Połączenia z DB2 - suplement

Wersja 7

Połączenia z DB2 - suplement

Wersja 7

Przed skorzystaniem z tych informacji i opisywanych przez nie produktów należy przeczytać informacje ogólne, które zawiera “Dodatek B. Uwagi” na stronie 171.

Niniejszy dokument zawiera informacje dotyczące produktów firmy IBM. Są one prezentowane zgodnie z warunkami umowy licencyjnej i są chronione prawem. Informacje zawarte w tej publikacji nie zawierają żadnych gwarancji dotyczących opisywanych produktów i żadnych zapisanych w niej stwierdzeń nie należy interpretować jako takich gwarancji.

Inne publikacje można zamawiać przez przedstawiciela lub oddział firmy IBM obsługujący rejon użytkownika.

Wysłanie informacji do firmy IBM daje jej prawo do ich używania i dystrybucji w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich nadawcy.

Spis treści

O czym jest ten podręcznik v
Struktura podręcznika v
Dla kogo przeznaczony jest ten podręcznik . . . vi
Inne źródła informacji vi
Korzystanie z sieci WWW vi
Publikacje dotyczące DRDA. vi
Publikacje dotyczące serwera DRDA vii
Inne publikacje pokrewne vii

Rozdział 1. Połączenia z DB2 for MVS/ESA w sieci DRDA 1
DB2 for MVS/ESA 1
Implementacja DB2 for MVS/ESA 3
Konfigurowanie requestera aplikacji 7
Dostarczanie informacji sieciowych. 7
Zapewnianie ochrony. 18
Reprezentacja danych 24
Konfigurowanie serwera aplikacji 25
Dostarczanie informacji sieciowych 25
Zapewnianie ochrony. 31
Reprezentacja danych 38

Rozdział 2. Połączenia z DB2 Universal Database for OS/390 w sieci DRDA. . . . 39
DB2 Universal Database for OS/390 39
Implementacja DB2 Universal Database for OS/390 42
Dodatkowe udoskonalenia ochrony 46
Konfigurowanie requestera aplikacji 47
Dostarczanie informacji sieciowych 48
Zapewnianie ochrony. 64
Reprezentacja danych 72
Konfigurowanie serwera aplikacji 73
Dostarczanie informacji sieciowych 74
Zapewnianie ochrony. 77
Zapewnianie ochrony sieci 79
Ochrona menedżera baz danych 81
Podsystem ochrony 82
Reprezentacja danych 83

Rozdział 3. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu SNA 85
Implementacja DB2 Universal Database for AS/400 85
Konfigurowanie requestera aplikacji 85
Dostarczanie informacji sieciowych 86
Zapewnianie ochrony. 91
Reprezentacja danych 94
Konfigurowanie serwera aplikacji 95
Dostarczanie informacji sieciowych 96
Zapewnianie ochrony. 96
Reprezentacja danych 99

Rozdział 4. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu TCP/IP 101
Podsumowanie informacji o DB2 Universal Database for AS/400 101
Konfigurowanie i korzystanie z serwera TCP/IP DRDA DB2 Universal Database for AS/400 . . 102
Konfigurowanie i korzystanie z klienta TCP/IP DRDA DB2 Universal Database for AS/400 . . 104
Uwagi dotyczące ochrony DRDA przy użyciu protokołu TCP/IP 104

Rozdział 5. Dodatkowe uwagi o DB2 Universal Database for AS/400 i DB2 Universal Database. 107

Rozdział 6. Połączenia z DB2 for VSE &VM w sieci DRDA 111
Omówienie DB2 for VM 111
Przykład przepływu komunikacji dla requestera aplikacji 114
Przykład przepływu komunikacji dla serwera aplikacji 115
Implementacja DB2 for VM 118
Opcje przetwarzania wstępnego lub uruchamiania aplikacji 118
Opcje uruchamiania serwera baz danych . . 120
Konfigurowanie requestera aplikacji w środowisku VM 122
Dostarczanie informacji sieciowych 122
Zapewnianie ochrony 130
Reprezentacja danych 134
Lista kontrolna włączania requestera aplikacji DRDA DB2 for VM 135
Konfigurowanie requestera aplikacji w środowisku VM 136
Dostarczanie informacji sieciowych 136
Zapewnianie ochrony 138

Reprezentacja danych 142
Lista kontrolna włączania serwera aplikacji DB2 for VM DRDA 143
Omówienie DB2 for VSE 144
Przykład przepływu komunikacji dla serwera aplikacji 145
Ograniczenia 146
Parametry uruchamiania serwera aplikacji . . . 146
Parametr RMTUSERS 146
Parametr SYNCPNT 147
Konfigurowanie serwera aplikacji w środowisku VSE 147
Dostarczanie informacji sieciowych 147
Zapewnianie ochrony 153
Reprezentacja danych 156
Lista kontrolna uaktywniania serwera aplikacji DB2 for VSE DRDA Application Server . . 156

Dodatek A. Najczęstsze problemy związane z połączeniami 159
Najczęstsze problemy z DB2 Connect 159
SQL0965 lub SQL0969 160
SQL1338 podczas wykonywania CONNECT 160
SQL1403N podczas wykonywania CONNECT 160
SQL5043N 161
SQL30020 162
SQL30060 162
SQL30061 162
SQL30073 z kodem powrotu 119C podczas wykonywania CONNECT 163
SQL30081N z kodem powrotu 1 164
SQL30081N z kodem powrotu 2 165
SQL30081N z kodem powrotu 9 165
SQL30081N z kodem powrotu 10 165
SQL30081N z kodem powrotu 20 166
SQL30081N z kodem powrotu 27 166
SQL30081N z kodem powrotu 79 167
SQL30081N z kodem błędu 10032 właściwym dla protokołu 167
Najczęstsze problemy z serwerem aplikacji DRDA z DB2 UDB 168
Błędy komunikacyjne występujące podczas wykonywania CONNECT 168
Błąd DRDA podczas wykonywania CONNECT 168
Błąd nieodnalezienia bazy danych podczas wykonywania CONNECT 168
Błąd ochrony podczas wykonywania CONNECT przez jednostkę logiczną 6.2 (LU 6.2) APPC/SNA 169
Błędy podczas wykonywania BIND 169

Dodatek B. Uwagi 171
Znaki towarowe 174

Indeks 177

Kontakt z firmą IBM 181
Informacje na temat produktu 181

O czym jest ten podręcznik

W tym podręczniku można znaleźć dodatkowe informacje, które mogą być pomocne podczas instalowania i konfigurowania różnych systemów zarządzania relacyjnymi bazami danych (RDBMS) DB2, takich jak requestery aplikacji DRDA czy serwery aplikacji. Informacje te pomogą skonfigurować:

- Serwery IBM DB2 Universal Database (UDB) wersja 7 pracujące jako serwery aplikacji DRDA.
- Requestery aplikacji IBM DB2 Connect wersja 7.
- Inne produkty zgodne z architekturą DRDA.

Informacje znajdujące się w tym podręczniku stanowią uzupełnienie do informacji zawartych w podręcznikach:

- *Quick Beginnings* dla DB2 Universal Database Enterprise Edition wersja 7,
- *Quick Beginnings* dla DB2 Universal Database Extended - Enterprise Edition wersja 7,
- *Quick Beginnings* dla DB2 Connect Enterprise Edition wersja 7,
- *Krótkie wprowadzenie* dla DB2 Connect Personal Edition wersja 7.

Najnowsze informacje na temat hostów (DB2 Universal Database for OS/390, DB2 Universal Database for AS/400 i DB2 for VSE & VM) można znaleźć w dołączonej do nich dokumentacji.

Informacje na temat konfigurowania menedżera DB2 Syncpoint Manager (SPM) w celu aktualizacji wielu hostów można znaleźć w podręczniku *Instalowanie i konfigurowanie - suplement*.

Struktura podręcznika

Podręcznik składa się z następujących rozdziałów:

- "Rozdział 1. Połączenia z DB2 for MVS/ESA w sieci DRDA" na stronie 1
- "Rozdział 2. Połączenia z DB2 Universal Database for OS/390 w sieci DRDA" na stronie 39
- "Rozdział 3. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu SNA" na stronie 85
- "Rozdział 4. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu TCP/IP" na stronie 101
- "Rozdział 5. Dodatkowe uwagi o DB2 Universal Database for AS/400 i DB2 Universal Database" na stronie 107

- “Rozdział 6. Połączenia z DB2 for VSE &VM w sieci DRDA” na stronie 111
- “Dodatek A. Najczęstsze problemy związane z połączeniami” na stronie 159
- “Dodatek B. Uwagi” na stronie 171.

Dla kogo przeznaczony jest ten podręcznik

Podręcznik przeznaczony jest dla osób, które mają zainstalowany produkt DB2 Universal Database lub DB2 Connect i chcą dowiedzieć się czegoś więcej na temat połączeń w kontekście tematów wymienionych powyżej.

Inne źródła informacji

W tej sekcji opisano inne przydatne źródła informacji.

Korzystanie z sieci WWW

Najnowsze informacje o DB2 Connect, DB2 Universal Database i innych produktach IBM można znaleźć w sieci WWW. Są to zarówno najnowsze publikacje, jak i uwagi oraz wskazówki w postaci Technotes. Aby znaleźć te informacje w sieci WWW, wykonaj następujące czynności:

1. W przeglądarce WWW wprowadź następujący adres URL:

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

2. Wybierz produkt “DB2 Universal Database”.
3. Wyszukaj “Technotes”, na przykład przy użyciu parametrów “DDCS”, “DRDA” lub “Connect”.

Publikacje dotyczące DRDA

Wymienione niżej podręczniki zawierają informacje związane z zagadnieniem, a odniesienia do nich można znaleźć w niniejszym podręczniku.

Numer	Tytuł podręcznika
SC26-4783	*Distributed Relational Database Architecture Connectivity Guide*
SC26-4773	*Distributed Relational Database Architecture Application Programming Guide*
SC26-4782	*Distributed Relational Database Architecture Problem Determination Guide*
SC26-4650	*Planning for Distributed Relational Database Architecture*
GC26-3195	*Distributed Relational Database Architecture Every Manager’s Guide*
G321-5482	*IBM Distributed Data Management Architecture Level 3: Reference*

Publikacje dotyczące serwera DRDA

Wymienione niżej podręczniki stanowią publikacje dotyczące serwera DRDA z bibliotek produktów DB2 Universal Database for AS/400, DB2 for OS/390 oraz DB2 for VSE & VM.

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

Inne publikacje pokrewne

Numer	Tytuł podręcznika
SG24-2006	*Migrating to DB2 Universal Database Version 5*
SG24-2213	*DB2 for OS/390 Version 5 Performance Topics*
SG24-4893	*DB2 Meets NT*
SG24-4894	*The Universal Connectivity Guide to DB2*
SG24-4693	*Getting Started with DB2 Stored Procedures*

Numer	Tytuł podręcznika
SG24-2212	*DRDA Support for TCP/IP in DB2 Universal Database for OS/390 V5.1 and DB2 Universal Database V5.0*
SC33-0814	*CICS for AIX Application Programming Guide*
SC33-0931	*CICS for AIX Customization and Operation Guide*
GC09-2829-00	*DB2 Connect Enterprise Edition for UNIX Quick Beginnings*
GC09-2828-00	*DB2 Connect Enterprise Edition for OS/2 and Windows Quick Beginnings*
GC85-0027-00	*DB2 Connect Personal Edition Krótkie wprowadzenie*
GG24-4155	*Distributed Relational Database Architecture: Using DDCS for AIX DRDA support with DB2 for MVS/ESA and DB2 Universal Database for AS/400*
GG24-4311	*Distributed Relational Database Architecture Cross Platform Connectivity and Application*
SC23-2443	*Encina for AIX Product Family Overview*

Rozdział 1. Połączenia z DB2 for MVS/ESA w sieci DRDA

DB2 for MVS/ESA jest systemem zarządzania relacyjną bazą danych IBM dla systemów MVS/XA i MVS/ESA. DB2 for MVS/ESA wersja 2 wydanie 3 to pierwsze wydanie DB2 for MVS/ESA, które mogło współużytkować rozproszone relacyjne dane przy użyciu innych protokołów DRDA obsługujących DBMS. W rozdziale tym opisano, w jaki sposób DB2 for MVS/ESA obsługuje systemy rozproszonych relacyjnych baz danych. Użytkownicy DB2 Universal Database for OS/390 *mogą pominąć ten rozdział* i zamiast niego przeczytać “Rozdział 2. Połączenia z DB2 Universal Database for OS/390 w sieci DRDA” na stronie 39.

W tym rozdziale skoncentrowano się na konfigurowaniu DB2 for MVS/ESA dla połączeń:

1. DB2 Connect (patrz “Konfigurowanie serwera aplikacji” na stronie 25),
2. Z serwerami DB2 Universal Database (patrz “Konfigurowanie requestera aplikacji” na stronie 7).

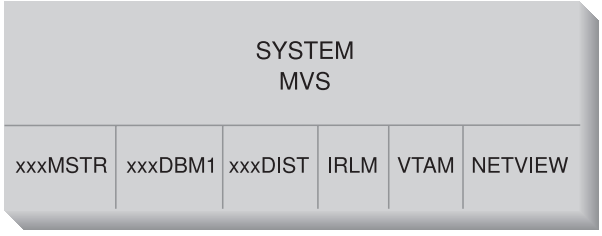
Informacje na temat połączenia dwóch systemów DB2 for MVS/ESA i bardziej szczegółowe informacje dotyczące definiowania połączeń DRDA z DB2 for MVS/ESA można znaleźć we fragmencie poświęconym łączeniu systemów rozproszonej bazy danych w podręczniku *IBM Database 2 Administration Guide*.

Przy użyciu AnyNet Feature VTAM wersja 4 wydanie 2 można uruchomić APPC przez sieć TCP/IP. AnyNet Feature składa się z AnyNet/MVS, uruchamianego na hoście i AnyNet/2, uruchamianego na stacji roboczej i ładowanego z hosta. Każda aplikacja APPC jest dostępna dla użytkowników w sieci TCP/IP bez konieczności wprowadzania zmian w aplikacji. Korzystając z APPC przez TCP/IP, aplikacja działająca na MVS/ESA może się komunikować z inną aplikacją APPC używającą AnyNet APPC przez TCP/IP w systemach MVS/ESA, OS/2, AIX/6000, OS/400 lub Windows. Więcej informacji na ten temat można znaleźć w podręczniku *VTAM AnyNet Feature for V4R2 Guide to SNA over TCP/IP*.

DB2 for MVS/ESA

Rys. 1 na stronie 2 przedstawia system MVS działający z pojedynczą kopią DB2 for MVS/ESA. W jednym systemie MSV może jednak działać wiele baz DB2 for MVS/ESA. Aby identyfikować kopie DB2 for MVS/ESA w danym systemie MVS (lub kopie DB2 for MVS/ESA w ramach kompleksu MVS/JES), każdemu systemowi DB2 jest nadawana *nazwa podsystemu* - łańcuch złożony z jednego do czterech znaków unikalnych w ramach kompleksu MVS/JES. Na Rys. 1 na stronie 2 nazwą podsystemu DB2 for MVS/ESA jest *xxxx*. Trzy nazwy przestrzeni adresowych MVS mają

przedrostki w nazwach podsystemów DB2 for MVS/ESA. Przestrzenie te określają produkt DB2 for MVS/ESA.



Rysunek 1. Przestrzenie adresowe MVS używane przez DB2 for MVS/ESA

Rys. 1 ilustruje przestrzenie adresowe MVS wykorzystywane w przetwarzaniu rozproszonych baz danych w DB2 for MVS/ESA. Ich współdziałanie umożliwia użytkownikom DB2 for MVS/ESA dostęp do lokalnych relacyjnych baz danych i komunikację z systemami zdalnymi DRDA. Przeznaczenie poszczególnych przestrzeni adresowych jest następujące:

xxxxMSTR
: Przestrzeń adresowa usług systemowych dla produktu DB2 for MVS/ESA, odpowiedzialna za uruchamianie i zatrzymywanie DB2 for MVS/ESA oraz kontrolowanie lokalnego dostępu do DB2 for MVS/ESA.

xxxxDBM1
: Przestrzeń adresowa usług baz danych odpowiedzialna za dostęp do relacyjnych baz danych kontrolowana przez DB2 for MVS/ESA. W tej przestrzeni jest realizowane wejście i wyjście dla zasobów baz danych w imieniu aplikacji SQL.

xxxxDIST
: Część DB2 for MVS/ESA obsługująca rozproszone bazy danych, zwane również *Distributed Data Facility* (DDF). Gdy nadchodzi żądanie związane z rozproszoną bazą danych, DDF przekazuje je do przestrzeni *xxxx*DBM1, aby można było wykonać operacje we/wy dla odpowiedniej bazy danych. Szczegółowy opis DDF zamieszczono dalej.

IRLM Menedżer blokad używany przez DB2 for MVS/ESA w celu kontroli dostępu do zasobów baz danych.

VTAM Menedżer komunikacji SNA dla systemu MVS. DDF wykorzystuje VTAM do realizacji komunikacji z rozproszoną bazą danych w imieniu DB2 for MVS/ESA.

NETVIEW
Produkt obsługujący punkt skupienia zarządzania siecią w systemach MVS. Jeśli podczas przetwarzania rozproszonych baz danych wystąpi błąd, DDF zapisuje informacje dotyczące błędu (zwane również *alertami*) w bazie danych monitora sprzętu NetView. Administratorzy systemu mogą korzystać z NetView, aby zapoznać się z błędami zapisanymi w bazie danych monitora sprzętu lub ustawić procedury automatycznego wykonywania komend wywołania po zapisaniu warunków alertu.

NetView może również służyć do diagnozowania błędów komunikacji VTAM. Więcej informacji na ten temat można znaleźć w podręczniku *Distributed Relational Database Architecture Problem Determination Guide*.

Na Rys. 1 na stronie 2 nie ma aplikacji SQL. Jeśli aplikacja używa DB2 do wprowadzenia instrukcji SQL, program musi się połączyć z produktem DB2 for MVS/ESA na jeden z następujących sposobów:

TSO Zadania wsadowe i użytkownicy zalogowani do TSO łączą się z DB2 for MVS/ESA za pomocą narzędzia TSO. Jest to technika używana do łączenia SPUFI i większości aplikacji QMF z DB2 for MVS/ESA.

CICS/ESA
Jeśli aplikacja CICS/ESA używa wywołań SQL, produkt CICS/ESA używa interfejsu przyłączenia CICS do kierowania żądań SQL do DB2 for MVS/ESA.

IMS/ESA
Transakcje uruchamiane w IMS/ESA korzystają z interfejsu przyłączenia IMS, aby przekazać instrukcje SQL do przetwarzania w DB2 for MVS/ESA.

DDF Narzędzie Distributed Data Facility jest odpowiedzialne za połączenie aplikacji rozproszonych z DB2 for MVS/ESA.

CAF Narzędzie Call Attachment Facility umożliwia podsystemom napisanym przez użytkownika bezpośrednie połączenie się z DB2 for MVS/ESA.

Implementacja DB2 for MVS/ESA

Architektura DRDA definiuje typy funkcji systemu zarządzania rozproszoną bazą danych. DB2 for MVS/ESA V2R3 obsługuje zdalne jednostki pracy. Program uruchamiany w jednym systemie może przy użyciu zdalnej jednostki pracy uzyskać dostęp do danych w systemie zdalnym DBMS, wykorzystując SQL dostarczany przez ten system. DB2 for MVS/ESA V3R1 obsługuje rozproszone jednostki pracy. Program uruchamiany w jednym systemie może - przy użyciu rozproszonej jednostki pracy - uzyskać dostęp do danych w wielu systemach zdalnych DBMS, wykorzystując język SQL, który jest w nich obsługiwany. Więcej informacji na temat typów dystrybucji zdefiniowanych przez DRDA można znaleźć w podręczniku *DRDA Connectivity Guide*.

Jak przedstawiono na Rys. 2 na stronie 5, DB2 for MVS/ESA obsługuje trzy konfiguracje połączeń z rozproszoną bazą danych, korzystając z dwóch metod dostępu:

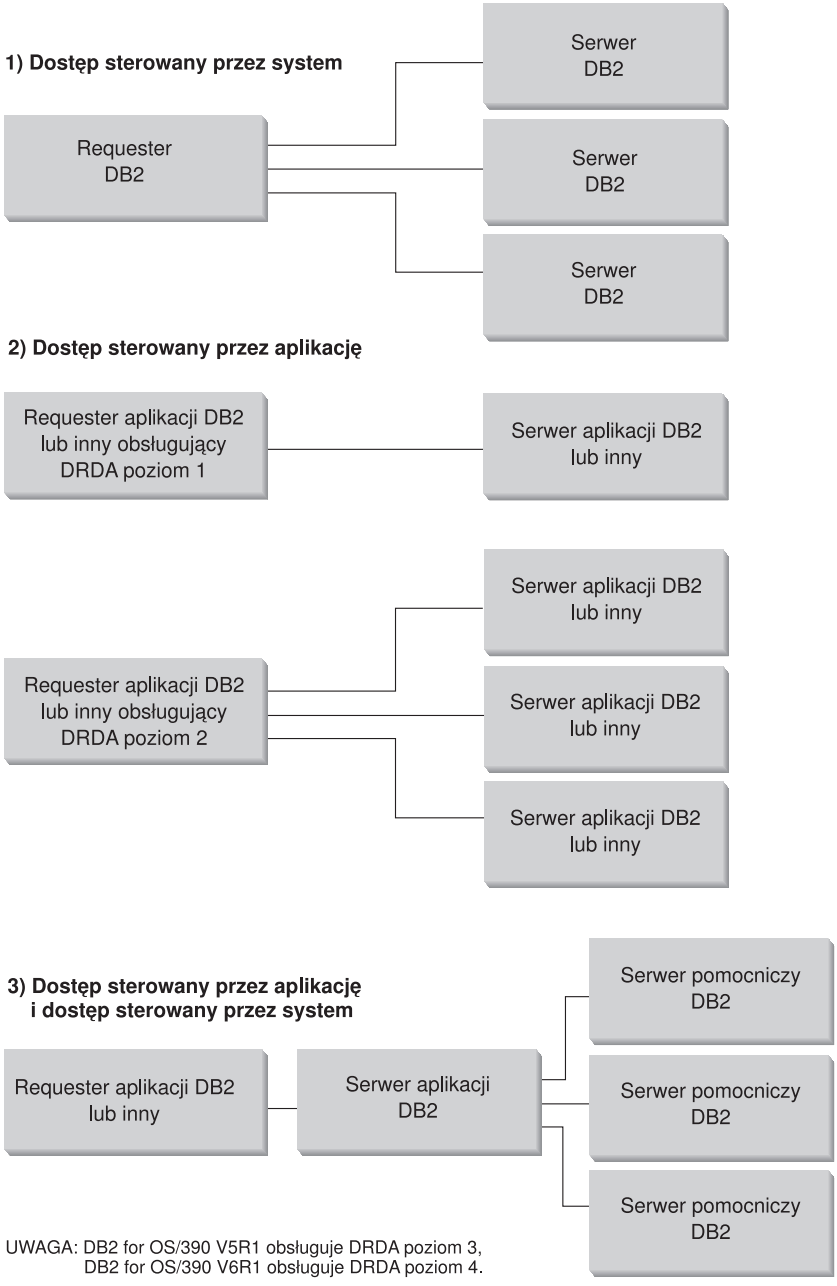
[1] *Dostęp sterowany przez system* umożliwia requesterowi DB2 for MVS/ESA połączenie z jednym lub kilkoma serwerami DB2 for MVS/ESA. Połączenie nawiązane między requesterem DB2 for MVS/ESA i serwerem nie pasuje do protokołów zdefiniowanych w DRDA i nie może być używane do łączenia z DB2 for MVS/ESA produktów innych niż DB2 for MVS/ESA. Ten rodzaj połączenia jest ustanawiany przy użyciu kodowania trzyczęściowych nazw lub aliasów w aplikacji.

[2] *Dostęp sterowany przez aplikację* umożliwia requesterowi DB2 for MVS/ESA lub requesterowi innemu niż DB2 for MVS/ESA, np. DB2 Connect połączenie się z jednym lub kilkoma serwerami aplikacji DB2 for MVS/ESA lub innymi niż DB2 for MVS/ESA, np. z DB2 Universal Database czy DB2 Universal Database for AS/400 przy użyciu protokołów DRDA. Liczba serwerów aplikacji, które mogą być jednocześnie połączone z requesterem, zależy od poziomu DB2 for MVS/ESA requestera aplikacji. Jeśli requesterem aplikacji jest DB2 for MVS/ESA V2R3, w tym samym czasie może być połączony tylko jeden serwer aplikacji. Ten typ połączenia jest ustanawiany przez wprowadzenie do kodu aplikacji instrukcji SQL CONNECT. Jeśli requesterem aplikacji jest DB2 for MVS/ESA V3R1, w tym samym czasie może być połączonych kilka serwerów aplikacji.

[3] Podczas ustanawiania połączenia można użyć obu metod dostępu jednocześnie.

Termin *serwer pomocniczy* określa systemy działające jako serwery w stosunku do serwerów aplikacji.

Jeśli wszystkie systemy w konfiguracji obsługują zatwierdzanie dwufazowe, obsługiwana jest rozproszona jednostka pracy (odczyt dla wielu miejsc i aktualizacja dla wielu miejsc). Jeśli nie wszystkie systemy obsługują zatwierdzanie dwufazowe, aktualizacja w ramach jednostki pracy jest ograniczona do jednego miejsca lub do podzbioru miejsc obsługujących zatwierdzanie dwufazowe.



Rysunek 2. Połączenia rozproszone DB2 for MVS/ESA

Tabela 1 zawiera porównanie typów połączeń rozproszonych baz danych DB2 for MVS/ESA.

Tabela 1. Porównanie połączeń rozproszonych baz danych DB2 for MVS/ESA

[1] Dostęp sterowany przez system.	**[2] Dostęp sterowany przez aplikację (dla wszystkich systemów obsługujących zatwierdzanie dwufazowe).**	**[3] Dostęp sterowany przez aplikację i dostęp sterowany przez system.**
Wszyscy partnerzy muszą być systemami DB2 for MVS/ESA.	Może łączyć dowolne systemy DRDA.	Requester aplikacji może być dowolnym systemem DRDA; serwery muszą być systemami DB2 for MVS/ESA.
Mogą łączyć się bezpośrednio z wieloma partnerami.	Mogą łączyć się bezpośrednio z wieloma partnerami.	Requester aplikacji łączy się bezpośrednio z serwerami aplikacji; serwery aplikacji mogą łączyć się z wieloma serwerami pomocniczymi DB2 for MVS/ESA.
Każda aplikacja SQL może mieć wiele konwersacji APPC z każdym serwerem.	Każda aplikacja SQL ma jedną konwersację APPC z każdym serwerem.	Aplikacja SQL utrzymuje jedną konwersację APPC z każdym serwerem; serwer aplikacji DB2 for MVS/ESA może dla aplikacji nawiązać wiele konwersacji APPC z każdym serwerem.
Może mieć dostęp zarówno do zasobów lokalnych, jak i zdalnych w jednym zakresie zatwierdzania.	Może mieć dostęp zarówno do zasobów lokalnych, jak i zdalnych w jednym zakresie zatwierdzania.	Requester aplikacji i serwer aplikacji mogą mieć dostęp do danych lokalnych i zdalnych.
Bardziej efektywny w przypadku obszernych zapytań i wielu zapytań współbieżnych.	Bardziej efektywny w przypadku instrukcji SQL uruchamianych bardzo rzadko w ramach jednego zatwierdzania.	Połączenie requester aplikacji-serwer aplikacji zachowuje się jak **[2]**; serwer pomocniczy zachowuje się jak **[1]**.
Może obsługiwać statyczny lub dynamiczny SQL, lecz serwer dynamicznie powiąże statyczny SQL za pierwszym razem, gdy jest on wykonywany w jednym zakresie zatwierdzania.	Może korzystać ze statycznego lub dynamicznego SQL.	Requester aplikacji i serwer aplikacji mogą korzystać ze statycznego lub dynamicznego SQL; serwery pomocnicze obsługują statyczny lub dynamiczny SQL, lecz wiążą dynamicznie statyczny SQL za pierwszym razem, gdy jest on wykonywany w zasięgu zatwierdzania.
Ograniczony do instrukcji SQL INSERT, DELETE i UPDATE oraz instrukcji, które obsługują SELECT.	Może używać dowolnych instrukcji obsługiwanych przez system, który je wykonuje.	Serwery aplikacji obsługują wszystkie rodzaje SQL; serwery pomocnicze obsługują tylko DML SQL (na przykład CREATE lub ALTER).

Konfigurowanie requestera aplikacji

DB2 for MVS/ESA implementuje obsługę requestera aplikacji DRDA jako integralną część DB2 for MVS/ESA Distributed Data Facility (DDF). Działanie DDF można zatrzymać niezależnie od lokalnych funkcji zarządzania bazą danych DB2 for MVS/ESA, lecz nie można uruchomić, gdy brak obsługi zarządzania lokalną bazą danych DB2 for MVS/ESA.

Jeśli DB2 for MVS/ESA pełni rolę requestera aplikacji, może połączyć aplikacje uruchamiane w systemie z serwerami baz danych DB2 Universal Database, DB2 for MVS/ESA, DB2 Universal Database for OS/390, DB2 Universal Database for AS/400 i DB2 for VSE & VM, które mają implementację funkcji serwera aplikacji DRDA.

Aby requester aplikacji DB2 for MVS/ESA miał dostęp do rozproszonych baz danych, muszą być spełnione następujące warunki:

- "Dostarczanie informacji sieciowych" — Requester aplikacji musi akceptować wartości RDB_NAME i wykonać ich translację na wartości SNA NETID.LUNAME. DB2 for MVS/ESA używa *baz danych komunikacji DB2 for MVS/ESA* w celu zarejestrowania nazw RDB_NAME i związanych z nimi parametrów sieciowych. Baza danych komunikacji umożliwia requesterowi aplikacji DB2 for MVS/ESA przekazywanie wymaganych informacji SNA do VTAM podczas żądań kierowanych do rozproszonych baz danych.
- "Zapewnianie ochrony" na stronie 18 — Aby żądania kierowane do zdalnej bazy danych były przyjmowane przez serwer aplikacji, requester aplikacji musi dostarczać informacji związanych z ochroną, wymaganych przez serwer. DB2 for MVS/ESA korzysta z bazy danych komunikacji i z RACF w celu dostarczenia wymaganych informacji związanych z ochroną.
- "Reprezentacja danych" na stronie 24 — Należy upewnić się, że identyfikator CCSID requestera aplikacji jest kompatybilny z serwerem aplikacji.

Dostarczanie informacji sieciowych

Większość procesów przetwarzania w środowisku rozproszonych baz danych wymaga wymiany komunikatów z innymi miejscami w sieci. Aby przetwarzanie odbywało się poprawnie, należy:

1. Zdefiniować system lokalny.
2. Zdefiniować system zdalny.
3. Zdefiniować komunikację.
4. Ustawić wielkości RU i pacing.

Definiowanie systemu lokalnego

Każdemu programowi w sieci przypisywany jest identyfikator NETID i nazwa jednostki logicznej (LU), ponieważ requester aplikacji DB2 for MVS/ESA musi mieć wartość NETID.LUNAME, gdy łączy się z siecią. Ponieważ requester aplikacji DB2 for MVS/ESA jest zintegrowany z lokalnym systemem zarządzania bazą danych DB2 for

MVS/ESA, musi mieć on również nazwę RDB_NAME. W publikacjach dotyczących DB2 for MVS/ESA, RDB_NAME DB2 for MVS/ESA jest określana jako nazwa *miejsca*.

Requester aplikacji DB2 for MVS/ESA w sieci SNA należy zdefiniować w następujący sposób:

1. Wybrać nazwę jednostki logicznej dla systemu DB2 for MVS/ESA. Identyfikator NETID dla systemu DB2 for MVS/ESA jest pobierany automatycznie z VTAM podczas uruchamiania DDF.
2. Zdefiniować nazwę jednostki logicznej i nazwę miejsca w *programie startowym* (BSDS) produktu DB2 for MVS/ESA. (DB2 for MVS/ESA ogranicza nazwę miejsca do 16 znaków).
3. Utworzyć definicję APPL VTAM w celu zarejestrowania wybranej nazwy jednostki logicznej w VTAM.

Konfigurowanie BSDS DDF: DB2 for MVS/ESA odczytuje BSDS podczas przetwarzania startowego w celu uzyskania parametrów instalacyjnych systemu. Jeden z rekordów zapisanych w BSDS nosi nazwę *rekordu DDF*, ponieważ zawiera informacje używane przez DDF do łączenia z VTAM. Informacje te obejmują:

- nazwę miejsca systemu DB2 for MVS/ESA,
- nazwę jednostki logicznej (LU) systemu DB2 for MVS/ESA,
- hasło używane podczas łączenia systemu DB2 for MVS/ESA z VTAM.

Informacje BSDS DDF można dostarczyć do DB2 for MVS/ESA na dwa sposoby:

- Użyć panelu instalacyjnego DDF DSNTIPR podczas pierwszego instalowania DB2 for MVS/ESA w celu dostarczenia wymaganych informacji BSDS DDF. Pominięto tu informacje o wielu parametrach instalacyjnych, ponieważ ważniejsze jest przekazanie wskazówek dotyczących sposobu łączenia DB2 for MVS/ESA z VTAM. Rys. 3 przedstawia sposób użycia panelu instalacyjnego w celu zapisania w BSDS DB2 for MVS/ESA nazwy miejsca SYDNEY, nazwy jednostki logicznej LUDBD1 i hasła PSWDBD1.

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

Rysunek 3. Panel instalacyjny DB2 for MVS/ESA o nazwie DSNTIPR

- Jeśli produkt DB2 for MVS/ESA jest już zainstalowany, można użyć programu narzędziowego obsługującego wykaz protokołu zmian (DSNJU003) w celu aktualizacji informacji znajdujących się w BSDS.

  Rys. 4 przedstawia sposób aktualizacji BSDS przez wprowadzenie nazwy miejsca SYDNEY, nazwy jednostki logicznej (LU) LUDBD1 i hasła 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
//*
```

Rysunek 4. Przykładowa definicja zestawu danych programu startowego DDF

Podczas uruchamiania programu narzędziowego DDF (automatycznie podczas uruchamiania DB2 for MVS/ESA lub przy użyciu komendy DB2 for MVS/ESA START DDF) łączy się z VTAM i przekazuje mu nazwę jednostki logicznej i hasło. VTAM rozpoznaje system DB2 for MVS/ESA, sprawdzając nazwę jednostki logicznej i hasło (jeśli jest ono wymagane) z wartościami zdefiniowanymi w APPL VTAM DB2 for MVS/ESA. Hasło VTAM jest używane w celu sprawdzenia, czy DB2 for MVS/ESA ma autoryzację do korzystania z podanej jednostki logicznej w systemie VTAM. Hasło VTAM nie jest przesyłane przez sieć i nie jest wykorzystywane do połączenia innych systemów w sieci z DB2 for MVS/ESA.

Jeśli VTAM nie wymaga hasła, należy pominąć parametr PASSWORD= w programie narzędziowym obsługującym wykaz protokołu zmian. Brak tego parametru wskazuje, że hasło VTAM nie jest wymagane.

Tworzenie definicji APPL VTAM: Po zdefiniowaniu nazwy jednostki logicznej VTAM i hasła w DB2 for MVS/ESA należy te wartości zarejestrować w VTAM. VTAM używa instrukcji APPL, aby zdefiniować nazwy jednostek logicznych. Rys. 5 na stronie 10 przedstawia sposób definiowania nazwy jednostki logicznej LUDBD1 w VTAM.

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

Rysunek 5. Przykładowa definicja APPL w DB2 for MVS/ESA

W instrukcji APPL VTAM dostępnych jest wiele parametrów. Ich znaczenie jest opisane szczegółowo w podręczniku *DB2 Administration Guide*. Parametry omawiane w tym podręczniku odpowiadają tytułom tematów. Niektóre ważniejsze parametry przedstawiono na Rys. 5.

LUDBD1

VTAM używa etykiety instrukcji APPL jako nazwy jednostki logicznej (LU). W tym przypadku nazwą jednostki logicznej jest LUDBD1. Składnia APPL nie zapewnia tyle miejsca, aby zmieściła się cała nazwa NETID.LUNAME. Wartość identyfikatora NETID nie jest podana w instrukcji APPL VTAM, ponieważ wszystkie aplikacje VTAM są automatycznie przystosowane do NETID dla systemu VTAM.

AUTOSES=1

Liczba sesji zwycięskich w rywalizacji o połączenie SNA, które są uruchamiane automatycznie podczas wprowadzenia żądania APPC Change Number of Sessions (Zmiana liczby sesji CNOS). Wartość AUTOSES powinna być różna od zera, aby w przypadku błędu w przetwarzaniu CNOS VTAM możliwe było dostarczenie odpowiedniej informacji dla DB2 for MVS/ESA.

Automatyczne uruchamianie wszystkich sesji APPC między dowolnymi dwoma partnerami rozproszonej bazy danych nie jest konieczne. Jeśli wartość AUTOSES jest mniejsza od limitu zwycięzców rywalizacji (DMINWNL), VTAM odkłada uruchomienie pozostałych sesji SNA do czasu, gdy będą one potrzebne aplikacji obsługującej rozproszone bazy danych.

DMINWNL=10

Liczba sesji, dla których dany system DB2 for MVS/ESA jest zwycięzcą rywalizacji. Parametr DMINWNL zawiera wartość domyślną dla przetwarzania CNOS, lecz można go przesłonić dla dowolnego partnera, dodając wiersz do tabeli SYSIBM.SYSLUMODES w bazie danych komunikacji DB2 for MVS/ESA.

DMINWNR=10

Liczba sesji, dla których zwycięzcą rywalizacji jest system partnerski. Parametr DMINWNR zawiera wartość domyślną dla przetwarzania CNOS. Można go przesłonić dla dowolnego partnera, dodając wiersz do tabeli SYSIBM.SYSLUMODES w bazie danych komunikacji DB2 for MVS/ESA.

DSESLIM=20

Całkowita liczba sesji (zwycięskich i pokonanych), które można uruchomić dla nazwy określonej grupy trybów, między DB2 for MVS/ESA i innym systemem rozproszonym. Parametr DSESLIM zawiera wartość domyślną dla przetwarzania CNOS. Można go przesłonić dla dowolnego partnera, dodając wiersz do tabeli SYSIBM.SYSLUMODES w bazie danych komunikacji DB2 for MVS/ESA.

Jeśli partner nie może obsługiwać liczby sesji podanej w parametrach DSESLIM, DMINWNL lub DMINWNR, proces CNOS negocjuje nową wartość dla tych parametrów, akceptowalną dla partnera.

EAS=9999

Szacunkowa całkowita liczba sesji wymaganych przez tę jednostkę logiczną VTAM.

MODETAB=RDBMODES

Określa tabelę VTAM MODE, w której znajdują się wszystkie nazwy trybów DB2 for MVS/ESA.

PRTCT=PSWDBD1

Określa hasło VTAM, które ma być użyte, gdy DB2 for MVS/ESA próbuje łączyć się z VTAM. Jeśli parametr PRTCT został pominięty, hasło nie jest wymagane i można pominąć parametr PASSWORD= w programie narzędziowym obsługującym wykaz protokołu zmian DB2 for MVS/ESA.

SECACPT=ALREADYV

Określa najwyższą wartość ochrony poziomu konwersacji w SNA akceptowaną przez system DB2 for MVS/ESA przy przyjmowaniu żądań w stosunku do rozproszonej bazy danych z serwera zdalnego. Parametr ALREADYV wskazuje, że dany system DB2 for MVS/ESA może akceptować trzy opcje ochrony sesji SNA z innych systemów DRDA, które żądają danych z tego systemu DB2 for MVS/ESA:

- SECURITY=SAME (sprawdzone uprzednio żądanie zawierające tylko identyfikator użytkownika wysyłającego żądanie).

- SECURITY=PGM (żądanie zawierające identyfikator użytkownika wysyłającego żądanie i jego hasło).
- SECURITY=NONE (żądanie nie zawierające żadnych informacji). DB2 for MVS/ESA odrzuca żądania DRDA zawierające specyfikację SECURITY=NONE.

Najlepiej zawsze podawać SECACPT=ALREADYV, ponieważ poziom ochrony konwersacji SNA dla każdego partnera DB2 for MVS/ESA jest pobierany z bazy danych komunikacji DB2 for MVS/ESA (kolumna USERSECURITY tabeli SYSIBM.SYSLUNAMES). Parametr SECACPT=ALREADYV umożliwia największą elastyczność w wyborze wartości dla USERSECURITY.

VERIFY=NONE

Określa poziom ochrony sesji SNA (weryfikacja jednostki logicznej) wymagany przez dany system DB2 for MVS/ESA. Wartość NONE wskazuje, że weryfikacja partnerskiej jednostki logicznej nie jest wymagana.

W DB2 for MVS/ESA nie ma ograniczeń w wyborze wartości dla parametru VERIFY. W sieciach niezaufanych zalecane jest używanie VERIFY=REQUIRED. Wartość ta powoduje, że VTAM odrzuca partnerów, którzy nie mogą wykonać weryfikacji partnerskiej jednostki logicznej. Jeśli użytkownik wybierze wartość VERIFY=OPTIONAL, VTAM przeprowadzi weryfikację partnerskiej jednostki logicznej tylko wobec tych partnerów, którzy zapewniają odpowiednią obsługę.

VPACING=2

Ustawia wartość pacingu VTAM na 2.

SYNCLVL=SYNCPT

Oznacza, że DB2 for MVS/ESA jest w stanie obsługiwać zatwierdzanie dwufazowe. VTAM używa tej informacji, aby przekazać partnerowi, że zatwierdzanie dwufazowe jest dostępne. Podanie parametru spowoduje, że DB2 for MVS/ESA automatycznie użyje zatwierdzania dwufazowego, jeśli tylko partner jest w stanie je obsłużyć.

ATNLOSS=ALL

Wskazuje, że DB2 for MVS/ESA musi być każdorazowo informowany o zakończeniu sesji VTAM. Umożliwia to wykonywanie przez DB2 for MVS/ESA resynchronizacji SNA, gdy jest to potrzebne.

Parametry DSESLIM, DMINWNL i DMINWNR umożliwiają ustanowienie domyślnego limitu liczby sesji VTAM dla wszystkich partnerów. W przypadku partnerów o szczególnych wymaganiach dotyczących limitu liczby sesji można użyć tabeli SYSIBM.SYSLUMODES w celu przesłonięcia domyślnej wartości limitu liczby sesji. Można na przykład podać domyślną wartość limitu liczby sesji VTAM, która jest odpowiednia dla systemów OS/2. W przypadku innych partnerów, aby zdefiniować żądane limity liczby sesji, można utworzyć wiersze w tabeli SYSIBM.SYSLUMODES. Rozważmy przykładowe wartości:

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

Parametry te umożliwiają każdemu partnerowi utworzenie czterech sesji z DB2 for MVS/ESA, gdzie partner jest zwycięzcą rywalizacji w każdej sesji. Ponieważ OS/2 tworzy konwersacje jednostki logicznej 6.2 z DB2 for MVS/ESA, ustanawiając OS/2 zwycięzcą rywalizacji w sesjach, użytkownik uzyskuje niewielki wzrost wydajności. Jeśli sesja OS/2 jest zwycięzcą rywalizacji, nie musi zabiegać o pozwolenie na uruchomienie nowej konwersacji jednostki logicznej 6.2.

Definiowanie systemów zdalnych

Jeśli aplikacja DB2 for MVS/ESA żąda danych z systemu zdalnego, DB2 for MVS/ESA przeszukuje tabele baz danych komunikacji, aby znaleźć informacje na temat systemu zdalnego m.in.:

- nazwę jednostki logicznej i programu transakcyjnego (TPN),
- informacje ochrony sieci wymagane przez miejsca zdalne,
- limity liczby sesji i nazwy trybów używane przy komunikacji z systemami zdalnymi.

Baza danych komunikacji jest grupą tabel SQL zarządzanych przez administratora systemu DB2 for MVS/ESA. Administrator DB2 for MVS/ESA musi użyć SQL, aby wstawić wiersze do bazy danych komunikacji w celu opisania każdego potencjalnego partnera DRDA. Baza danych komunikacji składa się z pięciu tabel:

1. **SYSIBM.SYSLOCATIONS**

   Tabela ta umożliwia DB2 for MVS/ESA określenie nazwy jednostki logicznej i nazwy programu transakcyjnego (TPN) dla każdej nazwy RDB_NAME wybranej przez aplikację DB2 for MVS/ESA. Tabela składa się z następujących kolumn:

   LOCATION
   Nazwa systemu zdalnego RDB_NAME. DB2 for MVS/ESA ogranicza wartość RDB_NAME do 16 bajtów, co zmniejsza o dwa bajty 18-bajtowy limit zdefiniowany w DRDA.

   LOCTYPE
   Kolumna obecnie nieużywana; musi być pusta.

   LINKNAME
   Nazwa jednostki logicznej systemu zdalnego.

   LINKATTR
   Nazwa programu transakcyjnego systemu zdalnego. Jeśli system zdalny jest systemem DB2 for MVS/ESA lub używa domyślnej wartości TPN DRDA (X'07F6C4C2'[1]), podając TPN można użyć łańcucha pustego, ponieważ DB2 for MVS/ESA automatycznie wybiera poprawną wartość.

   Jeśli system zdalny wymaga podania wartości TPN innej niż wartość domyślna TPN, należy podać ją w tym miejscu.

1. Ta wartość TPN dotyczy *obecnie* DB2 for VM.

2. **SYSIBM.SYSLUNAMES**

   Tabela ta definiuje atrybuty sieciowe systemów zdalnych. Tabela składa się z następujących kolumn:

   LUNAME
   Nazwa jednostki logicznej systemu zdalnego.

   SYSMODENAME
   Nazwa trybu logowania VTAM używana przy ustanawianiu konwersacji *międzysystemowej* DB2 for MVS/ESA-z-DB2 for MVS/ESA dla obsługi serwera pomocniczego DB2 for MVS/ESA (dostęp sterowany przez system). Wartość pusta w tej kolumnie oznacza, że dla konwersacji w systemie DB2 for MVS/ESA powinna być użyta wartość IBMDB2LM.

   USERSECURITY
   Opcje akceptowane przez ochronę sieci wymagane dla systemu zdalnego, gdy system DB2 for MVS/ESA działa jako serwer dla systemu zdalnego (wymagania w zakresie *ochrony połączeń przychodzących*).

   ENCRYPTPSWDS
   Określa, czy hasła wymieniane przy użyciu tego parametru są szyfrowane. Hasła szyfrowane są obsługiwane tylko przez requestery i serwery DB2 for MVS/ESA.

   MODESELECT
   Określa, czy w celu wybrania pozycji trybu logowania VTAM (nazwy trybu) na podstawie użytkownika i aplikacji wysyłającej żądanie jest używana tabela SYSIBM.SYSMODESELECT. Jeśli ta kolumna zawiera 'Y', do uzyskania nazwy trybu dla każdego wychodzącego żądania w stosunku do rozproszonej bazy danych jest używana tabela SYSIBM.SYSMODESELECT.

   Jeśli MODESELECT zawiera jakąkolwiek wartość różną od 'Y', dla żądań dostępu sterowanych przez system jest używana nazwa trybu IBMDB2LM, a dla żądań DRDA - nazwa trybu IBMRDB.

   Kolumna MODESELECT umożliwia ustawienie priorytetów żądań dotyczących rozproszonych baz danych przez podanie klasy usług (COS) VTAM związanej z nazwą trybu.

   USERNAMES
   Wymagany poziom sprawdzania źródła i translacji identyfikatora użytkownika. Kolumna ta zawiera także parametry ochrony używane przez system DB2 for MVS/ESA podczas żądań danych od partnera zdalnego (wymagania w zakresie *ochrony połączeń wychodzących*).
   NAZWY_UŻYTKOWNIKÓW mogą przyjmować wartość I, O lub B.

3. **SYSIBM.SYSLUMODES**

Tabela ta jest używana w celu zdefiniowania limitu liczby sesji jednostki logicznej 6.2 (limitów CNOS) dla wszystkich systemów partnerskich. Tabela składa się z następujących kolumn:

LUNAME
Nazwa jednostki logicznej systemu zdalnego.

MODENAME
Nazwa trybu logowania VTAM, którego limity są podawane. Wartość pusta powoduje przyjęcie wartości domyślnej IBMDB2LM kolumny MODENAME.

CONVLIMIT
Maksymalna liczba aktywnych konwersacji między lokalnym systemem DB2 for MVS/ESA i systemem zdalnym dla tego trybu logowania. Wartość ta jest używana do przesłonięcia parametru DSESLIM w instrukcji definicji APPL VTAM dla trybu logowania, który dostarcza domyślne wartości limitów liczby sesji dla DB2 for MVS/ESA.

Wartość wybrana w CONVLIMIT jest używana podczas działania procesów CNOS w celu ustawienia wartości DMINWNR i DMINWNL na CONVLIMIT/2.

AUTO Określa, czy przetwarzanie CNOS i wstępny przydział sesji są inicjowane automatycznie podczas uruchamiania DDF, czy są odraczane do czasu pierwszego odniesienia do nazwy jednostki logicznej przy użyciu tego trybu logowania.

4. **SYSIBM.SYSMODESELECT**

Tabela ta umożliwia podanie różnych nazw trybów dla użytkowników indywidualnych i aplikacji DB2 for MVS/ESA. Ponieważ każda nazwa trybu VTAM może mieć związaną z nią klasę usług (COS), można użyć tej tabeli do przypisania priorytetów transmisji sieciowej do aplikacji obsługujących rozproszone bazy danych przy użyciu kombinacji kolumn AUTHID, PLANNAME i LUNAME. Tabela składa się z następujących kolumn:

AUTHID
ID autoryzowanego użytkownika DB2 for MVS/ESA (ID użytkownika). Wartością domyślną jest wartość pusta, co oznacza, że podana nazwa trybu logowania odnosi się do wszystkich identyfikatorów autoryzowanego użytkownika.

PLANNAME
Nazwa planu związana z aplikacją żądającą dostępu do zdalnego systemu baz danych. Wartością domyślną jest wartość pusta, co oznacza, że podana nazwa trybu logowania odnosi się do wszystkich nazw planów. Nazwą planu dla komendy BIND PACKAGE jest DSNBIND.

LUNAME
Nazwa jednostki logicznej związana z systemem zdalnym baz danych.

MODENAME

Nazwa trybu logowania VTAM, który ma być użyty podczas routingu żądania rozproszonej bazy danych do wskazanego systemu zdalnego. Wartością domyślną jest wartość pusta, co oznacza, że dla konwersacji o dostępie sterowanym przez system powinna zostać użyta wartość IBMDB2LM, a dla konwersacji DRDA - wartość IBMRDB.

5. **SYSIBM.SYSUSERNAMES**

Tabela ta jest używana do zarządzania nazwami użytkowników przez dostarczanie haseł, translacji nazw i sprawdzanie źródeł. DB2 for MVS/ESA odwołuje się do nazwy użytkownika jako do identyfikatora autoryzowanego użytkownika. Większość innych produktów odwołuje się do tej nazwy jako do identyfikatora użytkownika.

Za pomocą tej tabeli użytkownik może użyć translacji nazw w celu wymuszenia użycia różnych wartości dla identyfikatora użytkownika SNA i ID autoryzowanego użytkownika DB2 for MVS/ESA. Proces translacji nazwy może zostać użyty dla żądań skierowanych do systemu zdalnego (żądań *wychodzących*) i dla żądań przychodzących z systemu zdalnego (żądań *przychodzących*). Jeśli hasła nie są szyfrowane, tabela ta jest źródłem haseł użytkowników, gdy zarówno ID użytkownika, jak i hasło są wysyłane do miejsca zdalnego. Tabela składa się z następujących kolumn:

TYPE Opis sposobu użycia wiersza (czy jest to wiersz opisujący translacje nazw dla wychodzących lub przychodzących żądań sprawdzania źródeł).

AUTHID

W przypadku translacji nazw wychodzących należy wykonać translację ID autoryzowanego użytkownika DB2 for MVS/ESA. W przypadku translacji nazw przychodzących należy wykonać translację ID użytkownika SNA. W każdym z tych przypadków wartość pusta AUTHID dotyczy wszystkich identyfikatorów autoryzowanych użytkowników i identyfikatorów użytkowników.

LUNAME

Nazwa jednostki logicznej (LU) systemu zdalnego, którego dotyczy dany wiersz. Jeśli jest to wartość pusta, wartość NEWAUTHID dotyczy wszystkich systemów.

NEWAUTHID

Nowa nazwa użytkownika (identyfikator użytkownika SNA lub ID autoryzowanego użytkownika DB2 for MVS/ESA). Jeśli jest to wartość pusta, nie należy wykonywać translacji identyfikatora.

PASSWORD

Hasło używane w konwersacji dotyczącej przydziału, jeśli hasła nie są szyfrowane (w SYSIBM.SYSLUNAMES ENCRYPTPSWDS = 'N'). Jeśli hasła są szyfrowane, kolumna ta jest ignorowana.

Definiowanie komunikacji

VTAM jest menedżerem komunikacji dla systemów MVS. VTAM akceptuje słowa jednostki logicznej 6.2 DB2 for MVS/ESA i wykonuje ich translację na strumienie danych jednostki logicznej 6.2, które mogą być transmitowane przez sieć. Ponieważ VTAM komunikuje się z aplikacjami partnerskimi zdefiniowanymi w bazie danych DB2 for MVS/ESA należy podać VTAM następujące informacje:

- Nazwę jednostki logicznej dla każdego serwera.

  Jeśli DB2 for MVS/ESA komunikuje się z VTAM, w celu identyfikacji miejsca docelowego DB2 for MVS/ESA może przesyłać do VTAM tylko nazwę jednostki logicznej (nie NETID.LUNAME). Nazwa ta musi być unikalna wśród nazw jednostek logicznych znanych lokalnemu systemowi VTAM, co pozwala VTAM określić zarówno NETID, jak i nazwę jednostki logicznej na podstawie wartości nazwy jednostki logicznej przekazanej przez DB2 for MVS/ESA. Jeśli nazwy jednostki logicznej są unikalne w sieci SNA przedsiębiorstwa, ułatwia to znacznie definiowanie zasobów VTAM. Czasami jest to jednak niemożliwe. Jeśli nazwy jednostek logicznych w sieci SNA nie są unikalne, należy użyć translacji nazw jednostek logicznych VTAM, tak aby utworzyć poprawną kombinację dla nieunikalnej nazwy jednostki logicznej. Opis tego procesu można znaleźć w rozdziale “Resource Name Translation” podręcznika *VTAM Network Implementation Guide*.

  Sposób umieszczenia i składnia definicji VTAM używanych w celu określenia nazw zdalnych jednostek logicznych są w dużym stopniu uzależnione od sposobu, w jaki system zdalny jest logicznie i fizycznie połączony z lokalnym systemem VTAM.
- Wielkość RU, wielkość okna pacingu i klasę usług dla każdego trybu. Dla każdej nazwy trybu podanej w bazie danych komunikacji należy utworzyć tabelę trybów VTAM. Należy również zdefiniować parametry IBMRDB i IBMDB2LM.
- Profile VTAM i RACF dla algorytmu weryfikacji jednostki logicznej, jeśli użytkownik zamierza korzystać z weryfikacji partnerskiej jednostki logicznej.

Ustawianie wielkości RU i pacingu

Pozycje tabeli trybów VTAM zawierają wielkości jednostek RU i liczby pacingu. Błędy popełnione przy definiowaniu tych wartości mogą negatywnie wpływać na wszystkie aplikacje VTAM.

Po wybraniu wielkości RU, limitów liczby sesji i liczb pacingu należy koniecznie zastanowić się nad wpływem tych wartości na sieć VTAM. Podczas instalowania nowego systemu obsługującego rozproszone bazy danych należy sprawdzić następujące elementy:

- W przypadku połączeń CTC VTAM CTC należy sprawdzić, czy parametr MAXBFRU jest wystarczająco duży, aby obsłużył wielkość RU plus 29 bajtów, które VTAM dodaje do nagłówka żądania SNA i nagłówka transmisji. MAXBFRU jest mierzony w jednostkach o wielkości 4 kB, więc MAXBFRU musi mieć co najmniej wartość 2, aby zmieścić jednostkę RU wielkości 4 kB.
- W przypadku połączeń NCP należy się upewnić, czy wartość MAXDATA jest odpowiednia, aby obsłużyć wielkość RU plus 29 bajtów. Jeśli określono wielkość RU 4 kB, MAXDATA musi mieć co najmniej wartość 4125.

Przy określaniu parametru NCP MAXBFRU należy wybrać wielkość, która może pomieścić jednostkę RU plus 29 bajtów. W przypadku połączeń NCP parametr MAXBFRU określa liczbę buforów we/wy VTAM, które mogą być używane, aby przechować jednostkę informacyjną ścieżki (PIU). Jeśli zostanie wybrana wielkość buforu IOBUF 441, MAXBFRU=10 poprawnie przetworzy jednostki RU o wielkości 4 kB, ponieważ 10*441 jest większe od 4096+29.

- W podręczniku *DRDA Connectivity Guide* opisano, jak określić wpływ rozproszonej bazy danych na pulę IOBUF VTAM. Jeśli używa się zbyt dużej części zasobów puli IOBUF, wydajność aplikacji VTAM zostaje obniżona.

Zapewnianie ochrony

Jeśli system zdalny przetwarza rozproszoną bazę danych w imieniu aplikacji SQL, musi być możliwe spełnienie wymogów ochrony requestera aplikacji, serwera aplikacji i łączącej je sieci. Wymagania te należą do co najmniej jednej z następujących kategorii:

- wybór nazw użytkowników,
- parametry ochrony sieci,
- ochrona menedżera baz danych,
- ochrona wymuszona przez zewnętrzny podsystem ochrony,
- reprezentacja danych.

Wybieranie nazw użytkowników

W systemach MVS każdemu użytkownikowi jest przypisany *ID użytkownika* składający się z 1 do 8 znaków. Wartość identyfikatora użytkownika musi być unikalna w danym systemie MVS, lecz może nie być unikalna w sieci SNA. Na przykład w systemie NEWYORK może istnieć użytkownik o nazwie JONES i inny użytkownik o tej samej nazwie w systemie DALLAS. Jeśli tych dwóch użytkowników to ta sama osoba, konflikt nie wystąpi. Jeśli natomiast JONES w DALLAS jest inną osobą niż JONES w NEWYORK, sieć SNA (i konsekwentnie systemy obsługujące rozproszone bazy danych w sieci) nie są w stanie rozróżnić tych użytkowników. Jeśli sytuacja ta nie ulegnie zmianie, JONES w DALLAS będzie korzystać z uprawnień nadanych użytkownikowi JONES w NEWYORK.

Aby wyeliminować konflikty nazewnictwa, DB2 for MVS/ESA obsługuje translacje nazw użytkowników. Jeśli aplikacja requestera aplikacji DB2 for MVS/ESA formułuje żądanie dotyczące rozproszonej bazy danych, DB2 for MVS/ESA wykonuje translację nazwy, o ile baza danych komunikacji zawiera wymaganie wykonania *translacji nazwy wychodzącej*. Jeśli wybrana zostanie translacja nazwy wychodzącej, DB2 for MVS/ESA wymusi przesłanie hasła przy każdym żądaniu wychodzącym dotyczącym rozproszonej bazy danych.

Translacja nazw wychodzących w DB2 for MVS/ESA jest uaktywniana przez ustawienie kolumny USERNAMES w tabeli SYSIBM.SYSLUNAMES na wartość 'O' lub 'B'. Jeśli kolumna ta jest ustawiona na 'O', dla żądań wychodzących jest

wykonywana translacja nazw użytkowników. Jeśli jest ustawiona na 'B', translacja nazw użytkowników jest wykonywana zarówno dla żądań przychodzących, jak i wychodzących.

Ponieważ autoryzacja DB2 for MVS/ESA zależy zarówno od identyfikatora użytkownika lokalnego, jak i identyfikatora użytkownika właściciela planu lub pakietu DB2 for MVS/ESA, proces translacji nazwy użytkownika lokalnego jest wykonywany dla identyfikatora użytkownika lokalnego, użytkownika właściciela planu i użytkownika właściciela pakietu.[2] Proces translacji nazw przeszukuje tabelę SYSIBM.SYSUSERNAMES w następującej kolejności, aby wyszukać wiersz, który jest zgodny z jednym z następujących wzorców (TYPE.AUTHID.LUNAME):

1. O.AUTHID.LUNAME — Reguła translacji dla określonego użytkownika do określonego systemu partnerskiego.
2. O.AUTHID.puste — Reguła translacji dla określonego użytkownika do dowolnego systemu partnerskiego.
3. O.puste.LUNAME — Reguła translacji dla dowolnego użytkownika do określonego systemu partnerskiego.

Jeśli nie odnaleziono wierszy pasujących do wzorca, DB2 for MVS/ESA odrzuca żądanie skierowane do rozproszonej bazy danych. Jeśli wiersz zostanie odnaleziony, jako ID autoryzowanego użytkownika jest używana wartość kolumny NEWAUTHID. (Wartość pusta w kolumnie NEWAUTHID oznacza, że oryginalna nazwa jest używana bez translacji).

Rozważmy przykład omawiany wcześniej. Użytkownikowi JONES z NEWYORK należy nadać inną nazwę (NYJONES), gdy JONES wysyła żądanie dotyczące rozproszonej bazy danych do DALLAS. Załóżmy, że aplikacja używana przez użytkownika JONES jest własnością DSNPLAN (właściciel planu DB2 for MVS/ESA) i nie należy wykonywać translacji identyfikatora użytkownika, gdy jest on przesyłany do DALLAS. Instrukcje SQL, których należy użyć, aby określić reguły translacji nazwy w bazie danych komunikacji, są przedstawione na Rys. 6 na stronie 20.

2. Jeśli żądanie jest wysyłane do serwera DB2 for MVS/ESA, translacja nazwy jest także wykonywana dla właściciela pakietu i właściciela planu. Nazwy właściciela planu i właściciela pakietu nie są związane z hasłem.

