на VTAM приложението за DB2
  5 RLST ACCESS ERROR    ===> NOLIMIT   NOLIMIT, NORUN или 1-5000000
  6 RESYNC INTERVAL      ===> 3         Минути между периода на ресинхронизация
  7 DDF THREADS          ===> ACTIVE    (ACTIVE или INACTIVE) Състояние на нишка
                                        за достъп до база данни, която записва/
                                        отменя промени и не съдържа заключвания/
                                        указатели на базата данни
  8 DB2 GENERIC LUNAME   ===>           Общо VTAM LU име за тази DB2 подсистема/
                                        група за общо ползване на данни
  9 IDLE THREAD TIMEOUT  ===> 120       0 или секунди докато нишката ACTIVE на
                                        пасивния сървър ще се прекрати (0-9999)
 10 EXTENDED SECURITY    ===> YES       Позволява промяна на парола и описателни
                                        кодове на грешка на защитата (YES или NO).
 НАТИСНЕТЕ: ENTER да продължите RETURN за край   HELP за повече информация
```

Фигура 15. DB2 Universal Database за OS/390 инсталационен панел DSNTIPR

- Ако DB2 Universal Database за OS/390 вече е инсталирано, можете да използвате помощната програма за промяна съдържанието на журнала (DSNJU003), за да обновите информацията в BSDS.

  Фигура 16 показва как да обновите BSDS с името на местоположение NEW_YORK3, LU името NYM2DB2 и паролата 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
//*
```

Фигура 16. Примерна дефиниция на Bootstrap Data Set DDF (за VTAM)

При стартиране на DDF (автоматично при стартиране на DB2 Universal Database за OS/390 или с командата на DB2 Universal Database за OS/390 START DDF) се създава връзка към VTAM и се прехвърля LU името и парола. VTAM разпознава DB2 Universal Database за OS/390 системата като сравнява LU името и паролата (ако е необходима VTAM парола) със стойностите, дефинирани в оператора на DB2 Universal Database за OS/390 VTAM APPL. VTAM паролата се използва, за да се провери дали DB2 Universal Database за OS/390 има оторизация да използва определеното LU име на VTAM системата. VTAM паролата не се прехвърля през мрежата и не се използва за свързване на други системи в мрежата към DB2 Universal Database за OS/390.

Ако VTAM не изисква парола, пропуснете ключовата дума PASSWORD= в помощната програма за промяна съдържанието на журнала. Липсата на ключовата дума посочва, че не е необходима VTAM парола.

Създаване на VTAM APPL дефиниция: След като дефинирате VTAM LU името и парола в DB2 Universal Database за OS/390, трябва да регистрирате тези стойности във VTAM. VTAM използва оператора APPL, за да дефинира локалните LU имена. Фигура 17 на страница 45 показва как да дефинирате LU името NYM2DB2 във 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
```

Фигура 17. Примерна VTAM APPL дефиниция за DB2 Universal Database за OS/390

За оператора VTAM APPL има много ключови думи. Значението на ключовите думи е представено подробно в *Ръководство за администриране на DB2 Universal Database за OS/390*. Представените тук ключови думи са свързани с темите на тази книга. Ключовите думи, които са от значение за Фигура 17, са описани както следва:

NYM2DB2

VTAM използва етикета на оператора APPL като LU име. В този случай LU името е NYM2DB2. Синтаксисът на APPL не позволява да се остави място за пълната стойност NETID.LUNAME. Стойността NETID не се определя във VTAM оператора APPL, защото на всички VTAM приложения автоматично им се присвоява стойност NETID за VTAM системата.

AUTOSES=1

Броят на SNA сесиите победители, които се стартират автоматично, когато се генерира APPC заявка за промяна броя на сесиите – Change Number of Sessions (CNOS). Трябва да се въведе различна от нула стойност за AUTOSES, за да се информира DB2 Universal Database за OS/390 при всяко неуспешно изпълнение на VTAM CNOS.

Не е необходимо автоматично да стартирате всички APPC сесии между всеки два участника в разпределена база данни. Ако стойността AUTOSES е по–малка от ограничението за сесии победители (DMINWNL), VTAM забавя стартирането на останалите SNA сесии, докато те станат необходими за приложение в разпределена база данни.

DMINWNL=10

Броят на сесиите, за които тази DB2 Universal Database за OS/390 система е победител. Параметърът DMINWNL се подразбира при CNOS обработка, но може да се замени за всеки конкретен участник, като се добави ред в таблицата SYSIBM.LUMODES в DB2 Universal Database за OS/390 комуникационната база данни.

DMINWNR=10

Броят на сесиите, за които системата партньор е победител. Параметърът DMINWNR се подразбира при CNOS обработка, но може да се замени за

всеки конкретен участник, като се добави ред в таблицата SYSIBM.LUMODES в DB2 Universal Database за OS/390 CDB.

DSESLIM=20

Общият брой на сесиите (печелещи и губещи сесии), които можете да установите между DB2 Universal Database за OS/390 и друга разпределена система за специфичното име на групата в този режим. Параметърът DSESLIM се подразбира при обработка на CNOS, но може да се замени за всеки конкретен партньор, като се добави ред в таблицата SYSIBM.LUMODES в DB2 Universal Database за OS/390 CDB.

Ако партньорът не поддържа броя на сесиите, заявени от параметрите DSESLIM, DMINWNL или DMINWNR, обработката на CNOS определя нови стойности за тези параметри, които са приемливи за него.

EAS=9999

Оценка за общия брой на сесиите, които тази VTAM LU изисква.

MODETAB=RDBMODES

Определя таблицата VTAM MODE, в която съществува всяко име на режим в DB2 Universal Database за OS/390.

PRTCT=PSWDBD1

Определя VTAM паролата, която да се използва при опитите да се свърже DB2 Universal Database за OS/390 към VTAM. Ако е пропусната ключовата дума PRTCT, не се изисква парола и трябва да пропуснете ключовата дума PASSWORD= в DB2 Universal Database за OS/390 помощната програма за промяна съдържанието на журнала.

SECACPT=ALREADYV

Определя най–високата стойност за защита на ниво SNA сесия, която се приема от тази DB2 Universal Database за OS/390 система, когато приеме заявка към разпределена база данни от отдалечена система. Ключовата дума ALREADYV посочва, че тази DB2 Universal Database за OS/390 система може да приеме три опции за защита на SNA сесия от други DRDA системи, които са изпратили заявка за данни от тази DB2 Universal Database за OS/390 система:

- SECURITY=SAME (валидността на заявката вече е проверена и съдържа само потребителския идентификатор).
- SECURITY=PGM (заявката съдържа паролата на заявителя или PassTicket).
- SECURITY=NONE (заявката не съдържа никаква информация за защита). DB2 Universal Database за OS/390 отхвърля DRDA заявките, които определят SECURITY=NONE.

Най–добре е винаги да определяте SECACPT=ALREADYV, защото нивото на защита на SNA диалога за всеки DB2 Universal Database за OS/390 партньор се взима от DB2 Universal Database за OS/390 CDB (колоната USERSECURITY на таблицата SYSIBM.LUNAMES). SECACPT=ALREADYV ви дава най–голяма гъвкавост при определянето на стойностите за USERSECURITY.

VERIFY=NONE

Определя нивото за защита на SNA сесия (валидност на LU на партньор), изисквано от тази DB2 Universal Database за OS/390 система. Стойност NONE посочва, че не е необходимо да се проверява валидността на LU на партньор.

DB2 Universal Database за OS/390 не ограничава вашия избор за ключовата дума VERIFY. В несигурна мрежа се препоръчва използването на

VERIFY=REQUIRED. Ако се използва VERIFY=REQUIRED, VTAM отхвърля партньорите, които не могат да изпълнят проверка на валидност на LU на партньора. Ако изберете VERIFY=OPTIONAL, VTAM проверява валидността на LU на партньора само за тези, които осигуряват поддръжка.

VPACING=2
Определя броя за VTAM стъпката на 2.

SYNCLVL=SYNCPT
Посочва, че DB2 Universal Database за OS/390 може да поддържа двуфазов протокол за записване на промените. VTAM използва тази информация, за да информира партньора, че е достъпен двуфазов протокол за записване на промените. При наличието на тази ключова дума DB2 Universal Database за OS/390 автоматично използва двуфазов протокол за записване на промените, ако партньорът го поддържа.

ATNLOSS=ALL
Посочва, че DB2 Universal Database за OS/390 трябва да се информира при всяко прекратяване на VTAM сесия. Така се осигурява, че при необходимост DB2 Universal Database за OS/390 изпълнява повторно синхронизиране на SNA.

DSESLIM, DMINWNL и DMINWNR ви позволяват да установите максималния брой VTAM сесии по подразбиране за всички партньори. При партньори, които имат специални изисквания по отношение на максималния брой сесии, може да се използва таблицата SYSIBM.LUMODES, за да се замени стойността по подразбиране. Например може да предпочетете да определите такъв максимален брой VTAM сесии по подразбиране, който е подходящ за вашите OS/2 системи. За другите партньори можете да създадете редове в таблицата SYSIBM.LUMODES, за да дефинирате съответния максимален брой сесии. Разгледайте следните примерни стойности:

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

Тези параметри позволяват на всеки партньор да създаде до четири сесии с DB2 Universal Database за OS/390, в които партньорът е победител за всяка от сесиите. Тъй като OS/2 създава LU 6.2 диалог с DB2 Universal Database за OS/390, като направи OS/2 победител за всички сесии, ще получите малко предимство в производителността. Ако OS/2 има достъпна сесия победител, не е необходимо да пита за позволение, за да стартира нов LU 6.2 диалог.

Дефиниране на локалната система (TCP/IP)

За удобство информацията в този раздел е обобщена от *DB2 Connect Enterprise Edition за OS/2 и Windows – Бърз старт*. За по–подробна информация се обърнете към *Справочник за инсталиране на DB2 Universal Database за OS/390* и *DRDA поддръжка за TCP/IP с DB2 Universal Database за OS/390 и DB2 Universal Database*.

Стъпките, необходими за дефиниране на TCP/IP комуникации с DB2 Universal Database за OS/390 са следните:

1. TCP/IP комуникациите трябва да са разрешени на DB2 Universal Database за OS/390 и на системата партньор.
2. Два подходящи номера на TCP/IP порта трябва да са присвоени на вашата мрежа от администратора. По подразбиране DB2 Universal Database за OS/390 използва порт номер 446 за свързвания на база данни и порт номер 5001 за повторно синхронизиране на заявки (двуфазов протокол за записване на промените).

3. Отдалеченият сървър или рикуестър на приложения трябва да използва същите номера на портове (или имена на услуги) като DB2 Universal Database за OS/390.
4. Уверете се, че TCP/IP опцията за вече проверена защита е установена на ДА. Вижте “Допълнителни усъвършенствания на защитата” на страница 40.
5. DB2 Universal Database за OS/390 BSDS трябва да включва допълнителни параметри. Фигура 18 очертава допълнителните параметри, необходими за TCP/IP комуникации.

```
//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
/*
//*
```

Фигура 18. Примерна дефиниция на Bootstrap Data Set DDF (за TCP/IP)

Дефиниране на отдалечени системи

Когато DB2 Universal Database за OS/390 приложение заяви данни от отдалечена система, търси в таблиците на комуникационната база данни (CDB), за да намери информация за отдалечената система. CDB е група от SQL таблици, управлявани от DB2 Universal Database за OS/390 системен администратор. Като DB2 Universal Database за OS/390 системен администратор можете да използвате SQL, за да вмъкнете редове в CDB и да опишете всеки потенциален DRDA участник. Пълно описание на CDB и как се използва, можете да намерите в *DB2 Universal Database за OS/390 SQL справочник* и *Ръководство за инсталиране на DB2 Universal Database за OS/390*.

Препратки към CDB търсене на информация, включително:

- LU името и TPN (при SNA свързвания)
- TCP/IP адресна информация (необходима само за изходящи TCP/IP SNA свързвания)
- Информацията за защитата на мрежата, необходима за отдалечената система
- Максималния брой сесии и имената на режимите, използвани при комуникация с отдалечената система (при SNA свързване)

Попълване на комуникационната база данни: Не е необходимо обновяване на CDB, ако ще използвате само входящи TCP/IP свързвания, така че ако планирате да използвате DB2 Universal Database за OS/390 само като TCP/IP сървър, не е необходимо да попълвате CDB и могат да се използват стойностите по

подразбиране. Обаче ако ще използвате входящи SNA свързвания трябва да осигурите поне един празен ред в SYSIBM.LUNAMES. Например, за да позволите да се приемат заявки за SNA свързване към база данни от всяка входяща DB2 Connect LU, използвайте SQL команда като следната:

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

Когато и да използвате DB2 Universal Database за OS/390 като рикуестър, CDB трябва да се обнови. Ще трябва да вмъкнете редове в таблицата SYSIBM.LOCATIONS и една от двете – таблицата SYSIBM.LUNAMES (при SNA свързвания) или таблицата SYSIBM.IPNAMES (при TCP/IP свързвания).

Освен това ако искате да управлявате изискванията за входящата защита или преобразуването на входящите потребителски идентификатори при SNA свързвания, може да са необходими допълнителни обновявания на CDB. Допълнителни примери са осигурени както следва: “Осигуряване на защита” на страница 56 описва как да дефинирате защита на потребителя, когато се настройва рикуестър за приложения, а “Осигуряване на защита” на страница 66 описва настройката на сървър на приложения.

Ръководството за администриране на DB2 Universal Database за OS/390 представя по–подробно изискванията за обновяване на таблиците в CDB. След като попълните CDB, можете да пишете запитвания за достъп до данни в отдалечени системи. *Справочникът за инсталиране на DB2 Universal Database за OS/390* освен това осигурява допълнителна информация за обновяване на CDB.

Как комуникационната база данни обслужва заявките: Когато изпраща заявка, DB2 Universal Database за OS/390 използва колоната LINKNAME на каталожната таблица SYSIBM.LOCATIONS, за да определи кой мрежов протокол да използва за изходното свързване. За да получите VTAM заявки, трябва да изберете LUNAME в инсталационния панел DSNTIPR на DB2 Universal Database за OS/390. За да получите TCP/IP заявки, трябва да изберете DRDA порт и порт за повторно синхронизиране в инсталационния панел DSNTIP5 на DB2 Universal Database за OS/390. TCP/IP използва номера на порт на сървъра, за да предаде мрежови заявки към правилната DB2 подсистема.

Ако стойността в колоната LINKNAME се намери в таблицата SYSIBM.IPNAMES, се използва TCP/IP при DRDA свързвания. Ако стойността се намери в таблицата SYSIBM.LUNAMES, се използват SNA. Ако едно и също име е както в SYSIBM.LUNAMES, така и в SYSIBM.IPNAMES, се използва TCP/IP при свързване към това място.

Забележка: Рикуестър не може да се свърже към дадено място, като използва едновременно SNA и TCP/IP протоколи. Например, ако таблицата SYSIBM.LOCATIONS определя LINKNAME на LU1 и ако LU1 е дефинирана едновременно в таблиците SYSIBM.IPNAMES и SYSIBM.LUNAMES, TCP/IP ще е единственият протокол, който ще се използва при свързване към LU1 от този рикуестър.

Таблици на комуникационната база данни: CDB се състои от следните таблици:

1. **SYSIBM.LOCATIONS**

   Тази таблица позволява на DB2 Universal Database за OS/390 да определи SNA или TCP/IP адресната информация, необходима при достъп до всяко RDB_NAME, избрано от DB2 Universal Database за OS/390 приложение *за изходящи заявки*. Колоните са:

LOCATION
RDB_NAME на отдалечена система. DB2 Universal Database за OS/390 ограничава стойността за RDB_NAME до 16 байта, което е с два байта по–късо от 18–байтовото ограничение, дефинирано в DRDA.

LINKNAME
LU името или TCP/IP атрибутите на отдалечената система.

PORT Името на TCP/IP порта или услугата (името на порта по подразбиране за DRDA е 446).

TPN Името на APPC транзакционната програма (TPN) на отдалечената система. Ако отдалечената система е DB2 Universal Database за OS/390 или отдалечената система използва стойността по подразбиране на DRDA TPN (X'07F6C4C2'), може да се използва празен низ, за да се определи TPN, защото DB2 Universal Database за OS/390 автоматично избира правилната стойност.

Ако отдалечената система изисква TPN стойност, различна от стойността по подразбиране, трябва да я въведете тук.

2. **SYSIBM.LUNAMES**

Тази таблица дефинира мрежовите атрибути на отдалечените системи, до които се осъществява достъп чрез SNA свързване. Колоните са:

LUNAME
LU името на отдалечената система.

SYSMODENAME
Името на VTAM режима на влизане в системата, използвано при установяване на *междусистемен* диалог DB2 Universal Database за OS/390–до–DB2 Universal Database за OS/390 за *поддръжка на вторичен сървър* от DB2 Universal Database за OS/390 (насочван от системата достъп). Ако тази колона е празна, IBMDB2LM трябва да се използва за DB2 Universal Database за OS/390 системни диалози

SECURITY_IN
Опциите за приемане от страна на мрежовата защита, които се изискват от отдалечената система, когато тази DB2 Universal Database за OS/390 система действа като сървър за отдалечената система (изисквания при *входяща защита*). Стойностите може да са:

- **V** посочва, че опцията е "verify" (проверка на валидност). Заявката за входящо свързване трябва да включва едно от следните: потребителски идентификатор и парола, потребителски идентификатор и RACF PassTicket или билет за DCE защита.
- **A** посочва, че опцията е "already verified" (вече проверен). Заявката не се нуждае от парола, въпреки че паролата се проверява, ако се изпрати. При тази опция заявката за входящо свързване се приема, ако включва едно от следните: потребителски идентификатор и парола, потребителски идентификатор и RACF PassTicket или билет за DCE защита.

  Ако колоната USERNAMES съдържа 'I' или 'B', няма да се извика RACF, за да провери валидността на заявките за входящо свързване, които съдържат само потребителски идентификатор.

SECURITY_OUT
Опциите за приемане от страна на мрежовата защита, които се изискват от отдалечената система, когато тази DB2 Universal Database за OS/390 система действа като рикуестър (изисквания при *изходяща защита*). Стойностите може да са:

- **A** посочва, че опцията е "already verified" (вече проверен). Заявките за изходящо свързване съдържат идентификатор за оторизация и не съдържат парола. Идентификаторът за оторизация, използван за изходяща заявка е или идентификаторът за оторизация на потребител на DB2, или преобразуван идентификатор, като зависи от стойността в колоната USERNAMES.
- **R** посочва, че опцията е "RACF PassTicket". Заявките за изходящо свързване съдържат потребителски идентификатор и RACF PassTicket. LU името на сървъра се използва като име на RACF PassTicket приложение.

  Идентификаторът за оторизация, използван за изходяща заявка е или идентификаторът за оторизация на потребител на DB2, или преобразуван идентификатор, като зависи от стойността в колоната USERNAMES.
- **P** посочва, че опцията е "password" (парола). Заявките за изходящо свързване съдържат идентификатор за оторизация и парола. Паролата се получава от таблицата SYSIBM.USERNAMES или от RACF, като зависи от стойността, определена в колоната ENCRYPTPWDS.

  В колоната USERNAMES трябва да е определено 'B' или 'O'.

ENCRYPTPSWDS
Дали са закодирани паролите, обменяни с този партньор. Закодирани пароли се поддържат само от DB2 Universal Database за OS/390 рикуестъри и сървъри.

MODESELECT
Определя дали да се използва таблицата SYSIBM.MODESELECT, за да се избере запис за VTAM режим за влизане (име на режим) на базата на крайния потребител и приложение, което прави заявката. Ако тази колона съдържа 'Y', таблицата SYSIBM.MODESELECT се използва за получаване на името на режима за всяка изходяща заявка към разпределена база данни.

Ако MODESELECT съдържа нещо различно от 'Y', се използва името на режима IBMDB2LM при заявки с насочван от системата достъп, а името на режим IBMRDB се използва при DRDA заявките.

Колоната MODESELECT ви позволява да определите приоритети за заявките към разпределена база данни, като се определи VTAM клас на услуга (COS – class of service), асоцииран с името на режима.

USERNAMES
Необходимото ниво за проверка откъде идва и преобразуване на потребителски идентификатор. Освен това тази колона определя параметрите на защита, използвани от тази DB2 Universal Database за OS/390 подсистема при заявка за данни от отдалечения партньор (изисквания за *изходяща защита*). USERNAMES може да има стойност I, O или B (само входящи, само изходящи или и двете).

GENERIC
Показва дали DB2 Universal Database за OS/390 трябва да използва своето истинско или общо LU име.

3. **SYSIBM.LUMODES**

Тази таблица се използва, за да предостави на VTAM максималния брой LU 6.2 сесии (CNOS ограничения) за партньорите при APPC (SNA) свързвания. Колоните са:

LUNAME
LU името на отдалечената система.

MODENAME
Името на VTAM режима на влизане, чиито ограничения се определят. Ако колоната MODENAME е празна, по подразбиране се запълва с IBMDB2LM.

CONVLIMIT
Максималният брой активни сесии между локалната DB2 Universal Database за OS/390 и отдалечената система за този режим на влизане. Тази стойност се използва, за да замени параметъра DSESLIM във VTAM оператора за дефиниране APPL за този режим на влизане, който определя максималния брой VTAM сесии по подразбиране за DB2 Universal Database за OS/390.

Стойността, избрана в CONVLIMIT, се използва при CNOS, за да се определят стойностите DMINWNR и DMINWNL на CONVLIMIT/2.

4. **SYSIBM.MODESELECT**

Тази таблица ви позволява да определите различни имена на режими за отделните крайни потребители и DB2 Universal Database за OS/390 приложения. Използва се само при SNA свързвания. Тъй като всяко име на VTAM режим може да има асоцииран клас на услуги (COS), можете да използвате тази таблица, за да присвоите приоритети при прехвърляне в мрежата за приложенията в разпределената база данни, на основата на комбинация от AUTHID, PLANNAME и LUNAME. Колоните са:

AUTHID
идентификатор за оторизация на DB2 Universal Database за OS/390 потребител (потребителски идентификатор). По подразбиране е празно, като показва, че определеното име на режим при влизане се прилага за всички идентификатори за оторизации.

PLANNAME
Името на плана, асоциирано с приложението, което заявява достъп до отдалечената база данни. По подразбиране е празно, като показва, че определеното име на режим при влизане се прилага за всички имена на план. Името на план, използвано за командата BIND PACKAGE е DSNBIND.

LUNAME
LU името, асоциирано с отдалечената база данни.

MODENAME
Името на VTAM режима на влизане, който да се използва, когато се насочва заявка за разпределена база данни към посочената отдалечена система. По подразбиране е празно, като посочва, че IBMDB2LM трябва да се използва при сесии с достъп, насочван от системата, а IBMRDB трябва да се използва при DRDA сесии.

5. **SYSIBM.USERNAMES**

Тази таблица се използва за управление на имената на крайните потребители, като осигурява пароли, преобразуване на имена и проверка откъде идва. DB2 Universal Database за OS/390 разглежда името на крайния потребител като идентификатор за оторизация. Повечето други продукти разглеждат това име като потребителски идентификатор.

С тази таблица можете да използване преобразуване на името, за да определите да се използват различни стойности за свързвания с потребителски идентификатори и DB2 Universal Database за OS/390 идентификатор за оторизация. Процесът за преобразуване на имената е позволен за заявки към отдалечена система (*изходящи* заявки) и за заявки, които идват от отдалечена система (*входящи* заявки). Ако паролите не са закодирани, от тази таблица се взима паролата на крайния потребител, когато към отдалечената система се изпраща потребителски идентификатор и парола. Колоните са:

TYPE Описанието за това как се използва реда (дали е ред, описващ преобразуване на име за изходящи, входящи заявки или заявки за проверка откъде идва).

I означава входящи свързвания, **O** означава изходящи свързвания.

Използвайте "O" при TCP/IP свързвания (при TCP/IP заявките не се изпълнява преобразуване на входящи имена и проверки откъде идва).

AUTHID
При преобразуване на изходящо име това е DB2 Universal Database за OS/390 идентификатора за оторизация, който да се преобразува. При преобразуване на входящо име това е SNA потребителския идентификатор, който да се преобразува. И в двата случая празна стойност на AUTHID се отнася за всички идентификатори за оторизация или потребителски идентификатори.

LINKNAME
Определя VTAM или TCP/IP мрежовите разположения, асоциирани с този ред. Ако тази колона е празна, това правило за преобразуване на имена се прилага за всеки TCP/IP или SNA партньор.

Ако се въведе някаква стойност за LINKNAME, едното или и двете от следните предположения трябва да е вярно:

- Съществува ред в SYSIBM.LUNAMES, в който стойността за LUNAME съответства на стойността, определена в колоната LINKNAME на SYSIBM.USERNAMES. Този ред определя VTAM място, асоциирано с това правило за преобразуване на имена.
- Съществува ред в SYSIBM.IPNAMES, в който стойността за LINKNAME съответства на стойността, определена в колоната LINKNAME на SYSIBM.USERNAMES. Този ред определя TCP/IP хост, асоцииран с това правило за преобразуване на имена.

  За TCP/IP клиенти не се изпълнява преобразуване на входящи имена и проверки откъде идва.

NEWAUTHID
Новото име на крайния потребител (SNA потребителски идентификатор или DB2 Universal Database за OS/390 идентификатор за оторизация). Ако е празно, означава, че не е необходимо да преобразувате идентификатора.

PASSWORD
Паролата, използвана на заделената сесия, ако паролите не са закодирани (ENCRYPTPSWDS = 'N' в SYSIBM.LUNAMES). Ако паролите са закодирани, тази колона се игнорира.

6. **SYSIBM.IPNAMES**

Тази таблица се използва при TCP/IP възли.

LINKNAME

Определената в тази колона стойност трябва да съответства на стойността, определена в колоната LINKNAME на SYSIBM.LOCATIONS.

SECURITY_OUT

Тази колона дефинира опцията за DRDA защита, използвана, когато SQL приложения на локалната DB2 се свързват към произволен отдалечен сървър, асоцииран с този TCP/IP хост:

- **A** посочва, че опцията е "already verified" (вече проверен). Заявките за изходящо свързване съдържат идентификатор за оторизация и не съдържат парола. Идентификаторът за оторизация, използван за изходяща заявка е или идентификаторът за оторизация на потребител на DB2, или преобразуван идентификатор, като зависи от стойността в колоната USERNAMES.
- **R** посочва, че опцията е "RACF PassTicket". Заявките за изходящо свързване съдържат потребителски идентификатор и RACF PassTicket. Определената в колоната LINKNAME стойност се използва като име на RACF PassTicket приложение за отдалечения сървър.

  Идентификаторът за оторизация, използван за изходяща заявка е или идентификаторът за оторизация на потребител на DB2, или преобразуван идентификатор, като зависи от стойността в колоната USERNAMES.
- **P** посочва, че опцията е "password" (парола). Заявките за изходящо свързване съдържат идентификатор за оторизация и парола. Паролата се получава от таблицата SYSIBM.USERNAMES.

  В колоната USERNAMES трябва да е определено "O".

USERNAMES

Тази колона управлява преобразуването на изходящите идентификатори за оторизация. Изходящото преобразуване се изпълнява, когато DB2 изпрати идентификатор за оторизация на отдалечен сървър.

- **O** показва, че се преобразува изходящия идентификатор. За да се преобразува идентификаторът, се използват редовете в таблицата SYSIBM.USERNAMES.

  Върху входящите идентификатори не се изпълнява преобразуване или проверки "откъде идва".
- Празна стойност показва, че не се изпълнява никакво преобразуване.

IPADDR

Тази колона съдържа IP адреса или името на област за отдалечения TCP/IP хост. Колоната IPADDR трябва да е дефинирана както следва:

- Ако IPADDR съдържа подравнен вляво символен низ, който съдържа четири цифрови стойности, разделени с десетични точки, DB2 приема, че стойността е IP адрес във формат с разделител десетична точка. Например, '123.456.78.91' ще се интерпретира като IP адрес с разделител точки.
- Всички други стойности се интерпретират като TCP/IP име на област, което може да се анализира с помощта на TCP/IP обръщението към сокет gethostbyname. В TCP/IP имената на

области не е от значение дали се използват главни или малки букви.

Дефиниране на комуникации (SNA)

VTAM е Комуникационен мениджър за OS/390 системите. VTAM приема функции на LU 6.2 от DB2 Universal Database за OS/390 и ги конвертира до потоци данни на LU 6.2, които можете да прехвърляте през мрежата. За да може VTAM да комуникира с приложенията партньори, дефинирани в DB2 Universal Database за OS/390 CDB, трябва да предоставите на VTAM следната информация:

- LU името за всеки сървър.

  При комуникации на DB2 Universal Database за OS/390 с VTAM, може да се предава само LU име (не NETID.LUNAME), за да се определи желаното предназначение. Това LU име трябва да е уникално в рамките на LU имената, известни на локалната VTAM система, за да може VTAM да определи NETID и LU името от стойността за LU име, получена от DB2 Universal Database за OS/390. Когато LU имената са уникални в рамките на SNA мрежата на предприятието, се опростява значително процесът на дефиниране на VTAM ресурсите. За съжаление това не винаги е възможно. Ако LU имената в рамките на вашите SNA мрежи не са уникални, трябва да използвате VTAM преобразуването на LU име, за да изградите правилната комбинация от NETID.LUNAME за LU името, което не е уникално. Този процес е описан в "Преобразуване имена на ресурси" в *Ръководство за мрежова реализация на VTAM*.

  Мястото и синтаксисът на VTAM дефинициите, използвани за дефиниране на отдалечени LU имена зависи от това как логически и физически е свързана отдалечената система към локалната VTAM система.
- Размерът на RU, размерът на стъпката на пакета и класът на услугите за всяко име на режим. Създайте запис в таблицата с VTAM режимите за всяко име на режим, определено в CDB. Освен това трябва да дефинирате IBMRDB и IBMDB2LM.
- VTAM и RACF профилите за алгоритъма за проверка валидността на LU, ако смятате да използвате проверка на валидността на LU на партньора.

Определяне RU размерите и стъпките: Записите, които дефинирате във VTAM таблицата с режими, определят размерите на RU и броя стъпки. Неправилното дефиниране на тези стойности може да има отрицателно влияние върху всички VTAM приложения.

След като изберете RU размерите, максималния брой сесии и броя на стъпките, изключително важно е да се провери какво е влиянието на тези стойности върху съществуващата VTAM мрежа. Трябва да разгледате следните неща, когато инсталирате нова система на разпределена база данни:

- При VTAM CTC свързвания проверете дали параметърът MAXBFRU е достатъчно голям, за да поеме RU размера плюс 29 байта, които VTAM добавя за заглавната част на SNA заявката и заглавната част на пакета за прехвърляне. MAXBFRU се измерва в единици от по 4K байта, така че MAXBFRU трябва да е поне 2, за да събере RU с размер 4K.
- При NCP свързвания се убедете, че MAXDATA е достатъчно голямо, за да поеме размера на RU плюс 29 байта. Ако определите размер на RU от 4K, MAXDATA трябва да е поне 4125.

  Ако определяте NCP параметъра MAXBFRU, изберете стойност, която събира размера на RU плюс 29 байта. При NCP, параметърът MAXBFRU дефинира

броя на входно/изходните буфери на VTAM, които могат да се използват за събиране на PIU. Ако изберете размер от 441 на IOBUF буфера, MAXBFRU=10 обработва правилно RU с размер 4K, защото 10*441 е повече от 4096+29.

- *DRDA Ръководство за свързваемост* описва как да оцените влиянието върху вашата разпределена база данни от VTAM IOBUF пула. Ако използвате прекалено много ресурси за IOBUF пула, производителността на VTAM се влошава за всички VTAM приложения.

Дефиниране на комуникации (TCP/IP)

Съображенията са както посочените преди това (вижте “Дефиниране на локалната система (TCP/IP)” на страница 47).

Осигуряване на защита

Когато отдалечена система изпълнява обработки в разпределена база данни от името на SQL приложение, трябва да може да удовлетвори изискванията за защитата на Средство за обработка на заявки, Сървър на приложения и мрежата, която ги свързва. Тези изисквания спадат към една или повече от следните категории:

- Избиране на имена на крайни потребители
- Параметри за защита на мрежата
- Защита на мениджъра на базата данни
- Защита, прилагана от външна подсистема за защита
- Представяне на данни

Избиране на имена на крайни потребители

При OS/390 системите на крайните потребители се присвояват *потребителски идентификатори* с дължина от 1 до 8 символа. Тази стойност трябва да е уникална в рамките на определената OS/390 система, но може да не е уникална в цялата мрежа. Например може да има потребител с име JONES в NEWYORK системата и друг потребител с име JONES в DALLAS системата. Ако тези два потребителя са един и същи човек, няма да има конфликт. Обаче, ако JONES в DALLAS е различен от JONES в NEWYORK, SNA мрежата (а следователно и разпределените бази данни в рамките на мрежата) не могат да различат JONES в NEWYORK от JONES в DALLAS. Ако не коригирате тази ситуация, JONES в DALLAS може да използва правата, предоставени на JONES в NEWYORK.

За да отстрани конфликтите в имената, DB2 Universal Database за OS/390 поддържа преобразуване на имената на крайните потребители. Когато приложение в DB2 Universal Database за OS/390 Средство за обработка на заявки направи заявка към разпределена база данни, DB2 Universal Database за OS/390 изпълнява преобразуване на името, ако комуникационната база данни посочи, че е необходимо *преобразуване на изходящо име*. Ако е избрано преобразуване на изходящо име, DB2 Universal Database за OS/390 винаги налага да се изпраща парола с всяка изходяща заявка към разпределена база данни.

Преобразуването на изходящото име в DB2 Universal Database за OS/390 се активира, ако в колоната USERNAMES в таблиците SYSIBM.LUNAMES или SYSIBM.IPNAMES е въведено 'O' или 'B'. Ако в USERNAMES е въведено 'O', преобразуването на името на крайния потребител се изпълнява за изходящите заявки. Ако USERNAMES е установено на 'B', преобразуването на името на крайния потребител се изпълнява както за входящите, така и за изходящите заявки.

Тъй като DB2 Universal Database за OS/390 оторизацията зависи от потребителския идентификатор на крайния потребител и от потребителския идентификатор на DB2 Universal Database за OS/390 плана, или собственика на пакета, процесът на преобразуване на името на крайния потребител се изпълнява върху потребителския идентификатор на крайния потребител, потребителския идентификатор на собственика на плана и потребителския идентификатор на собственика на пакета.[3]В процеса на преобразуване на имената се търси в таблицата SYSIBM.USERNAMES в следната последователност, за да се намери ред, който съответства на следния образец (TYPE.AUTHID.LINKNAME):

1. O.AUTHID.LINKNAME—Правило за преобразуване на специфичен краен потребител на специфичен партньор.
2. O.AUTHID.празно—Правило за преобразуване на специфичен краен потребител на произволен партньор.
3. O.празно.LINKNAME—Правило за преобразуване на произволен краен потребител на специфичен партньор.

Ако не се намери съответен ред, DB2 Universal Database за OS/390 отхвърля заявката за разпределената база данни. Ако редът се намери, стойността в колоната NEWAUTHID се използва като идентификатор за оторизация. (Празна стойност на NEWAUTHID означава, че трябва да се използва оригиналното име без преобразуване.)

Разгледайте примера, представен по–рано. Искате да дадете на JONES в NEWYORK различно име (NYJONES), когато JONES изпълнява заявки към разпределената база данни в DALLAS. В примера приемаме, че приложението, използване от JONES е собственост на DSNPLAN (собственик на DB2 Universal Database за OS/390 план) и не е необходимо да преобразувате този потребителски идентификатор, когато се изпраща в DALLAS. Необходимите SQL оператори, с които да се определят правилата за преобразуване на имената в CDB, са показани в Фигура 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');
```

Фигура 19. SQL за преобразуване на изходящо име (SNA)

Получените в резултат таблици на CDB са показани в Фигура 20 на страница 58:

[3] Ако заявката се изпрати на DB2 Universal Database за OS/390 сървър, преобразуването на имената се изпълнява за собственика на пакета и на плана. Към имената на собственика на пакета и плана никога няма асоциирана парола.

