IBM®

Połączenia z DB2 - suplement

Wersja 8

SDB2-CONN-SU

IBM®

Połączenia z DB2 - suplement

Wersja 8

SDB2-CONN-SU

Przed skorzystaniem z tych informacji i opisywanych przez nie produktów należy przeczytać informacje ogólne, które zawiera rozdział *Uwagi*.

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.

Publikacje firmy IBM można zamówić poprzez stronę WWW lub u lokalnego przedstawiciela firmy IBM.

- Aby zamówić książki poprzez stronę WWW, należy skorzystać ze strony IBM Publications Center pod adresem www.ibm.com/shop/publications/order
- Aby znaleźć najbliższego lokalnego przedstawiciela firmy IBM, należy skorzystać z informacji umieszczonych na stronie IBM Directory of Worldwide Contacts pod adresem www.ibm.com/planetwide

Aby zamówić książki DB2 w firmie IBM w Stanach Zjednoczonych lub Kanadzie, należy zadzwonić do działu DB2 Marketing and Sales pod numer 1-800-IBM-4YOU (426-4968).

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.

© Copyright International Business Machines Corporation 1993-2004. Wszelkie prawa zastrzeżone.

Spis treści

© Copyright IBM Corp. 1993-2004

Część 1. Ręczne konfigurowanie komunikacji

© Copyright IBM Corp. 1993-2004

Rozdział 1. Ręczne konfigurowanie komunikacji TCP/IP

Ręczne konfigurowanie komunikacji TCP/IP między programem DB2 Connect a serwerem bazy danych hosta i systemu iSeries

Połączenie TCP/IP między serwerem DB2 Connect a bazą danych hosta lub systemu iSeries może zostać skonfigurowane ręcznie. Protokół TCP/IP jest zwykle konfigurowany automatycznie za pomocą Asysty podczas konfigurowania.

Wymagania wstępne:

Przed rozpoczęciem procesu ręcznej konfiguracji połączenia TCP/IP między programem DB2 Connect i serwerem bazy danych hosta lub systemu iSeries należy się upewnić się, że:

- Protokół TCP/IP na serwerze DB2 i na komputerze hosta lub w systemie iSeries funkcjonuje sprawnie.
- Przy użyciu arkusza wartości parametrów TCP/IP zostały zidentyfikowane następujące wartości parametrów:
  - Nazwa hosta (*nazwa_hosta*) lub adres IP (*adres_ip*)
  - Nazwa usługi połączeń (*nazwa_usługi*) lub numer portu/protokół (*numer_portu/tcp*)
  - Nazwa docelowej bazy danych (*nazwa_docelowej_bazy_danych*)
  - Nazwa lokalnej bazy danych (*lokalna_nazwa_dcs*)
  - Nazwa węzła (*nazwa_węzła*)

Procedura postępowania:

Aby ręcznie skonfigurować komunikację TCP/IP między serwerem DB2 Connect a bazą danych hosta lub systemu iSeries:

1. Skonfiguruj protokół TCP/IP na serwerze DB2 Connect.
2. Wpisz węzeł TCP/IP do katalogu.
3. Wpisz bazę danych hosta lub systemu iSeries do katalogu jako bazę danych usługi Database Connection Service (DCS).
4. Wpisz bazę danych hosta lub systemu iSeries do katalogu.
5. Powiąż narzędzia i aplikacje z serwerem bazy danych hosta lub systemu iSeries.
6. Przetestuj połączenie z hostem lub systemem iSeries.

Uwaga: Powiadomienie protokołu TCP/IP o awarii partnera znajdującego się na innym komputerze hosta lub w innym systemie iSeries może nie być natychmiastowe ze względu na charakterystykę tego protokołu. W takim wypadku aplikacja kliencka, uzyskująca dostęp do serwera DB2 za pomocą protokołu TCP/IP lub odpowiadającego mu agenta na serwerze, może sprawiać wrażenie zawieszonej. Do wykrywania niepowodzeń i zerwanych połączeń TCP/IP produkt DB2 używa opcji gniazda TCP/IP SO_KEEPALIVE.

Zadania pokrewne:

- “Konfigurowanie protokołu TCP/IP na serwerze DB2 Connect” na stronie 4
- “Wpisywanie węzła TCP/IP do katalogu” na stronie 6
- “Wpisywanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS)” na stronie 7

© Copyright IBM Corp. 1993-2004

- “Wpisywanie bazy danych do katalogu” na stronie 7
- “Powiązanie narzędzi i aplikacji z serwerem bazy danych hosta lub systemu iSeries” na stronie 9
- “Testowanie połączenia z hostem lub systemem iSeries” na stronie 9
- “Ręczne konfigurowanie komunikacji APPC między programem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries” na stronie 11

Informacje pokrewne:

- “Arkusz wartości parametrów TCP/IP” na stronie 133

Zadania konfiguracyjne

Konfigurowanie protokołu TCP/IP na serwerze DB2 Connect

Konfigurowanie protokołu TCP/IP na serwerze DB2 Connect jest częścią większego zadania polegającego na konfigurowaniu komunikacji TCP/IP między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries.

Procedura postępowania:

Aby skonfigurować protokół TCP/IP na serwerze DB2 Connect:

- Sprawdź adres IP lokalnego systemu hosta.
- Zaktualizuj plik usług.

Po wykonaniu tych czynności można wpisać węzeł TCP/IP do katalogu.

Zadania pokrewne:

- “Dokonywanie translacji adresu IP lokalnego hosta lub systemu iSeries” na stronie 4
- “Aktualizowanie pliku usług” na stronie 5
- “Wpisywanie węzła TCP/IP do katalogu” na stronie 6

Zadania konfiguracji protokołu TCP/IP

Dokonywanie translacji adresu IP lokalnego hosta lub systemu iSeries

Dokonywanie translacji adresu IP lokalnego hosta lub systemu iSeries jest częścią większego zadania polegającego na konfigurowaniu komunikacji między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries. Serwer DB2 Connect musi znać adres hosta lub systemu iSeries, z którym próbuje nawiązać komunikację.

Uwaga: Jeśli w sieci znajduje się serwer nazw lub jeśli planowane jest bezpośrednie określanie adresu IP (*adres_ip*) hosta lub serwera iSeries, można przejść do sekcji opisującej wpisywanie węzła TCP/IP do katalogu.

Jeśli w sieci brak jest serwera nazw, można bezpośrednio określić nazwę hosta, która odpowiada adresowi IP (*adres_ip*) hosta lub systemu iSeries zapisanemu w lokalnym pliku hostów.

Jeśli planuje się obsługę klienta systemu UNIX korzystającego z sieciowych usług informacyjnych NIS (Network Information Services), nie używając w sieci serwera nazw domen, trzeba zaktualizować plik hostów znajdujący się na serwerze głównym NIS.

Tabela 1. Położenie lokalnych plików hostów i usług

System operacyjny	Katalog
Windows 98	windows
Windows NT i Windows 2000	winnt\system32\drivers\etc
UNIX	/etc

Procedura postępowania:

Aby dokonać translacji adresu IP lokalnego hosta lub systemu iSeries, za pomocą edytora tekstu dodaj w pliku hostów serwera DB2 Connect pozycję odpowiadającą nazwie hosta lub systemu iSeries.

Na przykład:

```
9.21.15.235     nyx   # adres hosta nyx
```

gdzie *9.21.15.235* oznacza adres IP (*adres_ip*), *nyx* oznacza nazwę hosta (*nazwa_hosta*), a znak # oznacza komentarz opisujący pozycję.

Jeśli host lub system iSeries znajduje się w innej domenie niż serwer DB2 Connect, trzeba podać pełną nazwę domeny, na przykład *nyx.spifnet.ibm.com*, gdzie *spifnet.ibm.com* oznacza nazwę domeny.

Następnym etapem jest wpisanie węzła TCP/IP do katalogu.

Zadania pokrewne:

- “Ręczne konfigurowanie komunikacji TCP/IP między programem DB2 Connect a serwerem bazy danych hosta i systemu iSeries” na stronie 3
- “Wpisywanie węzła TCP/IP do katalogu” na stronie 6
- “Aktualizowanie pliku usług” na stronie 5

Aktualizowanie pliku usług

Aktualizowanie pliku usług jest częścią większego zadania polegającego na konfigurowaniu protokołu TCP/IP na serwerze DB2 Connect. Jeśli planuje się wpisanie węzła TCP/IP do katalogu przy użyciu numeru portu (*numer_portu*), należy pominąć ten etap. Aktualizacja pliku usług serwera DB2 Connect jest konieczna, aby dodać nazwę usługi połączeń i numer portu zdalnego hosta, z którym ma nastąpić połączenie.

Procedura postępowania:

Aby zaktualizować plik usług, należy za pomocą edytora tekstu dodać do pliku usług serwera DB2 Connect nazwę usługi połączeń i numer portu zdalnego hosta. Plik ten znajduje się w tym samym katalogu, co lokalny plik hostów.

Na przykład:

```
host1  3700/tcp  # port usługi połączeń DB2
```

gdzie *host1* oznacza nazwę usługi połączeń, *3700* oznacza numer portu połączenia, *tcp* oznacza protokół komunikacyjny, a znak # oznacza komentarz opisujący pozycję.

Numer portu używanego po stronie serwera DB2 Connect musi odpowiadać numerowi portu używanego w systemie hosta. Należy się także upewnić, że port, którego numer został określony, nie jest używany przez żaden inny proces. Jeśli planuje się obsługę klienta systemu

UNIX korzystającego z sieciowych usług informacyjnych NIS (Network Information Services), trzeba zaktualizować plik usług znajdujący się na serwerze głównym NIS.

Następnym etapem jest wpisanie węzła TCP/IP do katalogu.

Zadania pokrewne:

- "Wpisywanie węzła TCP/IP do katalogu" na stronie 6

Wpisywanie węzła TCP/IP do katalogu

Wpisywanie węzła TCP/IP do katalogu jest częścią większego zadania polegającego na konfigurowaniu komunikacji między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries. W celu opisania zdalnego węzła trzeba dodać pozycję do katalogu węzła serwera DB2 Connect. Pozycja ta opisuje wybrany alias - *nazwa_węzła*, nazwę hosta - *nazwa_hosta* (lub adres IP - *adres_ip*) oraz nazwę usługi - *nazwa_usługi* (lub numer portu - *numer_portu*), które to parametry będą używane przez komputer klienta do uzyskania dostępu do zdalnego hosta.

Wymagania wstępne:

Użytkownik musi posiadać uprawnienia administratora systemu (SYSADM) lub kontrolera systemu (SYSCTRL). Jeśli opcja catalog_noauth ma wartość ON, można również zalogować się do systemu bez tych poziomów uprawnień.

Procedura postępowania:

Aby wpisać węzeł TCP/IP do katalogu:

1. W przypadku systemu UNIX należy skonfigurować środowisko instancji i wywołać procesor wiersza komend DB2. Uruchom skrypt startowy w następujący sposób:

   ```
   . INSTHOME/sqllib/db2profile    (dla powłoki Bash, Bourne lub Korn)
   source INSTHOME/sqllib/db2cshrc (dla powłoki C)
   ```

   gdzie *INSTHOME* jest katalogiem głównym danej instancji.
2. Wpisz węzeł do katalogu:

   ```
   catalog tcpip node nazwa_węzła remote [nazwa_hosta|adres_ip]
      server [nazwa_usługi|numer_portu]
   terminate
   ```

   Na przykład, aby wpisać do katalogu zdalny host *nyx* w węźle o nazwie *węzeł_db2*, używając nazwy usługi *host1*:

   ```
   catalog tcpip node węzeł_db2 remote nyx server host1
   terminate
   ```

   Aby wpisać do katalogu serwer zdalny o adresie IP *9.21.15.235* w węźle o nazwie *węzeł_db2*, używając numeru portu *3700*:

   ```
   catalog tcpip node węzeł_db2 remote 9.21.15.235 server 3700
   terminate
   ```

Aby zmienić wartości ustawione za pomocą komendy **catalog node**:

1. W procesorze wiersza komend uruchom komendę **uncatalog node**:

   ```
   db2 uncatalog node nazwa_węzła
   ```
2. Wpisz ponownie węzeł do katalogu, używając poprawnych wartości.

Następnym etapem jest wpisanie bazy danych do katalogu jako bazy danych DCS.

Zadania pokrewne:

- “Konfigurowanie protokołu TCP/IP na serwerze DB2 Connect” na stronie 4
- “Wpisywanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS)” na stronie 7

Informacje pokrewne:

- “CATALOG TCPIP NODE Command” w podręczniku *Command Reference*

Wpisywanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS)

Wpisywanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS) jest częścią większego zadania polegającego na konfigurowaniu komunikacji między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries. Aby program DB2 Connect umożliwiał dostęp do zdalnej bazy danych, musi być ona wpisana do katalogu jako baza danych DCS.

Wymagania wstępne:

Identyfikator użytkownika z uprawnieniami administratora systemu (SYSADM) lub kontrolera systemu (SYSCTRL).

Procedura postępowania:

Aby wpisać zdalną bazę danych do katalogu jako bazę danych DCS:

```
catalog dcs db lokalna_nazwa_dcs as nazwa_bazy_danych
terminate
```

gdzie:

- *lokalna_nazwa_dcs* oznacza lokalną nazwę bazy danych hosta lub systemu iSeries.
- *nazwa_bazy_danych* oznacza nazwę bazy danych hosta lub systemu iSeries.

Na przykład, aby dla zdalnej bazy danych hosta lub systemu iSeries o nazwie *newyork* utworzyć lokalną nazwę bazy danych *ny* dla programu DB2 Connect:

```
catalog dcs db ny as newyork
terminate
```

Następnym etapem jest wpisanie bazy danych do katalogu.

Zadania pokrewne:

- “Wpisywanie węzła TCP/IP do katalogu” na stronie 6
- “Wpisywanie bazy danych do katalogu” na stronie 7
- “Wpisywanie węzła APPC lub APPN do katalogu” na stronie 15

Informacje pokrewne:

- “CATALOG DCS DATABASE Command” w podręczniku *Command Reference*

Wpisywanie bazy danych do katalogu

Wpisywanie bazy danych do katalogu jest częścią większego zadania polegającego na konfigurowaniu komunikacji między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries. Zanim aplikacja klienta będzie mogła uzyskać dostęp do zdalnej bazy

danych, baza danych musi zostać wpisana do katalogu w węźle hosta lub systemu iSeries oraz w każdym węźle serwera DB2 Connect, który będzie nawiązywał z nią połączenie.

Podczas tworzenia bazy danych jest ona automatycznie wpisywana do katalogu hosta lub systemu iSeries z aliasem bazy danych (*alias_bazy_danych*) takim samym jak nazwa bazy danych (*nazwa_bazy_danych*). Serwer DB2 Connect do nawiązywania połączenia ze zdalną bazą danych hosta lub systemu iSeries używa informacji zawartych zarówno w katalogu bazy danych, jak i w katalogu węzła.

Wymagania wstępne:

- Identyfikator użytkownika z uprawnieniami administratora systemu (SYSADM) lub kontrolera systemu (SYSCTRL).
- Określ następujące parametry:
  - Nazwa bazy danych (*nazwa_bazy_danych*)
  - Alias bazy danych (*alias_bazy_danych*)
  - Nazwa węzła (*nazwa_węzła*)

Procedura postępowania:

Aby wpisać bazę danych do katalogu na serwerze DB2 Connect:

1. W przypadku systemu UNIX, skonfiguruj środowisko instancji i wywołaj procesor wiersza komend DB2. Uruchom skrypt startowy w następujący sposób:

   ```
   . INSTHOME/sqllib/db2profile    (dla powłoki Bash, Bourne lub Korn)
   source INSTHOME/sqllib/db2cshrc (dla powłoki C)
   ```

   gdzie *INSTHOME* jest katalogiem głównym danej instancji.
2. Wpisz bazę danych do katalogu:

   ```
   catalog database nazwa_bazy_danych as alias_bazy_danych at
   node nazwa_węzła authentication wartość_uwierzytelnienia
   ```

   Na przykład, aby wpisać do katalogu znaną usłudze DCS bazę danych *ny*, która ma posiadać lokalny alias bazy danych *lokalny* w węźle *węzeł_db2*, wpisz następujące komendy:

   ```
   catalog database ny as lokalny at node węzeł_db2
     authentication dcs
   terminate
   ```

   Aby zmienić wartości ustawione za pomocą komendy **catalog** *database*:

   a. W procesorze wiersza komend uruchom komendę **uncatalog** *database* w następujący sposób:

      ```
      uncatalog database alias_bazy_danych
      ```

   b. Ponownie wpisz bazę danych do katalogu, używając poprawnych wartości.

Następnym etapem jest powiązanie narzędzi i aplikacji z serwerem bazy danych.

Zadania pokrewne:

- “Wpisywanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS)” na stronie 7
- “Powiązanie narzędzi i aplikacji z serwerem bazy danych hosta lub systemu iSeries” na stronie 9

Informacje pokrewne:

- “CATALOG DATABASE Command” w podręczniku *Command Reference*

Powiązanie narzędzi i aplikacji z serwerem bazy danych hosta lub systemu iSeries

Powiązanie narzędzi i aplikacji z serwerem bazy danych hosta lub systemu iSeries jest częścią większego zadania polegającego na konfigurowaniu komunikacji między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries. Po przejściu wszystkich etapów konfigurowania komunikacji między serwerem DB2 Connect a hostem lub systemem iSeries należy powiązać narzędzia i aplikacje z serwerem bazy danych hosta lub systemu iSeries.

Wymagania wstępne:

Identyfikator użytkownika z uprawnieniem BINDADD.

Procedura postępowania:

Aby powiązać narzędzia i aplikacje z serwerem bazy danych hosta lub systemu iSeries:

```
connect to alias_bazy_danych user id_użytkownika using hasło
bind ścieżka_katalogu_wiązania@ddcsmvs.lst blocking all sqlerror continue
     messages mvs.msg grant public
connect reset
```

Na przykład:

```
connect to NYC3 user mój_id_użytkownika using moje_hasło
bind ścieżka_katalogu_wiązania@ddcsmvs.lst blocking all sqlerror continue
        messages mvs.msg grant public
connect reset
```

where *ścieżka_katalogu_wiązania* oznacza katalog z plikami o rozszerzeniu .lst. Na przykład, w przypadku systemu Windows ścieżka zwykle wygląda następująco \SQLLIB\BND\.

Następnym etapem jest testowanie połączenia z hostem lub systemem iSeries.

Pojęcia pokrewne:

- "Binding utilities to the database" w podręczniku *Administration Guide: Implementation*

Zadania pokrewne:

- "Wpisywanie bazy danych do katalogu" na stronie 7
- "Testowanie połączenia z hostem lub systemem iSeries" na stronie 9

Informacje pokrewne:

- "BIND Command" w podręczniku *Command Reference*

Testowanie połączenia z hostem lub systemem iSeries

Testowanie połączenia z hostem lub systemem iSeries jest częścią większego zadania polegającego na konfigurowaniu komunikacji między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries. Po zakończeniu procesu konfigurowania komunikacji między serwerem DB2 Connect a hostem lub systemem iSeries należy przetestować połączenie po stronie zdalnej bazy danych.

Wymagania wstępne:

- Do przetestowania połączenia potrzebne będzie połączenie ze zdalną bazą danych.

- Wartości parametrów *id_użytkownika* i *hasło* muszą być poprawne w systemie, w którym odbywa się uwierzytelnianie użytkowników. Domyślnie proces uwierzytelniania odbywa się na serwerze bazy danych hosta lub systemu iSeries.

Procedura postępowania:

Aby przetestować połączenie z hostem lub systemem iSeries, należy:

1. Uruchomić menedżera bazy danych, wpisując na serwerze bazy danych hosta lub systemu iSeries komendę **db2start** (jeśli menedżer nie jest już uruchomiony).
2. Połączyć się ze zdalną bazą danych:

   ```
   connect to alias_bazy_danych user ID_użytkownika using hasło
   ```

   Można na przykład wpisać następującą komendę:

   ```
   connect to nyc3 user ID_użytkownika using hasło
   ```

Uwierzytelnianie połączenia z bazami danych hosta jest ustawiane podczas konfigurowania programu DB2 Connect.

Jeśli połączenie z bazą danych zostanie nawiązane pomyślnie, zostanie wyświetlony komunikat zawierający jej nazwę. Pobieranie danych z bazy danych powinno teraz być możliwe.

Na przykład, aby pobrać listę wszystkich nazw tabel wymienionych w tabeli katalogu systemowego, należy wpisać następującą komendę SQL:

```
select nazwa_tabeli from syscat.tables
```

Jeśli połączenie z bazą danych nie jest już potrzebne, wpisanie komendy **db2 connect reset** zakończy sesję połączenia.

Zadania pokrewne:

- “Powiązanie narzędzi i aplikacji z serwerem bazy danych hosta lub systemu iSeries” na stronie 9

Rozdział 2. Ręczne konfigurowanie komunikacji APPC

Ręczne konfigurowanie komunikacji APPC między programem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries

Połączenie APPC między serwerem DB2 Connect a bazą danych hosta lub systemu iSeries może zostać skonfigurowane ręcznie. W większości przypadków komunikacja APPC może być konfigurowana automatycznie za pomocą Asysty podczas konfigurowania.

Uwaga: Należy rozważyć możliwość przejścia do protokołu TCP/IP, ponieważ połączenie SNA może nie być obsługiwane w przyszłej edycji programu DB2 Connect. Obsługa połączenia SNA wymaga znaczącej wiedzy na temat jego konfiguracji, a w trakcie samego procesu konfiguracji łatwo jest popełnić błąd. Protokół TCP/IP jest łatwy do skonfigurowania, charakteryzuje się niższymi kosztami obsługi i umożliwia uzyskanie doskonałej wydajności.

Wymagania wstępne:

- Protokół APPC musi być obsługiwany zarówno przez serwer DB2 Connect, jak i przez hosta lub system iSeries.
- Wartości parametrów znajdujących się w arkuszu wartości parametrów APPC muszą być znane.

Ograniczenia:

Protokół SNA nie jest obsługiwany przez program DB2 Connect wersja 8.1 działający na 64–bitowych platformach systemu Windows (64-bitowa wersja systemu Windows XP i 64-bitowy serwer Windows .NET).

Procedura postępowania:

Aby ręcznie skonfigurować serwer DB2 Connect w sposób umożliwiający korzystanie z komunikacji APPC na serwerze baz danych hosta lub systemu iSeries:

1. Zaktualizuj profile APPC na serwerze DB2 Connect.
2. Wpisz węzeł APPC lub APPN do katalogu.
3. Wpisz bazę danych hosta lub systemu iSeries do katalogu jako bazę danych usługi Database Connection Service (DCS).
4. Wpisz bazę danych hosta lub systemu iSeries do katalogu.
5. Powiąż narzędzia i aplikacje z serwerem bazy danych hosta lub systemu iSeries.
6. Przetestuj połączenie z hostem lub systemem iSeries.