```
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');
```

Rysunek 6. Instrukcje SQL dla translacji nazw wychodzących

Wynikowe tabele bazy danych komunikacji przedstawiono na Rys. 7 na stronie 21:

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	JONES	LUDALLAS	NYJONES	JONESPWD
0	DSNPLAN	LUDALLAS		PLANPWD

Rysunek 7. Translacja nazw wychodzących

Ochrona sieci

Po wybraniu nazw użytkowników reprezentujących aplikację zdalną requester aplikacji musi dostarczyć wymagane informacje dotyczące ochrony sieci jednostki logicznej 6.2 (LU 6.2). Jednostka logiczna 6.2 udostępnia trzy główne opcje ochrony sieci:

- Ochrona na poziomie sesji, sterowana przez parametr VERIFY w instrukcji APPL VTAM APPL. Sposób określania opcji ochrony na poziomie sesji przedstawiono po Rys. 5 na stronie 10.
- Ochrona na poziomie konwersacji, sterowana przez zawartość tabeli SYSIBM.SYSLUNAMES.
- Szyfrowanie danych, obsługiwane tylko przez VTAM 3.4 i późniejsze wydania VTAM.

Serwer aplikacji jest odpowiedzialny za zarządzanie zasobami baz danych, dlatego decyduje o tym, które opcje ochrony są wymagane od requestera aplikacji. Należy zapisać wymagania poziomu konwersacji każdego serwera aplikacji w tabeli SYSIBM.SYSLUNAMES, ustawiając kolumnę USERNAMES tabeli SYSIBM.SYSLUNAMES, tak aby oddawała wymagania serwera aplikacji.

Możliwe opcje ochrony konwersacji SNA:

SECURITY=SAME

Zwana również ochroną sprawdzoną uprzednio, ponieważ identyfikator użytkownika jest wysyłany do systemu zdalnego (hasło nie jest wysyłane). Tego poziomu ochrony konwersacji należy użyć, jeśli kolumna USERNAMES tabeli SYSIBM.SYSLUNAMES nie zawiera wartości 'O' lub 'B'.

Ponieważ DB2 for MVS/ESA dopasowuje translację nazwy użytkownika do ochrony konwersacji wychodzącej, nie pozwala on na użycie opcji SECURITY=SAME, gdy translacja wychodzącej nazwy użytkownika jest uaktywniona.

SECURITY=PGM

Powoduje wysłanie identyfikatora użytkownika i hasła do systemu zdalnego w celu sprawdzenia poprawności. Tej opcji ochrony należy użyć, jeśli kolumna USERNAMES tabeli SYSIBM.SYSLUNAMES zawiera wartość 'O' albo 'B'.

W zależności od opcji podanej w tabeli SYSIBM.SYSLUNAMES, DB2 for MVS/ESA uzyskuje hasło użytkownika z dwóch różnych źródeł:

- Hasła niezaszyfrowane są uzyskiwane z kolumny PASSWORD tabeli SYSIBM.SYSUSERNAMES. DB2 for MVS/ESA pobiera hasła z tabeli SYSIBM.SYSUSERNAMES, gdy kolumna ENCRYPTPSWDS tabeli SYSIBM.SYSLUNAMES nie jest ustawiona na 'Y'. Hasła uzyskane z tego źródła mogą być przenoszone do dowolnego serwera aplikacji DRDA.

  Rys. 8 definiuje hasła dla użytkowników SMITH i JONES. Kolumna LUNAME w przykładzie zawiera wartości puste, więc hasła te są używane dla wszystkich systemów, z których próbują skorzystać SMITH i JONES.

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

Rysunek 8. Wysyłanie haseł do systemów zdalnych

- Hasła zaszyfrowane są wysyłane do miejsc zdalnych, jeśli kolumna ENCRYPTPSWDS tabeli SYSIBM.SYSLUNAMES zawiera 'Y'. Hasła zaszyfrowane są pobierane z RACF (lub produktu równoważnego) i mogą być interpretowane jedynie przez inny system DB2 for MVS/ESA. Podczas

komunikowania się z systemem innym niż DB2 for MVS/ESA nie należy ustawiać kolumny ENCRYPTPSWDS na 'Y'.

DB2 for MVS/ESA przeszukuje tabelę SYSIBM.SYSUSERNAMES, aby określić, jaki identyfikator użytkownika (wartość NEWAUTHID) ma być przesłany do systemu zdalnego. Ta poddana translacji nazwa jest używana do pobrania hasła RACF. Jeśli użytkownik nie chce wykonywać translacji nazw, musi utworzyć wiersze w tabeli SYSIBM.SYSUSERNAMES, które spowodują wysłanie nazw bez translacji. Wykonanie instrukcji przedstawionych na Rys. 9 pozwala na wysłanie żądań do LUDALLAS i LUNYC bez translacji nazwy użytkownika (ID użytkownika).

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

Rysunek 9. Wysyłanie haseł zaszyfrowanych do systemów zdalnych

SECURITY=NONE

Opcja ta nie jest obsługiwana przez sieć DRDA, dlatego DB2 for MVS/ESA jej nie obsługuje.

Ochrona menedżera baz danych

Jednym ze sposobów zapewnienia przez requester aplikacji ochrony rozproszonej bazie danych jest translacja nazw połączeń przychodzących, co opisano w sekcji “Wybieranie nazw użytkowników” na stronie 18. Aby sterować dostępem do każdego serwera aplikacji, można użyć translacji nazw wychodzących wedle zasady tożsamości użytkownika wysyłającego żądanie i aplikacji wysyłającej żądanie. Inne sposoby używane przez requester aplikacji DB2 for MVS/ESA ochrony systemu rozproszonego:

Wiązanie aplikacji zdalnych

Użytkownicy wiążą aplikacje zdalne na serwerze aplikacji, wykorzystując komendę DB2 for MVS/ESA BIND PACKAGE. DB2 for MVS/ESA *nie* ogranicza użycia komendy BIND PACKAGE na requesterze. Użytkownik nie może jednak użyć pakietu zdalnego, dopóki pakiet ten jest włączony do planu DB2 for MVS/ESA. DB2 for MVS/ESA *ogranicza* użycie komendy BIND PLAN. Użytkownik nie może dodać pakietu zdalnego do planu, dopóki nie zostaną mu nadane uprawnienia BIND lub BINDADD przy użyciu instrukcji GRANT DB2 for MVS/ESA.

Podczas wiązania pakietu należy skorzystać z opcji ENABLE/DISABLE, aby określić, czy dany pakiet ma być używany przez TSO, CICS/ESA, IMS/ESA czy przez podsystem zdalny DB2 for MVS/ESA.

Wykonywanie aplikacji zdalnych

Aby użytkownik DB2 for MVS/ESA mógł uruchomić aplikację zdalną, musi mieć uprawnienia do uruchamiania planu DB2 for MVS/ESA związanego z aplikacją. Właściciel planu DB2 for MVS/ESA ma automatycznie uprawnienia do jego uruchomienia. Innym użytkownikom można nadać uprawnienia do uruchamiania planu używając, instrukcji DB2 for MVS/ESA GRANT EXECUTE. W ten sposób właściciel aplikacji obsługującej rozproszone bazy danych może kontrolować korzystanie z aplikacji dla każdego użytkownika osobno.

Podsystem ochrony

Zewnętrznym podsystemem ochrony systemów MVS jest RACF lub inne produkty, które obsługują interfejs kompatybilny z RACF. Requester aplikacji DB2 for MVS/ESA nie ma bezpośrednich odwołań do zewnętrznego podsystemu ochrony, z wyjątkiem obsługi hasła szyfrowanego opisanej w sekcji “Ochrona sieci” na stronie 69. Zewnętrzny podsystem ochrony jest jednak wykorzystywany pośrednio w requesterze aplikacji w następujących sytuacjach:

- Produkt odpowiedzialny za podłączenie użytkownika do DB2 for MVS/ESA korzysta z zewnętrznego podsystemu ochrony w celu sprawdzenia poprawności użytkownika (identyfikatora i hasła). Dzieje się to przed podłączeniem użytkownika do DB2 for MVS/ESA. Jak już powiedziano, CICS/ESA, TSO i IMS/ESA są przykładami produktów, które podłączają użytkowników do DB2 for MVS/ESA.
- Przy korzystaniu z ochrony na poziomie sesji SNA (przez parametr VERIFY instrukcji APPL produktu VTAM DB2 for MVS/ESA) zewnętrzny podsystem ochrony jest wywoływany przez VTAM w celu sprawdzenia poprawności systemu zdalnego.

Reprezentacja danych

DB2 for MVS/ESA jest dostarczany z domyślnym identyfikatorem kodowanego zestawu znaków (CCSID) instalacji o wartości 500. Wartość ta prawdopodobnie *nie* jest poprawna w przypadku instalacji użytkownika.

Podczas instalowania DB2 for MVS/ESA należy zmienić ustawienie identyfikatora CCSID na CCSID znaków tworzonych i wysyłanych do DB2 for MVS/ESA przez urządzenia wejściowe w konkretnym miejscu. Identyfikator ten jest zwykle uzależniony od używanego języka. Jeśli identyfikator CCSID instalacji jest niepoprawny, konwersja znaków będzie prowadziła do uzyskiwania nieprawidłowych wyników. *IBM DB2 Connect Podręcznik użytkownika* zawiera listę identyfikatorów CCSID obsługiwanych dla każdego języka.

Należy sprawdzić, czy podsystem DB2 for MVS/ESA ma możliwość konwersji każdego CCSID serwera aplikacji na instalacyjny CCSID podsystemu DB2 for MVS/ESA. DB2 for MVS/ESA obsługuje tabele konwersji dla najczęstszych kombinacji źródłowych i wynikowych CCSID, lecz nie dla każdej możliwej kombinacji. Jeśli zaistnieje taka

potrzeba, można dodać pozycje do zestawu dostępnych tabel i procedur konwersji. Więcej informacji na temat konwersji znaków DB2 for MVS/ESA można znaleźć w podręczniku *DB2 Administration Guide*.

Konfigurowanie serwera aplikacji

Obsługa serwera aplikacji w DB2 for MVS/ESA umożliwia działanie DB2 for MVS/ESA jako serwera requstera aplikacji DRDA. Requesterem aplikacji połączonym z serwerem aplikacji DB2 for MVS/ESA może być:

- requester DB2 for MVS/ESA;
- DB2 Connect wersja 7, który można uruchomić w systemie AIX, HP-UX, OS/2, SCO, Solaris, Linux, Windows 9x lub Windows NT;
- DB2 Universal Database Enterprise Edition wersja 6 lub DB2 Universal Database Extended - Enterprise Edition z obsługą DB2 Connect;
- requester produktu DDCS (Distributed Database Connection Services) wersja 2, który można uruchomić w systemie AIX, HP-UX, OS/2, Solaris, Windows 3.1, Windows 3.11 for Workgroups, Windows 95 lub Windows NT, a także SCO, SGI lub SINIX.;
- requester OS/400;
- requester DB2 for VM;
- każdy produkt, który obsługuje protokoły requestera aplikacji DRDA.

W przypadku każdego połączonego requestera aplikacji serwer aplikacji DB2 for MVS/ESA obsługuje dostęp do bazy danych w następujący sposób:

- Requester aplikacji może mieć dostęp do tabel zapisanych na serwerze aplikacji DB2 for MVS/ESA. Przed uruchomieniem aplikacji requester aplikacji musi utworzyć pakiet na serwerze aplikacji DB2 for MVS/ESA. Serwer aplikacji DB2 for MVS/ESA używa tego pakietu do umiejscowienia instrukcji SQL aplikacji podczas jej wykonywania.
- Requester aplikacji może poinformować serwer aplikacji DB2 for MVS/ESA o konieczności ograniczenia dostępu do czynności tylko do odczytu, jeśli połączenie requester-serwer DRDA nie obsługuje procesu zatwierdzania dwufazowego. Na przykład requester DB2 for MVS/ESA z interfejsem (front end) CICS poinformuje serwer aplikacji DB2 for MVS/ESA, że aktualizacja jest niedopuszczalna.
- Requester aplikacji może mieć także dostęp do tabel zapisanych w systemach innych niż DB2 for MVS/ESA w sieci przy użyciu dostępu bezpośredniego do systemu. Dostęp bezpośredni do systemu umożliwia requesterowi aplikacji nawiązywanie połączeń z wieloma systemami baz danych w pojedynczej jednostce pracy.

Dostarczanie informacji sieciowych

W przypadku serwera aplikacji DB2 for MVS/ESA, w celu odpowiedniego przetwarzania żądania rozproszonej bazy danych należy wykonać następujące czynności:

1. Zdefiniować serwer aplikacji dla lokalnego menedżera komunikacji.

2. Zdefiniować każdy możliwy docelowy serwer pomocniczy, tak aby serwer aplikacji DB2 for MVS/ESA mógł przekierować żądania SQL do ich miejsc docelowych.
3. Udostępnić niezbędną ochronę.
4. Udostępnić reprezentację danych.

Definiowanie serwera aplikacji

Aby serwer aplikacji mógł otrzymywać żądania rozproszonej bazy danych, musi być zdefiniowany w lokalnym menedżerze komunikacji i mieć unikalną nazwę RDB_NAME. Aby odpowiednio zdefiniować serwer aplikacji, należy:

1. Wybrać nazwę LU i RDB_NAME, które mają być używane przez serwer aplikacji DB2 for MVS/ESA. Zapisywanie tych nazw w DB2 for MVS/ESA i VTAM odbywa się tak samo, jak opisano w sekcji “Definiowanie systemu lokalnego” na stronie 7. Parametr RDB_NAME wybrany dla DB2 for MVS/ESA musi być dostarczony wszystkim użytkownikom i requesterom aplikacji, którzy wymagają połączenia z serwerem aplikacji.
2. Zarejestrować wartość NETID.LUNAME serwera aplikacji DB2 for MVS/ESA z każdym requesterem aplikacji żądającym dostępu, tak aby mógł on kierować żądania SNA do serwera DB2 for MVS/ESA. Jest to ważne nawet, gdy requester aplikacji może wykonać dynamiczny routing sieciowy, ponieważ musi on znać nazwę NETID.LUNAME przed użyciem dynamicznego routingu sieciowego.
3. Udostępnić wartość domyślną DRDA TPN (X'07F6C4C2') każdemu requesterowi aplikacji, ponieważ DB2 for MVS/ESA używa tej wartości automatycznie.
4. Utworzyć pozycję w tabeli trybów VTAM dla każdej nazwy trybu, która jest wymagana przez requester aplikacji. Pozycje te opisują wielkość RU, wielkość okna pacing i klasę usługi dla nazwy trybu.
5. Zdefiniować limit liczby sesji dla requesterów aplikacji łączących serwer aplikacji DB2 for MVS/ESA. Instrukcja VTAM APPL definiuje domyślne limity liczby sesji dla wszystkich systemów partnerskich. Aby ustanowić unikalne wartości domyślne dla danego partnera, można użyć tabeli SYSIBM.SYSLUMODES dla bazy danych komunikacji (CDB).

   W sekcji “Ustawianie wielkości RU i pacingu” na stronie 17 omówiono sposób przeglądania sieci VTAM.
6. Utworzyć pozycje w DB2 for MVS/ESA CDB, aby określić, które requestery aplikacji można połączyć z serwerem aplikacji DB2 for MVS/ESA. Oto dwa podstawowe sposoby definiowania pozycji CDB requesterów aplikacji w sieci:
   a. W tabeli SYSIBM.SYSLUNAMES dodać wiersz zapewniający użycie wartości domyślnych dla każdej jednostki logicznej, która nie została specjalnie opisana w CDB (wiersz domyślny zawiera znaki puste w kolumnie LUNAME). Podejście to umożliwia definiowanie specyficznych wartości dla niektórych jednostek logicznych w sieci, gdy dla wszystkich innych są ustanawiane wartości domyślne.

      Można na przykład umożliwić systemowi DALLAS (innemu niż system DB2 for MVS/ESA) wysyłanie zweryfikowanych żądań rozproszonej bazy danych

(LU 6.2 SECURITY=SAME) jednocześnie z żądaniami wysłania haseł przez systemy menedżerów baz danych. Ponadto można nie zapisywać pozycji w CDB dla każdego systemu menedżera baz danych, zwłaszcza jeśli jest ich wiele. Rys. 10 przedstawia sposób użycia bazy danych komunikacji do podania SECURITY=SAME systemowi DALLAS, przy jednoczesnym wymuszaniu opcji SECURITY=PGM dla pozostałych requesterów.

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

Rysunek 10. Ustanawianie wartości domyślnych dla połączeń requestera aplikacji

b. Użyć CDB, aby indywidualnie nadać uprawnienia każdemu requesterowi aplikacji w sieci, ustawiając CDB na jeden z następujących sposobów:
   - Nie zapisywać wiersza domyślnego w SYSIBM.SYSLUNAMES. Gdy nie ma wiersza domyślnego (wiersz zawierający pustą nazwę jednostki logicznej), DB2 for MVS/ESA wymaga wiersza w SYSIBM.SYSLUNAMES zawierającego nazwę jednostki logicznej dla każdego requestera aplikacji, który próbuje się połączyć. Jeśli odpowiadający wiersz nie zostanie odnaleziony w CDB, requesterowi aplikacji zostanie odmówione prawo dostępu.
   - Zapisać wiersz domyślny w SYSIBM.SYSLUNAMES, który określa, że wymagane jest sprawdzanie źródła (come-from checking) (kolumna USERNAMES jest ustawiona na 'I' lub 'B'). Powoduje to, że DB2 for MVS/ESA ogranicza dostęp do requesterów aplikacji i użytkowników zidentyfikowanych w tabeli SYSIBM.SYSUSERNAMES, co opisano w sekcji “Sprawdzanie źródła żądania” na stronie 32. Tego sposobu można używać, jeśli reguły translacji nazw wymagają wiersza z pustą nazwą jednostki logicznej w SYSIBM.SYSLUNAMES, ale użytkownik nie chce, aby produkt DB2 for MVS/ESA używał tego wiersza do nieograniczonego dostępu do serwera aplikacji DB2 for MVS/ESA.

   Na Rys. 11 na stronie 28 nie ma wiersza zawierającego puste znaki w kolumnie LUNAME, tak więc DB2 for MVS/ESA uniemożliwia dostęp do jednostek logicznych innych niż LUDALLAS i 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', ' ');
```

Rysunek 11. Identyfikowanie indywidualnych połączeń requestera aplikacji

Definiowanie serwerów pomocniczych

DB2 for MVS/ESA nie implementuje serwera baz danych w sposób zdefiniowany w DRDA. Zamiast tego DB2 for MVS/ESA dostarcza serwery pomocnicze, które zapewniają dostęp do wielu systemów DB2 for MVS/ESA w pojedynczej jednostce pracy przy użyciu dostępu bezpośredniego do systemu.

Różnice dotyczące języka SQL: Język SQL obsługiwany przez dostęp bezpośredni do systemu różni się znacznie od zdalnej jednostki pracy DRDA:

- Instrukcja SQL CONNECT nie jest używana do nawiązywania połączenia z serwerem pomocniczym. W zamian dostęp do serwera jest uzyskiwany przez podawanie trzyczęściowej nazwy obiektu SQL. Na przykład następująca instrukcja SQL jest kierowana do serwera o dostępie bezpośrednim z systemu CHICAGO:

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

- Nie są dopuszczalne instrukcje SQL DDL (na przykład CREATE).
- Dostęp bezpośredni z systemu nie obsługuje wiązania zdalnego (na przykład BIND PACKAGE). Użytkownik nie musi więc przed próbą wykonania aplikacji wiązać aplikacji na serwerze o dostępie bezpośrednim.
- Wysyłane do serwera pomocniczego instrukcje mogą być statyczne lub dynamiczne, ale wszystkie są wywoływane dynamicznie. Dzieje się tak dlatego, że serwer pomocniczy nie ma planu lub pakietu zawierającego instrukcje aplikacji w języku SQL. Serwer nie może więc wybrać z góry ścieżki dostępu do bazy danych.
- Pojedyncza aplikacja SQL może mieć dostęp do wielu serwerów pomocniczych jednocześnie.
- Za pomocą instrukcji SQL dla dowolnego zakresu zatwierdzonego może być zaktualizowany więcej niż jeden system DB2 for MVS/ESA.
- Aplikacja może używać wielu konwersacji jednostki logicznej 6.2 z serwerem pomocniczym w jednym zakresie zatwierdzania. Serwer aplikacji DB2 for MVS/ESA tworzy zazwyczaj jedną konwersację jednostki logicznej 6.2 (LU 6.2) dla każdego zapytania SQL tylko do odczytu. Umożliwia to serwerowi pomocniczemu przewidywanie żądań FETCH aplikacji SQL i wysyłanie odpowiedzi, zanim aplikacja jej rzeczywiście zażąda.

Nazwy obiektów SQL: Gdy serwer aplikacji DB2 for MVS/ESA otrzyma żądanie SQL, analizuje nazwę obiektu SQL, aby określić, czy obiekt ten znajduje się w sieci. DB2 for MVS/ESA akceptuje jedno-, dwu- lub trzyczęściowe nazwy obiektów SQL, w których nazwa przybiera jedną z następujących form:

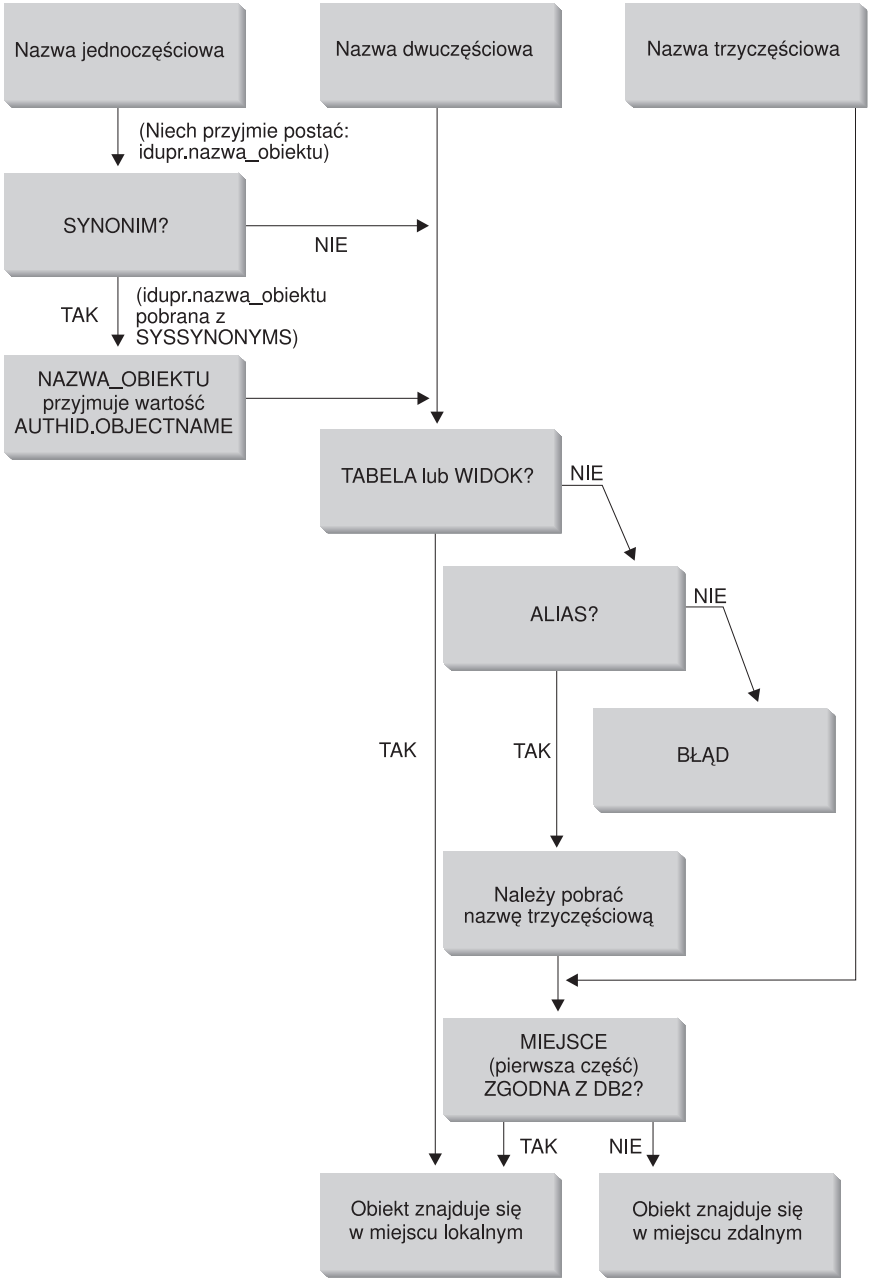
nazwa_obiektu określa nazwę tabeli, widoku, synonimu lub aliasu DB2 for MVS/ESA,

idupr.nazwa_obiektu określa właściciela obiektu oraz nazwę obiektu,

miejsce.id_autoryzowanych_użytkowników.nazwa_obiektu określa system, który jest właścicielem obiektu i użytkownika, który jest właścicielem obiektu oraz nazwę obiektu.

Jeśli nazwa miejsca (pierwsza część trzyczęściowej nazwy obiektu) jest zgodna z RDB_NAME lokalnego systemu DB2 for MVS/ESA, żądanie zidentyfikuje lokalny obiekt DB2 for MVS/ESA.

Jeśli nazwa miejsca jest niezgodna z nazwą RDB_NAME lokalnego systemu DB2 for MVS/ESA, serwer aplikacji DB2 for MVS/ESA ponownie skieruje żądanie do systemu zidentyfikowanego przez nazwę miejsca przy użyciu dostępu bezpośredniego do systemu. Systemem docelowym musi być inny system DB2 for MVS/ESA, ponieważ dostęp bezpośredni do systemu jest obsługiwany tylko między systemami DB2 for MVS/ESA. Dostęp bezpośredni do systemu nie obsługuje zdalnych funkcji wiązania. Aplikacje nie muszą więc być powiązane na serwerze przed wykonywaniem aplikacji. Rys. 12 na stronie 30 podsumowuje proces zastosowany przez DB2 for MVS/ESA do rozstrzygania nazw obiektów SQL.



Rysunek 12. Rozstrzygnięcie nazwy obiektu SQL przez DB2 for MVS/ESA

Definicja serwera: Aby serwer aplikacji DB2 for MVS/ESA ponownie skierował żądania SQL, należy zdefiniować każdy serwer pomocniczy w CDB i VTAM. Większość zdefiniowanych procesów jest podobna do tych, które opisano w sekcji “Definiowanie systemów zdalnych” na stronie 13. Aby połączyć serwery pomocnicze, należy:

1. W przypadku każdego serwera w CDB i VTAM zapisać wartości RDB_NAME i nazwę jednostki logicznej. Wartość TPN używana przez dostęp bezpośredni do systemu różni się od wartości domyślnej DRDA. Jednak różnica ta nie jest istotna, ponieważ DB2 for MVS/ESA automatycznie wybiera poprawną wartość.
2. W przypadku każdego serwera pomocniczego zdefiniować w SYSIBM.SYSLUNAMES wymagania dotyczące ochrony. Proces ten opisano w sekcji “Zapewnianie ochrony” na stronie 18.
3. Zdefiniować nazwę (lub nazwy) trybu użytą między serwerem aplikacji DB2 for MVS/ESA i serwerami pomocniczymi i umieścić ją w tabeli trybów VTAM. Domyślną nazwą trybu jest IBMDB2LM.
4. W przypadku każdego serwera pomocniczego zdefiniować limit liczby sesji. Proces ustalania limitu liczby sesji opisano w sekcji “Definiowanie systemu lokalnego” na stronie 7. Jednak dostęp bezpośredni do systemu może ustalić wiele konwersacji dla każdej aplikacji SQL. W przypadku połączeń o dostępie bezpośrednim można ustalić limity liczby sesji wyższe niż dla połączeń DRDA. Patrz rozdział “Connecting Distributed Database Systems” w podręczniku *DB2 Administration Guide*, aby uzyskać szczegółowe informacje na temat wyliczania liczby sesji jednostki logicznej 6.2 wymaganej przez aplikacje o dostępie bezpośrednim.

Jako właściciel zasobów bazy danych serwer pomocniczy steruje ochroną bazy danych przy użyciu obiektów SQL znajdujących się na serwerze. Jednak odpowiedzialność za ochronę ponosi również serwer aplikacji DB2 for MVS/ESA, który wydaje żądanie. Serwer ten steruje dostępem do obiektów SQL w następujący sposób:

- Serwer pomocniczy nie ma kopii planu DB2 for MVS/ESA. Żądający serwer aplikacji DB2 for MVS/ESA sprawdza więc, czy użytkownik może wywołać pakiet w systemie żądającym (serwer aplikacji).
- Statyczne instrukcje SQL są wykonywane dynamicznie na serwerze pomocniczym przy użyciu uprawnień nadanych właścicielowi pakietu DB2 for MVS/ESA w żądającym serwerze aplikacji DB2 for MVS/ESA.
- Dynamiczne instrukcje SQL są wykonywane przy użyciu uprawnień nadanych użytkownikowi w requesterze aplikacji.

Zapewnianie ochrony

Gdy requester aplikacji kieruje żądanie rozproszonej bazy danych do serwera aplikacji DB2 for MVS/ESA, należy uwzględnić następujące aspekty ochrony:

- sprawdzanie źródła żądania,
- wybór nazw użytkowników,
- parametry ochrony sieci,

- ochronę menedżera baz danych,
- ochronę wymuszoną przez zewnętrzny podsystem ochrony.

Sprawdzanie źródła żądania

Gdy serwer aplikacji DB2 for MVS/ESA otrzyma nazwę użytkownika od requestera aplikacji, może ograniczyć nazwy użytkowników otrzymywane z danego requestera aplikacji. Jest to wykonywane przy użyciu sprawdzania *źródła żądania*. Sprawdzanie to umożliwia serwerowi aplikacji określenie, czy podany ID użytkownika może być używany tylko przez określonych partnerów. Na przykład serwer aplikacji może ograniczyć JONES do "źródła żądania" DALLAS. Jeśli inny niż DALLAS requester aplikacji próbuje wysłać nazwę JONES do serwera aplikacji, serwer aplikacji może odrzucić to żądanie, ponieważ źródło żądania tej nazwy w sieci jest niepoprawne.

DB2 for MVS/ESA realizuje sprawdzanie źródła żądania jako część translacji nazwy przychodzącej użytkownika, którą opisano w następnej sekcji.

Wybieranie nazw użytkowników

Identyfikator użytkownika przysłany przez requester aplikacji może nie być unikalny w sieci SNA. Serwer aplikacji DB2 for MVS/ESA może wykonywać translacje nazw wychodzących w celu utworzenia nazw użytkowników unikalnych w całej sieci SNA. Podobnie może być konieczne wykonanie przez serwer aplikacji DB2 for MVS/ESA translacji nazw wychodzących w celu utworzenia unikalnych nazw użytkowników przeznaczonych dla serwerów pomocniczych związanych z aplikacją (informacje dotyczące translacji wychodzących nazw użytkowników można znaleźć w sekcji "Zapewnianie ochrony" na stronie 18).

Translacja nazw przychodzących jest możliwa, jeśli wartości w kolumnie USERNAMES tabeli SYSIBM.SYSLUNAMES są ustawione na 'I' (translacja nazw przychodzących) lub 'B' (translacja nazw przychodzących i wychodzących). Podczas translacji nazw przychodzących DB2 for MVS/ESA przekształca identyfikator użytkownika requestera aplikacji i nazwę właściciela planu DB2 for MVS/ESA (jeśli requester aplikacji jest innym systemem DB2 for MVS/ESA).

Jeśli requester aplikacji wysyła identyfikator i hasło użytkownika w APPC ALLOCATE, sprawdzana jest poprawność identyfikatora i hasła użytkownika zanim identyfikator zostanie poddany translacji. Kolumna PASSWORD w SYSIBM.SYSUSERNAMES nie jest używana do sprawdzenia poprawności hasła. Poprawność identyfikatora i hasła użytkownika jest natomiast sprawdzana przez zewnętrzny system ochrony (RACF lub produkt będący odpowiednikiem RACF).

Gdy sprawdzany jest przychodzący identyfikator użytkownika w ALLOCATE, DB2 for MVS/ESA ma informacje wyjściowe dotyczące autoryzacji, których użytkownik może użyć, aby dostarczyć listę dodatkowych autoryzacji AUTHID i wykonać dodatkowe sprawdzenie ochrony. Szczegółowe informacje można znaleźć w podręczniku *DB2 Administration Guide*.

Proces translacji nazw przychodzących wyszukuje wiersz w tabeli SYSIBM.SYSUSERNAMES, który musi być zgodny z jednym ze wzorców z poniższej listy (TYPE.AUTHID.LUNAME):

1. I.AUTHID.LUNAME — Określony użytkownik z określonego requestera aplikacji.
2. I.AUTHID.puste — Określony użytkownik z dowolnego requestera aplikacji.
3. I.puste.LUNAME — Dowolny użytkownik z określonego requestera aplikacji.

Jeśli wiersz nie zostanie odnaleziony, wystąpi odmowa dostępu. Jeśli wiersz zostanie odnaleziony, dostęp zdalny będzie dozwolony i nazwa użytkownika zostanie zmieniona na wartość z kolumny NEWAUTHID z wartością pustą NEWAUTHID wskazującą, że nazwa nie została zmieniona. Dowolne sprawdzenie autoryzacji do zasobów DB2 for MVS/ESA (na przykład uprawnienia tabeli SQL) wykonane przez DB2 for MVS/ESA jest przeprowadzane na nazwach użytkowników po translacji, a nie na pierwotnych nazwach użytkowników.

Jeśli serwer aplikacji DB2 for MVS/ESA otrzyma nazwę użytkownika od requestera aplikacji, przy użyciu funkcji translacji nazw przychodzących DB2 for MVS/ESA można wykonywać również inne operacje:

- Można zmienić nazwę użytkownika na unikalną. Na przykład następujące instrukcje SQL wykonują translację nazwy użytkownika JONES z requestera aplikacji NEWYORK (LUNAME LUNYC) na inną nazwę (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', ' ');
```

- Można zmienić nazwę użytkownika, tak aby cała grupa użytkowników była reprezentowana przez jedną nazwę. Na przykład wszyscy użytkownicy requestera aplikacji NEWYORK (LUNAME LUNYC) mogą mieć nazwę NYUSER. Umożliwi to nadawanie uprawnień SQL nazwie NYUSER i sterowanie dostępem SQL udzielonym użytkownikom z 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', ' ');
```

- Można ograniczyć nazwy użytkowników przesyłane przez określony requester aplikacji. Podczas translacji nazwy użytkownika następuje również sprawdzanie źródła żądania opisane w sekcji “Sprawdzanie źródła żądania” na stronie 32. Na przykład następujące instrukcje SQL dopuszczają tylko SMITH i JONES jako nazwy użytkowników z requestera aplikacji NEWYORK. Użytkownik o innej nazwie nie ma dostępu, ponieważ nie ma go w tabeli 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', ' ', ' ');
```

- Można ograniczyć requestery aplikacji, które mogą się połączyć z serwerem aplikacji DB2 for MVS/ESA. Jest to kolejna funkcja sprawdzania źródła żądania. Poniższy przykład akceptuje każdą nazwę użytkownika przysłaną przez requestera aplikacji NEWYORK (LUNYC) lub CHICAGO (LUCHI). Inne requestery aplikacji nie mają dostępu, ponieważ domyślny wiersz SYSIBM.SYSLUNAMES określa translację nazw przychodzących dla wszystkich żądań przychodzących.

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

Zapewnianie ochrony sieci

Jednostka logiczna 6.2 udostępnia trzy główne opcje ochrony sieci:

- ochronę na poziomie sesji,
- ochronę na poziomie konwersacji,
- szyfrowanie.

W sekcji “Ochrona sieci” na stronie 21 omówiono sposób określania ochrony na poziomie sesji i szyfrowania z DB2 for MVS/ESA. Serwer aplikacji DB2 for MVS/ESA używa ochrony na poziomie sesji i szyfrowania dokładnie w ten sam sposób, jak requester aplikacji DB2 for MVS/ESA.

Uwagi dotyczące ochrony sieci ograniczają się tylko do ochrony na poziomie konwersacji SNA. Aspekty ochrony na poziomie konwersacji są unikalne dla serwera aplikacji DB2 for MVS/ESA. Serwer aplikacji DB2 for MVS/ESA pełni dwie różne role w ochronie sieci:

- Jako requester serwerów pomocniczych serwer aplikacji DB2 for MVS/ESA jest odpowiedzialny za wydawanie żądań APPC, które zawierają parametry ochrony na poziomie konwersacji SNA wymagane przez serwery pomocnicze. Kolumny USERNAMES z tabeli SYSIBM.SYSLUNAMES i tabeli SYSIBM.SYSUSERNAMES są używane przez serwer aplikacji DB2 for MVS/ESA do definiowania wymagań dotyczących ochrony na poziomie konwersacji SNA dla

każdego serwera pomocniczego. Szczegóły tych definicji są identyczne jak te, które opisano w sekcji “Ochrona sieci” na stronie 21.

- Jako serwer requestera aplikacji serwer aplikacji DB2 for MVS/ESA narzuca ograniczenia dotyczące ochrony na poziomie konwersacji SNA dla requestera aplikacji. DB2 for MVS/ESA używa kolumny USERSECURITY z tabeli SYSIBM.SYSLUNAMES, aby określić poziom konwersacji wymagany dla każdego requestera aplikacji w sieci. W kolumnie USERSECURITY są stosowane następujące wartości:

  C Wskazuje, że DB2 for MVS/ESA wymaga, aby requester aplikacji wysłał identyfikator użytkownika i hasło (LU 6.2 SECURITY=PGM) z każdym żądaniem do rozproszonej bazy danych. Jeśli kolumna ENCRYPTPSWDS w SYSIBM.SYSLUNAMES zawiera 'Y', DB2 for MVS/ESA zakłada, że hasło jest już w zaszyfrowanym formacie RACF (jest to możliwe tylko dla requestera aplikacji DB2 for MVS/ESA). Jeśli kolumna ENCRYPTPSWDS nie zawiera 'Y', DB2 for MVS/ESA oczekuje hasła w formacie standardowym LU 6.2 (reprezentacja znakowa EBCDIC). W obu przypadkach DB2 for MVS/ESA przesyła wartości identyfikatora użytkownika i hasła do podsystemu ochrony w celu sprawdzenia poprawności. Podsystem ochrony udostępnia sprawdzenie identyfikatora i hasła użytkownika APPC; na przykład RACF ma funkcję służącą do sprawdzania identyfikatorów i haseł użytkowników APPC. Jeśli podsystem ochrony odrzuci parę identyfikator-hasło użytkownika, dostęp do rozproszonej bazy danych będzie niemożliwy.

  Inna wartość
  Wskazuje, że requester aplikacji może wysyłać już sprawdzony identyfikator użytkownika (LU 6.2 SECURITY=SAME) lub identyfikator i hasło użytkownika (LU 6.2 SECURITY=PGM). Jeśli identyfikator i hasło użytkownika zostaną wysłane, DB2 for MVS/ESA przetworzy je, jak to opisano dla wartości 'C'. Jeśli żądanie zawiera tylko identyfikator użytkownika, podsystem ochrony jest wywoływany, aby uwierzytelnić użytkownika, chyba że tabela SYSUSERNAMES jest używana do zarządzania przychodzącymi identyfikatorami użytkowników.

W przypadku wykrycia naruszenia ochrony LU 6.2 wymaga, aby serwer aplikacji DB2 for MVS/ESA zwrócił kod znaczenia uszkodzenia ochrony SNA ('080F6051'X) do requestera aplikacji. Ponieważ ten kod znaczenia nie opisuje przyczyny występowania awarii, DB2 for MVS/ESA dostarcza dwóch metod odczytywania przyczyny naruszenia ochrony rozproszonej:

- Wygenerowanie komunikatu DSNL030I, który zawiera identyfikator LUWID i kod przyczyny opisujący awarię. Komunikat DSNL030I zawiera także identyfikator AUTHID (jeśli jest znany), który został wysłany z odrzuconego żądania aplikacji.
- Zapisanie alertu w bazie danych monitorowania sprzętu NETVIEW, która zawiera informacje dostarczone w komunikacie DSNL030I.

Ochrona menedżera baz danych

Jako właściciel zasobów bazy danych serwer aplikacji DB2 for MVS/ESA steruje funkcjami ochrony baz danych dla obiektów SQL przechowywanych w serwerze aplikacji DB2 for MVS/ESA. Dostęp do obiektów zarządzanych przez DB2 for MVS/ESA jest sterowany przez uprawnienia nadawane użytkownikom przez administratora DB2 for MVS/ESA lub właścicieli obiektów indywidualnych. Oto dwie podstawowe klasy obiektów, które są sterowane przez serwer aplikacji DB2 for MVS/ESA:

- **Pakiety** — Użytkownicy indywidualni są autoryzowani do tworzenia, wymiany i uruchamiania pakietów przy użyciu instrukcji DB2 for MVS/ESA GRANT. Jeśli użytkownik jest właścicielem pakietu, może on automatycznie uruchamiać i wymieniać pakiet. Inni użytkownicy muszą mieć specjalną autoryzację do uruchamiania pakietu na serwerze aplikacji DB2 for MVS/ESA razem z instrukcją GRANT. Uprawnienie USE można nadać użytkownikom indywidualnym lub użytkownikom PUBLIC, co umożliwia wszystkim użytkownikom uruchomienie pakietu.

  Jeśli dana aplikacja jest powiązana z DB2 for MVS/ESA, pakiet zawiera instrukcje SQL z aplikacji. Instrukcje SQL są klasyfikowane jako:

  Statyczny SQL
  : Statyczny SQL oznacza, że instrukcja SQL oraz obiekty, do których się ona odnosi, są znane w momencie powiązania aplikacji z DB2 for MVS/ESA. Osoba tworząca pakiet musi mieć uprawnienia do wykonywania każdej statycznej instrukcji SQL zawartej w pakiecie.

    Gdy użytkownicy otrzymują uprawnienia do wykonywania pakietu, otrzymują automatycznie uprawnienia do wykonywania każdej zawartej w nim statycznej instrukcji SQL. W ten sposób użytkownicy nie potrzebują żadnych uprawnień z tabeli DB2 for MVS/ESA, jeśli pakiet, który wykonują, zawiera wyłącznie statyczne instrukcje SQL.

  Dynamiczny SQL
  : Dynamiczny SQL opisuje instrukcje SQL, które nie są znane aż do rozpoczęcia wykonywania programu. Innymi słowy instrukcja SQL jest tworzona przez program i dynamicznie wiązana z DB2 for MVS/ESA przy użyciu instrukcji SQL PREPARE. Gdy użytkownik wykonuje dynamiczną instrukcję SQL, musi mieć uprawnienia do tabeli wymagane do wykonywania instrukcji SQL. Ponieważ w momencie tworzenia planu lub pakietu instrukcja SQL jest nieznana, użytkownik nie otrzymuje automatycznie wymaganego uprawnienia od właściciela pakietu.

- **Obiekty SQL** — Są to tabele, widoki, synonimy i aliasy. Użytkownikom DB2 for MVS/ESA można nadawać różne poziomy uprawnień do tworzenia, usuwania, zmiany i odczytu indywidualnych obiektów SQL. Uprawnienia są wymagane do wiązania statycznej instrukcji SQL lub do wykonywania dynamicznej instrukcji SQL.

Po utworzeniu pakietu opcja DISABLE/ENABLE umożliwia kontrolowanie, które typy połączeń DB2 for MVS/ESA mogą uruchamiać pakiet. Można używać RACF i procedur

wyjściowych ochrony DB2 for MVS/ESA, aby umożliwić użytkownikom selektywne wykorzystanie DDF. Można użyć RLF, aby określić ograniczenia czasu procesora dla powiązań zdalnych i powiązań dynamicznych SQL.

Należy rozważyć pakiet DB2 for MVS/ESA o nazwie MYPKG, którego właścicielem jest JOE. JOE może umożliwić SAL wykonanie pakietu przez wydanie instrukcji DB2 for MVS/ESA, GRANT USE. Gdy SAL wykona pakiet:

- DB2 for MVS/ESA sprawdzi, czy SAL ma uprawnienia USE dla pakietu.
- SAL może wydać każdą statyczną instrukcję SQL w pakiecie, ponieważ JOE miał wymagane uprawnienia obiektu SQL do tworzenia pakietu.
- Jeśli pakiet ma dynamiczne instrukcje SQL, SAL musi mieć własne uprawnienia w tabeli SQL. Na przykład SAL nie może wydać instrukcji SELECT * FROM JOE.TABLE5, chyba że nadano jej prawo do odczytu tabeli JOE.TABLE5.

Podsystem ochrony

Wykorzystanie przez serwer aplikacji DB2 for MVS/ESA podsystemu ochrony (RACF lub produktu będącego odpowiednikiem RACF) zależy od sposobu zdefiniowania funkcji translacji nazw przychodzących w tabeli SYSIBM.SYSLUNAMES:

- Jeśli w kolumnie USERNAMES jest określone 'I' lub 'B', translacja nazw przychodzących jest aktywna i DB2 for MVS/ESA zakłada, że administrator DB2 for MVS/ESA wykorzystuje ją do wykonywania operacji związanych z ochroną systemu. Zewnętrzny podsystem ochrony jest wywoływany tylko wtedy, gdy requester aplikacji wyśle żądanie zawierające identyfikator i hasło użytkownika (SECURITY=PGM). Podsystem ochrony udostępnia sprawdzenie identyfikatora i hasła użytkownika APPC; na przykład RACF ma funkcję służącą do sprawdzania identyfikatorów i haseł użytkowników APPC.

  Jeśli żądanie z requestera aplikacji zawiera tylko identyfikator użytkownika (SECURITY=SAME), zewnętrzny system ochrony nie zostanie w ogóle wywołany, ponieważ reguły translacji nazw przychodzących definiują, który użytkownik może połączyć się z serwerem aplikacji DB2 for MVS/ESA.
- Jeśli w kolumnie USERNAMES jest określona wartość inna niż 'I' lub 'B', zostanie wykonane następujące sprawdzenie podsystemu ochrony:
  - Gdy z requestera aplikacji zostanie odebrane żądanie rozproszonej bazy danych, DB2 for MVS/ESA wywoła zewnętrzny system ochrony w celu sprawdzenia poprawności identyfikatora użytkownika (oraz hasła, jeśli zostało podane).
  - Zewnętrzny system ochrony jest wywoływany do sprawdzenia, czy użytkownik ma autoryzację do łączenia się z podsystemem DB2 for MVS/ESA.
- W pozostałych przypadkach informacje wyjściowe autoryzacji są dostarczane w celu zapewnienia listy pomocniczych identyfikatorów autoryzowanego użytkownika. Więcej informacji można znaleźć w podręczniku *DB2 Administration Guide*.

Reprezentacja danych

Należy się upewnić, że podsystem DB2 for MVS/ESA może przekształcić każdy skrócony identyfikator CCSID requestera aplikacji na skrócony identyfikator CCSID instalacji podsystemu DB2 for MVS/ESA. Więcej informacji można znaleźć w sekcji “Reprezentacja danych” na stronie 24.

Rozdział 2. Połączenia z DB2 Universal Database for OS/390 w sieci DRDA

DB2 Universal Database for OS/390 jest systemem zarządzania relacyjnymi bazami danych firmy IBM przeznaczonym dla systemów OS/390. Ten rozdział nie dotyczy wcześniejszych wydań produktu. Patrz “Rozdział 1. Połączenia z DB2 for MVS/ESA w sieci DRDA” na stronie 1.

W tym rozdziale opisano, jak połączyć requestery aplikacji DRDA (takie jak DB2 Connect) z serwerem aplikacji DB2 Universal Database for OS/390 oraz jak skonfigurować requestery aplikacji DB2 Universal Database for OS/390, aby mogły się komunikować z serwerami aplikacji DRDA, takimi jak DB2 Universal Database, w innych systemach.

Skoncentrowano się tu na połączeniach systemów innych niż DRDA z DB2 Universal Database for OS/390 przy użyciu połączeń sieciowych SNA. W produkcie DB2 Universal Database for OS/390 wersja 5 wprowadzono obsługę komunikacji z bazami danych przy użyciu wbudowanych połączeń TCP/IP (nie przy użyciu AnyNet) i omówiono sposoby użycia połączeń TCP/IP. Szczegółowe informacje o używaniu i konfigurowaniu połączeń TCP/IP można znaleźć w podręcznikach *DB2 Universal Database for OS/390 Installation Guide* oraz *DRDA Support for TCPIP with DB2 Universal Database for OS/390 and DB2 Universal Database*.

Więcej informacji na temat łączenia dwóch systemów DB2 Universal Database for OS/390 i sposobu definiowania połączeń DRDA z DB2 Universal Database for OS/390 można znaleźć we fragmencie dotyczącym łączenia systemów rozproszonych baz danych w podręczniku *DB2 Universal Database for OS/390 Administration Guide*.

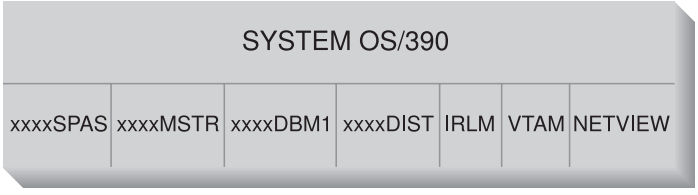
Uwagi:

1. Przy użyciu AnyNet Feature VTAM wersja 4 wydanie 2 można uruchomić APPC przez sieć TCP/IP. Zachęcamy użytkowników DB2 Universal Database for OS/390 wersja 5.1 do używania wbudowanej obsługi TCP/IP, a nie AnyNet APPC over TCP/IP.
2. W tym rozdziale nie podano informacji na temat korzystania z DCE.

DB2 Universal Database for OS/390

Rys. 13 na stronie 40 przedstawia system MVS działający z pojedynczą kopią DB2 Universal Database for OS/390. W jednym systemie można również uruchomić wiele kopii DB2 Universal Database for OS/390. Kopie DB2 Universal Database for OS/390 w danym systemie (lub kopie DB2 Universal Database for OS/390 w ramach kompleksu JES) można identyfikować za pomocą *nazwy podsystemu*, łańcucha złożonego z jednego

do czterech znaków unikalnych w ramach kompleksu JES. Na Rys. 13 nazwą podsystemu DB2 Universal Database for OS/390 jest *xxxx*. Trzy nazwy przestrzeni adresowych OS/390 są poprzedzone nazwą podsystemu DB2 Universal Database for OS/390. Przestrzenie te określają produkt DB2 Universal Database for OS/390.



Rysunek 13. Przestrzenie adresowe OS/390 używane przez DB2 Universal Database for OS/390

Rys. 13 ilustruje przestrzenie adresowe OS/390 wykorzystywane w przetwarzaniu rozproszonych baz danych w DB2 Universal Database for OS/390. Ich współdziałanie umożliwi użytkownikom DB2 Universal Database for OS/390 dostęp do lokalnych relacyjnych baz danych i komunikację z systemami zdalnymi DRDA. Przeznaczenie poszczególnych przestrzeni adresowych jest następujące:

xxxxSPAS
Przestrzeń adresowa procedur zapisanych w bazie DB2.

xxxxMSTR
Przestrzeń adresowa usług systemowych dla produktu DB2 Universal Database for OS/390, odpowiedzialna za uruchamianie i zatrzymywanie DB2 Universal Database for OS/390 i kontrolowanie lokalnego dostępu do DB2 Universal Database for OS/390.

xxxxDBM1
Przestrzeń adresowa usług baz danych, odpowiedzialna za dostęp do relacyjnych baz danych sterowanych przez DB2 Universal Database for OS/390. W przestrzeni tej jest realizowane wejście i wyjście dla zasobów baz danych w imieniu aplikacji SQL.

xxxxDIST
Część DB2 Universal Database for OS/390 obsługująca rozproszone bazy danych, zwane również *Distributed Data Facility* (DDF). Gdy nadchodzi żądanie związane z rozproszoną bazą danych, DDF przekazuje je do przestrzeni *xxxx*DBM1, aby można było wykonać operacje we/wy dla odpowiedniej bazy danych.

IRLM Menedżer blokad używany przez DB2 Universal Database for OS/390 w celu sterowania dostępem do zasobów baz danych.

VTAM Funkcje SNA programu IBM Communications Server for OS/390 (VTAM). DDF może wykorzystywać SNA lub TCP/IP do realizacji komunikacji rozproszonej bazy danych w imieniu DB2 Universal Database for OS/390. Na diagramie nie przedstawiono przestrzeni adresowej dla TCP/IP.

NETVIEW
Produkt stanowiący punkt skupienia zarządzania siecią w systemach OS/390. Jeśli podczas przetwarzania rozproszonych baz danych wystąpi błąd, DDF zapisuje informacje dotyczące błędu (zwane również *alertami*) w bazie danych monitora sprzętu NetView. Administratorzy systemu mogą korzystać z NetView, aby zapoznać się z błędami zapisanymi w bazie danych monitora sprzętu lub udostępnić procedury automatycznego wywoływania komend po zgłoszeniu wystąpienia warunków alertu.

NetView może również służyć do diagnozowania błędów komunikacji VTAM. Więcej informacji na ten temat można znaleźć w podręczniku *Distributed Relational Database Architecture Problem Determination Guide*.

Na Rys. 13 na stronie 40 nie ma aplikacji SQL. Jeśli aplikacja używa DB2 do wprowadzenia instrukcji SQL, program musi się połączyć z produktem DB2 Universal Database for OS/390 na jeden z następujących sposobów:

TSO Zadania wsadowe i użytkownicy zalogowani do TSO łączą się z DB2 Universal Database for OS/390 za pomocą narzędzia TSO. Jest to technika używana do łączenia SPUFI i większości aplikacji QMF z DB2 Universal Database for OS/390.

CICS/ESA
Jeśli aplikacja CICS/ESA używa wywołań SQL, produkt CICS/ESA używa interfejsu przyłączenia CICS do kierowania żądań SQL do DB2 Universal Database for OS/390.

IMS/ESA
Transakcje uruchamiane w IMS/ESA korzystają z interfejsu przyłączenia IMS, aby przekazać instrukcje SQL do przetwarzania w DB2 Universal Database for OS/390.

DDF Narzędzie Distributed Data Facility jest odpowiedzialne za połączenie aplikacji rozproszonych z DB2 Universal Database for OS/390.

CAF Narzędzie Call Attachment Facility umożliwia podsystemom napisanym przez użytkownika bezpośrednie połączenie się z DB2 Universal Database for OS/390.

Implementacja DB2 Universal Database for OS/390

Architektura DRDA definiuje typy funkcji systemu zarządzania rozproszoną bazą danych. DB2 Universal Database for OS/390 obsługuje zdalną jednostkę pracy. Program uruchamiany w jednym systemie może przy użyciu zdalnej jednostki pracy uzyskać dostęp do danych w zdalnym systemie DBMS, wykorzystując język SQL obsługiwany przez ten system.

DB2 Universal Database for OS/390 obsługuje również rozproszoną jednostkę pracy. Program uruchamiany w jednym systemie może przy użyciu rozproszonej jednostki pracy uzyskać dostęp do danych w zdalnym systemie DBMS, wykorzystując język SQL obsługiwany przez ten system zdalny. Więcej informacji na temat typów dystrybucji zdefiniowanych przez DRDA można znaleźć w podręczniku *DRDA Connectivity Guide*.

Jak pokazano na Rys. 14 na stronie 44 DB2 Universal Database for OS/390 obsługuje trzy konfiguracje połączeń z rozproszoną bazą danych korzystając z dwóch metod dostępu:

[1] *Dostęp sterowany przez system* (zwany również systemem używającym *prywatnego protokołu DB2 Universal Database for OS/390*) umożliwia requesterowi DB2 Universal Database for OS/390 połączenie z jednym lub kilkoma serwerami DB2 Universal Database for OS/390. Połączenie nawiązane między requesterem DB2 Universal Database for OS/390 i serwerem nie pasuje do protokołów zdefiniowanych w DRDA i nie może być używane do łączenia z DB2 Universal Database for OS/390 produktów innych niż DB2 Universal Database for OS/390. Ten rodzaj połączenia jest ustanawiany przy użyciu kodowania trzyczęściowych nazw lub aliasów w aplikacji.

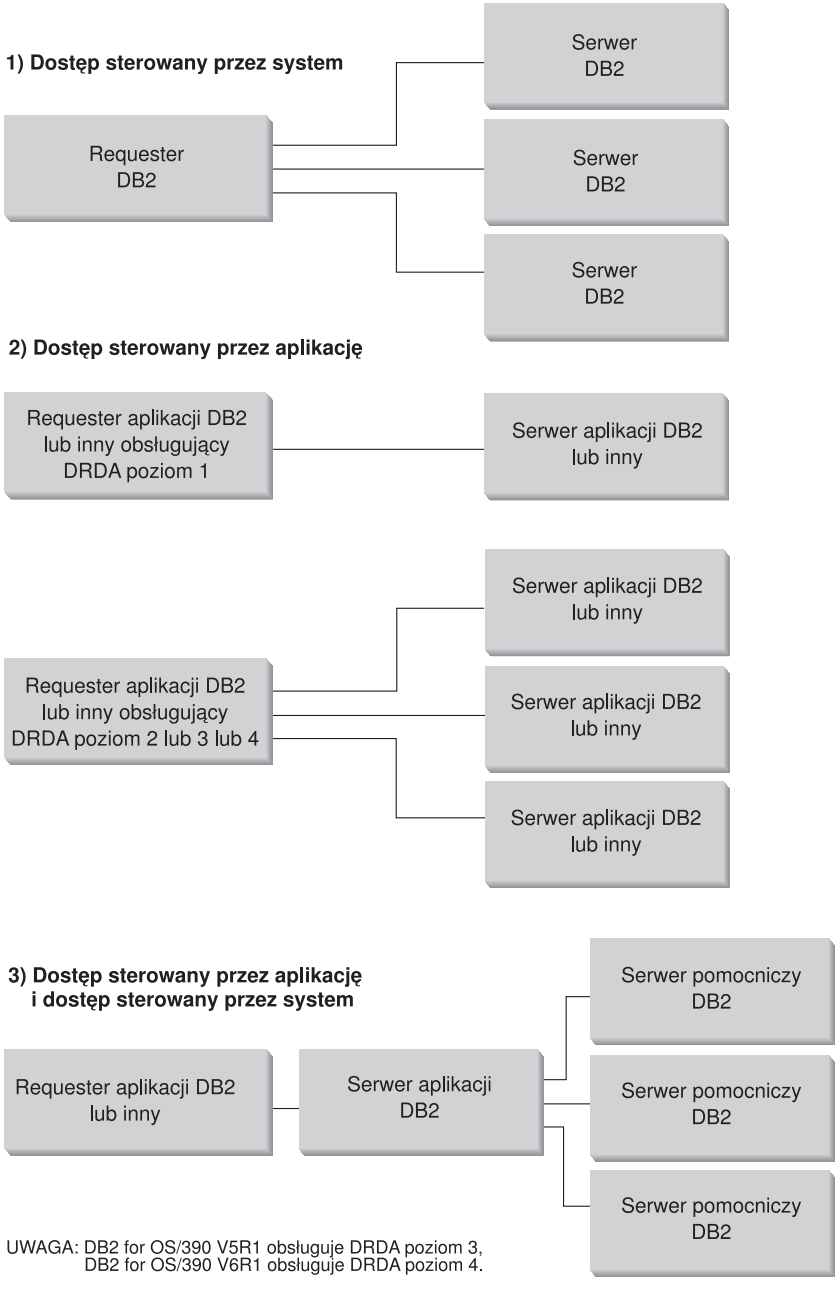
[2] *Dostęp sterowany przez aplikację* umożliwia requesterowi DB2 Universal Database for OS/390 lub innemu niż DB2 Universal Database for OS/390, np. DB2 Connect, połączenie się z jednym lub kilkoma serwerami aplikacji DB2 Universal Database for OS/390 lub innymi niż DB2 Universal Database for OS/390 np. DB2 Universal Database czy DB2 Universal Database for AS/400 przy użyciu protokołów DRDA. Liczba serwerów aplikacji, które mogą być jednocześnie połączone z requesterem, zależy od wersji requestera aplikacji DB2 Universal Database for OS/390. Jeśli requesterem aplikacji jest DB2 for MVS/ESA V2R3, w tym samym czasie może być połączony tylko jeden serwer aplikacji. Ten typ połączenia jest ustanawiany przez wprowadzenie do kodu aplikacji instrukcji SQL CONNECT. Jeśli requesterem aplikacji jest DB2 for MVS/ESA V3R1 lub nowszy, w tym samym czasie może być jednocześnie połączonych kilka serwerów aplikacji.

[3] Podczas ustanawiania połączenia można użyć obu metod dostępu jednocześnie. W ramach tego samego wątku nie można połączyć się przy użyciu DRDA i pamięci sterowanej przez system.

Termin *serwer pomocniczy* określa systemy działające jako serwery w stosunku do serwerów aplikacji.

Jeśli wszystkie systemy w konfiguracji obsługują zatwierdzanie dwufazowe, rozproszona jednostka pracy (odczyt dla wielu miejsc i aktualizacja dla wielu miejsc)

jest obsługiwana. Jeśli nie wszystkie systemy obsługują zatwierdzanie dwufazowe, aktualizacja w ramach jednostki pracy jest ograniczona do jednego miejsca lub do podzbioru miejsc obsługujących zatwierdzanie dwufazowe.



Rysunek 14. Połączenia rozproszone DB2 Universal Database for OS/390

Tabela 2 zawiera porównanie typów połączeń rozproszonych baz danych DB2 Universal Database for OS/390.

Tabela 2. Porównanie połączeń rozproszonych baz danych DB2 Universal Database for OS/390

[1] Dostęp sterowany przez system.	**[2] Dostęp sterowany przez aplikację (dla wszystkich systemów obsługujących zatwierdzanie dwufazowe).**	**[3] Dostęp sterowany przez aplikację i dostęp sterowany przez system.**
Wszyscy partnerzy muszą być systemami DB2 Universal Database for OS/390.	Może łączyć dowolne systemy DRDA.	Requester aplikacji może być dowolnym systemem DRDA; serwery muszą być systemami DB2 Universal Database for OS/390.
Mogą łączyć się bezpośrednio z wieloma partnerami.	Mogą łączyć się bezpośrednio z wieloma partnerami.	Requester aplikacji łączy się bezpośrednio z serwerami aplikacji; serwery aplikacji mogą łączyć się z wieloma serwerami pomocniczymi DB2 Universal Database for OS/390.
Każda aplikacja SQL może mieć wiele konwersacji z każdym serwerem.	Każda aplikacja SQL ma jedną konwersację z każdym serwerem.	Aplikacja SQL utrzymuje jedną konwersację z każdym serwerem; serwer aplikacji DB2 Universal Database for OS/390 dla aplikacji może nawiązać wiele konwersacji z każdym serwerem.
Może mieć dostęp zarówno do zasobów lokalnych, jak i zdalnych w jednym zakresie zatwierdzania.	Może mieć dostęp zarówno do zasobów lokalnych, jak i zdalnych w jednym zakresie zatwierdzania.	Requester aplikacji i serwer aplikacji mogą mieć dostęp do danych lokalnych i zdalnych.
Bardziej efektywny w przypadku obszernych zapytań i wielu zapytań współbieżnych.	Bardziej efektywny w przypadku instrukcji SQL uruchamianych bardzo rzadko w ramach jednego zatwierdzania.	Połączenie requester aplikacji-serwer aplikacji zachowuje się jak **[2]**; serwer pomocniczy zachowuje się jak **[1].**
Może obsługiwać statyczny lub dynamiczny SQL, lecz serwer dynamicznie powiąże statyczny SQL za pierwszym razem, gdy jest on wykonywany w jednym zakresie zatwierdzania.	Może korzystać ze statycznego lub dynamicznego SQL.	Requester aplikacji i serwer aplikacji mogą korzystać ze statycznego lub dynamicznego SQL; serwery pomocnicze obsługują statyczny lub dynamiczny SQL, lecz włączają dynamicznie statyczny SQL za pierwszym razem, gdy jest on uruchamiany w zasięgu zatwierdzania.
Ograniczony do instrukcji SQL INSERT, DELETE i UPDATE oraz instrukcji, które obsługują SELECT.	Może używać dowolnych instrukcji obsługiwanych przez system, który je wykonuje.	Serwery aplikacji obsługują wszystkie rodzaje SQL; serwery pomocnicze obsługują tylko DML SQL (na przykład CREATE lub ALTER).

Dodatkowe udoskonalenia ochrony

Rozszerzone kody ochrony

Do czasu powstania produktu DB2 Universal Database for OS/390 wersja 5.1 żądania połączeń dostarczające ID użytkowników lub hasła mogły nie powieść się z kodem przyczyny SQL30082 równym 0, ale bez żadnej innej wskazówki określającej przyczynę błędu.

W DB2 Universal Database for OS/390 wersja 5.1 wprowadzono możliwość obsługi kodów rozszerzonej ochrony. Określenie rozszerzonej ochrony stwarza dodatkowe możliwości diagnostyki, takie jak (PASSWORD EXPIRED) dodane do kodu przyczyny.

Aby to wykorzystać, parametr instalacji DB2 Universal Database for OS/390 ZPARM dla rozszerzonej ochrony powinien mieć wartość YES. Należy użyć panelu instalacji DB2 Universal Database for OS/390 DSN6SYSP, aby ustawić EXTSEC=YES. Można do tego celu użyć również ekranu 1 DDF (DSNTIPR). Domyślną wartością jest EXTSEC=NO. W przypadku hasła, które straciło ważność aplikacje PC, UNIX, Apple Macintosh lub sieci WWW korzystające z DB2 Connect otrzymają komunikat o błędzie SQL01404.

Ochrona protokołu TCP/IP sprawdzona uprzednio (TCP/IP Security Already Verified)

Aby udostępnić obsługę opcji ochrony DB2 Universal Database AUTHENTICATION=CLIENT, należy skorzystać z panelu instalacji DB2 Universal Database for OS/390 DSNTIP4 (DDF panel 2), aby ustawić wartość YES dla opcji Ochrona protokołu TCP/IP sprawdzona uprzednio).

Ochrona pulpitu ODBC i aplikacji Java

Aplikacje ODBC stacji roboczej i języka Java używają dynamicznego SQL. W niektórych instalacjach może to powodować naruszenie ochrony. DB2 Universal Database for OS/390 wprowadza nową opcję powiązania DYNAMICRULES(BIND), umożliwiającą wykonanie dynamicznego SQL z autoryzacją właściciela lub konsolidatora. W podręczniku *Command Reference* opisano w jaki sposób DB2 Connect określa opcję DYNAMICRULES.

DB2 Universal Database i DB2 Connect dostarczają nowego parametru konfiguracyjnego CLI/ODBC CURRENTPACKAGESET w pliku konfiguracyjnym DB2CLI.INI. Należy mu nadać nazwę schematu, który ma odpowiednie uprawnienia. Instrukcja schematu SQL SET CURRENT PACKAGESET będzie automatycznie wywoływana dla aplikacji po każdym połączeniu.

Aby zaktualizować plik DB2CLI.INI, należy użyć programu ODBC Manager. Więcej informacji można znaleźć w podręczniku *Instalowanie i konfigurowanie - suplement*.

Obsługa zmiany hasła

Jeśli instrukcja SQL CONNECT zwróci komunikat informujący, że hasło użytkownika straciło ważność, przy użyciu DB2 Connect wersja 5.2 i następne można zmienić hasło bez wpisywania się do TSO. Dzięki DRDA DB2 Universal Database for OS/390 może zmienić hasło użytkownika.

Użytkownik musi podać stare hasło, hasło nowe i potwierdzające. Jeśli na serwerze DB2 Connect Enterprise Edition określono ochronę DCS, to żądanie zmiany hasła jest wysyłane do serwera baz danych DB2 Universal Database for OS/390. Jeśli określono ochronę typu SERVER, hasło zostanie zmienione na serwerze DB2 Connect.

Dodatkową zaletą jest to, że nie jest wymagana osobna definicja jednostki logicznej. Dodatkowe informacje można znaleźć w podręczniku DB2 Connect Enterprise Edition *Krótkie wprowadzenie*(Quick Beginnings).

Konfigurowanie requestera aplikacji

DB2 Universal Database for OS/390 implementuje obsługę requestera aplikacji DRDA jako integralnej części DB2 Universal Database for OS/390 Distributed Data Facility (DDF). Działanie DDF może zostać wstrzymane niezależnie od lokalnych funkcji zarządzania bazą danych DB2 Universal Database for OS/390, lecz nie można go uruchomić przy braku obsługi zarządzania lokalną bazą danych DB2 Universal Database for OS/390.

Jeśli DB2 Universal Database for OS/390 działa jako requester aplikacji, może on połączyć aplikacje uruchamiane w systemie z serwerami zdalnymi baz danych DB2 Universal Database, DB2 for MVS/ESA, DB2 Universal Database for OS/390, DB2 Universal Database for AS/400 i DB2 for VSE & VM, które implementują funkcję serwera aplikacji DRDA.

Aby zdefiniować dostęp requestera aplikacji DB2 Universal Database for OS/390 do rozproszonych baz danych, należy wykonać czynności opisane w następujących punktach:

- “Dostarczanie informacji sieciowych” na stronie 48 — Requester aplikacji musi akceptować wartości RDB_NAME i dokonywać ich translacji na wartości SNA NETID.LUNAME lub wartości adresowe TCP/IP. DB2 Universal Database for OS/390 używa *bazy danych komunikacji DB2 Universal Database for OS/390* (CDB) w celu zarejestrowania nazw RDB_NAME i związanych z nimi parametrów sieciowych. Baza danych komunikacji umożliwia przekazywanie wymaganych informacji przez requester aplikacji DB2 Universal Database for OS/390 do serwera komunikacyjnego podczas żądań kierowanych do rozproszonych baz danych za pośrednictwem połączeń SNA lub TCP/IP.
- “Zapewnianie ochrony” na stronie 64 — Aby żądania kierowane do zdalnej bazy danych były przyjmowane przez serwer aplikacji, requester aplikacji musi dostarczać wymagane przez serwer informacje związane z ochroną. DB2 Universal Database for

OS/390 korzysta z podsystemu ochrony CDB i DCE, RACF lub innego, aby udostępnić wymagane informacje o ochronie sieci.

- "Reprezentacja danych" na stronie 72 — Należy upewnić się, że identyfikator CCSID requestera aplikacji jest kompatybilny z serwerem aplikacji.

Dostarczanie informacji sieciowych

Większość procesów przetwarzania w środowisku rozproszonych baz danych wymaga wymiany komunikatów z innymi miejscami w sieci. Aby przetwarzanie odbywało się poprawnie, należy:

1. Zdefiniować system lokalny.
2. Zdefiniować system zdalny.
3. Zdefiniować komunikację (dla połączeń SNA lub połączeń TCP/IP).
4. Ustawić wielkości jednostki RU i pacing (tylko dla połączeń SNA).

Patrz "Definiowanie systemu lokalnego (SNA)" lub "Definiowanie systemu lokalnego (TCP/IP)" na stronie 54.

Definiowanie systemu lokalnego (SNA)

Każdemu programowi w sieci przypisywany jest identyfikator NETID i nazwa jednostki logicznej (LU), tak więc requester aplikacji DB2 Universal Database for OS/390 łącząc się z siecią musi mieć wartość NETID.LUNAME (przypisaną przez VTAM). Ponieważ requester aplikacji DB2 Universal Database for OS/390 jest zintegrowany z lokalnym systemem zarządzania bazą danych DB2 Universal Database for OS/390, musi mieć również nazwę RDB_NAME. W publikacjach dotyczących DB2 Universal Database for OS/390, RDB_NAME DB2 Universal Database for OS/390 jest określana jako nazwa *miejsca*.

Należy zdefiniować requester aplikacji DB2 Universal Database for OS/390 w sieci SNA w następujący sposób:

1. Wybrać nazwę jednostki logicznej dla systemu DB2 Universal Database for OS/390. Identyfikator NETID dla systemu DB2 Universal Database for OS/390 jest pobierany automatycznie z VTAM podczas uruchamiania DDF.
2. Zdefiniować nazwę jednostki logicznej i nazwę miejsca w *programie startowym* (BSDS) produktu DB2 for MVS/ESA. (DB2 Universal Database for OS/390 ogranicza nazwę miejsca do 16 znaków).
3. Utworzyć definicję APPL VTAM w celu zarejestrowania wybranej nazwy jednostki logicznej w VTAM.
4. Należy zadbać, aby Extended Security był ustawiony na YES. Patrz "Dodatkowe udoskonalenia ochrony" na stronie 46.

Konfigurowanie BSDS DDF: DB2 Universal Database for OS/390 odczytuje BSDS podczas przetwarzania startowego w celu uzyskania parametrów instalacyjnych systemu. Jeden z rekordów zapisanych w BSDS nosi nazwę *rekordu DDF*, ponieważ zawiera informacje używane przez DDF do połączeń z VTAM. Informacje te obejmują:

- nazwę miejsca systemu DB2 Universal Database for OS/390,
- nazwę jednostki logicznej systemu DB2 Universal Database for OS/390,
- hasło używane podczas łączenia systemu DB2 Universal Database for OS/390 z VTAM.

Informacje BSDS DDF można dostarczać do DB2 Universal Database for OS/390 na dwa sposoby:

- Użyć panelu instalacyjnego DDF DSNTIPR podczas pierwszego instalowania DB2 Universal Database for OS/390 w celu dostarczenia wymaganych informacji BSDS DDF. Nie wspomniano tu o wielu parametrach instalacyjnych, ponieważ ważniejsze jest przekazanie wskazówek dotyczących sposobu łączenia DB2 Universal Database for OS/390 z VTAM. Rys. 15 przedstawia sposób użycia panelu instalacyjnego w celu zapisania w BSDS DB2 Universal Database for OS/390 nazwy miejsca NEW_YORK3, nazwy jednostki logicznej (LU) NYM2DB2 i hasła PSWDBD1.