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

Фигура 20. Преобразуване на изходящи имена

Фигура 21 показва по–прост пример за свързване към DB2 Universal Database DRDA AS чрез SNA връзка.

```
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');
```

Фигура 21. SQL за преобразуване на изходящо име (прост пример за SNA)

Фигура 22 на страница 59 показва прост пример за свързване към DB2 Universal Database DRDA AS чрез TCP/IP връзка.

```
-- DB2 за 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')
                                ;
```

Фигура 22. SQL за преобразуване на изходящо име (прост пример за TCP/IP)

Защита на мрежа

След като Средство за обработка на заявки избере имената на крайните потребители, които представляват отдалеченото приложение, Средство за обработка на заявки трябва да осигури необходимата информация за защита на мрежата.

При SNA свързвания LU 6.2 осигурява три основни функции за защита на мрежата:

- Защита на ниво сесия, която се контролира от ключовата дума VERIFY на VTAM оператора APPL. Обърнете се към изложението след Фигура 17 на страница 45 за обяснение как да определите параметрите за защита на ниво сесия.
- Защита на ниво диалог, която се контролира от съдържанието на таблицата SYSIBM.LUNAMES.
- Закодиране на данни, което се поддържа само за VTAM 3.4 и следващите версии на VTAM.

Тъй като Сървър на приложения е отговорен за управлението на ресурсите на базата данни, Сървър на приложения диктува кои функции за защита на мрежата трябва да се изискват от Средство за обработка на заявки. Трябва да запишете изискванията за защита на ниво диалог за всеки Сървър на приложения в

таблицата SYSIBM.LUNAMES или SYSIBM.IPNAMES, като настроите колоната USERNAMES да отразява изискванията на сървъра на приложенията.

Възможните опции за защита на SNA диалог са:

SECURITY=SAME

Също така е известно като вече проверена защита, защото към отдалечената система се изпраща само потребителски идентификатор на крайния потребител (не се изпраща парола). Използвайте това ниво на защита на диалог, когато колоната USERNAMES в SYSIBM.LUNAMES не съдържа 'O' или 'B'.

Тъй като DB2 Universal Database за OS/390 обвързва преобразуването на името на крайния потребител със защитата на изходящия диалог, няма да ви позволи да използвате SECURITY=SAME, когато е активирана функцията за преобразуване името на крайния потребител.

SECURITY=PGM

В този случай идентификаторът и паролата на крайния потребител се изпращат на отдалечената система, за да се провери тяхната валидност. Използвайте тази опция на защита, когато колоната USERNAMES в таблицата SYSIBM.LUNAMES съдържа 'O' или 'B'.

В зависимост от опциите, определени в таблицата SYSIBM.LUNAMES, DB2 Universal Database за OS/390 получава паролата на крайния потребител от два различни източника:

- Некодирани пароли се получават от колоната PASSWORD на таблицата SYSIBM.USERNAMES. DB2 Universal Database за OS/390 извлича пароли от таблицата SYSIBM.USERNAMES, когато в колоната ENCRYPTPSWDS в таблицата SYSIBM.LUNAMES не е въведено 'Y'. Получените от този източник пароли могат да се прехвърлят до всеки DRDA Сървър на приложения.

  Фигура 23 дефинира паролите за SMITH и JONES. Колоната LUNAME в примера съдържа празни места, така че тези пароли се използват за всяка отдалечена система, към която SMITH или JONES се опитва да получи достъп.

```
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');
```

Фигура 23. Изпращане на пароли към отдалечени системи (SNA)

- Закодираните пароли се изпращат на отдалечената система, когато колоната ENCRYPTPSWDS на SYSIBM.LUNAMES съдържа 'Y'. Закодираните пароли се извличат от RACF (или продукт, еквивалентен на RACF) и могат да се интерпретират само от друга DB2 Universal Database за OS/390 система. При комуникация със система, която не е DB2 Universal Database за OS/390, не определяйте ENCRYPTPSWDS да е 'Y'.

  DB2 Universal Database за OS/390 търси в таблицата SYSIBM.USERNAMES, за да определи потребителския идентификатор (стойността NEWAUTHID) да се прехвърля към отдалечената система. Така преобразуваното име се използва за извличане на RACF паролата. Ако не искате да преобразувате имената, трябва да създадете редове в

SYSIBM.USERNAMES, които да указват да се изпращат имената без преобразуване. Фигура 24 на страница 61 позволява заявките да се изпращат на LUDALLAS и LUNYC без преобразуване на името на крайния потребител (потребителски идентификатор).

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

Фигура 24. Изпращане на закодирани пароли към отдалечени системи (SNA)

SECURITY=NONE

Тази опция не се поддържа от DRDA, така че DB2 Universal Database за OS/390 не обезпечава тази опция за защита.

Защита на мениджъра на базата данни

Един от начините Средство за обработка на заявки да участва в защитата на разпределена база данни е чрез преобразуване на изходящите имена, както беше посочено по–горе в “Избиране на имена на крайни потребители” на страница 56. Можете да използвате преобразуването на изходящите имена, за да управлявате достъпа до всеки Сървър на приложения на базата на самоличността на крайния потребител, който изпраща заявката и приложението, което я прави. Други начини, чрез които DB2 Universal Database за OS/390 Средство за обработка на заявки дава своя принос в защитата на разпределената система са:

Изграждане на отдалечени приложения

Крайните потребители свързват отдалечените програми на Сървър на приложения с командата на DB2 Universal Database за OS/390 BIND PACKAGE. DB2 Universal Database за OS/390 *не* ограничава използването на командата BIND PACKAGE на рикуестъра. Но крайният потребител не може да използва отдалечен пакет, докато пакетът не е включен в план на DB2 Universal Database за OS/390. DB2 Universal Database за OS/390 *наистина* ограничава използването на командата BIND PLAN. Краен потребител не може да добави отдалечен пакет към план, освен ако не са му предоставени правата BIND или BINDADD с помощта на оператора на DB2 Universal Database за OS/390 GRANT.

При свързване на пакет използвайте опцията ENABLE/DISABLE, за да определите дали пакетът да се използва от TSO, CICS/ESA, IMS/ESA или от отдалечена DB2 Universal Database за OS/390 подсистема.

Изпълнение на отдалечени приложения

За да може краен потребител на DB2 Universal Database за OS/390 да изпълни отдалечено приложение, той трябва да има право да изпълни DB2 Universal Database за OS/390 плана, свързан с това приложение. Собственикът на DB2 Universal Database за OS/390 план автоматично има право да го изпълнява. На други крайни потребители може да се предоставят права за изпълнение на плана, като се използва оператора на DB2 Universal Database за OS/390 GRANT EXECUTE. По този начин собственикът на приложение в разпределена база данни може да контролира използването на приложението на база отделни потребители.

Подсистема за защита

Външната подсистема за защита на OS/390 системите обикновено се осигурява от RACF или други продукти, които предоставят интерфейс, съвместим с RACF. DB2

Universal Database за OS/390 Средство за обработка на заявки няма директни обръщения към външната подсистема за защита, с изключение на поддръжката на закодирани пароли, описана в “Защита на мрежа” на страница 59. Обаче външната подсистема за защита се използва косвено на Средство за обработка на заявки при следните ситуации:

- Продуктът, който отговаря за отдалечено свързване на ниво потребителски модел на крайния потребител към DB2 Universal Database за OS/390, използва външната подсистема за защита, за да провери валидността на крайния потребител (потребителски идентификатор и парола). Това става преди крайният потребител да се свърже на ниво потребителски модел към DB2 Universal Database за OS/390. Както беше посочено по–горе, CICS/ESA, TSO и IMS/ESA са примери за продукти, които свързват крайни потребители към DB2 Universal Database за OS/390.
- Ако използвате защита на ниво SNA сесия (чрез ключовата дума VERIFY на оператора на DB2 Universal Database за OS/390 VTAM APPL), VTAM се обръща към външната подсистема за защита, за да провери идентичността на отдалечената система.

Представяне на данни

DB2 Universal Database за OS/390 се доставя, като по подразбиране при инсталирането идентификаторът на кодиран набор символи (CCSID) е 500. Тази стойност по подразбиране вероятно *няма* да е правилна за вашата инсталация.

При инсталирането на DB2 Universal Database за OS/390, трябва да установите инсталационният идентификатор CCSID да съответства на идентификатора CCSID на символите, генерирани и изпратени към DB2 Universal Database за OS/390 от входните устройства на вашата система. Този CCSID обикновено се определя от използвания национален език. Ако инсталационният CCSID не е правилен, при конвертирането на символите ще се получат неправилни резултати. В *DB2 Connect: Ръководство на потребителя* можете да видите списък с поддържаните идентификатори CCSID за всяка държава или национален език.

Трябва да се уверите, че вашата DB2 Universal Database за OS/390 подсистема има възможността да конвертира от идентификатора CCSID на всеки сървър на приложения до инсталационния CCSID на вашата DB2 Universal Database за OS/390 подсистема. DB2 Universal Database за OS/390 осигурява таблици за конвертиране за най–разпространените комбинации от CCSID за системата източник и приемник, но не и за всички възможни комбинации. При необходимост можете да добавите множество от таблици за конвертиране и процедури за конвертиране. Обърнете се към *Ръководството за администриране на DB2 Universal Database за OS/390* за допълнителна информация за конвертирането на символи от DB2 Universal Database за OS/390.

Настройка на сървъра на приложения

Поддръжката на сървър на приложения в DB2 Universal Database за OS/390 позволява на DB2 Universal Database за OS/390 да действа като сървър за DRDA рикуестър на приложения. Средство за обработка на заявки, свързано към DB2 Universal Database за OS/390 Сървър на приложения, може да е:

- DB2 Universal Database за OS/390 рикуестър
- DB2 Connect
- DB2 Universal Database Enterprise Edition или DB2 Universal Database Extended – Enterprise Edition с активирана поддръжка на DB2 Connect.

- Рикуестър DB2 Версия 2, който може да работи на AIX, HP–UX, OS/2, Solaris, Windows 3.1, Windows 3.11 for Workgroups, Windows 95 или Windows NT, както и на Macintosh, SCO, SGI или SINIX. Тази функция се осигурява от шлюз за няколко потребителя DDCS (Distributed Database Connection Services – Обслужване на разпределени бази данни) версия 2.3, DDCS за един потребител версия 2.3 и DDCS за Windows версия 2.4.
- OS/400 рикуестър
- DB2 за VM рикуестър
- Всеки продукт, който поддържа протоколите DRDA Средство за обработка на заявки

За всяко Средство за обработка на заявки, свързано към DB2 Universal Database за OS/390 Сървър на приложения, DB2 Universal Database за OS/390 Сървър на приложения поддържа достъп до база данни както следва:

- На Средство за обработка на заявки е разрешен достъп до таблиците, записани на DB2 Universal Database за OS/390 сървъра на приложения. Средство за обработка на заявки трябва да създаде пакет на DB2 Universal Database за OS/390 Сървър на приложения, преди да може да се изпълни приложението. DB2 Universal Database за OS/390 Сървър на приложения използва пакета, за да намери SQL операторите на приложението по време на изпълнението.
- Средство за обработка на заявки може да информира DB2 Universal Database за OS/390 Сървър на приложения, че достъпът трябва да е ограничен само до четене, ако DRDA връзката рикуестър–сървър не поддържа двуфазовия протокол за записване на промените. Например, DDCS V2R3 рикуестър със CICS front end ще информира DB2 Universal Database за OS/390 сървъра на приложения, че не са позволени обновявания.
- Освен това на Средство за обработка на заявки може да е разрешен достъп до таблици, съхранени на други DB2 Universal Database за OS/390 системи в мрежата, с помощта на насочван от системата достъп. Насочваният от системата достъп позволява на средство за обработка на заявки да установи свързване към няколко бази данни в една единица работа.

Осигуряване на мрежова информация

За да може DB2 Universal Database за OS/390 Сървър на приложения правилно да обработва заявки към разпределени бази данни, трябва да изпълните следните стъпки:

1. Да дефинирате сървъра на приложения на локалната Комуникационен мениджър.
2. Да дефинирате разположението на всеки потенциален вторичен сървър, така че DB2 Universal Database за OS/390 сървърът на приложения да може да пренасочва SQL заявките към техните крайни местоположения.
3. Да осигурите необходимата защита.
4. Да осигурите представянето на данните.

Дефиниране на сървър на приложения (SNA)

За да може Сървър на приложения да получава заявки към разпределени бази данни, трябва да е дефиниран в локалната Комуникационен мениджър и да има уникално име RDB_NAME. Следващото изложение се отнася за SNA свързванията. За да дефинирате Сървър на приложения, трябва да изпълните следните стъпки:

1. Изберете LU името и RDB_NAME, което ще се използва от DB2 Universal Database за OS/390 Сървър на приложения. Записването на тези имена в DB2

Universal Database за OS/390 и VTAM става по същия начин, както е описано в "Дефиниране на локалната система (SNA)" на страница 42. Избраното от вас RDB_NAME за DB2 Universal Database за OS/390 трябва да се достави на всички крайни потребители и Средство за обработка на заявки, които изискват свързваемост към Сървър на приложения.

2. Регистрирайте стойността NETID.LUNAME за DB2 Universal Database за OS/390 Сървър на приложения с всеки Средство за обработка на заявки, който изисква достъп, така че Средство за обработка на заявки да може да насочва SNA заявките към DB2 Universal Database за OS/390 сървъра. Това е така дори за случаите, при които Средство за обработка на заявки може да изпълни динамично мрежово маршрутизиране, тъй като Средство за обработка на заявки трябва да знае стойността NETID.LUNAME, преди да може да използва динамичното мрежово маршрутизиране.
3. Осигурете стойността по подразбиране за DRDA TPN (X'07F6C4C2') за всяко Средство за обработка на заявки, тъй като DB2 Universal Database за OS/390 автоматично я използва.
4. Създайте запис във VTAM таблицата с режимите за всяко име на режим, което е заявено от Средство за обработка на заявки. Тези записи описват RU размерите, стъпката в размера на пакета и класа на услугите за всяко име на режим.
5. Дефинирайте максималния брой сесии за Средство за обработка на заявки, които могат да се свързват с DB2 Universal Database за OS/390 Сървър на приложения. Операторът VTAM APPL дефинира максималния брой сесии по подразбиране за всички партньори. Ако искате да установите различна стойност по подразбиране за определен партньор, можете да използвате таблицата SYSIBM.LUMODES на комуникационната база данни (CDB).

   Вижте "Определяне RU размерите и стъпките" на страница 55 за информация как да прегледате вашата VTAM мрежа.
6. Създайте записи в DB2 Universal Database за OS/390 CDB, за да определите кои Средство за обработка на заявки могат да се свързват към DB2 Universal Database за OS/390 Сървър на приложения. Двата основни подхода за дефиниране записите на CDB за Средство за обработка на заявки в мрежата са:
   a. Можете да вмъкнете ред в SYSIBM.LUNAMES, който осигурява стойности по подразбиране, които да се използват за всяка LU, която не е специфично описана в CDB (редът по подразбиране съдържа празни полета в колоната LUNAME). Този подход ви позволява да дефинирате специфични атрибути за някои LU в мрежата, а да установите стойността по подразбиране за всички останали LU.

      Например можете да позволите на DALLAS системата (друга DB2 Universal Database за OS/390 система), да изпраща вече проверени за валидност заявки към разпределени бази данни (LU 6.2 SECURITY=SAME), но да изисквате мениджър на базата данни системите да изпращат пароли. Освен това може да не искате да въвеждате запис в CDB за всяка мениджър на базата данни система, особено ако има голям брой такива системи. Фигура 25 на страница 65 показва как CDB може да се използва, за да се определи SECURITY=SAME за DALLAS системата, а да се наложи SECURITY=PGM за всички други системи, които изпращат заявки.

```
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', ' ');
```

Фигура 25. Установяване на стойности по подразбиране при свързване на рикуестър на приложения (SNA)

b. Можете да използвате CDB, за да се проверяват правата отделно за всеки Средство за обработка на заявки в мрежата, като настроите CDB по един от следните начини:

- Не записвайте ред по подразбиране в SYSIBM.LUNAMES. Ако няма ред по подразбиране (ред с празно име на LU), DB2 Universal Database за OS/390 изисква по един ред SYSIBM.LUNAMES с името на LU за всеки рикуестър на приложения, който се опитва да се свърже. Ако CDB не съдържа съответния ред, Средство за обработка на заявки не разрешава достъпа.
- Запишете ред по подразбиране в SYSIBM.LUNAMES, който определя, че е необходима проверка "откъде идва" (в колоната USERNAMES е въведено 'I' или 'B'). Така DB2 Universal Database за OS/390 позволява достъп само на тези Средство за обработка на заявки и крайни потребители, които са дефинирани в таблицата SYSIBM.USERNAMES, както е описано в “Проверка откъде идва” на страница 66 . Може да предпочетете да използвате този подход, ако правилата за преобразуване на имената изискват ред с празно име на LU в SYSIBM.LUNAMES, но не искате DB2 Universal Database за OS/390 да използва този ред, за да позволи неограничен достъп до DB2 Universal Database за OS/390 Сървър на приложения.

В Фигура 26 няма ред с празно поле в колоната LUNAME, така че DB2 Universal Database за OS/390 отказва достъп на всяка LU, различна от LUDALLAS или 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', ' ');
```

Фигура 26. Идентифициране при свързвания на отделни рикуестъри за приложения (SNA)

Дефиниране на сървър на приложения (TCP/IP)

За да може Сървър на приложения да получава заявки за разпределени бази данни през TCP/IP свързване, трябва да е дефиниран в локалната TCP/IP подсистема и да има уникално име RDB_NAME. Освен това DB2 Universal Database за OS/390 Bootstrap Dataset трябва да включва необходимите параметри и може да се наложи да обновите DB2 Universal Database за OS/390 комуникационната база данни (CDB).

1. Информация как да настроите TCP/IP параметрите на AS, потърсете в *Справочник за инсталиране на DB2 Universal Database за OS/390*. Как да настроите AR е описано в *DB2 Connect Enterprise Edition за OS/2 и Windows – Бърз старт* и *DB2 Connect Personal Edition: Бърз старт*.
2. Примерна дефиниция на Bootstrap Dataset е показана в Фигура 18 на страница 48.

3. Не е необходимо обновяване на CDB, ако ще използвате само входящи свързвания, така че ако планирате да използвате DB2 Universal Database за OS/390 само като сървър, не е необходимо да попълвате CDB и могат да се използват стойностите по подразбиране. Следва прост пример за това как да обновите SYSIBM.IPNAMES.

   Ако искате да разрешите заявки за входящо свързване към база данни за TCP/IP възлите, можете да използвате SQL команда като посочената, за да обновите тази таблица:

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

Осигуряване на защита

За случаите, когато Средство за обработка на заявки насочи заявка за разпределена база данни към DB2 Universal Database за OS/390 Сървър на приложения, могат да се разгледат следните съображения, свързани със защитата:

- Проверка откъде идва
- Избиране на имена на крайни потребители
- Параметри за защита на мрежата
- Защита на мениджъра на базата данни
- Защита, прилагана от външна подсистема за защита

Проверка откъде идва

Когато DB2 Universal Database за OS/390 Сървър на приложения получи име на краен потребител от Средство за обработка на заявки, Сървър на приложения може да наложи ограничение върху имената на крайните потребители, получени от даден Средство за обработка на заявки. Това се постига чрез използването на проверката *откъде идва*. Проверката откъде идва позволява на Сървър на приложения да определи, че даден потребителски идентификатор може да се използва само от определени партньори. Например, Сървър на приложения може да ограничи JONES да “идва от” DALLAS. Ако друго Средство за обработка на заявки (различен от DALLAS) се опита да изпрати името JONES на Сървър на приложения, тогава Сървър на приложения може да отхвърли заявката, защото името не идва от правилно местоположение в мрежата.

DB2 Universal Database за OS/390 реализира проверка откъде идва като част от преобразуването на входящите имена на крайни потребители, описано в следващия раздел.

Забележка: При TCP/IP входящи заявки не се изпълнява входящо преобразуване и проверки "откъде идва".

Избиране имена на крайни потребители

Потребителският идентификатор, предаден от Средство за обработка на заявки може да не е уникален в рамките на цялата SNA мрежа. Може да е необходимо DB2 Universal Database за OS/390 Сървър на приложения да изпълни преобразуване на входящите имена, за да създаде уникални имена на крайни потребители в рамките на SNA мрежата. Аналогично може да е необходимо DB2 Universal Database за OS/390 Сървър на приложения да изпълни преобразуване на изходящите имена, за да осигури уникални имена на крайни потребители за вторичните сървъри, използвани в приложението (вижте “Осигуряване на защита” на страница 56 за информация относно преобразуването на изходящите имена на крайните потребители).

Преобразуването на входящите имена се активира, като в колоната USERNAMES на таблицата SYSIBM.LUNAMES или SYSIBM.IPNAMES се въведе стойността 'I' (inbound translation–входящо преобразуване) или 'B' (both inbound and outbound translation – едновременно входящо и изходящо преобразуване). Когато е в сила преобразуване на входящи имена, DB2 Universal Database за OS/390 конвертира потребителския идентификатор, изпратен от Средство за обработка на заявки и името на собственика на DB2 Universal Database за OS/390 плана (ако Средство за обработка на заявки е друга DB2 Universal Database за OS/390 система).

Ако Средство за обработка на заявки изпрати едновременно потребителски идентификатор и парола с помощта на APPC функцията ALLOCATE, се проверява тяхната валидност преди преобразуването на потребителския идентификатор. Колоната PASSWORD в SYSIBM.USERNAMES не се използва за проверка валидността на паролата. Вместо това потребителският идентификатор и паролата се представят на външната система за защита (RACF или еквивалентен на RACF продукт), за да се провери валидността.

Когато се проверява входящ потребителски идентификатор на функцията ALLOCATE, DB2 Universal Database за OS/390 има оторизационни изходи, които можете да използвате, за да осигурите списък с вторични идентификатори AUTHID и да изпълните допълнителни проверки. За подробности се обърнете към *Ръководството за администриране на DB2 Universal Database за OS/390*.

При преобразуването на входящото име се търси ред в таблицата SYSIBM.USERNAMES, който трябва да отговаря на един от образците, показани в следния списък (TYPE.AUTHID.LINKNAME):

1. I.AUTHID.LINKNAME—Специфичен краен потребител от специфичен Средство за обработка на заявки
2. I.AUTHID.празно—Специфичен краен потребител от произволен Средство за обработка на заявки
3. I.празно.LINKNAME—Произволен краен потребител от специфичен Средство за обработка на заявки

Достъпът са отказва, ако не се намери ред. Ако се намери ред, се позволява отдалечен достъп и името на крайния потребител се променя на стойността, въведена в колоната NEWAUTHID. Празна стойност NEWAUTHID показва, че името не се променя. Всички DB2 Universal Database за OS/390 проверки за оторизация за ресурси (например права за SQL таблица), изпълнени от DB2 Universal Database за OS/390, се изпълняват върху преобразуваните имена на потребители, вместо върху първоначалните.

Когато DB2 Universal Database за OS/390 Сървър на приложения получи име на краен потребител от Средство за обработка на заявки, могат да се постигнат редица задачи с помощта на възможността на DB2 Universal Database за OS/390 за преобразуване на входящите имена:

- Можете да промените името на крайния потребител, така че да стане уникално. Например, следните SQL оператори преобразуват името на крайния потребител JONES от рикуестъра за приложения NEWYORK (LUNAME LUNYC) до различно име (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', ' ');
```

- Можете да промените името на крайния потребител така, че група потребители да се представят с едно име. Например, може да искате да представите всички потребители от NEWYORK Средство за обработка на заявки (LUNAME LUNYC) с името на потребител NYUSER. Така можете да предоставите SQL права на името NYUSER и да контролирате SQL достъпа, който се предоставя на потребителите от 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', ' ');
```

- Можете да ограничите имената на крайните потребители, предавани от определен Средство за обработка на заявки. Това приложение на възможността за преобразуване имената на крайните потребители изпълнява проверката "откъде идва", описана в “Проверка откъде идва” на страница 66. Например, следващите SQL оператори позволяват използването само на SMITH и JONES като имена на крайни потребители от Средство за обработка на заявки NEWYORK. На всяко друго име ще се откаже достъп, защото не е изброено в таблицата 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', ' ', ' ');
```

- Можете да ограничите различните Средство за обработка на заявки, на които е позволено свързване към DB2 Universal Database за OS/390 Сървър на приложения. Това е още една функция на проверката "откъде идва". Следващия пример приема всяко име на краен потребител, изпратено от Средство за обработка на заявки NEWYORK (LUNYC) или Средство за обработка на заявки CHICAGO (LUCHI). На всички други Средство за обработка на заявки се отказва достъп, тъй като в реда по подразбиране на SYSIBM.LUNAMES е определено преобразуване на входящото име за всички входящи заявки.

```
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', ' ', ' ');
```

Осигуряване на мрежова защита

При SNA свързвания LU 6.2 осигурява три основни функции за защита на мрежата:

- Защита на ниво сесия
- Защита на ниво диалог
- Закодиране

"Защита на мрежа" на страница 59 представя как да се определи защита на ниво сесия и закодиране с DB2 Universal Database за OS/390. DB2 Universal Database за OS/390 Сървър на приложения използва защита на ниво сесия и закодиране по абсолютно същия начин както DB2 Universal Database за OS/390 Средство за обработка на заявки.

Остава само да се разгледа защитата на ниво SNA диалог. Някои аспекти на защитата на ниво диалог са уникални за DB2 Universal Database за OS/390 Сървър на приложения. DB2 Universal Database за OS/390 Сървър на приложения играе две отделни роли в защитата на мрежата:

- Като рикуестър към вторични сървъри DB2 Universal Database за OS/390 Сървър на приложения отговаря за генерирането на APPC заявки, които съдържат параметрите за защита на ниво SNA диалог, необходими за вторичните сървъри. DB2 Universal Database за OS/390 Сървър на приложения използва колоната USERNAMES на таблиците SYSIBM.LUNAMES и SYSIBM.USERNAMES, за да дефинира изискванията за защитата на ниво SNA диалог за всеки вторичен сървър. Елементите на тези дефиниции са идентични с дефинициите в "Защита на мрежа" на страница 59.
- Като сървър за Средство за обработка на заявки, DB2 Universal Database за OS/390 Сървър на приложения диктува на Средство за обработка на заявки изискванията за защита на ниво SNA диалог. DB2 Universal Database за OS/390 използва колоната USERSECURITY от таблицата SYSIBM.LUNAMES, за да определи защитата на диалог, изисквана от всеки Средство за обработка на заявки в мрежата. Следните стойности се използват в колоната USERSECURITY:

  C Показва, че DB2 Universal Database за OS/390 изисква от Средство за обработка на заявки да изпрати потребителски идентификатор и парола (LU 6.2 SECURITY=PGM) с всяка заявка за разпределена база данни. Ако колоната ENCRYPTPSWDS в SYSIBM.LUNAMES съдържа 'Y', DB2 Universal Database за OS/390 приема, че паролата вече е в закодиран формат на RACF (това е възможно само за DB2 Universal Database за OS/390 Средство за обработка на заявки). Ако колоната ENCRYPTPSWDS не съдържа 'Y', DB2 Universal Database за OS/390 очаква паролата в стандартния формат LU 6.2 (EBCDIC представяне на символите). И в двата случая DB2 Universal Database за OS/390 предава стойностите за потребителски идентификатор и парола, за да се проверят от подсистемата за защита. Трябва да имате подсистема за защита, която осигурява проверка на APPC потребителски идентификатор и парола; например RACF има възможност да направи това. Ако подсистемата за защита отхвърли двойката потребителски идентификатор–парола, се отказва достъпът до разпределената база данни.

  Всички други стойности
  Показва, че Средство за обработка на заявки може да изпрати или вече проверен потребителски идентификатор (LU 6.2 SECURITY=SAME), или потребителски идентификатор и парола (LU 6.2 SECURITY=PGM). Ако се изпратят потребителски идентификатор и парола, DB2 Universal Database за OS/390 ги обработва, както е описано за стойността 'C' по–горе. Ако заявката съдържа само потребителски идентификатор, се генерира обръщение към подсистемата за защита, за да разпознае потребителя, освен ако не се използва таблицата SYSUSERNAMES за управление на входящи потребителски идентификатори.

Ако възникне нарушаване на защитата, LU 6.2 изисква от DB2 Universal Database за OS/390 Сървър на приложения да върне на Средство за обработка на заявки SNA

код на състояние за грешка в защитата ('080F6051'X). Тъй като този код на състояние не описва причината за проблема, DB2 Universal Database за OS/390 осигурява два метода за записване на причините при нарушаване защитата на разпределена система:

- Генерира се съобщение DSNL030I, което съдържа LUWID на рикуестъра и кода за причина на DB2 с описание за проблема. Освен това DSNL030I включва изпратения от отхвърлената заявка за приложение AUTHID, ако е известен.
- Предупреждение се записва в NETVIEW базата данни за следене на хардуера, което съдържа същата информация, както осигурената в съобщението DSNL030I.

Защита на мениджъра на базата данни

Като собственик на ресурси в база данни, DB2 Universal Database за OS/390 Сървър на приложения контролира функциите за защита на SQL обектите, които се намират на DB2 Universal Database за OS/390 Сървър на приложения. Достъпът до управляваните от DB2 Universal Database за OS/390 обекти се контролира от правата, които се предоставят на потребителите от администратора на DB2 Universal Database за OS/390 или от собствениците на отделните обекти. Двата основни класа обекти, които се управляват от DB2 Universal Database за OS/390 Сървър на приложения, са:

- **Пакети**—Отделните крайните потребители имат право да създават да заменят и да изпълняват пакети с помощта на оператора на DB2 Universal Database за OS/390 GRANT. Когато краен потребител е собственик на пакет, той може да изпълнява или да заменя пакета. На другите крайни потребители трябва специално да им е предоставено правото да изпълняват пакета на DB2 Universal Database за OS/390 Сървър на приложения с оператора GRANT. Възможността USE може да се предостави на отделни крайни потребители или на PUBLIC, което означава, че всички крайни потребители могат да изпълняват пакета.

  При свързване на приложение към DB2 Universal Database за OS/390 пакетът съдържа SQL операторите, които се намират в приложната програма. Тези SQL оператори са класифицирани като:

  Статичен SQL

  Статичен SQL означава, че SQL операторът и SQL обектите, които се съдържат в израза са известни в момента, когато приложението се свързва с DB2 Universal Database за OS/390. Този, който създава пакета, трябва да има право да изпълнява всеки от статичните SQL оператори, които се съдържат в пакета.

  Когато крайни потребители получат право да изпълняват пакет, те автоматично имат право да изпълняват всеки от статичните SQL оператори, които се съдържат в него. Затова не е необходима никаква таблица на DB2 Universal Database за OS/390 с права на достъп за крайните потребители, ако пакетът съдържа само статични SQL оператори.

  Динамичен SQL

  Динамичният SQL описва SQL израз, който не е известен, преди изпълнението на програмата. С други думи, SQL изразът се изгражда от програмата и динамично се свързва с DB2 Universal Database за OS/390 с помощта на оператора SQL PREPARE. Когато краен потребител изпълнява динамичен SQL оператор, потребителят трябва да има таблицата с права на достъп, необходима за изпълнението на SQL израза. Тъй като SQL изразът не е известен при създаването на

плана или пакета, крайният потребител не може автоматично да получи необходимите права като собственик на пакета.

- **SQL обекти**— Това са таблици, производни таблици, синоними или псевдоними. На потребителите на DB2 Universal Database за OS/390 може да се предоставят различни нива с права на достъп, за да създават, изтриват, променят или четат отделни SQL обекти. Тези права са необходими, за да се свържат статични SQL изрази или да се изпълнят динамични SQL изрази.

Когато създавате пакет, опцията DISABLE/ENABLE ви позволява да контролирате кои типове DB2 Universal Database за OS/390 свързване могат да стартират пакета. Можете да използвате RACF и DB2 Universal Database за OS/390 процедури за изход при защита, за да можете избирателно да разрешавате на крайни потребители да използват DDF. С помощта на RLF можете да определите ограничения върху процесорното време за отдалечени свързвания и изпълнение на динамичен SQL.

Да разгледаме пакета на DB2 Universal Database за OS/390 с име MYPKG, чийто собственик е JOE. JOE може да позволи на SAL да изпълни пакета с помощта на DB2 Universal Database за OS/390 оператора GRANT USE. Когато SAL изпълни пакета, възниква следното:

- DB2 Universal Database за OS/390 проверява дали на SAL е предоставено право за използване USE за пакета.
- SAL може да използва всеки статичен SQL израз в пакета, защото JOE е имал необходимите права за SQL обекти, за да създаде пакета.
- Ако пакетът има динамични SQL изрази, SAL трябва да има своя собствена SQL таблица с права на достъп. Например, SAL не може да използва SELECT * FROM JOE.TABLE5, освен ако на нея не е предоставен достъп за четене до JOE.TABLE5.

Подсистема за защита

Използването на подсистема за защита (RACF или еквивалентна на RACF) от DB2 Universal Database за OS/390 Сървър на приложения зависи от това как дефинирате функцията за преобразуване на входящите имена в таблицата SYSIBM.LUNAMES:

- Ако въведете 'I' или 'B' в колоната USERNAMES, се активира преобразуване на входящи имена и DB2 Universal Database за OS/390 приема, че администраторът на DB2 Universal Database за OS/390 използва тази функция, за да изпълни част от действията при защитата на системата. Външната подсистема за защита се извиква, само ако Средство за обработка на заявки изпрати заявка, която съдържа едновременно потребителски идентификатор и парола (SECURITY=PGM). Трябва да имате подсистема за защита, която осигурява проверка на APPC потребителски идентификатор и парола; например RACF има възможност да направи това.

  Ако заявката от Средство за обработка на заявки съдържа само потребителски идентификатор (SECURITY=SAME), изобщо няма да има обръщение към външната подсистема за защита, защото правилата за преобразуване на входящите имена определят кои потребители могат да се свързват към DB2 Universal Database за OS/390 Сървър на приложения.
- Ако въведете нещо различно от 'I' или 'B' в колоната USERNAMES, подсистемата за защита изпълнява следните проверки:
  — Когато Средство за обработка на заявки получи заявка на разпределена база данни, DB2 Universal Database за OS/390 се обръща към външната подсистема за защита, за да провери валидността на потребителския идентификатор на крайния потребител (и паролата, ако е осигурена).

— Външната подсистема за защита се извиква, за да провери дали крайният потребител има право да се свързва към DB2 Universal Database за OS/390 подсистемата.

- И в двата случай се осигурява изход при оторизацията, за да се осигури списък с вторични идентификатори за оторизация. За повече информация се обърнете към *Ръководство за администриране на DB2 Universal Database за OS/390*.

Представяне на данни

Трябва да се уверите, че вашата DB2 Universal Database за OS/390 подсистема има възможност да конвертира от идентификатора CCSID на всеки сървър на приложения до инсталационния CCSID на вашата DB2 Universal Database за OS/390 подсистема. За допълнителна информация се обърнете към “Представяне на данни” на страница 62.

Глава 3. Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на SNA

OS/400 съдържа DB2 Universal Database за AS/400, системата за управление на IBM релационна база данни за системите AS/400.

Съдържанието на тази глава обяснява как да конфигурирате AS/400 система да поддържа свързване:

1. От DB2 Connect работни станции (вижте “Настройка на сървъра на приложения” на страница 82) и
2. Към DB2 Universal Database сървър (вижте “Настройка на рикуестър за приложения”).

Информация за свързване на две AS/400 системи потърсете в *Програмиране за AS/400 разпределена база данни*.

DB2 Universal Database за AS/400 версия 4.2 въвежда поддръжка за DRDA комуникации с TCP/IP. Основен източник на информация за тази тема е също така *Програмиране за AS/400 разпределена база данни*, а обобщение на необходимите стъпки от това ръководство са представени в Глава 4, “Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на TCP/IP” на страница 89. Принципите са същите като тези, представени в тази глава, но задачите за конфигуриране на мрежата са много по–прости.

DB2 Universal Database за AS/400 реализация

В тази глава е описано как DB2 Universal Database за AS/400 осигурява поддръжка за разпределени бази данни. OS/400 версия 2 подверсия 1 модификация 1 лицензира програмна поддръжка на DRDA отдалечена единица работа, а OS/400 версия 3 подверсия 1 добави поддръжка за DRDA разпределена единица работа (DUOW). Тази поддръжка е част от операционната система OS/400. Това означава, че не са ви необходими лицензирани програми от DB2 Universal Database за AS/400 Мениджър за запитвания и пакета за SQL разработки, за да използвате DRDA поддръжка или да изпълнявате програми с вградени SQL оператори.