Zadania pokrewne:

- “Aktualizowanie profili APPC na serwerze DB2 Connect” na stronie 12
- “Wpisywanie węzła APPC lub APPN do katalogu” na stronie 15
- “Wpisywanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS)” na stronie 7
- “Wpisywanie bazy danych do katalogu” na stronie 7
- “Powiązanie narzędzi i aplikacji z serwerem bazy danych hosta lub systemu iSeries” na stronie 9
- “Testowanie połączenia z hostem lub systemem iSeries” na stronie 9

© Copyright IBM Corp. 1993-2004

- “Ręczne konfigurowanie komunikacji TCP/IP między programem DB2 Connect a serwerem bazy danych hosta i systemu iSeries” na stronie 3

Informacje pokrewne:

- “Arkusz wartości parametrów APPC” na stronie 135

Zadania konfiguracyjne

Aktualizowanie profili APPC na serwerze DB2 Connect

Aktualizowanie profili APPC na serwerze DB2 Connect jest częścią większego zadania polegającego na konfigurowaniu komunikacji APPC między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries.

Procedura postępowania:

Aby skonfigurować komunikację APPC programu DB2 Connect w celu uzyskania dostępu do serwera bazy danych zdalnego hosta lub systemu iSeries, należy zaktualizować profile APPC odpowiednie dla konfiguracji sieci:

- Skonfiguruj klienta API SNA dla serwera IBM eNetwork Communications Server for Windows.
- Skonfiguruj serwer Microsoft SNA Server.
- Skonfiguruj klienta Microsoft SNA Client.
- Skonfiguruj serwer IBM eNetwork Communications Server for AIX.
- Skonfiguruj architekturę Bull SNA for AIX.
- Skonfiguruj architekturę SNAPlus2 for HP-UX.

Następnym etapem jest wpisanie węzła APPC lub APPN do katalogu.

Zadania pokrewne:

- “Konfigurowanie klienta API SNA programu IBM eNetwork Communications Server for Windows” na stronie 12
- “Konfigurowanie programu Microsoft SNA Server” na stronie 13
- “Konfigurowanie oprogramowania Microsoft SNA Client” na stronie 13
- “Konfigurowanie pakietu IBM eNetwork Communications Server for AIX” na stronie 14
- “Konfigurowanie programu Bull SNA for AIX” na stronie 14
- “Konfigurowanie oprogramowania SNAPlus2 for HP-UX” na stronie 14
- “Wpisywanie węzła APPC lub APPN do katalogu” na stronie 15

Informacje pokrewne:

- “Produkty komunikacyjne APPC, które można skonfigurować przy użyciu Asysty podczas konfigurowania” na stronie 131

Podzadania aktualizowania profili APPC

Konfigurowanie klienta API SNA programu IBM eNetwork Communications Server for Windows

W produktach DB2 Enterprise Server Edition (ESE) for Windows and UNIX, wersja 8 oraz DB2 Connect Enterprise Edition (EE) for Windows and UNIX, wersja 8 zaprzestano obsługi następujących elementów:

- Możliwość zatwierdzania dwufazowego za pośrednictwem SNA. Aplikacje wymagające zatwierdzania dwufazowego muszą korzystać z połączeń TCP/IP. Zatwierdzanie dwufazowe za pośrednictwem połączenia TCP/IP z hostem lub z serwerem bazy danych iSeries było już dostępne w kilku poprzednich wersjach. Aplikacje hosta lub aplikacje iSeries wymagające obsługi zatwierdzania dwufazowego mogą korzystać z nowej możliwości obsługi zatwierdzania dwufazowego za pośrednictwem TCP/IP, ujętej w DB2 ESE, wersja 8.
- Aplikacje nie mogą już uzyskiwać dostępu do serwera DB2 UDB ESE w systemie UNIX lub Windows, ani do serwera DB2 Connect EE za pośrednictwem SNA. Mogą natomiast w dalszym ciągu uzyskiwać dostęp do hosta lub serwerów baz danych iSeries za pośrednictwem SNA, ale jedynie w przypadku zatwierdzania jednofazowego.

Zadania pokrewne:

- "Wpisywanie węzła APPC lub APPN do katalogu" na stronie 15

Konfigurowanie programu Microsoft SNA Server

W produktach DB2 Enterprise Server Edition (ESE) for Windows and UNIX, wersja 8 oraz DB2 Connect Enterprise Edition (EE) for Windows and UNIX, wersja 8 zaprzestano obsługi następujących elementów:

- Możliwość zatwierdzania dwufazowego za pośrednictwem SNA. Aplikacje wymagające zatwierdzania dwufazowego muszą korzystać z połączeń TCP/IP. Zatwierdzanie dwufazowe za pośrednictwem połączenia TCP/IP z hostem lub z serwerem bazy danych iSeries było już dostępne w kilku poprzednich wersjach. Aplikacje hosta lub aplikacje iSeries wymagające obsługi zatwierdzania dwufazowego mogą korzystać z nowej możliwości obsługi zatwierdzania dwufazowego za pośrednictwem TCP/IP, ujętej w DB2 ESE, wersja 8.
- Aplikacje nie mogą już uzyskiwać dostępu do serwera DB2 UDB ESE w systemie UNIX lub Windows, ani do serwera DB2 Connect EE za pośrednictwem SNA. Mogą natomiast w dalszym ciągu uzyskiwać dostęp do hosta lub serwerów baz danych iSeries za pośrednictwem SNA, ale jedynie w przypadku zatwierdzania jednofazowego.

Zadania pokrewne:

- "Konfigurowanie oprogramowania Microsoft SNA Client" na stronie 13
- "Ręczne konfigurowanie komunikacji APPC między programem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries" na stronie 11
- "Wpisywanie węzła APPC lub APPN do katalogu" na stronie 15

Konfigurowanie oprogramowania Microsoft SNA Client

W produktach DB2 Enterprise Server Edition (ESE) for Windows and UNIX, wersja 8 oraz DB2 Connect Enterprise Edition (EE) for Windows and UNIX, wersja 8 zaprzestano obsługi następujących elementów:

- Możliwość zatwierdzania dwufazowego za pośrednictwem SNA. Aplikacje wymagające zatwierdzania dwufazowego muszą korzystać z połączeń TCP/IP. Zatwierdzanie dwufazowe za pośrednictwem połączenia TCP/IP z hostem lub z serwerem bazy danych iSeries było już dostępne w kilku poprzednich wersjach. Aplikacje hosta lub aplikacje iSeries wymagające obsługi zatwierdzania dwufazowego mogą korzystać z nowej możliwości obsługi zatwierdzania dwufazowego za pośrednictwem TCP/IP, ujętej w DB2 ESE, wersja 8.
- Aplikacje nie mogą już uzyskiwać dostępu do serwera DB2 UDB ESE w systemie UNIX lub Windows, ani do serwera DB2 Connect EE za pośrednictwem SNA. Mogą natomiast w dalszym ciągu uzyskiwać dostęp do hosta lub serwerów baz danych iSeries za pośrednictwem SNA, ale jedynie w przypadku zatwierdzania jednofazowego.

Zadania pokrewne:

- “Konfigurowanie programu Microsoft SNA Server” na stronie 13
- “Wpisywanie węzła APPC lub APPN do katalogu” na stronie 15

Konfigurowanie pakietu IBM eNetwork Communications Server for AIX

W produktach DB2 Enterprise Server Edition (ESE) for Windows and UNIX, wersja 8 oraz DB2 Connect Enterprise Edition (EE) for Windows and UNIX, wersja 8 zaprzestano obsługi następujących elementów:

- Możliwość zatwierdzania dwufazowego za pośrednictwem SNA. Aplikacje wymagające zatwierdzania dwufazowego muszą korzystać z połączeń TCP/IP. Zatwierdzanie dwufazowe za pośrednictwem połączenia TCP/IP z hostem lub z serwerem bazy danych iSeries było już dostępne w kilku poprzednich wersjach. Aplikacje hosta lub aplikacje iSeries wymagające obsługi zatwierdzania dwufazowego mogą korzystać z nowej możliwości obsługi zatwierdzania dwufazowego za pośrednictwem TCP/IP, ujętej w DB2 ESE, wersja 8.
- Aplikacje nie mogą już uzyskiwać dostępu do serwera DB2 UDB ESE w systemie UNIX lub Windows, ani do serwera DB2 Connect EE za pośrednictwem SNA. Mogą natomiast w dalszym ciągu uzyskiwać dostęp do hosta lub serwerów baz danych iSeries za pośrednictwem SNA, ale jedynie w przypadku zatwierdzania jednofazowego.

Zadania pokrewne:

- “Ręczne konfigurowanie komunikacji APPC między programem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries” na stronie 11
- “Wpisywanie węzła APPC lub APPN do katalogu” na stronie 15

Konfigurowanie programu Bull SNA for AIX

W produktach DB2 Enterprise Server Edition (ESE) for Windows and UNIX, wersja 8 oraz DB2 Connect Enterprise Edition (EE) for Windows and UNIX, wersja 8 zaprzestano obsługi następujących elementów:

- Możliwość zatwierdzania dwufazowego za pośrednictwem SNA. Aplikacje wymagające zatwierdzania dwufazowego muszą korzystać z połączeń TCP/IP. Zatwierdzanie dwufazowe za pośrednictwem połączenia TCP/IP z hostem lub z serwerem bazy danych iSeries było już dostępne w kilku poprzednich wersjach. Aplikacje hosta lub aplikacje iSeries wymagające obsługi zatwierdzania dwufazowego mogą korzystać z nowej możliwości obsługi zatwierdzania dwufazowego za pośrednictwem TCP/IP, ujętej w DB2 ESE, wersja 8.
- Aplikacje nie mogą już uzyskiwać dostępu do serwera DB2 UDB ESE w systemie UNIX lub Windows, ani do serwera DB2 Connect EE za pośrednictwem SNA. Mogą natomiast w dalszym ciągu uzyskiwać dostęp do hosta lub serwerów baz danych iSeries za pośrednictwem SNA, ale jedynie w przypadku zatwierdzania jednofazowego.

Konfigurowanie oprogramowania SNAPlus2 for HP-UX

W produktach DB2 Enterprise Server Edition (ESE) for Windows and UNIX, wersja 8 oraz DB2 Connect Enterprise Edition (EE) for Windows and UNIX, wersja 8 zaprzestano obsługi następujących elementów:

- Możliwość zatwierdzania dwufazowego za pośrednictwem SNA. Aplikacje wymagające zatwierdzania dwufazowego muszą korzystać z połączeń TCP/IP. Zatwierdzanie dwufazowe za pośrednictwem połączenia TCP/IP z hostem lub z serwerem bazy danych iSeries było już dostępne w kilku poprzednich wersjach. Aplikacje hosta lub aplikacje

iSeries wymagające obsługi zatwierdzania dwufazowego mogą korzystać z nowej możliwości obsługi zatwierdzania dwufazowego za pośrednictwem TCP/IP, ujętej w DB2 ESE, wersja 8.

- Aplikacje nie mogą już uzyskiwać dostępu do serwera DB2 UDB ESE w systemie UNIX lub Windows, ani do serwera DB2 Connect EE za pośrednictwem SNA. Mogą natomiast w dalszym ciągu uzyskiwać dostęp do hosta lub serwerów baz danych iSeries za pośrednictwem SNA, ale jedynie w przypadku zatwierdzania jednofazowego.

Zadania pokrewne:

- “Ręczne konfigurowanie komunikacji APPC między programem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries” na stronie 11
- “Wpisywanie węzła APPC lub APPN do katalogu” na stronie 15

Wpisywanie węzła APPC lub APPN do katalogu

Wpisywanie węzła APPC lub APPN do katalogu jest częścią większego zadania polegającego na konfigurowaniu komunikacji APPC po stronie hosta dla programu DB2 Connect. Aby opisać zdalny węzeł, należy dodać pozycję do katalogu węzłów serwerów.

W większości wypadków trzeba dodać pozycję węzła APPC do katalogu węzłów. W przypadku 32-bitowych systemów operacyjnych Windows, można także dodać pozycję węzła APPN, jeśli węzeł lokalnego systemu SNA został skonfigurowany jako węzeł APPN.

Wymagania wstępne:

Identyfikator użytkownika z uprawnieniami administratora systemu (SYSADM) lub kontrolera systemu (SYSCTRL). Jeśli opcja catalog_noauth ma wartość ON, można również zalogować się do systemu bez tych poziomów uprawnień.

Procedura postępowania:

Aby wpisać węzeł do katalogu:

1. W przypadku systemu UNIX, skonfiguruj środowisko instancji i wywołaj procesor wiersza komend DB2. Uruchom skrypt startowy w następujący sposób:

   ```
   . INSTHOME/sqllib/db2profile    (dla powłoki Bash, Bourne lub Korn)
   source INSTHOME/sqllib/db2cshrc (dla powłoki C)
   ```

   gdzie *INSTHOME* jest katalogiem głównym danej instancji.
2. Aby wpisać węzeł APPC do katalogu, określ wybrany alias (*nazwa_węzła*), symboliczną nazwę docelową (*symboliczna_nazwa_docelowa*) i typ ochrony APPC (*typ_ochrony*), którego klient będzie używać dla połączeń APPC. Wprowadź następujące komendy:

   ```
   catalog "appc node  nazwa_węzła remote symboliczna_nazwa_docelowa
      security typ_ochrony"
   terminate
   ```

   Wielkości liter w parametrze *symboliczna_nazwa_docelowa* są rozróżniane i *muszą* dokładnie odpowiadać wielkościom liter symbolicznej nazwy docelowej zdefiniowanej uprzednio.

   Na przykład, aby wpisać do katalogu serwer zdalny baz danych przy użyciu symbolicznej nazwy docelowej *DB2CPIC* w węźle o nazwie *db2node*, korzystając z ochrony APPC typu *program*, wprowadź następujące komendy:

   ```
   catalog appc node węzeł_db2 remote DB2CPIC security program
   terminate
   ```

3. Aby wpisać węzeł APPN do katalogu, określ wybrany alias (*nazwa_węzła*), identyfikator sieci (**9**), zdalną partnerską jednostkę logiczną (**4**), nazwę programu transakcyjnego (**17**), tryb (**15**) oraz typ ochrony. Wpisz następujące komendy, podstawiając własne wartości:

```
catalog "appn node db2node network SPIFNET remote NYM2DB2
         tpname QCNTEDDM mode IBMRDB security PROGRAM"
terminate
```

Następnym etapem jest wpisanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS).

Zadania pokrewne:

- “Wpisywanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS)” na stronie 7

Wpisywanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS)

Wpisywanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS) jest częścią większego zadania polegającego na konfigurowaniu komunikacji między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries. Aby program DB2 Connect umożliwiał dostęp do zdalnej bazy danych, musi być ona wpisana do katalogu jako baza danych DCS.

Wymagania wstępne:

Identyfikator użytkownika z uprawnieniami administratora systemu (SYSADM) lub kontrolera systemu (SYSCTRL).

Procedura postępowania:

Aby wpisać zdalną bazę danych do katalogu jako bazę danych DCS:

```
catalog dcs db lokalna_nazwa_dcs as nazwa_bazy_danych
terminate
```

gdzie:

- *lokalna_nazwa_dcs* oznacza lokalną nazwę bazy danych hosta lub systemu iSeries.
- *nazwa_bazy_danych* oznacza nazwę bazy danych hosta lub systemu iSeries.

Na przykład, aby dla zdalnej bazy danych hosta lub systemu iSeries o nazwie *newyork* utworzyć lokalną nazwę bazy danych *ny* dla programu DB2 Connect:

```
catalog dcs db ny as newyork
terminate
```

Następnym etapem jest wpisanie bazy danych do katalogu.

Zadania pokrewne:

- “Wpisywanie węzła TCP/IP do katalogu” na stronie 6
- “Wpisywanie bazy danych do katalogu” na stronie 7
- “Wpisywanie węzła APPC lub APPN do katalogu” na stronie 15

Informacje pokrewne:

- “CATALOG DCS DATABASE Command” w podręczniku *Command Reference*

Wpisywanie bazy danych do katalogu

Wpisywanie bazy danych do katalogu jest częścią większego zadania polegającego na konfigurowaniu komunikacji między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries. Zanim aplikacja klienta będzie mogła uzyskać dostęp do zdalnej bazy danych, baza danych musi zostać wpisana do katalogu w węźle hosta lub systemu iSeries oraz w każdym węźle serwera DB2 Connect, który będzie nawiązywał z nią połączenie.

Podczas tworzenia bazy danych jest ona automatycznie wpisywana do katalogu hosta lub systemu iSeries z aliasem bazy danych (*alias_bazy_danych*) takim samym jak nazwa bazy danych (*nazwa_bazy_danych*). Serwer DB2 Connect do nawiązywania połączenia ze zdalną bazą danych hosta lub systemu iSeries używa informacji zawartych zarówno w katalogu bazy danych, jak i w katalogu węzła.

Wymagania wstępne:

- Identyfikator użytkownika z uprawnieniami administratora systemu (SYSADM) lub kontrolera systemu (SYSCTRL).
- Określ następujące parametry:
  - Nazwa bazy danych (*nazwa_bazy_danych*)
  - Alias bazy danych (*alias_bazy_danych*)
  - Nazwa węzła (*nazwa_węzła*)

Procedura postępowania:

Aby wpisać bazę danych do katalogu na serwerze DB2 Connect:

1. W przypadku systemu UNIX, skonfiguruj środowisko instancji i wywołaj procesor wiersza komend DB2. Uruchom skrypt startowy w następujący sposób:

   ```
   . INSTHOME/sqllib/db2profile    (dla powłoki Bash, Bourne lub Korn)
   source INSTHOME/sqllib/db2cshrc (dla powłoki C)
   ```

   gdzie *INSTHOME* jest katalogiem głównym danej instancji.
2. Wpisz bazę danych do katalogu:

   ```
   catalog database nazwa_bazy_danych as alias_bazy_danych at
   node nazwa_węzła authentication wartość_uwierzytelnienia
   ```

   Na przykład, aby wpisać do katalogu znaną usłudze DCS bazę danych *ny*, która ma posiadać lokalny alias bazy danych *lokalny* w węźle *węzeł_db2*, wpisz następujące komendy:

   ```
   catalog database ny as lokalny at node węzeł_db2
     authentication dcs
   terminate
   ```

   Aby zmienić wartości ustawione za pomocą komendy **catalog** *database*:

   a. W procesorze wiersza komend uruchom komendę **uncatalog** *database* w następujący sposób:

      ```
      uncatalog database alias_bazy_danych
      ```

   b. Ponownie wpisz bazę danych do katalogu, używając poprawnych wartości.

Następnym etapem jest powiązanie narzędzi i aplikacji z serwerem bazy danych.

Zadania pokrewne:

- “Wpisywanie bazy danych do katalogu jako bazy danych usługi Database Connection Service (DCS)” na stronie 7

- “Powiązanie narzędzi i aplikacji z serwerem bazy danych hosta lub systemu iSeries” na stronie 9

Informacje pokrewne:

- “CATALOG DATABASE Command” w podręczniku *Command Reference*

Powiązanie narzędzi i aplikacji z serwerem bazy danych hosta lub systemu iSeries

Powiązanie narzędzi i aplikacji z serwerem bazy danych hosta lub systemu iSeries jest częścią większego zadania polegającego na konfigurowaniu komunikacji między serwerem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries. Po przejściu wszystkich etapów konfigurowania komunikacji między serwerem DB2 Connect a hostem lub systemem iSeries należy powiązać narzędzia i aplikacje z serwerem bazy danych hosta lub systemu iSeries.

Wymagania wstępne:

Identyfikator użytkownika z uprawnieniem BINDADD.

Procedura postępowania:

Aby powiązać narzędzia i aplikacje z serwerem bazy danych hosta lub systemu iSeries:

```
connect to alias_bazy_danych user id_użytkownika using hasło
bind ścieżka_katalogu_wiązania@ddcsmvs.lst blocking all sqlerror continue
     messages mvs.msg grant public
connect reset
```

Na przykład:

```
connect to NYC3 user mój_id_użytkownika using moje_hasło
bind ścieżka_katalogu_wiązania@ddcsmvs.lst blocking all sqlerror continue
        messages mvs.msg grant public
connect reset
```

where *ścieżka_katalogu_wiązania* oznacza katalog z plikami o rozszerzeniu .lst. Na przykład, w przypadku systemu Windows ścieżka zwykle wygląda następująco \SQLLIB\BND\.

Następnym etapem jest testowanie połączenia z hostem lub systemem iSeries.

Pojęcia pokrewne:

- “Binding utilities to the database” w podręczniku *Administration Guide: Implementation*

Zadania pokrewne:

- “Wpisywanie bazy danych do katalogu” na stronie 7
- “Testowanie połączenia z hostem lub systemem iSeries” na stronie 9

Informacje pokrewne:

- “BIND Command” w podręczniku *Command Reference*

Testowanie połączenia z hostem lub systemem iSeries

Testowanie połączenia z hostem lub systemem iSeries jest częścią większego zadania polegającego na konfigurowaniu komunikacji między serwerem DB2 Connect a serwerem

bazy danych hosta lub systemu iSeries. Po zakończeniu procesu konfigurowania komunikacji między serwerem DB2 Connect a hostem lub systemem iSeries należy przetestować połączenie po stronie zdalnej bazy danych.

Wymagania wstępne:

- Do przetestowania połączenia potrzebne będzie połączenie ze zdalną bazą danych.
- Wartości parametrów *id_użytkownika* i *hasło* muszą być poprawne w systemie, w którym odbywa się uwierzytelnianie użytkowników. Domyślnie proces uwierzytelniania odbywa się na serwerze bazy danych hosta lub systemu iSeries.

Procedura postępowania:

Aby przetestować połączenie z hostem lub systemem iSeries, należy:

1. Uruchomić menedżera bazy danych, wpisując na serwerze bazy danych hosta lub systemu iSeries komendę **db2start** (jeśli menedżer nie jest już uruchomiony).
2. Połączyć się ze zdalną bazą danych:

   ```
   connect to alias_bazy_danych user ID_użytkownika using hasło
   ```

   Można na przykład wpisać następującą komendę:

   ```
   connect to nyc3 user ID_użytkownika using hasło
   ```

Uwierzytelnianie połączenia z bazami danych hosta jest ustawiane podczas konfigurowania programu DB2 Connect.

Jeśli połączenie z bazą danych zostanie nawiązane pomyślnie, zostanie wyświetlony komunikat zawierający jej nazwę. Pobieranie danych z bazy danych powinno teraz być możliwe.