```
                          DISTRIBUTED DATA FACILITY                =
==> _

 Enter data below:

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

Rysunek 15. Panel instalacyjny DB2 Universal Database for OS/390 o nazwie DSNTIPR

- Jeśli produkt DB2 Universal Database for OS/390 jest już zainstalowany, można użyć programu narzędziowego obsługującego wykaz protokołu zmian (DSNJU003) w celu aktualizacji informacji znajdujących się w BSDS.

  Rys. 16 na stronie 50 przedstawia sposób aktualizacji BSDS przez wprowadzenie nazwy miejsca NEW_YORK3, nazwy jednostki logicznej (LU) NYM2DB2 i hasła 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
//*
```

Rysunek 16. Przykładowa definicja zestawu danych programu startowego DDF (dla VTAM)

Podczas uruchamiania programu narzędziowego DDF (automatycznego uruchamiania DB2 Universal Database for OS/390 lub przy użyciu komendy DB2 Universal Database for OS/390 START DDF), łączy się ono z VTAM i przekazuje mu nazwę jednostki logicznej oraz hasło do VTAM. VTAM rozpoznaje system DB2 Universal Database for OS/390 sprawdzając nazwę jednostki logicznej i hasło (jeśli jest wymagane) z wartościami zdefiniowanymi w instrukcji APPL VTAM DB2 Universal Database for OS/390. Hasło VTAM jest używane do sprawdzenia, czy DB2 Universal Database for OS/390 ma autoryzację do korzystania z określonej nazwy jednostki logicznej w systemie VTAM. Hasło VTAM nie jest przesyłane przez sieć i nie jest wykorzystywane do połączenia innych systemów w sieci z DB2 Universal Database for OS/390.

Jeśli VTAM nie wymaga hasła, należy pominąć parametr PASSWORD= w programie narzędziowym obsługującym wykaz protokołu zmian. Brak tego parametru wskazuje, że hasło VTAM nie jest wymagane.

Tworzenie definicji APPL VTAM: Po zdefiniowaniu nazwy jednostki logicznej VTAM i hasła w DB2 Universal Database for OS/390 należy zarejestrować te wartości w VTAM. VTAM używa instrukcji APPL, aby zdefiniować nazwy jednostek logicznych. Rys. 17 na stronie 51 przedstawia sposób definiowania nazwy jednostki logicznej NYM2DB2 w VTAM.

```
 DB2APPLS VBUILD TYPE=APPL
*
*--------------------------------------------------------------------*
*                                                                    *
*           DEFINICJA APPL DLA SYSTEMU NEW_YORK3 DB2                 *
*                                                                    *
*--------------------------------------------------------------------*
*
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
```

Rysunek 17. Przykładowa definicja VTAM APPL dla DB2 Universal Database for OS/390

W instrukcji APPL VTAM dostępnych jest wiele parametrów. Ich znaczenie opisano szczegółowo w podręczniku *DB2 Universal Database for OS/390 Administration Guide*. Parametry omawiane w tym podręczniku odpowiadają tytułom tematów. Niektóre ważniejsze parametry przedstawiono na Rys. 17.

NYM2DB2

VTAM używa etykiety instrukcji APPL jako nazwy jednostki logicznej (LU). W tym przypadku nazwą jednostki logicznej jest NYM2DB2. Składnia APPL nie zapewnia tyle miejsca, aby zmieściła się cała nazwa NETID.LUNAME. Wartość identyfikatora NETID nie jest określona w instrukcji APPL VTAM, ponieważ wszystkie aplikacje VTAM są automatycznie przypisywane do NETID dla systemu VTAM.

AUTOSES=1

Liczba sesji zwycięskich w rywalizacji o połączenie SNA, które są uruchamiane automatycznie podczas wprowadzenia żądania APPC Change Number of Sessions (Zmiana liczby sesji CNOS). Wartość AUTOSES powinna być różna od zera, aby w przypadku błędu w przetwarzaniu CNOS VTAM możliwe było dostarczenie odpowiedniej informacji dla DB2 Universal Database for OS/390.

Automatyczne uruchamianie wszystkich sesji APPC między dowolnymi dwoma partnerami rozproszonej bazy danych nie jest konieczne. Jeśli wartość AUTOSES jest mniejsza od limitu zwycięzców rywalizacji (DMINWNL),

VTAM odkłada uruchomienie pozostałych sesji SNA do czasu, kiedy będą one potrzebne aplikacji obsługującej rozproszone bazy danych.

DMINWNL=10

Liczba sesji, dla których dany system DB2 Universal Database for OS/390 jest zwycięzcą rywalizacji. Parametr DMINWNL zawiera wartość domyślną dla przetwarzania CNOS, lecz można go przesłonić dla dowolnego partnera, dodając wiersz do tabeli SYSIBM.LUMODES w bazie danych komunikacji DB2 Universal Database for OS/390.

DMINWNR=10

Liczba sesji, dla których zwycięzcą rywalizacji jest system partnerski. Parametr DMINWNR zawiera wartość domyślną dla przetwarzania CNOS, lecz można go przesłonić dla dowolnego partnera, dodając wiersz do tabeli SYSIBM.LUMODES w bazie danych komunikacji DB2 Universal Database for OS/390.

DSESLIM=20

Całkowita liczba sesji (zwycięskich i pokonanych), które można uruchomić między DB2 Universal Database for OS/390 i innym rozproszonym systemem dla konkretnej nazwy grupy trybów. Parametr DSESLIM zawiera wartość domyślną dla przetwarzania CNOS, lecz można go przesłonić dla dowolnego partnera, dodając wiersz do tabeli SYSIBM.LUMODES w bazie danych komunikacji DB2 Universal Database for OS/390.

Jeśli partner nie może obsługiwać liczby sesji podanej w parametrach DSESLIM, DMINWNL lub DMINWNR, proces CNOS negocjuje nową wartość dla tych parametrów, akceptowalną dla partnera.

EAS=9999

Szacunkowa całkowita liczba sesji wymaganych przez tę jednostkę logiczną VTAM.

MODETAB=RDBMODES

Określa tabelę VTAM MODE, w której znajdują się wszystkie nazwy trybów DB2 Universal Database for OS/390.

PRTCT=PSWDBD1

Określa hasło VTAM, które ma być użyte, gdy DB2 Universal Database for OS/390 próbuje łączyć się z VTAM. Jeśli parametr PRTCT został pominięty, hasło nie jest wymagane i można pominąć parametr PASSWORD= w programie narzędziowym obsługującym wykaz protokołu zmian DB2 Universal Database for OS/390.

SECACPT=ALREADYV

Określa najwyższą wartość ochrony na poziomie konwersacji w SNA akceptowaną przez system DB2 Universal Database for OS/390 przy przyjmowaniu żądań w stosunku do rozproszonej bazy danych z serwera zdalnego. Parametr ALREADYV wskazuje, że dany system DB2 Universal

Database for OS/390 może akceptować trzy opcje ochrony sesji SNA z innych systemów DRDA, które żądają danych z tego systemu DB2 Universal Database for OS/390:

- SECURITY=SAME (sprawdzone uprzednio żądanie zawierające tylko identyfikator użytkownika wysyłającego żądanie).
- SECURITY=PGM (żądanie zawierające hasło requestera lub PassTicket).
- SECURITY=NONE (żądanie nie zawierające żadnych informacji). DB2 Universal Database for OS/390 odrzuca żądania DRDA zawierające specyfikację SECURITY=NONE.

Najlepiej zawsze podawać SECACPT=ALREADYV, ponieważ poziom ochrony konwersacji SNA dla każdego partnera DB2 Universal Database for OS/390 jest pobierany z bazy danych komunikacji DB2 Universal Database for OS/390 (kolumna USERSECURITY tabeli SYSIBM.LUNAMES). Parametr SECACPT=ALREADYV umożliwia największą elastyczność w wyborze wartości dla USERSECURITY.

VERIFY=NONE

Określa poziom ochrony sesji SNA (weryfikacja jednostki logicznej) wymagany przez dany system DB2 Universal Database for OS/390. Wartość NONE wskazuje, że weryfikacja partnerskiej jednostki logicznej nie jest wymagana.

W DB2 Universal Database for OS/390 nie ma ograniczeń w wyborze wartości dla parametru VERIFY. W sieciach niezaufanych zalecane jest używanie VERIFY=REQUIRED. Wartość ta powoduje, że VTAM odrzuca partnerów, którzy nie mogą wykonać weryfikacji partnerskiej jednostki logicznej. Jeśli użytkownik wybierze wartość VERIFY=OPTIONAL, VTAM przeprowadzi weryfikację partnerskiej jednostki logicznej tylko wobec tych partnerów, którzy zapewniają tę obsługę.

VPACING=2

Ustawia wartość pacingu VTAM na 2.

SYNCLVL=SYNCPT

Oznacza, że DB2 Universal Database for OS/390 jest w stanie obsługiwać zatwierdzanie dwufazowe. VTAM używa tej informacji, aby przekazać partnerowi, że jest dostępne zatwierdzanie dwufazowe. Podanie tego parametru powoduje, że DB2 Universal Database for OS/390 automatycznie używa dwufazowego zatwierdzania, jeśli tylko partner jest w stanie je obsłużyć.

ATNLOSS=ALL

Wskazuje, że DB2 Universal Database for OS/390 musi być każdorazowo informowany o zakończeniu sesji VTAM. Umożliwia to wykonywanie przez DB2 Universal Database for OS/390 resynchronizacji SNA, gdy jest to potrzebne.

Parametry DSESLIM, DMINWNL i DMINWNR umożliwiają ustanowienie domyślnego limitu liczby sesji VTAM dla wszystkich partnerów. W przypadku partnerów o szczególnych wymaganiach dotyczących limitu liczby sesji można użyć tabeli SYSIBM.LUMODES w celu przesłonięcia domyślnej wartości limitu liczby sesji. Można na przykład podać domyślną wartość limitu liczby sesji VTAM, która jest odpowiednia dla systemów OS/2. W przypadku innych partnerów, aby zdefiniować odpowiednie limity liczby sesji, można utworzyć wiersze w tabeli SYSIBM.LUMODES. Rozważmy przykładowe wartości:

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

Parametry te umożliwiają każdemu partnerowi utworzenie czterech sesji z DB2 Universal Database for OS/390, gdy partner jest zwycięzcą rywalizacji w każdej z sesji. Ponieważ OS/2 tworzy konwersacje jednostki logicznej 6.2 z DB2 Universal Database for OS/390, ustanawiając OS/2 zwycięzcą rywalizacji w sesjach, użytkownik uzyskuje niewielki wzrost wydajności. Jeśli sesja OS/2 jest zwycięzcą rywalizacji, nie musi zabiegać o pozwolenie na uruchomienie nowej konwersacji jednostki logicznej 6.2.

Definiowanie systemu lokalnego (TCP/IP)

Dla wygody czytelnika informacje znajdujące się w tej sekcji stanowią podsumowanie informacji zawartych w podręczniku *DB2 Connect Enterprise Edition for OS/2 and Windows Quick Beginnings*. Bardziej szczegółowe informacje można znaleźć w podręcznikach *DB2 Universal Database for OS/390 Installation Reference* i *DRDA Support for TCP/IP with DB2 Universal Database for OS/390 and DB2 Universal Database*.

Kroki, które należy wykonać, aby zdefiniować komunikację TCP/IP z DB2 Universal Database for OS/390.

1. Udostępnić komunikację TCP/IP w systemie DB2 Universal Database for OS/390 i systemie partnera.
2. Administrator sieci musi przypisać dwa odpowiednie numery portów TCP/IP. Domyślnie DB2 Universal Database for OS/390 do połączeń z bazą danych używa numeru portu 446, a dla żądań resynchronizacji (zatwierdzanie dwufazowe) używa numeru portu 5001.
3. Serwer zdalny aplikacji lub requester aplikacji musi używać tych samych numerów portów (lub nazw usług) co DB2 Universal Database for OS/390.
4. Upewnij się, że opcja Ochrona TCP/IP uprzednio sprawdzona (TCP/IP already verified security) jest ustawiona na YES. Patrz “Dodatkowe udoskonalenia ochrony” na stronie 46.
5. BDSD dla DB2 Universal Database for OS/390 musi zawierać dodatkowe parametry. Rys. 18 na stronie 55 przedstawia dodatkowe parametry, konieczne do udostępnienia komunikacji TCP/IP.

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

Rysunek 18. Przykładowa definicja zestawu danych programu startowego DDF (dla TCP/IP)

Definiowanie systemów zdalnych

Jeśli aplikacja DB2 Universal Database for OS/390 żąda danych z systemu zdalnego, to przeszukuje tabele baz danych komunikacji, aby znaleźć informacje na temat systemu zdalnego. Baza danych komunikacji jest grupą tabel SQL zarządzanych przez administratora systemu DB2 Universal Database for OS/390. Administrator systemu DB2 Universal Database for OS/390 może użyć SQL, aby wstawić wiersze do bazy danych komunikacji w celu opisania każdego potencjalnego partnera DRDA. Pełny opis CDB i sposób użycia można znaleźć w *DB2 Universal Database for OS/390 SQL Reference* i *DB2 Universal Database for OS/390 Installation Guide*.

Przy przeszukiwaniu baz danych komunikacji wyszukiwane są następujące informacje:

- nazwa jednostki logicznej i programu transakcyjnego (dla połączeń SNA),
- informacje o adresie TCP/IP (wymagane tylko dla połączeń wychodzących SNA TCP/IP),
- informacje ochrony sieci wymagane przez miejsca zdalne,
- limity liczby sesji i nazwy trybów używane przy komunikacji z miejscami zdalnymi (dla połączeń SNA).

Wypełnianie bazy danych komunikacji: Aktualizacje bazy danych komunikacji nie są wymagane, jeśli używane będą tylko przychodzące połączenia TCP/IP. Jeśli więc DB2 Universal Database for OS/390 ma być używany tylko jako serwer TCP/IP, nie należy wypełniać bazy danych komunikacji i zostaną użyte wartości domyślne. Jeśli jednak będą używane przychodzące połączenia SNA, należy umieścić w tabeli

SYSIBM.LUNAMES co najmniej jeden, pusty wiersz. Na przykład aby umożliwić przyjmowanie żądań połączenia z bazą danych przychodzących z dowolnych jednostek logicznych DB2 Connect należy użyć komendy SQL, takiej jak:

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

Jeśli produkt DB2 Universal Database for OS/390 będzie używany jako requester, zawsze należy zaktualizować bazę danych komunikacji. Należy umieścić wiersze w tabeli SYSIBM.LOCATIONS oraz w tabeli SYSIBM.LUNAMES (dla połączeń SNA) lub SYSIBM.IPNAMES (dla połączeń TCP/IP).

Dodatkowe aktualizacje bazy danych komunikacji mogą być potrzebne, jeśli użytkownik ma sterować wymaganiami ochrony przychodzących połączeń SNA lub translacją ID użytkownika dla tych połączeń. Dodatkowe przykłady można znaleźć w sekcji “Zapewnianie ochrony” na stronie 64, w której opisano definiowanie ochrony użytkownika podczas konfigurowania requestera aplikacji; oraz w sekcji “Zapewnianie ochrony” na stronie 77, w której opisano konfigurowanie serwera aplikacji.

Dokładne omówienie wymagań do aktualizacji tabel bazy danych komunikacji można znaleźć w podręczniku *DB2 Universal Database for OS/390 Administration Guide*. Po wypełnieniu bazy danych komunikacji użytkownik może kierować zapytania, które uzyskują dostęp do danych systemów zdalnych. Dodatkowe informacje na temat aktualizacji bazy danych komunikacji można również znaleźć w podręczniku *DB2 Universal Database for OS/390 Installation Reference*.

Sposób obsługi żądań przez bazę danych komunikacji: Podczas wysyłania żądania DB2 Universal Database for OS/390 używa kolumny LINKNAME tabeli katalogu SYSIBM.LOCATIONS, aby określić, jaki protokół sieciowy ma być użyty dla wychodzących połączeń z bazą danych. Aby odbierać żądania VTAM, należy wybrać LUNAME w panelu instalacyjnym DSNTIPR DB2 Universal Database for OS/390. Aby odbierać żądania TCP/IP, należy wybrać port DRDA oraz port resynchronizacji w panelu instalacyjnym DSNTIP5 DB2 Universal Database for OS/390. Do przekazania żądań sieciowych do właściwego podsystemu DB2 protokół TCP/IP używa numeru portu serwera .

Jeśli wartość znajdująca się w kolumnie LINKNAME zostanie odnaleziona w tabeli SYSIBM.IPNAMES, to dla połączeń DRDA będzie używany protokół TCP/IP. Jeśli wartość ta zostanie odnaleziona w tabeli SYSIBM.LUNAMES, to będzie używany protokół SNA. Jeśli ta sama nazwa znajduje się w obu tabelach SYSIBM.LUNAMES i SYSIBM.IPNAMES, to do połączenia z podanym miejscem będzie używany protokół TCP/IP.

Uwaga: Requester nie może połączyć się z podanym miejscem przy użyciu protokołu SNA, jak i TCP/IP. Na przykład jeśli w tabeli SYSIBM.LOCATIONS w kolumnie LINKNAME znajduje się wartość LU1, a LU1 zdefiniowano w tabeli SYSIBM.IPNAMES i SYSIBM.LUNAMES, to protokół TCP/IP jest jedynym protokołem używanym do połączenia z LU1 z tego requestera.

Tabele bazy danych komunikacji: Baza danych komunikacji zawiera następujące tabele:

1. **SYSIBM.LOCATIONS**

   Tabela ta umożliwia systemowi DB2 Universal Database for OS/390 podanie informacji o adresie SNA lub TCP/IP wymaganych podczas dostępu do każdej bazy RDB_NAME wybranej przez aplikację DB2 Universal Database for OS/390 *dla żądań wychodzących.* Tabela składa się z następujących kolumn:

   LOCATION
   Nazwa systemu zdalnego RDB_NAME. DB2 Universal Database for OS/390 ogranicza wartość RDB_NAME do 16 bajtów, co zmniejsza o dwa bajty 18-bajtowy limit zdefiniowany w DRDA.

   LINKNAME
   Nazwa jednostki logicznej lub atrybuty TCP/IP systemu zdalnego.

   PORT Nazwa portu TCP/IP lub nazwa usługi (domyślną nazwą portu dla DRDA jest 446).

   TPN Nazwa programu transakcyjnego APPC systemu zdalnego. Jeśli systemem zdalnym jest DB2 Universal Database for OS/390 lub system zdalny używa domyślnej wartości TPN DRDA (X'07F6C4C2'), to do podania TPN można użyć łańcucha pustego, ponieważ DB2 Universal Database for OS/390 automatycznie wybiera poprawną wartość.

   Jeśli system zdalny wymaga podania wartości TPN innej niż wartość domyślna TPN, należy podać ją w tym miejscu.

2. **SYSIBM.LUNAMES**

   W tabeli tej definiuje się atrybuty sieciowe systemów zdalnych, do których dostęp uzyskiwany jest za pomocą połączeń SNA. Tabela składa się z następujących kolumn:

   LUNAME
   Nazwa jednostki logicznej systemu zdalnego.

   SYSMODENAME
   Nazwa trybu logowania VTAM używana przy ustanawianiu konwersacji DB2 Universal Database for OS/390-DB2 Universal Database for OS/390 *międzysystemowej* dla *obsługi serwera pomocniczego* DB2 Universal Database for OS/390 (dostęp sterowany przez system). Wartość pusta w tej kolumnie oznacza, że dla konwersacji w systemie DB2 Universal Database for OS/390 powinna być użyta wartość IBMDB2LM.

   SECURITY_IN
   Opcje akceptowane przez ochronę sieci, wymagane dla systemu zdalnego, gdy system DB2 Universal Database for OS/390 działa jako serwer dla systemu zdalnego (wymagania *ochrony połączeń przychodzących*). Dopuszczalne wartości:

- **V** oznacza opcję ″verify″. Przychodzące żądanie połączenia musi zawierać: ID użytkownika i hasło, ID użytkownika i PassTicket RACF lub bilet ochrony DCE.
- **A** oznacza opcję ″already verified″. W przypadku żądania nie jest wymagane hasło, chociaż przysłane hasło jest sprawdzane. W przypadku tej opcji przychodzące żądanie połączenia jest akceptowane, jeśli zawiera: ID użytkownika, ID użytkownika i hasło, ID użytkownika i PassTicket RACF lub bilet ochrony DCE.

  Jeśli w kolumnie USERNAMES znajduje się ’I’ lub ’B’, podsystem ochrony RACF nie jest wywoływany do sprawdzenia poprawności przychodzących żądań połączeń zawierających tylko ID użytkownika.

SECURITY_OUT

Opcje akceptowane przez ochronę sieci wymagane dla systemu zdalnego, gdy system DB2 Universal Database for OS/390 działa jako requester (wymagania *ochrony połączeń przychodzących*). Dopuszczalne wartości:

- **A** oznacza opcję ″already verified″. Żądania połączeń wychodzących zawierają ID autoryzowanego użytkownika i nie zawierają hasła. ID autoryzowanego użytkownika używany dla żądania wychodzącego jest ID autoryzowanego użytkownika DB2 albo ID po translacji, w zależności od wartości znajdującej się w kolumnie USERNAMES.
- **R** oznacza opcję ″RACF PassTicket″. Żądania połączeń zewnętrznych zawierają ID użytkownika oraz PassTicket podsystemu ochrony RACF. Nazwa jednostki logicznej serwera jest używana jako nazwa aplikacji RACF PassTicket.

  ID autoryzowanego użytkownika używany dla żądania wychodzącego jest ID autoryzowanego użytkownika DB2 albo ID po translacji, w zależności od wartości znajdującej się w kolumnie USERNAMES.
- **P** oznacza opcję ″password.″ Żądania połączeń wychodzących zawierają ID autoryzowanego użytkownika i hasło. Hasło jest pobierane z tabeli SYSIBM.USERNAMES lub podsystemu RACF, w zależności od wartości podanej w kolumnie ENCRYPTPWDS.

  Kolumna USERNAMES musi zawierać wartość ’B’ lub ’O’.

ENCRYPTPSWDS

Określa, czy hasła wymieniane przy użyciu tego parametru są szyfrowane. Hasła szyfrowane są obsługiwane tylko przez requestery i serwery DB2 Universal Database for OS/390.

MODESELECT

Określa, czy w celu wybrania pozycji trybu logowania VTAM (nazwy trybu) na podstawie użytkownika i aplikacji formułującej żądanie jest używana tabela SYSIBM.MODESELECT. Jeśli kolumna ta zawiera 'Y', do uzyskania nazwy trybu dla każdego wychodzącego żądania w stosunku do rozproszonej bazy danych jest używana tabela SYSIBM.MODESELECT.

Jeśli MODESELECT zawiera jakąkolwiek wartość różną od 'Y', dla żądań dostępu sterowanego przez system jest używana nazwa trybu IBMDB2LM, a dla żądań DRDA nazwa trybu IBMRDB.

Kolumna MODESELECT umożliwia ustawienie priorytetów żądań dotyczących rozproszonych baz danych przez podanie klasy usług (COS) VTAM związanej z nazwą trybu.

USERNAMES
Wymagany poziom sprawdzania źródła i translacji identyfikatora użytkownika. Kolumna ta zawiera także parametry ochrony używane przez system DB2 Universal Database for OS/390 podczas żądań danych z partnera zdalnego (wymagania *ochrony połączeń wychodzących*). Parametr USERNAMES może przyjmować wartości I, O lub B (odpowiednio: tylko - przychodzące, tylko - wychodzące lub oba).

GENERIC
Wskazuje, czy DB2 Universal Database for OS/390 powinien użyć rzeczywistej, czy ogólnej nazwy jednostki logicznej (LU).

3. **SYSIBM.LUMODES**

Ta tabela jest używana w celu udostępnienia VTAM limitów sesji LU 6.2 (limity CNOS) dla systemów partnerskich używających połączeń APPC (SNA). Tabela składa się z następujących kolumn:

LUNAME
Nazwa jednostki logicznej systemu zdalnego.

MODENAME
Nazwa trybu logowania VTAM, którego limity są określane. Wartość pusta powoduje przyjęcie wartości domyślnej IBMDB2LM kolumny MODENAME.

CONVLIMIT
Maksymalna liczba aktywnych konwersacji między lokalnym systemem DB2 Universal Database for OS/390 i systemem zdalnym dla tego trybu logowania. Wartość ta jest używana do przesłonięcia parametru DSESLIM w instrukcji definicji APPL VTAM dla trybu logowania, który dostarcza domyślne wartości limitów liczby sesji dla DB2 Universal Database for OS/390.

Wartość wybrana w CONVLIMIT jest używana podczas działania procesów CNOS w celu ustawienia wartości DMINWNR i DMINWNL na CONVLIMIT/2.

4. **SYSIBM.MODESELECT**

Tabela ta umożliwia określenie różnych nazw trybów dla użytkowników indywidualnych i aplikacji DB2 Universal Database for OS/390. Jest ona używana tylko dla połączeń SNA. Ponieważ każda nazwa trybu VTAM może mieć związaną z nią klasę usług (COS), tabeli tej można użyć do przypisania priorytetów transmisji

sieciowej aplikacjom obsługującym rozproszone bazy danych, przy użyciu kombinacji kolumn AUTHID, PLANNAME i LUNAME. Tabela składa się z następujących kolumn:

AUTHID
ID autoryzowanego użytkownika DB2 Universal Database for OS/390 (ID użytkownika). Wartością domyślną jest wartość pusta, oznaczająca, że podana nazwa trybu logowania odnosi się do wszystkich identyfikatorów autoryzowanego użytkownika.

PLANNAME
Nazwa planu związana z aplikacją żądającą dostępu do zdalnego systemu baz danych. Wartością domyślną jest wartość pusta, oznaczająca, że podana nazwa trybu logowania odnosi się do wszystkich nazw planów. Nazwą planu dla komendy BIND PACKAGE jest DSNBIND.

LUNAME
Nazwa jednostki logicznej związana z systemem zdalnym baz danych.

MODENAME
Nazwa trybu logowania VTAM, który ma być użyty podczas routingu żądania rozproszonej bazy danych do wskazanego systemu zdalnego. Wartością domyślną jest wartość pusta, oznaczająca, że dla konwersacji o dostępie sterowanym przez system powinna być użyta wartość IBMDB2LM, a dla konwersacji DRDA - wartość IBMRDB.

5. **SYSIBM.USERNAMES**

Tabela ta jest używana do zarządzania nazwami użytkowników przez dostarczanie haseł, translacji nazw i sprawdzanie źródeł. DB2 Universal Database for OS/390 odwołuje się do nazwy użytkownika jako do identyfikatora autoryzowanego użytkownika. Większość innych produktów odwołuje się do tej nazwy jako do identyfikatora użytkownika.

Za pomocą tej tabeli użytkownik może użyć translacji nazw w celu wymuszenia użycia różnych wartości dla połączeń użytkownika o danym ID i ID autoryzowanego użytkownika DB2 Universal Database for OS/390. Proces translacji nazwy może zostać użyty dla żądań skierowanych do systemu zdalnego (żądań *wychodzących*) i dla żądań przychodzących z systemu zdalnego (żądań *przychodzących*). Jeśli hasła nie są szyfrowane, tabela ta jest źródłem haseł użytkowników, gdy zarówno ID użytkownika, jak i hasło są wysyłane do miejsca zdalnego. Tabela składa się z następujących kolumn:

TYPE Opis sposobu użycia wiersza (czy jest to wiersz opisujący translacje nazw dla wychodzących lub przychodzących żądań sprawdzania źródeł).

I oznacza połączenia przychodzące, **O** oznacza połączenia wychodzące.

W przypadku połączeń TCP/IP należy użyć ″O″ (dla żądań TCP/IP nie są wykonywane translacja ID połączenia przychodzącego i sprawdzenie źródła.

AUTHID

W przypadku translacji nazw wychodzących należy wykonać translację ID autoryzowanego użytkownika DB2 Universal Database for OS/390. W przypadku translacji nazw przychodzących należy wykonać translację ID użytkownika SNA. W każdym z tych przypadków wartość pusta AUTHID dotyczy wszystkich identyfikatorów autoryzowanych użytkowników i identyfikatorów użytkowników.

LINKNAME

Określa miejsce w sieci VTAM lub TCP/IP związane z tym wierszem. Wartość pusta w tej kolumnie oznacza, że reguła translacji tej nazwy ma zastosowanie dla dowolnego partnera TCP/IP lub SNA.

Jeśli w kolumnie LINKNAME znajduje się inna wartość niż pusta, co najmniej jedno z następujących stwierdzeń jest prawdziwe:

- Istnieje wiersz w tabeli SYSIBM.LUNAMES, taki że nazwa w kolumnie LUNAME odpowiada wartości podanej w kolumnie LINKNAME tabeli SYSIBM.USERNAMES. Ten wiersz określa miejsce VTAM związane z regułą translacji tej nazwy.
- Istnieje wiersz w tabeli SYSIBM.IPNAMES, taki że wartość w kolumnie LINKNAME odpowiada wartości podanej w kolumnie LINKNAME w tabeli SYSIBM.USERNAMES. Ten wiersz podaje host TCP/IP związany z regułą translacji tej nazwy.

  W przypadku klientów TCP/IP nie jest wykonywana translacja nazwy połączenia przychodzącego, ani sprawdzenie połączenia wychodzącego.

NEWAUTHID

Nowa nazwa użytkownika (identyfikator użytkownika SNA lub ID autoryzowanego użytkownika DB2 Universal Database for OS/390). Jeśli jest to wartość pusta, nie należy wykonywać translacji identyfikatora.

PASSWORD

Hasło używane w konwersacji dotyczącej przydziału, jeśli hasła nie są szyfrowane (ENCRYPTPSWDS = 'N' w tabeli SYSIBM.LUNAMES). Jeśli hasła są szyfrowane, kolumna ta jest ignorowana.

6. **SYSIBM.IPNAMES**

Ta tabela jest używana dla węzłów TCP/IP.

LINKNAME

Wartość podana w tej kolumnie musi odpowiadać wartości podanej w kolumnie LINKNAME tabeli SYSIBM.LOCATIONS.

SECURITY_OUT

Ta kolumna definiuje opcję ochrony DRDA używaną, gdy lokalne aplikacje DB2 SQL łączą się z dowolnym serwerem zdalnym związanym z hostem TCP/IP:

- **A** oznacza opcję ″already verified″. Żądania połączeń wychodzących zawierają ID autoryzowanego użytkownika i nie zawierają hasła. ID autoryzowanego użytkownika używany dla żądania wychodzącego jest ID autoryzowanego użytkownika DB2 albo ID po translacji, w zależności od wartości znajdującej się w kolumnie USERNAMES.
- **R** oznacza opcję ″RACF PassTicket″. Żądania połączeń zewnętrznych zawierają ID użytkownika oraz PassTicket podsystemu ochrony RACF. Wartość podana w kolumnie LINKNAME jest używana jako nazwa aplikacji RACF PassTicket dla zdalnego serwera.

  ID autoryzowanego użytkownika używany dla żądania wychodzącego jest ID autoryzowanego użytkownika DB2 albo ID po translacji, w zależności od wartości znajdującej się w kolumnie USERNAMES.
- **P** oznacza opcję ″password″. Żądania połączeń wychodzących zawierają ID autoryzowanego użytkownika i hasło. Hasło jest pobierane z tabeli SYSIBM.USERNAMES.

  Kolumna USERNAMES musi zawierać wartość ″O″.

USERNAMES

Ta kolumna steruje translacją ID autoryzowanego użytkownika dla połączenia wychodzącego. Translacja połączenia wychodzącego jest wykonywana, gdy ID autoryzowanego użytkownika jest wysyłany przez DB2 do serwera zdalnego.

- **O** oznacza, że ID połączenia wychodzącego ma być poddany translacji. Do wykonania tej translacji używane są wiersze tabeli SYSIBM.USERNAMES.

  W przypadku ID połączenia przychodzącego nie wykonuje się translacji ani sprawdzania źródła.
- Pozycja pusta oznacza, że translacja nie jest wykonywana.

IPADDR

Ta kolumna zawiera adres IP lub nazwę domeny zdalnego hosta TCP/IP. Kolumna IPADDR musi być wypełniona następująco:

- Jeśli kolumna ta zawiera łańcuch znaków wyrównany do lewej strony, zawierający cztery wartości numeryczne oddzielone kropkami, DB2 zakłada, że wartość w tej kolumnie jest adresem IP w formacie dziesiętnym z kropkami. Na przykład łańcuch ’123.456.78.91’ zostałby zinterpretowany jako adres IP w formacie dziesiętnym z kropkami.
- Pozostałe wartości są interpretowane jako nazwa domeny TCP/IP, która może być zanalizowana przez wywołanie gniazda gethostbyname TCP/IP. W nazwach domeny TCP/IP nie rozróżnia się wielkich i małych liter.

Definiowanie komunikacji (SNA)

VTAM jest menedżerem komunikacji dla systemów OS/390. VTAM akceptuje słowa jednostki logicznej 6.2 DB2 Universal Database for OS/390 i poddaje je konwersji na

strumienie danych jednostki logicznej 6.2, które mogą być przesyłane przez sieć. Ponieważ VTAM komunikuje się z aplikacjami partnerskimi zdefiniowanymi w bazie danych komunikacji DB2 Universal Database for OS/390, należy udostępnić VTAM następujące informacje:

- Nazwę jednostki logicznej dla każdego serwera.

  Jeśli DB2 Universal Database for OS/390 komunikuje się z VTAM w celu identyfikacji miejsca docelowego, to może przesyłać do VTAM tylko nazwę jednostki logicznej (nie NETID.LUNAME). Nazwa ta musi być unikalna wśród nazw jednostek logicznych znanych lokalnemu systemowi VTAM. Pozwala to VTAM określić zarówno NETID, jak i nazwę jednostki logicznej na podstawie wartości nazwy jednostki logicznej przekazanej przez DB2 Universal Database for OS/390. Jeśli nazwy jednostki logicznej są unikalne w sieci SNA przedsiębiorstwa, ułatwia to znacznie definiowanie zasobów VTAM. Czasami jest to jednak niemożliwe. Jeśli nazwy jednostek logicznych w sieci SNA nie są unikalne, należy użyć translacji nazw jednostek logicznych VTAM, tak aby utworzyć poprawną kombinację dla nieunikalnej nazwy jednostki logicznej. Opis tego procesu można znaleźć w rozdziale “Resource Name Translation” podręcznika *VTAM Network Implementation Guide*.

  Sposób umieszczenia i składnia definicji VTAM używanych w celu określenia nazw zdalnych jednostek logicznych są w dużym stopniu uzależnione od sposobu, w jaki system zdalny jest logicznie i fizycznie połączony z systemem lokalnym VTAM.
- Wielkość RU, wielkość okna pacingu i klasę usług dla każdego trybu. W przypadku każdej nazwy trybu podanej w bazie danych komunikacji należy utworzyć tabelę trybów VTAM. Należy również zdefiniować parametry IBMRDB i IBMDB2LM.
- Profile VTAM i RACF dla algorytmu weryfikacji jednostki logicznej, jeśli użytkownik zamierza korzystać z weryfikacji partnerskiej jednostki logicznej.

Ustawianie wielkości RU i pacingu: Pozycje tabeli trybów VTAM zawierają wielkości jednostek RU i liczby pacingu. Błędy popełnione przy definiowaniu tych wartości mogą negatywnie wpływać na wszystkie aplikacje VTAM.

Po wybraniu wielkości RU, limitów liczby sesji i liczby pacingu, należy koniecznie zastanowić się nad wpływem tych wartości na sieć VTAM. Podczas instalowania nowego systemu obsługującego rozproszone bazy danych należy sprawdzić następujące elementy:

- W przypadku połączeń CTC VTAM CTC należy sprawdzić, czy parametr MAXBFRU jest wystarczająco duży, aby obsłużył wielkość RU plus 29 bajtów, które dodaje VTAM do nagłówka żądania SNA i nagłówka transmisji. MAXBFRU jest mierzony w jednostkach o wielkości 4 kB, więc MAXBFRU musi mieć co najmniej wartość 2, aby zmieścić jednostkę RU wielkości 4 kB.
- W przypadku połączeń NCP należy się upewnić, czy wartość MAXDATA jest odpowiednia, aby obsłużyć wielkość RU plus 29 bajtów. Jeśli określono wielkość RU 4 kB, MAXDATA musi mieć co najmniej wartość 4125.

  Przy określaniu parametru NCP MAXBFRU należy wybrać wielkość, która może pomieścić jednostkę RU plus 29 bajtów. W przypadku połączeń NCP parametr

MAXBFRU określa liczbę buforów we/wy VTAM, które mogą być używane, aby przechować jednostkę informacyjną ścieżki. Jeśli zostanie wybrana wielkość buforu IOBUF 441, MAXBFRU=10 przetworzy poprawnie jednostki RU o wielkości 4 kB, ponieważ 10*441 jest większe od 4096+29.

- W podręczniku *DRDA Connectivity Guide* opisano, jak określić wpływ rozproszonej bazy danych na pulę IOBUF VTAM. Jeśli używa się zbyt dużej części zasobów puli IOBUF, wydajność aplikacji VTAM zostaje obniżona.

Definiowanie komunikacji (TCP/IP)

Przypadek TCP/IP opisano wcześniejszej (patrz "Definiowanie systemu lokalnego (TCP/IP)" na stronie 54).

Zapewnianie ochrony

Jeśli system zdalny przetwarza rozproszoną bazę danych w imieniu aplikacji SQL, musi być możliwe spełnienie wymogów ochrony requestera aplikacji, serwera aplikacji i łączącej je sieci. Wymagania te należą do co najmniej jednej z następujących kategorii:

- wybór nazw użytkowników,
- parametry ochrony sieci,
- ochrona menedżera baz danych,
- ochrona wymuszona przez zewnętrzny podsystem ochrony,
- reprezentacja danych.

Wybieranie nazw użytkowników

W systemach OS/390 każdemu użytkownikowi jest przypisany *ID użytkownika* składający się z 1 do 8 znaków. Wartość identyfikatora użytkownika musi być unikalna w danym systemie OS/390, lecz może nie być unikalna w sieci. Na przykład w systemie NEWYORK może istnieć użytkownik o nazwie JONES i inny użytkownik o tej samej nazwie w systemie DALLAS. Jeśli tych dwóch użytkowników to ta sama osoba konflikt nie wystąpi. Jeśli natomiast JONES w DALLAS jest inną osobą niż JONES w NEWYORK, sieć SNA (i konsekwentnie systemy obsługujące rozproszone bazy danych w sieci) nie są w stanie rozróżnić tych użytkowników. Jeśli sytuacja ta nie ulegnie zmianie, JONES w DALLAS będzie korzystać z uprawnień nadanych użytkownikowi JONES w NEWYORK.

Aby wyeliminować konflikty nazewnictwa, DB2 Universal Database for OS/390 obsługuje translacje nazw użytkowników. Jeśli aplikacja requestera aplikacji DB2 Universal Database for OS/390 formułuje żądanie dotyczące rozproszonej bazy danych, DB2 Universal Database for OS/390 wykonuje translację nazwy, o ile baza danych komunikacji zawiera wymaganie wykonania *translacji nazwy wychodzącej*. Jeśli wybrana zostanie translacja nazwy wychodzącej, DB2 Universal Database for OS/390 wymusi przesłanie hasła przy każdym żądaniu wychodzącym dotyczącym rozproszonej bazy danych.

Translacja nazw wychodzących w DB2 Universal Database for OS/390 jest uaktywniana przez ustawienie kolumny USERNAMES w tabeli SYSIBM.LUNAMES lub

SYSIBM.IPNAMES na wartość 'O' lub 'B'. Jeśli kolumna ta jest ustawiona na 'O', dla żądań wychodzących jest wykonywana translacja nazw użytkowników. Jeśli jest ustawiona na 'B', translacja nazw użytkowników jest wykonywana zarówno dla żądań przychodzących, jak i wychodzących.

Ponieważ autoryzacja DB2 Universal Database for OS/390 zależy zarówno od identyfikatora użytkownika lokalnego, jak i identyfikatora użytkownika DB2 Universal Database for OS/390 właściciela planu i pakietu, proces translacji nazwy użytkownika lokalnego jest wykonywany dla identyfikatora użytkownika lokalnego, identyfikatora właściciela planu oraz identyfikatora właściciela pakietu.[3]Proces translacji nazw przeszukuje tabelę SYSIBM.USERNAMES w następującej kolejności, aby wyszukać wiersz, który jest zgodny z jednym z następujących wzorców (TYPE.AUTHID.LINKNAME):

1. O.AUTHID.LINKNAME — Reguła translacji dla określonego użytkownika do określonego systemu partnerskiego.
2. O.AUTHID.puste — Reguła translacji dla określonego użytkownika do dowolnego systemu partnerskiego.
3. O.puste.LINKNAME — Reguła translacji dla dowolnego użytkownika do określonego systemu partnerskiego.

Jeśli nie odnaleziono wierszy pasujących do wzorca, DB2 Universal Database for OS/390 odrzuca żądanie skierowane do rozproszonej bazy danych. Jeśli wiersz zostanie odnaleziony, jako ID autoryzowanego użytkownika jest używana wartość kolumny NEWAUTHID. (Wartość pusta w kolumnie NEWAUTHID oznacza, że oryginalna nazwa jest używana bez translacji).

Rozważmy przykład omawiany wcześniej. Użytkownikowi JONES z NEWYORK należy nadać inną nazwę (NYJONES), gdy JONES wysyła żądanie dotyczące rozproszonej bazy danych do DALLAS. Załóżmy, że aplikacja używana przez użytkownika JONES jest własnością DSNPLAN (właściciel planu DB2 Universal Database for OS/390) i nie należy wykonywać translacji identyfikatora użytkownika, gdy jest on przesyłany do DALLAS. Instrukcje SQL, których należy użyć, aby określić reguły translacji nazwy w bazie danych komunikacji, przedstawiono na Rys. 19 na stronie 66.

3. Jeśli żądanie jest wysyłane do serwera DB2 Universal Database for OS/390, translacja nazwy jest także wykonywana dla właściciela pakietu i właściciela planu. Nazwy właściciela planu i właściciela pakietu nie są związane z hasłem.