Настройка на рикуестър за приложения

AS/400 реализира поддръжка на DRDA рикуестър за приложения като неделима част от операционната система OS/400. Тъй като поддръжката на рикуестъра за приложения е част от операционната система OS/400, тя е активна винаги, когато е активна и операционната система. Това е така и за поддръжката на сървър на приложения DB2 Universal Database за AS/400.

Когато DB2 Universal Database за AS/400 действа като рикуестър за приложения, може да се свърже към всеки сървър на приложения, който поддържа DRDA. За да осигурите достъп до разпределена база данни при DB2 Universal Database за AS/400 рикуестър за приложения, трябва да разгледате следното:

- Осигуряване на мрежова информация
- Осигуряване на защита
- Представяне на данните

Осигуряване на мрежова информация

Средство за обработка на заявки трябва да може да приема име на релационна база данни и да го преобразува в мрежови параметри. AS/400 използва директорията на релационната база данни, за да регистрира имената на релационните бази данни и техните съответни мрежови параметри. Тази директория позволява на AS/400 рикуестъра на приложения да предаде необходимата мрежова информация, за да установи свързвания в мрежата на разпределена база данни.

Голяма част от обработките в среда на разпределена база данни изискват обмен на съобщения с други системи във вашата мрежа. За да се изпълнят правилно тези обработки в SNA среда, трябва да направите следното:

- Да дефинирате локалната система в DB2 Universal Database за AS/400
- Да дефинирате отдалечената система в DB2 Universal Database за AS/400
- Да дефинирате комуникациите в DB2 Universal Database за AS/400

Дефиниране на локалната система в DB2 Universal Database за AS/400

Всеки рикуестър за приложения в мрежата на разпределена база данни трябва да има запис в своята директория на релационна база данни за своята локална релационна база данни и по един за всяка отдалечена релационна база данни, до която има достъп рикуестъра за приложения. Всяка AS/400 система в мрежата на разпределената база данни, която действа само като сървър на приложения трябва да има запис в своята директория на разпределена база данни за локалната релационна база данни. Допълнителна информация за директорията на релационната база данни потърсете в *Програмиране за AS/400 разпределена база данни*.

За да дефинирате локалната система, определете име на локалната база данни, като добавите запис с име на отдалечено място *LOCAL в директорията на релационната база данни. За да направите това, използвайте командата за добавяне на запис в директория на релационна база данни (ADDRDBDIRE). Следващият пример показва командата ADDRDBDIRE, като името на базата данни на рикуестъра за приложения е ROCHESTERDB:

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

Повече подробности за командите за директорията на релационната база данни потърсете в *Програмиране за AS/400 разпределена база данни*.

Забележка: В последните версии на OS/400, когато е необходимо, записът за локалното име на RDB се създава автоматично, ако не съществува. Името на системата в мрежовите атрибути ще се използва като име на локалната RDB.

Дефиниране на отдалечената система в DB2 Universal Database за AS/400

Всеки сървър на приложения в мрежа на разпределена БД също трябва да има локален запис в своята RDB директория. Освен това трябва да има запис за всяка отдалечена база данни в RDB директорията на всеки рикуестър за приложения. За да ги създадете:

- Дефинирайте отдалечените бази данни в локалната база данни, като добавите запис за всяка отдалечена база данни в директорията на релационната база

данни с помощта на командите ADDRDBDIRE или WRKRDBDIRE. При SNA свързвания информацията, която можете да определите, включва:

— Име на отдалечена база данни
— Име на отдалечено място на базата данни
— Име на локално място
— Име на режим, използван при установяване на комуникациите
— Идентификатор на отдалечена мрежа
— Име на устройството, използвано за комуникациите
— Име на транзакционна програма на отдалечената база данни

В повечето случаи единствената необходима информация е името на отдалечената база данни и името на отдалеченото място. [4] Когато е определено името само на отдалеченото място, се използват стойностите по подразбиране за останалите параметри. Системата избира описание на устройство с помощта на името на отдалеченото място.

Ако повече от едно описание на устройство съдържа едно и също име на отдалечено място, а се изисква описание на специфично устройство, тогава стойностите за локалното име на място и идентификаторът на отдалечената мрежа в записа в директорията на релационната база данни трябва да съответстват на стойностите в описанието на устройството. Избирането на описание на устройство може да се усложни, ако едно и също име на отдалечено място се използва в повече от едно описание на устройство. Използвайте уникални имена на отдалечени места във всяко описание на устройство, за да избегнете объркване. Името на транзакционната програма в отдалечената база данни по подразбиране приема DRDA стойността по подразбиране от X'07F6C4C2' за име на транзакционна програма.

Комуникационната информация в директорията на релационната база данни се използва за установяване на диалог с отдалечената система.

При TCP/IP свързвания (поддържани в DB2 Universal Database за AS/400 версия 4.2) са необходими само името на отдалечената база данни и асоциираните IP адрес и порт. Вижте Глава 4, “Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на TCP/IP” на страница 89.

Дефиниране на SNA комуникации

Този раздел описва конфигурирането на комуникациите в AS/400 с помощта на разширена мрежа с равностойни възли (APPN – Advanced Peer–to–Peer Networking). Освен това AS/400 системата позволява конфигурирането на разширени комуникации от–програма–до–програма (APPC), които не осигуряват поддръжка на мрежово маршрутизиране. AS/400 разпределена база данни работи с една от двете конфигурации. Повече информация за APPC конфигурациите вижте в *Конфигуриране OS/400 комуникации.*

Поддръжката на AnyNet от AS/400 дава възможност APPC приложения да работят през TCP/IP (Transmission Control Protocol/Internet Protocol) мрежи. Примерите в следващите раздели включват DDM, SNA разпределени услуги, предупреждения и транзитни съобщения на 5250 Display Station. След допълнително конфигуриране тези приложения, заедно с DRDA, могат да работят без промяна през TCP/IP

[4] “Име на място” в OS/400 е синоним на “LU име” във VTAM. “Име на отдалечено място” означава “име на партньор или отдалечена LU” на базата данни.

мрежи. За да определите поддръжка на AnyNet, трябва да въведете *ANYNW за параметъра LINKTYPE на командата CRTCTLAPPC.

Допълнителна информация за APPC през TCP/IP потърсете в *Конфигуриране на OS/400 комуникации* и *Конфигуриране и справочник за OS/400 TCP/IP*. (Отбележете, че собствена поддръжка на TCP/IP за DRDA комуникации се въвежда в DB2 Universal Database за AS/400 версия 4.2. Вижте Глава 4, “Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на TCP/IP” на страница 89.)

APPN осигурява мрежова поддръжка, която позволява на AS/400 система да участва и да управлява мрежа от системи, без да изисква мрежовата поддръжка, която традиционно се осигурява от mainframe система. Следващите стъпки показват как да конфигурирате AS/400 система за поддръжка на APPN.

1. Дефинирайте мрежовите атрибути с помощта на командата за промяна мрежовите атрибути (CHGNETA).

   Мрежовите атрибути съдържат:

   - Името на локалната система
   - Името на системата в APPN мрежата
   - Идентификаторът на локалната мрежа
   - Типът мрежов възел
   - Имената на мрежовите сървъри, използвани от AS/400 система, ако машината е краен възел
   - Контролните точки в мрежата, ако AS/400 е краен възел
2. Създаване на описание на линия.

   Описанието на линията отразява физическата линия на свързването и протокола за свързване на данни, който се използва между AS/400 система и мрежата. Използвайте следните команди, за да създадете описания на линията:

   - За създаване на описание на линия Ethernet – Create line description (Ethernet) (CRTLINETH)
   - За създаване на описание на линия SDLC – Create line description (SDLC) (CRTLINSDLC)
   - За създаване на описание на линия token ring – Create line description (token ring) (CRTLINTRN)
   - За създаване на описание на линия X.25 – Create line description (X.25) (CRTLINX25)
3. Създаване на описание на контролер.

   Описанието на контролера представя съседните системи в мрежата. Определете използването на APPN поддръжка, като въведете APPN(*YES), когато създавате описанието на контролера. Използвайте следните команди, за да създадете описания на контролери:

   - За създаване на описание на контролер APPC – Create controller description (APPC) (CRTCTLAPPC)
   - За създаване на описание на контролер SNA хост – Create controller description (SNA HOST) (CRTCTLHOST)

   Ако параметърът AUTOCRTCTL в описание на линия token–ring или Ethernet е установен на *YES, тогава автоматично се създава описание на контролер, когато системата получи заявка за стартиране на сесия през линия token–ring или Ethernet.
4. Създаване на описание на клас на услуга.

Използвайте описанието клас–на–услуга, за да изберете комуникационните маршрути (групи за прехвърляне) и определете приоритета за прехвърляне. Системата доставя пет описания на клас–на–услуги:

#CONNECT
Клас на услуга по подразбиране.

#BATCH
Клас на услуга за последователност от задания.

#BATCHSC
Същото като #BATCH, освен че се изисква защита на връзката за данни поне като в мрежа с пакетна комутация. Мрежите с пакетна комутация не винаги следват една и съща пътека през мрежата.

#INTER
Клас на услуга, обвързана с интерактивни комуникации.

#INTERSC
Същото като #INTER, освен че се изисква защита на връзката за данни поне като в мрежа с пакетна комутация.

Създайте други описания на клас–на–услуга с помощта на командата Create Class–of–Service (CRTCOSD).

5. Създаване на описание на режим.

Описанието на режима съдържа характеристиките на сесията и броя на сесиите, които може да се използват при договаряне на позволените стойности между локалното и отдалечено място. Освен това описанието на режима сочи към класа на услугата, който се използва за диалога. Със системата се доставят редица предварително дефинирани режими:

BLANK
Име на режима по подразбиране, определен в мрежовите атрибути при доставянето на системата.

#BATCH
Режим, предназначен за последователност от задания.

#BATCHSC
Същото като #BATCH, освен че описанието на асоциирания клас на услуга изисква защита на връзката за данни поне от тип на мрежа с превключване на пакети.

#INTER
Режим, предназначен за интерактивни комуникации.

#INTERSC
Същото като #INTER, освен че описанието на асоциирания клас на услуга изисква защита на връзката за данни поне от тип на мрежа с превключване на пакети.

IBMRDB
Режим, предназначен за DSDA комуникации.

Могат да се създадат други описания на режими с помощта на командата Create Mode Description (CRTMODD).

6. Създайте описания на устройства.

Описанието на устройство съдържа характеристиките на логическата връзка между локалните и отдалечените системи. Не е необходимо ръчно да създавате описания на устройства, ако AS/400 системата работи на хост система с APPN и като независима логическа единица (LU). AS/400 системата автоматично създава описанието на устройство и го прикрепва към съответното описание на

контролер при установяването на сесия. Ако AS/400 системата е зависима LU, тогава трябва ръчно да създадете описания на устройства с помощта на командата Create Device Description (CRTDEVAPPC). В описанието на устройство определете APPN(*YES), за да посочите, че се използва APPN.

7. Създайте списъци с APPN местоположения.

   Ако се изискват допълнителни локални местоположения (наречени *LU* на други системи) или специални характеристики на отдалечени местоположения за APPN, тогава трябва да създадете списъци с APPN местоположения. Името на локалното местоположение е името на контролна точка, определено в мрежовите атрибути. Ако се нуждаете от допълнителни местоположения за AS/400 системата, тогава трябва да имате списък с APPN локалните местоположения. Пример за специална характеристика на отдалечено местоположение е, ако отдалеченото местоположение е в мрежа, различна от тази, в която се намира локалното местоположение. Ако съществуват условията, е необходим списък с APPN отдалечени местоположения. Създайте списък с APPN местоположения, като използвате командата Create Configuration List (CRTCFGL).

8. Активиране на комуникации.

   Можете да активирате комуникационните описания, като използвате командата Vary Configuration (VRYCFG) или командата Work With Configuration Status (WRKCFGSTS). Ако описанията на линията са активирани, тогава се активират и съответните контролери и устройства, които са свързани към тази линия. Освен това командата WRKCFGSTS е полезна за преглед на състоянието на всяко свързване.

9. RU размери и стъпки

   RU размерите и стъпката се управляват от стойностите, определени в описанието на режима. Когато създадете описание на режима, се осигуряват стойности по подразбиране за RU размера и стъпката. Стойностите по подразбиране представляват оценка на AS/400 за повечето обкръжения, включително разпределена база данни. Ако стойността по подразбиране се взима за RU размер, AS/400 системата оценява най–добрата стойност, която да използва. Когато AS/400 системата комуникира с друга система, която поддържа адаптивна стъпка, определените стойности за стъпка са само отправна точка. Стъпката се настройва от всяка система в зависимост от способността на системата да обработва получените данни. За системи, които не поддържат адаптивна стъпка, стойностите на стъпката се договарят при стартирането на сесията и остават едни и същи през цялата сесия. За допълнителна информация вижте *Конфигуриране на OS/400 комуникации*.

Забележки:

1. Описанието на контролера е еквивалентно на макроса IBM NCP/VTAM (Network Control Program и Virtual Telecommunications Access Method – Програма за мрежово управление и Метод за виртуален достъп до телекомуникации) за физическа единица (PU – physical unit).
2. Описанието на устройство е еквивалентно на макроса NCP/VTAM за логическа единица (LU – logical unit). Описанието на устройство съдържа информация, подобна на тази, записана в профила в Комуникационния мениджър/2 1.1 на партнираща LU.
3. Описанието на режима е еквивалентно на NCP/VTAM таблицата за режими и профила Communications Manager Transmission Service Mode.

Допълнителна информация за конфигуриране на мрежова поддръжка и работа със списъци с местоположения потърсете в *Конфигуриране на OS/400 комуникации* и

Поддръжка на APPN. Примери, които показват използването на CL команди за дефиниране на системни конфигурации, вижте в *Програмиране за AS/400 разпределена база данни*.

Осигуряване на защита

Когато отдалечена система изпълнява обработки в разпределена база данни от името на SQL приложение, трябва да може да удовлетвори изискванията за защитата на рикуестъра за приложения, сървъра на приложения и мрежата, която ги свързва. Тези изисквания спадат към една или повече от следните категории:

- Избиране на имена на крайни потребители
- Параметри за защита на мрежата
- Защита на мениджъра на базата данни
- Защита, наложена от AS/400 защитата

Избиране на имена на крайни потребители

При AS/400 системите на потребителите се присвояват идентификатори с дължина от 1 до 10 символа, които са уникални за тази система, но не е задължително да са уникални в рамките на цялата мрежа. Този потребителски идентификатор се предава на отдалечената система, когато се установи свързване между две бази данни. За да се избегнат конфликти между потребителски идентификатори на системи в мрежата, често се използва преобразуване на изходящо име, за да се промени потребителският идентификатор и да се разреши конфликта преди изпращането по мрежата. Обаче AS/400 системата не дава възможност за преобразуване на изходящите имена за отстраняване на потенциални конфликти на сървъра. Тези конфликти трябва да се решат на сървъра на приложения, освен ако не използвате допълнителни клаузи USER и USING в SQL оператора CONNECT на AS/400. USER е валиден идентификатор на сървъра на приложения, а USING е съответната парола за потребителя.

Защита на мрежа

След като рикуестърът за приложения избере имената на крайните потребители, които представляват отдалеченото приложение, трябва да осигури необходимата за LU 6.2 информация за защита на мрежата. LU 6.2 осигурява три основни функции за защита на мрежата:

- Защита на ниво сесия, управлявана от ключовата дума LOCPWD на командата CRTDEVAPPC
- Защита на ниво диалог, управлявана от операционната система OS/400
- Закодиране, не се поддържа от операционната система OS/400

Защита на ниво сесия се осигурява чрез проверка LU–до–LU. Всяка LU има ключ, който трябва да съответства на ключа на отдалечената LU. Вие определяте ключа в ключовата дума LOCPWD на командата CRTDEVAPPC.

Тъй като сървърът на приложения е отговорен за управлението на ресурсите на базата данни, той диктува кои функции за защита на мрежата се изискват от рикуестъра за приложения. Администраторът на защитата на AS/400 трябва да провери изискванията за защита на всеки сървър на приложения, така че да нямат по–големи изисквания, отколкото AS/400 рикуестърът за приложения поддържа.

Възможните опции за защита на SNA диалог са:

SECURITY=SAME

Също така известно като вече проверена защита. Към отдалечената система се изпраща само потребителския идентификатор на потребителя на приложението. Не се изпраща парола. Във версиите преди AS/400 версия 2 подверсия 2 модификация 0 това ниво на защита на диалог беше единственото, поддържано от AS/400 рикуестър за приложения.

SECURITY=PGM

Към отдалечената система за проверка се изпращат потребителският идентификатор и паролата на потребителя на приложението. Във версиите преди AS/400 версия 2 подверсия 2 модификация 0 тази опция за защита не се поддържаше от AS/400 рикуестър за приложения.

SECURITY=NONE

Не се поддържа, когато AS/400 е рикуестър за приложения.

Защита на мениджъра на базата данни

AS/400 системата няма външна подсистема за защита. Защитата се изпълнява чрез операционната система OS/400, както е изложено в следващия раздел, "Системна защита."

Системна защита

Операционната система OS/400 управлява оторизацията за всички обекти в системата, включително програми, пакети, таблици, производни таблици и колекции.

Рикуестърът за приложения управлява оторизацията на обектите, които се намират на рикуестъра за приложения. Защитата на обектите на сървъра на приложения се управлява от сървъра на приложения на базата на което се изпраща потребителски идентификатор от рикуестъра за приложения. Изпратеният към сървъра на приложения потребителски идентификатор се асоциира с потребителя на AS/400 рикуестъра за приложения или потребителския идентификатор, въведен в клаузата USER на SQL оператора CONNECT на AS/400. Например, CONNECT TO име–на–БД USER потребителски–id USING парола.

Защитата на обектите може да се управлява с помощта на CL командите за права на обекти или със SQL операторите GRANT и REVOKE. CL командите за права на обекти включват Grant Object Authority (GRTOBJAUT) и Revoke Object Authority (RVKOBJAUT). Тези команди работят на всеки обект в системата. Операторите GRANT и REVOKE работят само на SQL обекти: таблици, производни таблици и пакети. Ако трябва да промените правата за други обекти, като програми или колекции, използвайте командите GRTOBJAUT и RVKOBJAUT.

Предоставяне и отменяне на права: Въведете следната команда на AS/400 система, за да предоставите права *USE на потребител USER1 за програмата PGMA:

```
GRTOBJAUT OBJ(PGMA) OBJTYPE(*PGM) USER(USER1) AUT(*USE)
```

Командата за отменяне на същите права е:

```
RVKOBJAUT OBJ(PGMA) OBJTYPE(*PGM) USER(USER1) AUT(*USE)
```

*PGM определя типът обект в този пример да е програма. *SQLPKG се използва при пакет, *LIB се използва за колекция, а *FILE се използва за таблица.

GRTOBJAUT и RVKOBJAUT също могат да се използват, за да не позволят на потребители да създават програми и пакети. Ако се отменят правата за някоя от командите CRTSQLxxx (където xxx = RPG, C, CBL, FTN или PLI), използвани при създаването на програмите, потребителят няма да може да създава програми. Ако

се отменят правата за командата CRTSQLPKG, потребителят няма да може да създава пакети от рикуестъра за приложения или на сървъра на приложения.

Например, въведете следната команда на AS/400 система, за да предоставите права *USE на потребител USER1 за командата CRTSQLPKG:

```
GRTOBJAUT OBJ(CRTSQLPKG) OBJTYPE(*CMD) USER(USER1) AUT(*USE)
```

Това влияе върху изпълнението на crtsqlpkg на рикуестъра за приложения. На сървъра на приложения тази команда дава възможност да се създават пакети.

Командата за отменяне на същите права е:

```
RVKOBJAUT OBJ(CRTSQLPKG) OBJTYPE(*CMD) USER(USER1) AUT(*USE)
```

Прилагане на оторизация по подразбиране: Когато се създават обекти, на тях се предоставя оторизация по подразбиране. По подразбиране създателят на таблица, производна таблица или програма получава всички права за тези обекти. Освен това по подразбиране на всички се предоставят същите права върху тези обекти, каквито имат върху библиотеката или колекцията от обекти.

Допълнителна информация за системната защита вижте в *AS/400 защита – справочник*.

Представяне на данни

Продуктите, които поддържат DRDA автоматично изпълняват всички необходими конвертирания на получаващата система. За да се изпълни това стойността на CCSID на рикуестъра за приложения трябва да се поддържа за конвертиране от получаващата система.

На рикуестър за приложения трябва да се погрижите за идентификатора CCSID, асоцииран с:

- Заявяващото задание

  OS/400 поддръжката за управление на работата инициализира идентификатора CCSID на заданието до идентификатора CCSID, въведен в потребителския профил. Ако стойността CCSID в потребителски профил е *SYSVAL, тогава за стойността на CCSID се взима системната стойност QCCSID. Системната стойност QCCSID първоначално се установява на CCSID 65535. Използването на 65535 за стойност на CCSID при задания, обслужващи опити за свързване от DB2 Universal Database ще доведе до отказ на опита за свързване. Промяната на системната стойност QCCSID влияе върху цялата система, така че се препоръчва да се промени стойността на CCSID на потребителския профил за заданието, под което се изпълнява заданието на сървъра. Въведете подходяща стойност за CCSID в профила на потребителя за заданието. Например, използвайте CCSID 37 за американски английски. Като цяло подходящо е да се използва идентификатора на кодиран набор символи по подразбиране за AS/400 системата, към която се свързвате.

  Стойността CCSID за заданието може да се промени с помощта на командата за промяна на задание Change Job (CHGJOB).А за следващите задания използвайте командата за промяна на потребителски профил Change User Profile (CHGUSRPRF), за да промените стойността CCSID на потребителския профил. За да видите каква стойност на CCSID е в сила за заданието, в CL програма използвайте командата за извличане атрибутите на задание Retrieve Job Attributes (RTVJOBA), за да получите текущата стойност на CCSID за заданието. Интерактивно използвайте командата за работа със задание Work

with Job (WRKJOB) и изберете опция 2 за представяне на атрибутите на дефиниция на задание в екрана Работа със задание.

- Физически файлове на база данни

  Физическите файлове на база данни по подразбиране са стойността по подразбиране на CCSID за заданието (която може да е различна от стойността CCSID за заданието) при създаването на файла, ако CCSID не е изрично определен в командата за създаване на физически файл Create Physical File (CRTPF) или за създаване на източник за физически файл Create Source Physical File (CRTSRCPF). Преди DB2 за AS/400 V3R1 по подразбиране се приемеше CCSID на заданието, който често беше 65535 и е неподходящ за използване в DRDA. Стойността CCSID за заданието по подразбиране никога не е 65535 и следователно е по–добре да се избере за CCSID на физическите файлове, до които се осъществява достъп чрез DRDA.

  Можете да използвате командата Display File Description (DSPFD), за да видите стойността на CCSID на файла или командата Display File Field Description (DSPFFD), за да видите стойността на CCSID за полетата на файла.

  Използвайте командата за промяна на физически файл Change Physical File (CHGPF), за да промените стойността на CCSID на физически файл. Не винаги може да се промени физически файл, ако съществува едно или повече от следните условия:

  — Логически файлове са дефинирани върху физическия файл. В този случай може да се наложи да направите следното:
    1. Запишете логическите и физическите файлове заедно с техните пътеки за достъп.
    2. Отпечатайте списък с правата за логическите файлове (DSPOBJAUT).
    3. Изтрийте логическите файлове.
    4. Променете физическите файлове.
    5. Възстановете физическите и логическите файлове и техните пътеки за достъп върху променените физически файлове.
    6. Предоставете съответните права за достъп до логическите файлове (вижте списъка, който сте отпечатали).
  — На файловете и полетата изрично се присвоява стойност за CCSID. За да промените физически файл, на който е присвоена стойност на CCSID на ниво полета, създайте отново физическия файл и копирайте данните в новия файл с помощта на параметъра FMTOPT(*MAP) на командата за копиране на файл Copy File (CPYF).
  — Форматите на записите са общи във версиите на OS/400 преди версия 3 подверсия 1.

Настройка на сървъра на приложения

Поддръжката на сървър на приложения в AS/400 позволява на тази система да действа като сървър за DRDA рикуестъри за приложения. Всеки клиент, който поддържа DRDA протоколи, може да е рикуестър за приложения, свързан към DB2 Universal Database за AS/400.

На рикуестъра за приложения е разрешен достъп до таблиците, съхранени локално на DB2 Universal Database за AS/400 сървъра на приложения. Рикуестърът за приложения трябва да създаде пакет на DB2 Universal Database за AS/400 сървъра на приложения, преди да може да изпълни някакви SQL оператори. Когато се

изпълнява програмата, DB2 Universal Database за AS/400 сървърът на приложения използва пакета със SQL операторите на приложението.

Осигуряване на мрежова информация

За да се обработят заявки за разпределена база данни на AS/400 сървър на приложения, ще е необходимо да определите име за базата данни на сървъра на приложения в RDB директорията. При SNA комуникации ще трябва да дефинирате сървъра на приложения и да определите размерите за единиците и стъпката за заявките и отговорите. За TCP/IP комуникации, поддържани от DB2 Universal Database за AS/400 версия 4.2, вижте Глава 4, “Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на TCP/IP” на страница 89.

Име на базата данни на сървъра на приложения

Можете да определите името на база данни на сървър на приложения (върху сървъра на приложения) по същия начин, както идентифицирате базата данни на рикуестъра за приложения (върху рикуестъра за приложения). Използвайте командата за добавяне на запис в директорията на релационната база данни Add Relational Database Directory Entry (ADDRDBDIRE) и определете *LOCAL като отдалечено местоположение.

Дефиниране на сървър на приложения в мрежата

При достъп чрез SNA, дефинирането на сървъра на приложения в мрежата е идентично с дефинирането на рикуестър за приложения в мрежата. Трябва да създадете описания на линия, контролер, устройство и режим, за да дефинирате едновременно сървъра на приложения и рикуестъра за приложения, който изпраща заявките. Информация за това как да дефинирате сървър на приложения в мрежата, вижте в “Дефиниране на локалната система в DB2 Universal Database за AS/400” на страница 74 и “Дефиниране на отдалечената система в DB2 Universal Database за AS/400” на страница 74. Освен това вижте *Програмиране за AS/400 разпределена база данни*.

Името на транзакционната програма, използвано за стартиране на базата данни на AS/400 сървър на приложение, е DRDA стойността по подразбиране X'07F6C4C2'. Това име на транзакционна програма е дефинирано в рамките на AS/400 системата, за да стартира сървъра на приложения. Когато този протокол се поддържа от DB2/400, съответният параметър за TCP/IP свързвания е порта. DB2/400 винаги ще използва като сървър добре известния DRDA порт 446.

Определяне RU размерите и стъпките

Трябва да се прегледат мрежовите дефиниции, за да се определи дали разпределената база данни въздейства върху съществуващата мрежа. Тези съображения са еднакви за сървъра на приложения и за рикуестъра за приложения.

Осигуряване на защита

Когато рикуестър за приложения насочи заявка за разпределена база данни към AS/400 сървър на приложения, трябва да се разгледат следните съображения, свързани със защитата:

- Избиране на имена на крайни потребители
- Параметри за защита на мрежата
- Защита на мениджъра на базата данни

- AS/400 защита

Избиране на имена на крайни потребители

Рикуестърът за приложения изпраща потребителски идентификатор към сървъра на приложения за нуждите на защитата. Заданието, което работи на AS/400 сървъра на приложения, използва този потребителски идентификатор, а в някои случаи потребителски идентификатор по подразбиране.

AS/400 сървърът на приложения не осигурява преобразуване на входящите потребителски идентификатори, за да се анализират конфликти сред потребителски идентификатори, които не са уникални или за да се групират няколко потребителя в един потребителски идентификатор. Всеки потребителски идентификатор, който се изпраща от Средство за обработка на заявки, трябва да съществува на сървъра на приложения. За да се групират входящите заявки в един потребителски идентификатор със загуба на част от защитата, трябва да се определи потребителски идентификатор по подразбиране в комуникационния запис в подсистемата, която обслужва заявките за стартиране на отдалечени задания. Вижте описанията на ADDCMNE и CHGCMNE в *AS/400 CL справочник*.

Защита на SNA мрежа

LU 6.2 осигурява три основни функции за защита на мрежата:

- Защита на ниво сесия
- Защита на ниво диалог
- Закодиране (не се поддържа от AS/400 системата)

DB2 Universal Database за AS/400 сървърът на приложения използва защита на ниво сесия по абсолютно същия начин както DB2 Universal Database за AS/400 рикуестъра за приложения.

Сървърът на приложения управлява използваните нива на SNA диалози. Параметърът SECURELOC в APPC описанието на устройство или стойността за защитено местоположение в списъка с APPN отдалечени местоположения определя какво ще се приеме от рикуестъра за приложения за диалога.

Възможните опции за защита на SNA диалог са:

SECURITY=SAME
: Също така известно като вече проверена защита. Сървърът за приложения изисква само потребителския идентификатор на потребителя на приложението. Не се изпраща парола. Използвайте това ниво на защита на диалог на сървъра на приложения, като за параметъра SECURELOC в APPC описанието на устройство въведете *YES или за защитено местоположение в списъка с APPN отдалечени местоположения въведете *YES.

SECURITY=PGM
: За да провери валидността, сървърът за приложения изисква едновременно потребителски идентификатор и парола. Използвайте това ниво на защита на диалог на сървъра на приложения, като за потребителски идентификатор по подразбиране в комуникационния запис на AS/400 подсистемата въведете стойност *NONE (няма потребителски идентификатор по подразбиране) и като определите параметърът SECURELOC или стойността за сигурно местоположение да е *NO.

SECURITY=NONE
: Сървърът за приложения не очаква потребителски идентификатор или парола. Диалогът е позволен с използването на потребителски профил по подразбиране на сървъра за приложения. За да използвате тази опция,

определете потребителски профил по подразбиране в комуникационната директория на подсистемата и определете *NO за параметъра SECURELOC или за стойността на сигурно местоположение.

SNA/DS (SNA Distribution Services) изисква потребителски идентификатор по подразбиране, така че SNA/DS трябва да има своя собствена подсистема за нормалния случай, когато не искате потребителски идентификатор по подразбиране за DRDA приложения.

Метод за групиране на входящи заявки за стартиране на задания в един потребителски идентификатор беше споменат в “Избиране на имена на крайни потребители” на страница 84. При този метод не се проверява валидността на потребителския идентификатор, изпратен от Средство за обработка на заявки. Заданието на сървъра за приложения се стартира под потребителски идентификатор по подразбиране, а потребителят, който е инициатор за свързването от сървъра за приложения има достъп до сървъра за приложения, дори ако неговият потребителски идентификатор има ограничени права. Това се прави, като се дефинира сървърът на приложения като несигурно местоположение, чрез определяне на потребителски идентификатор по подразбиране в комуникационния запис на AS/400 подсистемата и конфигуриране така рикуестъра за приложения, че да изпраща потребителски идентификатор само при обработката на свързването. Ако се изпрати парола, се използва потребителският идентификатор, изпратен с нея, вместо потребителския идентификатор по подразбиране.

Комуникационните записи в AS/400 подсистемата се разграничават от името на устройство и режим, използвано за стартиране на диалога. Като се присвоят различни потребителски идентификатори за различните двойки устройство/режим, потребителите могат да се групират според това как комуникират със сървъра на приложения.

Освен това AS/400 системата предлага функция за защита на мрежата, която се използва само за разпределена база данни и разпределено файлово управление. Съществува мрежов атрибут за тези типове системен достъп, който или отхвърля всички опити за достъп, или позволява защитата да се управлява от системата на базата на обект по обект.

Защита на TCP/IP мрежа

Нова команда CRTDDMTCPA е осигурена в DB2 Universal Database за AS/400 версия 4.2. С нея можете да определите дали сървърът да приема заявки за TCP/IP свързване без парола.

Защита на мениджъра на базата данни

Защитата се осъществява чрез функцията за защита на OS/400.

Системна защита

AS/400 системата няма външна подсистема за защита. Защитата се осъществява от функцията за защита на OS/400, която е неделима част от операционната система. Операционната система управлява правата за достъп до всички обекти в системата, включително програми, пакети, таблици, производни таблици и колекции.

Сървърът на приложения управлява правата за обектите, които се намират на сървъра на приложения. Защитата за тези обекти се базира на това кой потребителски идентификатор стартира заданието на сървъра на приложения. Този потребителски идентификатор се определя както е описано в “Избиране на имена на крайни потребители” на страница 84.

Защитата на обектите може да се управлява чрез използването на CL командите за права за достъп до обекти или чрез SQL операторите GRANT и REVOKE. CL командите за права на обекти включват Grant Object Authority (GRTOBJAUT) и Revoke Object Authority (RVKOBJAUT). Тези команди работят за всеки обект в системата. Операторите GRANT и REVOKE работят само на SQL обекти: таблици, производни таблици и пакети. Ако трябва да промените правата за други обекти, като програми или колекции, използвайте командите GRTOBJAUT и RVKOBJAUT.

Когато се създават обекти на системата, на тях се предоставя оторизация по подразбиране. Всички права получава потребителският идентификатор, който създава таблиците, производните таблици и пакетите. Всички други потребителски идентификатори (public) получават същите права, които имат за колекцията или библиотеката, в която е създаден обектът.

По време на изпълнение на пакета се проверяват правата за обектите, към които има обръщение от статични или динамични оператори в рамките на пакета. Ако създателят на пакета няма право да се обръща към тези обекти, се връщат предупредителни съобщения при създаването на пакета. По време на изпълнението потребителят, който изпълнява пакета, приема правата на създателя на пакета. Ако създателят на пакета има право за достъп до таблица, а потребителят, който изпълнява пакета няма, потребителят приема правата на създателя на пакета и може да използва таблицата.

Допълнителна информация за системната защита вижте в *AS/400 защита – справочник*.

Представяне на данни

Продуктите, които поддържат DRDA автоматично изпълняват всички необходими конвертирания на сървъра на приложения. За да се изпълни това стойността на CCSID на сървъра на приложения трябва да се поддържа за конвертиране от рикуестъра за приложения.

На сървър на приложения трябва да се погрижите за идентификатора CCSID, асоцииран с:

- Обслужване на задание в комуникационната подсистема

  Стойността на CCSID за обслужващото задание трябва да е съвместима с рикуестъра за приложения. Тази стойност на CCSID се установява от потребителския профил на потребителския идентификатор, която е заявил свързването. OS/400 поддръжката за управление на работата инициализира идентификатора CCSID на заданието до идентификатора CCSID в потребителския профил. Ако в потребителския профил липсва стойност за CCSID, тогава се взима стойността CCSID (QCCSID) от системата. Системната стойност QCCSID първоначално се установява на CCSID 65535.

  Преди да генерирате заявка към DB2 Universal Database за AS/400, трябва да се регистрирате и да използвате командата за промяна на потребителския профил Change User Profile (CHGUSRPRF), за да присвоите приемлива стойност за CCSID за потребителския профил за заданието, което ще обслужва DRDA заявките.
- SQL колекции

  SQL колекция се състои от OS/400 обект библиотека, журнал, получател на журнал, а понякога и от IDDU речник за данни, ако е определена клаузата WITH DATA DICTIONARY в оператора CREATE COLLECTION. Физическите и логически файлове, използвани за някои от тези обекти по подразбиране

използват стойността на CCSID за заданието в момента на създаване. Ако изпратите запитване към речника данни или каталога от рикуестър за приложения, който не поддържа стойността CCSID на тези файлове, може да видите нечетими или объркани данни. Рикуестърът за приложения може да генерира съобщение, че не поддържа тази стойност на CCSID. За да отстраните проблема, трябва да създадете нова SQL колекция със стойност CCSID на заданието, която е приемлива за другата система.

Стойността CCSID за заданието може да се промени с помощта на командата Change Job (CHGJOB). А за следващите задания използвайте командата Change User Profile (CHGUSRPRF), за да промените стойността CCSID на потребителския профил. В CL програма използвайте командата за извличане атрибутите на задание Retrieve Job Attributes (RTVJOBA), за да получите текущата стойност на CCSID за заданието. Интерактивно използвайте командата Work with Job (WRKJOB) и изберете опция 2 за представяне атрибутите на дефиниция на задание в екрана Работа със задание.