Na przykład, aby pobrać listę wszystkich nazw tabel wymienionych w tabeli katalogu systemowego, należy wpisać następującą komendę SQL:

```
select nazwa_tabeli from syscat.tables
```

Jeśli połączenie z bazą danych nie jest już potrzebne, wpisanie komendy **db2 connect reset** zakończy sesję połączenia.

Zadania pokrewne:

- “Powiązanie narzędzi i aplikacji z serwerem bazy danych hosta lub systemu iSeries” na stronie 9

Część 2. Konfigurowanie requesterów aplikacji hosta lub systemu iSeries

© Copyright IBM Corp. 1993-2004

Rozdział 3. Konfigurowanie requesterów aplikacji w systemach OS/390 i z/OS

Konfigurowanie programu DB2 jako requestera aplikacji (dla systemów OS/390 i z/OS)

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

Jeśli program DB2 for OS/390 and z/OS działa jako requester aplikacji, może on połączyć aplikacje uruchamiane w systemie z serwerami zdalnymi baz danych DB2 Universal Database for OS/390 and z/OS, DB2 for iSeries and DB2 Server for VSE & VM, które implementują funkcję serwera aplikacji DRDA.

Requester aplikacji musi akceptować wartości RDB_NAME i wykonać ich translację na wartości SNA NETID.LUNAME lub na wartości będące adresami TCP/IP. Program DB2 for OS/390 and z/OS korzysta ze swojej bazy danych Communications Database (CDB), aby rejestrować nazwy RDB_NAME i odpowiadające im parametry sieciowe. Baza danych komunikacji CDB umożliwia przekazywanie wymaganych informacji przez requester aplikacji DB2 for OS/390 and z/OS do serwera komunikacyjnego podczas żądań kierowanych do rozproszonych baz danych za pośrednictwem połączeń SNA lub TCP/IP.

Procedura postępowania:

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

1. Zdefiniować requester aplikacji DB2 w lokalnym systemie (SNA) lub zdefiniować requester aplikacji DB2 w lokalnym systemie (TCP/IP).
2. Zdefiniować zdalne systemy.

Pojęcia pokrewne:

- “Reprezentacja danych (dla systemów OS/390 i z/OS)” na stronie 123
- “Zagadnienia związane z ochroną w requesterach aplikacji (dla systemów OS/390 i z/OS)” na stronie 109
- “DB2 for OS/390 and z/OS” na stronie 69

Zadania pokrewne:

- “Definiowanie requestera aplikacji DB2 w systemie lokalnym – SNA (dla systemów OS/390 i z/OS)” na stronie 24
- “Definiowanie requestera aplikacji DB2 w systemie lokalnym – TCP/IP (dla systemów OS/390 i z/OS)” na stronie 26
- “Definiowanie systemów zdalnych (dla systemów OS/390 i z/OS)” na stronie 27
- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemów OS/390 i z/OS)” na stronie 45

© Copyright IBM Corp. 1993-2004

Zadania konfiguracyjne

Definiowanie requestera aplikacji DB2 w systemie lokalnym — SNA (dla systemów OS/390 i z/OS)

Definiowanie systemu lokalnego jest częścią większego zadania polegającego na konfigurowaniu programu DB2 for OS/390 and z/OS jako serwera aplikacji. Każdemu programowi w sieci przypisywany jest identyfikator NETID i nazwa jednostki logicznej, tak więc requester aplikacji DB2 for OS/390 and z/OS, łącząc się z siecią, musi mieć wartość NETID.LUNAME (przypisaną przez VTAM). Ponieważ requester aplikacji DB2 for OS/390 and z/OS jest zintegrowany z lokalnym systemem zarządzania bazą danych DB2 for OS/390 and z/OS, requester aplikacji musi mieć również nazwę RDB_NAME. W publikacjach dotyczących programu DB2 for OS/390 and z/OS, nazwa RDB_NAME DB2 for OS/390 and z/OS jest określana jako nazwa *miejsca*.

Procedura postępowania:

Aby zdefiniować requester aplikacji DB2 for OS/390 and z/OS w sieci SNA, należy:

1. Wybrać nazwę jednostki logicznej dla systemu DB2 for OS/390 and z/OS. Identyfikator NETID dla systemu DB2 for OS/390 and z/OS jest pobierany automatycznie z produktu VTAM podczas uruchamiania narzędzia DDF.
2. Zdefiniować nazwę jednostki logicznej i nazwę miejsca w *programie startowym* (BSDS) produktu DB2 for OS/390 and z/OS (długość nazwy w programie DB2 for OS/390 and z/OS jest ograniczona do 16 znaków).
3. Zarejestrować wybraną nazwę jednostki logicznej w produkcie VTAM przez utworzenie definicji APPL VTAM.
4. Należy zadbać, aby opcja Extended Security (Ochrona rozszerzona) miała wartość YES.

Konfigurowanie programu startowego BSDS DDF:

Program DB2 for OS/390 and z/OS odczytuje program startowy BSDS podczas przetwarzania startowego w celu uzyskania parametrów instalacyjnych systemu. Jeden z rekordów zapisanych w programie BSDS nosi nazwę *rekordu DDF*, ponieważ zawiera informacje używane przez narzędzie DDF do połączeń z produktem VTAM. Informacje te obejmują:

- nazwę miejsca dla systemu DB2 for OS/390 and z/OS
- nazwę jednostki logicznej dla systemu DB2 for OS/390 and z/OS
- hasło używane podczas łączenia systemu DB2 for OS/390 and z/OS z VTAM.

Informacje programu BSDS DDF można dostarczać do DB2 for OS/390 and z/OS na dwa sposoby:

- Użyć panelu instalacyjnego DDF DSNTIPR podczas pierwszego instalowania programu DB2 for OS/390 and z/OS w celu dostarczenia wymaganych informacji programu BSDS DDF. Nie wspomniano tu o wielu parametrach instalacyjnych, ponieważ ważniejsze jest przekazanie wskazówek dotyczących sposobu łączenia programu DB2 for OS/390 and z/OS z produktem VTAM. Rys. 1 na stronie 25 przedstawia sposób użycia panelu instalacyjnego w celu zapisania w programie BSDS DB2 for OS/390 and z/OS nazwy miejsca NEW_YORK3, nazwy jednostki logicznej 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 1. Panel instalacyjny programu DB2 for OS/390 and z/OS o nazwie DSNTIPR.

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

  Rys. 2 przedstawia sposób zaktualizowania programu BSDS przez wprowadzenie nazwy miejsca *NEW_YORK3*, nazwy jednostki logicznej *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 2. Przykładowa definicja zestawu danych programu startowego DDF (dla VTAM).

Podczas uruchamiania programu narzędziowego DDF (automatycznego uruchamiania programu DB2 for OS/390 and z/OS lub przy użyciu komendy DB2 for OS/390 and z/OS START DDF), łączy się on z produktem VTAM i przekazuje mu nazwę jednostki logicznej oraz hasło do VTAM. Produkt VTAM rozpoznaje system DB2 for OS/390 and z/OS, porównując nazwę jednostki logicznej i hasło (jeśli jest wymagane) z wartościami zdefiniowanymi w instrukcji DB2 for OS/390 and z/OS APPL VTAM. Hasło VTAM jest używane do sprawdzenia, czy program DB2 for OS/390 and z/OS 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 programem DB2 for OS/390 and z/OS.

Jeśli system VTAM nie wymaga hasła, należy pominąć parametr PASSWORD= w programie narzędziowym obsługującym spis protokołów zmian. Brak tego parametru oznacza, że hasło VTAM nie jest wymagane.

Rejestrowanie wybranej nazwy jednostki logicznej w produkcie VTAM przez utworzenie definicji APPL VTAM:

Po zdefiniowaniu nazwy jednostki logicznej VTAM i hasła w programie DB2 for OS/390 and z/OS należy zarejestrować te wartości w produkcie VTAM. System VTAM używa instrukcji APPL, aby zdefiniować nazwy jednostek logicznych. Rys. 3 przedstawia przykładową definicję dla nazwy jednostki logicznej *NYM2DB2*.

```
 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 3. Przykładowa definicja APPL VTAM dla programu DB2 for OS/390 and z/OS.

Zadania pokrewne:

- “Definiowanie requestera aplikacji DB2 w systemie lokalnym – TCP/IP (dla systemów OS/390 i z/OS)” na stronie 26
- “Definiowanie systemów zdalnych (dla systemów OS/390 i z/OS)” na stronie 27

Informacje pokrewne:

- “Parametry instrukcji APPL systemu VTAM programu DB2 Connect” na stronie 137

Definiowanie requestera aplikacji DB2 w systemie lokalnym – TCP/IP (dla systemów OS/390 i z/OS)

Procedura postępowania:

Aby zdefiniować komunikację TCP/IP z programem DB2 for OS/390 and z/OS:

1. W programie DB2 for OS/390 and z/OS oraz w systemie partnerskim musi być włączona komunikacja TCP/IP.
2. Administrator sieci musi przypisać dwa odpowiednie numery portów TCP/IP. Domyślnie program DB2 for OS/390 and z/OS 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 program DB2 for OS/390 and z/OS.
4. Upewnij się, że opcja sprawdzonej uprzednio ochrony TCP/IP (TCP/IP already verified security) ma wartość YES.
5. Program BSDS DB2 for OS/390 and z/OS musi zawierać dodatkowe parametry. Rys. 4 przedstawia dodatkowe parametry konieczne do umożliwienia 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 4. Przykładowa definicja zestawu danych programu startowego DDF (dla TCP/IP).

Zadania pokrewne:

- “Definiowanie requestera aplikacji DB2 w systemie lokalnym – SNA (dla systemów OS/390 i z/OS)” na stronie 24
- “Definiowanie systemów zdalnych (dla systemów OS/390 i z/OS)” na stronie 27

Definiowanie systemów zdalnych (dla systemów OS/390 i z/OS)

Gdy aplikacja DB2 for OS/390 and z/OS żąda danych z systemu zdalnego, powoduje ona wyszukiwanie informacji na temat systemu zdalnego w bazie danych komunikacji (Communication Database - CDB). Baza danych CDB to grupa tabel SQL zarządzanych przez administratora systemu DB2 for OS/390 and z/OS.

Procedura postępowania:

Administrator systemu DB2 for OS/390 and z/OS może użyć poleceń SQL, aby wstawić wiersze do bazy danych CDB w celu opisania każdego potencjalnego partnera DRDA.

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 dotyczące ochrony sieci wymagane przez miejsca zdalne
- limity liczby sesji i nazwy trybów używane przy komunikacji z miejscami zdalnymi (dla połączenia SNA).

Zapełnianie bazy danych komunikacji:

Aktualizacje bazy danych komunikacji (CDB) nie są wymagane, jeśli będą używane tylko przychodzące połączenia TCP/IP z bazą danych. Jeśli więc program DB2 for OS/390 and z/OS ma być używany tylko jako serwer TCP/IP, to nie należy wypełniać bazy CDB. W takim przypadku 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 program DB2 for OS/390 and z/OS będzie używany jako requester, zawsze należy aktualizować bazę CDB. Należy wstawić wiersze do tabeli SYSIBM.LOCATIONS oraz tabeli SYSIBM.LUNAMES (dla połączeń SNA) lub SYSIBM.IPNAMES (dla połączeń TCP/IP).

Dodatkowe aktualizacje bazy danych komunikacji mogą być wymagane, jeśli użytkownik ma kontrolować wymogi dotyczące ochrony przychodzących połączeń SNA lub konwersję identyfikatorów użytkownika dla tych połączeń.

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

Obsługiwanie żądań przez bazę danych komunikacji:

Podczas wysyłania żądania program DB2 for OS/390 and z/OS używa kolumny LINKNAME tabeli katalogu SYSIBM.LOCATIONS, aby określić protokół sieciowy, który ma zostać użyty dla wychodzących połączeń z bazą danych. Aby odbierać żądania VTAM, trzeba wybrać nazwę LUNAME w panelu instalacyjnym DSNTIPR programu DB2 for OS/390 and z/OS. Aby odbierać żądania TCP/IP, trzeba wybrać port DRDA i port ponownej synchronizacji w panelu instalacyjnym DSNTIP5 programu DB2 for OS/390 and z/OS. Do przekazywania 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 zarówno protokołu SNA, jak i TCP/IP. Na przykład, jeśli w tabeli SYSIBM.LOCATIONS w kolumnie LINKNAME znajduje się wartość LU1 i wartość LU1 zdefiniowano w tabeli SYSIBM.IPNAMES i SYSIBM.LUNAMES, to protokół TCP/IP jest jedynym protokołem używanym do połączenia z jednostką LU1 z poziomu tego requestera.

Zadania pokrewne:

- “Definiowanie requestera aplikacji DB2 w systemie lokalnym – SNA (dla systemów OS/390 i z/OS)” na stronie 24

- “Definiowanie requestera aplikacji DB2 w systemie lokalnym – TCP/IP (dla systemów OS/390 i z/OS)” na stronie 26

Rozdział 4. Konfigurowanie requesterów aplikacji w systemie AS/400

Konfigurowanie programu DB2 jako requestera aplikacji – SNA (dla systemu iSeries)

System iSeries implementuje obsługę requestera aplikacji DRDA jako integralną część systemu operacyjnego iSeries. Ponieważ obsługa requestera aplikacji jest częścią systemu operacyjnego OS/400, jest ona aktywna zawsze, gdy aktywny jest system operacyjny.

Procedura postępowania:

Requester aplikacji musi mieć możliwość zaakceptowania nazwy relacyjnej bazy danych i jej translacji na parametry sieciowe. System iSeries wykorzystuje katalog relacyjnych baz danych do rejestrowania nazw relacyjnych baz danych i odpowiadających im parametrów sieciowych. Katalog ten umożliwia requesterowi aplikacji iSeries 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. Gdy program DB2 UDB for iSeries pełni rolę requestera aplikacji, może połączyć się z dowolnym serwerem aplikacji, który obsługuje sieć DRDA. Aby umożliwić requesterowi aplikacji DB2 UDB for iSeries dostęp do rozproszonych baz danych, należy wykonać następujące czynności:

- Zdefiniować requester aplikacji DB2 for iSeries w systemie lokalnym.
- Zdefiniować system zdalny.
- Zdefiniować komunikację SNA.

Pojęcia pokrewne:

- “Reprezentacja danych (dla systemu iSeries)” na stronie 123
- “Uwagi dotyczące ochrony w requesterach aplikacji (dla systemu iSeries)” na stronie 115
- “Program DB2 UDB for iSeries” na stronie 77
- “Połączenie z programem DB2 UDB przy wykorzystaniu protokołu TCP/IP (dla systemu iSeries)” na stronie 51

Zadania pokrewne:

- “Definiowanie requestera aplikacji DB2 w systemie lokalnym – SNA (dla systemu iSeries)” na stronie 32
- “Definiowanie systemu zdalnego (dla systemu iSeries)” na stronie 32
- “Definiowanie komunikacji SNA (dla systemu iSeries)” na stronie 33
- “Konfigurowanie programu DB2 jako serwera aplikacji przy użyciu architektury SNA (dla systemu iSeries)” na stronie 49

© Copyright IBM Corp. 1993-2004

Zadania konfiguracyjne

Definiowanie requestera aplikacji DB2 w systemie lokalnym — SNA (dla systemu iSeries)

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 iSeries 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.

Procedura postępowania:

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 dodawania pozycji 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)
```

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

Zadania pokrewne:

• “Definiowanie systemu zdalnego (dla systemu iSeries)” na stronie 32

Definiowanie systemu zdalnego (dla systemu iSeries)

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.

Procedura postępowania:

Aby zdefiniować zdalne bazy danych w lokalnej bazie danych, należy:

- Dodać w katalogu relacyjnej bazy danych pozycję odpowiadającą każdej zdalnej bazie danych za pomocą komendy ADDRDBDIRE lub WRKRDBDIRE.

  W przypadku komunikacji SNA można określić informacje, takie jak:

  - nazwa zdalnej bazy danych
  - nazwa miejsca zdalnego bazy danych
  - nazwa miejsca lokalnego
  - nazwa trybu użytego do nawiązania połączenia
  - identyfikator sieci zdalnej
  - nazwa urządzenia użytego do komunikacji
  - nazwa programu transakcyjnego zdalnej bazy danych.

W większości przypadków jedyną potrzebną informacją jest nazwa zdalnej bazy danych i nazwa miejsca zdalnego [1] 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 jeden opis urządzenia zawiera te samą 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 być zgodne z wartością 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 tych komplikacji, 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.

Zadania pokrewne:

- "Definiowanie komunikacji SNA (dla systemu iSeries)" na stronie 33
- "Definiowanie requestera aplikacji DB2 w systemie lokalnym – SNA (dla systemu iSeries)" na stronie 32

Definiowanie komunikacji SNA (dla systemu iSeries)

System iSeries umożliwia także konfigurację zaawansowanej komunikacji między programami (APPC), która nie obsługuje routingu sieciowego. Rozproszona baza danych iSeries działa w obu konfiguracjach.

Obsługa połączenia AnyNet w systemie iSeries umożliwia działanie aplikacji APPC w sieci TCP/IP (Transmission Control Protocol/Internet Protocol). Zamieszczone dalej przykłady dotyczą między innymi zarządzania danymi rozproszonymi (DDM), usług SNADS (Systems Network Architecture Distribution Services), alertów i tranzytów terminalu typu 5250. Aplikacje te wraz z architekturą DRDA mogą być uruchamiane bez zmian w sieci TCP/IP z paroma dodatkowymi ustawieniami. Aby określić obsługę połączenia AnyNet, należy podać wartość *ANYNW w parametrze LINKTYPE komendy CRTCTLAPPC.

Procedura postępowania:

Mechanizm APPN zapewnia obsługę sieci umożliwiającą systemowi iSeries włączenie się do sieci systemów i ich kontrolę, która nie wymaga jej obsługi tradycyjnie dostarczanej przez system mainframe. Aby skonfigurować system iSeries do obsługi sieci APPN:

1. Zdefiniuj 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 używane przez system iSeries, jeśli komputer jest węzłem końcowym

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

- sieciowe punkty kontrolne, jeśli system iSeries jest punktem końcowym.

2. Utwórz opis linii.

   Opis linii to opis połączenia fizyczną linią i opis protokołu łącza danych, używanych między systemem iSeries 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. Utwórz opis kontrolera.

   Opis kontrolera określa systemy przylegające w sieci. Wskaż użycie obsługi APPN, wybierając ustawienie APPN(*YES) przy tworzeniu opisu kontrolera. Do utworzenia opisu kontrolera służą następujące komendy:

   - Utwórz opis kontrolera (APPC) (Create controller description - CRTCTLAPPC)
   - Utwórz opis kontrolera (HOST SNA) (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. Utwórz opis klasy usług.

   Użyj opisu klasy usług, aby wybierać trasy komunikacji (grupy transmisji) i nadawać priorytety transmisji. System dostarcza pięć opisów klasy usług:

   #CONNECT
   Domyślna klasa usług.

   #BATCH
   Klasa usług dla zadań wsadowych.

   #BATCHSC
   Taka jak klasa #BATCH, ale wymagana jest ochrona łącza danych na poziomie co najmniej sieci komutacji pakietów. W sieci komutacji pakietów dane nie zawsze przechodzą przez sieć tą samą ścieżką.

   #INTER
   Klasa usług dostosowana do komunikacji interaktywnej.

   #INTERSC
   Taka jak klasa #INTER, ale wymagana jest ochrona łącza danych na poziomie co najmniej sieci komutacji pakietów.

   Utwórz inne opisy klasy usług za pomocą komendy Utwórz klasę usługi (Create Class-of-Service - CRTCOSD).

5. Utwórz opis trybu.

   Opis trybu zawiera charakterystykę sesji i liczbę sesji, które mogą być używane podczas negocjowania dozwolonych wartości między miejscem lokalnym i zdalnym. Opis trybu wskazuje także na klasę usług 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
   Taki jak tryb #BATCH, ale skojarzony opis klasy usług wymaga ochrony łącza danych na poziomie co najmniej sieci komutacji pakietów.

#INTER
Tryb dostosowany do komunikacji interaktywnej.

#INTERSC
Taki jak tryb #INTER, ale skojarzony opis klasy usług wymaga ochrony łącza danych na poziomie co najmniej 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. Utwórz opisy urządzeń.

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

7. Utwórz listę miejsc APPN.

   Jeśli wymagane są dodatkowe miejsca lokalne (nazywane w innych systemach jednostkami logicznymi) lub specjalne charakterystyki miejsc zdalnych dla sieci APPN, należy utworzyć listę miejsc w sieci APPN. Nazwa miejsca lokalnego jest nazwą punktu kontrolnego określoną w atrybutach sieciowych. Jeśli potrzebne są dodatkowe miejsca dla systemu iSeries, wymagana jest lista miejsc lokalnych w sieci APPN. 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 w sieci APPN można utworzyć za pomocą komendy Utwórz listę konfiguracji (Create Configuration List - CRTCFGL).

8. Uaktywnij (udostępnij) komunikację.

   Opis komunikacji można aktywować 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 przydatna podczas przeglądania 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 iSeries dla większości środowisk, w tym rozproszonych baz danych. Jeśli wartość domyślna jest brana dla wielkości jednostki RU, system iSeries szacuje najlepszą wartość. Jeśli system iSeries komunikuje się z innym systemem, który obsługuje pacing dostosowujący się, podane wartości pacingu stanowią tylko punkt wyjściowy. Pacing jest dostosowywany przez każdy system do jego możliwości obsługi napływających danych. W przypadku systemów, które nie obsługują pacingu dostosowywanego, wartości pacingu są negocjowane na początku sesji i pozostają niezmienione przez całą sesję.

Uwagi:

1. Opis kontrolera jest odpowiednikiem makr jednostek fizycznych w systemie IBM Network Control Program and Virtual Telecommunications Access Method (NCP/VTAM).

2. Opis urządzenia jest odpowiednikiem makra jednostki logicznej (LU) w systemie 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).

Zadania pokrewne:

- “Definiowanie requestera aplikacji DB2 w systemie lokalnym – SNA (dla systemu iSeries)” na stronie 32
- “Definiowanie systemu zdalnego (dla systemu iSeries)” na stronie 32

Rozdział 5. Konfigurowanie requesterów aplikacji w systemie VM

Konfigurowanie programu DB2 jako requestera aplikacji (dla systemu VM)

Program DB2 for VM implementuje obsługę requestera aplikacji DRDA jako integralną część adaptera zasobów znajdującego się wraz z aplikacją na maszynie wirtualnej użytkownika. Obsługi requestera aplikacji można używać nawet wtedy, gdy maszyna wirtualna lokalnych menedżerów baz danych jest nieaktywna. Obsługę requestera aplikacji DRDA można uaktywnić, wykonując instrukcję SQLINIT EXEC z argumentem protocol(auto) lub protocol(drda).