```
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');
```

Rysunek 19. Instrukcje SQL dla translacji nazw wychodzących (SNA)

Wynikowe tabele bazy danych komunikacji przedstawiono na Rys. 20 na stronie 67.

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

Rysunek 20. Translacja nazw wychodzących

Na Rys. 21 na stronie 68 przedstawiono prostszy przykład połączenia produktu DB2 Universal Database z serwerem aplikacji DRDA przy użyciu połączenia SNA.

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

Rysunek 21. Instrukcje SQL translacji nazw wychodzących (prosty przykład dla SNA)

Na Rys. 22 na stronie 69 przedstawiono prosty przykład połączenia produktu DB2 Universal Database z serwerem aplikacji DRDA przy użyciu połączenia TCP/IP.

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

Rysunek 22. Instrukcje SQL translacji nazw wychodzących (prosty przykład dla TCP/IP)

Ochrona sieci

Po wybraniu nazw użytkowników reprezentujących aplikację zdalną, requester aplikacji musi dostarczyć wymagane informacje dotyczące ochrony sieci.

Jednostka logiczna 6.2 (LU 6.2) udostępnia trzy główne opcje ochrony sieci dla połączeń SNA:

- Ochrona na poziomie sesji, sterowana przez parametr VERIFY w instrukcji APPL VTAM APPL. Sposób określania opcji ochrony na poziomie sesji przedstawiono po Rys. 17 na stronie 51.
- Ochrona na poziomie konwersacji, sterowana wartościami znajdującymi się w tabeli SYSIBM.LUNAMES.

- Szyfrowanie danych, obsługiwane tylko przez VTAM 3.4 i późniejsze wydania VTAM.

Serwer aplikacji jest odpowiedzialny za zarządzanie zasobami baz danych, dlatego decyduje o tym, które opcje ochrony są wymagane od requestera aplikacji. Należy zapisać wymagania dotyczące ochrony na poziomie konwersacji każdego serwera aplikacji w tabeli SYSIBM.LUNAMES lub SYSIBM.IPNAMES, ustawiając w kolumnie USERNAMES wartości odzwierciedlające wymagania serwera aplikacji.

Możliwe opcje ochrony konwersacji SNA:

SECURITY=SAME

Zwana również ochroną sprawdzoną uprzednio, ponieważ identyfikator użytkownika jest wysyłany do systemu zdalnego (hasło nie jest wysyłane). Tego poziomu ochrony konwersacji należy użyć, jeśli kolumna USERNAMES tabeli SYSIBM.LUNAMES nie zawiera wartości 'O' lub 'B'.

Ponieważ DB2 Universal Database for OS/390 dopasowuje translację nazwy użytkownika do ochrony konwersacji wychodzącej, nie pozwala on na użycie opcji SECURITY=SAME, gdy translacja wychodzącej nazwy użytkownika jest uaktywniona.

SECURITY=PGM

Powoduje wysłanie identyfikatora użytkownika i hasła do systemu zdalnego w celu sprawdzenia poprawności. Tej opcji ochrony należy użyć, jeśli kolumna USERNAMES tabeli SYSIBM.LUNAMES zawiera wartość 'O' albo 'B'.

W zależności od opcji podanej w tabeli SYSIBM.LUNAMES, DB2 Universal Database for OS/390 pobiera hasło użytkownika z dwóch różnych źródeł:

- Hasła niezaszyfrowane są pobierane z kolumny PASSWORD tabeli SYSIBM.USERNAMES. DB2 Universal Database for OS/390 pobiera hasła z tabeli SYSIBM.USERNAMES, gdy kolumna ENCRYPTPSWDS tabeli SYSIBM.LUNAMES nie jest ustawiona na 'Y'. Hasła uzyskane z tego źródła mogą być przenoszone do dowolnego serwera aplikacji DRDA.

  Na Rys. 23 zdefiniowano hasła użytkowników SMITH i JONES. Kolumna LUNAME w przykładzie zawiera wartości puste, więc hasła te są używane dla wszystkich systemów, z których próbują skorzystać SMITH i JONES.

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

Rysunek 23. Wysyłanie haseł do miejsc zdalnych (SNA)

- Hasła zaszyfrowane są wysyłane do miejsc zdalnych, jeśli kolumna ENCRYPTPSWDS tabeli SYSIBM.LUNAMES zawiera 'Y'. Hasła zaszyfrowane są pobierane z RACF (lub produktu równoważnego RACF) i mogą być interpretowane jedynie przez inny system DB2 Universal Database for OS/390. Podczas komunikowania z systemem innym niż DB2 Universal Database for OS/390 nie należy ustawiać kolumny ENCRYPTPSWDS na 'Y'.

  DB2 Universal Database for OS/390 przeszukuje tabelę SYSIBM.USERNAMES, aby określić, jaki identyfikator użytkownika (wartość NEWAUTHID) ma być przesłany do systemu zdalnego. Ta poddana translacji nazwa jest używana do pobrania hasła RACF. Jeśli translacja nazw nie ma być wykonana, należy utworzyć wiersze w tabeli SYSIBM.USERNAMES, co spowoduje wysłanie nazw bez translacji. Wykonanie instrukcji przedstawionych na Rys. 24 pozwala na wysłanie żądań do LUDALLAS i LUNYC bez translacji nazwy użytkownika (ID użytkownika).

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

Rysunek 24. Wysyłanie haseł zaszyfrowanych do miejsc zdalnych (SNA)

SECURITY=NONE

Opcja ta nie jest obsługiwana przez architekturę DRDA, dlatego DB2 Universal Database for OS/390 jej nie obsługuje.

Ochrona menedżera baz danych

Jednym ze sposobów zapewnienia przez requester aplikacji ochrony rozproszonej bazie danych jest translacja nazw połączeń przychodzących, co opisano w sekcji “Wybieranie nazw użytkowników” na stronie 64. Aby sterować dostępem do każdego serwera aplikacji, można użyć translacji nazw wychodzących wedle zasady tożsamości użytkownika wysyłającego żądanie i aplikacji wysyłającej żądanie. Inne sposoby używane przez requester aplikacji DB2 Universal Database for OS/390 w celu ochrony systemu rozproszonego:

Wiązanie aplikacji zdalnych

Użytkownicy wiążą aplikacje zdalne na serwerze aplikacji, wykorzystując komendę BIND PACKAGE używanej w produkcie DB2 Universal Database for OS/390. DB2 Universal Database for OS/390 *nie* ogranicza użycia komendy BIND PACKAGE na requesterze. Użytkownik nie może jednak użyć pakietu zdalnego, dopóki pakiet ten jest włączony do planu DB2 Universal Database for OS/390. DB2 Universal Database for OS/390 *ogranicza* użycie komendy BIND PLAN. Użytkownik nie może dodać pakietu zdalnego do

planu, dopóki nie zostaną mu nadane uprawnienia BIND lub BINDADD za pomocą instrukcji GRANT używanej w DB2 Universal Database for OS/390.

Podczas wiązania pakietu należy skorzystać z opcji ENABLE/DISABLE, aby określić, czy dany pakiet ma być używany przez TSO, CICS/ESA, IMS/ESA czy przez podsystem zdalny DB2 Universal Database for OS/390.

Wykonywanie aplikacji zdalnych

Aby użytkownik DB2 Universal Database for OS/390 mógł uruchomić aplikację zdalną, musi mieć uprawnienia do uruchamiania planu DB2 Universal Database for OS/390 związanego z aplikacją. Właścicielowi planu DB2 Universal Database for OS/390 nadawane są automatycznie uprawnienia do jego uruchomienia. Używając instrukcję GRANT EXECUTE w DB2 Universal Database for OS/390 można nadać innym użytkownikom uprawnienia do uruchamiania planu. W ten sposób właściciel aplikacji obsługującej rozproszone bazy danych może kontrolować korzystanie z aplikacji na zasadzie dla każdego użytkownika osobno.

Podsystem ochrony

Zewnętrznym podsystemem ochrony dla systemów OS/390 jest zazwyczaj podsystem RACF lub inny produkt z interfejsem kompatybilnym z RACF. Requester aplikacji DB2 Universal Database for OS/390 nie ma bezpośrednich odwołań do zewnętrznego podsystemu ochrony, z wyjątkiem obsługi hasła szyfrowanego opisanej w sekcji “Ochrona sieci” na stronie 69. Zewnętrzny podsystem ochrony jest jednak wykorzystywany pośrednio w requesterze aplikacji w następujących sytuacjach:

- Produkt odpowiedzialny za podłączenie użytkownika do DB2 Universal Database for OS/390 korzysta z zewnętrznego podsystemu ochrony w celu sprawdzenia jego poprawności (ID użytkownika i hasło). Ma to miejsce przed podłączeniem użytkownika do DB2 Universal Database for OS/390. Jak stwierdzono wcześniej, CICS/ESA, TSO i IMS/ESA są przykładami produktów, które podłączają użytkowników do DB2 Universal Database for OS/390.
- Jeśli używana jest ochrona SNA na poziomie sesji (za pomocą parametru VERIFY w instrukcji APPL programu VTAM DB2 Universal Database for OS/390), zewnętrzny podsystem ochrony jest wywoływany przez VTAM w celu sprawdzenia poprawności systemu zdalnego.

Reprezentacja danych

Podczas instalacji produktu DB2 Universal Database for OS/390 domyślnie jest instalowany kodowany zestaw znaków (CCSID) równy 500. Wartość ta prawdopodobnie *nie* jest poprawna w przypadku instalacji użytkownika.

Podczas instalowania DB2 Universal Database for OS/390 należy zmienić identyfikator CCSID na CCSID znaków generowanych i wysyłanych do DB2 Universal Database for OS/390 za pomocą dostępnych urządzeń wejściowych po stronie użytkownika. Identyfikator ten jest zwykle uzależniony od używanego języka. Jeśli identyfikator CCSID instalacji jest niepoprawny, konwersja znaków będzie prowadziła do

uzyskiwania nieprawidłowych wyników. *IBM DB2 Connect Podręcznik użytkownika* zawiera listę identyfikatorów CCSID obsługiwanych dla każdego języka.

Należy sprawdzić, czy podsystem DB2 Universal Database for OS/390 może przekształcić każdy CCSID używany na serwerze aplikacji na instalowany CCSID podsystemu DB2 Universal Database for OS/390. DB2 Universal Database for OS/390 udostępnia tabele konwersji dla najczęściej występujących kombinacji źródłowych i docelowych CCSID, ale nie dla wszystkich kombinacji. Jeśli zaistnieje taka potrzeba, można dodać pozycje do zestawu dostępnych tabel konwersji i procedur konwersji. Więcej informacji na temat konwersji znaków w DB2 Universal Database for OS/390 można znaleźć w podręczniku *DB2 Universal Database for OS/390 Administration Guide*.

Konfigurowanie serwera aplikacji

Obsługa serwera aplikacji w DB2 Universal Database for OS/390 umożliwia działanie DB2 Universal Database for OS/390 jako serwera requsterów aplikacji DRDA. Requesterem aplikacji połączonym z serwerem aplikacji DB2 Universal Database for OS/390 może być:

- requester DB2 Universal Database for OS/390;
- DB2 Connect
- DB2 Universal Database Enterprise Edition lub DB2 Universal Database Extended - Enterprise Edition z obsługą DB2 Connect;
- requester DB2 wersja 2, który może działać w systemach AIX, HP-UX, OS/2, Solaris, Windows 3.1, Windows 3.11 for Workgroups, Windows 95 lub Windows NT, Macintosh, SCO, SGI lub SINIX. Funkcję tę udostępniają brama (DDCS) Distributed Database Connection Services dla wielu użytkowników wersja 2.3, brama DDCS dla jednego użytkownika wersja 2.3 oraz brama DDCS for Windows wersja 2.4;
- requester OS/400;
- requester DB2 for VM;
- każdy produkt, który obsługuje protokoły requestera aplikacji DRDA.

W przypadku każdego requestera aplikacji połączonego z serwerem aplikacji DB2 Universal Database for OS/390, serwer aplikacji DB2 Universal Database for OS/390 obsługuje dostęp do bazy danych w następujący sposób:

- Requester aplikacji może mieć dostęp do tabel zapisanych na serwerze aplikacji DB2 Universal Database for OS/390. Przed uruchomieniem aplikacji requester aplikacji musi utworzyć pakiet na serwerze aplikacji DB2 Universal Database for OS/390. Serwer aplikacji DB2 Universal Database for OS/390 używa tego pakietu do umiejscowienia instrukcji SQL aplikacji podczas jej wykonywania.
- Requester aplikacji może poinformować serwer aplikacji DB2 Universal Database for OS/390 o konieczności ograniczenia dostępu do czynności tylko do odczytu, jeśli połączenie requester-serwer DRDA nie obsługuje procesu zatwierdzania

dwufazowego. Na przykład requester DDCS V2R3 z interfejsem CICS poinformuje serwer aplikacji DB2 Universal Database for OS/390, że wykonanie aktualizacji jest niedopuszczalne.

- Requester aplikacji może mieć także dostęp do tabel zapisanych w innych systemach DB2 Universal Database for OS/390 w sieci przy użyciu bezpośredniego dostępu do systemu. Dostęp bezpośredni do systemu umożliwia requesterowi aplikacji nawiązywanie połączeń z wieloma systemami baz danych w pojedynczej jednostce pracy.

Dostarczanie informacji sieciowych

Aby serwer aplikacji DB2 Universal Database for OS/390 poprawnie przetworzył żądania skierowane do rozproszonej bazy danych, należy:

1. Zdefiniować serwer aplikacji dla lokalnego menedżera komunikacji.
2. Zdefiniować każde miejsce potencjalnego serwera pomocniczego, tak aby serwer aplikacji DB2 Universal Database for OS/390 mógł przekierować żądania SQL do ich miejsca docelowego.
3. Udostępnić niezbędną ochronę.
4. Udostępnić reprezentację danych.

Definiowanie serwera aplikacji (SNA)

Aby serwer aplikacji mógł otrzymywać żądania rozproszonej bazy danych, musi zostać zdefiniowany w lokalnym menedżerze komunikacji i mieć unikalną nazwę RDB_NAME. Niniejsze uwagi dotyczą połączeń SNA. Aby odpowiednio zdefiniować serwer aplikacji, należy:

1. Wybrać nazwy LU i RDB_NAME, które mają być używane przez serwer aplikacji DB2 Universal Database for OS/390. Zapisywanie tych nazw w DB2 Universal Database for OS/390 i VTAM odbywa się tak samo, jak opisano w sekcji “Definiowanie systemu lokalnego (SNA)” na stronie 48. Wybraną nazwę RDB_NAME dla DB2 Universal Database for OS/390 należy udostępnić wszystkim użytkownikom i requesterom aplikacji wymagającym połączeń z serwerem aplikacji.
2. Zarejestrować wartość NETID.LUNAME dla serwera aplikacji DB2 Universal Database for OS/390 z każdym requesterem aplikacji żądającym dostępu, tak aby requester aplikacji mógł kierować żądania SNA do serwera DB2 Universal Database for OS/390. Jest to ważne nawet, gdy requester aplikacji może wykonać dynamiczny routing sieciowy, ponieważ przed jego użyciem musi on znać wartość NETID.LUNAME.
3. Udostępnić domyślną nazwę programu transakcyjnego architektury DRDA (X'07F6C4C2') każdemu requesterowi aplikacji, ponieważ DB2 Universal Database for OS/390 używa tej wartości automatycznie.
4. Utworzyć pozycję w tabeli trybów VTAM dla każdej nazwy trybu, która jest wymagana przez requester aplikacji. Pozycje te opisują wielkość jednostki żądania (RU), wielkość okna pacing i klasę usługi dla nazwy trybu.

5. Zdefiniować limit liczby sesji dla requesterów aplikacji łączących się z serwerem aplikacji DB2 Universal Database for OS/390. Instrukcja VTAM APPL definiuje domyślne limity liczby sesji dla wszystkich systemów partnerskich. Aby ustanowić unikalne wartości domyślne dla danego partnera, można użyć tabeli SYSIBM.LUMODES bazy danych komunikacji (CDB).

   W sekcji “Ustawianie wielkości RU i pacingu” na stronie 63 omówiono sposób przeglądania sieci VTAM.

6. Utworzyć pozycje w bazie danych komunikacji produktu DB2 Universal Database for OS/390, aby zidentyfikować requestery aplikacji, które mają uprawnienia do łączenia się z serwerem aplikacji DB2 Universal Database for OS/390. Oto dwa podstawowe sposoby definiowania pozycji CDB requesterów aplikacji w sieci:

   a. W tabeli SYSIBM.LUNAMES można wstawić wiersz zawierający wartości domyślne dla dowolnej jednostki logicznej, która nie została opisana w bazie danych komunikacji (wiersz domyślny zawiera w kolumnie LUNAME puste znaki). Podejście to umożliwia definiowanie specyficznych wartości dla niektórych jednostek logicznych w sieci, gdy dla wszystkich innych są ustanawiane wartości domyślne.

      Można na przykład pozwolić systemowi DALLAS (innemu niż system DB2 Universal Database for OS/390) wysyłanie już sprawdzonych uprzednio żądań skierowanych do rozproszonej bazy danych (LU 6.2 SECURITY=SAME), jednocześnie z żądaniami wysłania haseł przez systemy menedżerów baz danych. Ponadto można nie zapisywać pozycji w CDB dla każdego systemu menedżera baz danych, zwłaszcza jeśli jest ich wiele. Na Rys. 25 przedstawiono sposób użycia bazy danych komunikacji do podania SECURITY=SAME systemowi DALLAS przy jednoczesnym wymuszeniu opcji SECURITY=PGM dla pozostałych requesterów.

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

Rysunek 25. Ustanawianie wartości domyślnych dla połączeń requestera aplikacji (SNA)

   b. Użyć CDB, aby indywidualnie autoryzować każdego requestera aplikacji w sieci, ustawiając CDB na jeden z następujących sposobów:

      - Nie należy zapisywać wiersza z wartościami domyślnymi w tabeli SYSIBM.LUNAMES. Gdy nie ma wiersza z wartościami domyślnymi (wiersz zawierający pustą nazwę jednostki logicznej), DB2 Universal Database for OS/390 wymaga wiersza w SYSIBM.LUNAMES zawierającego nazwę jednostki logicznej dla każdego requestera aplikacji, który próbuje się z nim połączyć. Jeśli odpowiadający wiersz nie zostanie odnaleziony w CDB, requesterowi aplikacji zostanie odmówione prawo dostępu.

- Zapisać w tabeli SYSIBM.LUNAMES wiersz z wartościami domyślnymi, w którym podano, że wymagane jest sprawdzanie źródła (kolumna USERNAMES jest ustawiona na wartość 'I' lub 'B'). Powoduje to, że DB2 Universal Database for OS/390 ogranicza dostęp do requesterów aplikacji i użytkowników identyfikowanych w tabeli SYSIBM.USERNAMES, co opisano w sekcji “Sprawdzanie źródła żądania” na stronie 77. Można użyć tego sposobu, jeśli reguły translacji nazw wymagają wiersza z pustą nazwą jednostki logicznej (LU) w tabeli SYSIBM.LUNAMES, ale użytkownik nie chce, aby produkt DB2 Universal Database for OS/390 używał tego wiersza do umożliwienia nieograniczonego dostępu do serwera aplikacji DB2 Universal Database for OS/390.

  Na Rys. 26 nie ma wiersza zawierającego puste znaki w kolumnie LUNAME, tak więc DB2 Universal Database for OS/390 uniemożliwia dostęp do jednostek logicznych innych niż LUDALLAS i 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', ' ');
```

Rysunek 26. Identyfikowanie indywidualnych połączeń requestera aplikacji (SNA)

Definiowanie serwera aplikacji (TCP/IP)

Aby serwer aplikacji mógł odbierać żądania rozproszonej bazy danych za pomocą połączeń TCP/IP, musi być zdefiniowany w lokalnym podsystemie TCP/IP i mieć unikalną nazwę RDB_NAME. Ponadto zestaw danych programu startowego produktu DB2 Universal Database for OS/390 musi zawierać niezbędne parametry. Może być również konieczna aktualizacja bazy danych komunikacji produktu DB2 Universal Database for OS/390.

1. Informacje na temat konfigurowania TCP/IP jako serwera aplikacji znajdują się w podręczniku *DB2 Universal Database for OS/390 Installation Reference*. Informacje na temat konfigurowania requestera aplikacji można znaleźć w podręczniku *DB2 Connect Enterprise Edition for OS/2 and Windows Quick Beginnings* oraz *DB2 Connect Personal Edition Krótkie wprowadzenie*.
2. Przykładową definicję zestawu danych programu startowego przedstawiono na Rys. 18 na stronie 55.
3. Aktualizacje bazy danych komunikacji nie są wymagane, jeśli będą używane tylko połączenia przychodzące. Jeśli więc DB2 Universal Database for OS/390 ma być używany tylko jako serwer, to nie należy wypełniać bazy danych komunikacji. W takim przypadku zostaną użyte wartości domyślne. Prosty przykład aktualizacji tabeli SYSIBM.IPNAMES zamieszczono niżej.

   Aby zezwolić węzłom TCP/IP na żądania połączeń z bazą danych, należy użyć następującej komendy SQL aktualizującej tę tabelę:

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

Zapewnianie ochrony

Jeśli requester aplikacji kieruje żądanie rozproszonej bazy danych do serwera aplikacji DB2 Universal Database for OS/390, należy uwzględnić następujące aspekty ochrony:

- sprawdzanie źródła żądania,
- wybór nazw użytkowników,
- parametry ochrony sieci,
- ochronę menedżera baz danych,
- ochronę wymuszoną przez zewnętrzny podsystem ochrony.

Sprawdzanie źródła żądania

Jeśli serwer aplikacji DB2 Universal Database for OS/390 odbiera nazwę użytkownika z requestera aplikacji, może on ograniczyć nazwy użytkowników odebrane z danego requestera aplikacji. Jest to wykonywane przy użyciu sprawdzania *źródła żądania*. Sprawdzanie to umożliwia serwerowi aplikacji określenie, czy podany ID użytkownika może być używany tylko przez określonych partnerów. Na przykład serwer aplikacji może ograniczyć JONES do "źródła żądania" DALLAS. Jeśli inny niż DALLAS requester aplikacji próbuje wysłać nazwę JONES do serwera aplikacji, serwer aplikacji może odrzucić to żądanie, ponieważ źródło żądania tej nazwy w sieci jest niepoprawne.

DB2 Universal Database for OS/390 realizuje sprawdzanie źródła żądania jako część translacji przychodzącej nazwy użytkownika, którą opisano w następnej sekcji.

Uwaga: W przypadku żądań przychodzących połączeń TCP/IP nie jest wykonywane sprawdzanie połączeń przychodzących i źródeł.

Wybieranie nazw użytkowników

Identyfikator użytkownika przysłany przez requester aplikacji może nie być unikalny w sieci SNA. Może być konieczne wykonanie translacji nazw przychodzących przez serwer aplikacji DB2 Universal Database for OS/390 w celu utworzenia unikalnych, w całej sieci, nazw użytkowników. Podobnie może być konieczne wykonanie przez serwer aplikacji DB2 Universal Database for OS/390 translacji nazw wychodzących w celu utworzenia unikalnych nazw użytkowników, przeznaczonych dla serwerów pomocniczych związanych z aplikacją (informacje dotyczące translacji wychodzących nazw użytkowników można znaleźć w sekcji "Zapewnianie ochrony" na stronie 64).

Translację nazw przychodzących można włączyć, ustawiając kolumnę USERNAMES tabeli SYSIBM.LUNAMES lub SYSIBM.IPNAMES na wartość 'I' (translacja nazw przychodzących) lub 'B' (translacja nazw przychodzących i wychodzących). Podczas translacji nazw przychodzących DB2 Universal Database for OS/390 wykonuje translację ID użytkownika wysłanego przez requester aplikacji i nazwę właściciela planu DB2 Universal Database for OS/390 (jeśli requesterem aplikacji jest inny system DB2 Universal Database for OS/390).

Jeśli requester aplikacji wysyła identyfikator i hasło użytkownika w APPC ALLOCATE, sprawdzana jest poprawność identyfikatora i hasła użytkownika zanim identyfikator zostanie poddany translacji. Kolumna PASSWORD w SYSIBM.USERNAMES nie jest używana do sprawdzania poprawności hasła. Poprawność identyfikatora i hasła użytkownika jest natomiast sprawdzana przez zewnętrzny system ochrony (RACF lub produkt będący odpowiednikiem RACF).

Gdy sprawdzany jest przychodzący identyfikator użytkownika w ALLOCATE, DB2 Universal Database for OS/390 ma informacje wyjściowe dotyczące autoryzacji, których użytkownik może użyć, aby dostarczyć listę dodatkowych autoryzacji AUTHID i wykonać dodatkowe sprawdzenie ochrony. Szczegółowe informacje na ten temat można znaleźć w podręczniku *DB2 Universal Database for OS/390 Administration Guide*.

Proces translacji nazw przychodzących szuka wiersza w tabeli SYSIBM.USERNAMES, który musi być zgodny z jednym ze wzorców z poniższej listy (TYPE.AUTHID.LINKNAME):

1. I.AUTHID.LINKNAME — Określony użytkownik z określonego requestera aplikacji.
2. I.AUTHID.puste — Określony użytkownik z dowolnego requestera aplikacji.
3. I.puste.LINKNAME — Dowolny użytkownik z określonego requestera aplikacji.

Jeśli wiersz nie zostanie odnaleziony, wystąpi odmowa dostępu. Jeśli wiersz zostanie odnaleziony, dostęp zdalny będzie dozwolony i nazwa użytkownika zostanie zmieniona na wartość z kolumny NEWAUTHID z wartością pustą NEWAUTHID, wskazującą, że nazwa nie została zmieniona. Dowolne sprawdzenie autoryzacji do zasobów DB2 Universal Database for OS/390 (na przykład uprawnienia do tabeli SQL) wykonane przez DB2 Universal Database for OS/390 jest przeprowadzane na nazwach użytkowników po translacji, a nie na pierwotnych nazwach użytkowników.

Jeśli serwer aplikacji DB2 Universal Database for OS/390 otrzyma nazwę użytkownika od requestera aplikacji, funkcje wykonujące translację nazw przychodzących można wykorzystać również do innych zadań:

- Można zmienić nazwę użytkownika na unikalną. Na przykład następujące instrukcje SQL wykonują translację nazwy użytkownika JONES z requestera aplikacji NEWYORK (LUNAME LUNYC) na inną nazwę (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', ' ');
```

- Można zmienić nazwę użytkownika, tak aby cała grupa użytkowników była reprezentowana przez jedną nazwę. Na przykład wszyscy użytkownicy requestera aplikacji NEWYORK (LUNAME LUNYC) mogą mieć nazwę NYUSER. Umożliwi

to nadawanie uprawnień SQL nazwie NYUSER i sterowanie dostępem SQL udzielonym użytkownikom z 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', ' ');
```