- SQL таблици и други DB2 Universal Database за AS/400 файлове, до които се осъществява достъп чрез DRDA

  SQL таблицата съответства на DB2 Universal Database за AS/400 физически файл в рамките на библиотека със същото име като вашата колекция. Колоните на таблицата също съответстват на дефинициите на полета на физическия файл. Стойността CCSID за таблицата или колоните на таблицата може да не е съвместима с рикуестъра за приложения. За да промените тази стойност, се обърнете към “Представяне на данни” на страница 81, където е описано как могат да се променят физическите файлове на база данни. Основен източник за несъвместимости на CCSID във версиите на OS/400 преди версия 3 подверсия 1 беше факта, че много файлове или SQL таблици получаваха по подразбиране стойност 65535 за CCSID. Във версия 3 подверсия 1 и следващите стойностите на CCSID за тези файлове се променят автоматично на някои други, които са по–подходящи.

Глава 4. Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на TCP/IP

В тази глава ще намерите обобщение на информацията в *Програмиране за AS/400 разпределена база данни*, където е обяснено как да настроите AS/400:

- Като DRDA рикуестър за приложения, който използва изходящи TCP/IP комуникации
- Като DRDA сървър на приложения, който използва входящи TCP/IP комуникации.

Принципите са същите, като представените в Глава 3, "Свързване на DB2 Universal Database за AS/400 в DRDA мрежа с помощта на SNA" на страница 73, но стъпките за конфигуриране са много по–прости.

Забележки:

1. При DRDA комуникации чрез TCP/IP 446 е номерът на порта по подразбиране за свързванията към база данни.
2. DB2 Universal Database за AS/400 версия 4 подверсия 2 не поддържа двуфазов протокол за записване на промените (разпределена единица работа) през TCP/IP комуникации.

Обобщение на информацията за DB2 Universal Database за AS/400

Програмиране за AS/400 разпределена база данни съдържа следните раздели, които трябва да прочетете:

- Глава 1. Разпределена релационна база данни и AS/400 система:
  - Работа на разпределена релационна база данни
  - DRDA и CDRA поддръжка.
- Глава 3. Комуникации за AS/400 разпределена релационна база данни:
  - Конфигуриране на комуникационна мрежа чрез TCP/IP
- Глава 4. Защита на AS/400 разпределена релационна база данни:
  - DRDA защита чрез TCP/IP
- Глава 5. Настройка на AS/400 разпределена релационна база данни:
  - Управление на работата при DRDA с TCP/IP
  - Настройка на TCP/IP сървър
- Глава 6. Задачи при администриране и работа на разпределена релационна база данни:
  - Управление на TCP/IP сървър
- Глава 8. Производителност на разпределена релационна база данни:
  - Фактори, които влияят върху тесните места в DRDA
- Глава 9. Отстраняване на проблеми в разпределена релационна база данни:
  - Обработване на откази за свързване при TCP/IP
  - Стартиране на сервизно задание за TCP/IP сървър
- Приложение B. Между–платформен достъп с помощта на DRDA.

Освен това трябва да знаете:

- TCP/IP номера на порта и името на хост за сървъра и рикуестъра.
- CCSID и кодовата страница за сървъра и рикуестъра.
- Потребителския идентификатор и парола, необходими при свързване към база данни.

Съображения при настройка и използване на DB2 Universal Database за AS/400 DRDA TCP/IP сървър

Основното съображение при настройка на DB2 Universal Database за AS/400 DRDA TCP/IP сървър е да осигурите стартирането на сървъра. CL командата за стартиране на DRDA сървър (също така известен като DDM сървър) е:

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

Освен това DRDA сървърът може да се стартира с помощта на командата за стартиране на TCP/IP сървър Start TCP/IP Server (STRTCPSVR) без параметри или като се въведе *ALL за параметъра SERVER. DRDA сървърът ще се стартира автоматично при стартирането на TCP/IP, ако се генерира следната CL команда:

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

Можете да проверите дали е стартиран сървърът, като използвате следната CL команда:

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

Тази команда ще представи разлистващ се списък със задания. Ако прегледате надолу с около страница, трябва да видите два реда, които съдържат следната информация:

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

(Редът QRWTSRVR може да се появява повече от веднъж в зависимост от това колко са активните задания на сървъра преди стартиране.)

Наличието на реда QRWTLSTN показва, че е активно заданието, което очаква заявки за DRDA и DDM свързвания. Това задание разпределя работата за заданието(ята) QRWTSRVR, когато се получат заявки за свързване.

Другият начин да се провери дали DRDA сървърът е стартиран, е като се генерира командата STRTCPSVR SERVER(*DDM) и се потърси съобщението 'DDM TCP/IP сървърът вече е активен'.

Името на заданието преди стартиране, използвано за определено свързване може да се намери, като се използва команда DSPLOG като:

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

където определеното време е преди момента, когато е направено свързването. В резултат ще се получи разлистващ се списък с хронологията на записите в журнала. Потърсете запис като този, който ще съдържа името на заданието на сървъра:

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

Това име на задание е полезно при преглеждане на журнала за заданията за все още активни задания. Освен това е полезно за стартиране на сервизно задание върху все още активните задания, за да се определи проблем или да се видят съобщенията на оптимизатора на запитвания. Примерна CL команда за стартиране на сервизно задание, което използва горната информация, може да е:

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

За да се постави обслуженото задание в режим за търсене на проблеми, изпълнете командата STRDBG:

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

В определени ситуации DRDA сървърът записва журнала на заданията, преди да се рециклира заданието и да се изчисти журналът. Това се получава, когато е открит сериозен проблем или когато заданието е приключило по време на обслужването (с помощта на командата STRSRVJOB).

За да намерите записания журнал на задание след приключването на заданието, използвайте следната команда:

```
WRKJOB userid/QPRTJOB
```

където userid е името на потребителски идентификатор, под което е осъществено свързването (SRR в горния пример).

В резултат ще се представи списък със задания, от които може да се избере или допълнително меню с едно задание. Изберете опция 4, 'Work with spooled files', за да намерите записания журнал на задание. Ще бъде този с име на файл QPJOBLOG, в случай че са обработени няколко файла. Опция 5 ще ви позволи да прегледате файла с журнала на заданието.

Пример за типа на съобщенията на оптимизатора на запитвания, които може да видите в журнала на заданието на сървъра, когато заданието е изпълнено в режим за тестване, са следните:

```
CPI4329    Information   00    03/30/98   16:14:57   QQQIMPLE
            QSYS        3911     QSQOPEN      QSYS         09C4
Съобщение . . . :   Използван е достъп на пристигнала последователност до файл TBL2.
Причина . . . . :   Използван е достъп на пристигнала последователност, за да се
  изберат записи от член TBL2 на файл TBL2 в библиотека SR. Ако файл TBL2
  в библиотека SR е логически файл, тогава членът TBL2 на физически файл
  TBL2 в библиотека SR е действителният файл, от който са избрани
  записите. Името *N за файла посочва, че е временен.
  Възстановяване . :   Използването на пътека за достъп може да
  повиши производителността на запитването, ако е определено
  избирането на запис. Ако не съществува пътеката за достъп, можете
  да решите да създадете такава, на която най-левите полета ключове
  съответстват при избора на запис. Съответствието на повече полета
  ключове в пътеката за достъп с полета в избора на запис ще повиши
  производителност. Като цяло за да се използва съществуваща пътека
  за достъп, се определя ред по полета, които трябва да съответстват на
  най-левите полета ключове на пътеката за достъп. За допълнителна
  информация се обърнете към книгата SQL програмиране за DB2 за AS/400 .
```

Съображения при настройка на DB2 Universal Database за AS/400 DRDA TCP/IP клиент

Освен съображенията за защитата, представени в следващия раздел, основното съображение при използване на DB2 Universal Database за AS/400 като DRDA рикуестър за приложения през TCP/IP е добавянето на запис в RDB директорията за отдалечения сървър на приложения. Това се изпълнява по подобен начин на описания в предишната глава, когато се използват SNA комуникации. Обаче вместо APPC параметри като име на отдалечена LU и име на транзакционна програма, има два TCP/IP параметъра: име на отдалечен хост или IP адрес и номер на порт или сервизно име. Вторият елемент от параметъра на отдалеченото местоположение може да се определи като *SNA (по подразбиране) или като *IP (за да показва, че при свързването ще се използва TCP/IP).

Съображения за защитата при използване на DRDA през TCP/IP

DRDA през собствен TCP/IP не използва услугите и концепциите на OS/400 за защита на комуникациите, като комуникационни устройства, режими, атрибути за сигурни местоположения и нива на защита на диалог, които са асоциирани с APPC комуникациите. Следователно настройката на защитата при TCP/IP е доста различна.

Поддържат се два типа защита от текущите реализации на DRDA през TCP/IP от DB2/400:

1. Само потребителски идентификатор
2. Потребителски идентификатор с парола

При DB2 Universal Database за AS/400 сървър на приложения (AS) защитата по подразбиране е потребителски идентификатор с парола. Това означава, че след инсталирането на системата входящите заявки за TCP/IP свързване трябва да съдържат парола заедно с потребителския идентификатор, под който трябва да се изпълнява заданието на сървъра. Командата CHGDDMTCPA може да се използва, за да се определи, че не се изисква парола. За да направите тази промяна, въведете CHGDDMTCPA PWDRQD(*NO). Трябва да имате специалните права *IOSYSCFG, за да използвате тази команда.

При DB2 Universal Database за AS/400 рикуестър за приложения (AR или клиент) има два метода, които може да се използват за изпращане на парола заедно с потребителския идентификатор при заявки за TCP/IP свързване. При отсъствие и на двата, ще се изпраща само потребителски идентификатор.

Първият начин за изпращане на парола е чрез формата USER/USING на SQL оператора CONNECT. Синтаксисът е:

```
CONNECT TO име-на-БД USER потребителски-id USING 'парола'
```

където думите с малки букви представляват подходящите параметри за свързване. В програма, която използва вграден SQL, стойностите на потребителски идентификатор и парола могат да се съдържат в хост променливи.

Друг начин за осигуряване на парола при изпращане на заявка за свързване през TCP/IP е като се използва записът за оторизация на сървъра. Списък с оторизации на сървъра е асоцииран с всеки потребителски профил на системата. По подразбиране списъкът е празен, но могат да се добавят записи с помощта на командата ADDSVRAUTE. Когато се направи опит за DRDA свързване през TCP/IP, DB2 Universal Database за AS/400 проверява списъка с оторизациите на сървъра за потребителски профил, под който работи клиентското задание. Ако се намери съответствие между RDB името в оператора CONNECT и името на SERVER в записа за оторизация, асоциирания параметър USRID в записа ще се използва като потребителски идентификатор на свързването, а ако е записан и параметър PASSWORD, тази парола също ще се изпрати заедно със заявката за свързване.

За да може да се запише парола с помощта на командата ADDSVRAUTE, стойността на QRETSVRSEC трябва да е установена на '1'. По подразбиране стойността е '0'. За да я промените, въведете:

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

Синтаксисът на командата ADDSVRAUTE е:

```
ADDSVRAUTE USRPRF(потр. профил) SERVER(име-на-БД) USRID(потр. идент.) PASSWORD(парола)
```

Параметърът USRPRF определя профила на потребителя, под който се изпълнява заданието на рикуестъра за приложения. Параметърът SERVER определя името на отдалечената RDB, а параметърът USRID определя профила на потребителя, под който ще работи заданието на сървъра. Параметърът PASSWORD определя паролата за профила на потребителя на сървъра.

Забележка: Много важно е името на RDB в параметъра SERVER да се въведе с главни букви.

Ако се пропусне параметърът USRPRF, по подразбиране ще се установи на профила на потребителя, под който се изпълнява командата ADDSVRAUTE. Ако се пропусне параметърът USRID, по подразбиране ще се установи стойността на параметъра USRPRF. Ако се пропусне параметърът PASSWORD или ако стойността на QRETSVRSEC е 0, няма да се запише парола в записа и при опит за свързване, който използва записа, механизмът за защита ще бъде от типа, който използва само потребителски идентификатор.

Запис с оторизация на сървър може да се премахне, като се използва командата RMVSVRAUTE или да се промени с командата CHGSVRAUTE. Вижте "AS/400 Справочник на командите" за пълно описание на тези команди.

Ако съществува запис за оторизация на сървъра за RDB, а се използва и форма USER/USING в оператор CONNECT, последното има предимство.

Глава 5. Допълнителни съображения при DB2 Universal Database за AS/400 и DB2 Universal Database

В този раздел са представени някои допълнителни съображения, които се отнасят за SQL операции между DB2 Universal Database за AS/400 и DB2 Common Server версия 2 или DB2 Universal Database. Останалата част от изложението се отнася за DB2 за OS/2, но в повечето случаи подобни съображения се отнасят и за DB2 Common Server версия 2 и DB2 Universal Database на други платформи, както следва:

1. При AS/400 имената на таблиците се дефинират от колекция (или име на библиотека) и се разполагат в DB2 Universal Database за AS/400 базата данни (по една база данни на AS/400). Обаче на PC компютър таблиците се дефинират от потребителски идентификатор (създателят на таблицата) и се разполагат в определена база данни (с няколко възможни бази данни на PC с DB2 за OS/2).
   a. Това означава, че запитване от DB2 за OS/2 (чрез DB2 Connect) към DB2 Universal Database за AS/400 ще използва потребителския идентификатор на заданието от страната приемник (на AS/400) за името на колекция (по подразбиране), ако името на таблицата, към която е отправено запитването е определено без име на колекция. Обърнете внимание или таблицата може да не се намери.
   b. Освен това означава, че запитване от DB2 Universal Database за AS/400 към DB2 за OS/2 ще има квалификатор на таблица по подразбиране, ако не е определен в запитването (във вида 'квалификатор.име–на–таблица'). Квалификаторът на таблица в DB2 за OS/2 (определен като колекция или библиотека от AS/400 рикуестер за приложение) по подразбиране приема потребителския идентификатор на потребителя, който е отправил запитването. Отново внимавайте, или запитването може да не намери таблицата.
   c. Може да пожелаете да създадете DB2 за OS/2 бази данни и таблици с общ потребителски идентификатор. При DB2 за OS/2 няма физически колекции, както в DB2 Universal Database за AS/400, а просто квалификатор на таблица, който е потребителският идентификатор на създателя.
2. Необходимо е DB2 Connect (или DDCS), ако DB2 за OS/2 ще е клиент, който използва протокола DRDA. Не е необходим, ако DB2 за OS/2 ще се използва само като сървър.
3. Много важно е да конфигурирате правилно DB2 Connect:
   a. Проверете дали имате най–новите версии на DB2 за OS/2 и DB2 Connect. Приложете всички налични пакети от типа FixPak, ако нямате най–новата версия.
   b. Следвайте инструкциите за инсталиране и конфигуриране, които сте получили в ръководството.
4. Ако използвате APPC, трябва да обърнете специално внимание правилно да конфигурирате комуникациите, с контролер и устройство, създадени за PC компютъра, когато DB2 за OS/2 се използва като рикуестер за приложения или като сървър на приложения. Освен това независимо от използвания комуникационен протокол трябва да има запис в RDB директорията за всяка база данни DB2 за OS/2, към която ще се свързва AS/400 системата.

   За да настроите за APPC комуникации, направете следното:

a. Можете ръчно да създадете описанията за устройство и контролер. Освен това можете да оставите системата да ги създаде вместо вас, ако имате token ring и параметърът за описание на линията AUTOCRTCLT е установен на *YES. Използвайте командата WRKLIND, за да разгледате описанието на линията, като използвате опция 2 за промяна. Преминете надолу към параметъра за автоматично създаване на контролер и вижте каква е вашата стойност за AUTOCRTCLT.

   Ако системата автоматично ще създаде контролерите, можете да активирате създаването на необходимите описания на контролери. От папката CM/2 на OS/2 изберете Start Communications и изпълнете Subsystem Management. От Subsystem Management погледнете подробностите за SNA подсистемата. Тук можете да погледнете в Логическите връзки. Отворете ги и активирайте връзката към желаната система, за да създадете автоматично контролера. Описанието за устройството ще се създаде автоматично по–късно.

b. Устройството и контролерът за PC на AS/400 трябва да е ACTIVE, за да работи мрежовото свързване между системите. Може да сте въвели стойност *NO за параметъра SWTDSC в описанието на контролера, така че контролерите, които са ACTIVE, ще останат ACTIVE. Освен това можете да установите параметъра ONLINE на *YES, така че на IPL контролерът ще стане активен. (Параметърът ONLINE в описанието на устройството може също да трябва да е *YES). Отбележете, че за да промените параметрите в описание на контролер, той трябва да е VARIED OFF и собственикът на контролера (параметъра CTLOWN) трябва да е установен на *USER.

c. За да добавите запис в RDB директорията за всяка база данни DB2 за OS/2, към която ще се свързва AS/400, използвайте командата ADDRDBDIRE: RDB името е името на база данни DB2 за OS/2, а името на отдалеченото местоположение е името на работната станция.

5. Правилната стойност на CCSID (обикновено 37 за американски клиенти) е необходима за всички таблици (физически файлове) на AS/400, използвани от DB2 за OS/2. Можете да видите стойността на CCSID с DSPFD, и да промените CCSID за физическите файлове с помощта на CHGPF. Освен това за да се свържете успешно, може да е необходимо да промените едно от следните: CCSID за заданието, CCSID за използвания потребителски профил или системния CCSID (QCCSID), ако по подразбиране е 65535. Обикновено най–доброто място да се направи тази промяна е в потребителския профил, под който ще се изпълни заданието на сървъра.
6. Преди да използвате DB2 Connect да взаимодейства с AS/400 сървър, трябва да създадете SQL пакети на AS/400 за приложните програми и за DB2 Connect помощните програми.

   a. DB2 командата PREP може да се използва за обработка на файла с кода на приложната програма, който съдържа вграден SQL. При тази обработка ще се създаде модифициран файл с код, който съдържа обръщенията на хост езика за SQL операторите и по подразбиране ще създаде SQL пакет в базата данни, към която в момента сте свързани.

   b. За да свържете DB2 Connect помощни програми към някой AS/400 DB2 сървър:

      1)

      ```
      CONNECT TO име-на-БД
      ```

      2)

      ```
      BIND пътека@DDCS400.LST BLOCKING ALL SQLERROR CONTINUE
               MESSAGES DDCS400.MGS GRANT PUBLIC
      ```

Заменете пътека в пътека@DDCS400.LST отгоре с пътеката по подразбиране C:\SQLLIB\BND\ или с локалната стойност, ако не сте инсталирали на мястото по подразбиране.

Забележка: PTF SF23624 е необходим за OS/400 V3R1, за да се избегне SQL код –901 от DB2 Universal Database за AS/400 базата данни за третия файл за свързване в списъка.

3)

```
CONNECT RESET
```

7. При интерактивен SQL от DB2 Universal Database за AS/400 към DB2 за OS/2:
   a. Използвайте атрибутите за сесия NAMING(*SQL), DATFMT(*ISO) и TIMFMT(*ISO). Работят и други формати освен *ISO, но не всички и използваният за датата формат (DATFMT) трябва също да се използва и за часа (TIMFMT).
   b. Отбележете съответствието между COLLECTION на AS/400 и квалификатор на таблица (потребителския идентификатор на създателя) при DB2 за OS/2. Вижте елемент 1 в този списък от съображения за SQL операции.
   c. При първата интерактивна сесия ТРЯБВА освен това да определите COMMIT(*CS) за управление на записването на промените; и след това (1) RELEASE ALL, (2) COMMIT и (3) CONNECT TO rdbname (където 'rdbname' се заменя с определената база данни). Освен това може да предпочете този път да изпълните GRANT EXECUTE ON PACKAGE QSQL400.QSQL0200 TO PUBLIC (или за специфични потребители), така че други да могат да използват създадения SQL PKG на PC компютъра за интерактивен SQL.
8. При програмите, създадени на AS/400 система, която осъществява достъп до база данни DB2 за OS/2, не забравяйте да използвате следните команди на DB2 за OS/2:
   a.

   ```
   GRANT ALL PRIVILEGES ON TABLE име-на-таблица TO потребител
   ```

   b.

   ```
   GRANT EXECUTE ON PACKAGE име-на-пакет (нормално AS/400 програмата) TO потребител
   ```

   При възможност определете 'PUBLIC' за потребител.
9. При разработката на AS/400 програми, които осъществяват достъп до DB2 за OS/2 (версия 2.1.1 или предишна), се генерираше съобщение (SQL5057) в отговор на командата CRTSQLxxx, в което се казва, че на PC компютъра е създаден SQL пакет, дори ако пакетът не е създаден. Това е коригирано в най–новото издание на DB2 за OS/2.

   Освен това в по–старите версии на DB2 за OS/2, няма да се създадат SQL пакети за OS/400 програми, които имат нещо в текстовото поле на своето описание за участник източник.
10. Запомнените процедури на езика C в DB2 за OS/2 не могат да използват argc и argv като параметри (не могат да са от тип main()). Това се различава от AS/400 запомнените процедури, които трябва да използват argc и argv. Запомнени процедури за DB2 за OS/2 вижте в примерите в поддиректорията \SQLLIB\SAMPLES. Потърсете OUTSRV.SQC и OUTCLI.SQC в поддиректорията C.
11. Използвайте главни букви за имената на запомнени процедури в DB2 за OS/2, към които има обръщение от AS/400. За момента AS/400 превръща имената на процедурите в главни букви. Обаче това означава, че няма да се намери процедура на PC, която е със същото име, но с малки букви. Не забравяйте, че

имената на процедури при запомнени процедури на AS/400 ще са с главни букви.

12. Освен това без съответния PTF за вграден SQL оператор CALL от AS/400 към DB2 за OS/2 ще работи само ако поставите името на процедурата в хост променлива (CALL:хост–име–на–процедура(...)). V3R7 PTF, който коригира това е SF35932. V3R2 PTF е SF36535.
13. Запомнените процедури на AS/400 не могат да включват COMMIT, когато са създадени да се изпълнят в същата активираща група, както извикващата програма (правилния начин да ги създадете). Обаче при DB2 за OS/2 запомнените процедури могат да включват COMMIT, но програмистът трябва да внимава, защото от страна на DB2 Universal Database за AS/400 няма да се знае, че е възникнало записване на промените.

Глава 6. Свързване на DB2 за VSE & VM в DRDA мрежа

SQL/DS (DB2 за VM) версия 3 подверсия 5 осигурява поддръжка на DRDA отдалечена единица работа за сървър на приложения и рикуестър за приложения при VM системи. SQL/DS (DB2 за VSE) версия 3 подверсия 5 осигурява поддръжка на DRDA отдалечена единица работа за сървър на приложения при VSE системи.

Освен това DB2 за VSE & VM версия 5 подверсия 1 осигурява поддръжка на DRDA разпределена единица работа за сървър на приложения при VM и VSE системи. Тази глава основно се съсредоточава върху свързването на DB2 за VSE & VM системи към различни отдалечени DRDA системи. Повече информация за свързването на две DB2 за VSE & VM системи потърсете в следните ръководства:

- *Планиране, администриране и използване на VM/ESA свързвания*
- *Администриране на DB2 за VM система*
- *Администриране на DB2 за VSE система*

Преглед на DB2 за VM

Всеки мениджър на база данни DB2 за VM може да управлява една или повече бази данни (по една в даден момент) и обикновено се представя от името на базата данни, която управлява в момента. Това име на релационна база данни е уникално в рамките на множеството от взаимосвързани SNA мрежи.

Различните DRDA и VM компоненти, които участват в работата на разпределена база данни, са описани по–долу. Тези компоненти позволяват на DB2 за VM мениджъри на бази данни да осъществява достъп до локални релационни бази данни и да комуникира с отдалечени DRDA системи в SNA мрежа.

AVS APPC/VTAM поддръжката (AVS) е компонент на VM, който позволява на VM приложения да имат достъп до SNA мрежа. Осигурява функцията за логически единици (LU–logical unit), както е дефинирана от SNA. Във VM обкръжението LU се разглежда като *шлюз*. В групово управлявана система AVS работи като VTAM приложение. Конвертира APPC/VM обръщенията в APPC/VTAM обръщения и обратно. APPC/VM използва AVS, за да насочва и преобразува потоци данни. AVS позволява на заявки на DB2 за VM да се насочват между локалната VM система и отдалечени SNA местоположения. AVS трябва да се използва винаги, когато DB2 за VM приложения или бази данни комуникират с бази данни или приложения, които не са DB2 за VM.

От страната на рикуестъра за приложения потребителят трябва да има право да се свързва чрез AVS шлюз, преди заявките да могат да се изпратят. От страната на сървъра на приложения, приемащият AVS шлюз трябва също да има право да се свързва към DB2 за VM сървър, преди AVS да може да прехвърли заявките на потребителя. Оторизацията се изпълнява, като се осигурят подходящите оператори за управление на IUCV директорията съответно на потребителския компютър, на компютъра с базата данни, и изпращащия и получаващия AVS компютър. Подробности как да направите това потърсете в *Планиране, администриране и използване на VM/ESA свързвания*.

APPC/VM
APPC/VM представлява API на ниво асемблер за VM, който осигурява подмножество от функциите на LU 6.2 както са дефинирани от SNA. На практика осигурява функции LU 6.2, които позволяват на приложения за

DB2 за VM да се свързват и да се обработват в локални и отдалечени мениджъри на бази данни. LU 6.2 функциите, поддържани от APPC/VM са изброени в ръководството *VM/ESA CP Програмни услуги*.

Комуникационна директория
Комуникационната директория е файл CMS NAMES, който играе специфична роля в установяването на APPC диалог между локален VM Средство за обработка на заявки и Сървър на приложения. Директорията осигурява необходимата информация за насочване и установяване на APPC диалог със сървъра приемник. Тази информация включва такива елементи, като име на LU, TPN, защита, име на режим, потребителски идентификатор, парола и име на база данни.

DB2 за VM използва етикета COMDIR :dbname, за да разграничи името RDB_NAME от съответните насочващи данни

Този специален файл и комуникационните му функции са описани във VM/ESA *Свързвания – планиране, администриране и използване*.

CRR CRR (Coordinated Resource Recovery – Координирано възстановяване на ресурси) е средство на VM, което координира записването или отменянето на записвания при защитени ресурси. Разпределените приложни програми, заедно със CRR, използват защитени диалози, за да осигурят целостта на ресурсите в транзакцията.

CRR сървър за възстановяване
CRR сървърът за възстановяване е компонент на CRR и се изпълнява в своя собствена виртуална машина. Отговаря за изпълнението на функциите за записване на точка на синхронизация и повторно синхронизиране.

GCS Системата за управление на група е VM компонент, който се състои от:

- Общ сегмент, който работи във виртуална машина
- Надзирател на виртуална машина, който събира много виртуални машини в група и надзирава тяхната работа
- Интерфейс между следните програмни продукти:
  - Virtual Telecommunications Access Method (VTAM)
  - APPC/VTAM поддръжка (AVS)
  - Remote Spooling Communications Subsystem (RSCS)
  - Управляваща програма CP)

  GCS надзирава изпълнението на VTAM приложения, като AVS във VM обкръжение. Виртуалните машини, които работят под ръководството на GCS не използват CMS.

Ресурсен адаптер
Ресурсният адаптер е частта от логиката на DB2 за VM, която се намира на вашата виртуална машина и позволява на вашите приложения да се обръщат със заявки за достъп към DB2 за VM сървър. Функцията на DRDA Средство за обработка на заявки е интегрирана в ресурсния адаптер.

TSAF Средството за прозрачен достъп до услуги (TSAF) е VM компонент, който осигурява комуникационна поддръжка между взаимосвързани VM системи. До осем VM системи могат да участват в TSAF колекция, която може да се разглежда като аналогична на VM локална мрежа (или глобална мрежа). Всяка участваща VM система трябва да има действаща TSAF виртуална машина. В рамките на TSAF колекция са уникални всички потребителски идентификатори и идентификатори на ресурси.

DB2 за VM използва TSAF, за да насочи заявките за разпределена база данни към друга DB2 за VM машина в рамките на TSAF колекцията. Ако локалната VM система няма AVS виртуална машина, DB2 за VM използва TSAF, за да насочи DRDA заявките към VM система, която има AVS виртуална машина. AVS дава възможност заявката да се препрати към други TSAF колекции и системи, които не са DB2 за VM.

TSAF колекция се разглежда като една или повече логически единици в SNA мрежата. Ресурсите, дефинирани като глобални в рамките на TSAF колекция, могат да се достигнат от отдалечени APPC програми, които се намират на произволно място в колекцията.

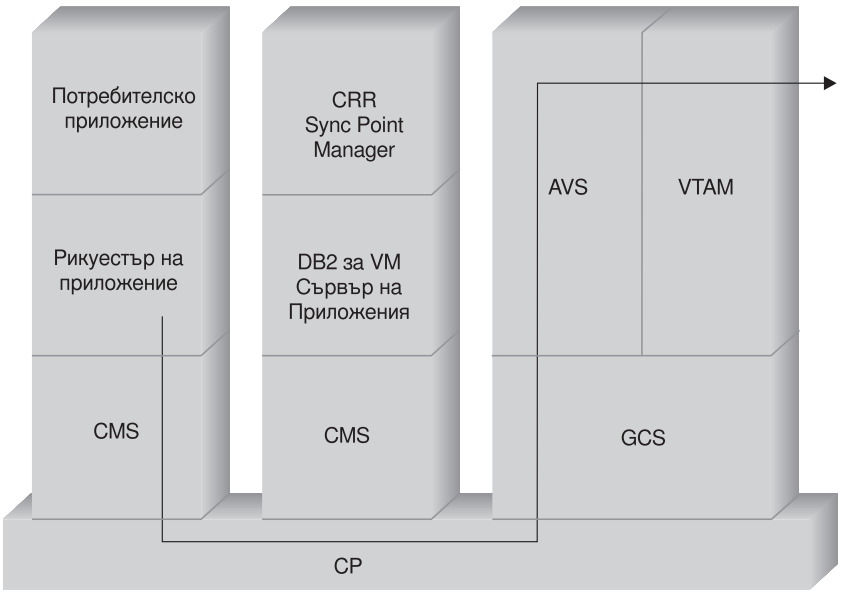
Обикновено TSAF колекция работи сама за себе си, като не зависи от VTAM и SNA мрежата. Обаче може да се кооперира с AVS и VTAM, за да направи своите глобални ресурси достъпни за отдалечени APPC програми, които се намират на произволно място в SNA мрежата. Необходимо е AVS машина и VTAM машина да работят върху един или повече от TSAF членовете. TSAF е описано във VM/ESA *Свързвания – планиране, администриране и използване*.

VTAM Виртуалният телекомуникационен метод за достъп (VTAM) осигурява поддръжка на мрежовите комуникации при свързваемост. DB2 за VM използва услугите на VTAM чрез AVS, за да насочи свързвания и заявки към отдалечени DRDA системи. VTAM се използва *само* за отдалечени заявки при достъп до SNA мрежата.

***IDENT**
AVS и TSAF използват името на транзакционната програма (TPN), за да насочват заявките между VM системи, които са свързани чрез TSAF и AVS. TPN може да е регистрирано в SNA или да е валидно буквено–числено име. VM разглежда стойността на TPN като идентификатор на ресурс. За да могат отдалечени DRDA системи да имат достъп до DB2 за VM сървър, DB2 за VM сървърът използва системната услуга VM IDENTIFY (*IDENT), за да се дефинира като мениджър на идентификатор на глобален ресурс (TPN). След като сървърът е идентифициран като глобален ресурс, TSAF и AVS могат да насочват DRDA заявки към DB2 за VM сървър, ако полученото име TPN съответства на идентификатора на ресурса.

Пример за комуникационен поток в рикуестър за приложения

Следващият пример показва каква роля играе всеки компонент при установяването на комуникации между VM рикуестър за приложения и отдалечен DRDA сървър. Фигура 27 на страница 102 показва как рикуестърът за приложения се свързва към AVS и използва VTAM за достъп до SNA мрежа. Достъпът до отдалечени ресурси не се насочва през локалния DB2 за VM сървър на приложения.



Фигура 27. Заявяване на достъп до отдалечен ресурс

Да предположим, че DB2 за VM рикуестър за приложения, който работи в TSAF колекция, трябва да се свърже към отдалечени данни, управлявани от DRDA сървър на приложения. По дефиниция това означава, че TSAF машина работи върху локалния VM хост, където се намира рикуестърът за приложения. Освен това AVS компонент и VTAM машина работят на VM система в тази TSAF колекция. AVS и VTAM може да се намират на същата система като рикуестъра за приложения и сървъра на приложения.

След стартирането си VTAM машината дефинира локалния AVS шлюз в SNA мрежата и активира една или повече сесии, които ще се използват по–късно при установяването на диалози.

След като стартира, AVS машината се споразумява за максималния брой сесии между локалния AVS шлюз и потенциалните партниращи LU.

Сървърът на приложения може да е активен или не. Операторът трябва да го стартира, преди да подаде заявки от такъв или различен рикуестър за приложения.

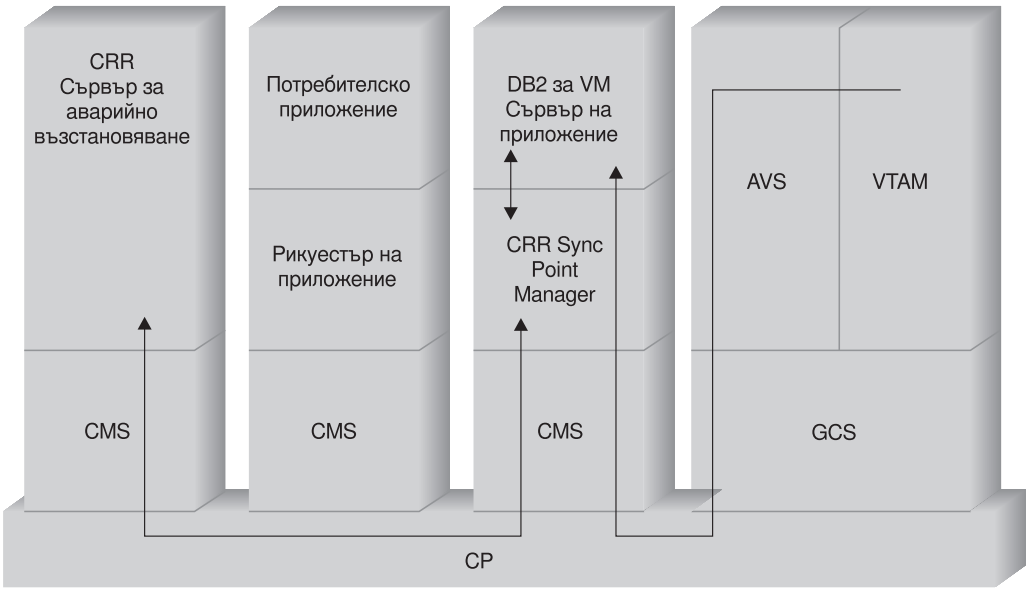
Рикуестърът за приложения подава APPC/VM оператора CONNECT, за да установи LU 6.2 диалог със сървъра на приложения. Функцията CONNECT използва CMS комуникационната директория, за да анализира името на релационната база данни в асоциираното LU име и TPN, които изграждат адреса на сървъра на приложения в SNA мрежата. Освен това CMS комуникационната директория определя защитата на ниво диалог и токените, свързани със защитата, като потребителски идентификатор и парола, за да ги предаде към отдалечената система за нуждите на оторизацията. Ако се използва SECURITY=PGM, рикуестърът за приложения може да подаде потребителски идентификатор и парола към сървъра на приложения. Можете да определите потребителския идентификатор и паролата в CMS комуникационната директория или в записа APPCPASS, дефиниран с директорията CP на потребителя на рикуестъра за приложения. Ако се използва SECURITY=SAME, към сървъра на приложения се изпраща само идентификаторът за влизане във VM на потребителя на рикуестъра за приложения, като не се изисква допълнителна парола.

Например, ако използвате SECURITY=SAME, хостът проверява дали AVS машина работи локално. В противен случай хостът установява свързване между рикуестъра за приложения и локалната TSAF машина Локалната TSAF машина проверява сред другите TSAF машини в TSAF колекцията за AVS машината и след това установява свързване към нея.