Procedura postępowania:

Jeśli program 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:

- Requester aplikacji musi mieć możliwość akceptowania wartości RDB_NAME i odwzorowywania ich na wartości SNA NETID.LUNAME. System DB2 for VM korzysta z katalogu CMS Communications Directory, aby wpisywać do katalogu nazwy RDB_NAME i odpowiadające im parametry sieciowe. Katalog Communications Directory umożliwia requesterowi aplikacji przekazywanie niezbędnych informacji SNA do systemu VTAM podczas wysyłania żądań rozproszonej bazy danych.

Wiele procesów w środowisku rozproszonych baz danych wymaga wymiany komunikatów z innymi miejscami w sieci. Aby komunikaty były wymieniane poprawnie, należy:

1. Zdefiniować requester aplikacji w systemie lokalnym.
2. Zdefiniować systemy zdalne w requesterze aplikacji.
3. Przygotować requester lub serwer aplikacji do komunikacji DRDA.

Pojęcia pokrewne:

- “DB2 for VM” na stronie 77
- “Zagadnienia związane z ochroną w requesterach aplikacji (dla systemu VM)” na stronie 118

Zadania pokrewne:

- “Definiowanie requestera aplikacji w systemie lokalnym (dla systemu VM)” na stronie 38
- “Definiowanie systemów zdalnych dla requestera aplikacji (dla systemu VM)” na stronie 39
- “Przygotowywanie requestera lub serwera aplikacji do komunikacji DRDA (dla systemu VM)” na stronie 41
- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemu VM)” na stronie 63

© Copyright IBM Corp. 1993-2004

Zadania konfiguracyjne

Definiowanie requestera aplikacji w systemie lokalnym (dla systemu VM)

Definiowanie requestera aplikacji DB2 for VM jest częścią większego zadania polegającego na skonfigurowaniu programu DB2 for VM jako requestera aplikacji. 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 on sam siebie jako celu żądań połączeń przychodzących. Tylko serwer aplikacji DB2 for VM może zaakceptować (lub odrzucić) przychodzące żądania połączeń. Dlatego requester aplikacji DB2 for VM nie identyfikuje nazw RDB_NAME i TPN dla siebie samego, tak jak to robi program DB2 dla systemów OS/290 i z/OS.

Procedura postępowania:

Należy zdefiniować requester aplikacji DB2 for VM w sieci SNA, wykonując następujące czynności:

1. Zdefiniuj nazwy bram AVS przy użyciu instrukcji definicji VTAM APPL.

   Aby wyznaczać trasę przychodzących żądań w sieci, requester aplikacji musi mieć zdefiniowane nazwy bram (na przykład nazwy jednostek logicznych). Rys. 5 ilustruje przykładową definicję bramy. Wymienione instrukcje znajdują się w maszynie wirtualnej VTAM. Gdy maszyna VTAM zostanie uruchomiona, bramy w sieci są identyfikowane, nie są jednak aktywowane, dopóki nie zostanie uruchomiona sterująca maszyna wirtualna 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 5. Przykład definicji bramy AVS.

2. Uaktywnij bramę.

   Bramę włącza się z maszyny wirtualnej AVS działającej na tym samym hoście, co requester aplikacji DB2 for VM (lub na innych hostach w ramach jednej kolekcji TSAF). Do profilu maszyny AVS należy dołączyć komendę AGW ACTIVATE GATEWAY GLOBAL lub wydać tę komendę interaktywnie z konsoli komputera AVS, aby brama była automatycznie włączana przy każdym starcie komponentu AVS.

3. Użyj 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 zapewnić obsługę wszystkich wymaganych sesji.

   Aby wyłączyć bramę, 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.
4. Sprawdź, czy identyfikator VTAM NETID podczas instalacji został zdefiniowany w systemie DB2 dla systemu DBMS VM.

   Identyfikator NETID hosta (lub innych hostów w ramach tej samej kolekcji TSAF), na którym znajduje się requester aplikacji, jest dostarczany przez produkt VTAM, gdy requester rozpoczyna pracę. Identyfikator NETID jest zapisywany w pliku CMS SNA NETID i jest przechowywany na dysku DB2 for VM, do którego dostęp jest możliwy przez requester aplikacji. Requester aplikacji korzysta z tego identyfikatora NETID w celu generowania parametru LUWID, który jest przesyłany z każdą konwersacją.

Zadania pokrewne:

- “Definiowanie systemów zdalnych dla requestera aplikacji (dla systemu VM)” na stronie 39
- “Przygotowywanie requestera lub serwera aplikacji do komunikacji DRDA (dla systemu VM)” na stronie 41

Definiowanie systemów zdalnych dla requestera aplikacji (dla systemu VM)

Definiowanie systemów zdalnych dla requestera aplikacji VM jest częścią większego zadania polegającego na konfigurowaniu programu DB2 for VM jako requestera aplikacji. Systemy zdalne muszą być zdefiniowane przez zarejestrowanie nazw jednostek logicznych, które umożliwiają systemowi VTAM odnalezienie żądanych punktów docelowych sieci. System AVS po uruchomieniu identyfikuje globalne nazwy bram (nazwy jednostek logicznych) dostępne dla routingu w sieci żądań SQL do systemu VTAM. Nazwa bramy musi być unikalna w obrębie zestawu nazw jednostek logicznych rozpoznawanego przez lokalny system VTAM, 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 zasobów VTAM.

Kiedy aplikacja DB2 for VM żąda danych z systemu zdalnego, system DB2 for VM szuka w CMS Communications Directory następujących informacji dotyczących systemu zdalnego:

- nazwa bramy (nazwa lokalnej jednostki logicznej),
- nazwa zdalnej jednostki logicznej,
- zdalna nazwa TPN,
- poziom ochrony konwersacji wymagany przez serwer aplikacji,
- identyfikator użytkownika identyfikujący requester aplikacji na serwerze aplikacji,
- hasło określające tożsamość requestera aplikacji na serwerze aplikacji,
- nazwa trybu opisująca charakterystykę sesji, która ma być używana w komunikacji z serwerem aplikacji,
- RDB_NAME.

Procedura postępowania:

Katalog komunikacji CMS jest plikiem CMS typu NAMES, który jest tworzony i zarządzany przez administratora systemu DB2 for VM.

Administrator może korzystać z opcji XEDIT, aby utworzyć ten plik i dodawać żądanie pozycji identyfikujących każdego potencjalnego partnera DRDA. Każda pozycja w katalogu jest zestawem znaczników i związanych z nimi wartości. Rys. 6 przedstawia przykładową pozycję. Podczas przeszukiwania klucz przeszukiwania jest porównywany z wartością znacznika :dbname dla każdej pozycji w pliku aż do znalezienia pasującego elementu lub do osiągnięcia końca pliku. Na przykład na Rys. 6 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 6. Przykładowa pozycja w katalogu Katalog komunikacji CMS.

Znacznik :tpn identyfikuje nazwę programu transakcyjnego uaktywniającego serwer aplikacji. Pierwsza część znacznika :luname identyfikuje bramę AVS (lokalną jednostkę logiczną) używaną do uzyskiwania dostępu do sieci SNA. Druga część identyfikuje nazwę zdalnej jednostki logicznej. Znacznik :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. Znacznik :security wskazuje poziom ochrony, który ma być używany w konwersacjach łączących requester aplikacji z serwerem aplikacji.

Katalog komunikacji CMS znajduje się na publicznym dysku systemowym dostępnym dla wszystkich requesterów aplikacji w danym systemie VM. Każdy program lub produkt wymagający zdalnego dostępu przez system VTAM może korzystać z katalogu Katalog komunikacji CMS.

Dostęp do katalogu Katalog komunikacji CMS można uzyskać na dwóch poziomach: na poziomie systemu i na poziomie użytkownika. Na przykład można utworzyć katalog na poziomie systemu na publicznym dysku systemowym dostępnym dla wszystkich requesterów aplikacji w danym systemie VM. Można również utworzyć własny katalog na poziomie użytkownika, który zastąpi istniejące pozycje lub wprowadzić nowe pozycje, których brakuje w katalogu na poziomie systemu. Najpierw przeszukiwany jest katalog na poziomie użytkownika. Jeśli przeszukiwanie nie powiedzie się, przeszukiwany jest katalog na poziomie systemu. Katalog na poziomie systemu jest rozszerzeniem katalogu na poziomie użytkownika; przeszukiwany jest tylko w sytuacji, gdy szukanych wartości nie odnaleziono w katalogu na poziomie użytkownika.

Każdy katalog jest identyfikowany dla aplikacji i uaktywniany komendą CMS SET COMDIR. Na przykład można użyć następującej sekwencji komend do identyfikowania katalogów na poziomie systemu i na poziomie użytkownika (odpowiednio na minidyskach A i S), lecz do uaktywniania w celu przeszukiwania można wybrać tylko katalog na poziomie systemu:

```
SET COMDIR FILE SYSTEM SCOMDIR NAMES S

SET COMDIR FILE USER UCOMDIR NAMES A

SET COMDIR OFF USER
```

Zadania pokrewne:

- “Definiowanie requestera aplikacji w systemie lokalnym (dla systemu VM)” na stronie 38
- “Przygotowywanie requestera lub serwera aplikacji do komunikacji DRDA (dla systemu VM)” na stronie 41

Przygotowywanie requestera lub serwera aplikacji do komunikacji DRDA (dla systemu VM)

Przygotowywanie requestera lub serwera aplikacji DB2 for VM jest częścią większego zadania polegającego na konfigurowaniu programu DB2 for VM jako requestera lub serwera aplikacji. Requester lub serwer aplikacji DB2 for VM może nie mieć zainstalowanej obsługi architektury DRDA.

Procedura postępowania:

Aby przygotować requester lub serwer aplikacji DB2 for VM do komunikacji DRDA, należy:

1. Użyj programu ARISDBMA do instalacji obsługi DRDA:
   - Użyj opcji ″ARISDBMA DRDA(ARAS=Y)″, jeśli zainstalowana jest obsługa dla requestera i serwera.
   - Użyj opcji ″ARISDBMA DRDA(AR=Y)″, jeśli zainstalowana jest tylko obsługa dla requestera.
   - Użyj opcji ″ARISDBMA DRDA(AS=Y)″, jeśli zainstalowana jest obsługa tylko dla serwera.
2. Ponownie zbudować bibliotekę ARISQLLD LOADLIB programu DB2 for VM.

Więcej informacji można znaleźć w sekcji ″Using a DRDA Environment″ książki *DB2 Server for VM System Administration*.

Część 3. Konfigurowanie serwerów aplikacji hosta lub systemu iSeries

© Copyright IBM Corp. 1993-2004

Rozdział 6. Konfigurowanie serwerów aplikacji w systemach OS/390 i z/OS

Konfigurowanie programu DB2 jako serwera aplikacji (dla systemów OS/390 i z/OS)

Obsługa serwera aplikacji w programach DB2 for OS/390 and z/OS umożliwia im działanie jako serwery requesterów aplikacji DRDA.

Procedura postępowania:

Aby skonfigurować program DB2 for OS/390 and z/OS jako serwer aplikacji:

1. Zdefiniuj serwer aplikacji w lokalnym podsystemie SNA.
2. Zdefiniuj serwer aplikacji w lokalnym podsystemie TCP/IP.

Pojęcia pokrewne:

- “Reprezentacja danych (dla systemów OS/390 i z/OS)” na stronie 123
- “DB2 for OS/390 and z/OS” na stronie 69
- “Zagadnienia związane z ochroną w serwerach aplikacji (dla systemów OS/390 i z/OS)” na stronie 93

Zadania pokrewne:

- “Definiowanie serwera aplikacji w podsystemie SNA (dla systemów OS/390 i z/OS)” na stronie 45
- “Definiowanie serwera aplikacji w lokalnym podsystemie TCP/IP (systemy OS/390 i z/OS)” na stronie 47
- “Konfigurowanie programu DB2 jako requestera aplikacji (dla systemów OS/390 i z/OS)” na stronie 23

Zadania konfiguracyjne

Definiowanie serwera aplikacji w podsystemie SNA (dla systemów OS/390 i z/OS)

Aby serwer aplikacji mógł odbierać żądania rozproszonej bazy danych, musi być zdefiniowany w lokalnym programie Communications Manager i mieć unikalną nazwę RDB_NAME. Poniższe uwagi dotyczą połączeń SNA.

Procedura postępowania:

Aby zdefiniować serwer aplikacji w podsystemie SNA, należy:

1. Wybrać nazwę jednostki logicznej i nazwę RDB_NAME, które mają być używane przez serwer aplikacji hosta DB2 UDB. Wybraną nazwę RDB_NAME dla programu DB2 UDB należy udostępnić wszystkim użytkownikom i requesterom aplikacji wymagającym połączeń z serwerem aplikacji.
2. Zarejestrować wartość NETID.LUNAME dla serwera aplikacji hosta DB2 UDB w każdym requesterze aplikacji żądającym dostępu, tak aby requester aplikacji mógł kierować żądania SNA do serwera hosta DB2 UDB. Jest to ważne nawet wtedy, gdy

© Copyright IBM Corp. 1993-2004

requester aplikacji może wykonać dynamiczny routing sieciowy, ponieważ musi on znać nazwę NETID.LUNAME przed użyciem dynamicznego routingu sieciowego.

3. Udostępnić domyślną nazwę programu transakcyjnego architektury DRDA (X'07F6C4C2') każdemu requesterowi aplikacji, ponieważ program DB2 UDB hosta korzysta z tej wartości w sposób automatyczny.
4. Dla każdej nazwy trybu żądanej przez requester aplikacji utworzyć pozycję w tabeli nazw trybów VTAM. Pozycje te opisują wielkości jednostek żądania (RU), wielkość okna pacingu i klasę usługi dla każdej nazwy trybu.
5. Zdefiniować limit liczby sesji dla requesterów aplikacji łączących się z serwerem aplikacji DB2 for OS/390 and z/OS. Instrukcja VTAM APPL definiuje domyślne limity liczby sesji dla wszystkich systemów partnerskich. Aby ustanowić unikalne wartości domyślne dla określonego partnera, można użyć tabeli SYSIBM.LUMODES bazy danych komunikacji (CDB).
6. Utworzyć pozycje w bazie danych CDB hosta DB2 UDB w celu ustalenia, które requestery aplikacji mają prawo do połączenia się z serwerem aplikacji hosta DB2 UDB. 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 atrybutów dla niektórych jednostek logicznych w sieci, gdy dla wszystkich innych są ustawiane wartości domyślne.

      Można na przykład pozwolić systemowi DALLAS (system DB2 UDB na innym hoście) na wysyłanie sprawdzonych uprzednio żądań skierowanych do rozproszonej bazy danych (LU 6.2 SECURITY=SAME), wymagając jednocześnie wysyłania haseł przez systemy menedżera bazy danych. Ponadto użytkownik może nie chcieć zapisywać pozycji w CDB dla każdego systemu menedżera bazy danych, zwłaszcza jeśli jest ich wiele. Na Rys. 7 przedstawiono sposób użycia bazy danych komunikacji do określenia ustawienia SECURITY=SAME dla systemu DALLAS przy jednoczesnym wymuszeniu opcji SECURITY=PGM dla wszystkich 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 7. Ustanawianie wartości domyślnych dla połączeń requestera aplikacji (SNA).

   b. Można użyć bazy CDB, aby indywidualnie autoryzować każdego requestera aplikacji w sieci, ustawiając bazę CDB na jeden z następujących sposobów:
      - Nie zapisuj wiersza z wartościami domyślnymi w tabeli SYSIBM.LUNAMES. Gdy nie ma wiersza z wartościami domyślnymi (wiersz zawierający pustą nazwę jednostki logicznej), program DB2 UDB hosta wymaga wiersza w tabeli SYSIBM.LUNAMES zawierającego nazwę jednostki logicznej dla każdego requestera aplikacji, który próbuje się z nim połączyć. Jeśli odpowiadający wiersz nie zostanie odnaleziony w bazie danych CDB, requesterowi aplikacji zostanie odmówione prawo dostępu.
      - Zapisz 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 program DB2 UDB hosta ogranicza dostęp do requesterów aplikacji i użytkowników identyfikowanych w

tabeli SYSIBM.USERNAMES. Można użyć tego sposobu, jeśli reguły konwersji nazw wymagają wiersza z pustą nazwą jednostki logicznej w tabeli SYSIBM.LUNAMES, ale nie zaleca się, aby program DB2 for OS/390 and z/OS używał tego wiersza do umożliwienia nieograniczonego dostępu do serwera aplikacji hosta DB2 UDB.

Na Rys. 8 nie ma wiersza zawierającego puste znaki w kolumnie LUNAME, tak więc program DB2 UDB hosta uniemożliwia dostęp do jednostek logicznych innych niż LUDALLAS lub 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 8. Identyfikowanie indywidualnych połączeń requestera aplikacji (SNA).

Zadania pokrewne:

- “Definiowanie serwera aplikacji w lokalnym podsystemie TCP/IP (systemy OS/390 i z/OS)” na stronie 47

Definiowanie serwera aplikacji w lokalnym podsystemie TCP/IP (systemy OS/390 i z/OS)

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 programu DB2 for OS/290 and z/OS musi zawierać niezbędne parametry, może być również konieczna aktualizacja bazy danych komunikacji (CDB) programu DB2 for OS/390 and z/OS.

Aktualizacje bazy danych komunikacji nie są wymagane, jeśli będą używane tylko połączenia przychodzące. Jeśli więc program DB2 for OS/390 and z/OS ma być używany tylko jako serwer, to nie trzeba wypełniać bazy danych komunikacji i mogą być użyte wartości domyślne. Poniżej przedstawiono prosty przykład aktualizacji tabeli SYSIBM.IPNAMES.

Procedura postępowania:

Aby umożliwić węzłom TCP/IP wysyłanie żądań połączeń z bazą danych, należy wprowadzić następującą komendę SQL aktualizującą daną tabelę:

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

Informacje na temat konfigurowania protokołu TCP/IP na serwerze aplikacji można znaleźć w podręczniku *DB2 for OS/390 Installation Guide*.

Zadania pokrewne:

- “Definiowanie serwera aplikacji w podsystemie SNA (dla systemów OS/390 i z/OS)” na stronie 45

Rozdział 7. Konfigurowanie serwerów aplikacji w systemie AS/400 (SNA)

Konfigurowanie programu DB2 jako serwera aplikacji przy użyciu architektury SNA (dla systemu iSeries)

Obsługa serwera aplikacji w systemie iSeries umożliwia mu działanie jako serwera dla requesterów aplikacji DRDA. Requesterem aplikacji połączonym z serwerem aplikacji DB2 Universal Database (UDB) for iSeries może być dowolny klient obsługujący protokoły DRDA.

Requester aplikacji ma dostęp do tabel zapisanych lokalnie na serwerze aplikacji DB2 UDB for iSeries. Przed uruchomieniem jakichkolwiek instrukcji SQL, requester aplikacji musi utworzyć pakiet na serwerze aplikacji DB2 UDB for iSeries. W czasie przetwarzania programu serwer aplikacji DB2 UDB for iSeries korzysta z pakietów zawierających instrukcje SQL aplikacji.

Procedura postępowania:

Aby przetwarzać żądania rozproszonej bazy danych na serwerze aplikacji iSeries, 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.

Nazywanie bazy 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 dodawania pozycji katalogu relacyjnych baz danych (Add Relational Database Directory Entry - ADDRDBDIRE) i określić *LOCAL jako miejsce zdalne.

Definiowanie serwera aplikacji w sieci:

W przypadku dostępu przy użyciu architektury SNA definiowanie serwera aplikacji dla sieci przebiega tak samo, jak definiowanie requestera aplikacji dla sieci. Dla serwera aplikacji oraz requestera aplikacji wysyłającego żądania należy utworzyć opis linii, kontrolera, urządzenia i trybu.

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

Ustawianie wielkości jednostki RU i pacingu:

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

© Copyright IBM Corp. 1993-2004

Pojęcia pokrewne:

- “Uwagi związane z ochroną w serwerach aplikacji (dla systemu iSeries)” na stronie 99
- “Program DB2 UDB for iSeries” na stronie 77

Zadania pokrewne:

- “Konfigurowanie protokołu TCP/IP na serwerze DB2 Connect” na stronie 4
- “Konfigurowanie programu DB2 jako requestera aplikacji – SNA (dla systemu iSeries)” na stronie 31

Rozdział 8. Konfigurowanie serwerów aplikacji w systemie AS/400 (TCP/IP)

Połączenie z programem DB2 UDB przy wykorzystaniu protokołu TCP/IP (dla systemu iSeries)

Temat ten zawiera podsumowanie informacji dostępnych w podręczniku *DB2 for AS/400 Distributed Database Programming* opisującym konfigurowanie programu DB2® UDB for iSeries jako:

- requestera aplikacji DRDA® korzystającego z komunikacji wychodzącej TCP/IP,
- serwera aplikacji DRDA korzystającego z komunikacji przychodzącej TCP/IP.

Zasady są identyczne z tymi, które przedstawiają sekcje ″Konfigurowanie programu DB2 UDB for iSeries™ jako requestera aplikacji przy użyciu architektury SNA″ i ″Konfigurowania programu DB2 UDB for iSeries jako serwera aplikacji przy użyciu architektury SNA″, ale kolejne kroki konfigurowania komunikacji są znacznie prostsze.

Uwagi:

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

Podsumowanie informacji na temat programu DB2 UDB for iSeries:

Podręcznik *DB2 for AS/400 Distributed Database Programming* zawiera następujące sekcje, które warto przeczytać:

- Distributed Relational Database Processing
- DRDA and CDRA Support
- Configuring a Communications Network using TCP/IP
- DRDA Security using TCP/IP
- Work Management for DRDA Use with TCP/IP
- Setting up the TCP/IP Server
- Managing a TCP/IP Server
- Factors that Affect Blocking for DRDA
- Handling Connection Request Failures for TCP/IP
- Starting a Service Job for a TCP/IP Server
- Cross-Platform Access Using DRDA.

Dodatkowo należy znać:

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

© Copyright IBM Corp. 1993-2004

Konfigurowanie i korzystanie z serwera TCP/IP DRDA programu DB2 UDB for iSeries:

Konfigurowanie serwera TCP/IP DRDA programu DB2 UDB for iSeries zapewnia, 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 uruchamiania serwera 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 CL:

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

Można sprawdzić, czy serwer jest uruchomiony, korzystając z następującej komendy:

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

Spowoduje ona wyświetlenie przewijanej listy 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 nasłuchujące żądań połączeń DRDA i DDM jest aktywne. Zadanie to przydziela pracę zadaniom QRWTSRVR w miarę otrzymywania żądań połączeń.

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).