- Można ograniczyć nazwy użytkowników przesyłane przez określony requester aplikacji. Podczas translacji nazwy użytkownika następuje również sprawdzanie źródła żądania opisane w sekcji “Sprawdzanie źródła żądania” na stronie 77. Na przykład następujące instrukcje SQL dopuszczają tylko SMITH i JONES jako nazwy użytkowników z requestera aplikacji NEWYORK. Użytkownik o innej nazwie nie ma dostępu, ponieważ nie ma go w tabeli 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', ' ', ' ');
```

- Można ograniczyć requestery aplikacji, które mogą się połączyć z serwerem aplikacji DB2 Universal Database for OS/390. Jest to kolejna funkcja sprawdzania źródła żądania. Poniższy przykład akceptuje każdą nazwę użytkownika przysłaną przez requestera aplikacji NEWYORK (LUNYC) lub CHICAGO (LUCHI). Inne requestery aplikacji nie mają dostępu, ponieważ domyślny wiersz SYSIBM.LUNAMES określa translację nazw przychodzących dla wszystkich żądań przychodzących.

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

Zapewnianie ochrony sieci

Jednostka logiczna 6.2 udostępnia trzy główne opcje ochrony sieci dla połączeń SNA:

- ochronę na poziomie sesji,
- ochronę na poziomie konwersacji,
- szyfrowanie.

W sekcji “Ochrona sieci” na stronie 69 omówiono sposób określenia ochrony na poziomie sesji i szyfrowania z DB2 Universal Database for OS/390. Serwer aplikacji DB2 Universal Database for OS/390 używa ochrony na poziomie sesji i szyfrowania dokładnie w taki sam sposób, jak requester aplikacji DB2 Universal Database for OS/390.

Uwagi dotyczące ochrony sieci ograniczają się tylko do ochrony na poziomie konwersacji SNA. Aspekty ochrony na poziomie konwersacji są unikalne dla serwera aplikacji DB2 Universal Database for OS/390. Serwer aplikacji DB2 Universal Database for OS/390 pełni dwie różne role w ochronie sieci:

- Jako requester serwerów pomocniczych serwer aplikacji DB2 Universal Database for OS/390 jest odpowiedzialny za wydawanie żądań APPC, które zawierają parametry ochrony na poziomie konwersacji SNA wymagane przez serwery pomocnicze. Serwer aplikacji DB2 Universal Database for OS/390 używa kolumny USERNAMES z tabeli SYSIBM.LUNAMES i tabeli SYSIBM.USERNAMES do definiowania wymagań dotyczących ochrony na poziomie konwersacji SNA dla każdego serwera pomocniczego. Szczegóły tych definicji są identyczne jak te, które opisano w sekcji “Ochrona sieci” na stronie 69.
- Jako serwer requestera aplikacji serwer aplikacji DB2 Universal Database for OS/390 narzuca ograniczenia dotyczące ochrony na poziomie konwersacji SNA dla requestera aplikacji. DB2 Universal Database for OS/390 używa kolumny USERSECURITY z tabeli SYSIBM.LUNAMES, aby określić poziom konwersacji wymagany dla każdego requestera aplikacji w sieci. W kolumnie USERSECURITY są stosowane następujące wartości:

  C Wskazuje, że DB2 Universal Database for OS/390 wymaga, aby requester aplikacji z każdym żądaniem wysłał identyfikator użytkownika i hasło (LU 6.2 SECURITY=PGM) do rozproszonej bazy danych. Jeśli kolumna ENCRYPTPSWDS w SYSIBM.LUNAMES zawiera 'Y', DB2 Universal Database for OS/390 zakłada, że hasło jest już w zaszyfrowanym formacie RACF (jest to możliwe tylko dla requestera aplikacji DB2 Universal Database for OS/390). Jeśli kolumna ENCRYPTPSWDS nie zawiera wartości 'Y', DB2 Universal Database for OS/390 oczekuje hasła w formacie standardowym LU 6.2 (reprezentacja znakowa EBCDIC). W obu przypadkach DB2 Universal Database for OS/390 przesyła wartości identyfikatora użytkownika i hasła do podsystemu ochrony w celu sprawdzenia poprawności. Podsystem ochrony udostępnia sprawdzenie identyfikatora i hasła użytkownika APPC; na przykład RACF ma funkcję służącą do sprawdzania identyfikatorów i haseł użytkowników APPC. Jeśli podsystem ochrony odrzuci parę identyfikator-hasło użytkownika, dostęp do rozproszonej bazy danych będzie niemożliwy.

  Inna wartość
  Wskazuje, że requester aplikacji może wysyłać już sprawdzony identyfikator użytkownika (LU 6.2 SECURITY=SAME) lub identyfikator i hasło użytkownika (LU 6.2 SECURITY=PGM). Jeśli identyfikator i hasło

użytkownika zostaną wysłane, DB2 Universal Database for OS/390 przetworzy je, jak to opisano dla wartości 'C'. Jeśli żądanie zawiera tylko identyfikator użytkownika, podsystem ochrony jest wywoływany, aby uwierzytelnić użytkownika, chyba że tabela SYSUSERNAMES jest używana do zarządzania przychodzącymi identyfikatorami użytkowników.

W przypadku wykrycia naruszenia ochrony LU 6.2 wymaga, aby serwer aplikacji DB2 Universal Database for OS/390 zwrócił kod znaczenia uszkodzenia ochrony SNA ('080F6051'X) do requestera aplikacji. Ponieważ niniejszy kod znaczenia nie opisuje przyczyny występowania uszkodzenia, DB2 Universal Database for OS/390 dostarcza dwóch metod odczytywania przyczyny naruszenia ochrony rozproszonej:

- Wygenerowanie komunikatu DSNL030I, który zawiera identyfikator LUWID i kod przyczyny opisujący awarię. Komunikat DSNL030I zawiera także identyfikator AUTHID (jeśli jest znany), który został wysłany z odrzuconego żądania aplikacji.
- Zapisanie alertu w bazie danych monitorowania sprzętu NETVIEW, która zawiera informacje dostarczone w komunikacie DSNL030I.

Ochrona menedżera baz danych

Jako właściciel zasobów bazy danych serwera aplikacji DB2 Universal Database for OS/390 steruje funkcjami ochrony bazy danych dla obiektów SQL rezydujących na serwerze aplikacji DB2 Universal Database for OS/390. Dostęp do obiektów zarządzanych przez DB2 Universal Database for OS/390 jest sterowany przez uprawnienia nadawane użytkownikom przez administratora DB2 Universal Database for OS/390 lub właścicieli obiektów indywidualnych. Oto dwie podstawowe klasy obiektów, które są sterowane przez serwer aplikacji DB2 Universal Database for OS/390:

- **Pakiety** — Użytkownicy indywidualni są autoryzowani do tworzenia, wymiany i uruchamiania pakietów przy użyciu instrukcji GRANT systemu DB2 Universal Database for OS/390. Gdy użytkownik jest właścicielem pakietu, może on automatycznie uruchamiać i wymieniać pakiet. Inni użytkownicy muszą mieć specjalną autoryzację do uruchamiania pakietu na serwerze aplikacji DB2 Universal Database for OS/390 przy użyciu instrukcji GRANT. Uprawnienie USE można nadać użytkownikom indywidualnym PUBLIC, co umożliwia wszystkim użytkownikom uruchomienie pakietu.

  Jeśli aplikacja zostaje powiązana z DB2 Universal Database for OS/390, pakiet zawiera instrukcje SQL w aplikacji. Instrukcje SQL są klasyfikowane jako:

  Statyczny SQL
  Statyczny SQL oznacza, że instrukcja SQL oraz obiekty, do których się ona odnosi, są znane w momencie powiązania aplikacji z DB2 Universal Database for OS/390. Osoba tworząca pakiet musi mieć uprawnienia do wykonywania każdej statycznej instrukcji SQL zawartej w pakiecie.

  Gdy użytkownicy otrzymują uprawnienia do wykonywania pakietu, otrzymują automatycznie uprawnienia do wykonywania każdej zawartej w nim statycznej instrukcji SQL. W ten sposób użytkownicy nie potrzebują

żadnych uprawnień do tabel DB2 Universal Database for OS/390, jeśli pakiet, który wykonują, zawiera wyłącznie statyczne instrukcje SQL.

Dynamiczny SQL
Dynamiczny SQL opisuje instrukcje SQL, które nie są znane aż do rozpoczęcia wykonywania programu. Innymi słowy instrukcja SQL jest tworzona przez program i dynamicznie wiązana z DB2 Universal Database for OS/390 przy użyciu instrukcji SQL PREPARE. Gdy użytkownik wykonuje dynamiczną instrukcję SQL, musi mieć uprawnienia do tabeli wymagane do wykonywania instrukcji SQL. Ponieważ w momencie tworzenia planu lub pakietu instrukcja SQL jest nieznana, użytkownik nie otrzymuje automatycznie wymaganych uprawnień od właściciela pakietu.

- **Obiekty SQL** — Są to tabele, widoki, synonimy i aliasy. Użytkownikom DB2 Universal Database for OS/390 można nadawać różne poziomy uprawnień do tworzenia, usuwania, zmiany i odczytu indywidualnych obiektów SQL. Uprawnienia są wymagane do wiązania statycznej instrukcji SQL lub do wykonywania dynamicznej instrukcji SQL.

Po utworzeniu pakietu opcja DISABLE/ENABLE umożliwia kontrolowanie, które typy połączeń DB2 Universal Database for OS/390 mogą uruchamiać pakiet. Można używać RACF i procedur wyjściowych ochrony DB2 Universal Database for OS/390, aby umożliwiać użytkownikom selektywne wykorzystanie DDF. Można użyć RLF, aby określić ograniczenia czasu procesora dla wiązań zdalnych i dynamicznego wykonywania SQL.

Należy rozważyć pakiet DB2 Universal Database for OS/390 o nazwie MYPKG, którego właścicielem jest JOE. JOE może umożliwić SAL wykonanie pakietu przez wydanie instrukcji DB2 Universal Database for OS/390 GRANT USE. Gdy SAL wykona pakiet:

- DB2 Universal Database for OS/390 sprawdzi, czy SAL ma uprawnienia USE dla pakietu.
- SAL może wydać każdą statyczną instrukcję SQL w pakiecie, ponieważ JOE miał wymagane uprawnienia obiektu SQL do tworzenia pakietu.
- Jeśli pakiet ma dynamiczne instrukcje SQL, SAL musi mieć własne uprawnienia w tabeli SQL. Na przykład SAL nie może wydać instrukcji SELECT * FROM JOE.TABLE5, chyba że nadano jej prawo do odczytu tabeli JOE.TABLE5.

Podsystem ochrony

Wykorzystanie przez serwer aplikacji DB2 Universal Database for OS/390 podsystemu ochrony (RACF lub produktu będącego odpowiednikiem RACF) zależy od sposobu zdefiniowania funkcji translacji nazw przychodzących w tabeli SYSIBM.LUNAMES:

- Jeśli w kolumnie USERNAMES jest określone 'I' lub 'B', translacja nazw przychodzących jest aktywna i DB2 Universal Database for OS/390 zakłada, że administrator DB2 Universal Database for OS/390 wykorzystuje translację nazw przychodzących do wykonywania części pracy związanej z ochroną systemu.

Zewnętrzny podsystem ochrony jest wywoływany tylko wtedy, gdy requester aplikacji wyśle żądanie zawierające identyfikator i hasło użytkownika (SECURITY=PGM). Podsystem ochrony udostępnia sprawdzenie identyfikatora i hasła użytkownika APPC; na przykład RACF ma funkcję służącą do sprawdzania identyfikatorów i haseł użytkowników APPC.

Jeśli żądanie z requestera aplikacji zawiera tylko identyfikator użytkownika (SECURITY=SAME), zewnętrzny system ochrony nie zostanie w ogóle wywołany, ponieważ reguły translacji nazw przychodzących definiują, który użytkownik może połączyć się z serwerem aplikacji DB2 Universal Database for OS/390.

- Jeśli w kolumnie USERNAMES jest określona wartość inna niż 'I' lub 'B', zostanie wykonane następujące sprawdzenie podsystemu ochrony:
  - Gdy z requestera aplikacji zostanie odebrane żądanie rozproszonej bazy danych, DB2 Universal Database for OS/390 wywoła zewnętrzny system ochrony w celu sprawdzenia poprawności identyfikatora użytkownika końcowego (oraz hasła, jeśli zostało udostępnione).
  - Zewnętrzny system ochrony jest wywoływany do sprawdzenia, czy użytkownik ma autoryzację do łączenia się z podsystemem DB2 Universal Database for OS/390.
- W pozostałych przypadkach informacje wyjściowe autoryzacji są udostępniane w celu zapewnienia listy pomocniczych identyfikatorów autoryzowanego użytkownika. Więcej informacji można znaleźć w podręczniku *DB2 Universal Database for OS/390 Administration Guide*.

Reprezentacja danych

Należy się upewnić, że podsystem DB2 Universal Database for OS/390 może przekształcić każdy skrócony identyfikator CCSID requestera aplikacji na skrócony identyfikator CCSID instalacji podsystemu DB2 Universal Database for OS/390. Więcej informacji można znaleźć w sekcji “Reprezentacja danych” na stronie 72.

Rozdział 3. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu SNA

System operacyjny OS/400 zawiera DB2 Universal Database for AS/400, system zarządzania relacyjnymi bazami danych firmy IBM dla systemów AS/400.

W rozdziale tym wyjaśniono, jak skonfigurować system AS/400, aby obsługiwał połączenia:

1. Od stacji roboczych DB2 Connect (patrz “Konfigurowanie serwera aplikacji” na stronie 95),
2. Do serwera DB2 Universal Database (patrz “Konfigurowanie requestera aplikacji”).

Informacje na temat łączenia dwóch systemów AS/400 można znaleźć w podręczniku *AS/400 Distributed Database Programming*.

W DB2 Universal Database for AS/400 wersja 4.2 wprowadzona została obsługa komunikacji DRDA przy użyciu protokołu TCP/IP. Głównym źródłem informacji na ten temat jest także podręcznik *AS/400 Distributed Database Programming* oraz podsumowanie wymaganych kroków z tego podręcznika, które można znaleźć w “Rozdział 4. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu TCP/IP” na stronie 101. Zasady są identyczne jak przedstawione w tym rozdziale, ale zadania konfiguracji sieci są znacznie prostsze.

Implementacja DB2 Universal Database for AS/400

W rozdziale tym opisano, jak DB2 Universal Database for AS/400 obsługuje systemy rozproszonych baz danych. Program licencjonowany OS/400 V2R2M1 obsługuje zdalne jednostki pracy DRDA, a OS/400 V3R1 obsługuje ponadto rozproszone jednostki pracy DRDA (DUOW). Obsługa ta jest częścią systemu operacyjnego OS/400. Oznacza to, że do korzystania z obsługi DRDA lub uruchomienia programów z instrukcjami SQL nie jest potrzebny program licencjonowany DB2 Universal Database for AS/400 Query Manager ani zestaw SQL Development Kit.

Konfigurowanie requestera aplikacji

System AS/400 implementuje obsługę requestera aplikacji DRDA jako integralną część systemu operacyjnego OS/400. Ponieważ obsługa requestera aplikacji jest częścią systemu operacyjnego OS/400, jest ona aktywna zawsze, gdy aktywny jest system operacyjny. Dotyczy to również obsługi serwera aplikacji w DB2 Universal Database for AS/400.

Jeśli DB2 Universal Database for AS/400 pełni rolę requestera aplikacji, może połączyć się z dowolnym serwerem aplikacji, który obsługuje sieć DRDA. Aby requester aplikacji DB2 Universal Database for AS/400 zapewniał dostęp do rozproszonej bazy danych, należy wziąć pod uwagę następujące zagadnienia:

- dostarczanie informacji sieciowych,
- zapewnianie ochrony,
- reprezentację danych.

Dostarczanie informacji sieciowych

Requester aplikacji musi mieć możliwość zaakceptowania nazwy relacyjnych baz danych i jej translacji na parametry sieciowe. System AS/400 wykorzystuje katalog relacyjnych baz danych do rejestrowania nazw relacyjnych baz danych i odpowiadających im parametrów sieciowych. Katalog ten umożliwia requesterowi aplikacji AS/400 przekazanie informacji sieciowych koniecznych do nawiązania komunikacji w sieci rozproszonych baz danych.

Większość procesów przetwarzania w środowisku rozproszonych baz danych wymaga wymiany komunikatów z innymi miejscami w sieci. Aby przetwarzanie w środowisku SNA odbywało się poprawnie, należy:

- Zdefiniować system lokalny w DB2 Universal Database for AS/400.
- Zdefiniować system zdalny w DB2 Universal Database for AS/400.
- Zdefiniować komunikację w DB2 Universal Database for AS/400.

Definiowanie systemu lokalnego w DB2 Universal Database for AS/400

Każdy requester aplikacji w sieci rozproszonych baz danych musi mieć pozycję w swoim katalogu relacyjnych baz danych dla swojej lokalnej relacyjnej bazy danych i jedną pozycję dla każdej zdalnej relacyjnej bazy danych, z której korzysta. Dowolny system AS/400 w sieci rozproszonych baz danych, który działa tylko jako serwer aplikacji, musi mieć w swoim katalogu relacyjnych baz danych pozycję dla lokalnej relacyjnej bazy danych. Więcej informacji o katalogu relacyjnych baz danych można znaleźć w podręczniku *AS/400 Distributed Database Programming*.

Aby zdefiniować system lokalny, należy nadać nazwę lokalnej bazie danych, dodając pozycję do katalogu relacyjnych baz danych z nazwą miejsca zdalnego jako *LOCAL. Aby to zrobić, należy użyć komendy Dodaj pozycję do katalogu relacyjnych baz danych (Add Relational Database Directory Entry - ADDRDBDIRE). Przykład komendy ADDRDBDIRE, gdzie nazwą bazy danych requestera aplikacji jest ROCHESTERDB:

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

Więcej informacji o komendach katalogu relacyjnych baz danych można znaleźć w podręczniku *AS/400 Distributed Database Programming*.

Uwaga: W najnowszych wersjach systemu OS/400 pozycja nazwy lokalnej relacyjnej bazy danych jest tworzona automatycznie, jeśli nie istnieje w momencie wywołania. Jako nazwa lokalna będzie użyta nazwa systemu określona w atrybutach sieciowych.

Definiowanie systemu zdalnego w DB2 Universal Database for AS/400

Każdy serwer aplikacji w rozproszonej sieci baz danych także musi mieć lokalną pozycję w swoim katalogu relacyjnych baz danych. Dodatkowo w katalogu relacyjnych baz danych musi znajdować się pozycja dla każdej zdalnej bazy danych każdego requestera aplikacji. Aby utworzyć wszystkie potrzebne pozycje, należy:

- Zdefiniować zdalną bazę danych jako lokalną bazę danych przez dodanie pozycji dla każdej zdalnej bazy danych w katalogu relacyjnych baz danych za pomocą komendy ADDRDBDIRE lub WRKRDBDIRE. W przypadku komunikacji SNA można określić następujące informacje:
  - nazwę zdalnej bazy danych,
  - nazwę miejsca zdalnego bazy danych,
  - nazwę miejsca lokalnego,
  - nazwę trybu użytego do nawiązania połączenia,
  - identyfikator sieci zdalnej,
  - nazwę urządzenia użytego do komunikacji,
  - nazwę programu transakcyjnego zdalnej bazy danych.

  W większości przypadków jedyną potrzebną informacją jest nazwa zdalnej bazy danych i nazwa miejsca zdalnego[4] bazy danych. Jeśli określona jest tylko nazwa miejsca zdalnego, zamiast pozostałych parametrów przyjmowane są wartości domyślne. System wybiera opis urządzenia, korzystając z nazwy miejsca zdalnego.

  Jeśli więcej niż jedno urządzenie zawiera identyczną nazwę miejsca zdalnego, a wymagany jest specyficzny opis urządzenia, wtedy wartości dla nazwy miejsca lokalnego i identyfikatora sieci zdalnej w pozycji katalogu relacyjnych baz danych powinny pasować do wartości w opisie urządzenia. Wybór opisu urządzenia może być bardziej skomplikowany, jeśli identyczna nazwa miejsca zdalnego jest użyta w więcej niż jednym opisie urządzenia. Aby uniknąć zamieszania, należy używać unikalnych nazw miejsc zdalnych w każdym opisie urządzenia. Jako domyślna wartość nazwy programu transakcyjnego przyjmowana jest domyślna nazwa programu transakcyjnego DRDA X'07F6C4C2'.

  Informacje dotyczące komunikacji w katalogu relacyjnych baz danych są używane do nawiązania konwersacji z systemem zdalnym.

4. “Nazwa miejsca” w systemie OS/400 jest równoznaczna z “nazwą jednostki logicznej” w VTAM. “Nazwa miejsca zdalnego” oznacza “nazwę partnerskiej lub zdalnej jednostki logicznej”.

W przypadku połączeń TCP/IP (obsługiwanych w DB2 Universal Database for AS/400 wersja 4.2), wymagana jest tylko nazwa zdalnej bazy danych oraz powiązane adresy IP i porty. Patrz “Rozdział 4. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu TCP/IP” na stronie 101.

Definiowanie komunikacji SNA

W tej sekcji opisano konfigurowanie komunikacji w systemie AS/400 przy użyciu zaawansowanej sieci każdy z każdym (APPN). System AS/400 umożliwia także konfigurację zaawansowanej komunikacji między programami (APPC), która nie obsługuje routingu sieciowego. Rozproszona baza danych AS/400 działa w obu konfiguracjach. Więcej informacji o konfiguracjach APPC można znaleźć w podręczniku *OS/400 Communications Configuration*.

Obsługa AnyNet w systemie AS/400 umożliwia działanie aplikacji APPC w sieci TCP/IP. Zamieszczone dalej przykłady zawierają zarządzanie danymi rozproszonymi (DDM), usługi SNADS (Systems Network Architecture Distribution Services), alerty i tranzyt terminalu typu 5250. Aplikacje te wraz z DRDA mogą być uruchamiane bez zmian w sieci TCP/IP z paroma dodatkowymi ustawieniami. Aby określić obsługę AnyNet, należy podać *ANYNW w parametrze LINKTYPE komendy CRTCTLAPPC.

Więcej informacji o APPC w sieci TCP/IP można znaleźć w podręcznikach *OS/400 Communications Configuration* i *OS/400 TCP/IP Configuration and Reference*. (Rodzima obsługa TCP/IP dla komunikacji DRDA jest dostarczana w DB2 Universal Database for AS/400 wersja 4.2. Patrz “Rozdział 4. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu TCP/IP” na stronie 101.

APPN zapewnia obsługę sieci umożliwiającą systemowi AS/400 włączenie się do sieci systemów i ich kontrolę, która nie wymaga obsługi sieci tradycyjnie dostarczanej przez system mainframe. Następujące kroki wyjaśniają, jak skonfigurować system AS/400 do obsługi APPN.

1. Zdefiniować atrybuty sieciowe za pomocą komendy Zmień atrybuty sieciowe (Change Network Attributes - CHGNETA).

   Atrybuty sieciowe zawierają:

   - nazwę systemu lokalnego,
   - nazwę systemu w sieci APPN,
   - identyfikator sieci lokalnej,
   - typ węzła sieci,
   - nazwy serwerów sieciowych używanych przez system AS/400, jeśli komputer jest węzłem końcowym,
   - sieciowe punkty kontrolne, jeśli AS/400 jest węzłem końcowym.

2. Utworzyć opis linii.

   Opis linii to opis połączenia fizyczną linią i protokołu łącza danych, używanego między systemem AS/400 i siecią. Do utworzenia opisu linii służą następujące komendy:

- Utwórz opis linii (Ethernet) (Create line description - CRTLINETH),
- Utwórz opis linii (SDLC) (Create line description - CRTLINSDLC),
- Utwórz opis linii (Token-Ring)(Create line description - CRTLINTRN)
- Utwórz opis linii (X.25) (Create line description - CRTLINX25).

3. Utworzyć opisy kontrolera.

   Opis kontrolera określa systemy przylegające w sieci. Należy wskazać użycie obsługi APPN przez podanie APPN(*YES) przy tworzeniu opisu kontrolera. Do utworzenia opisu kontrolera służą następujące komendy:

   - Utwórz opis kontrolera (APPC) (Create controller description - CRTCTLAPPC)
   - Utwórz opis kontrolera (SNA HOST)(Create controller description - CRTCTLHOST)

   Jeśli parametr AUTOCRTCTL w opisie linii Token-Ring lub Ethernet ma ustawioną wartość *YES, opis kontrolera będzie tworzony automatycznie, gdy system otrzyma przez linię Token-Ring lub Ethernet żądanie rozpoczęcia sesji.

4. Utworzyć opis klasy usług.

   Należy użyć opisu klasy usługi do wyboru trasy komunikacji i nadania priorytetów transmisji. System dostarcza pięć opisów klasy usług:

   #CONNECT
   Domyślna klasa usługi.

   #BATCH
   Klasa usługi dla zadań wsadowych.

   #BATCHSC
   Tak jak #BATCH, ale wymagana jest ochrona łącza danych co najmniej w sieci komutacji pakietów. W sieci komutacji pakietów dane nigdy nie przechodzą przez sieć tą samą ścieżką.

   #INTER
   Klasa usługi dostosowana do komunikacji interaktywnej.

   #INTERSC
   Tak jak #INTER, ale wymagana jest ochrona łącza danych co najmniej w sieci komutacji pakietów.

   Inne opisy klasy usługi tworzone są za pomocą komendy Utwórz klasę usługi (Create Class-of-Service - CRTCOSD).

5. Utworzyć opis trybu.

   Opis trybu zawiera charakterystykę sesji i liczbę sesji, które mogą być używane w negocjacji dozwolonych wartości między miejscem lokalnym i zdalnym. Opis trybu wskazuje także na klasę usługi użytą do konwersacji. Wraz z systemem dostarczanych jest kilka predefiniowanych trybów:

BLANK
Domyślna nazwa trybu określona w atrybutach sieciowych w dostarczonym systemie.

#BATCH
Tryb dostosowany do zadań wsadowych.

#BATCHSC
Tak jak #BATCH, ale powiązany opis klasy usługi wymaga ochrony łącza danych co najmniej w sieci komutacji pakietów.

#INTER
Tryb dostosowany do komunikacji interaktywnej.

#INTERSC
Tak jak #INTER, ale powiązany opis klasy usługi wymaga ochrony łącza danych co najmniej w sieci komutacji pakietów.

IBMRDB
Tryb dostosowany do komunikacji DRDA.

Inne opisy trybów można tworzyć za pomocą komendy Utwórz opis trybu (Create Mode Description - CRTMODD).

6. Utworzyć opisy urządzeń.

   Opis urządzenia zawiera charakterystykę połączenia logicznego między systemem lokalnym i zdalnym. Jeśli system AS/400 działa w sieci APPN jako niezależna jednostka logiczna (LU), nie należy ręcznie tworzyć opisu urządzenia. System AS/400 automatycznie tworzy opis urządzenia i przy ustanawianiu sesji podłącza go do odpowiedniego opisu kontrolera przy nawiązywaniu sesji. Jeśli system AS/400 jest zależną jednostką logiczną, konieczne jest ręczne utworzenie opisu urządzenia za pomocą komendy Utwórz opis urządzenia (Create Device Description - CRTDEVAPPC). W opisie urządzenia należy określić APPN(*YES), aby wskazać, że używana jest sieć APPN.

7. Utworzyć listę miejsc APPN.

   Jeśli wymagane są dodatkowe miejsca lokalne (nazywane w innych systemach *jednostkami logicznymi LU*) lub specjalne charakterystyki miejsc zdalnych dla APPN, należy utworzyć listę miejsc APPN. Nazwa miejsca lokalnego jest nazwą punktu kontrolnego określoną w atrybutach sieciowych. Jeśli potrzebne są dodatkowe miejsca dla systemu AS/400, wymagana jest lista miejsc lokalnych. Przykładem specjalnej charakterystyki miejsca zdalnego jest sytuacja, gdy miejsce to znajduje się w innej sieci niż miejsce lokalne. W takim wypadku wymagana jest lista miejsc zdalnych. Listę miejsc APPN można utworzyć za pomocą komendy Utwórz listę konfiguracji (Create Configuration List - CRTCFGL).

8. Uaktywnić (udostępnić) komunikację.

   Opis komunikacji można uaktywnić za pomocą komendy Zmień status konfiguracji (Vary Configuration - VRYCFG) lub komendy Pracuj ze statusami konfiguracji (Work With Configuration Status - WRKCFGSTS). Jeśli opisy linii są uaktywnione,

uaktywnione są także odpowiednie kontrolery i urządzenia podłączone do tej linii. Komenda WRKCFGSTS jest też użyteczna przy przeglądaniu statusu każdego połączenia.

9. Wielkości RU i pacing.

   Wielkości RU i pacing zależą od wartości określonych w opisie trybu. Przy tworzeniu opisu trybu zarówno wielkości RU, jak i pacing przyjmują wartości domyślne. Są to wartości szacunkowe systemu AS/400 dla większości środowisk, w tym rozproszonych baz danych. Jeśli wartość domyślna jest brana dla wielkości RU, system AS/400 szacuje najlepszą wartość. Jeśli system AS/400 komunikuje się z innym systemem, który obsługuje pacing dostosowujący się, podane wartości pacing stanowią tylko punkt wyjściowy. Pacing jest dopasowywany przez każdy system do jego możliwości obsłużenia napływających danych. W przypadku systemów, które nie obsługują pacingu dostosowującego się, wartości pacing są negocjowane na początku sesji i pozostają nie zmienione przez całą sesję. Więcej informacji można znaleźć w podręczniku *OS/400 Communications Configuration*.

Uwagi:

1. Opis kontrolera jest odpowiednikiem makr jednostek fizycznych (PU) w NCP/VTAM (IBM Network Control Program and Virtual Telecommunications Access Method).
2. Opis urządzenia jest odpowiednikiem makra jednostki logicznej (LU) w NCP/VTAM. Opis urządzenia zawiera informacje podobne do przechowywanych w profilu partnerskiej jednostki logicznej w programie Communications Manager/2 1.1.
3. Opis trybu jest odpowiednikiem tabel trybów NCP/VTAM i profilu CMTS (Communications Manager Transmission Service Mode).

Więcej informacji na temat konfiguracji do obsługi sieci i pracy z listami miejsc można znaleźć w podręcznikach *OS/400 Communications Configuration* i *APPN Support*. Przykłady wykorzystania CL w definiowaniu konfiguracji systemu można znaleźć w podręczniku *AS/400 Distributed Database Programming*.

Zapewnianie ochrony

Jeśli system zdalny przetwarza rozproszoną bazę danych w imieniu aplikacji SQL, musi być możliwe spełnienie wymogów ochrony requestera aplikacji, serwera aplikacji i sieci ich łączącej. Wymagania te należą do co najmniej jednej z następujących kategorii:

- wybór nazw użytkowników,
- parametry ochrony sieci,
- ochrona menedżera baz danych,
- ochrona narzucona przez ochronę AS/400.

Wybieranie nazw użytkowników

W systemach AS/400 użytkownicy są przypisani do identyfikatorów użytkowników, składających się z 1 do 10 znaków, unikalnych w danym systemie, ale niekoniecznie w całej sieci. Identyfikator użytkownika jest przekazywany do systemu zdalnego, gdy

między dwiema bazami danych ustanawiane jest połączenie. Aby zapobiec konfliktom w sieci między identyfikatorami użytkowników, przed wysłaniem nazwy przez sieć często stosowana jest translacja nazw wychodzących, zmieniająca identyfikator użytkownika. Jednak system AS/400 nie dokonuje translacji nazw wychodzących w celu rozwiązania potencjalnych konfliktów na serwerze. Konflikty te muszą być rozwiązane na serwerze aplikacji, o ile nie są użyte dodatkowe klauzule USER i USING instrukcji SQL CONNECT systemu AS/400. USER to poprawny identyfikator na serwerze aplikacji, a USING to odpowiadające mu hasło użytkownika.

Ochrona sieci

Po wybraniu nazw użytkowników reprezentujących aplikację zdalną, requester aplikacji musi dostarczyć wymagane informacje ochrony sieci jednostki logicznej 6.2 (LU 6.2). Jednostka logiczna 6.2 udostępnia trzy główne opcje ochrony sieci:

- ochrona na poziomie sesji, reprezentuje ją parametr LOCPWD w komendzie CRTDEVAPPC,
- ochrona na poziomie konwersacji, sterowana przez system operacyjny OS/400,
- szyfrowanie danych, którego nie obsługuje system operacyjny OS/400.

Ochrona na poziomie sesji jest udostępniana przez weryfikację między jednostkami logicznymi. Każda jednostka logiczna ma klucz, który musi pasować do klucza zdalnej jednostki logicznej. Klucz podawany jest w parametrze LOCPWD komendy CRTDEVAPPC.

Serwer aplikacji jest odpowiedzialny za zarządzanie zasobami baz danych, dlatego decyduje on, które opcje ochrony sieci są wymagane od requestera aplikacji. Administrator ochrony AS/400 musi sprawdzić wymagania ochrony każdego serwera aplikacji, aby nie wymagały one więcej niż obsługuje requester aplikacji AS/400.

Możliwe opcje ochrony konwersacji SNA:

SECURITY=SAME
: Zwana również ochroną sprawdzoną uprzednio. Do systemu zdalnego jest wysyłany tylko identyfikator użytkownika aplikacji, nie jest zaś wysyłane hasło. W wersjach poprzedzających system AS/400 wersja 2 wydanie 2 modyfikacja 0 ten poziom ochrony konwersacji był jedynym poziomem obsługiwanym przez requester aplikacji AS/400.

SECURITY=PGM
: Powoduje wysłanie identyfikatora i hasła użytkownika aplikacji do systemu zdalnego w celu sprawdzenia poprawności. W wersjach poprzedzających system AS/400 wersja 2 wydanie 2 modyfikacja 0 ta opcja ochrony nie była obsługiwana przez requester aplikacji AS/400.

SECURITY=NONE
: Opcja nie obsługiwana, jeśli system AS/400 jest requesterem aplikacji.

Ochrona menedżera baz danych

System AS/400 nie ma zewnętrznego podsystemu ochrony. Ochroną zajmuje się system operacyjny OS/400, jak to przedstawiono w sekcji “Ochrona systemu”.

Ochrona systemu

System operacyjny OS/400 steruje autoryzacją do wszystkich obiektów w systemie, włącznie z programami, pakietami, tabelami, widokami i kolekcjami.

Requester aplikacji steruje dostępem do obiektów, które się w nim znajdują. Ochroną obiektów na serwerze aplikacji zajmuje się serwer aplikacji na podstawie identyfikatora użytkownika wysłanego przez requester aplikacji. Identyfikator użytkownika wysyłany do serwera aplikacji jest powiązany z użytkownikiem requestera aplikacji lub identyfikatorem użytkownika podanym w klauzuli USER instrukcji SQL CONNECT systemu AS/400. Na przykład: CONNECT TO nazwa_bazy_danych USER ID_użytkownika USING hasło.

Ochroną obiektów można zarządzać za pomocą komend w języku CL uprawnień do obiektu lub instrukcji SQL GRANT i REVOKE. Komendy CL dotyczące uprawnień do obiektu to: Nadaj uprawnienia do obiektów (Grant Object Authority - GRTOBJAUT) i Odwołaj uprawnienia do obiektów (Revoke Object Authority - RVKOBJAUT). Komendy te działają na dowolny obiekt w systemie. Instrukcje GRANT i REVOKE działają tylko na obiekty SQL: tabele, widoki i pakiety. Aby zmienić autoryzację dla innych obiektów, takich jak programy czy kolekcje, należy użyć komend GRTOBJAUT i RVKOBJAUT.

Nadawanie i odwoływanie uprawnień: Aby nadać użytkownikowi USER1 uprawnienie *USE do programu PGMA, należy wprowadzić w systemie AS/400 komendę:

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

Komenda odwołania tego uprawnienia:

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

Wartość *PGM oznacza, że w tym przykładzie typem obiektu jest program. Wartość *SQLPKG jest używana do działań na pakietach, *LIB dla kolekcji, a *FILE dla tabeli.

Komendy GRTOBJAUT i RVKOBJAUT można także używać w celu zapobiegania tworzeniu przez użytkowników programów i pakietów. Użytkownik nie ma możliwości utworzenia programu, jeśli nie ma uprawnień do komend typu CRTSQLxxx (gdzie xxx = RPG, C, CBL, FTN lub PLI), które służą do tworzenia programów. Jeśli uprawnienie do komendy CRTSQLPKG jest odwołane, użytkownik nie ma możliwości tworzenia pakietów z requestera aplikacji lub na serwerze aplikacji.

Na przykład: w systemie AS/400 należy wprowadzić następującą komendę, aby nadać użytkownikowi USER1 uprawnienie *USE do programu CRTSQLPKG:

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

Wpływa ona na wykonanie komendy crtsqlpkg na requesterze aplikacji. Na serwerze aplikacji komenda ta zezwala na tworzenie pakietów.

Komenda odwołania tego uprawnienia:

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

Stosowanie autoryzacji domyślnej: Podczas tworzenia obiektów są jednocześnie tworzone autoryzacje domyślne. Użytkownik, który utworzy tabele, widoki i programy, ma wszystkie uprawnienia.

Więcej informacji o ochronie systemu można znaleźć w podręczniku *AS/400 Security - Reference*.

Reprezentacja danych

Produkty obsługujące DRDA automatycznie wykonują wszystkie niezbędne konwersje po stronie systemu odbiorczego. Aby to działało, wartość CCSID requestera aplikacji musi być obsługiwana przez system odbiorczy w celu konwersji.

W przypadku requestera aplikacji identyfikator CCSID powinien być analizowany w powiązaniu z:

- Zadaniem, które wysłało żądanie.

  Obsługa zarządzania pracą systemu OS/400 inicjuje zadanie z wartością CCSID podaną w profilu użytkownika. Jeśli wartość CCSID w profilu użytkownika wynosi *SYSVAL, to obsługa zarządzania pracą pobiera identyfikator CCSID z wartości systemowej QCCSID. Początkowa wartość systemowa QCCSID wynosi CCSID 65535. Użycie wartości 65535 jako identyfikatora CCSID zadania podczas prób połączenia z produktem DB2 Universal Database spowoduje niepowodzenie próby. Zmiana wartości systemowej QCCSID wpływa na cały system, dlatego też zalecane jest zmienienie identyfikatora CCSID w profilu użytkownika, który uruchomił zadanie serwera. Identyfikatorowi CCSID profilu użytkownika dla danego zadania należy nadać odpowiednią wartość, na przykład CCSID 37 dla języka angielskiego w wersji amerykańskiej. Zazwyczaj odpowiednim wyborem byłoby użycie domyślnego identyfikatora kodowanego zestawu znaków dla AS/400, z którym realizowane jest połączenie.

  Identyfikator CCSID zadania można zmienić za pomocą komendy Zmień zadania (Change Job - CHGJOB). Do zmiany wartości identyfikatora CCSID profilu użytkownika dla kolejnych zadań należy użyć komendy Zmień profil użytkownika (Change User Profile - CHGUSRPRF). Do sprawdzenia, jaki identyfikator CCSID został w rzeczywistości przypisany do zadania w programie języka CL, należy użyć komendy Odtwórz atrybuty zadania (Retrieve Job Attributes - RTVJOBA), aby uzyskać aktualny identyfikator CCSID. W trybie interaktywnym należy użyć komendy Pracuj z zadaniem (Work with Job - WRKJOB) i wybrać na ekranie Praca z zadaniem opcję 2, Wyświetlanie atrybutów definicji zadania (Display Job Definition Attributes).
- Plikami fizycznymi bazy danych.

Jeśli identyfikator CCSID nie jest bezpośrednio podany w komendzie Utwórz plik fizyczny (Create Physical File - CRTPF) lub w komendzie Utwórz fizyczny plik źródłowy (Create Source Physical File - CRTSRCPF) dla fizycznego pliku bazy danych przyjmowany jest domyślny identyfikator CCSID zadania, które utworzyło plik (inny niż identyfikator CCSID tego zadania). Przed produktem DB2 for AS/400 V3R1 domyślny był identyfikator CCSID zadania, który często wynosi 65535 i był niepoprawny dla DRDA. Domyślny identyfikator CCSID zadania nigdy nie wynosi 65535 i dlatego stanowi lepszy wybór na identyfikator CCSID plików fizycznych dostępnych za pośrednictwem sieci DRDA.

Do wyświetlenia identyfikatora CCSID pliku służy komenda Wyświetl opis pliku (Display File Description - DSPFD), a do wyświetlenia identyfikatora CCSID pól pliku służy komenda Wyświetlenie opisu pól pliku (Display File Field Description - DSPFFD).

Do zmiany identyfikatora CCSID pliku fizycznego służy komenda Zmień plik fizyczny (Change Physical File - CHGPF). Plik fizyczny nie może być zmieniony, jeśli zachodzi choćby jeden z następujących warunków:

- Pliki logiczne zostały zdefiniowane na podstawie pliku fizycznego. W takim przypadku można:
  1. Zachować pliki logiczne i fizyczne razem z ich ścieżkami dostępu.
  2. Wydrukować listę uprawnień dla plików logicznych (DSPOBJAUT).
  3. Usunąć pliki logiczne.
  4. Zmienić pliki fizyczne.
  5. Odtworzyć na podstawie zmienionych plików fizycznych, pliki fizyczne i logiczne oraz ich ścieżki dostępu.
  6. Nadać uprawnienia prywatne do plików logicznych (patrz wydrukowana lista).
- Pliki lub pola mają jawnie przypisaną wartość CCSID. Aby zmienić plik fizyczny z przypisanym na poziomie pól identyfikatorem CCSID, należy utworzyć ponownie plik fizyczny i skopiować dane do nowego pliku za pomocą parametru FMTOPT(*MAP) komendy Kopiowanie pliku (Copy File - CPYF).
- Formaty rekordu były współużytkowane w systemie OS/400 w wersji wcześniejszej niż wersja 3 wydanie 1.

Konfigurowanie serwera aplikacji

Obsługa serwera aplikacji w systemie AS/400 umożliwia systemowi działanie jako requestery aplikacji DRDA. Requesterem aplikacji połączonym z serwerem aplikacji DB2 Universal Database for AS/400 może być dowolny klient obsługujący protokoły DRDA.

Requester aplikacji ma dostęp do tabel zapisanych lokalnie na serwerze aplikacji DB2 Universal Database for AS/400. Przed uruchomieniem jakichkolwiek instrukcji SQL, requester aplikacji musi utworzyć pakiet na serwerze aplikacji DB2 Universal Database

for AS/400. W czasie przetwarzania programu serwer aplikacji DB2 Universal Database for AS/400 korzysta z pakietów zawierających instrukcje SQL aplikacji.

Dostarczanie informacji sieciowych

Aby przetwarzać żądania rozproszonej bazy danych na serwerze aplikacji AS/400, należy nadać nazwy bazie danych serwera aplikacji w katalogu RDB. W przypadku komunikacji SNA należy zdefiniować system serwera aplikacji oraz ustawić wielkości jednostek żądania i odpowiedzi oraz pacing. W przypadku komunikacji TCP/IP obsługiwanej począwszy od produktu DB2 Universal Database for AS/400 wersja 4.2 zobacz "Rozdział 4. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu TCP/IP" na stronie 101.

Nadawanie nazwy bazie danych serwera aplikacji

Bazę danych serwera aplikacji (na serwerze aplikacji) nazywa się tak samo, jak bazę danych requestera aplikacji (na requesterze aplikacji). Należy użyć komendy Dodaj pozycję katalogu relacyjnych baz danych (Add Relational Database Directory Entry - ADDRDBDIRE) i podać *LOCAL jako miejsce zdalne.

Definiowanie serwera aplikacji dla sieci

W przypadku dostępu przy użyciu SNA definiowanie serwera aplikacji dla sieci przebiega tak samo, jak definiowanie requestera aplikacji dla sieci. W przypadku obu stron wysyłających żądania, serwera aplikacji i requestera aplikacji, należy utworzyć opis linii, kontrolera, urządzenia i trybu. Informacje o tym, jak definiować serwer aplikacji dla sieci można znaleźć w sekcjach "Definiowanie systemu lokalnego w DB2 Universal Database for AS/400" na stronie 86 i "Definiowanie systemu zdalnego w DB2 Universal Database for AS/400" na stronie 87 oraz w podręczniku *AS/400 Distributed Database Programming*.

Nazwą programu transakcyjnego użytego do uruchomienia bazy danych serwera aplikacji AS/400 jest domyślna nazwa DRDA X'07F6C4C2'. Ta nazwa programu transakcyjnego jest zdefiniowana w systemie AS/400 do uruchomienia serwera aplikacji. W przypadku połączeń TCP/IP, gdy protokół ten jest obsługiwany przez DB2/400, parametrem jest port. DB2/400 jako serwer zawsze korzysta z dobrze znanego portu DRDA 446.

Ustawianie wielkości RU i pacingu

Aby sprawdzić wpływ sieci rozproszonej bazy danych na istniejącą sieć, należy przejrzeć definicje sieci. Odnosi się to zarówno do serwera aplikacji, jak i do requestera aplikacji.

Zapewnianie ochrony

Gdy requester aplikacji przekierowuje żądanie rozproszonej bazy danych do serwera aplikacji AS/400, należy uwzględnić następujące zagadnienia ochrony:

- wybór nazw użytkowników,
- parametry ochrony sieci,
- ochrona menedżera baz danych,

- ochrona systemu AS/400.

Wybieranie nazw użytkowników

Requester aplikacji wysyła identyfikator użytkownika do serwera aplikacji w celach związanych z ochroną. Zadanie uruchomione na serwerze aplikacji AS/400 korzysta z tego ID użytkownika lub, w niektórych przypadkach, z domyślnego ID użytkownika.

Serwer aplikacji AS/400 nie wykonuje translacji przychodzących ID użytkowników w celu rozwiązania konfliktów między nieunikalnymi identyfikatorami lub zgrupowaniami wielu użytkowników w jednym ID użytkownika. Każdy identyfikator użytkownika wysyłany z requestera aplikacji musi istnieć na serwerze aplikacji. Metodą zgrupowania przychodzących żądań w jednym ID użytkownika, powiązaną z pewną utratą ochrony, jest określenie domyślnego ID użytkownika w pozycji dotyczącej komunikacji w podsystemie obsługującym żądania uruchomienia zadania zdalnego. Opisy komend ADDCMNE i CHGCMNE można znaleźć w podręczniku *AS/400 CL Reference*.

Ochrona sieci SNA

Jednostka logiczna 6.2 udostępnia trzy główne opcje ochrony sieci:

- ochrona na poziomie sesji,
- ochrona na poziomie konwersacji,
- szyfrowanie (nieobsługiwane przez system AS/400).

Serwer aplikacji DB2 Universal Database for AS/400 korzysta z ochrony na poziomie sieci w taki sam sposób, jak requester aplikacji DB2 Universal Database for AS/400.

Serwer aplikacji steruje poziomami konwersacji SNA używanymi do konwersacji. Parametr SECURELOC w opisie urządzenia APPC lub wartość miejsca ochrony w spisie miejsc zdalnych APPN określa, co jest akceptowane od requestera aplikacji w celu konwersacji.

Możliwe opcje ochrony konwersacji SNA:

SECURITY=SAME

Zwana również ochroną sprawdzoną uprzednio. Do zdalnego systemu jest wysyłany tylko identyfikator użytkownika aplikacji, nie jest zaś wysyłane hasło. Aby skorzystać z tego poziomu ochrony konwersacji na serwerze aplikacji, należy ustawić parametr SECURELOC w opisie urządzenia APPC na wartość *YES lub wartość miejsca ochrony w spisie miejsc zdalnych APPN na wartość *YES.

SECURITY=PGM

Powoduje, że serwer aplikacji wymaga zarówno identyfikatora użytkownika, jak i jego hasła w celu sprawdzenia poprawności. Aby skorzystać z tego poziomu ochrony konwersacji na serwerze aplikacji, należy ustawić domyślny identyfikator użytkownika w pozycji definiowania komunikacji podsystemu AS/400 na *NONE (brak domyślnego identyfikatora użytkownika) oraz parametr SECURELOC lub wartość określającą chronione miejsce na *NO.

SECURITY=NONE

Serwer aplikacji nie oczekuje ani ID użytkownika, ani hasła. Konwersacja jest dozwolona, używany jest domyślny profil użytkownika na serwerze aplikacji. Aby skorzystać z tej opcji, należy podać domyślny profil użytkownika w katalogu komunikacji podsystemu i podać wartość *NO dla parametru SECURELOC lub wartość określającą chronione miejsce.

Usługi dystrybucyjne SNA (SNA/DS - SNA Distribution Services) wymagają domyślnego ID użytkownika, tak więc powinny mieć własny podsystem w przypadku zwykłych sytuacji, gdy aplikacjom DRDA nie jest potrzebny domyślny ID użytkownika.

Metodę grupowania przychodzących żądań uruchomienia zadania w jednym ID użytkownika opisano w rozdziale “Wybieranie nazw użytkowników” na stronie 97. Ta metoda nie sprawdza ID użytkownika wysłanego z requestera aplikacji. Zadanie serwera aplikacji jest uruchomione z domyślnym ID użytkownika i użytkownik, który zainicjował połączenie na serwerze aplikacji, ma prawa dostępu serwera aplikacji, nawet jeśli wysłany ID użytkownika ma ograniczoną autoryzację. Jest to zrealizowane przez zdefiniowanie serwera aplikacji jako miejsca niechronionego, podanie domyślnego ID użytkownika w pozycji dotyczącej komunikacji AS/400 i skonfigurowanie requestera aplikacji do wysyłania ID użytkownika tylko podczas nawiązywania połączenia. Jeśli wysyłane jest hasło, zamiast domyślnego ID użytkownika używany jest towarzyszący hasłu identyfikator użytkownika.

Pozycje dotyczące komunikacji AS/400 różnią się nazwą urządzenia i trybu użytego do rozpoczęcia konwersacji. Przez przypisanie różnych domyślnych ID użytkownika do różnych par urządzenie/tryb, użytkownicy mogą być grupowani ze względu na ich sposób komunikowania się z serwerem aplikacji.

System AS/400 oferuje także opcję ochrony sieci używaną tylko dla rozproszonej bazy danych i zarządzania plikami rozproszonymi. Atrybut sieciowy dla tych typów dostępu do systemu powoduje, że wszystkie próby dostępu są odrzucane albo umożliwiona jest ochrona kontrolowana przez system na podstawie obiektów.

Ochrona sieci TCP/IP

W DB2 Universal Database for AS/400 wersja 4.2 istnieje nowa komenda o nazwie CRTDDMTCPA. Umożliwia ona określenie, czy serwer będzie akceptował żądania połączenia TCP/IP bez hasła.

Ochrona menedżera baz danych

Cała ochrona jest realizowana przez funkcję ochrony systemu OS/400.

Ochrona systemu

System AS/400 nie ma zewnętrznego podsystemu ochrony. Cała ochrona jest realizowana przez funkcję ochrony systemu OS/400, która jest integralną częścią

systemu operacyjnego. System operacyjny steruje uprawieniami do wszystkich obiektów w systemie, włącznie z programami, pakietami, tabelami, widokami i kolekcjami.

Serwer aplikacji steruje autoryzacją do obiektów, które się w nim znajdują. Obiekty te są chronione w zależności od ID użytkownika, który rozpoczął zadanie serwera aplikacji. Określanie tego identyfikatora opisano w rozdziale “Wybieranie nazw użytkowników” na stronie 97.

Ochroną obiektów można zarządzać za pomocą komend CL uprawnień do obiektu lub instrukcji SQL GRANT i REVOKE. Komendy CL uprawnień do obiektu to: Nadaj uprawnienia do obiektów (Grant Object Authority - GRTOBJAUT) i Odwołaj uprawnienia do obiektów (Revoke Object Authority - RVKOBJAUT). Komendy te działają na dowolny obiekt w systemie. Instrukcje GRANT i REVOKE działają tylko na obiekty SQL: tabele, widoki i pakiety. Aby zmienić autoryzację dla innych obiektów, takich jak programy czy kolekcje, należy użyć komend GRTOBJAUT i RVKOBJAUT.

Podczas tworzenia obiektów dostają one autoryzację domyślną. Identyfikator użytkownika, który tworzy tabele, widoki i pakiety, ma wszystkie uprawnienia. Pozostałe ID użytkownika (publiczne) mają takie same uprawnienia, jak do kolekcji lub bibliotek, w których obiekt został utworzony.

Uprawnienia do obiektów, do których odnoszą się statyczne lub dynamiczne instrukcje w pakiecie, są sprawdzane w czasie przetwarzania pakietu. Jeśli autor pakietu nie ma uprawnień do obiektów, do których się odwołuje, podczas tworzenia pakietu zwracane są komunikaty ostrzegawcze. Podczas wykonywania, użytkownik wykonujący pakiet adoptuje uprawnienia autora pakietu. Jeśli autor pakietu ma autoryzację do tabeli, a użytkownik uruchamiający pakiet nie ma uprawnień, adoptuje on uprawnienia autora i ma możliwość korzystania z tabeli.

Więcej informacji o ochronie systemu można znaleźć w podręczniku *AS/400 Security - Reference*.

Reprezentacja danych

Produkty obsługujące DRDA automatycznie wykonują wszystkie niezbędne konwersje po stronie serwera aplikacji. Aby to działało, wartość CCSID serwera aplikacji musi być obsługiwana przez requester aplikacji w celu konwersji.

W przypadku serwera aplikacji ważny jest identyfikator CCSID w powiązaniu z:

- Obsługiwanym zadaniem w podsystemie komunikacyjnym.

  Identyfikator CCSID obsługiwanego zadania musi być kompatybilny z requesterem aplikacji. Identyfikator ten jest ustalany przez profil użytkownika żądającego połączenia. Obsługa zarządzania pracą systemu OS/400 inicjuje zadanie CCSID z wartości w profilu użytkownika. Jeśli identyfikator CCSID nie istnieje w profilu użytkownika, to obsługa zarządzania pracą pobiera CCSID (QCCSID) z wartości systemowej. Początkowo wartość systemowa QCCSID wynosi CCSID 65535.

Przed zainicjowaniem żądania do DB2 Universal Database for AS/400 należy się wpisać do systemu i użyć komendy Zmień profil użytkownika (Change User Profile - CHGUSRPRF) w celu przypisania akceptowalnej wartości CCSID do profilu użytkownika zadania, które będzie obsługiwało żądania DRDA.

- Kolekcjami SQL.

  Kolekcja SQL składa się z obiektu bibliotecznego systemu OS/400, kroniki, odbiornika kroniki oraz opcjonalnie ze słownika danych IDDU, jeśli klauzula WITH DATA DICTIONARY jest określona w instrukcji CREATE COLLECTION. Pliki fizyczne i logiczne używane dla niektórych spośród tych obiektów mają w momencie ich tworzenia domyślną wartość CCSID zadania. Jeśli użytkownik wyśle zapytanie do słownika danych lub katalogu z requestera aplikacji, który nie obsługuje wartości CCSID tych plików, mogą się pojawić nie dające się wyświetlić lub zniekształcone dane albo requester aplikacji wyda komunikat informujący, że wartość identyfikatora CCSID nie jest obsługiwana. Aby to naprawić, należy utworzyć nową kolekcję z wartością CCSID zadania akceptowalną dla innego systemu.

  Identyfikator CCSID zadania można zmienić za pomocą komendy Zmień zadanie (Change Job - CHGJOB). Do zmiany wartości identyfikatora CCSID profilu użytkownika dla kolejnych zadań należy użyć komendy Zmień profil użytkownika (Change User Profile - CHGUSRPRF). Aby uzyskać aktualny identyfikator CCSIDW w programie CL należy użyć komendy Odtwórz atrybuty zadania (Retrieve Job Attributes - RTVJOBA). W trybie interaktywnym należy użyć komendy Pracuj z zadaniem (Work with Job - WRKJOB) i wybrać na ekranie Praca z zadaniem opcję 2 Wyświetlanie atrybutów definicji zadania (Display Job Definition Attributes).

- Tabelami SQL i innymi plikami DB2 Universal Database for AS/400 dostępnymi w sieci DRDA.

  Tabela SQL odpowiada plikowi fizycznemu DB2 Universal Database for AS/400 w bibliotece o takiej samej nazwie jak kolekcja. Także kolumny tabeli odpowiadają definicjom pól pliku fizycznego. Wartości identyfikatora CCSID dla tabeli lub kolumn tabeli mogą być niekompatybilne z requesterem aplikacji. Aby zmienić tę wartość, należy zajrzeć do punktu “Reprezentacja danych” na stronie 94, w którym opisano zmienianie fizycznych plików bazy danych. Głównym źródłem niekompatybilności CCSID w wersjach systemu OS/400 wcześniejszych niż wersja 3 wydanie 1 było to, że wiele plików lub tabel SQL było domyślnie oznaczonych identyfikatorem CCSID 65535. W wersji 3 wydanie 1 i kolejnych, identyfikatory CCSID tych plików są automatycznie zmieniane na bardziej odpowiednie wartości.

Rozdział 4. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu TCP/IP

Rozdział ten stanowi krótkie podsumowanie informacji zawartych w podręczniku *AS/400e Distributed Database Programming* na temat konfigurowania systemu AS/400 do pracy jako:

- requester aplikacji DRDA korzystający z komunikacji wychodzącej TCP/IP,
- serwer aplikacji DRDA korzystający z komunikacji przychodzącej TCP/IP.

Zasady są identyczne z tymi, które przedstawia “Rozdział 3. Połączenia z DB2 Universal Database for AS/400 w sieci DRDA przy użyciu SNA” na stronie 85, ale kolejne kroki konfiguracji komunikacji są znacznie prostsze.

Uwagi:

1. W przypadku komunikacji DRDA korzystającej z protokołu TCP/IP domyślnym numerem portu dla połączeń bazy danych jest 446.
2. Produkt DB2 Universal Database for AS/400 wersja 4 wydanie 2 nie obsługuje zatwierdzania dwufazowego (rozproszonej jednostki pracy) w komunikacji z użyciem protokołu TCP/IP.

Podsumowanie informacji o DB2 Universal Database for AS/400

Podręcznik *AS/400 Distributed Database Programming* zawiera następujące rozdziały, które warto przeczytać:

- Chapter 1. Distributed Relational Database and the AS/400 System:
  - Distributed Relational Database Processing
  - DRDA and CDRA Support.
- Chapter 3. Communications for an AS/400 Distributed Relational Database:
  - Configuring a Communications Network using TCP/IP
- Chapter 4. Security for an AS/400 Distributed Relational Database:
  - DRDA Security using TCP/IP
- Chapter 5. Setting Up an AS/400 Distributed Relational Database:
  - Work Management for DRDA Use with TCP/IP
  - Setting up the TCP/IP Server
- Chapter 6. Distributed Relational Database Administration and Operation Tasks:
  - Managing a TCP/IP Server
- Chapter 8. Distributed Relational Database Performance:
  - Factors that Affect Blocking for DRDA
- Chapter 9. Handling Distributed Relational Database Problems:

- Handling Connection Request Failures for TCP/IP
- Starting a Service Job for a TCP/IP Server

- Appendix B. Cross-Platform Access Using DRDA.

Dodatkowo warto znać:

- Numer portu TCP/IP i nazwę hosta serwera i requestera.
- Identyfikator CCSID i stronę kodową serwera i requestera.
- ID użytkownika i hasło wymagane podczas łączenia się z bazą danych.

Konfigurowanie i korzystanie z serwera TCP/IP DRDA DB2 Universal Database for AS/400

Najważniejszą sprawą podczas konfiguracji serwera TCP/IP DRDA DB2 Universal Database for AS/400 jest upewnienie się, że serwer został uruchomiony. Serwer DRDA (zwany także serwerem DDM) uruchamia się za pomocą komendy:

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

Serwer DRDA można także uruchomić za pomocą komendy Uruchom Serwer TCP/IP (Start TCP/IP Server - STRTCPSVR) wprowadzonej bez parametrów lub z parametrem SERVER równym *ALL. Serwer DRDA zostanie uruchomiony automatycznie przy uruchamianiu protokołu TCP/IP, jeśli została wprowadzona komenda:

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

Sprawdzenie, czy serwer jest uruchomiony, umożliwia następująca komenda:

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

Wyświetli ona przewijalną listę zadań. Przy przewijaniu strony powinny być widoczne dwa wiersze zawierające następujące informacje:

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

(Liczba wystąpień wiersza QRWTSRVR zależy od tego, ile zadań jest aktywnych we wstępnej fazie uruchamiania serwera).

Obecność wiersza QRWTLSTN wskazuje, że zadanie, które nasłuchuje żądań połączeń DRDA i DDM jest aktywne. Zadanie to przydziela pracę zadaniu QRWTSRVR, w miarę otrzymywania żądań połączenia.

Inną metodą sprawdzenia, czy serwer DRDA jest uruchomiony, jest wydanie komendy STRTCPSVR SERVER(*DDM). Powinien pojawić się komunikat 'DDM TCP/IP server already active' (Serwer DDM jest już aktywny).

Nazwę zadania wstępnej fazy uruchamiania serwera dla poszczególnych połączeń można sprawdzić, wykonując komendę DSPLOG, na przykład:

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

gdzie określona godzina jest wcześniejsza niż godzina nawiązania połączenia. Zostanie wyświetlona przewijalna lista pozycji protokołu historii. Należy szukać pozycji podobnej do poniższej, która będzie zawierać nazwę zadania serwera:

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

Nazwa zadania jest użyteczna przy przeglądaniu protokołu zadań aktywnych. Przydaje się także do uruchomienia zadania obsługi zadań aktywnych w celu określenia problemów lub przejrzenia komunikatów optymalizatora zapytań. Przykładowa komenda języka CL uruchamiająca zadanie obsługi z wykorzystaniem powyższych informacji:

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

Aby wprowadzić obsługiwane zadanie w tryb debuggingu, należy wykonać komendę STRDBG:

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

W pewnych sytuacjach serwer DRDA zapisuje protokół zadania we wstępnej fazie uruchamiania serwera przed usunięciem zadania i wyczyszczeniem protokołu zadania. Ma to miejsce, gdy zostaje wykryta poważna awaria lub gdy zadanie zostanie zakończone w trakcie obsługi (przy użyciu komendy STRSRVJOB).

Aby odnaleźć zachowany protokół zadania po zakończeniu zadania, należy wykonać następującą komendę:

```
WRKJOB userid/QPRTJOB
```

gdzie userid jest nazwą ID użytkownika, pod którą zostało nawiązane połączenie (w przykładzie powyżej jest to SRR).

Zostanie wyświetlona lista zadań, z której można wybrać jedno zadanie lub opcję menu dla pojedynczego zadania. Należy wybrać opcję 4, Praca z wydrukami w kolejce (Work with spooled files), aby odnaleźć zachowany protokół zadania. Jeśli w kolejce jest więcej plików, należy odszukać plik o nazwie QPJOBLOG. Opcja 5 umożliwia przeglądanie pliku protokołu zadania.

Przykład komunikatu optymalizatora zapytań w protokole zadań serwera, który można zobaczyć, gdy zadanie zostanie uruchomione w trybie debuggingu:

```
CPI4329    Information   00    03/30/98   16:14:57   QQQIMPLE
           QSYS        3911     QSQOPEN      QSYS         09C4
Message . . . . :   Arrival sequence access was used for file TBL2.
Cause . . . . . :   Arrival sequence access was used to select
  records from member TBL2 of file TBL2 in library SR. If file TBL2
  in library SR is a logical file then member TBL2 of physical file
  TBL2 in library SR is the actual file from which records are
  being selected. A file name of *N for the file indicates it is a
  temporary file. Recovery  . . . :   The use of an access path may
```

```
improve the performance of the query if record selection is
specified. If an access path does not exist, you may want to
create one whose left-most key fields match fields in the record
selection.  Matching more key fields in the access path with
fields in the record selection will result in improved
performance. Generally, to force the use of an existing access
path, specify order by fields that match the left-most key fields
of that access path. For more information refer to the DB2 for
AS/400 SQL Programming book.
```

Konfigurowanie i korzystanie z klienta TCP/IP DRDA DB2 Universal Database for AS/400

Najważniejszą sprawą przy używaniu DB2 Universal Database for AS/400 jako requestera aplikacji DRDA, oprócz zagadnień ochrony omówionych w następnej sekcji, jest dodanie pozycji dla zdalnego serwera aplikacji do katalogu relacyjnych baz danych. Dokonuje się tego podobnie jak opisano w poprzednim rozdziale dotyczącym komunikacji SNA. Jednakże zamiast parametrów APPC, takich jak nazwa zdalnej jednostki logicznej i nazwa programu transakcyjnego, istnieją dwa parametry protokołu TCP/IP: nazwa zdalnego hosta lub jego adres IP i numer portu lub nazwa usługi. Drugi element parametru zdalnego miejsca może być określony jako *SNA (domyślnie) lub *IP (aby wskazać, że połączenie będzie korzystało z protokołu TCP/IP).

Uwagi dotyczące ochrony DRDA przy użyciu protokołu TCP/IP

Serwer DRDA z rodzimym TCP/IP nie używa usług ochrony komunikacji OS/400 i pojęć, takich jak urządzenia komunikacyjne, tryby, atrybuty miejsc chronionych i poziomy ochrony konwersacji, które są powiązane z komunikacją APPC. W przypadku tego ustawienia ochrony dla protokołu TCP/IP są zupełnie inne.

W aktualnej wersji implementacji DRDA dla DB2/400 wykorzystującej protokół TCP/IP obsługiwane są dwa rodzaje mechanizmów ochrony:

1. Tylko ID użytkownika.
2. ID użytkownika z hasłem.

W przypadku serwera aplikacji DB2 Universal Database for AS/400 domyślną ochroną jest ID użytkownika z hasłem. Oznacza to, że po zainstalowaniu systemu przychodzące żądania połączenia TCP/IP muszą mieć hasło powiązane z ID użytkownika, który uruchomił zadanie serwera. Aby określić, że hasło nie jest wymagane, można użyć komendy CHGDDMTCPA PWDRQD(*NO). Aby użyć tej komendy, należy mieć uprawnienia specjalne *IOSYSCFG.

W przypadku requestera aplikacji DB2 Universal Database for AS/400 (AR, klient) istnieją dwie metody, których można użyć do przesłania hasła z ID użytkownika wraz z żądaniem nawiązania połączenia TCP/IP. Jeśli nie można użyć żadnej z nich, zostanie wysłany tylko ID użytkownika.

Pierwszą metodą wysłania hasła jest użycie formatu USER/USING instrukcji CONNECT języka SQL. Składnia:

```
CONNECT TO nazwa_bazy_danych USER id_użytkownika USING 'hasło'
```

gdzie wyrazy napisane małymi literami oznaczają odpowiednie parametry połączenia. W programie korzystającym z wbudowanego SQL, wartości ID użytkownika i hasła mogą być zawarte w zmiennych języka bazowego.

Inną metodą dostarczenia hasła do żądania połączenia TCP/IP jest skorzystanie z pozycji listy autoryzowanych użytkowników serwera. Lista autoryzowanych użytkowników serwera jest powiązana z każdym profilem użytkownika w systemie. Domyślnie lista jest pusta, ale za pomocą komendy ADDSVRAUTE można dodawać pozycje. Podczas nawiązywania połączenia DRDA TCP/IP DB2 Universal Database for AS/400 sprawdza, czy profil użytkownika, z którym zostało uruchomione zadanie klienta, jest na liście autoryzowanych użytkowników serwera. Jeśli uda się dopasować nazwę relacyjnej bazy danych w instrukcji CONNECT i nazwę SERVER w autoryzacji, jako ID użytkownika dla połączenia jest używany parametr USERID powiązany z tą pozycją. Jeśli zapisany jest również parametr PASSWORD, to także to hasło jest wysyłane z żądaniem połączenia.

Aby zachować hasło za pomocą komendy ADDSVRAUTE, wartość systemowa QRETSVRSEC musi być ustawiona na ’1’. Wartością domyślną jest ’0’. Aby dokonać zmiany, należy wpisać:

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

Składnia komendy ADDSVRAUTE:

```
ADDSVRAUTE USRPRF(profil_użytkownika) SERVER(nazwa_rdb) USRID(id_użytkownika)
        PASSWORD(hasło)
```

Parametr USRPRF określa profil użytkownika, z którym jest uruchomione zadanie requestera aplikacji. Parametr SERVER określa nazwę zdalnej relacyjnej bazy danych, a parametr USRID określa profil użytkownika, z którym jest uruchomione zadanie serwera. Parametr PASSWORD określa hasło dla profilu użytkownika na serwerze.

Uwaga: Bardzo ważne jest określenie nazwy relacyjnej bazy danych (RDB) w parametrze SERVER wielkimi literami.

Jeśli pominięty jest parametr USRPRF, domyślnie przyjęty będzie profil użytkownika, z którym zostanie uruchomiona komenda ADDSVRAUTE. Jeśli pominięty jest parametr USRID, domyślnie przyjęta zostanie wartość parametru ID użytkownika o profilu USRPRF. Jeśli pominięty jest parametr PASSWORD lub wartość QRETSVRSEC wynosi 0, w pozycji nie będzie zachowane żadne hasło i przy próbie połączenia z wykorzystaniem pozycji jako mechanizmem ochrony użyty będzie tylko ID użytkownika.

Pozycja na liście autoryzowanych użytkowników może zostać usunięta za pomocą komendy RMVSVRAUTE, a zmieniona za pomocą komendy CHGSVRAUTE. Dokładny opis tych komend można znaleźć w podręczniku ″AS/400 Command Reference″.

Jeśli dla relacyjnej bazy danych istnieje pozycja na liście autoryzowanych użytkowników i używany jest format USER/USING instrukcji CONNECT, używany jest ten ostatni.

Rozdział 5. Dodatkowe uwagi o DB2 Universal Database for AS/400 i DB2 Universal Database

W tym rozdziale zawarto dodatkowe uwagi, które można zastosować do operacji SQL między DB2 Universal Database for AS/400 i DB2 Common Server wersja 2 lub DB2 Universal Database. Pozostałe uwagi dotyczą DB2 for OS/2, ale w większości przypadków podobne uwagi odnoszą się także do DB2 Common Server wersja 2 i DB2 Universal Database na innych platformach:

1. W systemie AS/400 nazwy tabel są kwalifikowane przez kolekcję (lub nazwę biblioteki) i umieszczane w bazie danych DB2 Universal Database for AS/400 (jedna baza danych na jeden system AS/400). Na komputerach PC tabele są kwalifikowane przez ID użytkownika (który utworzył tabelę) i umieszczane w określonej bazie danych (na komputerze PC z DB2 for OS/2 można utworzyć wiele baz danych).
   a. Oznacza to, że zapytanie DB2 for OS/2 (zadane za pośrednictwem DB2 Connect) do DB2 Universal Database for AS/400 użyje ID użytkownika po stronie docelowej (w systemie AS/400) dla (domyślnej) nazwy kolekcji, jeśli nazwa tabeli będącej obiektem zapytania została określona bez nazwy kolekcji. Przy nieostrożnym postępowaniu tabela może nie zostać odnaleziona.
   b. Oznacza to również, że zapytanie DB2 Universal Database for AS/400 do DB2 for OS/2 będzie miało niejawny kwalifikator tabeli, jeśli nie został on określony w zapytaniu (w postaci 'kwalifikator.nazwa-tabeli'). Domyślnie kwalifikator tabeli DB2 for OS/2 (określony przez requester aplikacji AS/400 jako kolekcja lub biblioteka) jest równy ID użytkownika, który wykonał to zapytanie. Przy nieostrożnym postępowaniu zapytanie może nie odnaleźć tabeli.
   c. Może się zdarzyć, że użytkownik zechce utworzyć bazy danych i tabele DB2 for OS/2 ze wspólnym ID użytkownika. W DB2 for OS/2 nie ma fizycznych kolekcji w takiej postaci jak w DB2 Universal Database for AS/400, ale po prostu kwalifikator tabeli, którym jest ID użytkownika, który ją utworzył.
2. DB2 Connect (lub DDCS) jest potrzebny, jeśli DB2 for OS/2 jest klientem korzystającym z protokołu DRDA. Nie jest natomiast potrzebny, jeśli DB2 for OS/2 jest używany jedynie jako serwer.
3. Bardzo ważne jest prawidłowe skonfigurowanie DB2 Connect:
   a. Należy upewnić się, że wersje DB2 for OS/2 i DB2 Connect są aktualne. Jeśli nie, należy zastosować dostępne poprawki FixPak.
   b. Należy postępować zgodnie z instrukcjami instalacji i konfiguracji zawartymi w podręczniku.
4. Jeśli użytkownik korzysta z APPC, ze szczególną uwagą musi podejść do prawidłowego skonfigurowania komunikacji z kontrolerem i urządzeniem

utworzonym dla komputera PC, gdy DB2 for OS/2 jest używany jako requester aplikacji lub serwer aplikacji. Ponadto, niezależnie od używanych protokołów komunikacyjnych potrzebna jest pozycja w katalogu relacyjnych baz danych dla każdej bazy danych DB2 for OS/2, z którą system AS/400 będzie się łączył.

Aby skonfigurować komunikację APPC:

a. Można ręcznie utworzyć opis urządzenia i kontrolera. Można również pozwolić, aby utworzył je system, jeśli sieć jest typu Token Ring i parametr AUTOCRTCLT opisu linii ma wartość *YES. Aby zobaczyć opis linii, należy skorzystać z komendy WRKLIND, używając opcji 2 Zmiana. Należy przejść do parametru 'Autocreate controller'(automatyczne tworzenie kontrolera) i sprawdzić wartość AUTOCRTCLT.

   Jeśli system automatycznie utworzy kontroler, można zainicjować utworzenie niezbędnych opisów kontrolera. W folderze CM/2 w systemie OS/2 należy wykonać komendę Uruchom komunikację (Start Communications) i uruchomić opcję Zarządzanie podsystemem (Subsystem Management). Z poziomu Subsystem Management przejrzeć szczegóły dotyczące podsystemu SNA. Znajduje się tu opcja Logical Links. Należy otworzyć i uaktywnić połączenie z żądanym systemem, aby automatycznie utworzyć kontroler. Opis urządzenia zostanie utworzony automatycznie.

b. Urządzenie i kontroler dla komputera PC w systemie AS/400 muszą mieć status ACTIVE, aby mogły działać sieciowe połączenia między systemami. Należy ustawić parametr SWTDSC w opisie kontrolera na wartość *NO, aby kontrolery mające status ACTIVE pozostały z takim statusem. Można także ustawić parametr ONLINE na wartość *YES, co spowoduje uaktywnienie kontrolera po każdym wykonaniu IPL. Również w opisie urządzenia może być potrzebne ustawienie parametru ONLINE na wartość *YES. Aby zmienić parametry w opisie kontrolera, musi on mieć status VARIED OFF i właściciel kontrolera (parametr CTLOWN) musi być ustawiony na wartość *USER.

c. Aby dodać pozycję w katalogu RDB dla każdej bazy danych DB2 for OS/2, z którą będzie się łączył system AS/400, należy skorzystać z komendy ADDRDBDIRE: nazwa RDB jest nazwą bazy danych DB2 for OS/2, a zdalna nazwa miejsca jest nazwą stacji roboczej.

5. Odpowiednia wartość CCSID (zwykle 37 dla użytkowników w USA) jest potrzebna dla każdej tabeli (plików fizycznych) w systemie AS/400 używanej przez DB2 for OS/2. Wartość CCSID można zobaczyć za pomocą komendy DSPFD oraz zmienić ją dla plików fizycznych komendą CHGPF. Ponadto, aby połączenie powiodło się, może zaistnieć potrzeba zmiany jednej z następujących wartości: identyfikatora CCSID zadania, identyfikatora CCSID użytego profilu użytkownika lub wartości systemowego identyfikatora CCSID, jeśli domyślnie wynosi ona 65535. Zazwyczaj najlepszym miejscem do dokonania tej zmiany jest profil użytkownika, z którym zostanie uruchomione zadanie serwera.
6. Przed użyciem DB2 Connect należy w systemie AS/400 utworzyć pakiety SQL dla aplikacji i dla programów narzędziowych DB2 Connect.

a. Do przetwarzania plików źródłowych aplikacji z wbudowanym SQL można użyć komendy DB2 PREP. Utworzy ona zmodyfikowany plik źródłowy zawierający wywołania języka bazowego dla instrukcji SQL i domyślnie pakiet w bazie, z którą aktualnie istnieje połączenie.

b. Aby powiązać programy narzędziowe DB2 Connect z dowolnym serwerem DB2 systemu AS/400:

   1)
   ```
   CONNECT TO nazwa_zdalnej_bazy_danych
   ```

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

   Należy zastąpić path w powyższej komendzie (path@DDCS400.LST) domyślną ścieżką C:\SQLLIB\BND\ lub wartością podaną podczas instalacji.

   Uwaga: Aby uniknąć kodu SQL -901 z bazy danych DB2 Universal Database for AS/400 przy trzecim systemie na liście w pliku powiązań, dla systemu OS/400 V3R1 potrzebna jest poprawka PTF SF23624.

   3)
   ```
   CONNECT RESET
   ```

7. W przypadku interaktywnego języka SQL z DB2 Universal Database for AS/400 do DB2 for OS/2:

   a. Należy użyć atrybutów sesji NAMING(*SQL), DATFMT(*ISO) i TIMFMT(*ISO). Zamiast *ISO można podać inny format, ale nie wszystkie formaty są poprawne. Formaty daty (DATFMT) i godziny (TIMFMT) powinny być takie same.

   b. Należy zwrócić uwagę na powiązania między COLLECTION w systemie AS/400 i kwalifikatorem tabeli (ID użytkownika, który utworzył tabelę) dla DB2 for OS/2. Punkt 1 na tej liście zawiera uwagi na temat operacji SQL.

   c. W przypadku pierwszej sesji interaktywnej NALEŻY także podać COMMIT(*CS) dla kontroli transakcji, a następnie (1) RELEASE ALL, (2) COMMIT i (3) CONNECT TO nazwa_zdalnej_bazy_danych (gdzie 'nazwa_zdalnej_bazy_danych' oznacza odpowiednią bazę danych). W tym momencie można również nadać odpowiednie uprawnienia wszystkim (lub określonym) użytkownikom, aby mogli korzystać z SQL PKG utworzonego na komputerze PC dla interaktywnego SQL (GRANT EXECUTE ON PACKAGE QSQL400.QSQL0200 TO PUBLIC).

8. W przypadku dowolnych programów utworzonych w systemie AS/400 mających dostęp do bazy danych DB2 for OS/2 należy pamiętać o użyciu następujących komend DB2 for OS/2:

   a.

```
GRANT ALL PRIVILEGES ON TABLE nazwa_tabeli TO użytkownik
```

b.