AVS компонентът в TSAF колекцията конвертира заявка за APPC/VM свързване към свое еквивалентно APPC/VTAM функционално обръщение. AVS след това използва съществуваща сесия или заделя нова сесия между своя шлюз (LU) и отдалечената LU. После AVS установява диалог с отдалечената LU и предава LU името, TPN, нивото на защита и потребителския идентификатор. Ако отдалечената LU също е VM система, сесията и диалога се обслужват от AVS компонента, който работи на тази система.

Пример за комуникационни потоци на сървър на приложения

Следващият пример показва каква роля играе всеки компонент при установяването на комуникации между отдалечен рикуестър за приложения и локален DB2 за VM DRDA сървър. Фигура 28 показва, че VTAM насочва входящо свързване към специфичен AVS шлюз и след това към сървър на приложения.



Фигура 28. Получаване на достъп до отдалечен ресурс

Да предположим, че DB2 за VM сървър на приложения работи в TSAF колекция. По дефиниция това означава, че TSAF машина работи върху локалния VM хост, където се намира сървърът на приложения. Освен това AVS компонент и VTAM машина работят на VM система в тази TSAF колекция. AVS и VTAM може също да се намират на същата система, като рикуестъра за приложения и сървъра на приложения.

След стартирането си VTAM машината дефинира локалния AVS шлюз в SNA мрежата и активира една или повече сесии, които ще се използват по–късно при установяването на диалози.

След като стартира, AVS машината се споразумява за максималния брой сесии между локалния AVS шлюз и потенциалните партниращи LU.

Сървърът на приложения може да е активен или не. Операторът трябва да го стартира, преди да подаде заявки от такъв или различен рикуестър за приложения. След стартирането си сървърът на приложения използва услугата *IDENT, за да регистрира на хост VM системата идентификатора на ресурс, който управлява. При всяко регистриране се създава запис в таблицата с вътрешни ресурси, която се поддържа от VM системата.

След като локалният AVS компонент установи сесията със своята партниращa LU, приема диалога и предава TPN, потребителски идентификатор и парола към VM хоста, за да се провери валидността. VM търси TPN в своята таблица с вътрешни ресурси. Тази таблица съдържа запис за всеки идентификатор на ресурс, регистриран чрез системната услуга *IDENT. Ако търсенето на TPN завърши с успех, VM проверява валидността на потребителския идентификатор и паролата чрез своята директория или чрез RACF или подобен продукт за защита.Ако проверката за валидност приключи успешно, AVS установява свързване към сървъра на приложения и му подава потребителския идентификатор за нуждите на правата за достъп до базата данни.

Ако търсенето в таблицата приключи неуспешно, AVS приема, че тази стойност на TPN може да се намира в друга VM система в TSAF колекцията и установява свързване към локалната TSAF машина, като подава потребителски идентификатор, парола и TPN. TSAF машината проверява другите TSAF машини в TSAF колекцията. Ако някоя от тези машини признае за съществуването на TPN в нейната таблица на ресурси, локалната TSAF машина се свързва към отдалечената TSAF машина и подава потребителския идентификатор и паролата, за да се провери тяхната валидност чрез съответната VM директория. Ако проверката за валидност приключи успешно, отдалечената TSAF машина се свързва към сървъра на приложения и му подава потребителския идентификатор за нуждите на правата за достъп до базата данни.

Ако рикуестърът за приложения иска да се възползва от DRDA поддръжката на разпределена единица работа, той установява защитен диалог (например SYNCLEVEL=SYNCPT) с DB2 за VM сървъра на приложения. Преди CMS да представи свързването към DB2 за VM, се създава CMS единица работа за защитения диалог на DB2 за VM машината. След това DB2 за VM използва тази CMS единица работа винаги, когато изпълнява работа за рикуестъра. Когато DB2 за VM започне да работи за рикуестъра, регистрира тази CMS единица работа на CRR мениджъра за точка на синхронизация. Затова когато DB2 получи указание да запише промени или да отхвърли промените в защитения диалог, ще попита CRR мениджъра за точка на синхронизация, за да запише или отхвърли единицата работа. След това CRR мениджърът за точка на синхронизация задейства записването или отхвърлянето на промените, като се обръща към CRR сървъра за възстановяване, за да изпълни записване на точка на синхронизация, когато е необходимо.

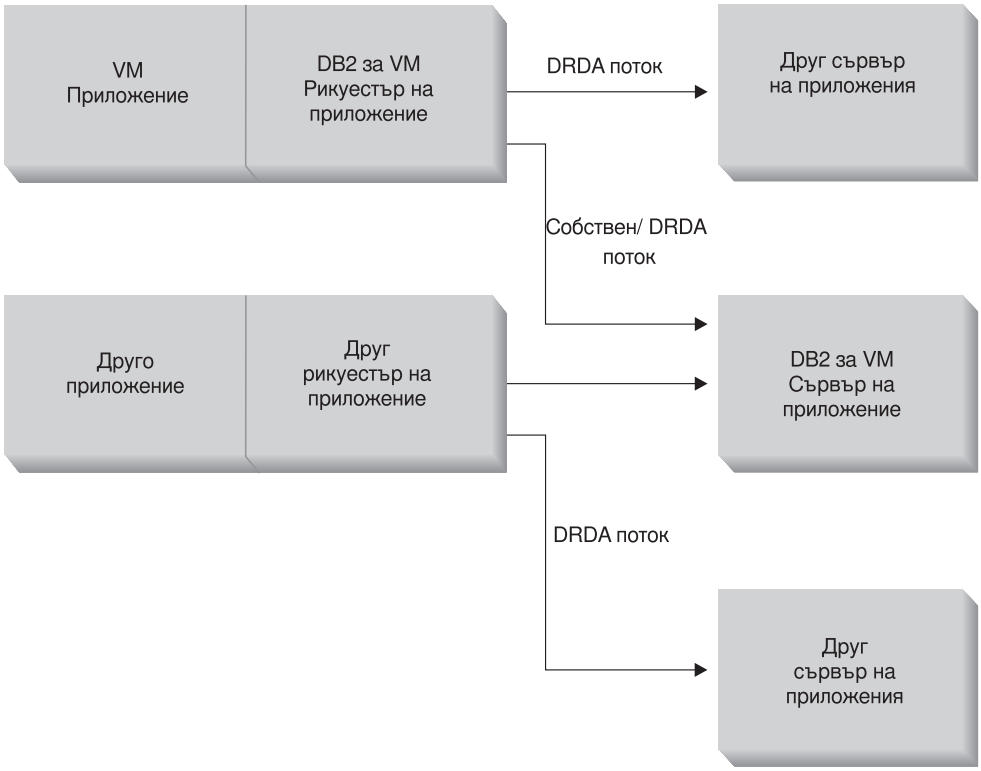
В зависимост от сложността на насочването на свързването APPC диалогът между рикуестър за приложения и сървър на приложения може да включва допълнителни системи. Но всички междинни свързвания се управляват от VM и са прозрачни за рикуестъра за приложения или за приложението потребител. Интерфейсът на APPC/VM позволява на DB2 за VM сървъри на приложения да комуникират с APPC приложни програми, които се намират на:

- Същата VM система
- Различна VM система
- VM система в SNA мрежа, на която работи AVS и VTAM

- VM система в друга TSAF колекция, на която работи AVS и VTAM
- Система, която не е VM, в SNA мрежа, поддържаща LU 6.2 протокола
- Система, която не е на IBM, но в SNA мрежа, която поддържа LU 6.2 протокола

DB2 за VM реализация

Както е показано в Фигура 29, VM приложение трябва да премине през DB2 за VM рикуестър за приложения (ресурсен адаптер), за да достигне до някоя база данни на DB2 за VM или DRDA Сървър на приложения. База данни на DB2 за VM Сървър на приложения може да получава SQL заявки от произволна система DB2 за VM или DRDA Средство за обработка на заявки.



Фигура 29. DB2 за VM рикуестър за приложения и сървър на приложения

Опции при предварителна обработка или изпълнение на приложение

DB2 за VM поддържа три опции за обработка на командата SQLINIT, които позволяват на потребителя и на администратора на базата данни да активират поддръжката на разпределена база данни. Потребителят може да определи една от следните опции SQLINIT, преди предварителната обработка или изпълнение на приложението:

PROTOCOL(SQLDS)

Заявява използването на частен SQLDS протокол. Това е опцията по подразбиране. Може да се използва между DB2 за VM рикуестър за приложения и сървър в локално или отдалечено обкръжение. DB2 за VM

сървърът за приложения приема, че рикуестърът използва същите стойности на CCSID като сървъра. Стойностите на CCSID по подразбиране [5] настроени от рикуестър чрез SQLINIT се игнорират и не се асоциира идентификатор на LU 6.2 LUWID с диалога. Ако използвате само DB2 за VM системи и един и същи идентификатор CCSID по подразбиране, тогава това е най–ефективната опция.

PROTOCOL(AUTO)

Обръща се към DB2 за VM рикуестъра за приложения, за да разбере дали сървърът за приложения е такава или различна система. След това автоматично избира използването на частен SQLDS протокол за подобните системи или DRDA протокол за различните системи. Може да се използва между еднакви (локални и отдалечени) и различни системи. Ако сървърът на приложения не е настроен с опция PROTOCOL=SQLDS, тогава рикуестърът за приложения и сървърът може да имат различни стойности на CCSID по подразбиране. Заявките и отговорите се конвертират. AUTO е препоръчваната опция при следните случаи:

- Ако трябва да осъществите достъп както до подобни, така и до различни системи
- Ако стойностите на CCSID по подразбиране са различни на рикуестъра и на сървъра (и опцията PROTOCOL на сървъра на приложения не е SQLDS)
- Ако се нуждаете от LU 6.2 LUWID, асоцииран с всеки диалог, така че да можете лесно да проследите задачата обратно до първоначалната и система. Това е полезно, ако управлявате много отдалечени DB2 за VM системи в мрежа на разпределена база данни.

PROTOCOL(DRDA)

Определя DB2 за VM рикуестърът за приложения да използва само DRDA протокол при комуникации със сървъра на приложения. Можете да използвате тази опция между еднакви (локални и отдалечени) и различни системи. Ако сървърът на приложения е същата система, тогава се използва DRDA протокол между две DB2 за VM системи. средство за обработка на заявки и Сървър на приложения може да имат различни стойности на CSID по подразбиране. Заявките и отговорите се конвертират. Можете да използвате тази опция между две DB2 за VM системи при тестване или при специфични приложения, където използването на DRDA протокола може да осигури по–добра производителност поради използването на по–голям буфер за изпращаните и получаваните данни.

Таблица 3 сравнява функционалните характеристики на опциите за обработка SQLINIT в DB2 за VM средство за обработка на заявки.

Таблица 3 (Страница 1 от 2). Сравнение на опциите за обработка SQLINIT на DB2 за VM рикуестър за приложения

[SQLDS]	[AUTO]	[DRDA]
И двата партньора трябва да са DB2 за VM системи	Свързва се към всяка DRDA система	Свързва се към всяка DRDA система

[5] В DB2 за VM рикуестърът за приложения и сървърът на приложения определят стойността на CCSID по подразбиране, като използват опция CHARNAME съответно за SQLINIT и SQLSTART. CHARNAME е символното име, което вътрешно се трансформира до съответните стойности на CCSID.

[6] Поддържа се разширен динамичен SQL при DRDA потоци, като се използва конвертиране до статични или динамични оператори. Прилагат се някои ограничения.

Таблица 3 (Страница 2 от 2). Сравнение на опциите за обработка SQLINIT на DB2 за VM рикуестър за приложения

Може да комуникира с партньор локално чрез TSAF или AVS/VTAM	Може да комуникира с DB2 за VM система локално или с отдалечена DB2 за VM система чрез TSAF или AVS. С различна система трябва да комуникира чрез AVS.	Може да комуникира с DB2 за VM система локално или с отдалечена DB2 за VM система чрез TSAF или AVS. С различна система трябва да комуникира чрез AVS.
Поддържа статичен, динамичен и разширен динамичен SQL	Поддържа статичен, динамичен и разширен динамичен SQL	Поддържа статичен, динамичен и разширен динамичен SQL [6]
DB2 за VM сървъра на приложения игнорира стойностите на CCSID, дефинирани от SQLINIT за рикуестъра за приложения	Стойностите на CCSID, дефинирани от SQLINIT за Средство за обработка на заявки, се уважават от DB2 за VM Сървър на приложения и се изпълнява правилното конвертиране (ако сървърът на приложения е настроен също с опцията AUTO)	Стойностите на CCSID, дефинирани от SQLINIT за Средство за обработка на заявки, се уважават от DB2 за VM Сървър на приложения и се изпълнява правилното конвертиране
Фиксиран размер на блок от 8K; Обръщение OPEN не връща редове; Средство за обработка на заявки трябва изрично да затвори указател	DB2 за VM към DB2 за VM: SQLDS метод; всички останали: DRDA метод	Променлив размер на блок от 1K до 32; по–компактни данни; обръщение OPEN връща един блок редове; Сървър на приложения може косвено да затвори указател, като спести необходимостта Средство за обработка на заявки да изпраща обръщение CLOSE
Може да използва команди INSERT и PUT за указатели за вмъкване на блок от редове в момент, когато се използва фиксиран размер на блок от 8K	DB2 за VM към DB2 за VM: SQLDS метод; всички останали: DRDA метод	PUT се конвертират в обикновени вмъквания от по един ред и се изпращат ред по ред
Поддържат се всички команди, уникални за DB2 за VM	DB2 за VM към DB2 за VM: SQLDS метод; всички останали: DRDA метод	Не се поддържат командите за оператори на DB2 за VM, някои оператори за DB2 за VM и някои команди ISQL и DBSU (Вижте *SQL справочник за DB2 за VSE & VM*).
LUWID не се поддържа	LUWID се поддържа	LUWID се поддържа

Опции за стартиране на сървър на база данни

Този раздел описва различните опции за стартиране на сървър на база данни.

Параметърът PROTOCOL

Администраторът на базата данни може да определи една от следните опции за параметъра `PROTOCOL`, когато стартира сървъра на базата данни.

SQLDS

Подразбираща се и препоръчвана опция, ако сървърът на приложения трябва да осигури поддръжка само на DB2 за VM рикуестъри за приложения или ако DB2 за VSE заявките за приложения се възползват от VSE достъп на гост. Сървърът на приложения използва само частния (SQLDS) поток.

Сървър на приложения е чувствителен по отношение на избраните опции за обработка от средство за обработка на заявки. Ако DB2 за VM рикуестър определи PROTOCOL(SQLDS), обработката на DB2 за VM сървър

продължава нормално с частните потоци. Ако DB2 за VM рикуестърът определи PROTOCOL(AUTO), DB2 за VM сървърът уведомява рикуестърът да превключи към частните потоци. Между рикуестъра за приложения и сървъра на приложения не се обменя информация за CCSID. Сървърът на приложения приема, че рикуестърът на приложения използва същите стойности за CCSID, както сървъра на приложения. Ако DB2 за VM рикуестърът определи PROTOCOL(DRDA), диалогът се прекратява. Ако рикуестър за приложения, различен от DB2 за VSE & VM, се опита да осъществи достъп до DB2 за VM сървър, диалогът се прекратява.

AUTO Препоръчваната опция, ако сървърът на приложения трябва да осигури поддръжка както за частния протокол, така и за DRDA протокола. DB2 за VM рикуестърите за приложения, които определят PROTOCOL(SQLDS) или PROTOCOL(AUTO), комуникират в частния поток. За рикуестър на приложения, който определя SQLDS, не се обменя информация за CCSID и сървърът за приложения приема, че стойностите на CCSID в рикуестъра за приложения са същите както в сървъра на приложения. При рикуестър, който е определил AUTO, се обменя информация за CCSID и се изпълнява съответното конвертиране на заявките и отговорите на база стойността на CCSID. DRDA потокът е необходим за рикуестърите, различни от DB2 за VM, както и за всички DB2 за VM рикуестъри, които са определили PROTOCOL(DRDA).

Параметърът SYNCPNT

Този параметър определя дали да се използва мениджър за синхронизация (SPM), за да координира дейности като DRDA–2 многосайтово четене, многосайтово записване на разпределена единица работа.

Ако е въведено Y, сървърът ще използва мениджър за синхронизация, ако е възможно, за да координира двуфазови записвания на промени и синхронизиране. Ако е въведено N, сървърът за приложения няма да използва SPM, за да изпълни двуфазови записвания на промените. Ако е въведено N, сървърът на приложения се ограничава до многосайтово четене, записване в една система на разпределени единици работа и може да е единствената записваща страна. Ако е въведено Y, но сървърът за приложения открие, че не е достъпен мениджър за синхронизация, тогава сървърът работи така, като че ли е въведено N.

По подразбиране е SYNCPNT=Y, когато PROTOCOL=AUTO. Когато PROTOCOL=SQLDS, параметърът SYNCPNT се установява на N.

Настройка на рикуестър за приложения във VM обкръжение

DB2 за VM реализира поддръжката на DRDA Средство за обработка на заявки като неделима част от ресурсния адаптер, който се намира на виртуалната машина с приложението на крайния потребител. Можете да използвате поддръжката на Средство за обработка на заявки, дори когато не е активна виртуалната машина на локалната мениджъри на бази данни. Можете да активирате поддръжката на DRDA рикуестър за приложения, като изпълните SQLINIT EXEC с ОПЦИЯ PROTOCOL(AUTO) или PROTOCOL(DRDA) (вижте “Опции при предварителна обработка или изпълнение на приложение” на страница 105).

Когато DB2 за VM действа като Средство за обработка на заявки, може да се свързва към DB2 за VM Сървър на приложения или някой друг сървър, който поддържа DRDA архитектурата. За да може DB2 за VM Средство за обработка на заявки да осигури достъп до разпределена база данни, трябва да знаете как да направите следното:

- "Осигуряване на мрежова информация" на страница 109. Рикуестърът за приложения трябва да може да приема стойности на RDB_NAME и да ги преобразува до SNA стойности NETID.LUNAME. DB2 за VM използва CMS комуникационната директория, за да каталогизира имената RDB_NAME и съответните им мрежови параметри. Комуникационната директория позволява на рикуестъра за приложения да подава необходимата SNA информация към VTAM, когато генерира заявки за разпределена база данни.
- "Осигуряване на защита" на страница 115. За да може сървър на приложения да приема заявки от отдалечена база данни, Средство за обработка на заявки трябва да осигури изискваната от сървъра на приложения информация за защитата. Когато генерира заявки за разпределени бази данни, за да осигури необходимата за мрежовата защита информация, DB2 за VM използва комуникационната директория и CP директорията от страната на средство за обработка на заявки, а допълнително и CP директорията или RACF от страната на Сървър на приложения.
- "Представяне на данни" на страница 119. Рикуестърът за приложения трябва да има стойност на CCSID, която е съвместима със сървъра на приложения.

Осигуряване на мрежова информация

Голяма част от обработките в среда на разпределена база данни изискват обмен на съобщения с други системи във вашата мрежа. За да изпълните правилно този процес, предприемете следните стъпки:

1. Дефинирайте локалната система
2. Дефинирайте отдалечената система
3. Дефинирайте комуникационната подсистема
4. Определете размерите на RU и стъпките
5. Подгответе DB2 за VM рикуестъра за приложения

Дефиниране на локалната система

DB2 за VM рикуестърът за приложения и DB2 за VM сървърът на приложения не зависят един от друг. DB2 за VM рикуестърът за приложения насочва заявките за свързване директно към локалните или отдалечени сървъри на приложения. Но не се дефинира като приемник за входящи заявки за свързване. Само DB2 за VM сървърът на приложения може да приема (или отхвърля) входящи заявки за свързване. Следователно DB2 за VM рикуестърът за приложения не идентифицира стойности за RDB_NAME и TPN за себе си, както DB2 Universal Database за OS/390.

Дефинирайте DB2 за VM рикуестър за приложения в SNA мрежата както следва:

1. Дефинирайте имена на AVS шлюзове с помощта на операторите за дефиниране VTAM APPL.

   Рикуестърът за приложения трябва да има дефинирани имена на шлюзове (например LU имената), за да насочва своите изходящи заявки в мрежата. Фигура 30 на страница 110 показва такъв пример. Тези оператори се намират върху VTAM виртуалната машина. При стартиране на VTAM шлюзовете се идентифицират в мрежата, но не се активират, докато не стартира управляващата AVS виртуална машина. Всяка AVS виртуална машина може да дефинира няколко шлюза върху VM хост.

```
        VBUILD TYPE=APPL
************************************************************
*                                                          *
*     Дефиниране на шлюз за DB2 за VM системата Торонто    *
*                                                          *
************************************************************
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
```

Фигура 30. Пример за дефиниране на AVS шлюз

В следващия списък са описани ключовите думи на оператора VTAM APPL, които са свързани с темите в това ръководство. (Операторът VTAM APPL поддържа много повече ключови думи от показаните тук).

TORGATE
VTAM използва етикета на оператора APPL като име на шлюз (LU). В Фигура 30, е дефиниран шлюзът TORGATE. Операторът VTAM APPL не определя стойност NETID. Тя автоматично се присвоява за всички VTAM приложения във VTAM системата.

AUTOSES=1
Шлюзът TORGATE определя, че една SNA сесия победител автоматично се стартира, когато се генерира командата на APPC за промяна броя на сесиите Change Number of Sessions (CNOS). Трябва да определите различна от нула стойност с помощта на AUTOSES при AVS, за да се информира при всички случаи, когато не приключи успешно командата CNOS. Не е необходимо автоматично да стартирате всички APPC сесии между всеки два участника в разпределена база данни. Ако стойността AUTOSES е по–малка от ограничението за сесии победители (DMINWNL), VTAM забавя стартирането на останалите сесии, докато те станат необходими за приложение в разпределена база данни.

DMINWNL=10
Шлюзът TORGATE определя, че тази DB2 за VM система е победител поне за 10 сесии. При обработката на CNOS се използва параметърът DMINWNL за стойност по подразбиране, но може да се замени за всеки отделен партньор, като се използва командата AGW CNOS от AVS виртуалната машина.

DMINWNR=10
Шлюзът TORGATE определя, че този партньор е победител поне за 10 сесии. При обработката на CNOS се използва параметърът DMINWNR за стойност по подразбиране, но може да се замени за всеки отделен партньор, като се използва командата AGW CNOS от AVS виртуалната машина.

DSESLIM=20
20 е общият брой на сесиите (както победили, така и загубили), които можете да установите между шлюза TORGATE и всички разпределени

системи партньори за специфично име на група и режим. При обработката на CNOS се използва параметърът DSESLIM като стойност по подразбиране, но може да се замени за всеки отделен партньор, като се използва командата AGW CNOS от AVS виртуалната машина. Ако партньорът не поддържа броя на сесиите, определени от параметрите DSESLIM, DMINWNL или DMINWNR, обработката на CNOS определя нови стойности за тези параметри, които са приемливи за него.

EAS=9999
Оценка за общия брой на сесиите, които се изискват от тази VTAM LU.

MODETAB=RDBMODES
Името на VTAM таблицата с режими е RDBMODES. Тази таблица съдържа всички имена на режими, които този шлюз може да използва при комуникации с други партньори в разпределената база данни.

SECACPT=ALREADYV
Това е параметърът за защита, който определя най–високото ниво на защита на APPC диалог, което този шлюз поддържа, когато получи заявка за разпределена база данни от отдалечен партньор. SECACPT=ALREADYV се препоръчва. Опцията ALREADYV поддържа следните нива на защита:

- SECURITY=NONE, заявката не съдържа никаква информация за защита. DB2 за VM отхвърля DRDA заявки, които използват това ниво на защита.
- SECURITY=PGM, заявката съдържа идентификатора и паролата на потребителя. DB2 за VM приема DRDA заявки, които използват това ниво на защита.
- SECURITY=SAME посочва, че валидността на заявката вече е проверена и съдържа само потребителския идентификатор.

SYNCLVL=SYNCPT
Параметърът SYNCLVL определя нивото за поддръжка на синхронизирането при AVS. Стойност SYNCPT посочва, че се поддържат нива на синхронизиране NONE, CONFIRM и SYNCPT. Ако този AVS шлюз ще се използва при DRDA–2 разпределена единица работа на DB2 за VM сървър, определете стойност SYNCPT. Ако НЯМА да се изпълнява разпределена единица работа, тогава въведете стойност CONFIRM (посочва, че се поддържат NONE и CONFIRM, но не и SYNCPT).

VERIFY=NONE
Определя нивото за защита на SNA сесия (валидност на LU партньор), изисквано от тази DB2 за VM система. Стойност NONE посочва, че не е необходимо да се проверява валидността на LU партньор.

DB2 за VM не ограничава избора на ключова дума VERIFY, но VTAM версията, която използвате, може да окаже влияние. В несигурна мрежа DB2 за VM препоръчва кодирането VERIFY=REQUIRED. Ако изберете VERIFY=OPTIONAL, VTAM проверява валидността на LU партньор само за тези, които осигуряват поддръжка. Ако се използва VERIFY=REQUIRED, VTAM отхвърля партньорите, които не могат да изпълнят проверка на валидност на LU партньор.

VPACING=2
Този параметър определя броя на стъпките за сесията, използвани между LU партньори и този шлюз. Стъпката на сесията е много важна при разпределени бази данни.

2. Активирайте шлюза.

   Активирането на шлюза се изпълнява от AVS виртуалната машина, която работи на същия хост (или други хостове в рамките на една и съща TSAF колекция) като DB2 за VM Средство за обработка на заявки. Включете командата на AGW ACTIVATE GATEWAY GLOBAL в профила на AVS машината или използвайте тази команда интерактивно от конзолата на AVS машината, за да активирате автоматично шлюза при всяко стартиране на AVS.
3. Използвайте командата AGW CNOS, за да договорите броя сесии между шлюза и всеки от LU партньорите.

   Стойността MAXCONN в CP директорията на AVS шлюза трябва да е достатъчно голяма, за да поддържа общия брой сесии, които се изискват.

   Използвайте командата AGW DEACTIVE GATEWAY от AVS виртуалната машина, за да деактивирате шлюза. Дефиницията на шлюза остава. Шлюзът може да се активира в произволен момент с помощта на командата AGW ACTIVATE GATEWAY GLOBAL.

   Вижте *Планиране, администриране и използване на VM/ESA свързвания* за форматите на AVS командите.
4. Проверете дали по време на инсталирането VTAM NETID е дефиниран в DB2 ЗА VM DBMS.

   NETID на хоста (или други хост системи в рамките на същата TSAF колекция), където се намира Средство за обработка на заявки, се доставя от VTAM, когато заявката влезе в мрежата. NETID се съхранява в CMS файла SNA NETID и се намира върху DB2 за VM диска, до който има достъп Средство за обработка на заявки. Средство за обработка на заявки използва тази стойност за NETID при генерирането на LUWID, който съпътства всеки диалог.

Дефиниране на отдалечени системи

Трябва да дефинирате отдалечените системи, като регистрирате имената на LU, които позволяват на VTAM да намери необходимото място в мрежата. При стартирането си AVS идентифицира имената на глобалните шлюзове (имената на LU), достъпни при насочване на SQL заявки в мрежата до VTAM. Имената на шлюзове трябва да са уникални в рамките на множеството имена на LU, които се разпознават от локалната VTAM система, така че да могат да се насочват входящите и изходящите заявки към правилното име на LU. Това е най–добрият начин да се осигури уникалност на имената на шлюзове в рамките на потребителската мрежа. От своя страна така се опростява процесът на дефиниране на VTAM ресурсите.

Когато DB2 за VM приложение заяви данни от отдалечена система, DB2 за VM търси в CMS комуникационната директория за следната информация, свързана с отдалечената система:

- Име на шлюз (локално име на LU)
- Име на отдалечена LU
- Отдалечена TPN
- Ниво на защита на диалог, изисквана от сървъра на приложения
- Потребителски идентификатор, който идентифицира рикуестъра за приложения на сървъра на приложения
- Парола, която дава оторизация на рикуестъра за приложения върху сървъра на приложения

- Име на режим, който описва характеристиките на сесията, използвани при комуникациите с Сървър на приложения
- RDB_NAME

Директория за CMS комуникации е CMS файл с тип на файл NAMES, който се създава и управлява от администратора на DB2 за VM системата. Като администратор можете да използвате XEDIT, за да създадете този файл и да добавите желаните записи, за да идентифицирате всеки потенциален DRDA партньор. Всеки запис в директорията се определя от етикетите и свързваните с тях стойности. Фигура 31 показва прост запис. Когато се изпълни търсене, ключът за търсене се сравнява със стойността на етикета :dbname за всеки запис във файла, докато не се намери съответствие или не се достигне края на файла. В примера в Фигура 31 мениджърът за продажбите в Торонто иска да създаде отчет за продажбите през месеца за поделението в Монреал, като отдалечено извлече данните от базата данни 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
```

Фигура 31. Прост запис в Директория за CMS комуникации

Етикетът :tpn определя името на транзакционната програма, която активира Сървър на приложения. Първата част от етикета :luname определя AVS шлюза (локалната LU), използван за получаване на достъп до SNA мрежата. Втората част определя името на отдалечената LU. Етикетът :modename определя VTAM режима, който дефинира характеристиките на сесията, заделена между локалната и отдалечената LU. Размерът на единицата заявка (RU – Request unit), стъпката и класа на услуги (COS – class of service) са примери за такива характеристики. Етикетът :security показва нивото на защита, което се използва при свързването на Средство за обработка на заявки към Сървър на приложения.

Директория за CMS комуникации е на общия системен диск, до който имат достъп всички средство за обработка на заявки в определена VM система. Всяка програма или продукт, която изисква достъп чрез VTAM, може да използва Директория за CMS комуникации.

Можете да осъществите достъп до две нива на Директория за CMS комуникации: системно ниво и потребителско ниво. Например, можете да създадете директория на системно ниво върху общия системен диск, достъпен от всички Средство за обработка на заявки в определена VM система. Освен това можете да създадете ваша собствена директория на потребителско ниво, която да заменя съществуващите стойности или да въвежда нови записи, които не се появяват в директорията на системно ниво. Най–напред се търси в директорията на потребителско ниво и ако търсенето не приключи успешно, тогава се търси и в директорията на системно ниво. Директорията на системно ниво е разширение към директорията на потребителско ниво; в нея се търси, само ако стойностите не се намерят в директорията на потребителско ниво.

Всяка от тези директории се идентифицира за приложението и се активира чрез командата CMS SET COMDIR. Например можете да използвате следната последователност от команди, за да идентифицирате едновременно директория на системно и на потребителско ниво (съответно на минидисковете S и A), но да изберете да активирате само директорията на системно ниво при търсенията:

```
SET COMDIR FILE SYSTEM SCOMDIR NAMES S

SET COMDIR FILE USER UCOMDIR NAMES A

SET COMDIR OFF USER
```

CMS комуникационната директория е описана подробно в *Планиране, администриране и използване на VM/ESA свързвания*. CMS командата SET COMDIR е описана в *VM/ESA CMS справочник за командите*.

Дефиниране на комуникационната подсистема

Във VM обкръжението комуникациите се управляват от комбинация от компоненти. Участващите в комуникациите между DRDA системи от различен тип компоненти са APPC/VM, CMS комуникационна директория, TSAF, AVS и VTAM.

APPC/VM е API на ниво асемблер на LU 6.2, който се използва от DB2 за VM Средство за обработка на заявки при заявки за комуникационни услуги. Директория за CMS комуникации осигурява информация за маршрутизиране и защита на разпределена система от партньори. AVS активира шлюза и преобразува изходящите APPC/VM потоци в APPC/VTAM потоци, а входящите APPC/VTAM потоци в APPC/VM потоци.

APPC/VM, TSAF и AVS зависят от CMS комуникационната директория, VTAM и *IDENT, за да насочат заявките към правилния DRDA партньор.

За да може VTAM да комуникира с приложенията върху партньора, идентифицирани в CMS комуникационната директория, трябва да осигурите следната информация:

1. Дефинирайте името на LU на всеки Средство за обработка на заявки и Сървър на приложения във VTAM. Мястото и синтаксисът на тези дефиниции зависи от това как отдалечената система е свързана логически и физически към VTAM системата.
2. Създайте запис в таблицата с VTAM режимите за всяко име на режим определено в CMS комуникационната директория. Тези записи описват размера на RU (request unit – единица заявка), размера на стъпката на пакета и класа на услугите за всяко име на режим.
3. Ако смятате да използвате проверка на валидността на LU партньор (защита на ниво сесия), определете VTAM и RACF профили (или еквивалентни) за нуждите на алгоритъма за проверката.

Съображения за максималния брой на AVS сесии: Когато рикуестър за приложения използва AVS при комуникации с отдалечен сървър на приложения, се инициира свързване. Ако това свързване доведе до надвишаване на установения максимален брой сесии, AVS поставя свързването в състояние на изчакване, докато не се освободи сесия. Когато се освободи сесия, AVS присвоява сесията на чакащото свързване и управлението се връща на потребителското приложение. За да се избегне тази ситуация, трябва да предвидите такива свръхнатоварвания и да увеличите максималния брой сесии, за да се позволят и допълнителни свързвания. Стойността MAXCONN в CP директорията на AVS машината трябва да е достатъчно голяма, за да поеме свръхнатоварване от APPC/VM свързвания.

Определяне размерите на RU и стъпките

Записите, които дефинирате в таблицата на VTAM режимите определят размера на RU и броя стъпки. Неправилното дефиниране на тези стойности може да има отрицателно влияние върху всички VTAM приложения.

След като изберете размера на единицата за заявки, RU, максималния брой сесии и стъпките, разгледайте влиянието на тези стойности върху съществуващата SNA мрежа. Трябва да прегледате следните елементи, когато инсталирате нова система на разпределена база данни:

- При VTAM CTC свързвания проверете дали параметърът MAXBFRU е достатъчно голям, за да поеме размера на RU плюс 29 байта, които VTAM добавя за заглавната част на SNA заявката и заглавната част на пакета за прехвърляне. MAXBFRU се измерва в единици от по 4K байта, така че MAXBFRU трябва да е поне 2, за да събере RU с размер 4K.
- При NCP свързвания се убедете, че MAXDATA е достатъчно голямо, за да поеме размера на RU плюс 29 байта. Ако определите размер на RU от 4K, MAXDATA трябва да е поне 4125.

  Ако определяте NCP параметъра MAXBFRU, изберете стойност, която събира размера на RU плюс 29 байта. При NCP, параметърът MAXBFRU дефинира броя на входно/изходните буфери на VTAM, които могат да съберат PIU. Ако изберете размер от 441 за IOBUF буфера, MAXBFRU=10 обработва правилно RU с размер от 4K, защото 10*441 е по–голямо от 4096+29.
- *Ръководство за DRDA свързване* описва как да оцените влиянието върху вашата разпределена база данни на VTAM IOBUF пула. Ако използвате прекалено много ресурси за IOBUF пула, производителността на VTAM се влошава за всички VTAM приложения.

Подготовка на рикуестър за приложения DB2 за VM

Върху DB2 за VM рикуестъра за приложения може да не е инсталирана DRDA поддръжка. Изпълнете следните стъпки, за да подготвите DB2 за VM рикуестър за приложения за DRDA комуникации:

1. Използвайте ARISDBMA, за да инсталирате DRDA поддръжката:
   - Използвайте "ARISDBMA DRDA(ARAS=Y)", ако инсталирате поддръжка за рикуестър и сървър.
   - Използвайте "ARISDBMA DRDA(AR=Y)", ако инсталирате поддръжка само на рикуестър.

   Подробности потърсете в ръководството *Администриране на DB2 за VM система*.
2. След като използвате ARISDBMA, изградете отново ARISQLLD LOADLIB на DB2 за VM. Повече подробности ще намерите в главата *Използване на DRDA обкръжение* на ръководството *Администриране на DB2 за VM система*.

Осигуряване на защита

Когато отдалечена система изпълнява обработки в разпределена база данни от името на SQL приложение, трябва да може да удовлетвори изискванията за защитата на Средство за обработка на заявки, Сървър на приложения и мрежата, която ги свързва. Тези изисквания спадат към една или повече от следните категории:

- Избиране на имена на крайни потребители
- Параметри за защита на мрежата

- Защита на мениджъра на базата данни
- Защита, прилагана от външна подсистема за защита

Избиране на имена на крайни потребители

При SQL и LU 6.2 на крайните потребители се присвояват потребителски идентификатори с дължина от 1 до 8 символа. Тази стойност трябва да е уникална в рамките на определената операционна система, но може да не е уникална в цялата SNA мрежа. Например може да има потребител с име JONES в TORONTO системата и друг потребител с име JONES в MONTREAL системата. Ако тези два потребителя са един и същи човек, няма да има конфликт. Обаче, ако JONES в TORONTO е различен от JONES в MONTREAL, SNA мрежата (а следователно и разпределените бази данни в рамките на мрежата) не могат да различат JONES в TORONTO от JONES в MONTREAL. Ако не предприемете стъпки, за да се предпазите от тази ситуация, JONES в TORONTO може да използва правата, предоставени на JONES в MONTREAL и обратно.

За да отстрани конфликтите в имената, DB2 за VM поддържа преобразуване на имената на крайните потребители. Обаче системата не налага преобразуване на потребителски идентификатори. Ако е необходимо системата да налага такова преобразуване, трябва да осигурите, че се изпълнява правилно входящо преобразуване на сървъра на приложения.

Изходящо преобразуване се изпълнява с помощта на Директория за CMS комуникации. Запис в Директория за CMS комуникации трябва да определя `:security.PGM`. В този случай съответните стойности в етикетите :userid и :password се прехвърлят към отдалечената система (Сървър на приложения) в заявката за свързване.

Като се създаде записът, показан в Фигура 32, потребителят с идентификатор JONES на локалната (TORONTO) система се преобразува до потребителски идентификатор JONEST, когато се свърже към MONTREAL_SALES_DB Сървър на приложения на системата MONTREAL. По този начин се елиминира двусмислеността на потребителския идентификатор.