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

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

gdzie określona godzina jest wcześniejsza niż godzina nawiązania połączenia. Zostanie wyświetlona przewijana 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 03/30/01 at 15:57:38.
```

Nazwa zadania przydaje się przy przeglądaniu protokołu zadań aktywnych. Jest również przydatna przy uruchomieniu 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 debugowania, należy wykonać komendę STRDBG:

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

W pewnych sytuacjach serwer DRDA zapisuje protokół zadania prestartu 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 zapisany protokół zadania po zakończeniu zadania, należy wykonać następującą komendę:

```
WRKJOB identyfikatorużytkownika/QPRTJOB
```

gdzie identyfikatorużytkownika to identyfikator użytkownika, przy użyciu którego nawiązano połączenie (w przykładzie powyżej jest to SRR).

Spowoduje to wyświetlenie listy zadań, z której można wybrać jedno zadanie lub opcję menu dla pojedynczego zadania. Należy wybrać opcję 4, Work with spooled files (Praca z plikami buforowymi), aby odnaleźć zachowany protokół zadania. Jeśli w kolejce jest więcej plików buforowych, 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 debugowania:

```
CPI4329    Information   00    03/30/01   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
  iSeries SQL Programming book.
```

Rysunek 9. Przykładowy komunikat optymalizatora zapytań.

Konfigurowanie klienta TCP/IP DRDA programu DB2 UDB for iSeries:

Najważniejszą sprawą przy używaniu programu DB2 UDB for iSeries jako requestera aplikacji DRDA, oprócz zagadnień ochrony omówionych w następnej sekcji, jest dodanie pozycji dla zdalnego serwera aplikacji do katalogu RDB. Jest to wykonywane podobnie jak opisano w poprzednim rozdziale dotyczącym komunikacji SNA. Jednak zamiast parametrów APPC, takich jak nazwa zdalnej jednostki logicznej i nazwa programu transakcyjnego, istnieją dwa parametry protokołu TCP/IP: nazwa hosta zdalnego lub jego adres IP i numer portu lub nazwa usługi. Drugi element parametru miejsca zdalnego może być określony jako *SNA (domyślnie) lub *IP (aby wskazać, że w połączeniu będzie używany protokół TCP/IP).

Uwagi dotyczące ochrony podczas korzystania z architektury DRDA używającej protokołu TCP/IP:

Serwer DRDA z rodzimym protokołem TCP/IP nie używa usług ochrony komunikacji OS/400® i takich pojęć, jak urządzenia komunikacyjne, tryby, atrybuty miejsc chronionych i

poziomy ochrony konwersacji, które są powiązane z komunikacją APPC. Dlatego ustawienia ochrony dla protokołu TCP/IP są zupełnie inne.

W aktualnej wersji implementacji architektury DRDA dla programu DB2 UDB for iSeries wykorzystującej protokół TCP/IP obsługiwane są dwa rodzaje mechanizmów ochrony:

1. Tylko identyfikator użytkownika.
2. Identyfikator użytkownika z hasłem.

W przypadku serwera aplikacji (AS) DB2 UDB for iSeries, domyślną ochroną jest identyfikator użytkownika z hasłem. Po zainstalowaniu systemu przychodzące żądania połączenia TCP/IP muszą mieć hasło powiązane z identyfikatorem użytkownika, który uruchomił zadanie serwera. Aby określić, że hasło nie jest wymagane, można użyć komendy CHGDDMTCP. Aby dokonać tej zmiany, należy wpisać komendę CHGDDMTCPA PWDRQD(*NO). Aby użyć tej komendy, należy mieć uprawnienia specjalne *IOSYSCFG.

W przypadku requestera aplikacji (AR) DB2 UDB for iSeries istnieją dwie metody, których można użyć do przesłania hasła z identyfikatorem użytkownika wraz z żądaniem nawiązania połączenia TCP/IP. Jeśli nie można użyć żadnej z nich, zostanie wysłany tylko identyfikator użytkownika.

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

```
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 identyfikatora użytkownika i hasła mogą być zawarte w zmiennych języka bazowego.

Inną metodą dostarczenia hasła dla 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 z wykorzystaniem protokołu TCP/IP program DB2 UDB for iSeries 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 pozycji autoryzacji, jako identyfikator 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 wartość ’1’. Wartością domyślną jest ’0’. Aby dokonać zmiany, należy wpisać:

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

Składnia komendy ADDSVRAUTE jest następująca:

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

Parametr USRPRF określa profil użytkownika, przy użyciu którego uruchomiono zadanie requestera aplikacji. Parametr SERVER określa nazwę zdalnej relacyjnej bazy danych, a parametr USRID określa profil użytkownika, przy użyciu którego uruchomiono zadanie serwera. Parametr PASSWORD określa hasło dla profilu użytkownika na serwerze.

Uwaga: Nazwa relacyjnej bazy danych (RDB) musi koniecznie zostać określona w parametrze SERVER wielkimi literami.

Jeśli parametr USRPRF zostanie pominięty, domyślnie przyjęty będzie profil użytkownika, przy użyciu którego uruchomiono komendę ADDSVRAUTE. Jeśli parametr USRID zostanie pominięty, domyślnie przyjęta zostanie wartość parametru USRPRF. Jeśli pominięty jest parametr PASSWORD lub wartość QRETSVRSEC wynosi 0, w pozycji nie będzie zachowane żadne hasło, a przy próbie połączenia z wykorzystaniem pozycji jako mechanizm ochrony użyty będzie tylko identyfikator użytkownika.

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

Jeśli dla relacyjnej bazy danych istnieje pozycja na liście autoryzowanych użytkowników i używana jest forma USER/USING instrukcji CONNECT, używana jest ta druga opcja.

Pojęcia pokrewne:

- “Reprezentacja danych (dla systemu iSeries)” na stronie 123
- “Uwagi związane z ochroną w serwerach aplikacji (dla systemu iSeries)” na stronie 99
- “Uwagi dotyczące ochrony w requesterach aplikacji (dla systemu iSeries)” na stronie 115
- “Program DB2 UDB for iSeries” na stronie 77

Zadania pokrewne:

- “Konfigurowanie programu DB2 jako serwera aplikacji przy użyciu architektury SNA (dla systemu iSeries)” na stronie 49
- “Konfigurowanie programu DB2 jako requestera aplikacji – SNA (dla systemu iSeries)” na stronie 31

Rozdział 9. Konfigurowanie serwerów aplikacji w systemie VSE

Konfigurowanie programu DB2 jako serwera aplikacji (dla systemu VSE)

Obsługa serwera aplikacji dla systemu DB2 for VSE umożliwia systemowi 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 z/OS and OS/390
- Requester DB2
- Requester DB2 UDB for iSeries
- Dowolny requester aplikacji z rodziny DB2 w tym także DB2 CONNECT lub dowolny inny produkt, który obsługuje protokoły requestera aplikacji DRDA i może połączyć się z serwerem aplikacji DB2 for VSE.

Procedura postępowania:

Aby nawiązać połączenie sieciowe z serwerem aplikacji VSE:

1. Uruchom sesje CICS LU 6.2 z systemami zdalnymi.
2. Zdefiniuj serwer aplikacji VSE.
3. Przygotuj i uruchom serwer aplikacji DB2 for VSE.

Pojęcia pokrewne:

- “Zagadnienia związane z ochroną w serwerach aplikacji (dla systemu VSE)” na stronie 104
- “Program DB2 for VSE” na stronie 88

Zadania pokrewne:

- “Uruchamianie sesji CICS LU 6.2 (dla systemu VSE)” na stronie 57
- “Definiowanie serwera aplikacji (dla systemu VSE)” na stronie 61
- “Przygotowywanie i uruchamianie serwera aplikacji DB2 (dla systemu VSE)” na stronie 61

Informacje pokrewne:

- “Lista kontrolna włączania serwera aplikacji DB2 (dla systemu VSE)” na stronie 131

Zadania konfiguracyjne

Uruchamianie sesji CICS LU 6.2 (dla systemu VSE)

Uruchamianie sesji CICS LU 6.2 jest częścią większego zadania polegającego na konfigurowaniu programu DB2 for VSE jako serwera aplikacji. Serwer aplikacji DB2 for VSE komunikuje się z requesterem aplikacji przez połączenia CISC LU 6.2. Partycja CICS użyta w tym celu musi mieć połączenia jednostki logicznej LU 6.2 z systemami zdalnymi wyposażonymi w aktywne requestery aplikacji.

© Copyright IBM Corp. 1993-2004

Procedura postępowania:

Aby uruchomić sesję CICS LU 6.2:

1. Zainstaluj moduły wymagane dla ISC.

   Do systemu należy włączyć następujące moduły, korzystając z tabeli inicjowania systemu (SIT) lub nadpisań podczas inicjowania:

   - Programy EXEC interfejsu (należy wybrać ustawienie EXEC=YES lub zostawić wartość domyślną).
   - Programy komunikacji między systemami (należy wybrać ustawienie ISC=YES).
   - Program sterowania terminalem wygenerowany przez ustawienie DFHSG PROGRAM=TCP. Wymagane jest podanie wersji ACCMETH=VTAM, CHNASSY=YES i VTAMDEV=LUTYPE6.

2. Zainstaluj CICS Restart Resynchronization Support (obsługę resynchronizacji ponownego uruchomienia CICS).

   Jeśli podczas instalowania systemu CICS nie włączono opcji CICS Restart Resynchronization Support (obsługa resynchronizacji ponownego uruchomienia CICS), zaktualizuj poniższe tabele CICS, aby umożliwić użycie narzędzia obsługującego resynchronizację ponownego uruchomienia CICS:

```
DFHJCT    Tabela sterująca kroniki

          Kronika wykorzystywana przez protokół systemowy CICS musi
          zostać zdefiniowana w parametrze DFHJCT przez określenie ustawienia
          JFILEID=SYSTEM
          w makrze DFHJCT TYPE=ENTRY.

DFHPCT    Tabela sterująca programu

          Aby utworzyć pozycję DFHPCT w celu użycia narzędzia CICS Restart
          Resynchronization, wpisz:

              DFHPCT TYPE=GROUP,FN=RMI

DFHPPT    Tabela programu przetwarzania

          Aby utworzyć pozycję DFHPPT w celu użycia narzędzia 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 określonego w makrze DFHJCT
          TYPE=INITIAL definiującej zestaw danych kroniki protokołu
          systemowego CICS.
```

Rysunek 10. Tabele, które należy zaktualizować w celu włączenia możliwości resynchronizacji ponownego uruchomienia CICS.

3. Zdefiniuj system CICS dla VTAM for VSE.

   W celu obsługi połączeń LU 6.2 należy zdefiniować system CICS w systemie VTAM for VSE jako główny węzeł aplikacji VTAM. Nazwa głównego węzła zakodowana w instrukcji APPL VTAM jest identyfikatorem APPLID partycji CICS określonej w tabeli SIT przez parametr APPLID. Jest to nazwa jednostki logicznej używanej przez system

VTAM (a więc przez partnerów komunikacji CICS) w celu identyfikacji systemu CICS. Patrz Rys. 11.

```
         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 11. Przykładowa definicja APPL VTAM dla systemu CICS.

AUTH=(ACQ,SPO,VPACE)
ACQ umożliwia systemowi CICS uzyskanie sesji LU 6.2.

SPO umożliwia systemowi CICS wydanie komendy MODIFY vtamname USERVAR.

VPACE umożliwia pacing przepływu danych między systemami.

ESA=30
Opcja ta określa liczbę jednostek adresowanych w sieci, dla których system CICS może uruchomić sesje. Liczba odzwierciedla całkowitą liczbę sesji równoległych dla tego systemu CICS.

PARSESS=YES
Określa obsługę sesji równoległych LUTYPE6.

SONSCIP=YES
Określa obsługę SON (powiadomienie o niedoborze sesji). Obsługa SON umożliwia systemowi CICS odzyskanie w niektórych przypadkach nieudanej sesji bez konieczności interwencji operatora.

APPC=NO
Jest niezbędne, aby system CICS mógł korzystać z makr VTAM. System CICS nie obsługuje makroinstrukcji APPCCMD.

Uwaga: Określenie SYNCLVL=SYNCPT nie jest konieczne, ponieważ zostało wprowadzone ustawienie APPC=NO. Serwer CICS zarządza wszystkimi działaniami z poziomu punktu synchronizacji SYNCPT dla rozproszonych jednostek pracy.

4. Zdefiniuj połączenia z systemami zdalnymi, używając protokołu LU 6.2.
   a. Zdefiniuj w systemie CICS wszystkie zdalne jednostki logiczne.

      Aby zdefiniować wszystkie zdalne jednostki logiczne przy użyciu komendy CONNECTION w RDO (bezpośrednie definiowanie zasobów):

      - Określ nazwę jednostki logicznej w parametrze NETNAME.
      - Wybierz ustawienie PROTOCOL=APPC, aby używane były protokoły jednostki logicznej LU 6.2.
      - Wybierz ustawienie AUTOCONNECT=YES i INSERVICE=YES, aby połączenie po zainstalowaniu zostało uaktywnione automatycznie i aby sesje rozpoczęły się automatycznie.

- Określ ochronę na poziome konwersacji, używając parametru ATTACHSEC. ATTACHSEC=IDENTIFY jest minimalnym poziomem ochrony wymaganym przez architekturę DRDA.
- Określ ochronę na poziomie sesji, używając parametru BINDPASSWORD. Wartością domyślną jest brak ochrony na poziomie sesji.

b. Zdefiniuj grupy sesji LU 6.2 z systemem zdalnym.

   W przypadku każdego połączenia zdefiniowanego powyżej połączenia zdefiniuj grupy sesji równoległych dla każdego połączenia ze zdalną jednostką logiczną przy użyciu komendy CEDA DEFINE SESSIONS:

   - Określ nazwę połączenia (zdefiniowaną powyżej) w parametrze CONNECTION.
   - Określ pozycję tabeli logmode VTAM w parametrze MODENAME.
   - Używaj parametru MAXIMUM w celu określenia:
     – maksymalnej liczby sesji
     – maksymalnej liczby sesji, które mają być obsługiwane jako zwycięzcy rywalizacji.

     Określić wartości używane przez oprogramowanie komunikacyjne requestera aplikacji DRDA.

   Uwaga: 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. Gdy połączenia ze strony użytkowników zdalnych mogą być pomyślnie nawiązywane, należy dopasować te parametry w celu określenia ich wartości optymalnych.

c. Zdefiniuj identyfikatory użytkowników i hasła do systemu CICS.

   Zdefiniuj wszystkich użytkowników w tabeli logowania do systemu CICS (DFHSNT). Można sprawdzić poprawność identyfikatorów użytkowników, wykonując komendę logon CESN na terminalu CICS. Lokalne zalogowanie się 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 - program obsługi uaktywniania CICS TRUE
   5) ARICDRAD - 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:

   - Użyj parametru TRANSACTION, aby podać nazwę TPN.
   - Określ ustawienie PROGRAM=ARICAXED, aby określić fazę.
   - Użyj parametru XTRANID, aby podać drugą szesnastkową nazwę transakcji.

   W tym czasie zdefiniuj również transakcje DAXP i DAXT, określając ustawienie PROGRAM=ARICDAXD.

Szczegółowe informacje dotyczące definiowania i nawiązywania połączeń CICS LU 6.2 z systemami zdalnymi można znaleźć w podręczniku *CICS on Open Systems: Intercommunication Guide*.

Zadania pokrewne:

- "Definiowanie serwera aplikacji (dla systemu VSE)" na stronie 61

Definiowanie serwera aplikacji (dla systemu VSE)

Definiowanie serwera aplikacji VSE jest częścią większego zadania polegającego na skonfigurowaniu programu DB2 for VSE jako serwera aplikacji.

Procedura postępowania:

Aby zdefiniować serwer aplikacji VSE:

1. Zaktualizuj katalog DBNAME w systemie DB2 for VSE.

   Do katalogu DBNAME dodaj pozycję dla każdej transakcji zdefiniowanej powyżej przy użyciu komendy CEDA DEFINE TRANSACTION. Gdy sesje LU 6.2 zostaną uruchomione, zdalny requester aplikacji może rozpocząć konwersację z serwerem aplikacji DB2 for VSE. Przydziela on konwersację jednostki logicznej 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, aby requester aplikacji mógł mieć do niej dostęp. Administrator bazy danych DB2 for VSE jest odpowiedzialny za aktualizację katalogu DBNAME i informowanie użytkowników zdalnych o odwzorowaniach typu TPN-serwer.

   Nazwa TPN i odpowiadająca jej nazwa serwera (nazwa bazy danych zdefiniowana w katalogu DBNAME) muszą być zidentyfikowane w requesterze aplikacji.

   - Requester aplikacji używa nazwy TPN do inicjowania 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 podręcznikach *DB2 Server for VSE System Administration* i *DB2 Server for VSE & VM Database Administration*.

Zadania pokrewne:

- "Uruchamianie sesji CICS LU 6.2 (dla systemu VSE)" na stronie 57
- "Przygotowywanie i uruchamianie serwera aplikacji DB2 (dla systemu VSE)" na stronie 61

Przygotowywanie i uruchamianie serwera aplikacji DB2 (dla systemu VSE)

Przygotowywanie i uruchamianie serwera aplikacji DB2 for VSE jest częścią większego zadania polegającego na konfigurowaniu programu DB2 for VSE jako serwera aplikacji.

Procedura postępowania:

Przygotowanie i uruchomienie serwera aplikacji DB2 for VSE

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 jest to konieczne, wykonaj transakcję DAXP, aby podać domyślne hasło i język, które będą używane po włączeniu obsługi CICS TRUE dla konkretnego systemu. Więcej szczegółów można znaleźć w podręczniku *DB2 Server for VSE & VM Operation*.
4. Uruchom system 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.
   - Wybierz ustawienie SYNCPNT=Y, aby włączyć obsługę rozproszonej jednostki pracy.
5. Wszyscy użytkownicy zdalni muszą mieć nadane przez serwer DB2 for VSE autoryzacje o różnych poziomach.

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 zostaje zwiększony o jeden (sprawdzany przez uruchomienie komendy CEMT I PR(ARICAXED)).
- Aby upewnić się, że identyfikator użytkownika zdalnego jest ustalony w tabeli logowania do systemu programu CICS, należy lokalnie zalogować się do systemu przy użyciu transakcji CESN z hasłem i identyfikatorem użytkownika zdalnego. Lokalne zalogowanie się do systemu musi się powieść.
- Jeśli serwer DB2 for VSE działa i aplikacja najpierw wykonuje czynności związane z rozproszoną jednostką pracy DRDA-2, obsługa TRUE dla serwera zostanie włączona 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 system DRDA odbierze kod rozpoznania X'08063426' lub X'FFFE0101', może to oznaczać, że serwer CICS nie może udostępnić więcej sesji. Niemożliwość udostępnienia większej ilości sesji może wiązać się z sytuacją, gdy wszystkie sesje są używane albo przeznaczone do zwolnienia, ale wykonywanie komendy UNBIND jeszcze się nie zakończyło. System CICS nie może udostępnić więcej sesji, jeśli występuje wiele jednoczesnych transakcji przychodzących, które trwają krótko. W takim wypadku należy zwiększyć liczbę sesji określoną w parametrze komendy MAXIMUM CEDA DEFINE SESSION, aby obliczyć liczbę sesji przeznaczonych do zwolnienia (przy użyciu komendy UNBIND), ale wykonywanie komendy UNBIND jeszcze nie zostało zakończone.

Zadania pokrewne:

- "Uruchamianie sesji CICS LU 6.2 (dla systemu VSE)" na stronie 57
- "Definiowanie serwera aplikacji (dla systemu VSE)" na stronie 61

Rozdział 10. Konfigurowanie serwerów aplikacji w systemie VM

Konfigurowanie programu DB2 jako serwera aplikacji (dla systemu VM)

Obsługa serwera aplikacji w systemie DB2 for VM pozwala systemowi 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 z/OS and OS/390
- Requester programu DB2 Universal Database for iSeries
- Requester DB2 for AIX
- Dowolny requester aplikacji rodziny DB2, w tym także DB2 CONNECT lub dowolny inny produkt obsługujący protokoły requesterów aplikacji DRDA, które mogą połączyć się z serwerem aplikacji DB2 for VM.

W wypadku 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 nawiązaniem połączenia requester aplikacji musi utworzyć pakiet zawierający instrukcje aplikacji SQL na serwerze aplikacji DB2 for VM.

Procedura postępowania:

Aby przetwarzać żądania rozproszonej bazy danych pochodzące z serwera aplikacji DB2 for VM:

1. Zdefiniuj serwer aplikacji.
2. Przygotuj requester aplikacji lub serwer aplikacji DB2 for VM.

Pojęcia pokrewne:

- “Zagadnienia związane z ochroną w serwerach aplikacji (dla systemu VM)” na stronie 101
- “DB2 for VM” na stronie 77
- “Reprezentacja danych (dla systemu VM)” na stronie 126

Zadania pokrewne:

- “Definiowanie serwera aplikacji (dla systemu VM)” na stronie 63
- “Przygotowywanie requestera lub serwera aplikacji do komunikacji DRDA (dla systemu VM)” na stronie 41
- “Konfigurowanie programu DB2 jako requestera aplikacji (dla systemu VM)” na stronie 37

Zadania konfiguracyjne

Definiowanie serwera aplikacji (dla systemu VM)

Definiowanie serwera aplikacji jest częścią większego zadania polegającego na konfigurowaniu programu DB2 for VM jako serwera aplikacji. Aby serwer aplikacji mógł odbierać żądania rozproszonej bazy danych, musi on być zdefiniowany w lokalnym

© Copyright IBM Corp. 1993-2004

podsystemie komunikacji i musi mieć przypisaną unikalną nazwę RDB_NAME. Wartość RDB_NAME jest dostarczana przy użyciu polecenia SQLSTART EXEC jako parametr DBNAME.

Procedura postępowania:

Aby zdefiniować serwer aplikacji:

1. Zdefiniuj serwer aplikacji programu DB2 for VM na potrzeby sieci SNA po wybraniu nazwy bramy oraz wartości RDB_NAME dla serwera aplikacji DB2 for VM. Wybrana wartość RDB_NAME musi być przekazana wszystkim użytkownikom (requesterowi aplikacji), którzy mogą wymagać połączenia z serwerem aplikacji DB2 for VM.

   Identyfikator NETID jest definiowany w produkcie VTAM jako parametr startowy i wszystkie rozproszone żądania pochodzące z requestera aplikacji są poprawnie kierowane do tego produktu. Identyfikator NETID nie jest ustawiany przez serwer aplikacji DB2 for VM.

   Serwer aplikacji DB2 for VM nie określa bramy, która ma być używana do kierowania żądań przychodzących z requestera aplikacji. Zadaniem tym steruje zawsze requester aplikacji. W przypadku requestera aplikacji DB2 for VM, Katalog komunikacji CMS określa go za pomocą znaczników :luname i :tpn.

   Aby serwer aplikacji DB2 for VM mógł obsługiwać działanie rozproszonej jednostki pracy, requester aplikacji musi wybrać tę bramę AVS, która została zdefiniowana w produkcie VTAM za pomocą parametru SYNCLVL=SYNCPT. Sprawdź, czy brama AVS została zdefiniowana tak, aby mogła obsługiwać rozproszone jednostki pracy.
2. Utwórz serwer odtwarzania CRR, który służy do zarządzania działaniem rozproszonej jednostki pracy dla serwerów aplikacji DB2 w ramach tego systemu VM. Aby to zrobić, należy postępować zgodnie z instrukcjami poinstalacyjnego ładowania dostarczonych przez IBM serwerów i pul plików. Polega to między innymi na zdefiniowaniu serwera CRR (VMSERVR) puli pliku CRR (VMSYSR). Sprawdź, czy podczas uruchamiania serwera odtwarzania CRR nazwa LUNAME jest równa nazwie bramy AVS, dla której określono parametr SYNCLVL=SYNCPT.
3. Sprawdź, czy katalog CP dla komputera serwera aplikacji zawiera instrukcję IUCV *IDENT. Identyfikuje ona serwer jako zasób globalny.
4. Dla każdej nazwy trybu żądanej przez requester aplikacji utwórz pozycję w tabeli trybów VTAM. Pozycje te opisują charakterystykę sesji, np. wielkość RU, zliczanie pacingu i klasa usług dla danej nazwy trybu.
5. Zdefiniuj limit liczby sesji dla requesterów aplikacji łączących się z serwerem aplikacji DB2 for VM. Instrukcja VTAM APPL definiuje domyślne limity liczby sesji dla wszystkich systemów partnerskich. Aby ustanowić unikalne wartości domyślne dla określonego partnera, użyj komendy AGW CNOS z maszyny wirtualnej AVS działającej na serwerze aplikacji. (Requester aplikacji zwykle żąda określenia limitów liczby sesji).

   Po wybraniu wielkości RU, limitów sesji i zliczania pacingu należy rozważyć wpływ tych wartości na pulę IOBUF VTAM.

Odwzorowywanie nazwy serwera na identyfikator RESID:

Identyfikator zasobu (RESID) jest terminem systemu VM określającym nazwę programu transakcyjnego. W środowisku VM jest on zwykle definiowany jako nazwa alfanumeryczna o długości wynoszącej najwyżej 8 bajtów. Aby ułatwić administrację, zwykle definiuje się identyfikator RESID identyczny z nazwą serwera. Rys. 12 na stronie 65 przedstawia przykładowy plik nazw RESID.

Więcej informacji na temat pozycji katalogu informacyjnego definiującej wartości dbname i RESID (jako nazwy TPN) można znaleźć w sekcji ″Przykład pozycji katalogu komunikacyjnego bez hasła″ będącej częścią tematu *Uwagi dotyczące ochrony requesterów*

aplikacji (dla systemu VM). Jeśli nazwa serwera aplikacji nie może być taka sama jak identyfikator RESID, serwer aplikacji DB2 for VM w celu dokonania odwzorowania korzysta z pliku RESID NAMES.