```
GRANT EXECUTE ON PACKAGE nazwa_pakietu (zazwyczaj nazwa programu AS/400) TO uży
```

Ewentualnie zamiast użytkownika można podać 'PUBLIC'.

9. W przypadku aplikacji AS/400 mających dostęp do DB2 for OS/2 (V.2.1.1 lub wcześniejsze) został wprowadzony komunikat (SQL5057) w odpowiedzi na komendę CRTSQLxxx, który mówi, że pakiet SQL został utworzony na komputerze PC, nawet jeśli nie jest to prawdą. Zostało to poprawione w najnowszym wydaniu DB2 for OS/2.

   Ponadto w starszych wersjach DB2 for OS/2 nie mogły być tworzone pakiety SQL zawierające cokolwiek w polu tekstowym swojego opisu elementu źródłowego.

10. Procedura w języku C zapisana w bazie DB2 for OS/2 nie może używać jako parametrów argc i argv (nie może być typu main()). Tym różni się od procedur zapisanych w bazie systemu AS/400, które muszą korzystać z parametrów argc and argv. Przykłady procedur zapisanych w bazie DB2 for OS/2 znajdują się w podkatalogu \SQLLIB\SAMPLES. Należy przejrzeć pliki OUTSRV.SQC i OUTCLI.SQC w podkatalogu C.

11. W przypadku nazw procedur zapisanych w bazie DB2 for OS/2 wywoływanych przez system AS/400 należy używać wielkich liter. Obecnie system AS/400 zamienia litery w nazwie procedury na wielkie. Jednak oznacza to, że procedura na komputerze PC mająca taką samą nazwę (zapisaną małymi literami) nie zostanie odnaleziona. Należy pamiętać, że nazwy procedur zapisanych w bazie w systemie AS/400 będą zapisane wielkimi literami.

12. Bez odpowiedniej poprawki PTF dla wbudowanego SQL instrukcja CALL z systemu AS/400 do DB2 for OS/2 będzie działała tylko, gdy nazwa procedury zostanie umieszczona w zmiennej języka bazowego (CALL :host-nazwa-procedury(...)). Poprawka PTF dla wersji V3R7 ma numer SF35932. Poprawka PTF dla wersji V3R2 ma numer SF36535.

13. Procedury zapisane w bazie w systemie AS/400 nie mogą zawierać instrukcji COMMIT, gdy są tworzone do uruchomienia w tej samej grupie aktywacji, co wywoływany program (odpowiednia metoda ich utworzenia). Jednak dla DB2 for OS/2 procedura zapisana w bazie może zawierać COMMIT, ale projektant aplikacji powinien zwrócić uwagę na to, że nie ma żadnej informacji o części DB2 Universal Database for AS/400, w której następuje zatwierdzenie.

Rozdział 6. Połączenia z DB2 for VSE &VM w sieci DRDA

SQL/DS (DB2 for VM) wersja 3 wydanie 5 umożliwia obsługę systemów VM przez serwer aplikacji i requester aplikacji zdalnej jednostki pracy DRDA. SQL/DS (DB2 for VSE) wersja 3 wydanie 5 umożliwia obsługę systemów VM przez serwer aplikacji zdalnej jednostki pracy DRDA.

Ponadto DB2 for VSE &VM wersja 5 wydanie 1 umożliwia obsługę zarówno systemów VM, jak i VSE przez serwer aplikacji rozproszonej jednostki pracy DRDA. W tym rozdziale skoncentrowano się na łączeniu systemów DB2 for VSE &VM z różnymi systemami zdalnymi DRDA. Więcej informacji na temat łączenia dwóch systemów DB2 for VSE &VM można znaleźć w następujących podręcznikach:

- *VM/ESA Connectivity Planning, Administration and Operation*
- *DB2 for VM System Administration*
- *DB2 for VSE System Administration*

Omówienie DB2 for VM

Każdy menedżer baz danych DB2 for VM może zarządzać jedną lub wieloma bazami danych (po jednej na raz). Do menedżera zwykle odwołuje się za pomocą nazwy bazy danych, którą w danej chwili zarządza menedżer. Nazwa relacyjnej bazy danych jest unikalna w obrębie połączonych sieci SNA.

Poniżej opisano różne komponenty DRDA i VM wykorzystywane w przetwarzaniu rozproszonych baz danych. Wymienione komponenty udostępniają menedżerom baz danych DB2 for VM lokalne relacyjne bazy danych i umożliwiają komunikację z systemami zdalnymi DRDA w sieci SNA.

AVS Obsługa APPC/VTAM (AVS) to komponent systemu VM umożliwiający aplikacjom VM dostęp do sieci SNA. Komponent ten zapewnia funkcje jednostki logicznej (LU) zdefiniowane przez SNA. Jednostka logiczna (LU) w środowisku VM jest określana jako *brama* (gateway). AVS działa w systemie sterującym grupami jako VTAM. Przekształca wywołania makr APPC/VM na wywołania makr APPC/VTAM i odwrotnie. APPC/VM wykorzystuje AVS do wyznaczania trasy i translacji strumieni danych. AVS pozwala na wyznaczanie trasy żądań DB2 for VM między lokalnym systemem VM i miejscami zdalnymi SNA. Komponent AVS musi być używany, gdy aplikacje lub bazy danych DB2 for VM komunikują się z aplikacjami lub bazami danych innego typu niż DB2 for VM.

Po stronie requestera aplikacji: aby żądanie zostało wysłane, użytkownik musi być autoryzowany do łączenia się przez bramę AVS. Po stronie serwera aplikacji: aby AVS mógł dalej przekazać żądanie użytkownika, odbierająca

brama AVS musi mieć autoryzację do łączenia się z serwerem DB2 for VM. Autoryzacja jest sprawdzana przez wprowadzenie odpowiednich instrukcji sterujących katalogami IUCV na komputerze użytkownika, na komputerze bazy danych oraz na wysyłających i odbierających komputerach AVS. Szczegółowe informacje na ten temat można znaleźć w podręczniku *VM/ESA Connectivity Planning, Administration, and Operation*.

APPC/VM
APPC/VM jest interfejsem API na poziomie asemblera VM udostępniającym podzbiór zbioru funkcji LU 6.2 zdefiniowanych przez SNA. W praktyce APPC/VM udostępnia komendy LU 6.2 pozwalające aplikacjom DB2 for VM na połączenie się z lokalnymi i zdalnymi menedżerami baz danych. Komendy LU 6.2 obsługiwane przez APPC/VM opisano w podręczniku *VM/ESA CP Programming Services*.

Communications Directory (Katalog komunikacyjny)
Katalog komunikacyjny to plik CMS NAMES pełniący szczególną rolę w nawiązywaniu konwersacji APPC między lokalnym requesterem aplikacji VM i serwerem aplikacji VM. Katalog ten dostarcza informacji niezbędnych do wyznaczania trasy i nawiązywania konwersacji APPC z serwerem docelowym. W skład informacji wchodzą takie pozycje, jak nazwa jednostki logicznej (LU), TPN, ochrona, nazwa trybu, ID użytkownika, hasło i nazwa bazy danych.

DB2 for VM korzysta ze znacznika COMDIR :dbname, aby wykonać translację nazwy RDB_NAME na odpowiadające jej dane routingu.

Ten plik specjalny i jego funkcje komunikacyjne opisano w podręczniku *VM/ESA Connectivity Planning, Administration, and Operation*.

CRR Coordinated Resource Recovery (CRR) jest narzędziem VM, które koordynuje zatwierdzanie i wycofywanie aktualizacji zasobów zabezpieczonych. Aplikacje rozproszone, we współpracy z CRR, wykorzystują konwersację chronioną co zapewnia integralność zasobów transakcji rozproszonej.

CRR Recovery Server
CRR Recovery Server jest komponentem CRR i działa na własnej maszynie wirtualnej. Jest on odpowiedzialny za funkcje resynchronizacji i protokołowania punktu synchronizacji.

GCS System sterujący grupami (GCS) jest komponentem systemu VM, składającym się z:

- współużytkowanego segmentu działającego w maszynie wirtualnej,
- nadzorcy maszyny wirtualnej, który wiąże wiele wirtualnych maszyn w grupę i nadzoruje ich działanie,
- interfejsu między następującymi programami:
  - Virtual Telecommunications Access Method (VTAM),
  - APPC/VTAM Support (AVS),
  - Remote Spooling Communications Subsystem (RSCS),

– Control Program (CP).

GCS nadzoruje wykonywanie aplikacji VTAM, takich jak AVS w środowisku VM. Maszyny wirtualne działające pod nadzorem GCS nie korzystają z CMS.

Adapter zasobów
Adapter zasobów jest częścią oprogramowania DB2 for VM, która znajduje się w maszynie wirtualnej użytkownika i pozwala aplikacjom użytkownika na żądanie dostępu do serwera DB2 for VM. Funkcja requestera aplikacji DRDA jest zintegrowana z adapterem zasobów.

TSAF Transparent Services Access Facility to komponent systemu VM umożliwiający komunikację między połączonymi systemami VM. W kolekcji TSAF może brać udział osiem systemów VM. Kolekcja może być pojmowana jako analogia sieci lokalnej VM (lub sieci rozległej). Każdy system VM należący do kolekcji musi mieć działającą maszynę wirtualną TSAF. Wewnątrz kolekcji TSAF wszystkie identyfikatory użytkowników i zasobów są unikalne.

DB2 for VM wykorzystuje TSAF do wyznaczania trasy żądań rozproszonych baz danych do innych maszyn DB2 for VM wewnątrz kolekcji TSAF. Jeśli lokalny system VM nie ma maszyny wirtualnej AVS, DB2 for VM wykorzystuje TSAF do wyznaczania trasy żądań DRDA do systemu VM, który ma maszynę wirtualną AVS. AVS pozwala przekazywać żądania do innych kolekcji TSAF i do systemów innych niż DB2 for VM.

Kolekcja TSAF jest widoczna jako jedna lub wiele jednostek logicznych w sieci SNA. Do zasobów zdefiniowanych jako globalne w obrębie kolekcji TSAF można uzyskać dostęp za pomocą aplikacji zdalnych APPC znajdujących się w dowolnym miejscu kolekcji.

Zwykle kolekcja TSAF działa autonomicznie, niezależnie od VTAM i sieci SNA. Może ona jednak współdziałać z AVS i VTAM. Jej zasoby globalne staną się wówczas dostępne z aplikacji zdalnych APPC znajdujących się w dowolnym miejscu sieci SNA. Aby to osiągnąć, maszyna AVS i maszyna VTAM muszą działać u jednego lub wielu członków kolekcji TSAF. Kolekcję TSAF opisano w podręczniku VM/ESA *Connectivity Planning, Administration, and Operation*.

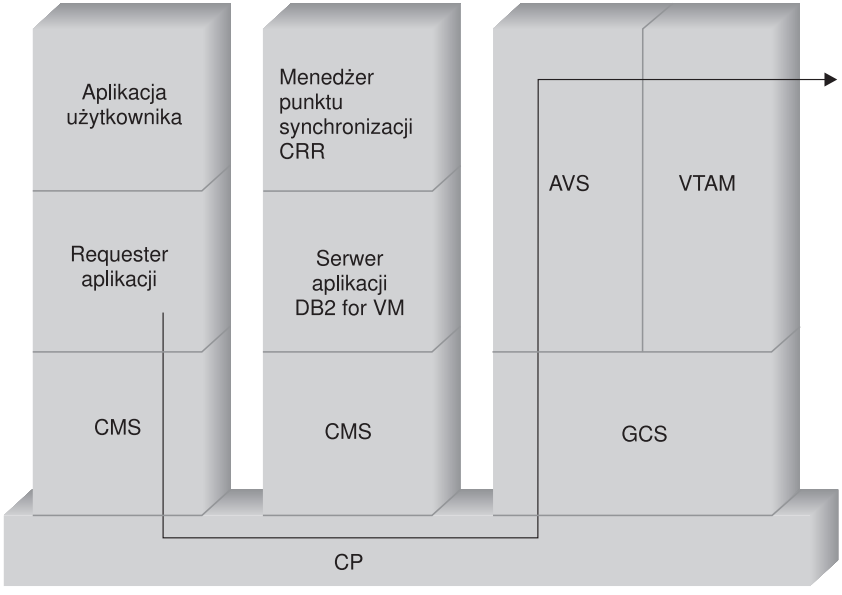
VTAM Virtual Telecommunications Access Method zapewnia obsługę połączeń komunikacji sieciowej. DB2 for VM wykorzystuje usługi VTAM przez AVS, aby wyznaczać trasy połączeń i żądań do systemów zdalnych DRDA. Metoda VTAM jest wykorzystywana *tylko* do żądań zdalnych, które mają dostęp do sieci SNA.

***IDENT**
AVS i TSAF używają nazwy programu transakcyjnego (TPN) do wyznaczania trasy żądań między systemami VM, połączonymi przez TSAF i AVS. TPN może być nazwą programu transakcyjnego zarejestrowanego w SNA lub prawidłową nazwą alfanumeryczną. VM odwołuje się do wartości TPN jako ID

zasobu. Aby serwer DB2 for VM był dostępny dla zdalnych systemów DRDA, korzysta z usługi systemowej VM IDENTIFY (*IDENT) w celu zdefiniowania się jako menedżer ID zasobu globalnego (TPN). Po zdefiniowaniu serwera jako zasobu globalnego, TSAF i AVS mogą wyznaczać trasy żądań DRDA do serwera DB2 for VM, jeśli otrzymana nazwa TPN odpowiada ID zasobu.

Przykład przepływu komunikacji dla requestera aplikacji

Poniższy przykład ukazuje rolę poszczególnych komponentów w nawiązywaniu komunikacji między requesterem aplikacji VM i serwerem zdalnym DRDA. Rys. 27 przedstawia, jak requester aplikacji łączy się z AVS i korzysta z VTAM, aby uzyskać dostęp do sieci SNA. Trasa dostępu do zasobów zdalnych nie prowadzi przez lokalny serwer aplikacji DB2 for VM.



Rysunek 27. Żądanie dostępu do zasobu zdalnego

Załóżmy, że DB2 for VM Application Requester należący do kolekcji TSAF ma uzyskać dostęp do zdalnych danych zarządzanych przez DRDA Application Server. Z definicji oznacza to, że maszyna TSAF działa na lokalnym hoście VM, na którym znajduje się requester aplikacji. Także komponent AVS i maszyna VTAM działają w systemie VM w tej kolekcji TSAF. AVS i VTAM także mogą znajdować się w tym samym systemie co requester aplikacji i serwer aplikacji.

Maszyna VTAM po uruchomieniu definiuje lokalną bramę AVS do sieci SNA i uaktywnia co najmniej jedną sesję do późniejszego użycia podczas nawiązywania konwersacji.

Maszyna AVS po uruchomieniu negocjuje limity liczby sesji między lokalną bramą AVS i potencjalnymi partnerskimi jednostkami logicznymi (LU).

Serwer aplikacji może być aktywny lub nieaktywny. Należy go uruchomić, aby mógł on przetwarzać żądania od podobnego lub niepodobnego requestera aplikacji.

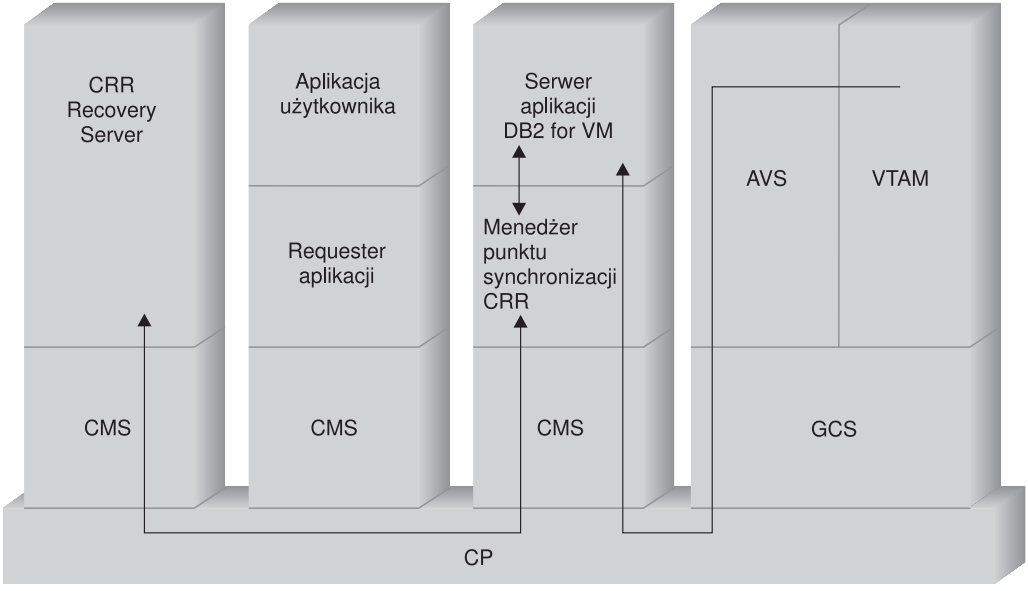
Requester aplikacji wydaje instrukcję APPC/VM CONNECT w celu nawiązania konwersacji LU 6.2 z serwerem aplikacji. Funkcja CONNECT wykorzystuje CMS Communications Directory do odwzorowania nazwy relacyjnej bazy danych na powiązaną nazwę LU i nazwę programu transakcyjnego odpowiadającą adresowi serwera aplikacji w sieci SNA. CMS Communications Directory określa także poziom ochrony konwersacji i tokeny ochrony, takie jak ID użytkownika i hasło, które przekazuje do ośrodka zdalnego w celu autoryzacji. Jeśli parametr SECURITY=PGM, requester aplikacji musi przekazać ID użytkownika i hasło do serwera aplikacji. ID użytkownika i hasło można określić w CMS Communications Directory lub w rekordzie APPCPASS zdefiniowanym przy użyciu katalogu CP użytkownika requestera aplikacji. Jeśli parametr SECURITY=SAME, wówczas tylko ID logowania w VM użytkownika requestera aplikacji jest wysyłany do serwera aplikacji, dodatkowe hasło nie jest wymagane.

Na przykład jeśli SECURITY=SAME, host sprawdza, czy maszyna AVS działa lokalnie. W pozostałych przypadkach host nawiązuje połączenie między requesterem aplikacji i lokalną maszyną TSAF. Lokalna maszyna TSAF odpytuje pozostałe maszyny TSAF w kolekcji TSAF w poszukiwaniu maszyny AVS, a następnie nawiązuje z nią połączenie.

Komponent AVS w kolekcji TSAF przekształca żądanie połączenia APPC/VM na odpowiadające mu wywołanie funkcji APPC/VTAM. Następnie wykorzystuje istniejącą sesję lub przydziela nową sesję między jego bramą (LU) i zdalną jednostką logiczną (LU). Potem AVS nawiązuje konwersację ze zdalną jednostką logiczną i przekazuje jej nazwę jednostki logicznej, poziom ochrony, TPN i ID użytkownika. Jeśli zdalna jednostka logiczna również jest systemem VM, to sesja i konwersacja jest obsługiwana przez działający w nim komponent AVS.

Przykład przepływu komunikacji dla serwera aplikacji

Poniższy przykład ukazuje rolę poszczególnych komponentów w nawiązywaniu komunikacji między zdalnym requesterem aplikacji i lokalnym serwerem DRDA DB2 for VM. VTAM kieruje przychodzące połączenia do określonej bramy AVS, a następnie do serwera aplikacji (patrz Rys. 28 na stronie 116).



Rysunek 28. Uzyskiwanie dostępu do zasobu zdalnego

Załóżmy, że DB2 for VM Application Server działa w kolekcji TSAF. Z definicji oznacza to, że maszyna TSAF działa na lokalnym hoście VM, na którym znajduje się serwer aplikacji. Także komponent AVS i maszyna VTAM działają w systemie VM w tej kolekcji TSAF. AVS i VTAM także mogą znajdować się w tym samym systemie co requester aplikacji i serwer aplikacji.

Maszyna VTAM po uruchomieniu definiuje lokalną bramę AVS do sieci SNA i uaktywnia co najmniej jedną sesję do późniejszego wykorzystania podczas nawiązywania konwersacji.

Maszyna AVS po uruchomieniu negocjuje limity liczby sesji między lokalną bramą AVS i potencjalnymi partnerskimi jednostkami logicznymi (LU).

Serwer aplikacji może być aktywny lub nieaktywny. Należy go uruchomić, aby mógł on przetwarzać żądania od podobnego lub niepodobnego requestera aplikacji. Serwer aplikacji po uruchomieniu korzysta z usługi *IDENT, aby zarejestrować ID zasobu, którym zarządza za pomocą systemu VM hosta. Każda rejestracja tworzy pozycję w wewnętrznej tabeli zasobów obsługiwanej przez system VM.

Po nawiązaniu sesji przez lokalny komponent AVS z partnerską jednostką logiczną, akceptuje on konwersację i przekazuje nazwę TPN, ID użytkownika i hasło do hosta

VM w celu sprawdzenia ich poprawności. System VM szuka nazwy TPN i jego wewnętrznej tabeli zasobów. Tabela ta zawiera pozycje dla każdego ID zasobu zarejestrowanego za pomocą usługi systemowej *IDENT. Jeśli wyszukiwanie TPN powiodło się, VM sprawdza poprawność ID użytkownika i hasła przy użyciu swojego katalogu, RACF lub podobnego produktu chroniącego. Jeśli sprawdzanie poprawności powiodło się, AVS nawiązuje połączenie z serwerem aplikacji i przekazuje mu ID użytkownika w celu sprawdzenia autoryzacji do bazy danych.

Jeśli przeszukiwanie tabel nie powiodło się, AVS zakłada, że TPN może znajdować się w innym systemie VM w kolekcji TSAF i nawiązuje połączenie z lokalną maszyną TSAF, przekazując jej ID użytkownika, hasło i TPN. Maszyna TSAF odpytuje pozostałe maszyny TSAF w kolekcji TSAF. Jeśli jedna z tych maszyn potwierdza istnienie TPN we własnej tabeli zasobów, lokalna maszyna TSAF łączy się ze zdalną maszyną TSAF i przekazuje jej ID użytkownika i hasło w celu sprawdzenia za pomocą katalogu VM. Jeśli sprawdzanie poprawności powiodło się, maszyna TSAF łączy się z serwerem aplikacji i przekazuje mu ID użytkownika w celu sprawdzenia autoryzacji do bazy danych.

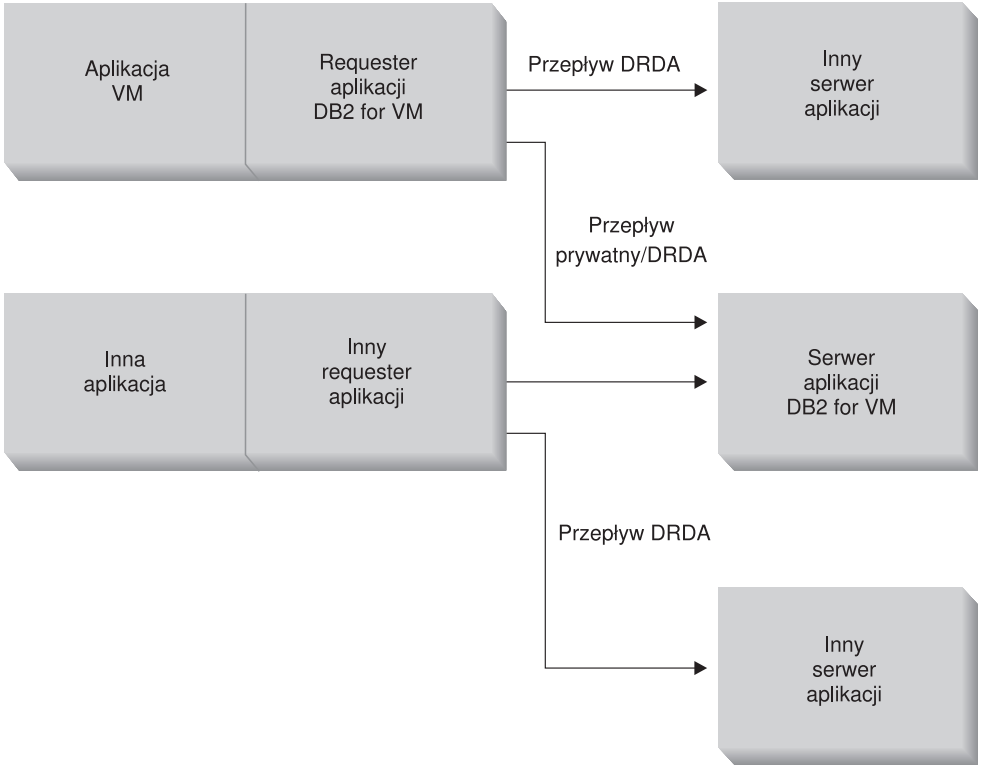
Jeśli requester aplikacji chce skorzystać z obsługi rozproszonej jednostki pracy DRDA, to nawiązuje konwersację zabezpieczoną (np. SYNCLEVEL=SYNCPT) z serwerem aplikacji DB2 for VM. Zanim CMS przedstawi połączenie DB2 for VM, tworzy jednostkę pracy CMS do konwersacji zabezpieczonej w maszynie DB2 for VM. Później DB2 for VM korzysta z tej jednostki pracy za każdym razem, gdy wykonuje pracę dla reqestera. Gdy DB2 for VM zaczyna wykonywać pracę dla requestera, rejestruje jednostkę pracy CMS za pomocą menedżera punktu synchronizacji CRR. Następnie, gdy DB2 odbiera wskazanie ″take commit″ lub ″take rollback″ w konwersacji zabezpieczonej, prosi menedżera punktu synchronizacji CRR o zatwierdzenie lub wycofanie zmian w jednostce pracy. Następnie menedżer punktu synchronizacji CRR wykonuje zatwierdzenie lub wycofanie zmian, prosząc CRR Recovery Server o protokołowanie punktu synchronizacji, jeśli jest to konieczne.

Konwersacja APPC między requesterem aplikacji i serwerem aplikacji może obejmować dodatkowe systemy; zależy to od złożoności routingu połączenia. Jednakże wszystkie pośrednie połączenia są zarządzane przez system VM i są przezroczyste dla requestera aplikacji lub aplikacji użytkownika. Interfejs APPC/VM pozwala serwerowi aplikacji DB2 for VM komunikować się z aplikacją APPC znajdującą się w:

- tym samym systemie VM,
- innym systemie VM,
- systemie VM w sieci SNA, na którym działają AVS i VTA,
- systemie VM w innej kolekcji TSAF, na którym działają AVS i VTAM,
- systemie w sieci SNA różnym od VM, obsługującym protokół LU 6.2,
- systemie w sieci SNA innego niż firmy IBM, obsługującym protokół LU 6.2.

Implementacja DB2 for VM

Jak przedstawiono na Rys. 29, aplikacja VM musi przejść przez requester aplikacji DB2 for VM (adapter zasobów), aby uzyskać dostęp do dowolnej bazy danych serwera aplikacji DB2 for VM lub DRDA. Baza danych serwera aplikacji DB2 for VM może odbierać żądania SQL od dowolnego requestera aplikacji DB2 for VM lub DRDA.



Rysunek 29. Requester aplikacji i serwer aplikacji DB2 for VM

Opcje przetwarzania wstępnego lub uruchamiania aplikacji

DB2 for VM obsługuje trzy opcje przetwarzania komendy SQLINIT, które pozwalają użytkownikowi i administratorowi bazy danych włączyć obsługę rozproszonych baz danych. Przed przetwarzaniem wstępnym lub uruchomieniem aplikacji użytkownik może określić jedną z następujących opcji SQLINIT:

PROTOCOL(SQLDS)
Żądanie użycia prywatnego protokołu SQLDS. Jest to opcja domyślna. Opcji tej można użyć między requesterem i serwerem aplikacji DB2 for VM w

środowisku lokalnym lub zdalnym. Serwer aplikacji DB2 for VM zakłada, że requester korzysta z tego samego CCSID co serwer. Domyślna wartość CCSID[5] ustawiona przez requester za pośrednictwem SQLINIT jest ignorowana, a żaden LU 6.2 LUWID nie jest związany z konwersacją. Jest to najbardziej efektywna opcja, jeśli używane są tylko systemy DB2 for VM i wszędzie jest ten sam domyślny identyfikator CCSID.

PROTOCOL(AUTO)

Żąda od requestera aplikacji DB2 for VM określenia, czy serwer aplikacji jest systemem podobnym czy niepodobnym oraz czy ma być używany prywatny protokół SQLDS dla systemu podobnego, czy protokół DRDA dla systemu niepodobnego. Opcji tej można używać między podobnymi (lokalnymi i zdalnymi) i niepodobnymi systemami. Jeśli na serwerze aplikacji nie jest ustawiona opcja PROTOCOL=SQLDS, requester aplikacji i serwer mają różne wartości domyślne CCSID. Żądania i odpowiedzi są odpowiednio przekształcane. AUTO jest opcją zalecaną w następujących przypadkach:

- Jeśli wymagany jest dostęp do podobnych, jak i niepodobnych systemów.
- Jeśli wartości domyślne CCSID są różne na serwerze i requesterze (i opcją PROTOCOL serwera aplikacji nie jest SQLDS).
- Jeśli wymagana jest jednostka logiczna LU 6.2 LUWID związana z każdą konwersacją, tak aby można było prześledzić drogę zadania wstecz, do źródła pochodzenia. Jest to użyteczne, gdy zarządza się wieloma systemami zdalnymi DB2 for VM w sieci rozproszonej bazy danych.

PROTOCOL(DRDA)

Wymusza na requesterze aplikacji DB2 for VM używanie do komunikacji z serwerem aplikacji tylko protokołu DRDA. Opcji tej można używać między podobnymi (lokalnymi i zdalnymi) i niepodobnymi systemami. Jeśli serwer aplikacji jest systemem podobnym, protokół DRDA jest używany między dwoma systemami DB2 for VM. Requester aplikacji i serwer aplikacji mają różne wartości domyślne CCSID. Żądania i odpowiedzi są odpowiednio przekształcane. Opcji tej można używać między dwoma systemami DB2 for VM do testowania lub dla określonych aplikacji, jeśli używanie protokołu DRDA może udostępnić większą przepustowość dzięki wykorzystaniu większych rozmiarów buforów do wysyłania i odbierania danych.

Tabela 3 na stronie 120 przedstawia porównanie funkcjonalne charakterystyki opcji przetwarzania SQLINIT requestera aplikacji DB2 for VM.

5. W DB2 for VM requester aplikacji i serwer aplikacji określają domyślny identyfikator CCSID, ustawiając opcję CHARNAME dla SQLINIT i odpowiednio dla SQLSTART. Nazwa CHARNAME jest nazwą symboliczną, która jest wewnętrznym odwzorowaniem na odpowiedni identyfikator CCSID.

6. Rozszerzony dynamiczny SQL jest obsługiwany za pomocą przepływów DRDA, przez przekształcanie w instrukcje dynamiczne lub statyczne. Mają zastosowanie pewne ograniczenia.

Tabela 3. Porównanie opcji przetwarzania SQLINIT requestera aplikacji DB2 for VM

[SQLDS]	[AUTO]	[DRDA]
Obaj partnerzy muszą być systemami DB2 for VM.	Łączy się z dowolnym systemem DRDA.	Łączy się z dowolnym systemem DRDA.
Może komunikować się z partnerem lokalnie przez TSAF lub AVS/VTAM.	Może komunikować się z systemem DB2 for VM lokalnie lub z systemem zdalnym DB2 for VM przez TSAF lub AVS. Z niepodobnym systemem musi komunikować się przez AVS.	Może komunikować się z systemem DB2 for VM lokalnie lub z systemem zdalnym DB2 for VM przez TSAF lub AVS. Z niepodobnym systemem musi komunikować się przez AVS.
Obsługuje statyczny, dynamiczny i rozszerzony dynamiczny SQL.	Obsługuje statyczny, dynamiczny i rozszerzony dynamiczny SQL.	Obsługuje statyczny, dynamiczny i rozszerzony dynamiczny SQL [6].
CCSID zdefiniowane przez SQLINIT dla requestera aplikacji są ignorowane przez serwer aplikacji DB2 for VM.	CCSID zdefiniowane przez SQLINIT dla requestra aplikacji są honorowane przez serwer aplikacji DB2 for VM, wykonywana jest odpowiednia konwersja (jeśli serwer aplikacji jest także ustawiony na AUTO).	CCSID zdefiniowane przez SQLINIT dla requestera aplikacji są honorowane przez serwer aplikacji DB2 for VM, wykonywana jest odpowiednia konwersja.
Stała wielkość bloków 8 kB; wywołanie OPEN nie zwraca żadnych wierszy; requester aplikacji musi jawnie zamknąć kursor.	DB2 for VM do DB2 for VM: metoda SQLDS; wszystkie inne: metoda DRDA.	Zmienna wielkość bloku - od 1 kB do 32 kB; bardziej zwarte pakowanie danych; wywołanie OPEN zwraca jeden blok wierszy; serwer aplikacji może jawnie zamknąć kursor, oszczędzając requesterowi aplikacji wysyłania wywołania CLOSE.
Może korzystać z instrukcji INSERT i PUT dla kursorów przy wstawianiu bloku wierszy, używając stałej wielkości bloku równej 8 kB.	DB2 for VM do DB2 for VM: metoda SQLDS; wszystkie inne: metoda DRDA.	PUT są przekształcane na zwykłe jednowierszowe wstawienia wierszy i wysyłają jeden wiersz na raz.
Wszystkie komendy unikalne dla DB2 for VM są obsługiwane.	DB2 for VM do DB2 for VM: metoda SQLDS; wszystkie inne: metoda DRDA.	Komendy operatora DB2 for VM, niektóre instrukcje DB2 for VM i część komend ISQL i DBSU nie jest obsługiwana (patrz *DB2 for VSE & VM SQL Reference*).
LUWID nie jest obsługiwany.	LUWID jest obsługiwany.	LUWID jest obsługiwany.

Opcje uruchamiania serwera baz danych

W tej sekcji opisano różne opcje uruchamiania serwera baz danych.

Parametr PROTOCOL

Podczas uruchamiania serwera baz danych administrator może nadać parametrowi PROTOCOL jedną z następujących wartości:

SQLDS

Opcja domyślna i zalecana, jeśli serwer aplikacji wymaga zapewnienia obsługi tylko dla requesterów aplikacji DB2 for VM lub żądania aplikacji DB2 for VSE

korzystającego ze współużytkowania gościnnego VSE. Serwer aplikacji korzysta jedynie z prywatnego przepływu (SQLDS).

Serwer aplikacji uwzględnia opcje przetwarzania wybrane przez requester aplikacji. Jeśli requester DB2 for VM określi PROTOCOL(SQLDS), przetwarzanie na serwerze DB2 for VM jest kontynuowane z prywatnymi przepływami. Jeśli requester DB2 for VM określi PROTOCOL(AUTO), serwer DB2 for VM zawiadamia requester o konieczności przełączenia na przepływ prywatny. Informacje o CCSID nie są wymieniane między requesterem aplikacji i serwerem aplikacji. Serwer aplikacji zakłada, że identyfikatory CCSID requestera aplikacji są takie same, jak identyfikatory CCSID serwera aplikacji. Jeśli requester DB2 for VM określa PROTOCOL(DRDA), konwersacja zostaje zakończona. Jeśli requester aplikacji inny niż DB2 for VSE &VM próbuje uzyskać dostęp do serwera DB2 for VM server, konwersacja zostaje zakończona.

AUTO Opcja zalecana, jeśli serwer aplikacji wymaga udostępnienia obsługi zarówno protokołu prywatnego, jak i protokołu DRDA. Requester aplikacji DB2 for VM, który określił opcję PROTOCOL(SQLDS) lub PROTOCOL(AUTO), komunikuje się w przepływie prywatnym. W przypadku requestera aplikacji, który podał opcję SQLDS, nie są wymieniane żadne informacje o CCSID. Serwer aplikacji zakłada, że identyfikatory CCSID są takie same, jak identyfikatory CCSID serwera. W przypadku requestera, który podał opcję AUTO, informacje o identyfikatorach CCSID są wymieniane i wykonywana jest odpowiednia konwersja CCSID żądań odpowiedzi. Przepływ DRDA jest wymagany przez requestery inne niż DB2 for VM lub przez requestery DB2 for VM, które podały opcję PROTOCOL(DRDA).

Parametr SYNCPNT

Parametr ten określa, czy menedżer punktu synchronizacji (SPM) zostanie użyty do koordynacji działania rozproszonej jednostki pracy podczas odczytu wielopunktowego DRDA-2 i zapisu wielopunktowego.

Jeśli podano wartość Y, serwer będzie używał menedżera punktu synchronizacji, o ile jest to możliwe, aby koordynować czynności zatwierdzania dwufazowego i resynchronizacji. Jeśli określona jest wartość N, serwer aplikacji nie będzie używał SPM w celu wykonania zatwierdzania dwufazowego. Jeśli podano wartość N, serwer aplikacji jest ograniczony do rozproszonych jednostek pracy wielopunktowego odczytu, jednopunktowego zapisu i może być jedynym punktem zapisu. Jeśli podano wartość Y, lecz serwer aplikacji otrzymuje informacje, że menedżer punktu synchronizacji nie jest dostępny, serwer będzie działał, jakby podano wartość N.

Jeśli PROTOCOL=AUTO, wartością domyślną jest SYNCPNT=Y. Jeśli PROTOCOL=SQLDS, parametr SYNCPNT ma wartość N.

Konfigurowanie requestera aplikacji w środowisku VM

DB2 for VM implementuje obsługę requestera aplikacji DRDA jako integralną część adaptera zasobów znajdującego się z aplikacją w maszynie wirtualnej użytkownika. Obsługi requestera aplikacji można używać, gdy maszyna wirtualna lokalnych menedżerów baz danych jest nieaktywna. Obsługę requestera aplikacji DRDA można uaktywnić, uruchamiając SQLINIT EXEC ZPROTOCOL(AUTO) lub PROTOCOL(DRDA) (patrz "Opcje przetwarzania wstępnego lub uruchamiania aplikacji" na stronie 118).

Jeśli DB2 for VM działa jako requester aplikacji, może się on łączyć z serwerem aplikacji DB2 for VM lub z dowolnym innym serwerem obsługującym architekturę DRDA. Aby skonfigurować requester aplikacji DB2 for VM, tak aby zapewniał on dostęp do rozproszonej bazy danych, należy zapoznać się z następującymi zagadnieniami:

- "Dostarczanie informacji sieciowych". Requester aplikacji musi mieć możliwość akceptowania wartości RDB_NAME i odwzorowywania ich na wartości SNA NETID.LUNAME. DB2 for VM korzysta z CMS Communications Directory, aby wpisywać do katalogu nazwy RDB_NAME i odpowiadające im parametry sieciowe. Communications Directory umożliwia requesterowi aplikacji przekazywanie niezbędnych informacji SNA do VTAM, gdy wydawane są żądania rozproszonej bazy danych.
- "Zapewnianie ochrony" na stronie 130. Aby serwer aplikacji mógł akceptować żądania zdalnych baz danych, requester aplikacji musi dostarczać informacji o ochronie wymaganych przez serwer aplikacji. DB2 for VM korzysta z Communications Directory i katalogu CP po stronie requestera aplikacji i katalogu CP lub opcjonalnie RACF po stronie serwera aplikacji, aby podczas wydawania żądań rozproszonej bazy danych dostarczać wymaganych informacji o ochronie sieci.
- "Reprezentacja danych" na stronie 134. Requester aplikacji musi mieć identyfikator CCSID zgodny z identyfikatorem serwera aplikacji.

Dostarczanie informacji sieciowych

Wiele procesów w środowisku rozproszonych baz danych wymaga wymiany komunikatów z innymi miejscami w sieci. Aby komunikaty były wymieniane poprawnie, należy:

1. zdefiniować system lokalny,
2. zdefiniować system zdalny,
3. zdefiniować podsystem komunikacyjny,
4. ustawić wielkości RU i pacing,
5. przygotować requester aplikacji DB2 for VM.

Definiowanie systemu lokalnego

Requester aplikacji DB2 for VM i serwer aplikacji DB2 for VM są niezależne od siebie. Requester aplikacji DB2 for VM kieruje połączenie bezpośrednio do lokalnych lub zdalnych serwerów aplikacji. Jednak nie definiuje sam siebie jako celu żądań połączeń przychodzących. Tylko serwer aplikacji DB2 for VM może zaakceptować (lub odrzucić)

przychodzące żądania połączeń. W przypadku tego requester aplikacji DB2 for VM nie identyfikuje nazw RDB_NAME i TPN dla siebie samego, tak jak to robi DB2 Universal Database for OS/390.

Należy zdefiniować requester aplikacji DB2 for do sieci SNA, wykonując następujące kroki:

1. Zdefiniować nazwy bram AVS przy użyciu instrukcji definiowania VTAM APPL.

   Aby wyznaczać trasę przychodzących żądań w sieci, requester aplikacji musi mieć zdefiniowane nazwy bram (na przykład nazwy LU). Rys. 30 ilustruje przykładową definicję bramy. Wymienione instrukcje znajdują się w maszynie wirtualnej VTAM. Gdy VTAM uruchamia się, bramy w sieci zostają zidentyfikowane, nie są jednak aktywne, dopóki nie zostanie uruchomiona sterująca maszyna AVS. Każda maszyna wirtualna AVS może definiować wiele bram na hoście VM.

```
                VBUILD TYPE=APPL
************************************************************
*                                                          *
*     Gateway Definition for Toronto DB2 for VM System     *
*                                                          *
************************************************************
TORGATE  APPL  APPC=YES,                                   X
               AUTHEXIT=YES,                               X
               AUTOSES=1,                                  X
               DMINWNL=10,                                 X
               DMINWNR=10,                                 X
               DSESLIM=20,                                 X
               EAS=9999,                                   X
               MAXPVT=100K,                                X
               MODETAB=RDBMODES,                           X
               PARSESS=YES,                                X
               SECACPT=ALREADYV,                           X
               SYNCLVL=SYNCPT,                             X
               VPACING=2
```

Rysunek 30. Przykład definicji bramy AVS

Poniżej opisano parametry instrukcji VTAM APPL, dotyczące zagadnień omawianych w tym podręczniku. (Instrukcja VTAM APPL obsługuje o wiele więcej parametrów).

TORGATE
: VTAM korzysta z etykiety instrukcji APPL jako nazwy bramy (LU). Na Rys. 30 zdefiniowano bramę TORGATE. Instrukcja VTAM APPL nie określa NETID. NETID dla wszystkich aplikacji VTAM w systemie VTAM jest przydzielany automatycznie.

AUTOSES=1
: Brama TORGATE określa, że wygrywająca rywalizację sesja SNA

uruchamia się automatycznie po wydaniu komendy APPC Change Number of Sessions (CNOS). Aby uzyskać informacje o wszystkich wypadkach nieprawidłowego zakończenia przetwarzania, należy dla AVS podać niezerową wartość AUTOSES. Automatyczne uruchamianie wszystkich sesji APPC między dowolnymi dwoma partnerami rozproszonej bazy danych nie jest konieczne. Jeśli wartość AUTOSES jest mniejsza od limitu zwycięzcy rywalizacji (MINWNL), VTAM opóźnia uruchomienie pozostałych sesji, dopóki nie są one wymagane przez aplikację rozproszonej bazy danych.

DMINWNL=10

Brama TORGATE określa, że dany system DB2 for VM jest zwycięzcą rywalizacji w co najmniej 10 sesjach. Przetwarzanie CNOS domyślnie wykorzystuje parametr DMINWNL, lecz przez wydanie komendy AGW CNOS z maszyny wirtualnej AVS można go nadpisać dla dowolnego partnera.

DMINWNR=10

Brama TORGATE określa, że dany system partnerski jest zwycięzcą rywalizacji w co najmniej 10 sesjach. Przetwarzanie CNOS domyślnie wykorzystuje parametr DMINWNR, lecz przez wydanie komendy AGW CNOS z maszyny wirtualnej AVS można go nadpisać dla dowolnego partnera.

DSESLIM=20

Ogólna liczba sesji (zarówno zwycięzców, jak i przegranych) dozwolona między bramą TORGATE i wszystkimi partnerskimi systemami rozproszonymi dla określonego trybu nazwy grupy wynosi 20. Przetwarzanie CNOS domyślnie wykorzystuje parametr DSESLIM, lecz przez wydanie komendy AGW CNOS z maszyny wirtualnej AVS można go nadpisać dla dowolnego partnera. Jeśli partner nie może obsługiwać tylu sesji, ile określono w parametrach DSESLIM, DMINWNL lub DMINWNR, proces CNOS negocjuje nowe wartości tych parametrów, możliwe do zaakceptowania przez partnera.

EAS=9999

Oszacowanie łącznej liczby sesji, które są wymagane przez daną jednostkę logiczną VTAM.

MODETAB=RDBMODES

Nazwa tabeli trybów VTAM ma wartość RDBMODES. Wymieniona tabela zawiera nazwy wszystkich trybów, których dana brama może używać do komunikacji z innymi partnerami rozproszonej bazy danych.

SECACPT=ALREADYV

Parametr akceptacji ochrony, który identyfikuje najwyższy poziom ochrony konwersacji APPC obsługiwany przez daną bramę w momencie prezentacji

żądania rozproszonej bazy danych z partnera zdalnego. SECACPT=ALREADYV jest zalecane. Opcja ALREADYV obsługuje następujące poziomy ochrony:

- SECURITY=NONE - żądanie nie zawierające informacji o ochronie. DB2 for VM odrzuca żądania DRDA korzystające z tego poziomu ochrony.
- SECURITY=PGM - żądanie zawierające identyfikator i hasło użytkownika requestera. DB2 for VM akceptuje żądania DRDA korzystające z tego poziomu ochrony.
- SECURITY=SAME - uprzednio sprawdzone żądanie, które zawiera tylko ID użytkownika requestera.

SYNCLVL=SYNCPT

Parametr SYNCLVL określa poziom obsługi synchronizacji dla AVS. Wartość SYNCPT wskazuje, że poziom synchronizacji wynosi NONE. Obsługiwane są wartości CONFIRM i SYNCPT. Jeśli brama AVS jest wykorzystywana do działania rozproszonej jednostki pracy DRDA-2 na serwerze DB2 for VM, należy podać wartość SYNCPT. Jeśli działanie rozproszonej jednostki pracy NIE będzie zakończone, należy podać wartość CONFIRM (wskazującą, że NONE i CONFIRM są obsługiwane, a SYNCPT nie).

VERIFY=NONE

Identyfikuje poziom ochrony sesji SNA (weryfikację partnerskiej jednostki logicznej) wymagany przez system DB2 for VM. Wartość NONE wskazuje, że weryfikacja partnerskiej jednostki logicznej nie jest wymagana.

DB2 for VM nie ogranicza możliwości parametru VERIFY, lecz uruchomiona wersja VTAM może wpłynąć na możliwości wyboru. W sieci niezaufanej DB2 for VM zaleca się ustawienie wartości VERIFY=REQUIRED. Jeśli zostanie wybrane VERIFY=OPTIONAL, VTAM przeprowadzi weryfikację partnerskiej jednostki logicznej tylko wobec tych partnerów, którzy zapewniają tę obsługę. VERIFY=REQUIRED powoduje, że VTAM odrzuca partnerów, którzy nie mogą wykonać weryfikacji partnerskiej jednostki logicznej.

VPACING=2

Parametr ustawiający licznik pacingu sesji, wykorzystywany między partnerską jednostką logiczną i daną bramą. Pacing sesji jest bardzo ważny dla systemów rozproszonych baz danych.

2. Uaktywnić bramę.

   Bramę włącza się z maszyny wirtualnej AVS działającej na tym samym hoście co requester aplikacji DB2 for VM (lub na innych hostach wewnątrz jednej kolekcji TSAF). Do profilu maszyny AVS należy dołączyć komendę AGW ACTIVATE GATEWAY GLOBAL lub wydać tę komendę interaktywnie z konsoli maszyny AVS, aby brama była automatycznie włączana przy każdym starcie AVS.

3. Używać komendy AGW CNOS do negocjowania liczby sesji między bramą i każdą jej partnerską jednostką logiczną.

   Sprawdź, czy wartość MAXCONN w katalogu CP maszyny bramy AVS jest wystarczająco duża, aby obsłużyć całkowitą liczbę wymaganych sesji.

   Aby wyłączyć, wydaj komendę AGW DEACTIVE GATEWAY z maszyny wirtualnej AVS. Definicja bramy pozostaje niezmieniona. Bramę można w dowolnej chwili włączyć ponownie za pomocą komendy AGW ACTIVATE GATEWAY GLOBAL.

   Formaty komend AVS można znaleźć w podręczniku *VM/ESA Connectivity Planning, Administration and Operation*.

4. Sprawdzić, czy VTAM NETID podczas instalacji został zdefiniowany dla DB2 FOR VM DBMS.

   Identyfikator NETID hosta (lub innych hostów wewnątrz tej samej kolekcji TSAF), na którym znajduje się requester aplikacji jest dostarczany przez VTAM, gdy requester rozpoczyna pracę. Identyfikator NETID jest zapisywany w pliku CMS SNA NETID i jest przechowywany na dysku DB2 dla VM, do którego dostęp jest możliwy przez requester aplikacji. Requester aplikacji korzysta z identyfikatora sieciowego NETID w celu generowania parametru LUWID, który jest przesyłany razem z każdą konwersacją.

Definiowanie systemów zdalnych

Systemy zdalne muszą być zdefiniowane przez zarejestrowanie nazw jednostek logicznych, które umożliwiają VTAM odnalezienie żądanych punktów docelowych sieci. AVS po uruchomieniu identyfikuje globalne nazwy bram (nazwy jednostek logicznych) dostępne dla routingu w sieci żądań SQL do VTAM. Nazwa bramy musi być unikalna w obrębie zestawu nazw jednostek logicznych rozpoznawanego przez lokalny system VTAM, tak aby zarówno żądania przychodzące, jak i wychodzące były kierowane do odpowiedniej nazwy jednostki logicznej. Jest to najlepszy sposób zapewnienia unikalności nazw w całej sieci użytkownika. Jednocześnie uproszczeniu ulega proces definiowania zasobu VTAM.

Jeśli aplikacja DB2 for VM żąda danych ze zdalnego systemu, DB2 for VM szuka w CMS Communications Directory następujących informacji dotyczących systemu zdalnego:

- nazwa bramy (nazwa lokalnej jednostki logicznej),
- nazwa zdalnej jednostki logicznej,
- nazwa zdalnej nazwy TPN,
- poziom ochrony konwersacji wymagany przez serwer aplikacji,
- ID użytkownika identyfikujący requester aplikacji dla serwera aplikacji,
- hasło określające tożsamość requestera aplikacji dla serwera aplikacji,
- nazwa trybu opisująca charakterystykę sesji, która ma być używana w komunikacji z serwerem aplikacji,
- RDB_NAME.

CMS Communications Directory jest plikiem CMS typu NAMES, który jest zakładany i zarządzany przez administratora systemu DB2 for VM. Administrator może korzystać z XEDIT przy tworzeniu pliku i dodawaniu żądanych pozycji identyfikujących każdego potencjalnego partnera DRDA. Każda pozycja w katalogu jest zestawem tokenów i związanych z nimi wartości. Rys. 31 przedstawia przykładową pozycję. Podczas przeszukiwania klucz przeszukiwania jest porównywany z wartością tokenu :dbname dla każdej pozycji w pliku, aż do znalezienia pasującego elementu lub do osiągnięcia końca pliku. Na przykład na Rys. 31 kierownik sprzedaży w Toronto chce utworzyć miesięczny raport sprzedaży filii w Montrealu, uzyskując zdalnie dostęp do danych z bazy danych 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
```

Rysunek 31. Przykładowa pozycja w CMS Communications Directory

Token :tpn identyfikuje nazwę programu transakcyjnego uaktywniającego serwer aplikacji. Pierwsza część tokenu, :luname, identyfikuje bramę AVS (lokalną jednostkę logiczną) używaną przy uzyskiwaniu dostępu do sieci SNA. Druga część identyfikuje nazwę zdalnej jednostki logicznej. Token :modename identyfikuje tryb VTAM definiujący charakterystyki sesji przydzielonych między lokalnymi i zdalnymi jednostkami logicznymi. Wielkość jednostki żądania (RU), pacing i klasa usługi (COS) są przykładami takich charakterystyk. Token :security wskazuje poziom ochrony, który ma być używany w konwersacjach łączących requester aplikacji z serwerem aplikacji.

CMS Communications Directory znajduje się na publicznym dysku systemowym, dostępnym dla wszystkich requesterów aplikacji w danym systemie VM. Każdy program lub produkt wymagający zdalnego dostępu przez VTAM może korzystać z CMS Communications Directory.

Dostęp do CMS Communications Directory można uzyskać na dwóch poziomach: na poziomie systemu i na poziomie użytkownika. Na przykład można utworzyć katalog poziomu systemu na publicznym dysku systemowym, dostępnym dla wszystkich requesterów aplikacji w danym systemie VM. Można również utworzyć własny katalog poziomu użytkownika, który nadpisze istniejące pozycje lub wprowadzić nowe pozycje, których brakuje w katalogu poziomu systemu. Najpierw jest przeszukiwany katalog poziomu użytkownika. Jeśli przeszukiwanie nie powiedzie się, przeszukiwany jest katalog poziomu systemu. Katalog poziomu systemu jest rozszerzeniem katalogu

poziomu użytkownika; przeszukiwany jest tylko w sytuacji, gdy szukanych wartości nie odnaleziono w katalogu poziomu użytkownika.

Każdy z katalogów jest identyfikowany dla aplikacji i uaktywniany komendą CMS SET COMDIR. Na przykład można użyć następującej sekwencji komend do identyfikowania katalogów poziomu systemu i poziomu użytkownika (odpowiednio na minidyskach A i S), lecz do uaktywniania w celu przeszukiwania można wybrać tylko katalog poziomu systemu:

```
    SET COMDIR FILE SYSTEM SCOMDIR NAMES S

SET COMDIR FILE USER UCOMDIR NAMES A

SET COMDIR OFF USER
```

CMS Communications Directory szczegółowo opisano w podręczniku *VM/ESA Connectivity Planning, Administration and Operation*. Komendę CMS SET COMDIR jest opisano w podręczniku *VM/ESA CMS Command Reference*.

Definiowanie podsystemu komunikacyjnego

W środowisku VM komunikacją zarządza kilka komponentów. W komunikacji między niepodobnymi systemami DRDA biorą udział komponenty: APPC/VM, CMS Communications Directory, TSAF, AVS i VTAM.

APPC/VM jest interfejsem API LU 6.2 poziomu asemblera, który requester aplikacji DB2 for VM wykorzystuje do żądania usług komunikacyjnych. CMS Communications Directory dostarcza informacji o routingu i ochronie rozproszonego systemu partnerskiego. AVS uaktywnia bramę i wykonuje translację wychodzących przepływów APPC/VM na przepływy APPC/VTAM, a przychodzących przepływów APPC/VTAM na przepływy APPC/VM.

Przy ustalaniu trasy żądań do odpowiedniego partnera DRDA APPC/VM, TSAF i AVS polega na CMS Communications Directory, VTAM i *IDENT.

Aby VTAM mógł komunikować się z partnerską aplikacją zidentyfikowaną w CMS Communications Directory, należy mu dostarczyć następujących informacji:

1. Zdefiniować nazwę jednostki logicznej każdego requestera aplikacji i serwera aplikacji VTAM. Położenie i składnia tych definicji zależy od sposobu, w jaki serwer zdalny jest logicznie i fizycznie połączony z systemem VTAM.
2. Utworzyć tabelę trybów VTAM dla każdej nazwy trybu określonej w CMS Communications Directory. Pozycje te opisują wielkość jednostki żądania (RU), wielkość okna pacingu i klasę usług dla danej nazwy trybu.
3. Jeśli będzie używana weryfikacja partnerskiej jednostki logicznej (ochrona poziomu sesji), dla algorytmu weryfikacji należy podać profile VTAM i RACF (lub ich odpowiedniki).

Uwagi dotyczące limitu liczby sesji AVS: Jeśli requester aplikacji korzysta z AVS do komunikowania się z serwerem zdalnym aplikacji, połączenie jest inicjowane. Jeśli połączenie powoduje przekroczenie ustalonego limitu sesji, AVS zawiesza je, dopóki sesja nie będzie dostępna. Gdy sesja staje się dostępna, AVS przydziela zawieszone połączenie do sesji i sterowanie zostaje zwrócone do aplikacji użytkownika. Aby uniknąć tej sytuacji, należy zaplanować maksymalne użytkowanie, zwiększając limit sesji dla pewnej liczby dodatkowych połączeń. Należy sprawdzić, czy wartość MAXCONN w katalogu CP maszyny AVS jest wystarczająco duża, aby obsłużyć maksymalne użytkowanie połączeń APPC/VM.

Ustawianie wielkości RU i pacingu

Pozycje zdefiniowane w tabeli trybów VTAM określają wielkości jednostek żądania (RU) i zliczanie pacingu. Niepoprawne zdefiniowanie tych wartości może wywołać niepożądany efekt we wszystkich aplikacjach VTAM.

Po wybraniu wielkości jednostek żądań (RU), limitów sesji i zliczania pacingu należy rozważyć wpływ wywierany przez te wartości na sieć SNA. Przy instalowaniu nowego systemu rozproszonej bazy danych należy przejrzeć następujące pozycje:

- W przypadku połączeń VTAM CTC należy sprawdzić, czy parametr MAXBFRU jest wystarczająco duży, aby obsłużyć wielkość jednostki żądań (RU) plus 29 bajtów, które VTAM dodaje do nagłówka żądania i nagłówka transmisji SNA. MAXBFRU jest mierzony w jednostkach po 4096 bajtów, dlatego aby obsłużyć RU o wielkości 4 kB, MAXBFRU musi mieć wartość co najmniej 2.
- W przypadku połączeń NCP należy się upewnić, że parametr MAXDATA jest wystarczająco duży, aby obsłużyć wielkość jednostki żądań (RU) plus 29 bajtów. Jeśli określono wielkość jednostki żądań (RU) równej 4096, MAXDATA musi mieć wartość co najmniej 4125.

  Jeśli określono parametr NCP MAXBFRU, należy wybrać wartość, która pozwoli pomieścić wielkość danej jednostki zdalnej (RU) plus 29 bajtów. W przypadku NCP parametr MAXBFRU określa liczbę buforów VTAM we/wy, które mogą utrzymywać PIU. Jeśli wielkość buforu IOBUF została ustawiona na 441, MAXBFRU=10 poprawnie przetwarza jednostkę żądań o wielkości 4 kB RU, ponieważ 10*441 jest większe od 4096+29.
- Podręcznik *DRDA Connectivity Guide* opisuje sposób, w jaki można uzyskać dostęp do informacji o wpływie rozproszonej bazy danych na pulę VTAM IOBUF. Jeśli używa się zbyt dużej części zasobów puli IOBUF, wydajność wszystkich aplikacji VTAM zostaje obniżona.

Przygotowanie requestera aplikacji DB2 for VM

Requester aplikacji DB2 for VM może nie mieć zainstalowanej obsługi DRDA. Aby przygotować requester aplikacji DB2 for VM do komunikacji DRDA, należy:

1. Użyć ARISDBMA do instalacji obsługi DRDA:
   - Użyć ″ARISDBMA DRDA(ARAS=Y)″, jeśli zainstalowana jest obsługa dla requestera i serwera.

- Użyć ″ARISDBMA DRDA(AR=Y)″, jeśli zainstalowana jest tylko obsługa dla requestera.

Szczegółowe informacje na ten temat można znaleźć w podręczniku *DB2 for VM System Administration*.

2. Po wydaniu komendy ARISDBMA należy ponownie zbudować ARISQLLD LOADLIB DB2 for VM. W rozdziale *Using a DRDA Environment* podręcznika *DB2 for VM System Administration* można znaleźć szczegółowe informacje na ten temat.

Zapewnianie ochrony

Jeśli system zdalny przetwarza rozproszoną bazę danych w imieniu aplikacji SQL, musi być możliwe spełnienie wymogów ochrony requestera aplikacji, serwera aplikacji i łączącej je sieci. Wymagania te należą do co najmniej jednej z następujących kategorii:

- wybór nazw użytkowników,
- parametry ochrony sieci,
- ochrona menedżera baz danych,
- ochrona wymuszona przez zewnętrzny podsystem ochrony.

Wybieranie nazw użytkowników

Zarówno w SQL, jak i w LU 6.2 użytkownicy otrzymują identyfikatory użytkowników o długości 1 do 8 znaków. Identyfikator użytkownika musi być unikalny w obrębie systemu operacyjnego, lecz nie musi być unikalny w całej sieci SNA. Na przykład może istnieć użytkownik nazwany JONES w systemie TORONTO i inny użytkownik nazwany JONES w systemie MONTREAL. Jeśli tych dwóch użytkowników to ta sama osoba, to konflikt nie wystąpi. Jednak jeśli JONES w TORONTO nie jest tą samą osobą co JONES w MONTREAL, sieć SNA (i konsekwentnie systemy rozproszonych baz danych wewnątrz tej sieci) nie może odróżnić użytkownika JONES w TORONTO od użytkownika JONES w MONTREAL. Jeśli nie podejmie się żadnych kroków w celu zapobieżenia tej sytuacji, to użytkownik JONES w TORONTO będzie mógł używać uprawnień nadanych użytkownikowi JONES w MONTREAL i odwrotnie.

Aby wyeliminować konflikty nazewnictwa, DB2 for VM obsługuje translację nazw użytkowników. System nie wymusza jednak translacji ID użytkowników. Jeśli wymagana jest translacja wymuszona przez system, należy się upewnić, że właściwa translacja nazw przychodzących wykonywana jest na serwerze aplikacji.

Translacja nazw wychodzących jest wykonywana przy użyciu CMS Communications Directory. Pozycja w CMS Communications Directory musi określać :security.PGM. W tym przypadku odpowiednie wartości w tokenach :userid i :password przepływają do miejsca zdalnego (serwera aplikacji) w żądaniu połączenia.

Utworzenie pozycji pokazanej na Rys. 32 na stronie 131 powoduje, że użytkownik o identyfikatorze JONES w systemie lokalnym (TORONTO) jest odwzorowywany na identyfikator użytkownika JONEST podczas łączenia się z serwerem aplikacji

MONTREAL_SALES_DB w systemie MONTREAL. W ten sposób wyeliminowana jest niejednoznaczność identyfikatorów użytkowników.

```
  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
```

Rysunek 32. Translacja nazw wychodzących

Ochrona sieci

Po wybraniu nazwy użytkownika reprezentującej requester aplikacji w punkcie zdalnym (serwer aplikacji), requester aplikacji musi dostarczyć wymaganych informacji dotyczących ochrony sieci jednostki logicznej 6.2 (LU 6.2). Jednostka logiczna 6.2 dostarcza trzech głównych mechanizmów ochrony sieci:

- ochrona na poziomu sesji, określona przy użyciu parametru VERIFY w instrukcji APPL VTAM,
- ochrona na poziomie konwersacji, określona w CMS Communications Directory,
- szyfrowanie.

Ponieważ serwer aplikacji jest odpowiedzialny za zarządzanie zasobami baz danych, określa opcje ochrony sieci wymagane od requestera aplikacji. Należy zapisać wymagania dotyczące ochrony serwera aplikacji w katalogu komunikacyjnym requestera aplikacji, ustawiając odpowiednią wartość w tokenie :security.

DRDA obsługuje następujące opcje ochrony na poziomie konwersacji SNA:

SECURITY=SAME

Znane także jako sprawdzona wcześniej ochrona, ponieważ tylko identyfikator użytkownika (identyfikator logowania) jest wysyłany do systemu zdalnego. Hasło nie jest wysyłane. Ten poziom ochrony konwersacji jest używany, gdy w katalogu komunikacyjnym requestera aplikacji danego serwera aplikacji jest określony :security.SAME. Jeśli korzysta się z tej opcji, translacja wychodzącej nazwy użytkownika nie jest wykonywana. Identyfikator użytkownika wysyłany do zdalnego miejsca DRDA jest ID logowania użytkownika CMS. Token :userid w CMS Communications Directory jest ignorowany w przypadku :security.SAME.

SECURITY=PGM

Ta opcja powoduje, że zarówno ID użytkownika, jak i hasło są wysyłane do zdalnego systemu (serwera aplikacji) celem sprawdzenia. Ta opcja ochrony jest

używana, gdy :security.PGM jest podany w pozycji CMS Communications Directory requestera aplikacji. Gdy korzysta się tej opcji, translacja wychodzącej nazwy użytkownika jest wykonywana.

DB2 for VM nie obsługuje szyfrowania haseł. Hasło może zostać podane w tokenie :password lub może być przechowywane w pozycji katalogu CP użytkownika używającego instrukcji katalogu APPCPASS. Instrukcja APPCPASS zalecana jest, gdy występuje potrzeba zwiększenia ochrony hasła. Jeśli hasło nie zostało podane na pozycji CMS Communications Directory, to na pozycji katalogu systemu użytkownika (VM) szukana jest instrukcja APPCPASS.

Instrukcja APPCPASS: System VM udostępnia instrukcję APPCPASS w celu zwiększenia ochrony identyfikatora użytkownika i hasła, używanych przez requester aplikacji do łączenia się z serwerem aplikacji. APPCPASS jest elastyczna i pozwala przechowywać informacje ochrony na jeden z następujących sposobów:

- **ID użytkownika i hasło:** W tym przypadku tokeny :userid i :password w CMS Communications Directory muszą być puste.
- **Tylko ID użytkownika:** W tym przypadku token :userid w CMS Communications Directory musi być pusty, a token :password musi zawierać hasło użytkownika.
- **Tylko hasło:** W tym przypadku token :password w CMS Communications Directory musi być pusty, a token :userid musi zawierać ID użytkownika.

Rys. 33 ilustruje przypadek, w którym ID użytkownika jest przechowywany w katalogu komunikacyjnym użytkownika, a hasło w pozycji katalogu użytkownika VM. W pozycji katalogu komunikacyjnego ID użytkownika jest ustawiony na MTLSOU, lecz hasło nie jest ustawione. Hasło jest przechowywane w pozycji katalogu użytkownika VM.

```
  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
```

Rysunek 33. Przykład pozycji katalogu komunikacyjnego bez hasła

Gdy APPC/VM inicjuje połączenie między requesterem aplikacji i serwerem aplikacji, używając konwersacji SECURITY=PGM, odczytuje tokeny :userid i :password i przekazuje je do serwera aplikacji. Jeśli co najmniej jeden z nich jest pusty, APPC/VM szuka brakujących informacji w pozycji katalogu użytkownika VM. W takim przypadku instrukcja APPCPASS w pozycji katalogu VM powinna mieć następującą formę:

```
APPCPASS TORGATE MTLGATE MTLSOU Q6VBN8XP
```

Instrukcja ta mówi APPC/VM, że użytkownik (requester aplikacji) żądający połączenia przez (lokalną) bramę AVS TORGATE, partnerską jednostkę logiczną (LU) nazwaną MTLGATE i ID użytkownika MTLSOU powinien wysłać hasło Q6VBN8XP do serwera aplikacji. Na serwerze aplikacji użytkownik jest rozpoznawany dzięki tym dwóm elementom identyfikacyjnym.

Umieszczenie instrukcji PPCPASS w katalogu VM nie jest zadaniem użytkownika. Użytkownik musi poprosić o to programistę systemów VM.

Więcej informacji na temat ochrony poziomu konwersacji i instrukcji APPCPASS można znaleźć w podręczniku *VM/ESA Connectivity Planning, Administration, and Operation*.

Ochrona menedżera baz danych

Jako część ogólnej struktury rozproszonej bazy danych w DRDA, requester aplikacji może brać udział w kontrolowaniu, którzy użytkownicy końcowi mogą tworzyć żądania rozproszonej bazy danych. W DB2 for VM requester aplikacji może brać udział w ochronie rozproszonej bazy danych na trzy sposoby:

Translacja nazw wychodzących
: Translacji wychodzących nazw użytkowników można używać do kontrolowania dostępu do określonego requestera aplikacji na podstawie identyfikacji użytkownika tworzącego żądanie. DB2 for VM próbuje wykonać translację nazwy użytkownika przed wysłaniem żądania do miejsca zdalnego. Najlepszym sposobem jest jednak sprawdzanie przez serwer aplikacji pochodzenia i wykonywanie translacji nazw przychodzących, ponieważ użytkownicy requestera aplikacji VM mogą za pomocą CMS User Communications Directory nadpisać translację nazw wychodzących.