```
 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
```

Фигура 32. Преобразуване на изходящи имена

Защита на мрежа

След като се избере името на крайния потребител, което представлява рикуестъра за приложения на отдалечената система (Сървър на приложения), рикуестърът за приложения трябва да осигури необходимата информация за защита на мрежата LU 6.2. LU 6.2 осигурява три основни механизми за защита на мрежата:

- Защита на ниво сесия, определена с помощта на параметъра VERIFY на оператора VTAM APPL.

- Защита на ниво диалог, определена в Директория за CMS комуникации.
- Закодиране.

Тъй като сървърът на приложения е отговорен за управлението на ресурсите на базата данни, той определя кои механизми за защита на мрежата трябва да се осигурят от рикуестъра за приложения. Трябва да запишете изискванията към защитата на сървъра на приложения в комуникационната директория на рикуестъра за приложения, като определите подходяща стойност в етикета :security.

Поддържаните от DRDA опции за защита на ниво SNA диалог са:

SECURITY=SAME

Също така е известно като вече проверена защита, защото към отдалечената система се изпраща само идентификаторът (идентификаторът при влизане) на крайния потребител. Паролата не се изпраща. Това ниво на защита на диалога се използва, когато в комуникационната директория на рикуестъра за приложения за сървъра на приложения е определено `:security.SAME`. Когато се използва тази опция, не се изпълнява преобразуване на изходящото име на крайния потребител. Потребителският идентификатор, който се изпраща към отдалечената DRDA система, е идентификаторът на влизане на CMS потребителя. Етикетът :userid в Директория за CMS комуникации се игнорира при защита от типа :security.SAME.

SECURITY=PGM

При тази опция за проверка на валидността към отдалечената система (Сървър на приложения) се изпраща както потребителски идентификатор, така и парола. Тази опция за защита се използва, когато е определено `:security.PGM` в записа на Директория за CMS комуникации на рикуестъра за приложения. Когато се използва тази опция, се изпълнява преобразуване на изходящото име на крайния потребител.

DB2 за VM не поддържа закодиране на паролата. Паролата може да се определи в етикета `:password`, или може да се съхрани в записа на CP директорията на крайния потребител, който използва оператора за директория APPCPASS. Операторът APPCPASS се препоръчва, ако искате да увеличите максимално защитата на паролата. Ако паролата не е въведена в записа на Директория за CMS комуникации, записът на директорията на потребителската система (VM) се търси за оператор APPCPASS.

APPCPASS оператор: VM осигурява оператора APPCPASS, за да увеличи максимално защитата на потребителския идентификатор и паролата, използвани от Средство за обработка на заявки при свързване към Сървър на приложения. APPCPASS е гъвкав в това, че ви позволява да съхраните информацията за защита по един от следните начини:

- **Потребителски идентификатор и парола:** В този случай етикетите :userid и :password в Директория за CMS комуникации трябва да са оставени празни.
- **Само потребителски идентификатор:** В този случай етикетът :userid в Директория за CMS комуникации трябва да е празен, а етикетът :password трябва да съдържа паролата на потребителя.
- **Само парола:** В този случай етикетът :password в Директория за CMS комуникации трябва да е празен, а етикетът :userid трябва да съдържа идентификатора на потребителя.

Фигура 33 на страница 118 илюстрира случая, при който потребителският идентификатор се съхранява в комуникационната директория на потребителя, а паролата в записа на VM директорията. В записа на комуникационната директория

потребителският идентификатор се установява на MTLSOU, а паролата не се определя. Паролата се съхранява в запис на VM директорията на потребителя.

```
 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
```

Фигура 33. Пример за запис в комуникационна директория без парола

Когато APPC/VM е инициатор за свързването между Средство за обработка на заявки и Сървър на приложения, като се използва защита на диалог от тип SECURITY=PGM, се четат стойностите на етикетите :userid и :password и се прехвърлят към Сървър на приложения. Ако един или и двата от тези етикета са празни, липсващата информация се търси в запис на VM директорията на потребителя. В този случай трябва да имате оператор APPCPASS в запис на VM директорията, както следва:

```
APPCPASS TORGATE MTLGATE MTLSOU Q6VBN8XP
```

Този оператор казва на APPC/VM, че потребителят (Средство за обработка на заявки), който заявява свързването през (локалния) AVS шлюз TORGATE, партниращата LU с име MTLGATE и потребителският идентификатор MTLSOU трябва да изпратят паролата Q6VBN8XP към Сървър на приложения. Потребителят се разпознава по тези две части на идентификацията на Сървър на приложения.

Поставянето на оператора APPCPASS във VM директорията не е задача на крайния потребител. Крайният потребител трябва да предаде заявка на VM системния програмист, който трябва от своя страна да направи това.

Допълнителна информация за защита на ниво диалог и оператора APPCPASS потърсете в *Планиране, администриране и използване на VM/ESA свързвания*.

Защита на мениджъра на базата данни

Като част от общата защита на разпределената база данни в DRDA, Средство за обработка на заявки може да играе роля при управлението кои крайни потребители може да отправят заявки към разпределена база данни. При DB2 за VM в защитата на разпределена база данни Средство за обработка на заявки може да участва в по три начина:

Изходящо преобразуване на името на потребителя

Можете да използвате изходящото преобразуване на името на потребителя, за да управлявате достъпа до определен Сървър на приложения на базата на идентичността на крайния потребител, който отправя заявката. DB2 за VM се опитва да преобразува името на крайния потребител, преди да изпрати заявката към отдалечената система. Все пак най–добрият начин е да накарате Сървър на приложения да изпълни проверка от типа откъде идва и входящо преобразуване, защото потребителите на VM Средство за обработка на заявки могат потенциално да заменят изходящото преобразуване с тяхната CMS потребителска комуникационна директория.

Предварителна обработка на приложение

Крайните потребители обработват предварително отдалечените приложения на определен Сървър на приложения, като използват командата на DB2 за VM SQLPREP EXEC или командата на помощната програма за услуги на базата данни (DBSU) RELOAD PACKAGE. DB2 за VM не ограничава използването на тези услуги. Когато краен потребител предварително обработи приложение, той става собственик на получения в резултат пакет.

Изпълнение на приложение

За да може краен потребител на DB2 за VM да изпълни отдалечено приложение, той трябва да има права на отдалечената система (Сървър на приложения) да изпълни отдалечения пакет, асоцииран към конкретното приложение. Създателят (собственикът) на пакета автоматично получава право да изпълни пакета. На другите крайни потребители може да се предоставят права за изпълнение на пакета с помощта на оператора на DB2 за VM GRANT EXECUTE. По този начин собственикът на приложение в разпределена база данни може да контролира използването на приложението на база на отделни потребители.

Подсистема за защита

Външната подсистема за защита на VM системите се осигурява от RACF или от еквивалентни продукти, които имат интерфейс, съвместим с RACF. DB2 за VM Средство за обработка на заявки няма директен интерфейс с външната подсистема за защита. Външната подсистема за защита не се използва за осигуряване на парола за защита на ниво диалог. Ако изберете да използвате защита на ниво диалог, VTAM се обръща към външната подсистема за защита, за да провери идентичността на името на отдалечената LU при проверката на партниращата LU.

Представяне на данни

Рикуестърът на приложения трябва да има подходящи стойности по подразбиране за CHARNAME и CCSID. Избирането на правилните стойности осигурява целостта на представянето на символните данни и намалява натоварването, свързано със CCSID конвертирането.

Например, ако вашият DB2 за VM рикуестър за приложения е генериран с кодова страница 37 и символен набор 697(CP/CS 37/697) за символи от тип Американски английски, тогава рикуестърът за приложения трябва да има стойност по подразбиране на CHARNAME – ENGLISH. Това е така, защото CP/CS 37/697 съответства на CCSID със стойност 37, което съответства на CHARNAME – ENGLISH.

Стойността по подразбиране за CHARNAME на току що инсталирана или мигрирана система е INTERNATIONAL, а CCSID е 500. Тази стойност вероятно *няма* да е правилна за вашата инсталация. За да представите текущите стойности по подразбиране на CCSID, използвайте следната команда:

```
SQLINIT QUERY
```

Подходящата стойност на CCSID за рикуестъра за приложения може да не се поддържа от таблиците за конвертиране на сървъра на приложения. В този случай можете да установите свързване, като изпълните едно от следните предложения:

- Оставете сървърът на приложения да обнови своята таблица за CCSID конвертиране, за да поддържа конвертирането между стойността по подразбиране на CCSID на рикуестъра за приложения и стойността по подразбиране на CCSID на сървъра на приложения (за подробности как да

разширите поддръжката на CCSID конвертиране се обърнете към ръководствата на сървъра на приложения).

- Променете стойността по подразбиране на CCSID на рикуестъра за приложения, така че да се поддържа от сървъра на приложения. Това може да доведе до проблеми с данните и трябва да сте наясно с последствията. Следва пример на такива последствия:

  Рикуестър за приложения използва контролер, дефиниран със CP/CS 37/697. Сървърът на приложения не поддържа конвертиране от CCSID 37, но поддържа конвертиране от CCSID 285 (това е CHARNAME UK–ENGLISH за SQL/DS).

  Ако рикуестърът за приложения се промени да използва по подразбиране UK–ENGLISH за CHARNAME (и 285 за CCSID), тогава целостта на данните няма да се обслужва. Например на местата, където сървърът на приложения има предвид символа за британска лира (ц), рикуестърът за приложения ще представи символа за долар ($). Освен това може да се различават и други символи.

  За да се промени стойността на CCSID на DB2 за VM рикуестър за приложения, трябва да определите параметъра CHARNAME на SQLINIT EXEC. По–подробна информация вижте в ръководството *Администриране на DB2 за VM*.

Подходящата стойност на CCSID за сървъра на приложения може да не се поддържа от таблиците за конвертиране на рикуестъра за приложения. В този случай можете да установите свързване, като изпълните едно от следните предложения:

- Обновете таблицата за конвертиране, използвана от рикуестъра за приложения, така че да поддържа конвертирането между стойностите по подразбиране на CCSID съответно на сървъра на приложения и на рикуестъра за приложения. Подробности за това как да обновите системната таблица SYSTEM.SYSSTRINGS вижте в *Администриране на DB2 за VM*. Тази таблица се използва, за да се създаде CMS файла ARISSTR MACRO, който се използва от рикуестъра за приложения при поддръжката на CCSID конвертирането.
- Оставете сървърът на приложения да промени своята стойност по подразбиране на CCSID. Това трябва да се направи, само ако е подходящо, като се отчете защо е избрана стойността по подразбиране на CCSID на сървъра на приложения. Тази стойност влияе върху всички рикуестъри за приложения, които се свързват към сървъра, терминала на оператора, който се използва със сървъра на приложения и данните, съхранени в таблиците върху сървъра на приложения.

Списък за активиране на DB2 за VM DRDA рикуестър за приложения

Следващият списък обобщава стъпките, които трябва да се изпълнят, за да се разрешат DRDA комуникации на DRDA рикуестър за приложения, като се приема, че вашата VM система е инсталирана с ACF/VTAM като метод за достъп и че са изпълнени VTAM дефинициите, необходими при комуникациите с отдалечените системи, като NCP дефиниции.

1. Дефинирайте локален AVS шлюз за VTAM
2. Инсталирайте DRDA поддръжка в DB2 за VM рикуестър за приложения с помощта на ARISDBMA.
3. Настройте CMS комуникационната директория и добавете необходимите оператори APPCPASS към VM директорията на VM машината на

приложението. Използвайте CMS командата SET COMDIR, за да разрешите комуникационната директория.

4. Стартирайте VTAM и AVS, така че VM приложенията да могат да комуникират отдалечено чрез SNA мрежата.
5. Използвайте SQLINIT и определете параметрите DBNAME, PROTOCOL и CHARNAME, за да посочите базата данни по подразбиране, използвания протокол и използваните стойности за CCSID.
6. Подгответе приложенията на отдалечения сървър.

Настройка на сървър на приложения във VM обкръжение

Поддръжката на сървър на приложения в DB2 за VM позволява на DB2 за VM да действа като сървър за DRDA рикуестъри за приложения. Към DB2 за VM сървър на приложения може да се свържат следните рикуестъри за приложения:

- DB2 за VM рикуестър
- DB2 Universal Database за OS/390 рикуестър
- OS/400 рикуестър
- DB2 за AIX рикуестър
- Към DB2 за VM сървър на приложения може да се свързва всеки рикуестър за приложения от фамилията DB2, включително DB2 CONNECT или друг продукт, който поддържа протоколите на DRDA рикуестър за приложения.

DB2 за VM сървърът на приложения позволява на всеки свързан към него рикуестър за приложения да има достъп до обектите на базата данни (като таблици), които се съхраняват локално на DB2 за VM сървъра на приложения. Рикуестърът за приложения трябва да създаде пакет за SQL операторите на приложението на DB2 за VM сървъра на приложения, преди да може да се установи свързването.

За да може DB2 за VM сървър на приложения да обработва заявки за разпределена база данни, трябва да предприемете следните стъпки:

1. Да дефинирате сървъра на приложения в локалната комуникационна подсистема.
2. Да осигурите необходимата защита.
3. Да осигурите представянето на данните.

Осигуряване на мрежова информация

Дефиниране на сървър на приложения

За да може Сървър на приложения да получава заявки за разпределена база данни, трябва да дефинирате Сървър на приложения в локалната комуникационна подсистема и да присвоите уникално име RDB_NAME.

Използвайте следните стъпки, за да дефинирате сървъра на приложения:

1. Дефинирайте DB2 за VM сървъра на приложения в SNA мрежата. След като изберете името на шлюз и RDB_NAME за DB2 за VM сървър на приложения, следвайте процедурите, описани в “Осигуряване на мрежова информация” на страница 109. Избраното от вас име RDB_NAME за DB2 за VM трябва да се достави на всички потребители (рикуестъри за приложения), които може да изискват свързване към DB2 за VM сървъра на приложения.

NETID се дефинира за VTAM като стартов параметър и всички разпределени заявки от Средство за обработка на заявки се насочват правилно. DB2 за VM Сървър на приложения не установява NETID.

DB2 за VM Сървър на приложения не определя кой шлюз да се използва при маршрутизиране на входящи заявки за разпределена база данни от Средство за обработка на заявки. Винаги Средство за обработка на заявки управлява това. В случая на DB2 за VM Средство за обработка на заявки това се определя от Директория за CMS комуникации с помощта на етикетите :luname и :tpn.

За да може DB2 за VM сървърът на приложения да поддържа възможността за разпределена единица работа, рикуестърът за приложения трябва да избере AVS шлюз, който е дефиниран във VTAM с помощта на параметъра SYNCLVL=SYNCPT. Проверете дали AVS шлюзът е дефиниран така, че да поддържа разпределени единици работа.

2. Създайте CRR сървър за възстановяване, който да се използва за управление на разпределени единици работа за DB2 за VM сървъри на приложения на тази VM система. За да направите това, изпълнете стъпките при зареждане след инсталиране на доставените от IBM сървъри и файловите пулове, описани в *Ръководство за инсталиране на VM/ESA*. Това включва дефиниране на CRR сървър (VMSERVR) и CRR файлов пул (VMSYSR). Проверете дали при стартирането на CRR сървъра за възстановяване е определено LUNAME, което е еднакво с името на AVS шлюз, за което е било определено SYNCLVL=SYNCPT.
3. Уверете се, че в CP директорията за сървъра на приложения има оператор IUCV *IDENT. Това определя сървъра като глобален ресурс.
4. Създайте запис във VTAM таблицата с имената на режимите за всяко име на режим, което е използвано в заявки на Средство за обработка на заявки. Тези записи описват характеристики на сесията, като размер на RU, стъпка и клас услуга за определения режим.
5. Дефинирайте максималния брой сесии за Средство за обработка на заявки, които могат да се свързват към DB2 за VM Сървър на приложения. Операторът VTAM APPL дефинира максималния брой сесии по подразбиране за всички партньори. За да установите уникални стойности по подразбиране за определен партньор, използвайте командата AGW CNOS от AVS виртуална машина, която работи на Сървър на приложения. (Максималният брой сесии обикновено се изисква от рикуестъра за приложения.)

   След като изберете размерите на RU, максималния брой сесии и стъпките, проверете какво е влиянието на тези стойности върху VTAM IOBUF пула.

Трансформиране името на сървъра до RESID: Идентификатор на ресурс (RESID) е VM терминът за име на транзакционна програма. Във VM обкръжението често се дефинира като буквено–числено име с дължина до 8 байта. Обикновено дефинирате RESID да е идентичен с името на сървъра, за да улесните администрирането. Фигура 34 показва примерен файл с имена RESID.

```
 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
```

Фигура 34. Пример за файл с имена RESID

В Фигура 33 на страница 118 вижте записа в комуникационната директория, който дефинира dbname и RESID (като TPN). Ако името на Сървър на приложения не може да е същото като RESID, тогава DB2 за VM сървърът на приложения използва файла RESID NAMES, за да осигури трансформирането. Ще ви е необходимо такова преобразуване, ако:

- Използвате RESID, различен от името на сървъра
- Използвате име на сървър, което е по–дълго от 8 байта
- Използвате RESID с 4–байтова шестнайсетично десетична стойност, както стойността на DRDA TPN по подразбиране – X'07F6C4C2'

По време на инсталирането по подразбиране се използва името на сървъра, определено в SQLDBINS EXEC като RESID. За да създадете запис за трансформиране във файла RESID NAMES, определете параметъра RESID в SQLDBINS.

Когато стартирате база данни с помощта на SQLSTART DB(server_name), DB2 за VM се обръща към съответния RESID и информира VM, че това е ресурсът, който VM трябва да управлява. Ако не се намери запис във файла RESID NAMES, DB2 за VM приема, че RESID е еднакъв с името на сървъра и казва това на VM. За допълнителна информация вижте ръководството *Администриране на DB2 за VM*.

Подготовка и стартиране на DB2 за VM сървър на приложения

Върху DB2 за VM сървъра на приложения може да не е инсталирана DRDA поддръжка. Изпълнете следните стъпки, за да подготвите DB2 за VM сървъра на приложения за DRDA комуникации:

1. Използвайте ARISDBMA, за да инсталирате DRDA поддръжката:
   - Използвайте "ARISDBMA DRDA(ARAS=Y)", ако инсталирате поддръжка за рикуестър и сървър.
   - Използвайте "ARISDBMA DRDA(AS=Y)", ако инсталирате поддръжка само на сървър.

   Подробности потърсете в ръководството *Администриране на VM/ESA система*.
2. След като използвате ARISDBMA, изградете отново ARISQLLD LOADLIB на DB2 за VM. Повече подробности ще намерите в главата *Използване на DRDA обкръжение* на ръководството *Администриране на DB2 за VM*.

Осигуряване на защита

Когато Средство за обработка на заявки насочи заявка за разпределена база данни към DB2 за VM сървър на приложения, трябва да се разгледат следните съображения, свързани със защитата:

- Входящо преобразуване на името на крайния потребител
- Параметри за защита на мрежата
- Защита на мениджъра на базата данни
- Защита, прилагана от външна подсистема за защита

Имена на крайни потребители

При SQL и LU 6.2 на крайните потребители се присвояват потребителски идентификатори с дължина от 1 до 8 байта. Тази стойност трябва да е уникална в рамките на определената операционна система, но може да не е уникална в цялата SNA мрежа. За да се отстранят конфликтите между имената, DB2 за VM може

допълнително да използва функцията за преобразуване на потребителски идентификатор, осигурена чрез AVS, но само при следните условия:

- DB2 за VM Сървър на приложения трябва да работи във VM/ESA обкръжение.
- Заявката за входящо свързване трябва да е насочена през AVS шлюз.
- Партниращият Средство за обработка на заявки трябва да използва защита на ниво диалог от типа SECURITY=SAME (също така известна като *вече проверена* в SNA терминологията).

Ако свързването се насочва към сървъра през AVS с помощта на опцията SECURITY=SAME, тогава се изисква преобразуване на AVS потребителски идентификатор. Командата AGW ADD USERID, използвана от AVS машината, трябва да осигурява защита при свързването на потребителите, които идват от определена отдалечена LU или AVS шлюз. Трябва да съществува преобразуване за всички входящи LU и потребителски идентификатори, които се свързват с помощта на защита SECURITY=SAME. Командата е гъвкава и можете да приемете всички потребителски идентификатори от определена LU или от всички отдалечени LU като цяло. Или да приемете само определено множество от потребителски идентификатори от определена LU.

Ако използвате командата AGW ADD USERID за оторизация на входящи (вече проверени) потребителски идентификатори на локална AVS машина, не се изпълнява проверка на валидността от хоста. Това означава, че не е задължително да съществуват оторизирани идентификатори на хоста, но свързването се приема.

Два начина да се промени текущата оторизация на AVS потребителски идентификатор са:

- Да спрете AVS, с помощта на командата AGW STOP. Така изцяло се нулира оторизацията на потребителските идентификатори.
- Да изтриете потребителски идентификатор с помощта на командата AGW DELETE USERID.

Например случаят с идентичните потребителски идентификатори в различни градове показва как AVS функцията за преобразуване може да разреши конфликта в имената. Да предположим, че съществува потребител с идентификатор JONES в системата Toronto и друг потребител със същия идентификатор в системата Montreal. Ако JONES от Montreal иска да получи достъп до данни в системата Toronto, следните действия в системата Toronto отстраняват конфликта в имената и не позволяват на JONES от Montreal да използва правата, предоставени на JONES от системата Toronto:

1. AVS операторът трябва да използва командата AGW ADD USERID, за да трансформира идентификатора на потребителя от Montreal до локален потребителски идентификатор. Например, ако операторът генерира `AGW ADD USERID MTLGATE JONES MONTJON`, потребителят от Montreal ще получи идентификатор MONTJON в системата Toronto. Ако всички други потребители на Montreal имат право да се свързват (свързване чрез отдалечен LU MTLGATE) и локално се разпознават чрез техните отдалечени потребителски идентификатори, тогава операторът трябва да използва командата `AGW ADD USERID MTLGATE * =`. Освен това тези AVS команди може да се добавят към AVS профила, така че да се изпълняват автоматично при стартирането на AVS.
2. В този случай администраторът трябва да използва командата на DB2 ЗА VM GRANT, за да предостави определени права специално за преобразувания потребителски идентификатор MONTJON.

Освен това тези действия може да се изпълнят върху системата Montreal, за да сте сигурни, че JONES в Toronto не използва правата, предоставени на JONES в Montreal, когато осъществява достъп до отдалечени данни върху системата Montreal.

AVS командите, които поддържат преобразуването на потребителски идентификатори са описани в *Планиране, администриране и използване на VM/ESA свързвания*.

Защита на мрежа

LU 6.2 осигурява три основни функции за защита на мрежата:

- Защита на ниво сесия
- Защита на ниво диалог
- Закодиране

В “Защита на мрежа” на страница 116 вижте изложението как да определите защита на ниво сесия за DB2 за VM. DB2 за VM Сървър на приложения използва защита на ниво сесия по същия начин, както и DB2 за VM Средство за обработка на заявки.

Средство за обработка на заявки може да изпраща вече проверен потребителски идентификатор (SECURITY=SAME) или потребителски идентификатор и парола (SECURITY=PGM). Ако се изпратят потребителски идентификатор и парола, тяхната валидност се проверява от CP, RACF или еквивалентна подсистема спрямо VM директорията на Сървър на приложения хоста. Ако не приключи успешно проверката за валидност, заявката за свързване се отхвърля; в противен случай се приема. Ако заявката съдържа само потребителски идентификатор, DB2 за VM приема заявката, без да проверява валидността на потребителския идентификатор.

Забележка: DB2 за VM не осигурява възможности за закодиране, защото VM/ESA не поддържа закодиране.

Защита на мениджъра на базата данни

DB2 за VM Сървър на приложения проверява дали потребителският идентификатор, получен от VM има права CONNECT за достъп до базата данни и след това отказва свързването, ако няма тези права.

Като собственик на ресурси в база данни, DB2 за VM Сървър на приложения контролира функциите за защита на SQL обектите, които се намират на DB2 за VM Сървър на приложения. Достъпът до обектите, управлявани от DB2 за VM, се контролира чрез множество от права, които се предоставят на потребителите от системния администратор на DB2 за VM или от собственика на определения обект. DB2 за VM Сървър на приложения управлява два класа обекти:

- **Пакети:** Отделните крайни потребители имат право да създават, заменят и изпълняват пакети с помощта на оператора на DB2 за VM GRANT. Когато краен потребител създаде пакет, той автоматично получава право да изпълнява или да заменя пакета. На другите крайни потребители трябва изрично да се предостави право да изпълняват пакета на DB2 за VM Сървър на приложения с помощта на оператора GRANT EXECUTE. Правото RUN може да се предостави на отделни крайни потребители или на PUBLIC, което означава, че всички крайни потребители могат да изпълняват пакета.

  Когато приложение се обработва предварително на DB2 за VM, пакетът съдържа SQL операторите, които се намират в приложната програма. Тези SQL оператори са класифицирани като:

  — **Статичен SQL:** Това означава, че SQL операторите и SQL обектите, които се съдържат в изразите, са известни в момента на предварителна обработка на приложението. Създателят на пакета трябва да има право да изпълнява всеки от статичните SQL оператори в пакета.

Когато на краен потребител се предоставя право да изпълни пакет, той автоматично получава право да изпълни всеки от статичните SQL оператори, които се съдържат в него. Затова крайните потребители не се нуждаят от таблица с права в DB2 за VM, ако пакетът съдържа само статични SQL оператори.

— **Динамичен SQL:** Описва SQL израз, който не е известен преди изпълнението на пакета. SQL изразът се изгражда от програмата и динамично се обработва предварително на DB2 за VM с помощта на оператора SQL PREPARE или оператора EXECUTE IMMEDIATE. Когато краен потребител изпълнява динамичен SQL израз, потребителят трябва да има таблицата с права на достъп, необходима за неговото изпълнение. Тъй като SQL изразът не е известен при създаването на пакета, крайният потребител не може автоматично да получи необходимите права като собственик на пакета.

- **SQL обекти:** Може да са таблици, производни таблици и синоними. На потребителите на DB2 за VM може да се предоставят различни нива с права на достъп, за да създават, изтриват, променят или четат отделни SQL обекти. Тези права са необходими, за да се обработят предварително статични SQL изрази или да се изпълнят динамични SQL изрази.

Подсистема за защита

Не е задължително използването на тази подсистема от DB2 за VM сървър на приложения. Ако сървърът на приложения трябва да провери идентичността на името на LU на рикуестър за приложения, VTAM се обръща към подсистемата за защита, за да провери валидността на партниращата LU. Решението дали да се провери валидността на партниращата LU се взима в зависимост от стойността, определена в параметъра VERIFY на оператора VTAM APPL за шлюза, който се използва от DB2 за VM сървъра на приложения при получаване на входящи заявки за разпределена база данни.

Освен това подсистемата за защита може да се извика от CP, за да провери валидността на потребителски идентификатор и парола, изпратени от рикуестър за приложения. Ако подсистемата за защита е RACF и нямате RACF системен профил, валидността се проверява от RACF. Ако имате RACF системен профил, например, RACFPROF, използвайте следните инструкции, за да използвате тази проверка за валидност от RACF:

```
RALTER VMXEVENT RACFPROF DELMEM (APPCPWVL/NOCTL

RALTER VMXEVENT RACFPROF ADDMEM (APPCPWVL/CTL

SETEVENT REFRESH RACFPROF
```

Представяне на данни

Трябва да изберете най–подходящите стойности по подразбиране за CHARNAME и CCSID за вашата инсталация. Като се използват най–подходящите стойности, се осигурява целостта при представянето на символните данни и се намалява натоварването, свързано с конвертиранията на база CCSID.

Например, ако към вашия DB2 за VM сървър на приложения се свързват само локални потребители, чиито терминални контролери са генерирани с кодова страница 37 и символен набор 697 (CP/CS 37/697) за символи от тип Американски английски, тогава сървърът на приложения трябва да има по подразбиране стойност ENGLISH за CHARNAME. Това е така, защото CP/CS 37/697 съответства на CCSID със стойност 37, което съответства на CHARNAME – ENGLISH.

За да отстраните ненужното CCSID конвертиране, изберете стойността по подразбиране на CCSID за сървъра да е същата като CCSID на рикуестърите за приложения, които най–често осъществяват достъп до сървъра на приложения.

Следва пример за това как тези две цели може да влязат в конфликт:

- Сървър на приложения има по–малко от пет локални рикуестъра за приложения (при VM рикуестърите за приложения параметърът за протокола ще се установи на SQL/DS) и много (около 100) рикуестъри, които се свързват към сървъра на приложения чрез DRDA протокол. Локалните рикуестъри за приложения имат контролери, които са дефинирани със CP/CS 37/697. Отдалечените рикуестъри за приложения използват CCSID 285.

  Ако по подразбиране стойността на CHARNAME за сървъра на приложения се установи на ENGLISH, това ще запази целостта на данните за локалните рикуестъри, но ще предизвика натоварване от CCSID конвертиране за всички отдалечени рикуестъри за приложения.

  Ако по подразбиране стойността на CHARNAME за сървъра на приложения се установи на UK–ENGLISH, ще се избегне натоварването от CCSID конвертирания за всички отдалечени рикуестъри за приложения, но ще доведе до проблеми с целостта на данните за локалните рикуестъри — определени символи няма да се представят правилно на локалните рикуестъри за приложения, например знака за британска лира ще се представя като долар.

За да представите текущата стойност на CCSID за системата, изпълнете запитване към таблицата SYSTEM.SYSOPTIONS. Стойността по подразбиране на CCSID за сървъра на приложения обикновено е стойността на CCSIDMIXED. Ако тази стойност е нула, тогава за системна стойност по подразбиране на CCSID се използва CCSIDSBCS. Стойностите на CHARNAME, CCSIDSBCS, CCSIDMIXED и CCSIDGRAPHIC в тази таблица се обновяват до стойностите, използвани като системни стойности по подразбиране при всяко стартиране на базата данни. Стойностите в тази таблица може и да не са системните стойности по подразбиране. Потребител с права на DBA може да ги промени, въпреки че не се препоръчва. За да промените стойността на CCSID на сървър на приложения, трябва да определите параметъра CHARNAME на SQLSTART EXEC при следващото стартиране на сървъра на приложения. По–подробна информация потърсете в ръководството *Администриране на VM/ESA система*.

При току що инсталирана база данни по подразбиране стойността на CHARNAME за сървъра на приложения е INTERNATIONAL, а на CCSID е 500. Тази стойност вероятно *няма* да е правилна за вашата система. Стойността по подразбиране на CHARNAME при мигрирана система е ENGLISH, а на CCSID е 37.

Списък за активиране на DB2 за VM DRDA сървър на приложения

В следващия списък са обобщени стъпките, които трябва да изпълните, за да са разрешени DRDA комуникации на DRDA сървър на приложения, като се приема, че вашата VM система е инсталирана с ACF/VTAM като метод за достъп и че са изпълнени VTAM дефинициите, необходими при комуникациите с отдалечените системи, като NCP дефиниции.

1. Дефинирайте локален AVS шлюз за VTAM.
2. Създайте CRR сървър за възстановяване. Проверете дали LUNAME, определено от CRR сървъра за възстановяване съответства на името на AVS шлюз, който може да обслужи диалозите SYNCLVL=SYNCPNT.

3. Инсталирайте DRDA поддръжка в DB2 за VM сървър на приложения с помощта на ARISDBMA.
4. Добавете оператор IUCV *IDENT към CP директорията на VM сървъра, така че да може да се идентифицира като глобален ресурс.
5. Дефинирайте в CP локалните потребителски идентификатори и пароли, които ще се използват от отдалечените рикуестъри за приложения. Ако е необходимо, дефинирайте трансформирането на отдалечените потребителски идентификатори до локални VM потребителски идентификатори с помощта на командата AVS AGW ADD USERID.
6. Създайте запис във VTAM таблицата с имената на режимите за всяко име на режим, което е използвано в заявки на рикуестъри за приложения.
7. Стартирайте VTAM и AVS, така че VM приложенията да могат да комуникират отдалечено чрез SNA мрежата.
8. Установете максималния брой сесии за всички партниращи системи, където се намират рикуестърите за приложения.
9. Стартирайте DB2 за VM сървъра на приложения с параметрите DBNAME, PROTOCOL и SYNCPNT. Когато е стартиран мениджърът на базата данни, уверете се, че се е идентифицирал като GLOBAL ресурс.
10. Подгответе приложенията на DB2 за VM сървъра на приложения.

DB2 за VSE Преглед

Във VSE/ESA работната среда DB2 за VSE осигурява функциите на сървър на приложения в DRDA обкръжение. Не се осигурява функцията на рикуестър за приложения. В този раздел са описани различните компоненти на DB2 за VSE и VSE, включени в работата на разпределена база данни. Тези компоненти позволяват на системата за управление на DB2 за VSE базата данни да комуникира с отдалечени DRDA рикуестъри за приложения в SNA мрежа.

CICS(ISC)
Компонентът за управление на междусистемни комуникации на системата за управление на информацията на клиентите (CICS – Customer Information Control System) осигурява SNA LU 6.2 (APPC) функциите на DB2 за VSE сървър на приложения.

CICS(SPM)
CICS компонентът за управление на синхронизацията е неделима част от DB2 за VSE поддръжката на DRDA разпределена единица работа. Действа като участник, който определя точката на синхронизация и отговаря за координирането на действията при двуфазовия протокол за записване на промените на VSE/ESA система.

CICS(TRUE)
CICS TRUE (task–related user exit–изход за потребителя в зависимост от задачата) е интерфейс, използван от AXE транзакцията за интерфейс със CICS мениджъра за синхронизация.

ACF/VTAM
CICS(ISC) използва VTAM за VSE, за да установи или свърже сесии LU–към–LU с отдалечени системи. DB2 за VSE използва LU 6.2 обикновени диалози през тези сесии, за да комуникира с отдалечени DRDA рикуестъри за приложения.

AXE APPC–XPCC–Exchange (AXE) транзакцията е CICS транзакция, активирана от отдалечения DRDA рикуестър за приложения. Насочва DRDA потока данни между отдалечения рикуестър за приложения и DB2 за VSE сървъра

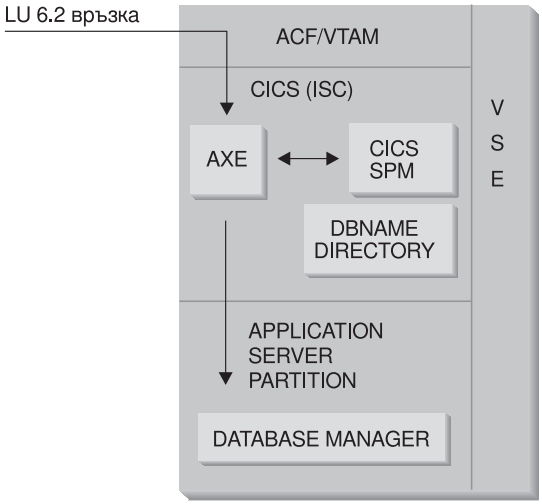
на приложения, като използва CICS LU 6.2 поддръжката и VSE XPCC функциите.

DBNAME директория
DBNAME (име на база данни) директорията преобразува входящите заявки за заделяне на диалог до предварително определен сървър на приложения, идентифициран според входящото TPN. Повече подробности вижте в *Ръководство за SQL/DS системно администриране за VSE*.

XPCC XPCC (Cross Partition Communication Control–Междудялово комуникационно управление) is е VSE макро интерфейс, който осигурява трансфер на данни между VSE дялове.

Пример за комуникационни потоци на сървър на приложения

Фигура 35 показва каква роля играе всеки компонент при установяването на комуникации между DB2 за VSE Сървър на приложения и отдалечен Средство за обработка на заявки.



Фигура 35. Получаване на достъп до сървър на приложения

Рикуестърът на приложения подава функцията APPC ALLOCATE със специфично име на LU и име на транзакционна програма (TPN), за да установи LU 6.2 диалог със сървъра на приложения. Името на LU се използва за насочване на заявката ALLOCATE през VTAM до CICS. Когато получи ALLOCATE, CICS проверява дали е дефинирана AXE транзакция с тази стойност на TPN и изпълнява CICS регистриране. Ако защитата на ниво диалог за CICS свързването е VERIFY, се очаква да се получат от рикуестъра за приложения потребителски идентификатор и парола и те се използват при регистрирането. CICS таблицата за регистриране (DFHSNT) трябва да се обнови с този потребителски идентификатор и парола, така че да се приеме свързването. Ако нивото на защита е IDENTIFY, се изисква само потребителски идентификатор и CICS се доверява на проверката на системата за защита на отдалечената система. Ако проверката на системата за защита приключи успешно, CICS стартира AXE транзакцията, за да насочва заявките и отговорите между рикуестъра за приложения и сървъра на приложения. За използваната стойност на TPN от рикуестъра за приложения трябва също да има запис, дефиниран в директорията DBNAME на DB2 за VSE, който да сочи към работещия DB2 за VSE сървър в рамките на VSE системата.

Ако рикуестърът за приложения иска да се възползва от поддръжката на разпределена единица работа, той определя SYNCLVL за SYNCPT във функцията APPC ALLOCATE. Когато се стартира AXE транзакцията, тя изпраща запитване към CICS, за да определи SYNCLVL на диалога. Ако е SYNCPT, изпълнява следното:

- При необходимост AXE транзакцията позволява поддръжка на TRUE, така че да може да комуникира със CICS мениджър за синхронизация.
- Регистрира логическа единица работа със CICS мениджъра за синхронизация.

Ограничения

За разлика от VM системите DB2 за VSE сървърът на приложения приема DRDA потоци от отдалечени рикуестъри за приложения. Собствени протоколи не се поддържат. В резултат VM рикуестъри за приложения нямат достъп до VSE сървър с PROTOCOL=SQLDS.

DB2 за VSE DRDA сървър не може да насочи заявки от отдалечени рикуестъри за приложения към DB2 за VM сървър с помощта на VSE достъп на гост. Такива заявки трябва да се изпращат директно към DB2 за VM DRDA сървър.

Параметри за стартиране на сървър на приложения

Параметърът RMTUSERS

Администраторът на база данни може да определи параметърът RMTUSERS при стартиране на сървъра на приложения, за да установи максималния брой на отдалечени рикуестъри за приложения, които могат да се свързват към сървъра. Това е подобно на стойността MAXCONN във VM директорията на DB2 за VM сървъра на база данни. Този параметър помага да се балансира натоварването между локалните и отдалечени обработки.

Когато стойността на RMTUSERS е по–голяма от броя на наличните DB2 за VSE агенти (дефинирани от NCUSER), някои отдалечени потребители трябва да чакат агент на DB2 за VSE да обслужи тяхната заявка. Обикновено агент на DB2 за VSE се присвоява повторно на чакащия потребител в края на логическа единица работа (LUW – logical unit of work). Сървърът на приложения DB2 за VSE поддържа права на достъп, като по този начин позволява на отдалечен потребител да запази агент на DB2 за VSE за няколко LUW до края на диалога.

Параметърът SYNCPNT

Този параметър определя дали да се използва мениджър за синхронизация (SPM), за да координира дейности като DRDA–2 многосайтово четене, многосайтово записване на разпределена единица работа.

Ако е въведено Y, при възможност сървърът ще използва мениджър за синхронизация, за да координира двуфазови записвания на промени и синхронизиране. Ако е въведено N, сървърът за приложения няма да използва SPM, за да изпълни двуфазови записвания на промените. Ако е въведено N, сървърът на приложения се ограничава до многосайтово четене, записване в една система на разпределени единици работа и може да е единствената записваща страна. Ако е въведено Y, но сървърът за приложения открие, че не е достъпен мениджър за синхронизация, тогава сървърът работи така, като че ли е въведено N.

По подразбиране е SYNCPNT=Y, когато RMTUSERS е по–голямо от нула. Когато RMTUSERS=0, параметърът SYNCPNT се установява на N.

Настройка на сървър на приложения във VSE обкръжение

Поддръжката на сървър на приложения за DB2 за VSE позволява на DB2 за VSE да действа като сървър за DRDA рикуестъри за приложения. Към DB2 за VSE сървър на приложения може да се свържат следните рикуестъри за приложения:

- DB2 за VM рикуестър
- DB2 Universal Database за OS/390 рикуестър
- DB2 рикуестър
- OS/400 рикуестър
- Към DB2 за VM сървър на приложения може да се свързва всеки рикуестър за приложения от фамилията DB2, включително DB2 CONNECT или друг продукт, който поддържа протоколите на DRDA рикуестър за приложения.

Осигуряване на мрежова информация

За да установите мрежово свързване към VSE сървър на приложения, са необходими следните стъпки:

1. Да установите CICS LU 6.2 сесии към отдалечените системи
2. Да дефинирате Сървър на приложения

Установяване на CICS LU 6.2 сесии

DB2 за VSE сървър на приложения комуникира със своите рикуестъри за приложения чрез CICS LU 6.2 връзки. CICS компонентът, използван за тази цел, трябва да има LU 6.2 връзки към отдалечените системи с рикуестърите за приложения. *Ръководството за CICS/VSE комуникации* съдържа подробности за дефиниране и установяване на CICS LU 6.2 връзки с отдалечени системи.

Инсталиране и дефиниране на ресурси на CICS за LU 6.2 комуникации

1. Инсталирайте модулите, необходими за ISC.

   Трябва да включите следните модули във вашата система с помощта на SIT или инициализационни замени:

   - EXEC интерфейсни програми (определете EXEC=YES или оставете по подразбиране).
   - Програми за междусистемни комуникации (определете ISC=YES).
   - Програма за терминално управление, генерирана от DFHSG PROGRAM=TCP. Изисква се версия, която определя ACCMETH=VTAM, CHNASSY=YES и VTAMDEV=LUTYPE6.
2. Инсталирайте поддръжка на CICS повторно синхронизиране при рестарт

   Ако не е активирана поддръжката на CICS повторното синхронизиране при рестарт при инсталирането на CICS системата, трябва да обновите следните CICS таблици и да активирате тази възможност:

DFHJCT Журнална управляваща таблица

Използва се за журнал на CICS системата и трябва да се дефинира в DFHJCT, като се определи JFILEID=SYSTEM в макроса DFHJCT TYPE=ENTRY.

DFHPCT Програмна управляваща таблица

За да генерирате DFHPCT запис за използване на възможността на CICS за повторно синхронизиране при рестарт, въведете:

```
DFHPCT TYPE=GROUP,FN=RMI
```

DFHPPT Таблица за обработка на програми

За да генерирате DFHPPT запис за използване на възможността на CICS за повторно синхронизиране при рестарт, въведете:

```
DFHPPT TYPE=GROUP,FN=RMI
```

DFHSIT Таблица за инициализация на системата

Макросът DFHSIT трябва да включва параметъра JCT. Въведете JCT=YES или JCT=(jj<,....>), където jj е стойността на параметъра SUFFIX, определена в макроса DFHJCT TYPE=INITIAL, дефиниращ множеството данни в CICS системния журнал.

3. Дефинирайте CICS във VTAM за VSE.

   За да поддържа LU 6.2 свързвания, CICS трябва да се дефинира във VTAM за VSE като основен възел на VTAM приложение. Името на основния възел на приложения в оператора VTAM APPL е APPLID за CICS частта, определена в SIT от параметъра APPLID. Това е името на LU, използвано от VTAM (и следователно използвано от CICS комуникационните партньори), за да идентифицират CICS системата.

   Вижте Фигура 36.

```
         VBUILD  TYPE=APPL
*************************************************************************
*                                                                       *
*    LU дефиниция за VSE SQL/DS системата Toronto                       *
*                                                                       *
*************************************************************************
VSEGATE  APPL  ACBNAME=VSEGATE,
               AUTH=(ACQ,SPO,VPACE),
               APPC=NO,
               SONSCIP=YES,
               ESA=30
               MODTAB=RDBMODES,
               PARSESS=YES,
               VPACING=0
```

Фигура 36. Примерна VTAM APPL дефиниция за CICS

AUTH=(ACQ,SPO,VPACE)

ACQ позволява на CICS да използва LU 6.2 сесии.

SPO позволява на CICS да подава командата MODIFY vtamname USERVAR.

VPACE позволява разделяне на стъпки на междусистемните потоци.

ESA=30

Тази опция определя броя на единиците с мрежови адреси, с които CICS може да установи сесии. Броят трябва да включва общия брой паралелни сесии за тази CICS система.

PARSESS=YES

Определя поддръжка на LUTYPE6 паралелни сесии.

SONSCIP=YES

Определя поддръжка на SON (session outage notification). В определени случаи SON позволява на CICS да възстанови проблемна сесия, без да е необходима намесата на оператор.

APPC=NO

Това е необходимо, за да може CICS да използва VTAM макроси. CICS не подава APPCCMD макро инструкции.

Забележка: SYNCLVL=SYNCPT не е необходимо, защото е определено APPC=NO. CICS управлява всички дейности за SYNCPT точка на синхронизация за разпределена единица работа.

4. Дефинирайте връзки към отдалечените системи с помощта на LU 6.2 протокол.
   a. Дефинирайте всички отдалечени LU за CICS.

      Дефинирайте всички отдалечени LU с помощта на командата CEDA DEFINE CONNECTION чрез RDO (resource definition online):

      - Определете името на отдалечена LU в параметъра NETNAME.
      - Определете PROTOCOL=APPC, за да сте сигурни, че се използват LU6.2 протоколи.
      - Определете AUTOCONNECT=YES и INSERVICE=YES, така че автоматично при инсталирането да се задейства свързването и така сесиите автоматично да се придобиват.
      - Определете защитата на ниво диалог с помощта на параметъра ATTACHSEC. ATTACHSEC=IDENTIFY е минималното ниво на защита, изисквано от DRDA.
      - Определете защитата на ниво сесия с помощта на параметъра BINDPASSWORD. По подразбиране се приема без защита на ниво сесия.

      Повече подробности за защитата на ниво сесия и диалог потърсете в “Осигуряване на защита” на страница 136.

   b. Дефинирайте групи от LU 6.2 сесии с отдалечената система.

      За всяко свързване, дефинирано горе, определете групи от паралелни сесии за всяка връзка към отдалечената LU с помощта на командата CEDA DEFINE SESSIONS:

      - Въведете името на диалога (дефинирано горе) в параметъра CONNECTION.
      - Определете записа във VTAM таблицата на режимите с параметъра MODENAME.
      - Използвайте параметъра MAXIMUM, за да определите:
        — Максималния брой сесии
        — Максималния брой сесии, които се поддържат като победители.

Определете стойностите, използвани от комуникационния софтуер на DRDA рикуестър за приложения, например IBM комуникационен сървър за OS/2.

Отбележете, че ако дефинирате SENDSize и RECEIVESize с по–големи стойности, може да се подобри скоростта на предаване на данните, обаче ще е необходимо повече виртуално място за съхранение в мрежата. 4 килобайта е размерът, който се поддържа от всички нива на SNA мрежовата поддръжка. Следователно, когато определяте DRDA сървър, определете размерите на буферите за изпращане и получаване на 4 килобайта. Когато успешно могат да се правят свързвания от отдалечени потребители, настройте тези параметри, за да определите оптималната стойност.

c. Дефинирайте потребителските идентификатори и пароли в CICS

   Дефинирайте всички потребители в CICS таблицата за регистриране (DFHSNT). Можете да тествате валидността на потребителски идентификатор, като изпълните CESN влизане в системата от CICS терминал. Локалното регистриране трябва да е успешно.

d. Дефинирайте модулите за зареждане (фази) в CICS с помощта на командата CEDA DEFINE PROGRAM:
   1) ARICAXED – AXE транзакцията
   2) ARICDIRD – DBNAME директорията и процедура за търсене
   3) ARICDAXD – DAXP и DAXT указател за транзакции
   4) ARICDEBD – Указател за разрешаване на CICS TRUE поддръжка
   5) ARICDRAD – Самият CICS TRUE
   6) ARICDR2 – DR2DFLT управляващ блок

   За всеки от горните, трябва да се определи опцията LANGUAGE=ASSEMBLER.

e. За всяко име TPN, определено от рикуестъра за приложения, дефинирайте AXE транзакция с помощта на командата CEDA DEFINE TRANSACTION:
   - Използвайте параметъра TRANSACTION, за да определите TPN
   - Въведете PROGRAM=ARICAXED, за да определите фазата
   - Използвайте параметъра XTRANID, за да определите второ шестнайсетично десетично име на транзакция.

   Освен това в този момент дефинирайте DAXP и DAXT транзакциите, като определите PROGRAM=ARICDAXD.

Примерни дефиниции: Обърнете се към *Ръководството за DRDA свързвания* за примерни дефиниции.

Дефиниране на сървър на приложения

1. Обновете DB2 за VSE директорията DBNAME.

   Добавете запис към директорията DBNAME за всяка транзакция, дефинирана горе, с помощта на командата CEDA DEFINE TRANSACTION. Когато са установени LU 6.2 сесиите, отдалечен рикуестър за приложения може да стартира диалог с DB2 за VSE Сървър на приложения. Изпълнява това, като заделя LU 6.2 диалог със Сървър на приложения и определя TPN (transaction program name – име на транзакционна програма). Въведената стойност за TPN трябва да е CICS идентификатора на транзакция за AXE транзакцията, отговорна за насочване на заявките към и от DB2 за VSE сървъра. TPN трябва да е в DB2 за VSE директорията DBNAME, за да се преобразува до DB2 за

VSE сървъра, до който има достъп рикуестъра за приложения. Администраторът на DB2 за VSE базата данни отговаря за обновяването на директорията DBNAME и информирането на отдалечените потребители за преобразуването TPN–до–сървър.

TPN и съответното име на сървър (име на база данни, както е дефинирано в директорията DBNAME) трябва да се идентифицирани на рикуестъра за приложения:

- Рикуестърът за приложения използва TPN, за да създаде AXE транзакция за маршрутизиране.
- Рикуестърът за приложения цитира името на сървъра в първоначалния DRDA поток като име на база данни приемник. DB2 за VSE сървърът използва това име на сървър, за да провери дали рикуестърът за приложения осъществява достъп до правилния сървър. При липса на съответствие с името на сървъра, Средство за обработка на заявки отказва достъп до сървъра и Средство за обработка на заявки приключва диалога.

2. Използвайте процедурата ARISBDID, за да изградите и асемблирате директорията DBNAME (member ARISDIRD.A).

За допълнителни подробности вижте ръководството *Администриране на DB2 за VSE система*.

Подготовка и стартиране на DB2 за VSE сървър на приложения

1. AXE транзакцията поддържа журнал за грешки, който е CICS временна опашка за съхранение с име ARIAXELG. Този журнал за грешки съдържа съобщенията, които отразяват комуникационни проблеми и аварийно прекъсване на DRDA сесии. Дефинирайте този журнал като "възстановим" с помощта на CICS TST.
2. Изпълнете процедурата ARIS342D, за да инсталирате поддръжка на DRDA Сървър на приложения.
3. Ако е необходимо, подайте DAXP транзакцията, за да определите парола и език по подразбиране, които ще се използват, когато се активира поддръжка на CICS TRUE за определен сървър. За допълнителни подробности вижте ръководството *Използване на DB2 за VSE*.
4. Стартирайте DB2 за VSE с параметрите DBNAME, RMTUSERS и SYNCPNT:
   - Използваната стойност за DBNAME трябва да е дефинирана в директорията DBNAME.
   - Параметърът RMTUSERS трябва да е различен от нула.
   - Определете SYNCPNT=Y, за да активирате поддръжката за разпределена единица работа.
5. Всички отдалечени потребители трябва да са оторизирани от DB2 за VSE сървъра с различни права. За допълнителни подробности се обърнете към *Администриране на DB2 за VSE база данни*.

Откриване на проблеми:

- Ако рикуестърът на приложения успее да достигне партниращата CICS с валидна стойност на TPN (TPN се дефинира в директорията DBNAME), се стартира AXE транзакция. Броячът за използвани програми ARICAXED се увеличава с единица (проверява се с подаване на CEMT I PR(ARICAXED)).
- За да сте сигурни, че отдалеченият потребителски идентификатор е въведен в CICS таблицата за регистриране, изпълнете локално свързване с помощта на CESN транзакцията, като използвате

потребителския идентификатор и парола на отдалечения потребител. Локалното регистриране трябва да е успешно.

- Когато работи DB2 за VSE сървъра и приложение за първи път изпълни действия, свързани с DRDA–2 разпределена единица работа, на сървъра ще се активира автоматично поддръжката на TRUE. Потърсете съобщение ARI0187I, което посочва, че поддръжката на TRUE успешно е активирана. Обаче ако се появи съобщение ARI0190E, което показва, че е възникнала грешка при активирането на TRUE, потърсете предишни съобщения за грешка на конзолата.
- Ако вашата DRDA приложна програма получи код на състояние X'08063426' или X'FFFE0101', може да е признак, че CICS изпитва недостиг от сесии. CICS може да изпита недостиг от сесии, ако всички сесии се използват или са предвидени за UNBIND, който не е приключил. Може да се предизвика липса на сесии, ако има много едновременни входящи транзакции, които са къси по продължителност. В този случай увеличете броя на сесиите, определен в параметъра CEDA DEFINE SESSIONS MAXIMUM, като вземете предвид сесиите, които са предназначени за UNBIND, но UNBIND не е приключил.

Осигуряване на защита

DB2 за VSE сървърът на приложения зависи от CICS при защитата на междусистемните комуникации. CICS предлага редица нива на защита:

- Защита при свързване на програми

  CICS реализация на проверка на валидност на LU–до–LU на ниво SNA LU 6.2 сесия. Реализацията на защитата по време на свързване на програми не е задължителна в LU 6.2 архитектурата. От страната на сървъра на приложения може да се активира, като се въведе BINDPASSWORD в командата CEDA DEFINE CONNECTION, когато се дефинира свързването на Средство за обработка на заявки. От страната на рикуестъра за приложения партниращата LU, която служи като Средство за обработка на заявки трябва също да поддържа защита по време на свързване на програми и да използва същата парола за проверка на партниращата LU.

  Можете да използвате защита на ниво свързване на програми, за да не позволите на неоторизирани отдалечени системи да установяват (свързват) сесии със CICS.

- Защита на връзка

  Защитата на връзка може да се използва, за да се ограничи отдалечена система (и резидентния DRDA рикуестър на приложения) да се свързва само по отношение на определено множество от AXE транзакции.

  Например, можете да дефинирате две AXE транзакции: AXE2 с ключ за защита 2 и AXE3 с ключ за защита 3. На рикуестъри за приложения от отдалечена система може да се присвои оперативна защита 3 (например с помощта на параметъра OPERSECURITY в командата CEDA DEFINE SESSION), като им позволи да се свързват само към AXE3. AXE3 може да няма привилегирован достъп до сървъра, докато AXE2 може да има. Обърнете се към *Администриране на DB2 за VSE система* за описание на правата на достъп за сървър на приложения от отдалечени рикуестъри за приложения.

Обърнете се към *Ръководство за CICS комуникации* за информация как да активирате защита на връзка.

- Защита на потребител

  CICS реализацията на защита на ниво SNA LU 6.2 диалог осигурява проверка на крайния потребител.

  Защитата на потребител проверява валидността на потребителски идентификатор спрямо CICS таблица на регистрации (DFHSNT), преди да приеме заявка за стартиране на диалог. Например, DRDA рикуестъри за приложения, които не са дефинирани в CICS таблицата на регистрациите, не могат да се свързват с AXE транзакция, за да стартират диалог с DB2 за VSE сървър. Защитата на ниво потребител за отдалечена система може да се избере чрез командата CEDA DEFINE CONNECTION, като се използва параметърът ATTACHSEC. Трите нива за защита при свързване на приложения са:

  — LOCAL. Не се поддържа от DRDA.

  — IDENTIFY. Еквивалентно на SECURITY=SAME (или вече проверена защита) в терминологията на LU 6.2. При това ниво на защита CICS "се доверява" на отдалечената система за проверката на нейните потребители, като им позволява да използват диалог на DB2 за VSE сървъра. Изисква се само потребителски идентификатор за процеса на регистрация на CICS. Обаче ако се предаде и парола, CICS изпълнява регистрирането заедно с паролата.

  — VERIFY. Еквивалент на SECURITY=PGM в терминологията на LU 6.2. При това ниво на защита CICS очаква отдалечената система да изпрати потребителски идентификатор и парола, когато заявява диалог и отхвърля свързването, ако не се предостави парола.

- Задължително закодиране на ниво SNA LU 6.2 сесия. Не се поддържа.

Тъй като сървърът на приложения е отговорен за управлението на ресурсите на базата данни, той определя кои механизми за защита на мрежата трябва да се осигурят от рикуестъра за приложения. Например, при DB2 за VM рикуестър за приложения трябва да запишете изискванията към защитата на ниво диалог на сървъра на приложения в комуникационната директория на рикуестъра за приложения, като определите подходяща стойност в етикет :security, както в Фигура 37 на страница 138:

```
:nick.VSE1     :tpn.TOR3
               :luname.TORGATE VSEGATE
               :modename.IBMRDB
               :security.PGM
               :userid.SALESMGR
               :password.PROFIT
               :dbname.TORONTO3



Където:TOR3    - ID на AXE транзакция, преобразуван до БД TORONTO3.
       TORGATE - VM/APPC шлюз.
       VSEGATE - APPLID на CICS/VSE дял, който служи като шлюз
                 за TORONTO3.
       SALESMGR/PROFIT - USERID/PASSWORD дефинирани в DFHSNT на
                         VSEGATE и оторизирани в TORONTO3
       TORONTO3 - Името, определено в DBNAME стартовия параметър, когато
                  DB2 за VSE сървър на приложения е стартиран (или
                  името на базата данни по подразбиране, определена от
                  директорията DBNAME, ако е пропуснато DBNAME при стартиране).
```

Фигура 37. Пример за запис в CMS комуникационна директория

Защита на мениджъра на базата данни

Не се поддържа преобразуване на потребителския идентификатор от VSE сървър на приложения. CICS използва директно предадения от рикуестъра потребителски идентификатор.

След като се стартира от рикуестъра за приложения, AXE транзакцията извлича потребителския идентификатор от CICS и го предава на DB2 за VSE сървър. За да настроите необходимите права на потребител по отношение ресурсите на базата данни, трябва да обновите потребителския идентификатор в каталога SYSTEM.SYSUSERAUTH на DB2 за VSE.

DB2 за VSE сървърът на приложения проверява дали потребителският идентификатор, получен от CICS, има права CONNECT за достъп до базата данни и отхвърля свързването, ако няма тези права.

Като собственик на ресурси в база данни, DB2 за VSE Сървър на приложения контролира функциите за защита на SQL обектите, които се намират на DB2 за VSE Сървър на приложения. Достъпът до обектите, управлявани от DB2 за VSE се контролира чрез множество от права, които се предоставят на потребителите от системния администратор на DB2 за VSE или от собственика на определения обект. DB2 за VSE Сървър на приложения управлява два класа обекти:

- **Пакети:** Отделните крайни потребители имат право да създават, заменят и изпълняват пакети с помощта на оператора на DB2 за VSE GRANT. Когато краен потребител създаде пакет, той автоматично получава право да изпълнява или да заменя пакета. На другите крайни потребители трябва изрично да се предостави право да изпълнят пакета на DB2 за VSE Сървър на приложения с помощта на оператора GRANT EXECUTE. Правото RUN може да се предостави на отделни крайни потребители или на PUBLIC, което означава, че всички крайни потребители могат да изпълняват пакета.

  Когато приложение се обработва предварително на DB2 за VSE, пакетът съдържа SQL операторите, които се намират в приложната програма. Тези SQL оператори са класифицирани като:

— **Статичен SQL:** Това означава, че SQL операторите и SQL обектите, които се съдържат в изразите са известни в момента на предварителна обработка на приложението. Създателят на пакета трябва да има право да изпълнява всеки от статичните SQL оператори в пакета.

Когато на краен потребител се предоставя право да изпълни пакет, той автоматично получава право да изпълни всеки от статичните SQL оператори, които се съдържат в него. Затова крайните потребители не се нуждаят от таблица с права в DB2 за VSE, ако пакетът съдържа само статични SQL оператори.

— **Динамичен SQL:** Описва SQL израз, който не е известен преди изпълнението на пакета. SQL изразът се изгражда от програмата и динамично се обработва предварително на DB2 за VSE с помощта на оператора SQL PREPARE или оператора EXECUTE IMMEDIATE. Когато краен потребител изпълнява динамичен SQL израз, потребителят трябва да има таблица с права на достъп, необходима за изпълнението му. Тъй като SQL изразът не е известен при създаването на пакета, крайният потребител не може автоматично да получи необходимите права като собственик на пакета.

- **SQL обекти:** Това може да са таблици, производни таблици и синоними. На потребителите на DB2 за VSE може да се предоставят различни нива с права на достъп, за да създават, изтриват, променят или четат отделни SQL обекти. Тези права са необходими, за да се обработят предварително статични SQL изрази или да се изпълнят динамични SQL изрази.

Представяне на данни

Вижте “Представяне на данни” на страница 126.

Списък за активиране на DB2 за VSE DRDA сървър на приложения

В следващия списък са обобщени стъпките, необходими за активиране на DRDA Сървър на приложения, като се приема, че вашата VSE система е инсталирана с ACF/VTAM като метод за достъп и че са изпълнени VTAM дефинициите, необходими при комуникациите с отдалечените системи, като NCP дефиниции.

1. Инсталирайте CICS ISC поддръжка и поддръжката за рестартиране на синхронизацията.
2. Дефинирайте CICS във VTAM за VSE.
3. Съставете таблицата VTAM LOGMODE със записа IBMRDB.
4. Съставете CICS таблица за регистрации с дефинирани всички отдалечени потребителски идентификатори и пароли.
5. Стартирайте CICS с правилната SIT информация:
   - ISC=YES
   - TST=YES, ARIAXELG дефинирано като RECOVERABLE в DFHTST и асемблирано
   - APPLID=LU име (както е дефинирано в оператора VTAM APPL)
6. Дефинирайте отдалечените системи в CICS (RDO може да се използва):
   - CEDA DEF CONNECTION
   - CEDA DEF SESSION
   - CEDA DEF PROGRAM
   - CEDA DEF TRANSACTION

Тези оператори трябва да имат всички дефиниции под една група, например с име IBMG. Инсталирайте групата с: CEDA INSTALL GROUP(IBMG).

7. Обновете директорията DBNAME (ARISDIRD.A):
   - Дефинирайте на CICS всички TPN, изброени в директорията. Не могат да се използват TPN, които не са дефинирани на CICS.
   - Дефинирайте всеки DB2 за VSE DRDA сървър на приложения в директорията с валидна стойност за TPN.
8. Изпълнете процедурата ARISBDID, за да сглобите обновената директорията DBNAME.
9. Подгответе DB2 за VSE сървъра:
   - Изпълнете процедурата ARIS342D, за да инсталирате DRDA поддръжката.
   - Ако активни DB2 за VSE приложения (например ISQL) се изпълняват от CICS дял, предоставете права за планиране на CICS APPLID, определен в CICS SIT таблицата.
   - Предоставете права на всички отдалечени потребители.
10. Ако е необходимо, изпълнете DAXP CICS транзакцията.
11. Стартирайте DB2 за VSE с правилния параметър RMTUSERS и евентуално с параметрите DBNAME и SYNCPNT.
12. Подгответе приложенията на VSE DRDA Сървър на приложения.

Приложение A. Най–разпространени проблеми при свързване

В това приложение са представени най–честите симптоми за проблемите при свързване, които се срещат на DB2 Connect от DB2 UDB работна станция, когато използва DB2 Connect и DB2 UDB DRDA–AS:

- "Най–чести проблеми в DB2 Connect" и
- "Най–разпространени проблеми с DB2 UDB DRDA AS" на страница 149.

Тази информация може да ви помогне и в процеса на анализиране на проблема. Също така вижте: *Справочник на съобщенията*, *Ръководство за отстраняване на проблеми* и *DB2 Connect: Ръководство на потребителя*.

Най–чести проблеми в DB2 Connect

В този раздел са представени най–честите симптоми за проблемите при свързване, които се срещат при използването на DB2 Connect. При всеки случаи разполагате с:

- Комбинация от номер на съобщение и код на връщане (или специфичен за протокола код на връщане), свързан с това съобщение. Всяка комбинация от съобщение и код на връщане има отделно заглавие, като заглавията са подредени по номера на съобщението и след това по кода на връщане.
- Осигурява се `симптом`, обикновено във вид на списък с примерни съобщения.
- Предлага се `решение`, което посочва вероятната причина за грешката. При някои случаи се предлага повече от едно възможно решение.

Забележки:

1. Обърнете се към ръководството `Бърз старт` за продукт и най–новите Последни бележки, за да научите най–новата информация за препоръчваните пакети с корекции на софтуера.
2. За комбинациите от съобщения и кодове на връщане, специфични за APPC комуникациите, може да се посочи и SNA код на състояние. Засега всяка информация за SNA кодове на състоянието, свързана с определено съобщение, трябва да се получи от SNA подсистема.

   Понякога SNA кодовете на състояние може да се прегледат, като се разгледат системните журнали. Дали този случай се отнася за вас, зависи от използваната SNA подсистема, а в някои ситуации може да се наложи да пресъздадете проблема, като активирате SNA трасирането, за да получите информация за кодовете на състояние.
3. Терминът `шлюз` се отнася за DB2 Connect Enterprise Edition.

SQL0965 или SQL0969

Симптом

Съобщенията SQL0965 и SQL0969 може да се генерират с редица различни кодове на връщане от DB2 Universal Database за AS/400, DB2 Universal Database за OS/390, DB2 за MVS/ESA и DB2 за VM & VSE.

Когато срещнете някое от двете съобщения, трябва да погледнете оригиналния SQL код в документацията на сървъра на базата данни, генерирал съобщението.

Решение

SQL кодът, получен от хост базата данни не може да се преведе. Коригирайте проблема на базата на кода за грешка и след това отново предайте неуспешната команда.

SQL1338 по време на CONNECT

Симптом / Причина

Не е дефинирано или не е дефинирано правилно името на символно предназначение.

Например това може да се случи, когато се използва APPC възел, а името на символно предназначение, определено в DB2 директорията на възлите, не отговаря на CPI–C запис в конфигурацията на локалната APPC комуникационна подсистема.

Друга причина може да е, че на компютъра е инсталиран повече от един SNA стек. Може да се наложи да проверите PATH и LIBPATH, за да се уверите, че най–напред е посочен стекът, който искате да използвате.

Решения

1. Проверете дали името на CPIC Side информационния профил, определено в запис на DB2 директорията на възлите, отговаря на SNA конфигурацията (използването на главни и малки букви е от значение).
2. Може да се наложи да проверите PATH и LIBPATH, за да се уверите, че най–напред е посочен SNA стекът, който искате да използвате.

SQL1403N по време на CONNECT

Симптом

SQL1403N Посоченото име на потребител и/или парола са неправилни.

Решение

1. На DB2 Connect работната станция не е разпознат потребителя. Проверете дали автентичността на потребителя трябва да се проверява на DB2 Connect работната станция.

   Ако това е така, проверете дали е въведена правилната парола в оператора CONNECT.

   В противен случай записът в системната директория на базата данни трябва да е определен неправилно със стойността AUTHENTICATION SERVER (това е стойността по подразбиране, ако изрично не е определен тип за разпознаване). В този случай трябва да запишете отново записа, като използвате тип AUTHENTICATION DCS или CLIENT.
2. Не е достъпна парола, която да се изпрати на сървъра на базата данни приемник. Ако записът в системната директория на базата данни е със стойност AUTHENTICATION DCS, тогава трябва да се предаде парола от DB2 клиент към сървъра на базата данни приемник. При някои платформи,

например AIX, паролата може да се получи, само ако е осигурена с оператор CONNECT.

SQL5043N

Симптом

Поддръжката на един или повече комуникационни протоколи не може да се стартира успешно. Основните функции на мениджъра на базата данни обаче са стартирани успешно.

Вероятно TCP/IP протоколът не е стартирал на DB2 Connect шлюза. Преди това може да е имало успешно свързване на клиента.

Ако `diaglevel = 4`, тогава `db2diag.log` може да съдържа подобен запис:

```
 1997-05-30-14.09.55.321092   Instance:svtdbm5   Node:000
PID:10296(db2tcpcm)   Appid:none
common_communication  sqlcctcpconnmgr_child   Probe:46
DIA3205E адресът на сокет "30090", конфигуриран в TCP/IP сервизния файл и
необходим за TCP/IP поддръжката на сървъра се използва от друг процес.
```

Решение

Това предупреждение е симптом, че DB2 Connect, който действа като шлюз за отдалечени клиенти, има проблеми при поддържането на един или повече комуникационни протоколи. Тези протоколи може да са TCP/IP, APPC и други и обикновено съобщението посочва, че не е конфигуриран правилно един от дефинираните на DB2 Connect комуникационни протоколи.

Често причината може да се състои в това, че не е дефинирана или е дефинирана неправилно променливата на профила DB2COMM. Като цяло проблемът се получава в резултат от несъответствие между променливата DB2COMM и имената, дефинирани в конфигурацията на мениджъра на базата данни (например svcename, nname или tpname).

Възможен сценарий е да сте имали преди това успешни свързвания и след това да получите съобщението за грешка SQL5043, без да сте променили конфигурацията. Ако се използва TCP/IP протокол, това може да се случи, когато отдалечената система неправилно прекрати свързването поради някаква причина. В този случай от страната на клиента връзката може все още да изглежда, като че ли съществува и може да успеете да я възстановите без други интервенции, ако използвате показаните по–долу команди.

Най–вероятно един от клиентите, свързващи се към шлюза, все още има указател към TCP/IP порта. На всеки компютър клиент, който е свързан към шлюза:

1. db2 terminate
2. db2stop

SQL30020

Симптом

SQL30020N Изпълнението не бе успешно поради разпределена протоколна грешка (Distributed Protocol Error), която ще повлияе върху успешното изпълнение на следващите команди и SQL оператори.

Решения

При тази грешка трябва да се обърнете към сервиз.

Проверете db2dump директорията за ffdc dump (pid.000). След това форматирайте този dump файл с db2fdump и в получения файл потърсете "ERROR". Тук може да е посочено MVS ABEND. В този случай проверете MVS конзолата за допълнителна информация и проверете кода abend в DB2 Ръководството за MVS съобщения и кодове.

SQL30060

Симптом

SQL30060N "<ID–за–оторизация>" не притежава необходимите права, за да изпълни операцията <операция>".

Решение

При свързване към DB2 за MVS или DB2 за OS/390 не са обновени правилно комуникационните таблици на базата данни (CDB). Обърнете се към:

- DB2 Connect: Бърз старт или
- DB2 Приложение за свързваемост

SQL30061

Симптом

Свързване към грешен хост или AS/400 сървър на база данни – не е намерена база данни приемник.

Решение

Може да е определено грешно име на сървър на базата данни в записа на DCS директорията. Когато това се случи, към приложението се връща SQLCODE –30061.

Проверете DB2 възела, базата данни и записите в директорията за DCS. Полето с името на базата данни приемник в записа на директорията за DCS трябва да съответства на името на базата данни, което зависи от платформата. Например за DB2 Universal Database за OS/390 база данни използваното име трябва да е същото като посоченото в полето "LOCATION=locname" в Boot Strap Data Set (BSDS), което също така се осигурява и в съобщението DSNL004I (LOCATION=location), когато се стартира помощното средство за разпределени данни DDF (Distributed Data Facility).

Ръководството DB2 Connect Бърз старт съдържа примери, които показват как да обновите DB2 каталозите. Вижте раздела "Обновяване на DB2 директории" във всяка глава, която описва SNA конфигурирането или вижте главата "Конфигуриране на хост или AS/400 база данни за DB2 Connect" и раздела "Конфигуриране на TCP/IP свързване".

Правилните команди за APPC или APPN възел са:

```
db2 catalog appc node <име_на_възел> remote <име_на_символно_назначение> security program
db2 catalog dcs database <локално_име> as <истинско_db_име>
db2 catalog database <локално_име> as <псевдоним> at node <име_на_възел>
            authentication dcs
```

Правилните команди за TCP/IP възел са:

```
db2 catalog tcpip node <име_на_възел> remote <адрес_или_име_на_хост>
            server <номер_на_порт_или_име_на_услуга>
db2 catalog dcs database <локално_име> as <истинско_db_име>
db2 catalog database <локално_име> as <псевдоним> at node <име_на_възел>
            authentication dcs
```

След това за да се свържете към базата данни, изпълнявате:

```
db2 connect to <псевдоним> user <име_на_потребител> using <парола>
```

SQL30073 с код на връщане 119C при CONNECT

Симптом

Генерира се съобщение SQL30073 с код на връщане 119C. Това се получава, когато сървърът на базата данни приемник не поддържа кодовата страница, използвана от DB2 клиента (който преминава през DB2 Connect). Кодовата таблица се получава от конфигурацията на операционната система, в която работи DB2 клиента.

Вижте *Ръководство за администриране* за допълнителна информация.

Решение

Често този проблем може да се разреши, като се инсталира корекция в сървъра на базата данни приемник. Свържете се със съответната сервизна организация, за да получите и приложите корекцията, която може да ви препоръчат при този симптом.

Като временно решение потребителят може да замени кодовата страница по подразбиране, като настрои променливата на обкръжението DB2CODEPAGE. Проверете кода на географското положение или определете DB2CODEPAGE=850.

На UNIX платформи потребителят може да има възможност да превключи към различна кодова страница, ако въведе различна стойност за променливата на обкръжението LANG.

SQL30081N с код на връщане 1

Симптом

Симптомът е следното съобщение плюс SNA код на състояние:

```
 db2 connect to <име на база данни> user <id на потребител>
Въведете парола за <id на потребител>:
SQL30081N  Открита е комуникационна грешка.
Използван комуникационен протокол:
"APPC".
Използван комуникационен API: "CPI-C".
Място, където е открита грешката: "".
Комуникационната функция, открила
грешката: "cmallc".
Кодове за грешка, специфични за протокола: "1", "*",
"0x10030021".
SQLSTATE=08001
```

Решение(я)

В този пример кодът на състояние е 10030021.

Най–често срещаните кодове на състояния, свързани с това съобщение за грешка, както и предлаганото решение при всеки отделен случай, са както следва:

1. `SQL30081N с код на връщане 1 и sna код на състояние 0877002C`

   Определено е грешно мрежово име.

2. `SQL30081N с код на връщане 1 и SNA код на състояние ffff0003`

   Определен е грешен MAC адрес или не е активна SNA връзката.

3. `SQL30081N с код на връщане 1 и SNA код на състояние 10030021`

   Има несъответствие между тип на LU.

4. `SQL30081N с код на връщане 1 и SNA код на състояние 084B6031`

   MAXDBAT в DSNZPARM (в DB2 за MVS или DB2 за OS/390 хост) е установен на 0

Други предположения:

1. При създаването на профила на локалната LU, дефинирайте LU като LU по подразбиране. Например в панела със списъка с компонентите на SNA в CM/2 направете едно от следните:
   - Маркирайте полето 'Използвай тази локална LU като псевдоним на локална LU по подразбиране' или
   - Определете променливата на профила или на обкръжението `APPCLLU` на шлюз DB2 Connect Enterprise Edition да бъде името на локалната LU. Например на OS/2 системи можете да направите това, като редактирате CONFIG.SYS, а на Windows NT системи чрез Control Panel.
2. Проверете дали SNA е стартирана на DB2 Connect шлюза
3. Ако използвате DB2 за MVS или DB2 за OS/390, проверете дали е стартирано адресното пространство на Помощното средство за разпределени данни DDF (Distributed Data Facility) и дали работи DB2.

SQL30081N с код на връщане 2

Симптом

Получено е съобщение SQL30081N с код на връщане 2 и SNA код на състояние 08120022.

Решение

Параметърът NUMILU на NCP (хост страната на връзката) може да е установен на стойността по подразбиране (0). Проверете това. При необходимост променете NCP дефиницията и опитайте отново, след като влезе в сила направената промяна.

SQL30081N с код на връщане 9

Симптом

Симптомът е следното съобщение (SNA код на състояние не е необходим в този случай):

```
   db2 connect to <база данни> user <id на потребител>
SQL30081N  Открита е комуникационна грешка.
Използван комуникационен протокол:
"APPC".
Използван комуникационен API: "CPI-C".
Място, където е открита грешката: "".
Комуникационната функция, открила
грешката: "cmsend".
Кодове за грешка, специфични за протокола: "9", "*",
 "0x10086021".
SQLSTATE=08001
```

Решение

Проблемът е, че в DB2 Connect системата не е дефинирано правилно името на Транзакционната програма. Например, може да сте обновили SNA конфигурацията, но все още да не сте я проверили на DB2 Connect шлюза. За допълнителни подробности се обърнете към ръководствата *DB2 Connect Enterprise Edition за OS/2 и Windows – Бърз старт* или *DB2 Connect Personal Edition: Бърз старт*.

SQL30081N с код на връщане 10

Симптом

Симптомът е следното съобщение (SNA код на състояние не е необходим в този случай):

```
SQL30081N  Открита е комуникационна грешка.
Използван комуникационен
протокол: "APPC". Използван комуникационен API: "CPI-C".
Място, където
е открита грешката: "". Комуникационната функция, открила
грешката:
 "cmrcv". Кодове за грешка, специфични за протокола: "10", "*", "*".
SQLSTATE=08001
```

Решение

Проверете дали DB2 е инсталирана правилно.

Ако използвате DB2 Connect за OS/2 шлюз, може да видите следното, ако TP името не е дефинирано правилно:

```
 Кодове за грешка, специфични за протокола: "10", "*", "0x084C0000".
SQLSTATE=08001
```

Например в CM/2 в този случай трябва да е дефинирано както следва:

```
 Име на транзакционна програма   = 'tpname'    (дефинирано от потребителя)
Пътека и име на файл на OS/2 програма = notused
```

и (на следващия екран за CM/2 конфигурация)

```
Тип представяне - фонов режим
Тип работа - На опашка, предварително заредени оператори
```

SQL30081N с код на връщане 20

Симптом

```
   SQL30081N  Открита е комуникационна грешка.
Използван комуникационен
протокол: "APPC". Използван комуникационен API: "CPI-C".
Място, където
е открита грешката: "". Комуникационната функция, открила
грешката:
 "xcstp". Кодовете за грешка, специфични за протокола, са: "20", "*", "*".  SQLSTATE=08001
SQLSTATE=08001
```

Решение

Проверете дали SNA подсистемата е стартирала на DB2 Connect

SQL30081N с код на връщане 27

Симптом

Получено е съобщение SQL30081N с код на връщане 27 и SNA код на състояние 800Axxxx.

Решение

Прекалено голям VTAM PIU (Path Information Unit).

SQL30081N с код на връщане 79

Симптом

```
   SQL30081N  Открита е комуникационна грешка.
Използван комуникационен
 протокол: "TCP/IP". Използван комуникационен API: "SOCKETS".
 Място, където
 е открита грешката: "". Комуникационната функция, открила
 грешката:
 "connect".  Кодове за грешка, специфични за протокола: "79", "*", "*".
SQLSTATE=08001
```

Решение(я)

Тази грешка може да възникне в случай, че отдалечен клиент не успее да се свърже към DB2 Connect шлюз. Освен това може да възникне при свързване от DB2 Connect шлюз към хост.

1. Променливата на профила `DB2COMM` може да е настроена неправилно на DB2 Connect шлюза. Проверете това. Например командата `db2set db2comm=tcpip` трябва да се появи в `sqllib/db2profile`, когато DB2 Extended Enterprise Edition работи на AIX.
2. Може да има несъответствие между името на TCP/IP услуга и/или номера на порт в спецификациите на DB2 клиента и DB2 Connect шлюза. Проверете записите във файловете на TCP/IP `услугите` и на двете машини.
3. Проверете дали DB2 е стартирана на DB2 Connect шлюза. Въведете стойност 4 за `diaglevel` на конфигурацията на Мениджъра на базата данни, като използвате командата:

   ```
   db2 update dbm cfg using diaglevel 4
   ```

След като спрете и рестартирате DB2, погледнете във файла db2diag.log, за да проверите дали са стартирали DB2 TCP/IP комуникациите. Би трябвало да видите резултат, подобен на показания:

```
1998-02-03-12.41.04.861119   Instance:svtdbm2   Node:00
PID:86496(db2sysc)   Appid:none
common_communication  sqlcctcp_start_listen   Probe:80
DIA3000I Поддръжката на "TCPIP" протокол е стартирана успешно.
```

SQL30081N със специфичен за протокола код за грешка 10032

Симптом

```
   SQL30081N  Открита е комуникационна грешка.
Използван комуникационен
 протокол: "TCP/IP". Използван комуникационен API: "SOCKETS".
 Място, където
 е открита грешката: "9.21.85.159".  Комуникационна функция,
 открила
 грешката: "send".  Кодове за грешка, специфични за протокола: "10032",
 "*", "*".
SQLSTATE=08001
```

Решение

Това съобщение за грешка може да се получи, когато се опитвате да се откачите от машина, където TCP/IP комуникациите вече са прекъснати. Отстранете проблема с TCP/IP подсистемата.

На повечето машини начинът да се коригира проблемът, е просто да рестартирате TCP/IP протокола за машината. Понякога може да е необходимо да се рециклира цялата машина.

Най–разпространени проблеми с DB2 UDB DRDA AS

В този раздел са представени най–разпространените сценарии, когато се използва DB2 UDB DRDA AS.

Комуникационни грешки при CONNECT

Проверете дали следните елементи са настроени правилно от страната на DB2 UDB.

APPC/SNA LU 6.2

1. SNA конфигурация

   Проверете дали TP името е конфигурирано, ако е необходимо това.

   Освен това ако се използва защита от тип SAME от DRDA AR, проверете дали е активирана за DRDA AR LU.
2. Параметър TPNAME от конфигурацията на мениджъра на базата данни
3. Променлива на обкръжението DB2COMM, настроена да включва APPC

Уверете се, че db2start приключва без никакви предупреждения.

TCP/IP

1. Файл на услугите
2. Параметър SVCENAME от конфигурацията на мениджъра на базата данни
3. Променлива на обкръжението DB2COMM, настроена да съдържа TCPIP. Уверете се, че db2start приключва без никакви предупреждения.

DRDA грешка при CONNECT

APPC/SNA LU 6.2

Ако се използва SNA сървър за AIX, уверете се, че името на група за изпълнимия файл ~/sqllib/adm/db2sysc се намира в полето "Trusted group names" в профила "SNA System Defaults" от SNA конфигурацията.

TCP/IP

Ако DRDA AR е DB2 за OS/390, уверете се, че са приложени следните поправки: APAR PQ05771/PTF UQ06843 and APAR PQ07537/PTF UQ09146.

Грешка, че не е открита база данни при CONNECT

Уверете се, че DRDA AR е конфигуриран с псевдоним за DB2 UDB базата данни приемник.

Грешка от защитата при CONNECT през APPC/SNA LU 6.2

Има някои специални съображения по отношение на параметъра AUTHENTICATION в конфигурацията на мениджъра на DB2 UDB базата данни, ако свързването от DRDA AR е през APPC/SNA LU 6.2. Ако възникне грешка от защитата, проверете дали дали е настроен правилно параметърът AUTHENTICATION от конфигурацията на мениджъра на базата данни, както следва:

1. Client

   При тази стойност ще работят както SAME, така и PROGRAM свързвания.

2. Server

   При тази стойност ще работят само свързвания със защита PROGRAM, които отиват на DB2 UDB DRDA AS на AIX със SNA сървър и на OS/2 със CS/2 V4 (с конфигуриран SPM).

3. DCS

   Сега може да се използва разпознаване тип DCS с DB2 UDB Версия 7 DRDA AS, за да се позволят APPC свързвания от DRDA клиенти, които използват защита SAME (не е необходима парола), като в същото време се прилага тип разпознаване SERVER (което изисква парола) за всички други заявки на клиенти.

   При този случай ще работи следното:

   a. DB2 UDB DRDA AS на AIX със SNA сървър и на OS/2 със CS/2 V4 (с конфигуриран SPM):

      ```
      Защита SAME
      ```

   b. DB2 UDB DRDA AS на OS/2 със CM/2 1.11, Windows NT и Sun Solaris:

Защита SAME или PROGRAM

Тези разлики съществуват, защото някои комуникационни подсистеми не разкриват входящата парола на DB2 UDB.

Грешки при BIND

SQLCA със SQLCODE –4930 може да се върне, ако DRDA AS не поддържа посочена опция на bind. Полето SQLERRMC съдържа информация за опциите на командата bind, които причиняват грешката.

Приложение B. Забележки

IBM може да не предлага продуктите, услугите или компонентите, дискутирани в този документ, във всички страни. Информация за продуктите и услугите, които се предлагат във вашата област можете да получите от местния представител на IBM. Споменаването на продукт, програма или услуга на IBM не е предназначено да твърди или внушава, че само този продукт, програма или услуга на IBM може да се използва. Всеки функционално еквивалентен продукт, програма или услуга, който не нарушава лицензионните права на IBM, може да се използва като заместител. Потребителят сам носи отговорността да прецени и провери работата на всеки продукт, програма или услуга, които не са на IBM.

IBM може да има патенти или заявки за патенти относно обекти, споменати в този документ. Предоставянето на този документ не дава право на никакъв лиценз върху тези патенти. Може да изпращате писмени запитвания за патенти на адрес:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504–1785
U.S.A.

За запитвания за лиценз относно двубайтова (DBCS) информация се свържете с Отдела за лицензни права на IBM във вашата страна или изпратете писмени запитвания на адрес:

IBM World Trade Asia Corporation
Licensing
2–31 Roppongi 3–chome, Minato–ku
Tokyo 106, Japan

Следващия параграф не се отнася за Великобритания, както и всяка друга страна, където такива изключения са несъвместими с местния закон:INTERNATIONAL BUSINESS MACHINES CORPORATION ОСИГУРЯВА ТОВА ИЗДАНИЕ ВЪВ ВИДА, В "КОЙТО Е" БЕЗ ГАРАНЦИЯ ОТ НИКАКЪВ ВИД, ДИРЕКТНА ИЛИ КОСВЕНА, ВКЛЮЧИТЕЛНО, НО НЕ И САМО КОСВЕНИТЕ ГАРАНЦИИ ЗА НЕ–НАРУШЕНИЕ, ПРИГОДНОСТ ЗА ПРОДАЖБА ИЛИ ПРИЛОЖИМОСТ ЗА НЯКАКВА ОПРЕДЕЛЕНА ЦЕЛ. В някои страни не се позволява отхвърляне на директните или косвени гаранции в определени случаи, следователно това твърдение може да не се отнася за вас.

Тази информация може да включва технически неточности или печатни грешки. Периодично информацията тук се променя; тези промени се вмъкват в новите издания на публикацията. По всяко време и без предупреждение IBM може да направи подобрения и/или промени в продукта(ите) и/или програмата(ите), описани в тази публикация.

Всички препратки в тази информация към страници в Web, които не са на IBM, са само за удобство и по никакъв начин не служат като препоръка за тези страници в Web. Материалите на тези страници в Web не са част от материалите за този продукт на IBM и използването на тези страници в Web е изцяло на ваш риск.

Когато изпращате информация до IBM, вие предоставяте на IBM правото да ползва или разпространява тази информация по всякакъв начин, който фирмата счита за подходящ, без това да води до някакви задължения към вас.

Притежатели на лиценз за тази програма, които желаят да получат информация за нея във връзка с (i) осъществяването на обмен на информация между независимо създадени програми и други програми (включително и тази) и (ii) взаимното използване на обменената информация, трябва да се свържат с:

IBM Canada Limited
Office of the Lab Director
1150 Eglinton Ave. East
North York, Ontario
M3C 1H7
CANADA

Такава информация може да е достъпна в съответствие с определени директиви и условия, включващи в някои случаи заплащане или такса.

Лицензионната програма, описана в тази информация и всички налични лицензионни материали са осигурени от IBM под условията на IBM Customer Agreement, IBM International Program License Agreement или някое еквивалентно споразумение между нас.

Всички данни за производителност, които се представят тук са определени в контролирана среда. Следователно резултатите, получени в друга работна среда може значително да се различават. Някои измервания може да са направени в системи на ниво разработка и няма гаранция, че тези измервания ще са същите при стандартните системи. Още повече, че някои измервания може да са оценени чрез екстраполация. Действителните резултати може да се различават. Потребителите на този документ трябва да проверят дали данните са приложими за тяхната специфична среда.

Информацията относно продуктите, които не са на IBM, е получена от доставчиците на тези продукти, техни публикации или други обществено достъпни източници. IBM не е тествал тези продукти и не може да потвърди точността на производителността, съвместимостта или другите твърдения, свързани с продуктите, които не са на IBM. Въпросите за възможностите на продуктите, които не са на IBM, трябва да се отправят към доставчиците на тези продукти.

Всички твърдения относно бъдещи насоки или намерения на IBM могат да се променят или отхвърлят без предупреждение и представляват само цели.

Тази информация може да съдържа примери за данни и отчети, използвани във всекидневни бизнес операции. За по–пълното им илюстриране примерите съдържат имена на индивиди, компании, марки и продукти. Тези имена са измислени и всички съвпадения с имена и адреси, използвани от реални бизнес агенти, са напълно случайни.

ЛИЦЕНЗ ЗА ПРАВА ЗА КОПИРАНЕ:

Тази информация може да съдържа примерни приложни програми в съответния програмен код, които илюстрират техники за програмиране за различни платформи. Можете да копирате, променяте или разпространявате тези примерни програми в произволен вид без заплащане на IBM при разработка, използване, маркетинг или разпространение на приложни програми, които са в съответствие с интерфейса за приложно програмиране за платформата, за която са написани примерните програми. Тази примери не са тествани изцяло и при всички възможни условия. Следователно IBM не може да гарантира или потвърди надеждността, възможностите за обслужване или функционирането на тези програми.

Всяко копие или всяка част от тези примерни програми или техни производни трябва да включва следния знак за запазени права:

Търговски марки

Следващите термини, които може да са отбелязани със звездичка(*), са търговски марки на International Business Machines Corporation в САЩ, други страни или и двете.

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

Следните термини са търговски марки или регистрирани търговски марки на други компании:

Microsoft, Windows и Windows NT са търговски марки и регистрирани търговски марки на Microsoft Corporation.

Java и всички базирани на Java търговски марки и фирмени знаци, както и Solaris са търговски марки на Sun Microsystems, Inc. в САЩ и други страни или и двете.

Tivoli и NetView са търговски марки на Tivoli Systems Inc. в САЩ, в други страни или и двете.

UNIX е регистрирана търговска марка в САЩ, други страни или и двете и е лицензирана изключително чрез X/Open Company Limited.

Имена на други фирми, продукти или услуги, които може да са отбелязани с две звездички(**), може да са търговски марки или марки на услуги на други.

Индекс

A

ACF/VTAM 128
ALREADYV оператор 111
APPC/VM поддръжка 99
APPC/VTAM поддръжка 99
APPCPASS оператор 117
APPL оператор
  DB2 пример 9, 45
  SQL/DS пример 110
APPN (advanced peer–to–peer networking – разширена мрежа с равностойни възли)
  списъци с местоположения, създаване 78
AS/400
  публикации vi
AUTHENTICATION=CLIENT 41
AVS
  компонент на VM 99
  Съображения за максималния брой сесии 114
AXE 128

B

BSDS (bootstrap data set), обновяване 8, 44

C

CCSID (coded character set identifier – идентификатор на кодиран набор символи)
  OS/400 по подразбиране 81
CCSID (coded character set identifier)
  DB2 по подразбиране 21, 62
CHARNAME 106, 119, 126
CHGNETA команда 76
CICS LU 6.2 сесии 131
CICS(ISC) 128
CLI/ODBC приложения
  CURRENTPACKAGESET 41
CMS комуникационна директория
  защита 118
  каталогизиране на имена RDB_NAME 113
comdir
  CMS 113
  VM 100
  примерен запис 118
CRR (Coordinated Resource Recovery–Координирано възстановяване на ресурси) сървър 100
CRTCFGL команда 78
CRTCOSD команда 77
CRTCTLAPPC команда 76
CRTCTLHOST команда 76
CRTDDMTCPA команда 85
CRTDEVAPPC команда 78
CRTLINETH команда 76
CRTLINSDLC команда 76
CRTLINTRN команда 76
CRTLINX25 команда 76
CRTMODD команда 77
CURRENTPACKAGESET 41

D

DB2 LINKNAME таблица 12, 48
DB2 Universal Database за AS/400
  TCP/IP свързвания, настройка 75
  собствени TCP/IP свързвания 76
DB2 Universal Database за OS/390
  DYNAMICRULES(BIND) 41
  TCP/IP – вече изпълнена проверка 41
DBNAME директория 129
DDF запис 7, 43
DRDA
  публикации vi
DRDA сървър
  публикации vi

G

GCS (group control system–система за управление на група) 100

I

IDENT 101

L

LINKNAME таблица 12, 48

M

MVS
  публикации vi
MVS (multiple virtual storage), DB2
  адресни пространства 1, 35

O

ODBC приложения
  CURRENTPACKAGESET 41
OS/400
  активиране на комуникации 78
  мрежови атрибути 76
  публикации vi

R

RDB_NAME
  CMS комуникационна директория 113
RELOAD PACKAGE команда 119
RESID (TPN) 122
RESID NAMES файл
  SQL/DS на VM 122
RU размер
  DB2 рикуестър за приложения 15, 55
  OS/400 рикуестър за приложения 78
  OS/400 сървър на приложения 83
  SQL/DS рикуестър за приложения 115

S

SET CURRENT PACKAGESET 41
SQL (Structured Query Language) 24, 25
  DB2 вторични сървъри
    имена на обекти 25
    разлики 24
  динамични 31, 70
  обекти, SQL/DS мениджър на базата данни – защита 126, 139
  обекти, защита на DB2 32, 71
  статичен 31, 70
SQL справочници vi

SQL/DS
публикации vi
SQL/DS VM
опции за обработка
PROTOCOL 105
SQL/DS VSE
CICS LU 6.2 сесии 131
SQLINIT 105
SYSIBM.IPNAMES таблица 53
SYSIBM.LOCATIONS таблица 48
SYSIBM.LUMODES таблица 51
SYSIBM.LUNAMES таблица 50
SYSIBM.MODESELECT
таблица 52
SYSIBM.SYSLOCATIONS
таблица 12
SYSIBM.SYSLUMODES
таблица 13
SYSIBM.SYSLUNAMES
таблица 12
SYSIBM.SYSMODESELECT
таблица 13
SYSIBM.SYSUSERNAMES
таблица 14
SYSIBM.USERNAMES таблица 52

T

TCP/IP
добре известен порт 446 за
DRDA 83
защита на AS/400 85
защитата вече проверена 41
TPN (име на транзакционна
програма)
DB2 SYSIBM.LOCATIONS
таблица 48
DB2 SYSIBM.SYSLOCATIONS
таблица 12
DRDA стойност по
подразбиране, OS/400 75
OS/400 сървър на
приложения 83
SQL/DS на VM RESID 122
TSAF (Transparent Services Access
Facility–Средство за прозрачен
достъп до услуги) 100

V

VM
DRDA компоненти 99
запис в директория 118
комуникационна директория
(comdir) 100
публикации vi
ресурсен адаптер 100
VRYCFG команда 78
VSE
публикации vi
VTAM 9, 11, 45, 47
APPL оператор
DB2 пример 9, 45
максимален брой сесии по
подразбиране 11, 47
параметри, използвани в
SQL/DS на VM 110
DRDA, роля 101
опции на защита 111

W

WRKCFGSTS команда 78

X

XPCC 129

А

анализ на имена на обекти,
DB2 26
анализиране на имена на обекти,
DB2 26

В

вторичен сървър 4, 24, 38

Д

динамичен SQL 31, 70
CURRENTPACKAGESET 41
директория за разпределена база
данни, OS/400
информация за запис 75
директория на разпределена база
данни, OS/400
описание 74
директория с имена на база
данни 129
достъп, насочен от
приложението 3, 37
достъп, насочен от системата 3,
37

З

защита 16, 18, 20, 27, 28, 30, 31,
32, 56
OS/400 система 80
SQL/DS подсистема 119
имена на крайни потребители
DB2 рикуестър за
приложения 16, 56
защита *(продължение)*
имена на крайни потребители
(продължение)
DB2 сървър на
приложения 28, 66
OS/400 рикуестър за
приложения 79
SQL/DS рикуестър за
приложения 116
мрежа
DB2 Universal Database за
AS/400 сървър на
приложения 84
DB2 сървър на
приложения 30, 68
OS/400 рикуестър за
приложения 79
SQL/DS на VM сървър на
приложения 125
SQL/DS рикуестър за
приложения 116
обработка
DB2 сървър на
приложения 27, 66
SQL/DS на VM сървър на
приложения 123
проверка откъде идва в
DB2 27, 66
рикуестър за приложения
DB2 мениджър на базата
данни 20, 61
DB2 мрежа 18, 59
DB2 подсистема 20, 61
OS/400 мениджър на базата
данни 80
SQL/DS мениджър на база
данни 118
сървър на приложения
DB2 мениджър на базата
данни 31, 70
DB2 подсистема 32, 71
OS/400 имена на крайни
потребители 84
SQL/DS мениджър на база
данни 125
SQL/DS на VM
подсистема 126
защита на мениджъра на базата
данни
DB2 рикуестър за
приложения 20, 61
DB2 сървър на приложения 31,
70
OS/400 рикуестър за
приложения 80
SQL/DS на VM сървър на
приложения 125
SQL/DS рикуестър за
приложения 118

защита на мрежа
DB2 Universal Database за AS/400 сървър на приложения 84
DB2 рикуестър за приложения 18, 59
DB2 сървър на приложения 30, 68
SQL/DS на VM сървър на приложения 125
SQL/DS рикуестър за приложения 116
защити при свързване на приложения, нива 137

И

име на локална база данни, OS/400 74
име на отдалечена база данни, OS/400 83
имена на крайни потребители 16, 28, 56
DB2 28, 66
рикуестър за приложения
DB2 16, 56
OS/400 79
SQL/DS на VM 116
сървър на приложения
OS/400 84
SQL/DS на VM 123

К

клас на услуга
OS/400 описание 76
създаване 77
команда за добавяне на запис в директория на релационна база данни (ADDRDBDIRE) 74
команда за промяна на мрежовите атрибути 76
комуникации 12, 13, 14, 15, 48, 50, 51, 52, 53
VM поток – примери 101
директория, VM
обкръжение 100, 113
подсистема
DB2 рикуестър за приложения 15, 55
OS/400 рикуестър за приложения 75
поток, SQL/DS VSE 129
таблици в база данни, DB2
SYSIBM.IPNAMES 53
SYSIBM.LOCATIONS 48
SYSIBM.LUMODES 51
SYSIBM.LUNAMES 50
SYSIBM.MODESELECT 52
комуникации *(продължение)*
таблици в база данни, DB2 *(продължение)*
SYSIBM.SYSLOCATIONS 12
SYSIBM.SYSLUMODES 13
SYSIBM.SYSLUNAMES 12
SYSIBM.SYSMODESELECT 13
SYSIBM.SYSUSERNAMES 14
SYSIBM.USERNAMES 52
конфигурационен списък, създаване 78
Координирано възстановяване на ресурси (CRR – Coordinated Resource Recovery) 100

Л

локална система
SQL/DS рикуестър за приложения 109
дефиниране на DB2 7
дефиниране на DB2 (VTAM) 42

М

мрежова информация
DB2 сървър на приложения 22, 63
OS/400 рикуестър за приложения 74
OS/400 сървър на приложения 83
SQL/DS VSE сървър на приложения 131
SQL/DS на VM сървър на приложения 121
SQL/DS рикуестър за приложения 109

О

обменяне на съобщения
DB2 7, 42
обработка
опции, DB2 5, 39
описание на режим, създаване 77
описание на устройство, създаване 78
описания на контролери, създаване 76
описания на линията, създаване 76
отдалечена единица работа
DB2 свързвания 3, 37
оторизация по подразбиране, AS/400 81

П

пакети
SQL/DS мениджър на базата данни – защита 125, 138
защита на DB2 сървър на приложения 31, 70
представяне на данни
DB2 рикуестър за приложения 21, 62
DB2 сървър на приложения 33, 72
OS/400 рикуестър за приложения 81
OS/400 сървър на приложения 86
SQL/DS на VM сървър на приложения 126
SQL/DS рикуестър за приложения 119
преобразуване на входящи имена
DB2 сървър на приложения 28, 66
SQL/DS на VM сървър на приложения 123
преобразуване на изходящо име
DB2 рикуестър за приложения 16, 56
SQL/DS рикуестър за приложения 116
примери
ADDRDBDIRE команда 74
DB2 VTAM APPL оператор 9, 45
дефиниране на AVS шлюз 110
Запис в CMS комуникационната директория 138
Запис в комуникационна директория на VM 118
предоставяне на права за достъп, OS/400 80
примери за VM комуникационен поток 101
проверка откъде идва
DB2 сървър на приложения 27, 66
публикации
AS/400 vi
DRDA vi
MVS vi
OS/400 vi
SQL/DS vi
VM vi
VSE vi
сървър на приложения vi

P

разпределена база данни
  DB2 свързвания 3, 37
  достъп, DB2 рикуестър за приложения 6, 42
разпределена единица работа
  достъп, насочен от приложението 3, 37
  достъп, насочен от системата 3, 37
ресурсен адаптер, VM 100
рикуестър за приложения, DB2 6, 11, 15, 16, 18, 20, 21, 41, 48, 55, 56, 62
  RU размер 15, 55
  дефиниция на локална система (VTAM) 42
  защита
    имена на крайни потребители 16, 56
    мениджър на база данни 20, 61
    мрежа 18, 59
    подсистема 20, 61
  комуникации подсистема 15
  комуникационна подсистема 55
  локална система дефиниция 7
  отдалечена система, дефиниция 11, 48
  представяне на данни 21, 62
  стъпка 15, 55
рикуестър за приложения, OS/400 73, 82
  RU размер 78
  защита 79
  комуникации определения 75
  мрежова информация 74
  представяне на данни 81
  стъпка 78
рикуестър за приложения, SQL/DS VM 108, 120
  RU размер 115
  защита
    имена на крайни потребители 116
    мениджър на база данни 118
    мрежа 116
    подсистема 119
  комуникации подсистема 114
  локална система дефиниция 109
  мрежова информация 109
  отдалечена система, дефиниция 112
  представяне на данни 119
рикуестър за приложения, SQL/DS VM *(продължение)*
  стъпка 115
  Съображения за максималния брой AVS сесии 114

C

свързване 39
  сървъри с достъп, насочен от системата 26
  типове
    DB2 разпределена база данни 5, 39
    SQL/DS на VM разпределена база данни 105
сесия
  ограничения при достъп, насочен от системата 27
  ограничения, SQL/DS на VM 114
система за управление на група (GCS) 100
системна защита, OS/400 80
Средство за прозрачен достъп до услуги (Transparent Services Access Facility – TSAF) 100
статичен SQL 31, 70
стъпка 15, 55
  брояч
    DB2 рикуестър за приложения 15, 55
    OS/400 рикуестър за приложения 78
    OS/400 сървър на приложения 83
    SQL/DS рикуестър за приложения 115
съображения за конфигурацията
  промяна на парола 41
съобщение
  обмен, DB2 7, 42
сървър на приложения
  публикации vi
сървър на приложения, DB2 21, 22, 27, 28, 30, 31, 32, 33, 62, 72
  вторичен сървър 24
  достъп, насочен от системата 24
  защита
    имена на крайни потребители 28, 66
    мениджър на база данни 31, 70
    мрежа 30, 68
    подсистема 32, 71
  защита на мениджъра на базата данни 31, 70
сървър на приложения, DB2 *(продължение)*
  мрежова информация 22, 63
  представяне на данни 33, 72
  преобразуване на входящи имена 28, 66
  проверка откъде идва 27, 66
сървър на приложения, OS/400 82, 86
  RU размер 83
  защита 83
  име на отдалечена база данни 83
  имена на крайни потребители 84
  мрежова информация 83
  описание 83
  представяне на данни 86
сървър на приложения, SQL/DS VM 121
  входящо преобразуване на имена 123
  защита
    мениджър на база данни 125
    мрежа 125
  имена на крайни потребители 123
  мрежова информация 121
  описание 121
  представяне на данни 126
сървър на приложения, SQL/DS VSE 131, 140
  защита
    връзка 136
    мениджър на база данни 138
    потребител 137
    свързване на програми 136
  мрежова информация 131
  описание 134

Свързване с IBM

Ако имате технически проблем, моля отделете време да прегледате и изпълните действията, предложени в *Ръководството за решаване на проблеми*, преди да се свържете с отдела за поддръжка на клиенти на DB2. От това ръководство ще разберете каква информация ще е хубаво да имате, така че отдела за поддръжка на клиенти на DB2 да ви обслужи по–добре.

За да получите информация или да поръчате някой от продуктите на DB2 Universal Database, обърнете се към представителството или локалния офис на IBM във вашата страна или към оторизиран дилър на софтуер на IBM.

Ако живеете в САЩ, можете да позвъните на един от следните номера:

- 1–800–237–5511 за поддръжка на клиенти
- 1–888–426–4343, за да научите за възможните опции за обслужване

Информация за продукти

Ако живеете в САЩ, можете да позвъните на един от следните номера:

- 1–800–IBM–CALL (1–800–426–2255) или 1–800–3IBM–OS2 (1–800–342–6672), за да поръчате продукти или да получите обща информация.
- 1–800–879–2755, за да получите издания.

http://www.ibm.com/software/data/
Страниците за DB2 в World Wide Web предоставят осъвременена информация за DB2, свързана с новости, описания на продукти, графици за образователни курсове и др.

http://www.ibm.com/software/data/db2/library/
DB2 Product and Service Technical Library предоставя достъп до често задавани въпроси, поправени грешки, книги и най–нова техническа информация за DB2.

Забележка: Възможно е тази информация да е само на английски.

http://www.elink.ibmlink.ibm.com/pbl/pbl/
Страниците в Web за поръчка на международни публикации осигурява информация за това как да поръчате книги.

http://www.ibm.com/education/certify/
Програмата Professional Certification Program от страниците на IBM в Web осигурява информация за тестове получаване на сертификати за множество продукти на IBM, включително DB2.

ftp.software.ibm.com
Включете се като anonymous. В директорията `/ps/products/db2` можете да намерите демонстрации, поправени грешки, информация и помощни средства, отнасящи се до DB2 и много други продукти.

comp.databases.ibm–db2, bit.listserv.db2-l
Тези интернет групи от новини са на разположение на потребителите, за да обсъждат опита си в работата с DB2 продукти.

В Compuserve: GO IBMDB2
Въведете тази команда, за да осъществите достъп до фамилията форуми IBM DB2. Всички DB2 продукти се поддържат чрез тези форуми.

Информация за това как да се свържете с IBM извън САЩ, можете да получите от Приложение A на *Наръчник за поддръжка на софтуер на IBM*. За достъп до този документ отидете на следната страница в Web: http://www.ibm.com/support/, и след това изберете връзката IBM Software Support Handbook в долната част на тази страница.

Забележка: В някои страни оторизираните дилъри на IBM трябва да се свържа с тяхната структура за поддръжка на дилърите, вместо с Центъра за поддръжка на IBM.

Отпечатано в ЕО

CONN-SUPP-00