```
 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 12. Przykład pliku nazw RESID.

Odwzorowanie jest niezbędne, gdy:

- używany jest identyfikator RESID inny niż nazwa serwera,
- używana jest nazwy serwera dłuższa niż 8 bajtów,
- używany jest identyfikator RESID z 4-bajtową wartością szesnastkową, taką jak domyślna wartość TPN DRDA X'07F6C4C2'.

Podczas instalacji domyślnie używana jest nazwa serwera określona w programie SQLDBINS EXEC jako RESID. Aby utworzyć pozycję odwzorowywania w pliku RESID NAMES, należy określić parametr RESID w ustawieniu SQLDBINS.

Jeśli baza danych zostanie uruchomiona przy użyciu komendy SQLSTART DB(nazwa_serwera), system DB2 for VM szuka odpowiedniego identyfikatora RESID i informuje system VM, że jest to zasób, który będzie kontrolowany przez system VM. Jeśli pozycja nie zostanie odnaleziona w pliku RESID NAMES, system DB2 for VM zakłada, że identyfikator RESID jest identyczny z nazwą serwera i przekazuje tę informację systemowi VM.

Więcej informacji na temat dokonywanego po instalacji ładowania dostarczonych przez IBM serwerów i pul plików można znaleźć w podręczniku *VM/ESA Installation Guide*.

Więcej informacji dotyczących tematu ″Korzystanie ze środowiska DRDA″ można znaleźć w podręczniku *DB2 Server for VM System Administration*.

Pojęcia pokrewne:

- “Zagadnienia związane z ochroną w serwerach aplikacji (dla systemu VM)” na stronie 101
- “Reprezentacja danych (dla systemu VM)” na stronie 126

Część 4. Pojęcia dotyczące hosta i systemu iSeries

© Copyright IBM Corp. 1993-2004

Rozdział 11. Pojęcia

DB2 for OS/390 and z/OS

Program DB2® Universal Database (UDB) dla OS/390® i z/OS™ jest systemem zarządzania relacyjnymi bazami danych firmy IBM® przeznaczonym dla baz danych DB2 for OS/390 and z/OS. Rys. 13 na stronie 70 przedstawia pojedynczą kopię programu DB2 UDB for OS/390 and z/OS działającą w systemie OS/390 lub z/OS. W jednym systemie można również uruchomić wiele kopii programu DB2 UDB for OS/390 and z/OS. Kopie programu DB2 for OS/390 and z/OS w danym systemie (lub kopie programu DB2 for OS/390 and z/OS w ramach kompleksu JES) można identyfikować za pomocą nazwy podsystemu, który jest unikalnym w ramach kompleksu JES łańcuchem złożonym z jednego do czterech znaków.

Requestery aplikacji:

Requesterem aplikacji połączonym z serwerem aplikacji DB2 dla OS/390 lub z/OS może być:

- Requester DB2 dla OS/390 lub z/OS
- DB2 Connect
- Serwer DB2 Universal Database™ Enterprise Server Edition z włączoną obsługą programu DB2 Connect™
- Requester DB2 wersja 2, który może być uruchomiony w systemie AIX, HP-UX, OS/2, Solaris, Windows® 3.1, Windows 3.11 for Workgroups, Windows 95 lub Windows NT albo w systemie 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 dla Windows wersja 2.4
- Requester DB2 UDB for iSeries™
- Requester DB2 for VM
- Każdy produkt, który obsługuje protokoły requestera aplikacji DRDA.

Serwery aplikacji:

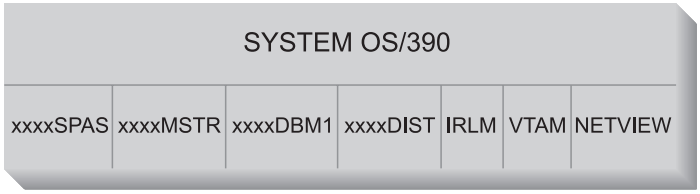
Serwery aplikacji DB2 for OS/390 and z/OS obsługują dostęp do baz danych w następujący sposób:

- Requester aplikacji ma dostęp do tabel zapisanych lokalnie na serwerze aplikacji DB2 for OS/390 and z/OS. Przed uruchomieniem jakichkolwiek instrukcji SQL, requester aplikacji musi utworzyć pakiet na serwerze aplikacji DB2 for OS/390 and z/OS. Serwer aplikacji DB2 for OS/390 and z/OS używa tego pakietu do umiejscowienia instrukcji SQL aplikacji podczas jej wykonywania.
- Requester aplikacji może poinformować serwer aplikacji DB2 for OS/390 and z/OS 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 frontowym interfejsem CICS® poinformuje serwer aplikacji DB2 Universal Database for z/OS and OS/390, że aktualizacja jest niedopuszczalna.
- Requester aplikacji może mieć także dostęp do tabel zapisanych w innych systemach DB2 for OS/390 and z/OS 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.

© Copyright IBM Corp. 1993-2004

Przestrzenie adresowe w systemach OS/390 i z/OS:

Na Rys. 13 nazwą systemu DB2 for OS/390 and z/OS jest *xxxx*. Trzy nazwy przestrzeni adresowych w systemach OS/390 i z/OS mają przedrostki w nazwach podsystemów DB2 for OS/390 and z/OS. Przestrzenie te określają produkt DB2 for OS/390 and z/OS.



Rysunek 13. Przestrzenie adresowe w systemach OS/390 i z/OS używane przez program DB2 for OS/390 and z/OS.

Rys. 13 przedstawia przestrzenie adresowe w systemach OS/390 i z/OS wykorzystywane w przetwarzaniu rozproszonych baz danych w programie DB2 for OS/390 and z/OS. Ich współdziałanie umożliwia użytkownikom programu DB2 for OS/390 and z/OS dostęp do lokalnych relacyjnych baz danych i komunikację ze zdalnymi systemami hosta lub iSeries. Przeznaczenie poszczególnych przestrzeni adresowych jest następujące:

xxxxSPAS
Przestrzeń adresowa procedur zapisanych w bazie DB2.

xxxxMSTR
Przestrzeń adresowa usług systemowych produktu DB2 for OS/390 and z/OS odpowiedzialna za uruchamianie i zatrzymywanie programu DB2 for OS/390 and z/OS i kontrolowanie lokalnego dostępu do niego.

xxxxDBM1
Przestrzeń adresowa usług baz danych, odpowiedzialna za dostęp do relacyjnych baz danych sterowanych przez program DB2 for OS/390 and z/OS. W przestrzeni tej jest realizowane wejście i wyjście dla zasobów baz danych na rzecz aplikacji SQL.

xxxxDIST
Część programu DB2 for OS/390 and z/OS obsługująca rozproszone bazy danych, zwana 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 program DB2 for OS/390 and z/OS w celu sterowania dostępem do zasobów baz danych.

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

NETVIEW
Produkt obsługujący punkt skupienia zarządzania siecią w systemach OS/390 i z/OS. 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 oprogramowania NetView, aby zapoznać się z błędami zapisanymi w bazie danych monitora sprzętowego lub udostępnić procedury automatycznego wywoływania komend po zgłoszeniu wystąpienia warunków alertu.

Oprogramowanie NetView może również służyć do diagnozowania błędów komunikacji VTAM.

Narzędzia połączeniowe w systemach OS/390 i z/OS:

Na Rys. 13 na stronie 70 nie ma aplikacji SQL. Jeśli aplikacja używa programu DB2 do wprowadzenia instrukcji SQL, program musi się połączyć z produktem DB2 for OS/390 and z/OS na jeden z następujących sposobów:

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

CICS/ESA®
Jeśli aplikacja CICS/ESA używa wywołań SQL, produkt CICS/ESA używa interfejsu przyłączenia CICS do kierowania żądań SQL do programu DB2 for OS/390 and z/OS.

IMS/ESA®
Transakcje uruchamiane w IMS/ESA korzystają z interfejsu przyłączenia IMS™, aby przekazać instrukcje SQL do przetwarzania w programie DB2 for OS/390 and z/OS.

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

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

Połączenia rozproszonych baz danych:

Architektura DRDA® definiuje typy funkcji systemu zarządzania rozproszoną bazą danych. Program DB2 for OS/390 and z/OS 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.

Program DB2 for OS/390 and z/OS również obsługuje zdalną jednostkę pracy. Program uruchamiany w jednym systemie może przy użyciu rozproszonej jednostki pracy uzyskać dostęp do danych w zdalnym systemie DBMS, korzystając z języka SQL obsługiwanego przez ten system zdalny.

Jak przedstawiono na Rys. 14 na stronie 73, program DB2 for OS/390 and z/OS obsługuje trzy konfiguracje połączeń z rozproszoną bazą danych, korzystając z dwóch metod dostępu:

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

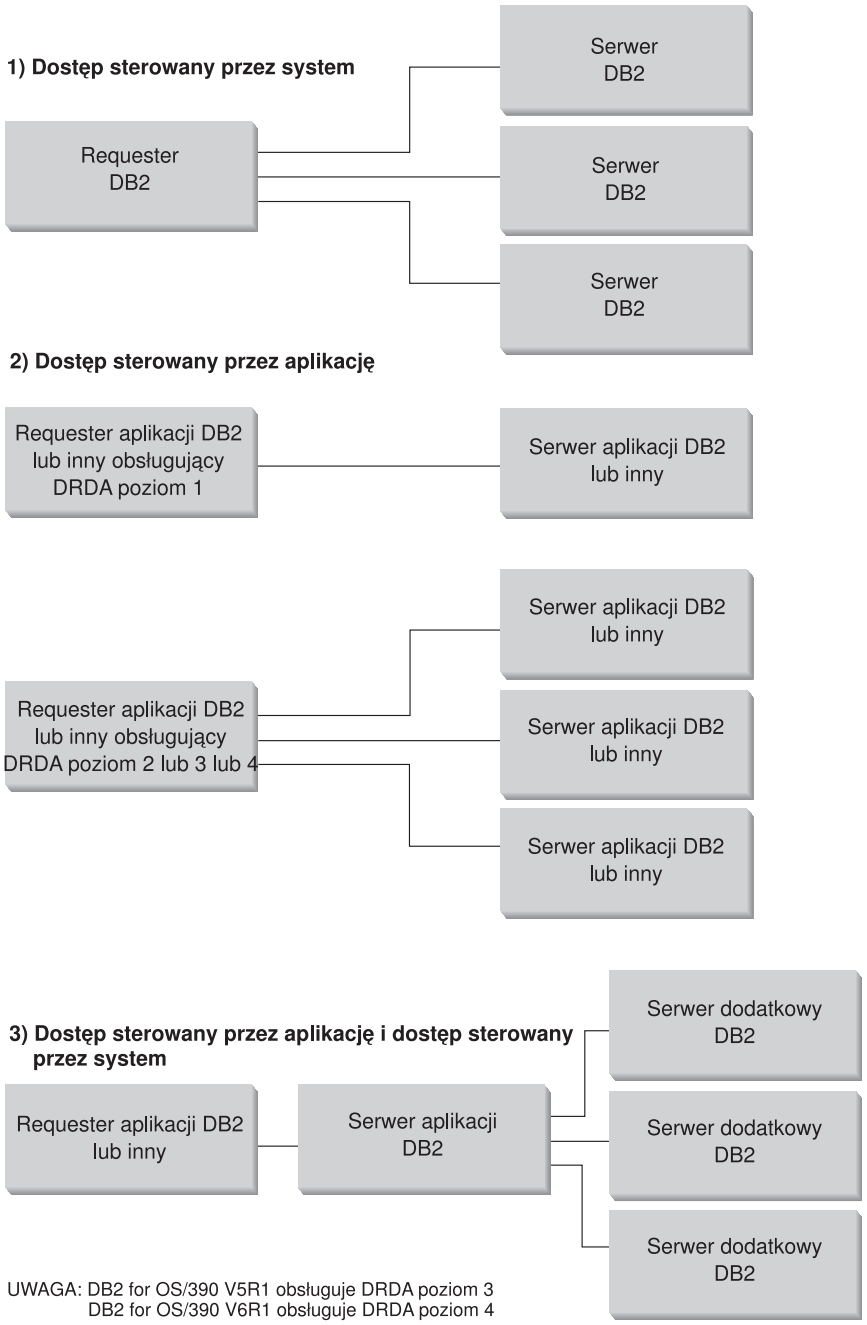
[2] *Dostęp sterowany przez aplikację* umożliwia requesterowi DB2 for OS/390 and z/OS lub innemu niż DB2 for OS/390 and z/OS, np. DB2 Connect, połączenie się z jednym lub kilkoma serwerami aplikacji DB2 for OS/390 and z/OS lub innymi niż DB2 for OS/390 and z/OS, np. DB2 Universal Database i DB2 UDB for iSeries, przy użyciu protokołów DRDA. Liczba serwerów aplikacji, które mogą być jednocześnie połączone z

requesterem, zależy od wersji requestera aplikacji DB2 for OS/390 and z/OS. Ten typ połączenia jest ustanawiany przez wprowadzenie do kodu instrukcji SQL CONNECT w aplikacji.

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

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

Jeśli wszystkie systemy w konfiguracji obsługują zatwierdzanie dwufazowe, rozproszona jednostka pracy (odczyt na wielu serwerach i aktualizacja na wielu serwerach) 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 for OS/390 and z/OS.

Tabela 2 zawiera porównanie typów połączeń rozproszonych baz danych DB2 for OS/390 and z/OS.

Tabela 2. Porównanie połączeń rozproszonych baz danych DB2 for OS/390 and z/OS.

[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 OS/390 and z/OS.	Może łączyć dowolne systemy DRDA.	Requester aplikacji może być dowolnym systemem DRDA; serwery muszą być systemami DB2 for OS/390 and z/OS.

Tabela 2. Porównanie połączeń rozproszonych baz danych DB2 for OS/390 and z/OS. (kontynuacja)

[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.**
Może łączyć się bezpośrednio z wieloma partnerami.	Może łączyć się bezpośrednio z wieloma partnerami.	Requester aplikacji łączy się bezpośrednio z serwerami aplikacji; serwery aplikacji mogą łączyć się z wieloma serwerami dodatkowymi DB2 for OS/390 and z/OS.
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 for OS/390 and z/OS może dla aplikacji 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 i serwer aplikacji mają dostęp do danych lokalnych i zdalnych.
Bardziej wydajny w przypadku obszernych zapytań i wielu zapytań współbieżnych.	Bardziej wydajny w przypadku instrukcji SQL uruchamianych bardzo rzadko w ramach jednego zatwierdzania.	Połączenie requester aplikacji-serwer aplikacji zachowuje się jak **[2]**; serwer dodatkowy zachowuje się jak **[1].**
Może obsługiwać statyczny lub dynamiczny SQL, ale serwer dynamicznie powiąże statyczny SQL za pierwszym razem, gdy jest on wykonywany w zasięgu zatwierdzania.	Może korzystać ze statycznego lub dynamicznego SQL.	Requester aplikacji i serwer aplikacji mogą korzystać ze statycznych lub dynamicznych instrukcji SQL; serwery dodatkowe obsługują statyczne lub dynamiczne instrukcje SQL, lecz wiążą dynamicznie statyczne instrukcje SQL za pierwszym razem, gdy są one wykonywane w zasięgu zatwierdzania.
Ograniczony do instrukcji SQL INSERT, DELETE i UPDATE oraz instrukcji, które obsługują instrukcję SELECT.	Może używać dowolnych instrukcji obsługiwanych przez system, który je wykonuje.	Serwery aplikacji obsługują wszystkie rodzaje języka SQL; serwery dodatkowe obsługują tylko język DML SQL (na przykład CREATE lub ALTER).

Dodatkowe udoskonalenia ochrony:

Kody ochrony rozszerzonej

Do czasu powstania produktu DB2 UDB dla OS/390 wersja 5.1 żądania połączenia dostarczające ID użytkownika lub hasła mogły zakończyć się niepowodzeniem z kodem przyczyny SQL30082 równym 0, ale bez żadnej innej wskazówki określającej przyczynę błędu. W programie DB2 UDB dla OS/390 wersja 5.1 wprowadzone zostało rozszerzenie umożliwiające obsługę kodów ochrony rozszerzonej. Określenie ochrony rozszerzonej dostarcza, poza kodem przyczyny, dodatkowe informacje diagnostyczne, takie jak (PASSWORD EXPIRED).

Aby to wykorzystać, parametr instalacji DB2 Universal Database for z/OS and OS/390 ZPARM dla ochrony rozszerzonej powinien mieć wartość YES. Należy użyć ekranu instalacji DB2 Universal Database for z/OS and OS/390 DSN6SYSP, aby ustawić wartość parametru EXTSEC=YES. Można do tego celu użyć również ekranu 1 DDF (DSNTIPR). Domyślną wartością jest EXTSEC=NO. W przypadku hasła o przekroczonym okresie ważności aplikacje Windows, UNIX i sieci WWW korzystające z programu DB2 Connect otrzymają komunikat o błędzie SQL01404.

Sprawdzona uprzednio ochrona protokołu TCP/IP

Aby zapewnić obsługę opcji ochrony DB2 Universal Database AUTHENTICATION=CLIENT, należy skorzystać z ekranu instalacji DB2 Universal Database for z/OS and OS/390 DSNTIP4 (DDF ekran 2), aby ustawić wartość YES dla opcji sprawdzonej uprzednio ochrony TCP/IP.

Ochrona ODBC i aplikacji w języku Java™ na stacji roboczej

Aplikacje ODBC i aplikacje w języku Java dla stacji roboczych używają dynamicznego SQL. Może to powodować naruszenie ochrony w niektórych instalacjach. Program DB2 Universal Database for z/OS and OS/390 wprowadza nową opcję wiązania DYNAMICRULES(BIND) umożliwiającą wykonanie dynamicznego SQL z autoryzacją właściciela lub konsolidatora.

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

Do aktualizowania pliku DB2CLI.INI służy program ODBC Manager.

Obsługa zmiany hasła

Jeśli instrukcja SQL CONNECT zwróci komunikat informujący, że hasło użytkownika o danym identyfikatorze wygasło, to przy użyciu programu DB2 Connect istnieje możliwość zmiany hasła bez podpisywania się w systemie TSO. Dzięki architekturze DRDA program DB2 Universal Database for z/OS and OS/390 może zmienić hasło użytkownika.

Użytkownik musi podać stare hasło z hasłem nowym i hasłem potwierdzającym. Jeśli na serwerze produktu DB2 Connect Enterprise Edition określono ochronę DCS, żądanie zmiany hasła jest wysyłane do serwera baz danych DB2 Universal Database for z/OS and OS/390. Jeśli podano ochronę typu SERVER, hasło zostanie zmienione na serwerze DB2 Connect.

Dodatkową korzyścią jest to, że nie jest wymagana oddzielna definicja jednostki logicznej.

Pojęcia pokrewne:

- “Reprezentacja danych (dla systemów OS/390 i z/OS)” na stronie 123
- “Zagadnienia związane z ochroną w requesterach aplikacji (dla systemów OS/390 i z/OS)” na stronie 109
- “Zagadnienia związane z ochroną w serwerach aplikacji (dla systemów OS/390 i z/OS)” na stronie 93

Zadania pokrewne:

- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemów OS/390 i z/OS)” na stronie 45
- “Konfigurowanie programu DB2 jako requestera aplikacji (dla systemów OS/390 i z/OS)” na stronie 23
- “Ustawianie wielkości i pacingu jednostek żądań (RU) (dla systemów OS/390 i z/OS)” na stronie 76

Pojęcia podrzędne

Definiowanie komunikacji - SNA (dla systemów OS/390 i z/OS)

Produkt VTAM to Communications Manager dla systemów OS/390 i z/OS. Akceptuje on komendy jednostki logicznej LU 6.2 z programu DB2 for OS/390 and z/OS i poddaje je konwersji na strumienie danych jednostki logicznej LU 6.2, które mogą być przesyłane przez sieć.