Przetwarzanie wstępne aplikacji
: Użytkownicy końcowi przetwarzają wstępnie aplikacje dla określonego serwera aplikacji, korzystając z komendy SQLPREP EXEC w DB2 for VM lub programu narzędziowego Database Service Utility (DBSU)RELOAD PACKAGE. DB2 for VM nie ogranicza używania tych usług. Gdy dany użytkownik przetwarza wstępnie aplikację, to on właśnie jest właścicielem pakietu wynikowego.

Wykonywanie aplikacji
: Aby użytkownik DB2 for VM mógł uruchomić zdalną aplikację, musi mieć w punkcie zdalnym (serwerze aplikacji) uprawnienia do uruchamiania pakietu zdalnego związanego z tą określoną aplikacją. Autor (właściciel) tego pakietu jest automatycznie autoryzowany do uruchomienia pakietu. Inni użytkownicy mogą otrzymać uprawnienia do uruchomienia pakietu za pomocą instrukcji DB2 for VM GRANT EXECUTE. W ten sposób właściciel aplikacji rozproszonej bazy danych może kontrolować używanie aplikacji na poziomie użytkownik-użytkownik.

Podsystem ochrony

Zewnętrzny podsystem ochrony w systemach VM jest dostarczony przez RACF lub produkt będący jego odpowiednikiem, który zapewnia zgodność interfejsu z RACF. Requester aplikacji DB2 for VM nie współpracuje bezpośrednio z zewnętrznym podsystemem ochrony. Zewnętrzny podsystem ochrony nie jest używany do zapewniania haseł dla ochrony na poziomie konwersacji. Jeśli zostanie wybrana ochrona na poziomie sesji, to zewnętrzny podsystem ochrony będzie wywoływany podczas weryfikacji partnerskiej jednostki logicznej (LU) przez VTAM do sprawdzania poprawności tożsamości nazwy zdalnej jednostki logicznej (LU).

Reprezentacja danych

Requester aplikacji musi mieć ustawione odpowiednie wartości domyślne CHARNAME i CCSID. Dobranie poprawnych wartości zapewnia integralność reprezentacji danych znakowych i redukuje nakład wydajności związany z konwersją identyfikatorów CCSID.

Na przykład jeśli posiadany requester aplikacji DB2 for VM został wygenerowany ze stroną kodową 37 i zestawem znaków 697(CP/CS 37/697) dla znaków US ENGLISH, to requester aplikacji powinien ustawić wartość domyślną CHARNAME na ENGLISH. Jest tak dlatego, że CP/CS 37/697 odpowiada identyfikatorowi CCSID równemu 37, który z kolei odpowiada wartości CHARNAME równej ENGLISH.

Domyślną wartością CHARNAME nowo zainstalowanego lub migrowanego systemu jest INTERNATIONAL, a identyfikator CCSID wynosi 500. Prawdopodobnie *nie* odpowiada to wartości używanej podczas instalacji. Aby wyświetlić wartości bieżących identyfikatorów CCSID, należy skorzystać z następującej komendy:

```
SQLINIT QUERY
```

Odpowiednia wartość CCSID dla requestera aplikacji może nie być obsługiwana przez tabele konwersji na serwerze aplikacji. W takim przypadku należy nawiązać połączenie, wykonując jedną z następujących czynności:

- Należy zaktualizować tabele konwersji CCSID serwera aplikacji, tak aby obsługiwał on konwersję między domyślnym CCSID requestera aplikacji i domyślnym CCSID serwera aplikacji (należy przeczytać podręczniki produktów serwera aplikacji. Znajdują się w nich szczegółowe informacje dotyczące dodawania obsługi konwersji CCSID).
- Należy zmienić domyślny CCSID requestera aplikacji CCSID obsługiwany przez serwer aplikacji. Może to spowodować problemy z integralnością danych, należy więc być świadomym konsekwencji. Konsekwencje mogą być następujące:

  Requester aplikacji korzysta ze sterownika zdefiniowanego za pomocą CP/CS 37/697. Serwer aplikacji nie obsługuje konwersji z CCSID 37, lecz obsługuje konwersję z CCSID 285 (jest to CHARNAME UK-ENGLISH dla SQL/DS).

  Jeśli requester aplikacji został zmieniony, tak aby mógł używać domyślnego CHARNAME równego UK-ENGLISH (i identyfikatora CCSID równego 285), to nie zostanie zachowana integralność danych. Jeśli serwer aplikacji chce

wyświetlić np. znak funta brytyjskiego (Ł), requester aplikacji wyświetla znak dolara amerykańskiego ($). Inne znaki także mogą się różnić.

Aby zmienić wartość CCSID dla requestera aplikacji DB2 for VM, należy nadać parametrowi CHARNAME wartość SQLINIT EXEC. Więcej informacji można znaleźć w podręczniku *DB2 for VM System Administration*.

Prawidłowa wartość CCSID dla serwera aplikacji może być jedną z wartości nie obsługiwanych przez tabele konwersji requestera aplikacji. W takim przypadku należy nawiązać połączenie, wykonując jedną z następujących czynności:

- Należy zaktualizować tabele konwersji CCSID requestera aplikacji, tak aby mogły obsługiwać konwersję między domyślnym CCSID serwera aplikacji i domyślnym CCSID requestera aplikacji. (Należy przeczytać podręczniki do produktów serwera aplikacji. Znajdują się w nich szczegółowe informacje dotyczące dodawania obsługi konwersji CCSID). Szczegółowe informacje na temat tabeli systemowej SYSTEM.SYSSTRINGS można znaleźć w podręczniku *DB2 for VM System Administration*. Tabela ta jest używana przy tworzeniu pliku CMS ARISSTR MACRO, który jest stosowany przez requester aplikacji do obsługi konwersji identyfikatorów CCSID.
- Należy zmienić domyślny identyfikator CCSID serwera aplikacji. Czynność ta powinna zostać wykonana, jeśli tylko jest to możliwe. Należy wziąć pod uwagę cele wybrania domyślnego identyfikatora CCSID serwera aplikacji. Domyślny identyfikator CCSID serwera aplikacji będzie miał wpływ na wszystkie requestery aplikacji połączone z nim, na terminal operatora używany z serwerem aplikacji i na dane przechowywane w tabelach na serwerze aplikacji.

Lista kontrolna włączania requestera aplikacji DRDA DB2 for VM

Poniższa lista kontrolna podsumowuje kroki niezbędne do włączenia komunikacji requestera aplikacji DRDA. Założono, że system VM został zainstalowany z ACF/VTAM jako metodą dostępu teleprzetwarzania oraz że definicje VTAM niezbędne do komunikacji z systemami zdalnymi, na przykład definicje NCP są pełne.

1. Należy zdefiniować lokalną bramę AVS do VTAM.
2. Należy zainstalować obsługę DRDA w requesterze aplikacji DB2 for VM, używając ARISDBMA exec.
3. Należy ustawić katalog komunikacyjny CMS i dodać wszystkie niezbędne instrukcje APPCPASS do katalogu VM na komputerze aplikacji. Aby włączyć katalog komunikacyjny, należy skorzystać z komendy SET COMDIR CMS.
4. Należy uruchomić VTAM i AVS, tak aby aplikacje VM mogły zdalnie komunikować się przez sieć SNA.
5. Należy uruchomić SQLINIT i podać parametry DBNAME, PROTOCOL i CHARNAME, aby wskazać domyślną bazę danych, protokół i identyfikatory CCSID, które będą używane.
6. Należy przygotować aplikacje na serwerze zdalnym.

Konfigurowanie requestera aplikacji w środowisku VM

Obsługa serwera aplikacji w DB2 for VM pozwala DB2 for VM działać jako serwer requesterów aplikacji DRDA. Requesterem aplikacji połączonym z serwerem aplikacji DB2 for VM może być:

- requester DB2 for VM,
- requester DB2 Universal Database for OS/390,
- requester OS/400,
- requester DB2 for AIX,
- dowolny requester aplikacji rodziny DB2, w tym także DB2 CONNECT lub dowolny inny produkt obsługujący protokoły requesterów aplikacji DRDA, mogących połączyć się z serwerem aplikacji DB2 for VM.

W przypadku każdego requestera aplikacji połączonego z serwerem aplikacji DB2 for VM serwer aplikacji DB2 for VM pozwala requesterowi aplikacji na dostęp do obiektów baz danych (np. tabel) przechowywanych lokalnie na serwerze aplikacji DB2 for VM. Przed zawiązaniem połączenia requester aplikacji musi utworzyć pakiet zawierający instrukcje aplikacji SQL na serwerze aplikacji.

Aby serwer aplikacji DB2 for VM przetworzył żądania rozproszonej bazy danych, należy:

1. Zdefiniować serwer aplikacji w lokalnym podsystemie komunikacji.
2. Udostępnić niezbędną ochronę.
3. Udostępnić reprezentację danych.

Dostarczanie informacji sieciowych

Definiowanie serwera aplikacji

Aby serwer aplikacji odbierał żądania rozproszonej bazy danych, należy zdefiniować serwer aplikacji w lokalnym podsystemie komunikacyjnym i przydzielić unikalną nazwę RDB_NAME.

Aby zdefiniować serwer aplikacji, należy:

1. Zdefiniować serwer aplikacji DB2 for VM w sieci SNA. Po wybraniu nazwy bramy i parametru RDB_NAME dla DB2 for VM Application Server należy postępować zgodnie z procedurami opisanymi w sekcji “Dostarczanie informacji sieciowych” na stronie 122. Nazwa RDB_NAME wybrana dla DB2 for VM musi być dostarczona do wszystkich użytkowników (requesterów aplikacji), którzy mogą wymagać połączenia z serwerem aplikacji DB2 for VM.

   Identyfikator NETID jest definiowany w VTAM jako parametr startowy i wszystkie rozproszone żądania z requestera aplikacji będą do niego poprawnie kierowane. Serwer aplikacji DB2 for VM nie ustawia identyfikatora NETID.

   Serwer aplikacji DB2 for VM nie określa, której bramy należy używać do kierowania rozproszonych żądań przychodzących z requestera aplikacji. Robi to

requester aplikacji. W przypadku requestera aplikacji DB2 for VM, CMS Communications Directory określa bramę za pomocą tokenów :luname i :tpn.

Aby serwer aplikacji DB2 for VM mógł obsługiwać działanie rozproszonej jednostki pracy, requester aplikacji musi wybrać bramę AVS, która została zdefiniowana w VTAM za pomocą parametru SYNCLVL=SYNCPT. Należy sprawdzić, czy brama AVS została zdefiniowana, tak aby mogła obsługiwać rozproszoną jednostkę pracy.

2. Utworzyć serwer odtwarzania CRR używany do zarządzania pracą rozproszonej jednostki pracy dla serwerów aplikacji DB2 for VM w systemie VM. Aby to zrobić, należy postępować zgodnie z instrukcjami poinstalacyjnego ładowania dostarczonych przez IBM serwerów i pul plików opisanych w podręczniku *VM/ESA Installation Guide*. W ich skład wchodzi definiowanie serwera CRR (VMSERVR) puli pliku CRR (VMSYSR). Należy sprawdzić, czy podczas uruchamiania serwera odtwarzania CRR nazwa LUNAME jest równa nazwie bramy AVS, dla której określono parametr SYNCLVL=SYNCPT.
3. Sprawdzić, czy katalog CP dla maszyny serwera aplikacji znajduje się instrukcja IUCV *IDENT. Identyfikuje ona serwer jako zasób globalny.
4. W przypadku każdej nazwy trybu żądanej przez requester aplikacji utworzyć pozycję w tabeli trybów VTAM. Niniejsze pozycje opisują charakterystyki sesji, takie jak wielkość RU, zliczanie pacingu i klasa usług dla danej nazwy trybu.
5. Zdefiniować limity sesji dla requesterów aplikacji, które łączą się z serwerem aplikacji DB2 for VM. Instrukcja VTAM APPL definiuje domyślne limity sesji dla wszystkich partnerskich systemów. Aby ustalić unikalne wartości domyślne dla określonego partnera, należy użyć komendy AGW CNOS z maszyny wirtualnej AVS działającej na serwerze aplikacji. (Requester aplikacji zwykle żąda określenia limitów sesji.)

   Po wybraniu wielkości RU, limitów sesji i zliczania pacingu należy rozważyć wpływ tych wartości na pulę IOBUF VTAM.

Odwzorowanie nazwy serwera na identyfikator RESID: ID zasobu (RESID) jest terminem systemu VM określającym nazwę programu transakcyjnego. W środowisku VM jest on zwykle definiowany jako nazwa alfanumeryczna o długości maksymalnie 8 bajtów. Aby ułatwić administrację, zwykle definiuje się RESID identyczny z nazwą serwera. Rys. 34 przedstawia przykładowy plik nazw RESID.
Rys. 33 na stronie 132 zawiera pozycję katalogu komunikacyjnego definiującą

```
  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
```

Rysunek 34. Przykład pliku nazw RESID

wymienione dbname i RESID (jako nazwy TPN). Jeśli nazwa serwera aplikacji nie

może być taka sama, jak RESID, przy wykonywaniu odwzorowania serwer aplikacji DB2 for VM korzysta z pliku RESID NAMES. Odwzorowanie jest niezbędne, gdy:

- używa się RESID innego niż nazwa serwera,
- używa się nazwy serwera dłuższej niż 8 bajtów,
- używa się RESID z 4-bajtową wartością szesnastkową, taką jak domyślny TPN DRDA X'07F6C4C2'.

Podczas instalacji domyślnie używa się nazwy serwera określonej w SQLDBINS EXEC jako RESID. Aby utworzyć pozycję odwzorowywania w pliku RESID NAMES, należy podać parametr RESID w SQLDBINS.

Jeśli baza danych zostanie uruchomiona przy użyciu SQLSTART DB(nazwa_serwera), DB2 for VM szuka odpowiedniego RESID i informuje VM, że jest to zasób, który będzie kontrolowany przez system VM. Jeśli pozycja nie zostanie odnaleziona w pliku RESID NAMES, DB2 for VM zakłada, że RESID jest identyczny z nazwą serwera i przekazuje tę informację systemowi VM. Więcej informacji można znaleźć w podręczniku *DB2 for VM System Administration*.

Przygotowywanie i uruchamianie serwera aplikacji DB2 for VM

Serwer aplikacji DB2 for VM może nie mieć zainstalowanej obsługi DRDA. Aby przygotować serwer aplikacji DB2 for VM do komunikacji DRDA, należy:

1. Użyć ARISDBMA do instalacji obsługi DRDA:
   - Użyć ″ARISDBMA DRDA(ARAS=Y)″, jeśli zainstalowana jest obsługa dla requestera i serwera.
   - Użyć ″ARISDBMA DRDA(AS=Y)″, jeśli zainstalowana jest obsługa tylko dla serwera.

   Szczegółowe informacje na ten temat można znaleźć w podręczniku *VM/ESA System Administration*.
2. Po wydaniu komendy ARISDBMA należy ponownie zbudować ARISQLLD LOADLIB DB2 for VM. Szczegółowe informacje na ten temat można znaleźć w rozdziale *Using a DRDA Environment* podręcznika *DB2 for VM System Administration*.

Zapewnianie ochrony

Gdy requester aplikacji wyznacza trasę żądania rozproszonej bazy danych do serwera aplikacji DB2 for VM, należy rozważyć następujące zagadnienia związane z ochroną:

- translacja przychodzących nazw użytkowników,
- parametry ochrony sieci,
- ochrona menedżera baz danych,
- ochrona wymuszona przez zewnętrzny podsystem ochrony.

Nazwy użytkowników

Zarówno w SQL, jak i w LU 6.2 użytkownicy otrzymują identyfikatory użytkowników o długości 1 do 8 znaków. Identyfikator użytkownika musi być unikalny w obrębie systemu operacyjnego, lecz nie musi być unikalny w całej sieci SNA. Aby wyeliminować konflikty nazw, DB2 for VM może opcjonalnie korzystać z funkcji translacji ID użytkowników dostarczanej przez AVS, lecz muszą być spełnione następujące warunki:

- Serwer aplikacji DB2 for VM musi działać w środowisku VM/ESA.
- Przychodzące żądania połączeń muszą być kierowane przez bramę AVS.
- Partner requestera aplikacji musi korzystać z parametru SECURITY=SAME (zwanego także *already veryfied (sprawdzony uprzednio)* w terminologii SNA).

Jeśli połączenie jest kierowane do serwera przez AVS przy użyciu opcji SECURITY=SAME, to wymagana jest translacja ID użytkownika AVS. Komenda AGW ADD USERID wydana z maszyny AVS musi udostępnić zerowanie ochrony w stosunku do łączących się użytkowników z określonej jednostki logicznej (LU) lub bramy AVS. Musi istnieć odwzorowanie dla wszystkich przychodzących jednostek logicznych (LU) i identyfikatorów użytkowników, którzy łączą się, używając SECURITY=SAME. Komenda jest elastyczna; można akceptować wszystkie identyfikatory użytkowników z danej jednostki logicznej lub ogólnie wszystkie jednostki logiczne. Można też akceptować jedynie określony zbiór identyfikatorów użytkowników z określonej jednostki logicznej.

Jeśli podczas autoryzacji przychodzących (uprzednio sprawdzonych) identyfikatorów użytkowników na lokalnej maszynie AVS korzysta się z komendy AGW ADD USERID, na hoście nie przeprowadza się żadnego sprawdzania poprawności. Oznacza to, że identyfikatory autoryzowanych użytkowników nie muszą istnieć na hoście, a połączenie i tak zostanie zaakceptowane.

Poniżej podano dwa sposoby zmiany bieżących autoryzacji AVS identyfikatora użytkownika:

- Należy zatrzymać AVS za pomocą komendy AGW STOP. Wszystkie autoryzacje ID użytkowników zostają wyzerowane.
- Należy usunąć ID użytkownika za pomocą komendy AGW DELETE USERID.

Przykład identycznych identyfikatorów użytkowników w różnych miastach przedstawia, w jaki sposób funkcja translacji AVS może rozstrzygać konflikt nazw. Załóżmy, że w systemie Toronto istnieje użytkownik o identyfikatorze JONES, a w systemie Montreal istnieje inny użytkownik o takim samym identyfikatorze. Jeśli JONES w systemie Montreal chce uzyskać dostęp do danych w systemie Toronto, to aby wyeliminować konflikt nazw i zapobiec użyciu przez użytkownika JONES w systemie Montreal uprawnień nadanych użytkownikowi JONES w systemie Toronto, należy wykonać następujące działania w systemie Toronto:

1. Operator AVS musi użyć komendy AGW ADD USERID do wykonania translacji identyfikatora użytkownika z Montrealu na lokalny identyfikator użytkownika. Na

przykład jeśli operator wydaje komendę AGW ADD USERID MTLGATE JONES MONTJON, użytkownik z Montrealu w systemie Toronto jest rozpoznawany jako MONTJON. Jeśli wszyscy użytkownicy z systemu Montreal mają pozwolenie na połączenie się (połączenie przez zdalną JEDNOSTKĘ LOGICZNĄ MTLGATE) i są lokalnie rozpoznawani za pomocą zdalnych identyfikatorów użytkowników, wówczas operator musi wydać komendę AGW ADD USERID MTLGATE * =. Te komendy AVS można także dodać do profilu AVS, tak aby automatycznie były wykonywane z chwilą uruchomienia AVS.

2. W tym szczególnym przypadku DBA musi użyć komendy GRANT DB2 FOR VM, aby nadać uprawnienia identyfikatorowi użytkownika MONTJON (po translacji).

Opisane działania można także wykonać w systemie Montreal, aby upewnić się, że użytkownik JONES w Toronto uzyskując dostęp do zdalnych danych w systemie Motreal nie korzysta z uprawnień nadanych użytkownikowi JONES w systemie Montreal.

Opis komend AVS obsługujących translację identyfikatorów użytkowników można znaleźć w podręczniku *VM/ESA Connectivity Planning, Administration and Operation*.

Ochrona sieci

Jednostka logiczna 6.2 udostępnia trzy główne opcje ochrony sieci:

- ochronę na poziomie sesji,
- ochronę na poziomie konwersacji,
- szyfrowanie.

Sposoby ochrony na poziomie sesji dla DB2 for VM opisano w sekcji “Ochrona sieci” na stronie 131. Serwer aplikacji DB2 for VM korzysta z ochrony na poziomie sesji w taki sam sposób, jak requester aplikacji DB2 for VM.

Requester aplikacji wysyła sprawdzony wcześniej identyfikator użytkownika (SECURITY=SAME) albo identyfikator użytkownika i hasło (SECURITY=PGM). Jeśli wysyłane są identyfikator użytkownika i hasło, program CP, RACF lub inny program tego typu sprawdza poprawność katalogu VM na hoście serwera aplikacji. Jeśli sprawdzanie poprawności nie powiodło się, żądanie jest odrzucane, w przeciwnym wypadku jest akceptowane. Jeśli żądanie zawiera tylko identyfikator użytkownika, DB2 for VM akceptuje żądanie bez sprawdzania poprawności identyfikatora użytkownika.

Uwaga: DB2 for VM nie umożliwia szyfrowania, ponieważ VM/ESA nie obsługuje szyfrowania.

Ochrona menedżera baz danych

Serwer aplikacji DB2 for VM sprawdza, czy identyfikator użytkownika określony przez VM ma uprawnienie CONNECT, aby uzyskać dostęp do bazy danych, a następnie odrzuca połączenie, jeśli nie ma ono uprawnień.

Jako właściciel zasobu bazy danych serwer aplikacji DB2 for VM steruje funkcjami ochrony bazy danych dla obiektów SQL znajdujących się na serwerze aplikacji DB2 for VM. Dostęp do obiektów zarządzanych przez VM jest sterowany za pomocą zbioru uprawnień, które są nadawane użytkownikom przez administratora systemu DB2 for VM lub właściciela określonego obiektu. Serwer aplikacji DB2 for VM steruje dwoma klasami obiektów:

- **Pakiety:** Użytkownicy indywidualni mają autoryzację do tworzenia, wymieniania i uruchamiania pakietów za pomocą instrukcji GRANT DB2 for VM. Gdy użytkownik tworzy pakiet, automatycznie zostają mu nadane autoryzacje do uruchamiania i wymieniania tego pakietu. Inni użytkownicy mający specjalne autoryzacje do uruchamiania pakietu na serwerze aplikacji DB2 for VM za pomocą instrukcji GRANT EXECUTE. Uprawnienie RUN można nadać użytkownikom indywidualnym lub wszystkim (PUBLIC), co umożliwia wszystkim użytkownikom uruchomienie pakietu.

  Gdy aplikacja jest przetwarzana wstępnie na DB2 for VM, pakiet zawiera instrukcje SQL znajdujące się w aplikacji. Instrukcje SQL są klasyfikowane jako:

  – **Statyczny SQL:** Oznacza to, że instrukcja SQL i obiekty SQL, do których odwołuje się instrukcja, są znane w czasie przetwarzania wstępnego aplikacji. Autor pakietu musi mieć uprawnienie do uruchamiania każdej statycznej instrukcji SQL w pakiecie.

    Gdy użytkownik otrzymuje uprawnienie do wykonywania pakietu, automatycznie uzyskuje uprawnienia do wykonywania każdej statycznej instrukcji SQL znajdującej się w tym pakiecie. Jeśli pakiet zawiera tylko statyczne instrukcje SQL, to użytkownicy nie muszą mieć żadnych uprawnień do tabeli DB2 for VM.

  – **Dynamiczny SQL:** Opisuje instrukcję SQL, która nie jest znana do chwili uruchomienia pakietu. Instrukcja SQL jest budowana przez program i dynamicznie przetwarzana wstępnie na DB2 for VM za pomocą instrukcji SQL PREPARE lub EXECUTE IMMEDIATE. Gdy użytkownik uruchamia dynamiczną instrukcję SQL, musi mieć uprawnienia do tabeli wymagane do uruchomienia instrukcji SQL. Ponieważ instrukcja SQL nie jest znana w momencie tworzenia pakietu, użytkownik nie otrzymuje automatycznie wymaganych uprawnień od właściciela pakietu.

- **Obiekty SQL:** Obiektami mogą być tabele, widoki i synonimy. Użytkownicy DB2 for VM mogą otrzymać różne poziomy uprawnień do tworzenia, usuwania, zmiany i czytania poszczególnych obiektów SQL. Uprawnienia te są wymagane do przetwarzania wstępnego statycznych instrukcji SQL lub uruchamiania dynamicznych instrukcji SQL.

Podsystem ochrony

Serwer aplikacji DB2 for VM korzysta z tego podsystemu opcjonalnie. Jeśli serwer aplikacji wymaga sprawdzenia tożsamości nazwy jednostki logicznej requestera aplikacji, to VTAM wywołuje podsystem ochrony w celu wymiany weryfikacji partnerskiej jednostki logicznej. Decyzja o weryfikacji jednostki logicznej podejmowana

jest w zależności od wartości określonej w parametrze VERIFY instrukcji APPL VTAM dla bramy, której serwer aplikacji DB2 for VM używa do odbierania przychodzących żądań rozproszonej bazy danych.

Podsystem ochrony wywoływany jest również przez CP w celu sprawdzenia poprawności ID użytkownika i hasła wysłanego z requestera aplikacji. Jeśli podsystemem ochrony jest RACF i brakuje profilu systemu RACF, to RACF przeprowadza sprawdzanie poprawności. Jeśli w systemie istnieje profil RACF, na przykład RACFPROF, aby zażądać sprawdzenia poprawności z RACF, należy użyć następujących instrukcji:

```
    RALTER VMXEVENT RACFPROF DELMEM (APPCPWVL/NOCTL

RALTER VMXEVENT RACFPROF ADDMEM (APPCPWVL/CTL

SETEVENT REFRESH RACFPROF
```

Reprezentacja danych

Do instalacji należy dobrać najodpowiedniejszy domyślny parametr CHARNAME i identyfikator CCSID. Używanie odpowiednich wartości zapewnia integralność reprezentacji danych znakowych i redukuje obciążenie wydajności związane z konwersją identyfikatorów CCSID.

Na przykład jeśli do serwera aplikacji DB2 for VM dostęp uzyskują tylko użytkownicy lokalni, których kontrolery terminali są generowane w stronie kodowej 37 i z zestawem znaków 697 (CP/CS 37/697), aby uzyskać znaki US ENGLISH, należy ustawić domyślną wartość CHARNAME serwera aplikacji na ENGLISH. Jest tak dlatego, że CP/CS 37/697 odpowiada identyfikatorowi CCSID równemu 37, który z kolei odpowiada wartości CHARNAME równej ENGLISH.

Aby wyeliminować zbędną konwersję CCSID, należy wybrać domyślny identyfikator CCSID użytkownika serwera aplikacji równy identyfikatorowi CCSID requestera aplikacji, który najczęściej uzyskuje dostęp do serwera aplikacji.

Poniższy przykład ilustruje konflikt obu wyżej wymienionych celów:

- Serwer aplikacji ma mniej niż pięć lokalnych requesterów aplikacji (dla requesterów aplikacji parametr protokołu byłby ustawiony na SQL/DS) i wiele (około 100) zdalnych requesterów aplikacji, które uzyskują dostęp do serwera aplikacji za pomocą protokołu DRDA. Lokalne requestery aplikacji mają sterowniki, które są zdefiniowane przy użyciu CP/CS 37/697. Zdalne requestery aplikacji korzystają z identyfikatora CCSID równego 285.

  Jeśli domyślnie CHARNAME serwera aplikacji ma wartość ENGLISH, utrzymuje to integralność danych dla lokalnych requesterów aplikacji, lecz powoduje zwiększenie kosztów wydajności na konwersję CCSID dla wszystkich zdalnych requesterów aplikacji.

  Jeśli domyślnie wartość CHARNAME serwera aplikacji jest ustawiona na UK_ENGLISH, pozwala to uniknąć nadmiernych kosztów wydajności na konwersję

CCSID ponoszonego przez wszystkie zdalne requestery, lecz powoduje problemy z integralnością danych lokalnych requesterów aplikacji. Pewne znaki nie są wyświetlane poprawnie na lokalnych requesterach aplikacji, na przykład brytyjski znak funta jest wyświetlany jako znak dolara.

Aby wyświetlić bieżący identyfikator CCSID systemu, należy wykonać zapytanie w tabeli SYSTEM.SYSOPTIONS. Domyślnym identyfikatorem CCSID serwera aplikacji jest zwykle wartość CCSIDMIXED. Jeśli wartość ta wynosi zero, domyślnym identyfikatorem CCSID jest wartość CCSIDSBCS. Wartości CHARNAME, CCSIDSBCS, CCSIDMIXED i CCSIDGRAPHIC w tej tabeli są aktualizowane do wartości używanych jako wartości domyślne systemu przy każdym uruchomieniu bazy danych. Wartości w tej tabeli nie muszą zawsze być równe domyślnym wartościom systemowym. Użytkownik z uprawnieniem DBA może zmienić te wartości, jednak nie jest to zalecane. Aby zmienić domyślny identyfikator CCSID serwera aplikacji, przy następnym uruchomieniu serwera aplikacji należy podać parametr CHARNAME równy SQLSTART EXEC. Bardziej szczegółowe informacje na ten temat znajdują się w podręczniku *VM/ESA System Administration*.

W przypadku nowo zainstalowanej bazy danych parametr CHARNAME serwera aplikacji ma wartość INTERNATIONAL, a domyślny identyfikator CCSID wynosi 500. Prawdopodobnie *nie* odpowiada to danemu systemowi. Domyślną wartością CHARNAME dla systemu migrowanego jest ENGLISH, a domyślny identyfikator CCSID wynosi 37.

Lista kontrolna włączania serwera aplikacji DB2 for VM DRDA

Poniższa lista kontrolna podsumowuje kroki niezbędne do włączenia serwera aplikacji DRDA do komunikacji DRDA. Przyjęto założenie, że system VM jest zainstalowany z ACF/VTAM jako metodą dostępu teleprzetwarzania i wprowadzono wszystkie definicje VTAM niezbędne do komunikacji z systemami zdalnymi, na przykład definicje NCP.

1. Należy zdefiniować lokalną bramę AVS do VTAM.
2. Należy utworzyć CRR Recovery Server. Należy upewnić się, że LUNAME określona przez CRR Recovery Server odpowiada nazwie bramy AVS, która może obsłużyć konwersacje SYNCLVL=SYNCPNT.
3. Należy zainstalować obsługę DRDA na serwerze aplikacji DB2 for VM, używając ARISDBMA exec.
4. Należy podać instrukcję IUCV *IDENT do katalogu CP na serwerze VM, tak aby mógł zidentyfikować siebie jako zasób globalny.
5. Należy zdefiniować identyfikatory i hasła w CP, które zostaną użyte przez zdalne requestery aplikacji. Jeśli to konieczne, należy odwzorować dowolne identyfikatory użytkowników zdalnych na lokalne identyfikatory użytkowników, używając komendy AVS AGW ADD USERID.
6. W przypadku każdego trybu, którego zażąda requester aplikacji, należy utworzyć pozycję w tabeli nazw trybów VTAM.

7. Należy uruchomić VTAM i AVS, tak aby aplikacje VM mogły zdalnie komunikować się przez sieć SNA.
8. Należy ustalić limity sesji dla wszystkich systemów partnerskich, na których znajdują się requestery aplikacji.
9. Należy uruchomić serwer aplikacji DB2 for VM z parametrami DBNAME, PROTOCOL i SYNCPNT. Gdy menedżer baz danych zostanie uruchomiony, należy się upewnić, że zidentyfikował sam siebie jako zasób GLOBAL.
10. Należy przygotować aplikacje na serwerze aplikacji DB2 for VM.

Omówienie DB2 for VSE

W środowisku VSE/ESA DB2 for VSE obsługuje funkcje serwera aplikacji środowiska DRDA. Funkcja requestera aplikacji nie jest obsługiwana. W sekcji tej opisano różne komponenty DB2 for VSE i VSE wykorzystywane przy przetwarzaniu rozproszonych baz danych. Komponenty te umożliwiają systemowi zarządzania bazą danych DB2 for VSE komunikowanie się ze zdalnymi requesterami aplikacji w sieci SNA.

CICS(ISC)
Komponent komunikacji między systemami Customer Information Control System (CICS) dostarcza funkcje SNA LU 6.2 (APPC) do serwera aplikacji DB2 for VSE.

CICS(SPM)
Komponent zarządzania punktem synchronizacji CICS jest składnikiem obsługi rozproszonej jednostki pracy DRDA DB2 for VSE. Działa on jak uczestnik punktu synchronizacji i jest odpowiedzialny za koordynację zatwierdzania dwufazowego w systemie VSE/ESA.

CICS(TRUE)
Procedura użytkownika związana z zadaniem CICS jest interfejsem używanym przez transakcję AXE w celu połączenia z menedżerem punktu synchronizacji CICS.

ACF/VTAM
W celu uruchomienia lub powiązania sesji typu LU-LU z systemami zdalnymi CICS(ISC) korzysta z VTAM for VSE. DB2 for VSE używa podstawowej konwersacji jednostki logicznej 6.2 tych sesji, aby komunikować się ze zdalnymi requesterami aplikacji DRDA.

AXE Transakcja APPC-XPCC-Exchange jest transakcją CICS uaktywnianą przez zdalny requester aplikacji DRDA. Kieruje ona wymianą strumieni danych DRDA między zdalnym requesterem aplikacji a serwerem aplikacji DB2 for VSE korzystającym z obsługi jednostki logicznej LU 6.2 CICS i funkcji XPCC VSE.

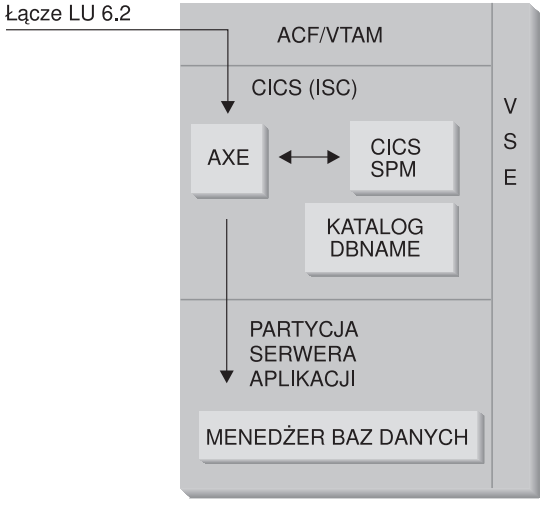
katalog DBNAME
Katalog DBNAME (nazw baz danych) odwzorowuje przychodzące żądania przydzielenia konwersacji do odpowiedniego serwera aplikacji

identyfikowanego przez przychodzącą nazwę programu transakcyjnego. Więcej szczegółowych informacji na ten temat można znaleźć w podręczniku *SQL/DS System Administration Guide for VSE*.

XPCC Cross Partition Communication Control (Kontrola komunikacji między partycjami) jest interfejsem typu makro VSE, który obsługuje transfer danych między partycjami VSE.

Przykład przepływu komunikacji dla serwera aplikacji

Rys. 35 przedstawia rolę każdego z komponentów w nawiązaniu komunikacji między serwerem aplikacji DB2 for VSE a zdalnym requesterem aplikacji.



Rysunek 35. Uzyskiwanie dostępu do serwera aplikacji

Requester aplikacji wysyła komendę APPC ALLOCATE wraz z konkretną nazwą jednostki logicznej i nazwą programu transakcyjnego w celu nawiązania konwersacji jednostki logicznej LU 6.2 z serwerem aplikacji. Nazwa LU jest używana do skierowania żądania ALLOCATE przez VTAM do CICS. Po otrzymaniu komendy ALLOCATE, CICS sprawdza, czy transakcja AXE jest zdefiniowana dla tej nazwy programu transakcyjnego (TPN) i wpisuje się do CICS. Jeśli poziomem ochrony konwersacji dla połączenia CICS jest VERIFY, z requestera aplikacji ma zostać przekazany zarówno identyfikator użytkownika, jak i hasło. Są one używane przy wpisywaniu się do systemu. Aby połączenie zostało zaakceptowane, tabela wpisywania do systemu CICS (DFHSNT) musi być aktualizowana przy użyciu tego identyfikatora użytkownika i hasła. Jeśli poziom ochrony jest ustawiony na IDENTIFY, wymagany jest tylko identyfikator użytkownika i CICS powierza sprawdzanie uprawnień systemowi

zdalnemu. Jeśli kontrola powiodła się, CICS uruchamia transakcję AXE, która przekierowuje żądania i odpowiedzi wymieniane między requesterem aplikacji i serwerem aplikacji. Nazwa TPN używana przez requester aplikacji również musi mieć zdefiniowaną w katalogu DBNAME DB2 for VSE pozycję, która wskazuje serwer DB2 for VSE w systemie VSE.

Jeśli requester aplikacji chce skorzystać z obsługi rozproszonej jednostki pracy, podaje w APPC ALLOCATE wartość SYNCPT jako wartość parametru SYNCLVL. Po uruchomieniu transakcji AXE pobiera on z CICS wartość SYNCLVL dla konwersacji. Jeśli jest to SYNCPT, wykonuje następujące czynności:

- Jeśli to konieczne, transakcja AXE umożliwia obsługę typu TRUE, tak aby mogła ona komunikować się z menedżerem punktu synchronizacji CICS.
- Zapisuje logiczną jednostkę pracy przy użyciu menedżera punktu synchronizacji CICS.

Ograniczenia

W przeciwieństwie do swojej kopii działającej w VM, serwer aplikacji DB2 for VSE przyjmuje przepływy DRDA ze zdalnych requesterów aplikacji. Prywatne protokoły nie są obsługiwane. W rezultacie żądania aplikacji VM nie mogą korzystać z serwera VSE dla PROTOCOL=SQLDS.

Serwer DRDA DB2 for VSE nie może kierować żądań ze zdalnych requesterów aplikacji do serwera DB2 for VM przy użyciu współużytkowania dla gościa VSE. Takie żądania powinny być wysyłane bezpośrednio do serwera DRDA VM.

Parametry uruchamiania serwera aplikacji

Parametr RMTUSERS

Administrator baz danych może podczas uruchamiania serwera aplikacji podać parametr RMTUSERS, aby ustawić maksymalną liczbę zdalnych requesterów aplikacji, które mogą łączyć się z serwerem. Jest on podobny do wartości MAXCONN w katalogu VM na serwerze baz danych DB2 for VM. Pomaga zrównoważyć obciążenie między przetwarzaniem lokalnym i zdalnym.

Jeśli wartość RMTUSERS jest większa niż liczba dostępnych agentów DB2 for VSE (zdefiniowanych przez NCUSER), niektórzy użytkownicy zdalni muszą czekać na dostęp do agenta, aby spełnił ich żądania. Zwykle agent DB2 for VSE jest przypisywany ponownie do oczekującego użytkownika na końcu logicznej jednostki pracy (LUW). Serwer aplikacji DB2 for VSE obsługuje uprawniony dostęp, który umożliwia użytkownikom zdalnym utrzymanie agenta DB2 for VSE dla wielu LUW do końca konwersacji.

Parametr SYNCPNT

Parametr ten określa, czy menedżer punktu synchronizacji (SPM) zostanie użyty do koordynacji działania rozproszonej jednostki pracy podczas odczytu z wielopunktowego DRDA-2 i zapisu wielopunktowego.

Jeśli określona jest wartość Y, serwer, jeśli to jest możliwe, użyje menedżera punktu synchronizacji, aby koordynować zatwierdzanie dwufazowe i resynchronizację. Jeśli określona jest wartość N, serwer aplikacji nie będzie używał SPM w celu wykonania zatwierdzania dwufazowego. W takim przypadku serwer aplikacji ogranicza rozproszone jednostki pracy wykonujące odczyt i zapis wielopunktowy i może pozostać jedynie zapis dla jednego miejsca. Jeśli określona jest wartość Y, lecz serwer aplikacji stwierdzi, że menedżer punktu synchronizacji jest niedostępny, serwer będzie działał, tak jakby określona była wartość N.

Jeśli RMTUSERS jest większe od zera, wartością domyślną jest SYNCPNT=Y. Jeśli RMTUSERS=0, parametr SYNCPNT jest ustawiony na N.

Konfigurowanie serwera aplikacji w środowisku VSE

Obsługa serwera aplikacji dla DB2 for VSE umożliwia DB2 for VSE działanie jako serwer dla requesterów aplikacji DRDA. Requesterem aplikacji połączonym z serwerem aplikacji VSE może być:

- requester DB2 for VM,
- requester DB2 Universal Database for OS/390,
- requester DB2,
- requester OS/400,
- dowolny requester aplikacji z rodziny DB2 w tym także DB2 CONNECT lub dowolny inny produkt, który obsługuje protokoły requestera aplikacji DRDA mogący połączyć się z serwerem aplikacji DB2 for VSE.

Dostarczanie informacji sieciowych

Aby nawiązać połączenie sieciowe z serwerem aplikacji VSE, należy wykonać następujące czynności:

1. Uruchomić sesje CICS LU 6.2 z systemami zdalnymi.
2. Zdefiniować serwer aplikacji.

Uruchamianie sesji LU 6.2 CICS

Serwer aplikacji DB2 for VSE komunikuje się z requesterem aplikacji przez połączenia LU 6.2 CICS. Partycja CICS użyta w tym celu musi mieć połączenia jednostki logicznej (LU) 6.2 z systemami zdalnymi z aktywnymi requesterami aplikacji. Szczegółowe informacje dotyczące definiowania i nawiązywania połączeń LU 6.2 CICS z systemami zdalnymi można znaleźć w podręczniku *CICS/VSE Intercommunications Guide*.

Instalowanie i definiowanie zasobów CICS dla komunikacji LU 6.2:

1. Należy zainstalować moduły wymagane dla ISC.

   Do systemu należy włączyć następujące moduły, korzystając z tabeli inicjowania systemu (SIT) lub nadpisań inicjowania:

   - Programy interfejsu EXEC (należy podać EXEC=YES lub zostawić wartość domyślną).
   - Programy komunikacji między systemami (należy podać ISC=YES).
   - Program sterowania terminalem wygenerowany przez DFHSG PROGRAM=TCP. Wymagane jest podanie wersji ACCMETH=VTAM, CHNASSY=YES i VTAMDEV=LUTYPE6.

2. Należy zainstalować CICS Restart Resynchronization Support (obsługę resynchronizacji ponownego uruchomienia CICS).

   Jeśli podczas instalowania systemu CICS nie wyrażono zgody na użycie CICS Restart Resynchronization Support (obsługi resynchronizacji ponownego uruchomienia CICS), należy zaktualizować następujące tabele CICS, aby umożliwić użycie narzędzia obsługującego resynchronizację ponownego uruchomienia CICS:

   ```
   DFHJCT    Tabela kontrolna kroniki

             Kronika wykorzystywana przez protokół systemowy CICS musi
             zostać zdefiniowana w DFHJCT przez podanie frazy
             JFILEID=SYSTEM w makrze DFHJCT TYPE=ENTRY.

   DFHPCT    Tabela kontrolna programu

             Aby utworzyć pozycję DFHPCT w celu użycia CICS Restart
             Resynchronization, wpisz:

                 DFHPCT TYPE=GROUP,FN=RMI

   DFHPPT    Tabela programu przetwarzania

             Aby utworzyć pozycję DFHPPT w celu użycia CICS Restart
             Resynchronization, wpisz:

                 DFHPPT TYPE=GROUP,FN=RMI

   DFHSIT    Tabela inicjowania systemu

             Makro DFHSIT musi zawierać parametr JCT.
             Określ JCT=YES lub JCT=(jj<,....>) , gdzie jj jest
             wartością parametru SUFFIX podanego w makrze th DFHJCT
             TYPE=INITIAL definiującym zestaw danych kroniki protokołu systemowego CIC
   ```

3. Należy zdefiniować CICS dla VTAM for VSE.

   W celu obsługi połączeń LU 6.2 należy zdefiniować CICS w produkcie VTAM for VSE jako główny węzeł aplikacji VTAM. Nazwa głównego węzła zakodowana w instrukcji APPL VTAM jest identyfikatorem APPLID partycji CICS podanej w SIT przez parametr APPLID. Jest to nazwa jednostki logicznej używanej przez VTAM (a więc przez partnerów komunikacji CICS) w celu identyfikacji systemu CICS.

Patrz Rys. 36.

```
                    VBUILD TYPE=APPL
*********************************************************************
*                                                                   *
*    LU Definition for Toronto VSE SQL/DS System                    *
*                                                                   *
*********************************************************************
VSEGATE  APPL  ACBNAME=VSEGATE,
               AUTH=(ACQ,SPO,VPACE),
               APPC=NO,
               SONSCIP=YES,
ESA=30
               MODTAB=RDBMODES,
               PARSESS=YES,
               VPACING=0
```

Rysunek 36. Przykładowa definicja APPL VTAM dla CICS

AUTH=(ACQ,SPO,VPACE)
ACQ umożliwia CICS uzyskanie sesji LU 6.2.

SPO umożliwia CICS wprowadzenie komendy MODIFY vtamname USERVAR.

VPACE umożliwia pacing przepływu danych między systemami.

ESA=30
Opcja ta podaje liczbę jednostek adresowanych w sieci, z którymi CICS może uruchomić sesje. Liczba odzwierciedla całkowitą liczbę sesji równoległych dla tego systemu CICS.

PARSESS=YES
Określa obsługę sesji równoległej LUTYPE6.

SONSCIP=YES
Określa obsługę SON (session outage notification). Obsługa SON umożliwia CICS odzyskanie w niektórych przypadkach błędnej sesji bez konieczności interwencji operatora.

APPC=NO
Jest niezbędna do wykorzystywania przez CICS makr VTAM. CICS nie obsługuje makroinstrukcji APPCCMD.

Uwaga: Określenie SYNCLVL=SYNCPT nie jest konieczne, ponieważ zostało wprowadzone APPC=NO. CICS zarządza wszystkimi działaniami związanymi z punktem synchronizacji SYNCPT dla rozproszonych jednostek pracy.

4. Należy zdefiniować połączenia z systemami zdalnymi używającymi protokołu LU 6.2.

a. Należy zdefiniować w CICS wszystkie zdalne jednostki logiczne.

   Aby zdefiniować wszystkie zdalne jednostki logiczne przy użyciu komendy CONNECTION w RDO (bezpośrednie definiowanie zasobów), należy:

   - Podać nazwę jednostki logicznej w parametrze NETNAME.
   - Podać PROTOCOL=APPC, aby zapewnić używanie protokołów LU6.2.
   - Podać AUTOCONNECT=YES i INSERVICE=YES, tak aby połączenie po zainstalowaniu zostało uaktywnione automatycznie i aby sesje rozpoczęły się automatycznie.
   - Podać ochronę na poziome konwersacji, używając parametru ATTACHSEC. ATTACHSEC=IDENTIFY jest minimalnym poziomem ochrony wymaganym przez DRDA.
   - Podać ochronę na poziomie sesji, używając parametru BINDPASSWORD. Wartością domyślną jest brak ochrony na poziomie sesji.

   Więcej informacji na temat konwersji i ochrony na poziomie sesji można znaleźć w sekcji “Zapewnianie ochrony” na stronie 153.

b. Należy zdefiniować grupy sesji LU 6.2 z systemem zdalnym.

   W przypadku każdego zdefiniowanego powyżej połączenia należy zdefiniować grupy sesji równoległych dla każdego połączenia ze zdalną jednostką logiczną przy użyciu komendy CEDA DEFINE SESSIONS:

   - Podać nazwę połączenia (zdefiniowaną powyżej) w parametrze CONNECTION.
   - Podać pozycję tabeli logmode VTAM w parametrze MODENAME.
   - Podać parametr MAXIMUM w celu określenia:
     – maksymalnej liczby sesji,
     – maksymalnej liczby sesji, które mają być obsługiwane jako zwycięzcy rywalizacji.

     Podać wartości używane przez oprogramowanie komunikacyjne requestera aplikacji DRDA, na przykład IBM Communications Server for OS/2.

   Należy zauważyć, że określenie większej wartości SENDSize i RECEIVESize może przyspieszyć transmisję danych, choć w sieci będzie potrzebna większa pamięć wirtualna. 4 kilobajty to wielkość, którą obsługują wszystkie warstwy sieci SNA. Podczas konfigurowania serwera DRDA należy ustawić wielkości buforu wysyłania i odbierania na 4 kilobajty. Podczas nawiązywania połączeń przez użytkowników zdalnych można zoptymalizować oba parametry.

c. Należy zdefiniować identyfikatory użytkowników i hasła dla CICS.

   Należy zdefiniować wszystkich użytkowników w tabeli wpisywania do systemu CICS (DFHSNT). Można sprawdzić poprawność identyfikatorów użytkowników, wykonując komendę logon CESN na terminalu CICS. Lokalne wpisanie do systemu musi się powieść.

d. Należy zdefiniować moduły logowania (fazy) w CICS przy użyciu komendy CEDA DEFINE PROGRAM:

   1) ARICAXED - transakcja AXE,
   2) ARICDIRD - katalog DBNAME i procedura wyszukiwania,
   3) ARICDAXD - program obsługi transakcji DAXP i DAXT,
   4) ARICDEBD - CICS TRUE program obsługi uaktywniania,
   5) ARICDRAD - samo CICS TRUE,
   6) ARICDR2 - blok sterujący DR2DFLT.

   W przypadku każdego z nich powinna zostać określona opcja LANGUAGE=ASSEMBLER.

e. W przypadku każdej nazwy TPN określonej przez requester aplikacji należy zdefiniować transakcję AXE, używając komendy CEDA DEFINE TRANSACTION:

   - Należy użyć parametru TRANSACTION, aby podać nazwę TPN.
   - Należy podać PROGRAM=ARICAXED, aby określić fazę.
   - Należy użyć parametru XTRANID, aby podać drugą szesnastkową nazwę transakcji.

   W tym czasie zdefiniuj również transakcje DAXP i DAXT, podając PROGRAM=ARICDAXD.

Przykładowe definicje: Przykładowe definicje znajdują się w podręczniku *DRDA Connectivity Guide*.

Definiowanie serwera aplikacji

1. Należy zaktualizować katalog DBNAME w DB2 for VSE.

   Do katalogu DBNAME należy dodać pozycję dla każdej transakcji zdefiniowanej powyżej przy użyciu komendy CEDA DEFINE TRANSACTION. Gdy sesje jednostki logicznej 6.2 (LU 6.2) zostaną uruchomione, zdalny requester aplikacji może rozpocząć konwersację z serwerem aplikacji DB2 for VSE. Przydziela on konwersację jednostki logicznej 6.2 (LU 6.2) z serwerem aplikacji, podając nazwę programu transakcyjnego (TPN). Nazwa ta musi być identyfikatorem transakcji CICS dla transakcji AXE odpowiedzialnej za kierowanie żądań do lub z serwera DB2 for VSE. Nazwa programu transakcyjnego musi znajdować się w katalogu DBNAME produktu DB2 for VSE odwzorowanym na serwer DB2 for VSE, tak aby requester aplikacji mógł mieć do niej dostęp. Administrator bazy danych DB2 for VSE jest odpowiedzialny za aktualizację katalogu DBNAME i poinformowanie użytkowników zdalnych o odwzorowaniu TPN-serwer.

   Nazwa TPN i odpowiadająca jej nazwa serwera (nazwa bazy danych, jak to zdefiniowano w katalogu DBNAME) muszą być zidentyfikowane w requesterze aplikacji.

   - Requester aplikacji używa nazwy TPN do zainicjowania transakcji routera AXE.

- Requester aplikacji odwołuje się do nazwy serwera w początkowym przepływie DRDA jako do nazwy docelowej bazy danych. Serwer DB2 for VSE używa tej nazwy serwera do sprawdzenia, czy requester aplikacji uzyskuje dostęp do właściwego serwera. Niezgodność nazwy serwera uniemożliwia requesterowi aplikacji dostęp do serwera i requester aplikacji kończy konwersację.

2. Do utworzenia i skonsolidowania katalogu DBNAME (element ARISDIRD.A) należy użyć procedury ARISBDID.

Więcej informacji na ten temat można znaleźć w podręczniku *DB2 for VSE System Administration*.

Przygotowywanie i uruchamianie serwera DB2 for VSE Application Server

1. Transakcja AXE obsługuje protokół błędów, który jest kolejką pamięci tymczasowej CICS o nazwie ARIAXELG. Ten protokół błędów zawiera użyteczne komunikaty o błędach, zarejestrowane podczas występowania problemów z komunikacją i nieprawidłowego zakończenia sesji DRDA. Protokół ten należy zdefiniować jako "odtwarzalny" przy użyciu TST CICS.
2. Należy uruchomić procedurę ARIS342D, aby zainstalować obsługę serwera aplikacji DRDA.
3. Jeśli to konieczne, należy wykonać transakcję DAXP, aby podać domyślne hasło i język, które będą używane po włączeniu obsługi CICS TRUE dla konkretnego systemu. Dodatkowe informacje znajdują się w podręczniku *DB2 for VSE Operation*.
4. Należy uruchomić DB2 for VSE z parametrami DBNAME, RMTUSERS i SYNCPNT:
   - Używany parametr DBNAME musi być zdefiniowany w katalogu DBNAME.
   - Parametr RMTUSERS musi mieć wartość różną od zera.
   - Należy podać SYNCPNT=Y, aby udostępnić obsługę rozproszonej jednostki pracy.
5. Wszyscy użytkownicy zdalni muszą mieć nadane przez serwer DB2 for VSE autoryzacje o różnych poziomach. Dodatkowe informacje można znaleźć w podręczniku *DB2 for VSE Database Administration*.

Określanie problemów:

- Jeśli requester aplikacji zdołał nawiązać komunikację z partnerską jednostką CICS z poprawną nazwą TPN (nazwa TPN jest zdefiniowana w katalogu DBNAME), uruchamiana jest transakcja AXE. Licznik użytkowników programu ARICAXED jest zwiększany o jeden (sprawdzany przez uruchomienie CEMT I PR(ARICAXED)).
- Aby upewnić się, że ID zdalnego użytkownika jest ustanowiony w tabeli wpisania się do systemu programu CICS, należy lokalnie wpisać się do systemu przy użyciu

transakcji CESN z hasłem i ID zdalnego użytkownika. Lokalne wpisanie do systemu musi się powieść.

- Jeśli serwer DB2 for VSE działa i aplikacja po raz pierwszy wykonuje czynności rozproszonej jednostki pracy DRDA-2, obsługa TRUE dla serwera będzie udostępniona automatycznie. Komunikat ARI0187I oznacza pomyślne udostępnienie obsługi TRUE. Jeśli jednak pojawi się komunikat ARI0190E oznaczający wystąpienie błędu podczas udostępniania obsługi TRUE, należy przejrzeć na konsoli wcześniejsze komunikaty o błędach.
- Jeśli program DRDA odbierze kod rozpoznania X'08063426' lub X'FFFE0101', może to oznaczać, że CICS nie może udostępnić więcej sesji; np. gdy wszystkie sesje są używane albo przeznaczone do zwolnienia, ale wykonywanie UNBIND jeszcze się nie zakończyło. CICS nie może udostępnić więcej sesji, jeśli występuje wiele jednoczesnych transakcji przychodzących, które trwają krótko. W takim przypadku należy zwiększyć liczbę sesji określoną w parametrze komendy MAXIMUM CEDA DEFINE SESSION, aby obliczyć liczbę sesji przeznaczonych do zwolnienia (przy użyciu UNBIND), ale wykonanie UNBIND jeszcze się nie zakończyło.

Zapewnianie ochrony

Ochrona komunikacji międzysystemowej na serwerze aplikacji DB2 for VSE zależy od programu CICS. CICS udostępnia kilka poziomów ochrony:

- Ochrona typu bind-time.

  Implementacja CICS sprawdzania typu LU-LU na poziomie sesji jednostki logicznej LU 6.2 SNA. W architekturze LU 6.2 implementacja ochrony typu bind-time jest opcjonalna. Można ją udostępnić po stronie serwera aplikacji, podając BINDPASSWORD w komendzie CEDA DEFINE CONNECTION podczas definiowania połączenia z requesterem aplikacji. W requesterze aplikacji partnerska jednostka logiczna obsługująca go musi również zapewnić ochronę typu bind-time i używać tego samego hasła do sprawdzenia partnerskiej jednostki logicznej.

  Można użyć ochrony typu bind-time, aby uniemożliwić nieautoryzowanym systemom zdalnym uruchomienie (powiązanie) sesji z CICS.

- Ochrona połączenia.

  Ochrony połączenia można użyć, aby ograniczyć systemowi zdalnemu (i jego rezydentnym requesterom aplikacji DRDA) podłączanie tylko niektórych zestawów transakcji AXE.

  Można na przykład zdefiniować dwie transakcje AXE: AXE2 z kluczem ochrony 2 i AXE3 z kluczem ochrony 3. Requesterom aplikacji z systemu zdalnego można przypisać operator ochrony 3 (na przykład za pomocą parametru OPERSECURITY w komendzie CEDA DEFINE SESSION), pozwalając im na podłączenie tylko

transakcji AXE3. Transakcja AXE3 może nie mieć uprawnień dostępu do serwera, podczas gdy transakcja AXE2 może mieć takie uprawnienia. Opis uprawnień dostępu do serwera aplikacji dla zdalnych requesterów aplikacji można znaleźć w podręczniku *DB2 for VSE System Administration*.

Informacje na temat sposobu udostępnienia ochrony połączenia można znaleźć w podręczniku *CICS Intercommunication Guide*.

- Ochrona użytkownika.

  Implementacja CICS ochrony na poziomie konwersacji jednostki logicznej LU 6.2 SNA udostępnia sprawdzanie użytkownika.

  Ochrona użytkownika sprawdza poprawność ID użytkownika w tabeli CICS wpisania się do systemu (DFHSNT) przed zaakceptowaniem uruchomienia konwersacji przez żądanie. Na przykład requestery aplikacji DRDA nie zdefiniowane w tabeli programu CICS wpisania się do systemu nie mogą podłączać transakcji AXE, aby rozpocząć konwersację z serwerem DB2 for VSE. Poziom ochrony użytkownika dla zdalnego systemu można wybrać przez użycie parametru ATTACHSEC komendy CEDA DEFINE CONNECTION. Oto trzy poziomy ochrony podłączenia:

  – LOCAL. Poziom nie obsługiwany przez DRDA.
  – IDENTIFY. Odpowiednik SECURITY=SAME (lub uprzednio zweryfikowano) w terminologii jednostki LU 6.2. W przypadku tego poziomu ochrony CICS "ufa" systemowi zdalnemu, że sprawdzi on swoich użytkowników, zanim pozwoli im przydzielić konwersację z serwerem DB2 for VSE. W procesie wpisania się do systemu CICS wymagany jest tylko ID użytkownika. Jeśli jednak przekazywane jest również hasło, to CICS wykonuje wpisanie się do systemu z hasłem.
  – VERIFY. Odpowiednik SECURITY=PGM w terminologii jednostki LU 6.2. W przypadku tego poziomu ochrony CICS oczekuje od zdalnego systemu, że nadeśle on zarówno ID, jak i hasło użytkownika podczas przydzielania konwersacji i odrzuci połączenie, jeśli hasło nie zostało nadesłane.