Procedura postępowania:

Ponieważ produkt VTAM komunikuje się z aplikacjami partnerskimi zdefiniowanymi w bazie CDB DB2 for OS/390 and z/OS, należy mu udostępnić następujące informacje:

- Nazwę jednostki logicznej dla każdego serwera.

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

  Sposób umieszczenia i składnia definicji VTAM używanych do określania 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 klasa usług dla każdej nazwy 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.

Pojęcia pokrewne:

- “DB2 for OS/390 and z/OS” na stronie 69

Ustawianie wielkości i pacingu jednostek żądań (RU) (dla systemów OS/390 i z/OS)

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

Procedura postępowania:

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

- W wypadku połączeń CTC VTAM należy sprawdzić, czy wartość parametru MAXBFRU jest wystarczająco wysoka, aby umożliwić obsługę wielkości RU plus 29 bajtów, które system VTAM dodaje do nagłówka żądania SNA i nagłówka transmisji. Wartość MAXBFRU jest mierzona w jednostkach o wielkości 4 kB, więc parametr MAXBFRU musi mieć wartość wynoszącą co najmniej 2, aby zmieścić jednostkę RU o wielkości 4 kB.
- W wypadku połączeń NCP należy upewnić się, czy wartość MAXDATA jest odpowiednia, aby umożliwić obsługę wielkości RU plus 29 bajtów. Jeśli określono wielkość RU 4 kB, parametr MAXDATA musi mieć wartość co najmniej 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 systemu 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.

- Podręcznik *DRDA Connectivity Guide* opisuje sposób, w jaki można uzyskać dostęp do informacji o wpływie rozproszonej bazy danych na pulę VTAM IOBUF. Jeśli wykorzystywana jest zbyt duża część zasobów puli IOBUF, wydajność aplikacji VTAM zostaje obniżona.

Pojęcia pokrewne:

- "DB2 for OS/390 and z/OS" na stronie 69

Program DB2 UDB for iSeries

System operacyjny OS/400 zawiera program DB2® UDB for iSeries - system zarządzania relacyjnymi bazami danych firmy IBM® dla systemów iSeries™. W programie DB2 Universal Database for AS/400 wersja 4.2 wprowadzono obsługę komunikacji DRDA® z wykorzystaniem protokołu TCP/IP.

Program licencjonowany OS/400® wersja 2 wydanie 1 modyfikacja 1 obsługuje zdalne jednostki pracy DRDA, a OS/400 wersja 3 wydanie 1 obsługuje ponadto rozproszone jednostki pracy DRDA (DUOW). Obsługa ta jest częścią systemu operacyjnego OS/400. Oznacza to, że do korzystania z obsługi architektury DRDA lub do uruchamiania programów z instrukcjami wbudowanego SQL nie jest potrzebny licencjonowany program DB2 UDB for iSeries Query Manager ani zestaw SQL Development Kit.

Pojęcia pokrewne:

- "Reprezentacja danych (dla systemu iSeries)" na stronie 123
- "Uwagi związane z ochroną w serwerach aplikacji (dla systemu iSeries)" na stronie 99
- "Uwagi dotyczące ochrony w requesterach aplikacji (dla systemu iSeries)" na stronie 115

Zadania pokrewne:

- "Konfigurowanie programu DB2 jako serwera aplikacji przy użyciu architektury SNA (dla systemu iSeries)" na stronie 49
- "Konfigurowanie programu DB2 jako requestera aplikacji – SNA (dla systemu iSeries)" na stronie 31

DB2 for VM

Program SQL/DS™ (DB2 for VM) wersja 3 wydanie 5 umożliwia obsługę systemów VM przez serwer aplikacji zdalnej jednostki pracy DRDA®.

Każdy menedżer baz danych DB2® for VM może zarządzać jedną lub wieloma bazami danych (po jednej naraz). Odwołanie do menedżera zwykle następuje za pomocą nazwy bazy danych, którą w danej chwili zarządza. Nazwa relacyjnej bazy danych jest unikalna w obrębie połączonych sieci SNA.

Oprogramowanie 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 oprogramowanie 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 Server for VM System Administration*
- *DB2 Server for VSE System Administration*

Przetwarzanie rozproszonych baz danych - komponenty DRDA i VM:

Poniżej opisano różne komponenty DRDA i VM wykorzystywane w przetwarzaniu rozproszonych baz danych. Wymienione komponenty udostępniają menedżerom bazy 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 w środowisku VM jest określana jako *brama* (gateway). System AVS działa w systemie sterującym grupami jako aplikacja VTAM®. Przekształca on wywołania makr APPC/VM na wywołania makr APPC/VTAM i odwrotnie. Komponent APPC/VM wykorzystuje rozwiązanie 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 komponent 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. Szczegóły dotyczące wykonywania tych czynności 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 jednostki logicznej LU 6.2 zdefiniowanych przez SNA. W praktyce komponent APPC/VM udostępnia komendy jednostki logicznej LU 6.2 pozwalające aplikacjom DB2 for VM na łączenie się z lokalnymi i zdalnymi menedżerami bazy danych. Komendy jednostki logicznej LU 6.2 obsługiwane przez APPC/VM są wymienione 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, TPN, ochrona, nazwa trybu, identyfikator użytkownika, hasło i nazwa bazy danych.

DB2 for VM korzysta ze znacznika COMDIR: dbname, aby wykonać translację nazwy RDB_NAME na odpowiadające jej dane dotyczące 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 narzędziem CRR, wykorzystują konwersację chronioną, co zapewnia integralność zasobów transakcji rozproszonej.

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

GCS System sterujący grupami (GCS, Group control system) jest komponentem systemu VM składającym się z następujących elementów:

- współużytkowany segment działający na maszynie wirtualnej
- nadzorca maszyny wirtualnej, który wiąże wiele wirtualnych maszyn w grupę i nadzoruje ich działanie
- interfejs między następującymi programami:
  - metoda dostępu do sieci telekomunikacyjnej (Virtual Telecommunications Access Method - VTAM)
  - obsługa APPC/VTAM (system AVS)
  - podsystem zdalnego buforowania komunikacji (Remote Spooling Communications Subsystem - RSCS)
  - program sterujący (Control Program - CP)

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

Adapter zasobów
Adapter zasobów jest częścią oprogramowania DB2 for VM, która znajduje się na 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 najwyżej 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.

Program 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, program 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.

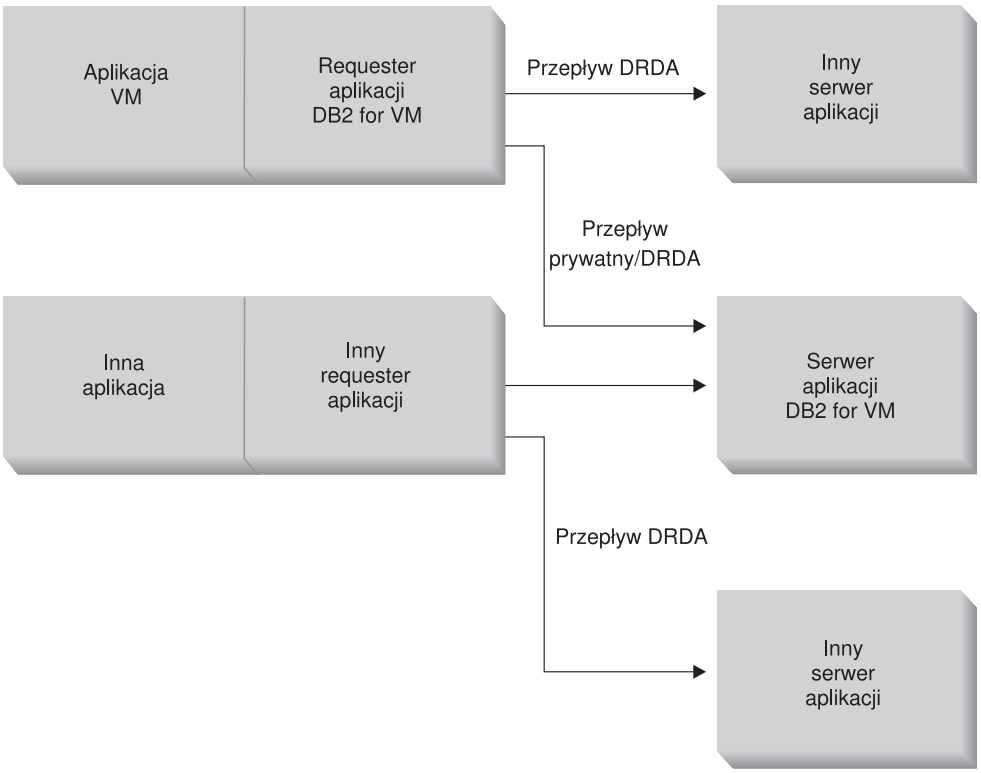
Zwykle kolekcja TSAF działa autonomicznie, niezależnie od usług VTAM i sieci SNA. Może ona jednak współdziałać z systemem AVS i VTAM, aby jej zasoby globalne były dostępne z aplikacji zdalnych APPC znajdujących się w dowolnym miejscu sieci SNA. Aby to osiągnąć, maszyna AVS i maszyna VTAM muszą działać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

VTAM Virtual Telecommunications Access Method zapewnia obsługę połączeń

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

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

Jak przedstawiono na Rys. 15, 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 15. Requester aplikacji i serwer aplikacji DB2 for VM.

Opcje przetwarzania wstępnego lub uruchamiania aplikacji:

Program 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 identyfikatora CCSID co serwer. Domyślna wartość identyfikatora CCSID[2] ustawiona przez requester za pośrednictwem SQLINIT jest ignorowana, a żaden identyfikator LUWID jednostki logicznej LU 6.2 nie jest związany z konwersacją. Jest to najbardziej wydajna 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 zarówno do podobnych, jak i do niepodobnych systemów.
- Jeśli wartości domyślne CCSID są różne na serwerze i requesterze (i opcją PROTOCOL serwera aplikacji nie jest SQLDS).
- Jeśli wymagany jest identyfikator LUWID jednostki logicznej LU 6.2 związany z każdą konwersacją, 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 mogą mieć różne wartości domyślne identyfikatora 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 przedstawia porównanie funkcjonalne charakterystyki opcji przetwarzania SQLINIT requestera aplikacji DB2 for VM.

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.

2. W programie DB2 for VM requester aplikacji i serwer aplikacji określają domyślny identyfikator CCSID, ustawiając wartość CHARNAME dla parametru SQLINIT i odpowiednio dla SQLSTART. Nazwa CHARNAME jest nazwą symboliczną, która jest wewnętrznym odwzorowaniem na odpowiedni identyfikator CCSID.

3. 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. (kontynuacja)

[SQLDS]	[AUTO]	[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 [3].
Identyfikatory CCSID zdefiniowane przez opcję SQLINIT dla requestera aplikacji są ignorowane przez serwer aplikacji DB2 for VM.	Identyfikatory CCSID zdefiniowane za pomocą polecenia SQLINIT dla requestera aplikacji są honorowane przez serwer aplikacji DB2 for VM, wykonywana jest odpowiednia konwersja (jeśli serwer aplikacji jest także ustawiony na wartość AUTO).	Identyfikatory CCSID zdefiniowane za pomocą polecenia 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.	Elementy PUT są przekształcane na zwykłe jednowierszowe wstawienia wierszy i wysyłają jeden wiersz naraz.
Wszystkie komendy unikalne dla systemu 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 Server for VSE & VM SQL Reference*).
Identyfikator LUWID nie jest obsługiwany.	Identyfikator LUWID jest obsługiwany.	Identyfikator LUWID jest obsługiwany.

Opcje uruchamiania serwera baz danych:

W tej sekcji opisano różne opcje uruchamiania maszyny serwera baz danych.

Parametr PROTOCOL:

Podczas uruchamiania maszyny serwera baz danych administrator może nadać parametrowi PROTOCOL jedną z następujących wartości:

SQLDS

Opcja domyślna i zalecana w wypadku, gdy 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 opcję PROTOCOL(SQLDS), przetwarzanie na serwerze DB2 for VM jest kontynuowane z prywatnymi przepływami. Jeśli requester DB2 for VM określi opcję PROTOCOL(AUTO), serwer DB2 for VM zawiadamia requester o konieczności przełączenia na przepływ prywatny. Informacje o identyfikatorze 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 określi opcję 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 wypadku requestera aplikacji, który określił 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 identyfikatorów CCSID żądań odpowiedzi. Przepływ DRDA jest wymagany przez requestery inne niż DB2 for VM lub przez requestery DB2 for VM, które określiły opcję PROTOCOL(DRDA).

Parametr SYNCPNT:

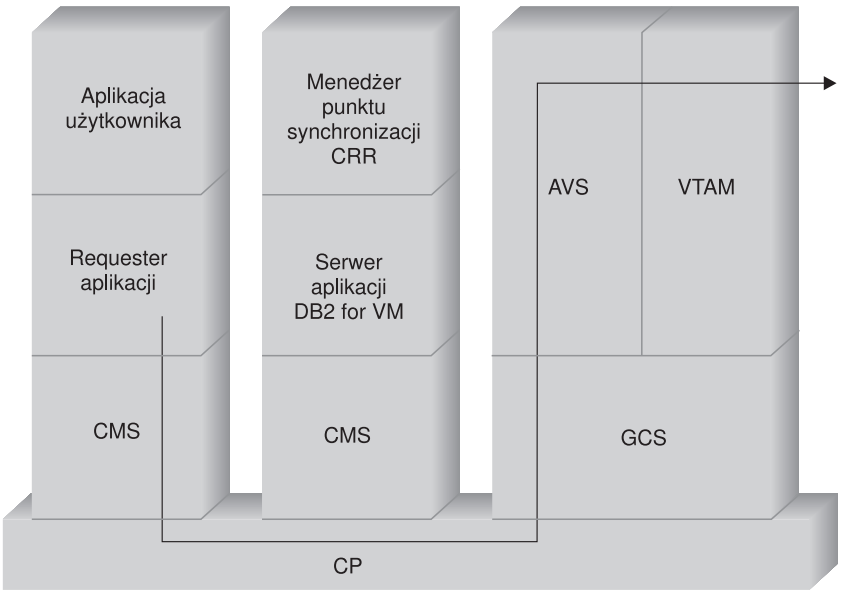
Parametr ten określa, czy menedżer punktu synchronizacji (SPM) zostanie użyty do koordynacji działania rozproszonej jednostki pracy podczas odczytu wielopunktowego DRDA-2 i zapisu wielopunktowego.

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 menedżera 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 określona jest wartość Y, lecz serwer aplikacji stwierdzi, że menedżer punktów synchronizacji jest niedostępny, serwer będzie działał, tak jakby określona była wartość N.

Jeśli PROTOCOL=AUTO, wartością domyślną jest SYNCPNT=Y. Jeśli PROTOCOL=SQLDS, parametr SYNCPNT ma wartość N.

Przykład przepływu komunikacji dla requestera aplikacji:

Poniższy przykład ukazuje rolę poszczególnych komponentów w nawiązywaniu komunikacji między requesterem aplikacji VM i serwerem zdalnym DRDA. Rys. 16 na stronie 84 przedstawia, jak requester aplikacji łączy się z komponentem AVS i korzysta z maszyny VTAM, aby uzyskać dostęp do sieci SNA. Trasa dostępu do zasobów zdalnych nie prowadzi przez lokalny serwer aplikacji DB2 for VM.



Rysunek 16. Żądanie dostępu do zasobu zdalnego.

Załóżmy, że requester aplikacji DB2 for VM należący do kolekcji TSAF ma uzyskać dostęp do zdalnych danych zarządzanych przez serwer aplikacji DRDA. 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. System AVS i produkt 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.

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

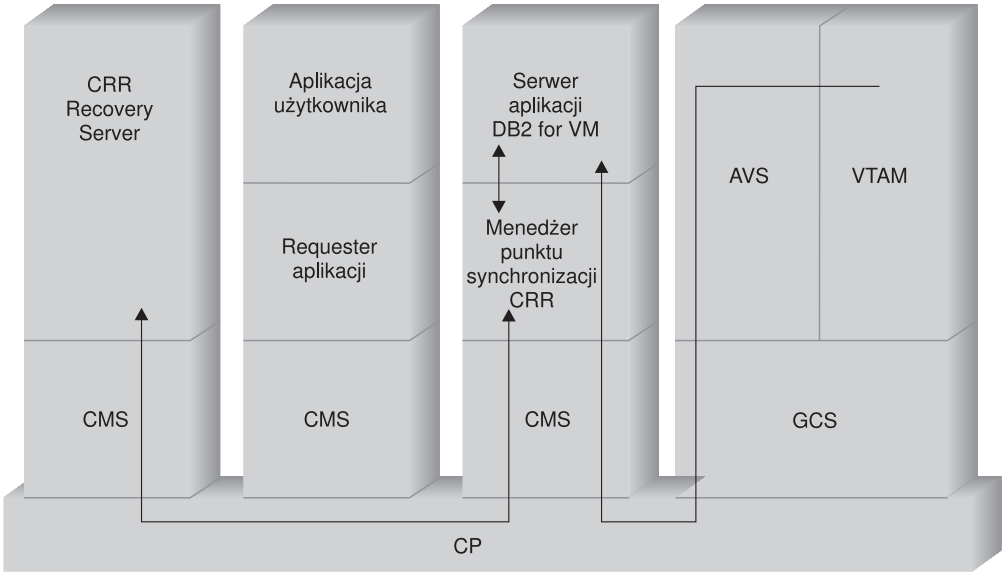
Requester aplikacji wydaje instrukcję APPC/VM CONNECT w celu nawiązania konwersacji LU 6.2 z serwerem aplikacji. Funkcja CONNECT wykorzystuje katalog CMS Communications Directory do odwzorowania nazwy relacyjnej bazy danych na nazwę powiązanej jednostki logicznej i nazwę programu transakcyjnego odpowiadającą adresowi serwera aplikacji w sieci SNA. Katalog CMS Communications Directory określa także poziom ochrony konwersacji i znaczniki ochrony, takie jak identyfikator użytkownika i hasło, które przekazuje do ośrodka zdalnego w celu autoryzacji. Jeśli parametr SECURITY=PGM, requester aplikacji musi przekazać identyfikator użytkownika i hasło do serwera aplikacji. Identyfikator użytkownika i hasło można określić w katalogu CMS Communications Directory lub w rekordzie APPCPASS zdefiniowanym przy użyciu katalogu CP użytkownika requestera aplikacji. Jeśli parametr SECURITY=SAME, wówczas tylko identyfikator logowania w systemie VM użytkownika requestera aplikacji jest wysyłany do serwera aplikacji, a 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 (jednostka logiczna) i zdalną jednostką logiczną. Potem komponent AVS nawiązuje konwersację ze zdalną jednostką logiczną i przekazuje jej nazwę jednostki logicznej, poziom ochrony, TPN i identyfikator użytkownika. Jeśli zdalna jednostka logiczna również jest systemem VM, to sesja i konwersacja są obsługiwane przez działający w tym systemie 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. Rys. 17 pokazuje, że produkt VTAM kieruje przychodzące połączenia do określonej bramy AVS, a następnie do serwera aplikacji.



Rysunek 17. Uzyskiwanie dostępu do zasobu zdalnego.

Załóżmy, że serwer aplikacji DB2 for VM działa w kolekcji TSAF. 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. System AVS i produkt 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.

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

Po rozpoczęciu sesji przez lokalny komponent AVS z partnerską jednostką logiczną, akceptuje on konwersację i przekazuje nazwę TPN, identyfikator 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 identyfikatora zasobu zarejestrowanego za pomocą usługi systemowej *IDENT. Jeśli wyszukiwanie TPN powiodło się, system VM sprawdza poprawność identyfikatora użytkownika i hasła przy użyciu swojego katalogu, RACF® lub podobnego produktu chroniącego. Jeśli sprawdzanie poprawności powiodło się, system AVS nawiązuje połączenie z serwerem aplikacji i przekazuje mu identyfikator użytkownika w celu sprawdzenia autoryzacji do bazy danych.

Jeśli przeszukiwanie tabel nie powiodło się, maszyna AVS zakłada, że TPN może znajdować się w innym systemie VM w kolekcji TSAF i nawiązuje połączenie z lokalną maszyną TSAF, przekazując jej identyfikator 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 identyfikator 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 identyfikator 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 system CMS przedstawi połączenie programowi DB2 for VM, tworzy on jednostkę pracy CMS do konwersacji zabezpieczonej w maszynie DB2 for VM. Później program DB2 for VM korzysta z tej jednostki pracy za każdym razem, gdy wykonuje pracę dla requestera. Gdy program DB2 for VM zaczyna wykonywać pracę dla requestera, rejestruje jednostkę pracy CMS za pomocą menedżera punktów synchronizacji CRR. Następnie, gdy program DB2 odbiera wskazanie ″take commit″ lub ″take rollback″ w konwersacji zabezpieczonej, prosi menedżera punktów synchronizacji CRR o zatwierdzenie lub wycofanie zmian w jednostce pracy. Następnie, jeśli jest to konieczne, menedżer punktów synchronizacji CRR wykonuje zatwierdzenie lub wycofanie zmian, wysyłając do serwera CRR Recovery Server żądanie protokołowania punktów synchronizacji.

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 VTAM,
- systemie VM w innej kolekcji TSAF, na którym działają AVS i VTAM,
- systemie w sieci SNA innym niż VM, obsługującym protokół LU 6.2,
- systemie w sieci SNA innym niż system firmy IBM, obsługującym protokół LU 6.2.

Pojęcia pokrewne:

- “Zagadnienia związane z ochroną w serwerach aplikacji (dla systemu VM)” na stronie 101
- “Reprezentacja danych (dla systemu VM)” na stronie 126
- “Zagadnienia związane z ochroną w requesterach aplikacji (dla systemu VM)” na stronie 118
- “Program DB2 for VSE” na stronie 88

Zadania pokrewne:

- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemu VM)” na stronie 63
- “Konfigurowanie programu DB2 jako requestera aplikacji (dla systemu VM)” na stronie 37

Informacje pokrewne:

- “Lista kontrolna włączania requestera aplikacji DB2 (dla systemu VM)” na stronie 132

Pojęcia podrzędne

Definiowanie komunikacji – requester aplikacji (dla systemu VM)

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.

Komponent APPC/VM jest interfejsem API LU 6.2 poziomu asemblera, który requester aplikacji DB2 for VM wykorzystuje do żądania usług komunikacyjnych. Katalog komunikacji CMS 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 komponencie CMS Communications Directory, VTAM i *IDENT.