- Obowiązkowa kryptografia na poziomie sesji jednostki logicznej LU 6.2 SNA nie jest obsługiwana.

Ponieważ serwer aplikacji jest odpowiedzialny za zarządzanie zasobami baz danych, narzuca on mechanizmy ochrony sieci, które musi udostępnić requester aplikacji. Na przykład w przypadku serwera aplikacji DB2 for VM należy zapisać wymagania dotyczące ochrony na poziomie konwersacji serwera aplikacji w katalogu komunikacji requestera aplikacji, ustawiając odpowiednią wartość w katalogu :security, co przedstawiono na Rys. 37 na stronie 155:

```
:nick.VSE1     :tpn.TOR3
               :luname.TORGATE VSEGATE
               :modename.IBMRDB
               :security.PGM
               :userid.SALESMGR
               :password.PROFIT
               :dbname.TORONTO3



Gdzie: TOR3    - Identyfikator transakcji AXE odwzorowany na bazę danych TORONTO3.
       TORGATE - Brama VM/APPC.
       VSEGATE - Identyfikator APPLID partycji CICS/VSE wykorzystywany jako brama
                 do TORONTO3.
       SALESMGR/PROFIT - USERID/PASSWORD zdefiniowane w DFHSNT z
                         VSEGATE i autoryzowane w TORONTO3
       TORONTO3 - Nazwa określona w parametrze uruchomienia DBNAME, gdy
                  serwer aplikacji DB2 for VSE został uruchomiony (lub
                  nazwa domyślnej bazy danych określona przez katalog DBNAME,
                  jeśli DBNAME została pominięta przy uruchomieniu).
```

Rysunek 37. Przykładowa pozycja katalogu CMS Communication Directory

Ochrona menedżera baz danych

Translacja ID użytkownika nie jest obsługiwana przez serwer aplikacji VSE. CICS używa ID użytkownika przesłanego bezpośrednio z requestera.

Transakcja AXE po uruchomieniu przez requester aplikacji pobiera ID użytkownika z CICS i przesyła go do serwera DB2 for VSE. Aby ustawić wymagany poziom uprawnień użytkownika do zasobów bazy danych, należy zaktualizować ID użytkownika w katalogu SYSTEM.SYSUSERAUTH produktu DB2 for VSE.

Serwer aplikacji DB2 for VSE sprawdza, czy ID użytkownika określony przez CICS ma uprawnienia CONNECT dostępu do bazy danych i odrzuca połączenie, jeśli użytkownik nie ma właściwych uprawnień.

Jako właściciel zasobów bazy danych serwera aplikacji DB2 for VSE steruje funkcjami ochrony bazy danych dla obiektów SQL rezydujących na serwerze aplikacji DB2 for VSE. Dostęp do obiektów zarządzanych przez DB2 for VSE jest realizowany przez zestaw uprawnień, które są nadawane użytkownikom przez administratora systemu DB2 for VSE lub właściciela konkretnego obiektu. Serwer aplikacji DB2 for VSE kontroluje dwie klasy obiektów:

- **Pakiety:** Użytkownicy indywidualni mają autoryzację do tworzenia, wymiany i uruchamiania pakietów przy użyciu instrukcji GRANT w systemie DB2 for VSE. Gdy użytkownik tworzy pakiet, automatycznie zostaje autoryzowany do uruchamiania i wymieniania tego pakietu. Inni użytkownicy muszą zostać specjalne autoryzowani do uruchamiania pakietu na serwerze aplikacji DB2 for VSE za pomocą

instrukcji GRANT EXECUTE. Uprawnienie RUN można nadawać użytkownikom indywidualnym lub wszystkim (PUBLIC), co umożliwia wszystkim użytkownikom uruchomienie pakietu.

Gdy aplikacja jest wstępnie przetwarzana w DB2 for VSE, pakiet zawiera instrukcje SQL znajdujące się w programie. Instrukcje SQL są klasyfikowane jako:

– **Statyczny SQL:** Oznacza to, że instrukcja SQL i obiekty SQL, do których odwołuje się instrukcja, są znane w czasie wstępnego przetwarzania aplikacji. Autor pakietu musi mieć uprawnienia do uruchamiania każdej statycznej instrukcji SQL w pakiecie.

  Gdy użytkownikowi nadano uprawnienia do wykonywania pakietu, automatycznie nadano mu uprawnienia do wykonywania każdej statycznej instrukcji SQL znajdującej się w pakiecie. W ten sposób użytkownicy nie potrzebują żadnych uprawnień do tabel DB2 for VSE, jeśli pakiet zawiera tylko statyczne instrukcje SQL.

– **Dynamiczny SQL:** Opisuje instrukcję SQL, która nie jest znana do chwili uruchomienia pakietu. Instrukcja SQL jest tworzona przez program i dynamicznie przetwarzana przez DB2 for VSE przy użyciu instrukcji SQL PREPARE lub EXECUTE IMMEDIATE. Gdy użytkownik uruchamia dynamiczną instrukcję SQL, musi mieć uprawnienia do tabeli wymagane w celu uruchomienia instrukcji SQL. Ponieważ instrukcja SQL nie jest znana w momencie tworzenia pakietu, użytkownik nie otrzymuje automatycznie wymaganych uprawnień od właściciela pakietu.

- **Obiekty SQL:** Obiektami mogą być tabele, widoki i synonimy. Użytkownikom DB2 for VSE można nadawać różne poziomy uprawnień do tworzenia, usuwania, zmiany i odczytu indywidualnych obiektów SQL. Uprawnienia te są wymagane do przetwarzania wstępnego statycznych instrukcji SQL lub uruchamiania dynamicznych instrukcji SQL.

Reprezentacja danych

Patrz “Reprezentacja danych” na stronie 142.

Lista kontrolna uaktywniania serwera aplikacji DB2 for VSE DRDA Application Server

Lista kontrolna podana poniżej zawiera podsumowanie kroków, które należy wykonać, aby udostępnić serwer aplikacji DRDA. Zakłada się, że system VSE jest zainstalowany z ACF/VTAM z używaną przez niego metodą dostępu teleprzetwarzania oraz że definicje VTAM potrzebne do komunikacji z systemami zdalnymi, takie jak definicje NCP, zostały już przygotowane.

1. Należy zainstalować obsługę CICS ISC i obsługę Restart Resynchronization.
2. Należy zdefiniować CICS dla VTAM for VSE.
3. Należy połączyć tabelę VTAM LOGMODE z pozycją IBMRDB.
4. Należy połączyć tabelę wpisania się do systemu CICS ze wszystkimi zdefiniowanymi identyfikatorami i hasłami użytkowników.
5. Należy uruchomić CICS z właściwymi informacjami SIT:

- ISC=YES,
- TST=YES, ARIAXELG zdefiniowany jako RECOVERABLE w DFHTST i zasemblowany,
- APPLID=LU nazwa (jak to zdefiniowano w instrukcji VTAM APPL).

6. Należy zdefiniować zdalne systemy dla CICS (można użyć bezpośredniego definiowania zasobów - RDO):
   - CEDA DEF CONNECTION,
   - CEDA DEF SESSION,
   - CEDA DEF PROGRAM,
   - CEDA DEF TRANSACTION.

   Instrukcje te powinny mieć wszystkie definicje w jednej grupie o nazwie IBMG. Należy zainstalować grupę za pomocą komendy CEDA INSTALL GROUP(IBMG).
7. Należy zaktualizować katalog DBNAME (ARISDIRD.A):
   - Należy zdefiniować wszystkie nazwy TPN dla CICS znajdujące się w tym katalogu. Nazwy TPN nie zdefiniowane dla CICS są bezużyteczne.
   - Należy zdefiniować wszystkie serwery aplikacji DB2 for VSE DRDA w tym katalogu z poprawną nazwą TPN.
8. Należy uruchomić procedurę ARISBDID, aby połączyć zaktualizowany katalog DBNAME.
9. Należy przygotować serwer DB2 for VSE:
   - Należy uruchomić procedurę ARIS342D, aby zainstalować obsługę DRDA.
   - Jeśli aplikacje online DB2 for VSE (na przykład ISQL) są uruchamiane z partycji CICS, należy nadać uprawnienie do planowania identyfikatorowi CICS APPLID podanemu w tabeli CICS SIT.
   - Należy nadać uprawnienia wszystkim użytkownikom zdalnym.
10. Jeśli to konieczne, należy uruchomić transakcję DAXP CICS.
11. Należy uruchomić DB2 for VSE z właściwym parametrem RMTUSERS i opcjonalnie z parametrami DBNAME i SYNCPNT.
12. Należy przygotować aplikacje na serwerze aplikacji VSE DRDA.

Dodatek A. Najczęstsze problemy związane z połączeniami

W tym dodatku przedstawiono najczęstsze problemy z połączeniami, które mogą występować na stacji roboczej DB2 Connect DB2 UDB podczas używania DB2 Connect i serwera aplikacji DRDA z DB2 UDB:

- "Najczęstsze problemy z DB2 Connect" i
- "Najczęstsze problemy z serwerem aplikacji DRDA z DB2 UDB" na stronie 168.

Informacje te będą pomocne w rozwiązywaniu problemów. Patrz także: *Komunikaty*, *Troubleshooting Guide* i *IBM DB2 Connect Podręcznik użytkownika*.

Najczęstsze problemy z DB2 Connect

W tej sekcji przedstawiono najczęstsze problemy z połączeniami, występujące podczas używania DB2 Connect. W każdym przypadku użytkownik ma do dyspozycji:

- Kombinację numeru komunikatu i kodu powrotu (lub kodu powrotu specyficznego dla używanego protokołu) związanego z tym komunikatem. Każda kombinacja komunikatu i kodu powrotu ma oddzielny nagłówek. Nagłówki są uporządkowane według numerów komunikatów, a w następnej kolejności według kodów powrotu.
- Opisy problemów są udostępniane zwykle w postaci listy przykładowych komunikatów.
- Sugerowane rozwiązanie określa możliwą przyczynę błędu. W niektórych sytuacjach podawanych jest kilka sugerowanych rozwiązań.

Uwagi:

1. Aktualne informacje o zalecanych poziomach poprawek można znaleźć w podręczniku Krótkie wprowadzenie (Quick Beginnings) dla używanego produktu oraz w najnowszym Release Notes (Uwagi do wydania).
2. W przypadku kombinacji kodu komunikatu i kodu powrotu specyficznych dla komunikacji APPC można również podać kod rozpoznania SNA. Dotychczas kod rozpoznania SNA związany z komunikatem trzeba było pobierać z podsystemu SNA.

   Czasami kody rozpoznania SNA są umieszczane w protokołach systemowych. Zależy to jednak od używanego podsystemu SNA. Czasami, aby uzyskać kody rozpoznania, należy najpierw uaktywnić śledzenie SNA, a następnie odtworzyć problem.
3. Termin brama odnosi się do wersji DB2 Connect Enterprise Edition.

SQL0965 lub SQL0969

Opis problemu
Komunikaty SQL0965 i SQL0969 mogą pojawiać się z wieloma różnymi kodami powrotu z DB2 Universal Database for AS/400, DB2 Universal Database for OS/390, DB2 for MVS/ESA i DB2 for VM &VSE.

Jeśli pojawi się taki komunikat, należy odnaleźć oryginalny kod SQL w dokumentacji dla serwera baz danych wydającego komunikat.

Rozwiązanie
Kod SQL odebrany od bazy danych hosta nie może być przekształcany. Należy poprawić błąd na podstawie kodu błędu, a następnie wprowadzić ponownie komendę, której wykonanie nie powiodło się.

SQL1338 podczas wykonywania CONNECT

Opis problemu / przyczyna
Nie zdefiniowano symbolicznej nazwy docelowej lub zdefiniowano ją nieprawidłowo.

Sytuacja taka może mieć na przykład miejsce, gdy używany jest węzeł APPC, a symboliczna nazwa docelowa określona w katalogu węzłów DB2 nie odpowiada pozycji CPI-C w konfiguracji lokalnego podsystemu komunikacyjnego APPC.

Inną przyczyną może być zainstalowanie więcej niż jednego stosu SNA. Konieczne może być sprawdzenie PATH i LIBPATH, co pozwoli zapewnić, że najpierw wystąpi odniesienie do stosu, który ma być używany.

Rozwiązanie
1. Należy sprawdzić, czy nazwa profilu informacji ubocznych interfejsu CPIC określona w katalogu węzłów DB2 odpowiada konfiguracji SNA (uwzględnia rozróżnianie wielkich i małych liter).
2. Konieczne może być sprawdzenie PATH i LIBPATH, co pozwoli zapewnić, że najpierw wystąpi odniesienie do stosu SNA, który ma być używany.

SQL1403N podczas wykonywania CONNECT

Opis problemu
SQL1403N Nazwa użytkownika lub hasło jest niepoprawne.

Rozwiązanie
1. Użytkownik nie został uwierzytelniony na stacji roboczej DB2 Connect. Należy określić, czy użytkownik może być uwierzytelniony na stacji roboczej DB2 Connect.

   Jeśli tak, należy upewnić się, że określono poprawne hasło w instrukcji CONNECT, jeśli jest to konieczne.

Jeśli nie, pozycja systemowego katalogu baz danych musiała zostać niepoprawnie wpisana przy użyciu AUTHENTICATION SERVER (wartość domyślna, jeśli jawnie nie określono AUTHENTICATION). Jeśli miało to miejsce, należy ponownie umieścić pozycję w katalogu przy użyciu AUTHENTICATION DCS lub CLIENT.

2. Hasło niedostępne do wysłania do bazy danych serwera docelowego. Jeśli pozycja systemowego katalogu baz danych została wpisana przy użyciu AUTHENTICATION DCS, to hasło musi być przesłane od klienta DB2 do bazy danych serwera docelowego. Na niektórych platformach, na przykład AIX, hasło można otrzymać jedynie, gdy jest ono udostępniane w instrukcji CONNECT.

SQL5043N

Opis problemu

Obsługa jednego lub więcej protokołów komunikacyjnych nie uruchomiła się pomyślnie. Jednak podstawowe funkcje menedżera baz danych uruchomiły się pomyślnie.

Być może protokół TCP/IP nie został uruchomiony w bramie DB2 Connect, albo poprzednio wystąpiło pomyślne połączenie klienta.

Jeśli diaglevel = 4, to db2diag.log może zawierać pozycje podobne do określonej poniżej.

```
   1997-05-30-14.09.55.321092   Instance:svtdbm5   Node:000
PID:10296(db2tcpcm)   Appid:none
common_communication  sqlcctcpconnmgr_child   Probe:46
DIA3205E Socket address "30090" configured in the TCP/IP
services file and
required by the TCP/IP server support is being used by another
process.
```

Rozwiązanie

Ostrzeżenie to sygnalizuje, że produkt DB2 Connect działający jako brama dla klientów zdalnych ma trudności z obsługiwaniem jednego lub większej liczby protokołów komunikacyjnych klienta. Mogą to być protokoły TCP/IP, APPC lub inne. Komunikat ten zazwyczaj oznacza, że jeden z protokołów komunikacyjnych zdefiniowanych dla DB2 Connect nie jest poprawnie zdefiniowany.

Częstą przyczyną może być nie zdefiniowana lub zdefiniowana niepoprawnie zmienna profilu DB2COMM. Zwykle problem stanowi niezgodność między zmienną DB2COMM a nazwami zdefiniowanymi w konfiguracji menedżera baz danych (na przykład svcename, nname lub tpname).

Możliwym scenariuszem jest wykorzystanie połączenia, które poprzednio powiodło się, a następnie pobranie komunikatu o błędzie SQL5043, gdy żadna konfiguracja nie zmieniła się. Taka sytuacja może mieć miejsce przy użyciu protokołu TCP/IP, gdy system zdalny z jakiegoś powodu niepoprawnie zakończył połączenie. Gdy to się stanie,

może się wydawać, że połączenie nadal istnieje po stronie klienta, i że będzie możliwe przywrócenie połączenia po uruchomieniu komend wymienionych poniżej.

Bardziej prawdopodobne jest, że jeden z klientów łączących się z bramą nadal ma uchwyt na porcie TCP/IP. Na każdej maszynie klienta połączonej z bramą należy wykonać komendy:

1. db2 terminate,
2. db2stop.

SQL30020

Opis problemu
SQL30020N Wykonanie nie powiodło się z powodu błędu protokołu rozproszonego, który będzie miał wpływ na poprawne wykonanie kolejnych komend lub instrukcji SQL.

Rozwiązanie
Po wystąpieniu tego błędu należy się skontaktować z serwisem.

Należy sprawdzić ffdc dump (pid.000) w katalogu db2dump. Następnie należy sformatować ten plik zrzutu za pomocą db2fdump i poszukać w pliku wynikowym słowa ″ERROR″. Może się tu znajdować MVS ABEND. Jeśli tak się zdarzy, należy poszukać dalszych informacji na konsoli MVS i znaleźć kod zakończenia w podręczniku DB2 for MVS Messages and Codes.

SQL30060

Opis problemu
SQL30060N ″<ID-autoryzowanego-użytkownika>″ nie ma uprawnienia do przeprowadzenia operacji ″<operacja>″.

Rozwiązanie
Podczas połączenia z DB2 for MVS lub DB2 for OS/390 tabele komunikacyjne baz danych nie zostały poprawnie zaktualizowane. Należy skorzystać z podręcznika:

- DB2 Connect Quick Beginnings (Krótkie wprowadzenie)

SQL30061

Opis problemu
Połączenie z nieprawidłową lokalizacją hosta lub serwera baz danych AS/400 - nie można odnaleźć docelowej bazy danych.

Rozwiązanie
Być może w pozycji katalogu DCS określono nieprawidłową nazwę bazy danych serwera. W takiej sytuacji do aplikacji zwracany jest kod SQLCODE -30061.

Należy sprawdzić węzeł DB2, bazę danych i pozycje katalogu DCS. Nazwa docelowej bazy danych w pozycji katalogu DCS musi odpowiadać nazwie bazy danych w

zależności od platformy. Na przykład w przypadku bazy danych DB2 Universal Database for OS/390 używana nazwa powinna być taka sama, jak w polu ″LOCATION=nazwa_miejsca″ zbioru danych programu startowego (BSDS). Jest ona także podawana w komunikacie DSNL004I (LOCATION=miejsce) przy uruchamianiu Distributed Data Facility (DDF).

W podręczniku DB2 Connect Quick Beginnings można znaleźć przykłady aktualizowania katalogu DB2. Patrz punkt ″Update the DB2 Directories″ (″Aktualizacja katalogu DB2″) znajdujący się w każdym rozdziale opisującym konfigurowanie SNA lub rozdział ″Configuring Host and AS/400 Databases for DB2 Connect″ (″Konfigurowanie hostów i baz danych AS/400 dla potrzeb DB2 Connect″), punkt ″Configuring the TCP/IP Connection″ (″Konfigurowanie połączenia TCP/IP″).

Komendy poprawne dla węzła APPC lub APPN:

```
db2 catalog appc node <nazwa_węzła> remote <sym_nazw_doc> security program
db2 catalog dcs database <nazwa_lokalna> as <rzecz_nazwa_bazy_danych>
db2 catalog database <nazwa_lokalna> as <alias> at node <nazwa_węzła>
            authentication dcs
```

Komendy poprawne dla węzła TCP/IP:

```
db2 catalog tcpip node <nazwa_węzła> remote <nazwa_lub_adres_hosta>
            server <numer_portu_lub_nazwa_usługi>
db2 catalog dcs database <nazwa_lokalna> as <rzecz_nazwa_bazy_danych>
db2 catalog database <nazwa_lokalna> as <alias> at node <nazwa_węzła>
            authentication dcs
```

Aby następnie połączyć się z bazą danych, należy wpisać:

```
db2 connect to <alias> user <nazwa_użytkownika> using <hasło>
```

SQL30073 z kodem powrotu 119C podczas wykonywania CONNECT

Opis problemu

Komunikat SQL30073 jest wydawany z kodem powrotu 119C. Komunikat pojawia się, gdy baza danych serwera docelowego nie obsługuje strony kodowej używanej przez klienta DB2 (za pośrednictwem DB2 Connect). Strona kodowa jest pobierana z konfiguracji środowiska operacyjnego, w którym jest uruchomiony klient DB2.

Więcej informacji można znaleźć w podręczniku *Administration Guide*.

Rozwiązanie

Problem ten można rozwiązać, instalując poprawkę w systemie baz danych serwera docelowego. Poprawki zalecane w tej sytuacji można uzyskać w serwisie odpowiedniego produktu.

Jako tymczasowe rozwiązanie użytkownik może zastosować przesłonięcie domyślnej strony kodowej, ustawiając zmienną środowiskową. Należy sprawdzić ustawienia narodowe lub ustawić DB2CODEPAGE=850.

Na platformach UNIX użytkownik może spróbować zmienić stronę kodową, zmieniając wartość zmiennej środowiskowej LANG.

SQL30081N z kodem powrotu 1

Opis problemu

Wyświetlany jest następujący komunikat z kodem rozpoznania SNA:

```
  db2 connect to <nazwa_bazy_danych> user <id_użytkownika>
  Podaj hasło dla <id_użytkownika>:
SQL30081N  Wykryto błąd komunikacyjny.
   Używany protokół komunikacyjny: "APPC".
   Używany zestaw komunikacyjnych funkcji API: "CPI-C".
  Miejsce
  wykrycia błędu: "".  Funkcja komunikacyjna wykrywająca
  błąd:
  "cmallc".  Kod błędu specyficzny dla protokołu: "1", "*",
  "0x10030021".
   SQLSTATE=08001
```

Rozwiązanie

W podanym przykładzie kod rozpoznania wynosi 10030021.

Poniżej podano najczęściej występujące kody rozpoznania związane z tym komunikatem o błędzie i sugerowane rozwiązania dla każdego przypadku:

1. `SQL30081N z kodem powrotu 1 i kodem rozpoznania SNA 0877002C.`

   Podano nieprawidłową nazwę sieciową.

2. `SQL30081N z kodem powrotu 1 i kodem rozpoznania SNA ffff0003.`

   Podano nieprawidłowy adres MAC lub połączenie SNA nie jest aktywne.

3. `SQL30081N z kodem powrotu 1 i kodem rozpoznania SNA 10030021.`

   Błędny typ jednostki logicznej.

4. `SQL30081N z kodem powrotu 1 i kodem rozpoznania SNA 084B6031.`

   Parametr MAXDBAT w DSNZPARM (na hoście DB2 for MVS lub DB2 for OS/390) jest ustawiony na 0.

Inne sugestie:

1. Podczas tworzenia profilu lokalnej jednostki logicznej (LU) należy zdefiniować jednostkę logiczną jako domyślną. Na przykład na panelu opcji SNA w CM/2 należy wykonać jedno z opisanych działań:

- Zaznaczyć pole wyboru 'Use this local LU as your default local LU alias'.
- Ustawić profil lub zmienną środowiskową APPCLLU w systemie bramy DB2 Connect Enterprise Edition na nazwę lokalną LU. Można to zrobić w systemie OS/2 przez edycję pliku CONFIG.SYS lub w systemie Windows NT za pomocą Panelu sterowania.

2. Należy sprawdzić, czy uruchomiono SNA na bramie DB2 Connect.
3. Jeśli używany jest produkt DB2 for MVS lub DB2 for OS/390, należy sprawdzić, czy została uruchomiona przestrzeń adresowa Distributed Data Facility (DDF) i czy DB2 działa.

SQL30081N z kodem powrotu 2

Opis problemu
Komunikat SQL30081N jest odbierany z kodem powrotu 2 i kodem rozpoznania 08120022.

Rozwiązanie
Parametr NUMILU na NCP (koniec połączenia znajdujący się na hoście) może być ustawiony na wartość domyślną (0). Należy to sprawdzić. Następnie, jeśli to konieczne, zmodyfikować definicję NCP przed ponowną próbą, po wprowadzeniu zmian.

SQL30081N z kodem powrotu 9

Opis problemu
Wyświetlany jest następujący komunikat (w tym przypadku nie jest wymagany kod rozpoznania SNA):

```
   db2 connect to <baza_danych> user <id_użytkownika>
SQL30081N  Wykryto błąd komunikacyjny.
   Używany protokół komunikacyjny: "APPC".
   Używany zestaw komunikacyjnych funkcji API: "CPI-C".
   Miejsce
   wykrycia błędu: "".  Funkcja komunikacyjna wykrywająca błąd:
   "cmsend".  Kod błędu specyficzny dla protokołu: "9", "*",
"0x10086021".
   SQLSTATE=08001
```

Rozwiązanie
Problem polega na tym, że w systemie DB2 Connect nie zdefiniowano poprawnie nazwy programu transakcyjnego (TPNAME). Na przykład użytkownik mógł zaktualizować konfigurację SNA, ale jeszcze nie zweryfikował jej na bramie DB2 Connect. Dodatkowe informacje można znaleźć w podręcznikach *DB2 Connect Enterprise Edition for OS/2 and Windows Quick Beginnings* i *DB2 Connect Personal Edition Krótkie wprowadzenie*.

SQL30081N z kodem powrotu 10

Opis problemu
Wyświetlany jest następujący komunikat (nie jest wymagany kod rozpoznania SNA):

```
SQL30081N  Wykryto błąd komunikacyjny.
   Używany protokół komunikacyjny: "APPC".
   Używany zestaw komunikacyjnych funkcji API: "CPI-C".
   Miejsce wykrycia błędu: "".  Funkcja komunikacyjna wykrywająca błąd:
   "cmrcv".  Kody błędów właściwe dla protokołu: "10", "*", "*".
   SQLSTATE=08001
```

Rozwiązanie

Należy sprawdzić, czy produkt DB2 jest poprawnie zainstalowany.

Jeśli używana jest brama DB2 Connect for OS/2 i nazwa TP nie jest odpowiednio zdefiniowana, można skorzystać z następujących parametrów:

```
Kody błędów właściwe dla protokołu: "10", "*", "0x084C0000".
SQLSTATE=08001
```

Na przykład w CM/2, w tym przypadku definicja powinna wyglądać następująco:

```
Transaction program name        = 'tpname'    (definiowana przez użytkownika)
OS/2 program path and file name = notused
```

i (na następnym ekranie konfiguracyjnym CM/2)

```
Presentation type - background
Operation type - Queued, operator preloaded
```

SQL30081N z kodem powrotu 20

Opis problemu

```
SQL30081N  Wykryto błąd komunikacyjny.
Używany protokół komunikacyjny: "APPC".
Używany zestaw komunikacyjnych funkcji API: "CPI-C".
Miejsce wykrycia błędu: "".  Funkcja komunikacyjna wykrywająca błąd:
"xcstp".  Kody błędów właściwe dla protokołu: "20", "*", "*".
SQLSTATE=08001
```

Rozwiązanie

Należy sprawdzić, czy w systemie DB2 Connect uruchomiono podsystem SNA.

SQL30081N z kodem powrotu 27

Opis problemu

Komunikat SQL30081N jest odbierany z kodem powrotu 27 i kodem rozpoznania SNA 800Axxxx.

Rozwiązanie

Jednostka informacyjna ścieżki (PIU) VTAM jest za duża.

SQL30081N z kodem powrotu 79

Opis problemu

```
SQL30081N  Wykryto błąd komunikacyjny.
Używany protokół komunikacyjny: "TCP/IP".
Używany zestaw komunikacyjnych funkcji API: "SOCKETS".
Miejsce wykrycia błędu: "".  Funkcja komunikacyjna wykrywająca błąd:
"connect".  Kody błędów właściwe dla protokołu: "79", "*", "*".
SQLSTATE=08001
```

Rozwiązanie

Ten błąd może wystąpić, jeśli klient zdalny nie zdoła połączyć się z bramą DB2 Connect lub brama DB2 Connect łączy się z hostem.

1. Zmienna profilu DB2COMM może być niepoprawnie ustawiona na bramie DB2 Connect. Należy to sprawdzić. Na przykład komenda db2set db2comm=tcpip powinna pojawić się w sqllib/db2profile, gdy w systemie AIX uruchamiany jest produkt DB2 Extended Enterprise Edition.
2. Może istnieć niezgodność między nazwą usługi TCP/IP i/lub specyfikacjami numerów portów na kliencie DB2 i bramie DB2 Connect. Należy sprawdzić pozycje w plikach TCP/IP Services na obu maszynach.
3. Należy sprawdzić, czy uruchomiono DB2 na bramie DB2 Connect. Należy ustawić wartość 4 poziomu diaglevel konfiguracji menedżera baz danych za pomocą komendy:

   ```
   db2 update dbm cfg using diaglevel 4
   ```

   Po zatrzymaniu i ponownym uruchomieniu DB2 należy sprawdzić w pliku db2diag.log, czy uruchomiono komunikację DB2 TCP/IP. Powinien zostać wyświetlony tekst podobny do podanego poniżej:

   ```
   1998-02-03-12.41.04.861119   Instance:svtdbm2   Node:00
   PID:86496(db2sysc)   Appid:none
   common_communication  sqlcctcp_start_listen   Probe:80
   DIA3000I "TCPIP" protocol support was successfully started.
   ```

SQL30081N z kodem błędu 10032 właściwym dla protokołu

Opis problemu

```
SQL30081N  Wykryto błąd komunikacyjny.
Używany protokół komunikacyjny: "TCP/IP".
Używany zestaw komunikacyjnych funkcji API: "SOCKETS".
Miejsce wykrycia błędu: "9.21.85.159".  Funkcja komunikacyjna
wykrywająca błąd: "send".
Kody błędów właściwe dla protokołu: "10032",
"*", "*".
SQLSTATE=08001
```

Rozwiązanie

Ten błąd pojawia się, gdy podjęto próbę odłączenia się od maszyny, na której komunikacja TCP/IP załamała się. Należy rozwiązać problem z podsystemem TCP/IP.

Na większości maszyn ponowne uruchomienie protokołu TCP/IP rozwiązuje problem. Niekiedy może być konieczne wyłączenie i włączenie maszyny.

Najczęstsze problemy z serwerem aplikacji DRDA z DB2 UDB

W tej sekcji przedstawiono najczęstsze scenariusze rozwiązywania problemów podczas używania serwera aplikacji DRDA z DB2 UDB.

Błędy komunikacyjne występujące podczas wykonywania CONNECT

Należy sprawdzić, czy następujące parametry są poprawnie ustawione po stronie DB2 UDB:

Jednostka logiczna 6.2 (LU 6.2) APPC/SNA

1. Konfiguracja SNA.

   Jeśli jest to konieczne, należy sprawdzić, czy została skonfigurowana nazwa TP.

   Ponadto jeśli ma być używana ochrona SAME z DRDA AR, należy sprawdzić, czy była ona udostępniona dla jednostki logicznej DRDA AR.
2. Parametr TPNAME konfiguracji menedżera baz danych.
3. Zmienna środowiskowa DB2COMM ustawiona, tak aby uwzględniała APPC.

Należy się upewnić, że db2start zakończy się bez ostrzeżenia. db2start.

TCP/IP

1. Plik Services.
2. Parametr SVCENAME konfiguracji menedżera baz danych.
3. Zmienna środowiskowa DB2COMM ustawiona, tak aby uwzględniała TCP/IP. Należy się upewnić, że db2start zakończy się bez ostrzeżeń.

Błąd DRDA podczas wykonywania CONNECT

Jednostka logiczna 6.2 (LU 6.2) APPC/SNA

Jeśli używany jest serwer SNA dla AIX, należy sprawdzić, czy nazwa grupy dla pliku wykonywanego ~/sqllib/adm/db2sysc znajduje się w polu ″Trusted group names″ w profilu ″SNA System Defaults″ konfiguracji SNA.

TCP/IP

Jeśli serwerem DRDA AR jest DB2 for OS/390, należy sprawdzić, czy zastosowano następujące poprawki: APAR PQ05771/PTF UQ06843 i APAR PQ07537/PTF UQ09146.

Błąd nieodnalezienia bazy danych podczas wykonywania CONNECT

Należy upewnić się, że w konfiguracji requestera aplikacji DRDA znajduje się alias docelowej bazy danych DB2 UDB.

Błąd ochrony podczas wykonywania CONNECT przez jednostkę logiczną 6.2 (LU 6.2) APPC/SNA

Jeśli połączenie z requesterem aplikacji DRDA jest realizowane przez jednostkę logiczną 6.2 (LU 6.2) APPC/SNA, należy uwzględnić ustawienie AUTHENTICATION w konfiguracji menedżera baz danych DB2 UDB. Jeśli wystąpi błąd ochrony, należy zadbać o poprawne ustawienie parametru AUTHENTICATION konfiguracji menedżera baz danych:

1. Klient

   Z taką wartością parametru będą działały połączenia zarówno z typem ochrony SAME, jak i PROGRAM.

2. Serwer

   Z taką wartością parametru będą działały tylko połączenia z typem ochrony PROGRAM skierowane do serwera aplikacji DRDA z DB2 UDB w systemie AIX z serwerem SNA i w systemie OS/2 z CS/2 V4 (ze skonfigurowanym SPM).

3. DCS

   Obecnie można użyć AUTHENTICATION DCS na serwerze DB2 UDB wersja 7 DRDA AS, aby umożliwić połączenia APPC klientom DRDA używającym SAME (hasło nie jest wymagane), wymuszając jednocześnie uwierzytelnianie SERVER (hasło jest wymagane) wszystkich żądań pozostałych klientów.

   Z taką wartością parametru będą działały:

   a. Serwer aplikacji DRDA z DB2 UDB w systemie AIX z serwerem SNA i w systemie OS/2 z CS/2 V4 (ze skonfigurowanym SPM):

      ```
      Security SAME
      ```

   b. Serwer aplikacji DRDA z DB2 UDB w systemie OS/2 z CM/2 1.11, Windows NT i Sun Solaris:

      ```
      Security SAME or PROGRAM
      ```

Różnice wiążą się z tym, że niektóre podsystemy komunikacyjne nie udostępniają haseł przychodzących DB2 UDB.

Błędy podczas wykonywania BIND

Jeśli komenda BIND wydana przez serwer aplikacji DRDA nie jest obsługiwana, może zostać zwrócony obszar komunikacyjny SQL z kodem SQLCODE -4930. Pole SQLERRMC zawiera informacje o opcji komendy BIND powodującej błąd.

Dodatek B. Uwagi

Powoływanie się w tej publikacji na produkty, programy lub usługi firmy IBM nie oznacza, że firma IBM udostępnia je we wszystkich krajach, w których prowadzi działalność. Informacje o produktach i usługach dostępnych w danym kraju można uzyskać od lokalnego przedstawiciela firmy IBM. Jakakolwiek wzmianka na temat produktu, programu lub usługi firmy IBM nie oznacza, że może być zastosowany jedynie ten produkt, ten program lub ta usługa firmy IBM. Zamiast nich można zastosować dowolny, równoważny funkcjonalnie produkt, program lub usługę, pod warunkiem, że nie narusza to własności intelektualnej firmy IBM. Jednak cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

Firma IBM może być właścicielem patentów związanych z tematyką tej publikacji, może też mieć zgłoszone kolejne wnioski patentowe. Używanie tego dokumentu nie daje żadnych praw do tych patentów. Wnioski o przyznanie licencji można zgłaszać na piśmie pod adresem:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Wnioski o przyznanie licencji na informacje dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej firmy IBM (IBM Intellectual Property Department) lub zgłaszać na piśmie pod adresem:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

Poniższy akapit nie obowiązuje w Wielkiej Brytanii, a także w innych krajach, w których jego treść pozostaje w sprzeczności z lokalnymi przepisami prawa:

FIRMA INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W TAKIM STANIE, W JAKIM SIĘ OBECNIE ZNAJDUJE, “AS IS”, BEZ JAKICHKOLWIEK GWARANCJI, ZARÓWNO WYRAŹNYCH, JAK I DOMNIEMANYCH, W TYM BEZ DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ CZY TEŻ UŻYTECZNOŚCI DLA OKREŚLONYCH CELÓW LUB GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwo niektórych krajów nie dopuszcza

zastrzeżeń dotyczących gwarancji wyraźnych i domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w tej publikacji mogą zawierać niedokładności techniczne i błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany będą odzwierciedlane w kolejnych wydaniach tej publikacji. Firma IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez uprzedniego powiadomienia.

Wszelkie wzmianki w tej publikacji na temat stron internetowych innych firm zostały wprowadzone wyłącznie dla wygody użytkowników i w żadnym wypadku nie stanowią zachęty do ich odwiedzania. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych do tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

Firma IBM ma prawo do używania i dystrybucji informacji przysłanych przez użytkownika, w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich nadawcy.

Informacje na temat możliwości stosowania programów, takich jak: (i) wymiana informacji między niezależnie tworzonymi programami a innymi programami (włącznie z tym) czy (ii) wspólne używanie wymienianych informacji, można uzyskać pod adresem:

IBM Canada Limited
Office of the Lab Director
1150 Eglinton Ave. East
North York, Ontario
M3C 1H7
CANADA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym w niektórych przypadkach uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w tej publikacji i wszystkie dotyczące go licencjonowane materiały są dostarczane przez firmę IBM na warunkach określonych w umowach IBM Customer Agreement, IBM International Program License Agreement lub innych podobnych umowach, zawieranych pomiędzy firmą IBM a użytkownikami.

Wszelkie dane dotyczące wydajności zostały zebrane w kontrolowanym środowisku. W związku z tym, rezultaty uzyskane w innych środowiskach operacyjnych mogą się znacząco różnić. Niektóre pomiary mogły zostać wykonane na systemach będących w fazie rozwoju i nie ma gwarancji, że pomiary te wykonane na ogólnie dostępnych systemach dadzą takie same wyniki. Niektóre z pomiarów mogły być estymowane przez ekstrapolację. Rzeczywiste wyniki mogą być inne. Użytkownicy poninni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów innych firm zostały uzyskane od dostawców tych produktów z opublikowanych zapowiedzi lub innych powszechnie dostępnych źródeł. IBM nie testował tych produktów i nie może potwierdzić dokładności pomiarów wydajności, kompatybilności ani żadnych innych danych związanych z tymi produktami. Pytania dotyczące możliwości produktów innych firm należy kierować do dostawców tych produktów.

Wszelkie stwierdzenia dotyczące planów i zamiarów firmy IBM mogą zostać zmnienione lub wycofane bez powiadomienia.

Publikacja ta może zawierać przykładowe dane i raporty używane w codziennych operacjach biznesowych. W celu kompleksowego ich zilustrowania, podane przykłady zawierają nazwy osób, firm i ich produktów. Wszystkie te nazwy są fikcyjne i jakiekolwiek podobieństwo do istniejących nazw i adresów przedsiębiorstw jest całkowicie przypadkowe.

LICENCJA PRAW AUTORSKICH:

Niniejsza publikacja może zawierać przykładowe aplikacje w kodzie źródłowym, ilustrujące techniki programowania w różnych systemach operacyjnych. Użytkownik może kopiować, modyfikować i rozpowszechniać te programy przykładowe w dowolnej formie bez uiszczania opłat, w celu rozbudowy, użytkowania, handlowym lub w celu dystrybucji aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane były programy przykładowe. Programy przykładowe nie zostały gruntownie przetestowane. Firma IBM zatem, nie może gwarantować lub sugerować niezawodności, użyteczności i funkcjonalności tych programów.

Każda kopia lub dowolna część programów przykładowych, albo też dowolna praca pochodna musi zawierać poniższą informację o prawach autorskich:

© (nazwa_firmy_użytkownika) (rok). Części niniejszego kodu pochodzą z programów przykładowych firmy IBM Corp. © Copyright IBM Corp. _rok_lub_lata_. Wszelkie prawa zastrzeżone.

Znaki towarowe

Poniższe nazwy, które mogą być oznaczone gwiazdką (*), są znakami towarowymi firmy International Business Machines Corporation w Stanach Zjednoczonych i/lub innych krajach.

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

Poniższe nazwy są znakami towarowymi lub zastrzeżonymi znakami towarowymi innych firm:

Microsoft, Windows i Windows NT są znakami towarowymi lub zastrzeżonymi znakami towarowymi firmy Microsoft Corporation.

Java, wszystkie znaki towarowe i logo związane z nazwą Java oraz Solaris są znakami towarowymi firmy Sun Microsystems, Inc. w Stanach Zjednoczonych i/lub innych krajach.

Tivoli i NetView są zastrzeżonymi znakami towarowymi firmy Tivoli Systems Inc. w Stanach Zjednoczonych i/lub innych krajach.

UNIX jest zastrzeżonym znakiem towarowym w Stanach Zjednoczonych i innych krajach używanym wyłącznie przez firmę X/Open Company Limited.

Nazwy innych firm, produktów i usług, które mogą być oznaczone podwójną gwiazdką (**), mogą być znakami towarowymi lub znakami usług innych firm.

Indeks

A

ACF/VTAM 144
adapter zasobów, VM 113
ADDRDBDIRE, komenda 86
aplikacje CLI/ODBC
  CURRENTPACKAGESET 46
aplikacje ODBC
  CURRENTPACKAGESET 46
APPN (zaawansowana sieć typu każdy z każdym)
  lista miejsc, tworzenie 90
AS/400
  publikacje vii
AUTHENTICATION=CLIENT 46
autoryzacja domyślna, AS/400 94
AVS
  komponent VM 111
  uwagi dotyczące limitu liczby sesji 129
AXE 144

B

BSDS (zestaw danych programu startowego), aktualizacja 9, 49

C

CCSID (coded character set identifier), OS/400, wartości domyślne 94
  wartość domyślna dla DB2 24, 72
CHARNAME 119, 134, 142
CHGNETA, komenda 88
CICS(ISC) 144
comdir
  CMS 127
  przykład pozycji 132
  VM 112
Coordinated Resource Recovery (CRR) 112
Coordinated Resource Recovery (CRR) Server 112
CRTCFGL, komenda 90
CRTCOSD, komenda 89
CRTCTLAPPC, komenda 89
CRTCTLHOST, komenda 89
CRTDDMTCPA, komenda 98
CRTDEVAPPC, komenda 90
CRTLINETH, komenda 88
CRTLINSDLC, komenda 88
CRTLINTRN, komenda 88
CRTLINX25, komenda 88
CRTMODD, komenda 90
CURRENTPACKAGESET 46

D

DB2 Universal Database for AS/400
  konfiguracja połączeń TCP/IP 88
  rdzenne połączenia TCP/IP 88
DB2 Universal Database for OS/390
  DYNAMICRULES(BIND) 46
  TCP/IP, sprawdzony uprzednio 46
dostęp sterowany przez aplikację 3, 42
dostęp sterowany przez system 3, 42
DRDA
  publikacje vi
dynamiczny SQL 36, 81
  CURRENTPACKAGESET 46

G

GCS (system sterujący grupami) 112

I

IDENT 113
informacje dotyczące sieci
  DB2, serwer aplikacji 25, 74
  OS 400, serwer aplikacji 96
  requester aplikacji OS/400 86
  requester aplikacji SQL/DS 122
  serwer aplikacji SQL/DS na VM 136
  serwer aplikacji VSE SQL/DS 147
instrukcja ALREADYV 124
Instrukcja APPCPASS 132
instrukcja APPL
  przykład DB2 10, 51
  przykład SQL/DS 123

K

katalog DBNAME 144
katalog komunikacyjny CMS
  ochrona 132
  wpisywanie do katalogu nazw RDB_NAME 127
katalog nazw baz danych 144
katalog relacyjnej bazy danych, OS/400
  informacje o wpisie 87
  opis 86
klasa usługi
  opis OS/400 89
  tworzenie 89
komunikacja 13, 14, 15, 16, 17, 55, 57, 59, 60, 61
komunikacja 13, 14, 15, 16, 17, 55, 57, 59, 60, 61 *(kontynuacja)*
  katalog, środowisko VM 112, 127
  podsystem
    requester aplikacji DB2 17, 62
    requester aplikacji OS/400 88
  przepływ informacji, SQL/DS VSE 145
  przykłady przepływ VM 114
  tabele baz danych, DB2
    SYSIBM.IPNAMES 61
    SYSIBM.LOCATIONS 55
    SYSIBM.LUMODES 59
    SYSIBM.LUNAMES 57
    SYSIBM.MODESELECT 59
    SYSIBM.SYSLOCATIONS 13
    SYSIBM.SYSLUMODES 14
    SYSIBM.SYSLUNAMES 14
    SYSIBM.SYSMODESELECT 15
    SYSIBM.SYSUSERNAMES 16
    SYSIBM.USERNAMES 60
komunikaty
  wymiana, DB2 7, 48

L

LINKNAME, tabela 13, 55
LINKNAME, tabela DB2 13, 55
lista konfiguracji, tworzenie 90

M

MVS
  publikacje vii
MVS (multiple virtual storage) przestrzenie adresowe DB2 1
MVS (multiple virtual storage), przestrzenie adresowe DB2 40

N

nazwa obiektu, rozstrzyganie przez DB2 31
nazwy użytkowników 18, 32, 64
  DB2 32, 77
  requester aplikacji
    DB2 18, 64
    OS/400 91
    SQL/DS na VM 130
  serwer aplikacji
    OS/400 97
    SQL/DS na VM 139
nazywanie lokalnej bazy danych, OS/400 86

nazywanie zdalnej bazy danych, OS/400 96

O

obsługa APPC/VM 112
obsługa APPC/VTAM 111
ocenianie wielkości RU
  OS 400, serwer aplikacji 96
  requester aplikacji DB2 17, 63
  requester aplikacji OS/400 91
  requester aplikacji SQL/DS 129
ochrona 18, 21, 23, 24, 31, 32, 34, 36, 37, 64
  nazwy użytkowników
    DB2, serwer aplikacji 32, 77
    requester aplikacji DB2 18, 64
    requester aplikacji OS/400 91
    requester aplikacji SQL/DS 130
  podsystem SQL/DS 134
  przetwarzanie
    DB2, serwer aplikacji 31, 77
    serwer aplikacji SQL/DS na VM 138
  requester aplikacji
    menedżer baz danych DB2 23, 71
    menedżer baz danych OS/400 93
    menedżer baz danych SQL/DS 133
    podsystem DB2 24, 72
    sieć DB2 21, 69
  serwer aplikacji
    menedżer baz danych DB2 36, 81
    menedżer baz danych SQL/DS 140
    OS/400, nazwy użytkowników 97
    podsystem DB2 37, 82
    podsystem SQL/DS na VM 141
  sieć
    DB2 Universal Database for AS/400, serwer aplikacji 97
    DB2, serwer aplikacji 34, 79
    requester aplikacji OS/400 92
    requester aplikacji SQL/DS 131
    serwer aplikacji SQL/DS na VM 140
  sprawdzanie źródła żądania w DB2 32, 77
  system OS/400 93
ochrona menedżera baz danych
  DB2, serwer aplikacji 36, 81
  requester aplikacji DB2 23, 71
  requester aplikacji OS/400 93
ochrona menedżera baz danych *(kontynuacja)*
  requester aplikacji SQL/DS 133
  serwer aplikacji SQL/DS na VM 140
ochrona podłączenia, poziomy 154
ochrona systemu, OS/400 93
ochrona w sieci
  DB2 Universal Database for AS/400, serwer aplikacji 97
  DB2, serwer aplikacji 34, 79
  requester aplikacji DB2 21, 69
  requester aplikacji SQL/DS 131
  serwer aplikacji SQL/DS na VM 140
opis kontrolera, tworzenie 89
opis linii, tworzenie 88
opis trybu, tworzenie 90
opis urządzenia, tworzenie 90
OS/400
  atrybuty sieciowe 88
  publikacje vii
  uaktywnianie komunikacji 90

P

pacing 17, 63
  liczba
    OS 400, serwer aplikacji 96
    requester aplikacji DB2 17, 63
    requester aplikacji OS/400 91
    requester aplikacji SQL/DS 129
pakiety
  ochrona menedżera baz danych SQL/DS 141, 155
  ochrona serwera aplikacji DB2 36, 81
plik RESID NAMES
  SQL/DS na VM 137
połączenie 45
  dostęp bezpośredni do systemu, serwery 31
  typy
    rozproszona baza danych DB2 6, 45
    rozproszona baza danych SQL/DS na VM 118
przetwarzanie
  opcje, DB2 6, 45
przykłady
  ADDRDBDIRE, komenda 86
  CMS Communication Directory, pozycja katalogu 155
  definicja bramy AVS 123
  instrukcja APPL VTAM DB2 10, 51
przykłady *(kontynuacja)*
  nadawanie uprawnień, OS/400 93
  pozycja comdir VM 132
  przykłady przepływu komunikacji VM 114
publikacje
  AS/400 vii
  DRDA vii
  MVS vii
  OS/400 vii
  serwer aplikacji vii
  SQL/DS vii
  VM vii
  VSE vii

R

RDB_NAME
  katalog komunikacyjny CMS 127
rekord DDF 8, 48
RELOAD PACKAGE, komenda 133
reprezentacja danych
  DB2, serwer aplikacji 38, 83
  OS 400, serwer aplikacji 99
  requester aplikacji DB2 24, 72
  requester aplikacji OS/400 94
  requester aplikacji SQL/DS 134
  serwer aplikacji SQL/DS na VM 142
requester aplikacji, DB2 7, 13, 17, 18, 21, 23, 24, 25, 47, 55, 63, 64, 73
  definicja systemu lokalnego (VTAM) 48
  definiowanie systemu lokalnego 7
  definiowanie systemu zdalnego 13, 55
  ocenianie wielkości RU 17, 63
  ochrona
    menedżer baz danych 23, 71
    nazwy użytkowników 18, 64
    podsystem 24, 72
    sieć 21, 69
  pacing 17, 63
  podsystem komunikacyjny 17, 62
  reprezentacja danych 24, 72
requester aplikacji, OS/400 85, 95
  definiowanie komunikacji 88
  informacje dotyczące sieci 86
  ocenianie wielkości RU 91
  ochrona 92
  pacing 91
  reprezentacja danych 94
requester aplikacji, SQL/DS VM 122, 135
  definiowanie systemu lokalnego 122

requester aplikacji, SQL/DS VM 122, 135 *(kontynuacja)*
definiowanie systemu zdalnego 126
informacje dotyczące sieci 122
ocenianie wielkości RU 129
ochrona
menedżer baz danych 133
nazwy użytkowników 130
podsystem 134
sieć 131
pacing 129
podsystem komunikacyjny 128
reprezentacja danych 134
uwagi dotyczące limitu liczby sesji AVS 129
RESID (TPN) 137
rozproszona baza danych
dostęp, requester aplikacji DB2 7, 47
połączenia DB2 3, 42
rozproszona jednostka pracy
dostęp sterowany przez aplikację 3, 42
dostęp sterowany przez system 3, 42
rozstrzyganie nazw obiektów, DB2 31

S

serwer aplikacji
publikacje vii
serwer aplikacji, DB2 25, 32, 34, 36, 37, 38, 73, 83
dostęp sterowany przez system 28
informacje dotyczące sieci 25, 74
ochrona
menedżer baz danych 36, 81
nazwy użytkowników 32, 77
podsystem 37, 82
sieć 34, 79
ochrona menedżera baz danych 36, 81
reprezentacja danych 38, 83
serwer pomocniczy 28
sprawdzanie źródła żądania 32, 77
translacja nazw przychodzących 32, 77
serwer aplikacji, OS/400 95, 99
informacje dotyczące sieci 96
nazwy użytkowników 97
nazywanie zdalnej bazy danych 96
ocenianie wielkości RU 96
ochrona 96
opis 96
reprezentacja danych 99
serwer aplikacji, SQL/DS VM 136
informacje dotyczące sieci 136
serwer aplikacji, SQL/DS VM 136 *(kontynuacja)*
nazwy użytkowników 139
ochrona
menedżer baz danych 140
sieć 140
opis 136
reprezentacja danych 142
translacja nazw przychodzących 139
serwer aplikacji, VSE SQL/DS 147, 157
informacje dotyczące sieci 147
ochrona
bind-time 153
menedżer baz danych 155
połączenie 153
użytkownik 154
opis 151
serwer DRDA
publikacje vii
serwer pomocniczy 4, 28, 42
sesja
limity, dostęp bezpośredni do systemu 31
limity, SQL/DS na VM 129
sesje LU 6.2 CICS 147
SET CURRENT PACKAGESET 46
sprawdzanie źródła żądania
DB2, serwer aplikacji 32, 77
SQL (Structured Query Language) 28
DB2, serwery pomocnicze
nazwy obiektów 28
różnice 28
dynamiczny 36, 81
obiekty, ochrona DB2 36, 82
obiekty, ochrona menedżera baz danych SQL/DS 141, 156
statyczny 36, 81
SQL Reference, publikacje vii
SQL/DS
publikacje vii
SQL/DS VM
opcje przetwarzania PROTOCOL 118
SQLINIT 118
statyczny SQL 36, 81
SYSIBM.IPNAMES, tabela 61
SYSIBM.LOCATIONS, tabela 55
SYSIBM.LUMODES, tabela 59
SYSIBM.LUNAMES, tabela 57
SYSIBM.MODESELECT, tabela 59
SYSIBM.USERNAMES, tabela 60
system lokalny
definiowanie DB2 7
system lokalny *(kontynuacja)*
definiowanie DB2 (VTAM) 48
requester aplikacji SQL/DS 122
system sterujący grupami (GCS) 112

T

tabela SYSIBM.SYSLOCATIONS 13
tabela SYSIBM.SYSLUMODES 14
tabela SYSIBM.SYSLUNAMES 14
tabela SYSIBM.SYSMODESELECT 15
tabela SYSIBM.SYSUSERNAMES 16
TCP/IP
dobrze znany port 446 dla DRDA 96
ochrona sprawdzona uprzednio 46
ochrona w systemie AS/400 98
TPN (nazwa programu transakcyjnego)
domyślne DRDA, OS/400 87
OS 400, serwer aplikacji 96
RESID SQL/DS na VM 137
SYSIBM.LOCATIONS, tabela DB2 55
tabela SYSIBM.SYSLOCATIONS DB2 13
translacja nazw przychodzących
DB2, serwer aplikacji 32, 77
serwer aplikacji SQL/DS na VM 139
translacja nazw wychodzących
requester aplikacji DB2 18, 64
requester aplikacji SQL/DS 131
Transparent Services Access Facility (TSAF) 113
TSAF (Transparent Services Access Facility) 113

U

uwarunkowania konfiguracji
zmiana hasła 47

V

VM
adapter zasobów 113
comdir, communications directory 112
komponenty DRDA 111
pozycja katalogu 132
publikacje vii
VRYCFG, komenda 90
VSE
publikacje vii
VSE SQL/DS
sesje LU 6.2 CICS 147
VTAM 10, 12, 51, 54
DRDA, rola w 113

VTAM 10, 12, 51, 54 *(kontynuacja)*
instrukcja APPL
domyślny limit liczby sesji 12, 54
parametry używane w SQL/DS na VM 123
przykład DB2 10, 51
opcje ochrony 124

W

WRKCFGSTS, komenda 90
wymiana komunikatów
DB2 7, 48

X

XPCC 145

Z

zdalna jednostka pracy
połączenia DB2 4, 42
zmiana atrybutów sieciowych, komenda 88

Kontakt z firmą IBM

W przypadku problemów technicznych należy przejrzeć informacje które zawiera *i wykonać opisane tam czynności przed skontaktowaniem się z Obsługą klienta DB2. Książka ta zawiera informacje, których zebranie pomoże Obsłudze klienta DB2 w szybszym rozwiązaniu problemu.*

Informacje o tym, jak zamawiać opcje produktu DB2 Universal Database, można uzyskać od przedstawiciela firmy IBM działającego w lokalnym oddziale firmy lub od dowolnego autoryzowanego sprzedawcy programów firmy IBM.

Dla osób mieszkających w USA dostępne są następujące numery telefonów:

- 1-800-237-5511 - obsługa klienta,
- 1-888-426-4343 - informacje o dostępnych opcjach serwisowych.

Informacje na temat produktu

Dla osób mieszkających w USA dostępne są następujące numery telefonów:

- 1-800-IBM-CALL (1-800-426-2255) lub 1-800-3IBM-OS2 (1-800-342-6672) - zamawianie produktów i informacje ogólne.
- 1-800-879-2755 - zamawianie publikacji.

http://www.ibm.com/software/data/
Strony WWW produktu DB2 zawierają informacje o nowościach, opisy produktów, harmonogramy szkoleń i wiele innych.

http://www.ibm.com/software/data/db2/library/
Biblioteka DB2 Product and Service Technical Library umożliwia dostęp do najczęściej zadawanych pytań, książek i najnowszych danych technicznych dotyczących DB2.

Uwaga: Informacje te mogą być dostępne wyłącznie w języku angielskim.

http://www.elink.ibmlink.ibm.com/pbl/pbl/
Strona WWW umożliwiająca zamawianie publikacji.

http://www.ibm.com/education/certify/
Strona WWW Professional Certification Program zawiera informacje o testach certyfikacyjnych dla wielu produktów IBM, w tym DB2.

ftp.software.ibm.com
Zaloguj się jako użytkownik anonymous. W katalogu /ps/products/db2 znajdują się wersje demonstracyjne, poprawki, informacje i narzędzia związane z produktem DB2 i innymi produktami.

comp.databases.ibm-db2, bit.listserv.db2-l
Internetowe grupy dyskusyjne służące do wymiany różnorodnych informacji i doświadczeń między użytkownikami produktów DB2.

W Compuserve: GO IBMDB2
Wpisz to polecenie, aby uzyskać dostęp do forum dotyczącego rodziny IBM DB2. Forum to swą tematyką obejmuje wszystkie produkty DB2.

Informacje o sposobach kontaktowania się z firmą IBM poza Stanami Zjednoczonymi zawiera Dodatek A książki *IBM Software Support Handbook*. Aby uzyskać dostęp do tego podręcznika, przejdź do strony WWW o adresie http://www.ibm.com/support/, a następnie kliknij odsyłacz IBM Software Support Handbook, znajdujący się w dolnej części tej strony.

Uwaga: W niektórych krajach autoryzowani przedstawiciele firmy IBM powinni skontaktować się z reprezentantami struktury przedstawicielskiej zamiast z centrum IBM Support Center.