Aby metoda VTAM mogła komunikować się z partnerską aplikacją zidentyfikowaną w CMS Communications Directory, należy dostarczyć następujących informacji:

1. Zdefiniować w produkcie VTAM nazwę jednostki logicznej każdego requestera aplikacji i serwera aplikacji. Położenie i składnia tych definicji zależy od sposobu logicznego i fizycznego połączenia serwera z systemem VTAM.
2. Utworzyć tabelę trybów VTAM dla każdej nazwy trybu określonej w katalogu komunikacyjnym CMS Communications Directory. Pozycje te określają wielkość jednostki żądania (RU), wielkość okna pacingu i klasę usług dla danej nazwy trybu.
3. Jeśli będzie używana weryfikacja partnerskiej jednostki logicznej (ochrona na poziomie sesji), dla algorytmu weryfikacji należy podać profile VTAM i RACF (lub ich odpowiedniki).

Zagadnienia dotyczące limitu liczby sesji AVS:

Jeśli requester aplikacji korzysta z komponentu AVS do komunikowania się z serwerem zdalnym aplikacji, inicjowane jest połączenie. Jeśli połączenie powoduje przekroczenie ustalonego limitu sesji, AVS zawiesza je, dopóki sesja nie będzie dostępna. Gdy sesja staje się dostępna, system AVS przydziela zawieszone połączenie do sesji i sterowanie zostaje zwrócone do aplikacji użytkownika. Aby uniknąć tej sytuacji, należy zaplanować maksymalne wykorzystanie, zwiększając limit sesji dla pewnej liczby dodatkowych połączeń. Należy sprawdzić, czy wartość MAXCONN w katalogu CP maszyny AVS jest wystarczająco duża, aby obsłużyć maksymalne wykorzystanie połączeń APPC/VM.

Pojęcia pokrewne:

• "DB2 for VM" na stronie 77

Ustawianie wielkości i pacingu jednostek żądań (RU) (dla systemu VM)

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

- W wypadku połączeń CTC VTAM należy sprawdzić, czy wartość parametru MAXBFRU jest wystarczająco wysoka, aby umożliwić obsługę wielkości RU plus 29 bajtów, które system VTAM dodaje do nagłówka żądania SNA i nagłówka transmisji. Wartość MAXBFRU jest mierzona w jednostkach o wielkości 4 kB, więc parametr MAXBFRU musi mieć wartość wynoszącą co najmniej 2, aby zmieścić jednostkę RU o wielkości 4 kB.
- W wypadku połączeń NCP należy upewnić się, czy wartość MAXDATA jest odpowiednia, aby umożliwić obsługę wielkości RU plus 29 bajtów. Jeśli określono wielkość jednostki żądań (RU) równą 4096, parametr MAXDATA musi mieć wartość co najmniej 4125.

  Jeśli określono parametr NCP MAXBFRU, należy wybrać wartość, która pozwoli pomieścić wielkość danej jednostki żądania (RU) plus 29 bajtów. W przypadku NCP parametr MAXBFRU określa liczbę buforów we/wy VTAM, które mogą pomieścić jednostki PIU. Jeśli wielkość buforu IOBUF została ustawiona na 441, parametr MAXBFRU=10 poprawnie przetwarza jednostkę żądania o wielkości 4 kB, ponieważ 10*441 jest większe niż suma 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 wykorzystywana jest zbyt duża część zasobów puli IOBUF, wydajność aplikacji VTAM zostaje obniżona.

Pojęcia pokrewne:

• "DB2 for VM" na stronie 77

Program DB2 for VSE

Program SQL/DS™ (DB2 for VSE) wersja 3 wydanie 5 umożliwia obsługę systemów VSE przez serwer aplikacji zdalnej jednostki pracy DRDA®.

W środowisku VSE/ESA™ program DB2® for VSE obsługuje funkcje serwera aplikacji środowiska DRDA. Funkcja requestera aplikacji nie jest obsługiwana. W sekcji tej opisano

różne komponenty oprogramowania DB2 for VSE i VSE wykorzystywane przy przetwarzaniu rozproszonych baz danych. Komponenty te umożliwiają systemowi zarządzania baz danych DB2 for VSE komunikowanie się ze zdalnymi requesterami aplikacji w sieci SNA.

CICS(ISC)
Komponent komunikacji między systemami Customer Information Control System (CICS) zapewnia funkcje SNA LU 6.2 (APPC) dla serwera aplikacji DB2 for VSE.

CICS(SPM)
Komponent zarządzania punktem synchronizacji CICS® jest składnikiem obsługi rozproszonej jednostki pracy DRDA DB2 for VSE. Działa on jako 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 między jednostkami logicznymi z systemami zdalnymi serwer CICS(ISC) korzysta z produktu VTAM® for VSE. System DB2 for VSE używa podstawowej konwersacji jednostki logicznej LU 6.2 tych sesji, aby komunikować się ze zdalnymi requesterami aplikacji DRDA.

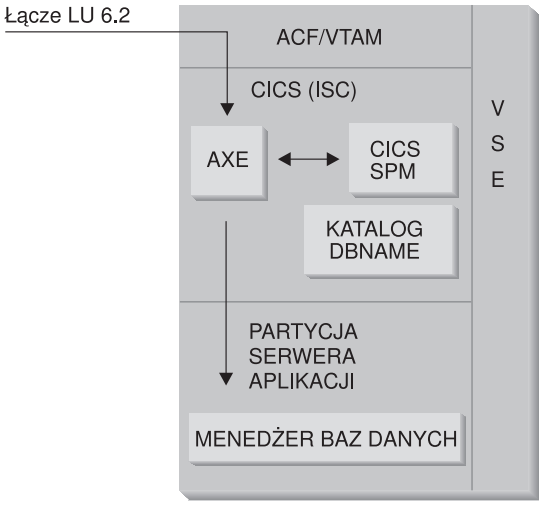
AXE Transakcja APPC-XPCC-Exchange jest transakcją CICS uaktywnianą przez zdalny requester aplikacji DRDA. Kieruje ona wymianą strumieni danych DRDA między zdalnym requesterem aplikacji a serwerem aplikacji DB2 for VSE korzystającym z obsługi jednostki logicznej CICS LU 6.2 i funkcji XPCC VSE.

katalog DBNAME
Katalog DBNAME (nazw baz danych) odwzorowuje przychodzące żądania przydzielenia konwersacji do określonego wstępnie 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. 18 na stronie 90 przedstawia rolę każdego z komponentów w nawiązaniu komunikacji między serwerem aplikacji DB2 for VSE a zdalnym requesterem aplikacji.



Rysunek 18. Uzyskiwanie dostępu do serwera aplikacji.

Requester aplikacji wysyła komendę APPC ALLOCATE wraz z nazwą określonej jednostki logicznej i nazwą programu transakcyjnego w celu nawiązania konwersacji jednostki logicznej LU 6.2 z serwerem aplikacji. Nazwa jednostki logicznej jest używana do skierowania żądania ALLOCATE przez system VTAM do systemu CICS. Po otrzymaniu komendy ALLOCATE system CICS sprawdza, czy transakcja AXE jest zdefiniowana dla tej nazwy programu transakcyjnego (TPN) i przeprowadza logowanie do systemu 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 logowaniu się do systemu.

Aby połączenie zostało zaakceptowane, tabela logowania 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 system CICS powierza sprawdzanie uprawnień systemowi zdalnemu. Jeśli kontrola przebiegnie pomyślnie, 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, requester wykonuje następujące czynności:

- Jeśli to konieczne, transakcja AXE umożliwia obsługę typu TRUE, tak aby mogła ona komunikować się z menedżerem punktu synchronizacji CICS.
- Rejestruje logiczną jednostkę pracy w menedżerze punktu synchronizacji CICS.

Ograniczenia serwera aplikacji:

W przeciwieństwie do swojego odpowiednika w systemie 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 przy ustawieniu 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 określić 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 parametr NCUSER), część użytkowników zdalnych musi czekać na dostęp do agenta, który ma zrealizować 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 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 menedżera 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 jednopunktowy. 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 parametr RMTUSERS ma wartość większą od zera, wartością domyślną jest SYNCPNT=Y. Jeśli parametr RMTUSERS=0, parametr SYNCPNT ma wartość N.

Zadania pokrewne:

- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemu VSE)” na stronie 57

Rozdział 12. Zagadnienia dotyczące ochrony serwerów aplikacji

Zagadnienia związane z ochroną w serwerach aplikacji (dla systemów OS/390 i z/OS)

Gdy requester aplikacji przekierowuje żądanie rozproszonej bazy danych do serwera aplikacji DB2® dla OS/390® i z/OS™, należy uwzględnić następujące zagadnienia ochrony:

- Sprawdzanie źródła żądania
- Nazwy użytkowników
- Ochrona sieci
- Ochrona menedżera baz danych
- Podsystem ochrony

Pojęcia pokrewne:

- "Zagadnienia związane z ochroną w requesterach aplikacji (dla systemów OS/390 i z/OS)" na stronie 109
- "DB2 for OS/390 and z/OS" na stronie 69

Zadania pokrewne:

- "Konfigurowanie programu DB2 jako serwera aplikacji (dla systemów OS/390 i z/OS)" na stronie 45

Pojęcia podrzędne

Sprawdzanie źródła (dla systemów OS/390 i z/OS)

Kiedy serwer aplikacji hosta otrzymuje od requestera aplikacji nazwę użytkownika, serwer może wprowadzić ograniczenia co do odbieranych od danego requestera aplikacji nazw użytkowników. Jest to wykonywane przy użyciu sprawdzania *źródła żądania*. Sprawdzanie źródła pozwala serwerowi na określenie, że dany identyfikator użytkownika może być jedynie używany przez określonych partnerów.

Na przykład, serwer aplikacji może wprowadzić ograniczenie, że żądania użytkownika JONES będą mogły "przychodzić" tylko ze źródła o nazwie 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.

Sprawdzanie źródła jest zaimplementowane w systemie hosta w ramach konwersji przychodzącej nazwy użytkownika, którą opisano w następnej sekcji.

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

Pojęcia pokrewne:

- "Zagadnienia związane z ochroną w serwerach aplikacji (dla systemów OS/390 i z/OS)" na stronie 93

© Copyright IBM Corp. 1993-2004

Nazwy użytkowników - serwer aplikacji (dla systemów OS/390 i z/OS)

Identyfikator użytkownika przysłany przez requester aplikacji może nie być unikalny w sieci SNA. Może być konieczne wykonanie konwersji nazw przychodzących przez serwer aplikacji DB2® w celu utworzenia unikalnych w całej sieci nazw użytkowników. Podobnie może być konieczne wykonanie przez serwer aplikacji DB2 konwersji nazw wychodzących w celu utworzenia unikalnych nazw użytkowników, przeznaczonych dla serwerów dodatkowych związanych z aplikacją.

Konwersję nazw przychodzących można włączyć, ustawiając dla kolumny USERNAMES tabeli SYSIBM.LUNAMES lub SYSIBM.IPNAMES wartość 'I' (konwersja nazw przychodzących) lub 'B' (konwersja nazw przychodzących i wychodzących). Podczas konwersji nazw przychodzących program DB2 wykonuje konwersję identyfikatora użytkownika wysłanego przez requester aplikacji i nazwę właściciela planu DB2 (jeśli requesterem aplikacji jest inny system DB2).

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

Gdy sprawdzany jest przychodzący identyfikator użytkownika w poleceniu ALLOCATE, program DB2 ma informacje wyjściowe dotyczące autoryzacji, których użytkownik może użyć, aby dostarczyć listę dodatkowych autoryzacji AUTHID i wykonać dodatkowe sprawdzenie ochrony. Więcej szczegółowych informacji można znaleźć w podręczniku *DB2 for OS/390 Administration Guide*.

Proces konwersji nazw przychodzących szuka w tabeli SYSIBM.USERNAMES wiersza, 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.blank — Określony użytkownik z dowolnego requestera aplikacji.
3. I.blank.LINKNAME — Dowolny użytkownik z określonego requestera aplikacji.

Jeśli wiersz nie zostanie odnaleziony, nastąpi odmowa dostępu. Jeśli wiersz zostanie odnaleziony, dostęp zdalny będzie dozwolony i nazwa użytkownika zostanie zmieniona na wartość z kolumny NEWAUTHID z wartością pustą NEWAUTHID oznaczającą, że nazwa nie została zmieniona. Dowolne sprawdzenie autoryzacji do zasobów programu DB2 (na przykład uprawnienia do tabeli SQL) wykonane przez program DB2 jest przeprowadzane względem nazw użytkowników po translacji, a nie względem pierwotnych nazw użytkowników.

Jeśli serwer aplikacji DB2 otrzyma nazwę użytkownika od requestera aplikacji, funkcje DB2 wykonujące konwersję nazw przychodzących można wykorzystać również do innych zadań:

- Można zmienić nazwę użytkownika tak, aby była unikalna. Na przykład poniższe 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', ' ');
```

Rysunek 19. Zmienianie nazwy użytkownika na unikalną.

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

Rysunek 20. Zmienianie nazwy użytkownika, tak aby grupa użytkowników była reprezentowana przez jedną nazwę.

- Można ograniczyć nazwy użytkowników przesyłane przez określony requester aplikacji. Podczas konwersji nazwy użytkownika następuje również sprawdzanie źródła żądania. 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 istnieje on 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', ' ', ' ');
```

Rysunek 21. Ograniczanie nazw użytkowników przesyłanych przez określony requester aplikacji.

- Można ograniczyć requestery aplikacji, które mogą się połączyć z serwerem aplikacji DB2. Jest to kolejna opcja sprawdzania źródła żądania. W poniższym przykładzie akceptowana jest każda nazwa użytkownika przysłana przez requester aplikacji NEWYORK (LUNYC) lub CHICAGO (LUCHI). Inne requestery aplikacji nie mają dostępu, ponieważ domyślny wiersz SYSIBM.LUNAMES określa konwersję 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', ' ', ' ');
```

Rysunek 22. Ograniczanie requesterów aplikacji, które mogą się połączyć.

Pojęcia pokrewne:

- "Zagadnienia związane z ochroną w serwerach aplikacji (dla systemów OS/390 i z/OS)" na stronie 93

Ochrona sieci - serwer aplikacji (dla systemów OS/390 i z/OS)

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

- ochrona na poziomie sesji
- ochrona na poziomie konwersacji
- szyfrowanie

Pozostałe uwagi na temat ochrony sieci dotyczą ochrony na poziomie konwersacji SNA. Niektóre aspekty ochrony na poziomie konwersacji mają zastosowanie tylko dla serwera aplikacji DB2®. Więcej szczegółowych informacji można znaleźć w podręczniku *DB2 for OS/390 Administration Guide*. Serwer aplikacji DB2 pełni dwie różne role w ochronie sieci:

- Jako requester serwerów dodatkowych serwer aplikacji DB2 jest odpowiedzialny za wydawanie żądań APPC, które zawierają parametry ochrony na poziomie konwersacji SNA wymagane przez serwery dodatkowe. Serwer aplikacji DB2 używa kolumny USERNAMES z tabeli SYSIBM.LUNAMES i tabeli SYSIBM.USERNAMES do definiowania wymagań dotyczących ochrony na poziomie konwersacji SNA dla każdego serwera dodatkowego.
- Jako serwer requestera aplikacji, serwer aplikacji DB2 narzuca ograniczenia dotyczące ochrony na poziomie konwersacji SNA dla requestera aplikacji. Program DB2 używa kolumny USERSECURITY z tabeli SYSIBM.LUNAMES, aby określić poziom konwersacji wymagany dla każdego requestera aplikacji w sieci. W kolumnie USERSECURITY stosowane są następujące wartości:

  C Wskazuje, że program DB2 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 tabeli SYSIBM.LUNAMES zawiera wartość 'Y', program DB2 zakłada, że hasło jest już w zaszyfrowanym formacie RACF® (jest to możliwe tylko dla requestera aplikacji DB2). Jeśli kolumna ENCRYPTPSWDS nie zawiera wartości 'Y', program DB2 oczekuje hasła w formacie standardowym LU 6.2 (reprezentacja znakowa EBCDIC). W obu przypadkach program DB2 przesyła wartości identyfikatora użytkownika i hasła do podsystemu ochrony w celu sprawdzenia poprawności. Podsystem ochrony udostępnia sprawdzanie identyfikatora i hasła użytkownika APPC; na przykład system RACF ma możliwość sprawdzania identyfikatorów i haseł użytkowników APPC. Jeśli podsystem ochrony odrzuci parę identyfikator-hasło użytkownika, dostęp do rozproszonej bazy danych nie będzie możliwy.

Inna wartość

Wskazuje, że requester aplikacji może wysyłać sprawdzony uprzednio identyfikator użytkownika (LU 6.2 SECURITY=SAME) lub identyfikator i hasło użytkownika (LU 6.2 SECURITY=PGM). Jeśli identyfikator i hasło użytkownika zostaną wysłane, program DB2 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 jednostka logiczna LU 6.2 wymaga, aby serwer aplikacji DB2 zwrócił kod znaczenia niepowodzenia ochrony SNA ('080F6051'X) do requestera aplikacji. Ponieważ niniejszy kod znaczenia nie opisuje przyczyny występowania niepowodzenia, program DB2 dostarcza dwóch metod odczytywania przyczyny naruszenia ochrony rozproszonej:

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

Pojęcia pokrewne:

- “Zagadnienia związane z ochroną w serwerach aplikacji (dla systemów OS/390 i z/OS)” na stronie 93

Ochrona menedżera bazy danych - serwer aplikacji (dla systemów OS/390 i z/OS)

Jako właściciel zasobu bazy danych, serwer aplikacji DB2® steruje funkcjami ochrony bazy danych dla obiektów SQL znajdujących się na serwerze aplikacji DB2. Dostęp do obiektów zarządzanych przez program DB2 jest sterowany za pomocą uprawnień nadawanych użytkownikom przez administratora programu DB2 lub właścicieli obiektów indywidualnych. Oto dwie podstawowe klasy obiektów, które są sterowane przez serwer aplikacji DB2:

- **Pakiety** — Użytkownicy indywidualni mają uprawnienia do tworzenia, wymieniania i uruchamiania pakietów za pomocą instrukcji GRANT programu DB2. Gdy użytkownik jest właścicielem pakietu, może on automatycznie uruchamiać i zastępować pakiet. Inni użytkownicy mający specjalne uprawnienia do uruchamiania pakietu na serwerze aplikacji DB2 za pomocą instrukcji GRANT. Uprawnienie USE można nadać użytkownikom indywidualnym PUBLIC, co umożliwia wszystkim użytkownikom uruchomienie pakietu.

  Jeśli aplikacja zostaje powiązana z programem DB2, 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 odwołuje, są znane w momencie powiązania aplikacji z programem DB2. 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. Jeśli pakiet zawiera tylko statyczne instrukcje SQL, to użytkownicy nie muszą mieć żadnych uprawnień do tabeli DB2.

  Dynamiczny SQL

  Dynamiczny SQL opisuje instrukcję SQL, która nie jest znana aż do rozpoczęcia wykonywania programu. Innymi słowy instrukcja SQL jest tworzona przez program i dynamicznie wiązana z programem DB2 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. Użytkownicy programu DB2 mogą otrzymać różne poziomy uprawnień do tworzenia, usuwania, zmieniania i odczytywania poszczególnych obiektów SQL. Uprawnienia są wymagane do wiązania statycznych instrukcji SQL lub do wykonywania dynamicznych instrukcji SQL.

Po utworzeniu pakietu opcja DISABLE/ENABLE umożliwia kontrolowanie, które typy połączeń DB2 mogą uruchamiać pakiet. Można używać narzędzia RACF® i procedur wyjściowych ochrony programu DB2, aby umożliwiać użytkownikom selektywne wykorzystanie narzędzia DDF. Można użyć narzędzia RLF, aby określić ograniczenia czasu procesora dla powiązań zdalnych i powiązań dynamicznych SQL.

Rozważmy pakiet DB2 o nazwie MYPKG, którego właścicielem jest JOE. JOE może umożliwić SAL uruchomienie pakietu przez wydanie instrukcji DB2 GRANT USE. Gdy SAL wykona pakiet:

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

Pojęcia pokrewne:

- “Zagadnienia związane z ochroną w serwerach aplikacji (dla systemów OS/390 i z/OS)” na stronie 93

Podsystem ochrony - serwer aplikacji (dla systemów OS/390 i z/OS)

Wykorzystanie przez serwer aplikacji DB2® podsystemu ochrony (narzędzia RACF lub produktu będącego jego odpowiednikiem) zależy od sposobu zdefiniowania funkcji konwersji nazw przychodzących w tabeli SYSIBM.LUNAMES:

- Jeśli w kolumnie USERNAMES jest określona wartość 'I' lub 'B', konwersja nazw przychodzących jest aktywna i program DB2 zakłada, że administrator programu DB2 wykorzystuje konwersję 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 narzędzie 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 konwersji nazw przychodzących definiują, który użytkownik może połączyć się z serwerem aplikacji DB2.
- 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, program DB2 wywoła zewnętrzny system ochrony w celu sprawdzenia poprawności identyfikatora użytkownika (oraz hasła, jeśli zostało udostępnione).

– Zewnętrzny system ochrony jest wywoływany do sprawdzenia, czy użytkownik ma autoryzację do łączenia się z podsystemem DB2.
- W pozostałych przypadkach informacje wyjściowe autoryzacji są udostępniane w celu zapewnienia listy pomocniczych identyfikatorów autoryzowanego użytkownika.

Więcej informacji można znaleźć w podręczniku *DB2 UDB for OS/390® and z/OS™ Administration Guide*.

Pojęcia pokrewne:

- "Zagadnienia związane z ochroną w serwerach aplikacji (dla systemów OS/390 i z/OS)" na stronie 93

Uwagi związane z ochroną w serwerach aplikacji (dla systemu iSeries)

Gdy requester aplikacji przekierowuje żądanie rozproszonej bazy danych do serwera aplikacji iSeries™, należy uwzględnić następujące zagadnienia związane z ochroną:

- nazwy użytkowników
- parametry ochrony sieci
- ochrona menedżera bazy danych
- ochrona w systemie iSeries

Nazwy użytkowników:

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

Serwer aplikacji iSeries nie wykonuje konwersji przychodzących identyfikatorów użytkowników w celu rozwiązania konfliktów między nieunikalnymi identyfikatorami lub zgrupowaniami wielu użytkowników pod jednym identyfikatorem użytkownika. Każdy identyfikator użytkownika wysyłany z requestera aplikacji musi istnieć na serwerze aplikacji. Metodą zgrupowania żądań przychodzących w jednym identyfikatorze użytkownika, powiązaną z pewnym obniżeniem poziomu ochrony, jest określenie domyślnego identyfikatora 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 w sieci SNA:

Jednostka logiczna LU 6.2 udostępnia trzy główne opcje zabezpieczające sieci:

- ochrona na poziomie sesji
- ochrona na poziomie konwersacji
- szyfrowanie (nie jest obsługiwane przez system iSeries)

Serwer aplikacji DB2® UDB for iSeries korzysta z ochrony na poziomie sesji w dokładnie ten sam sposób, jak czyni to requester aplikacji DB2 UDB for iSeries.

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 iSeries na *NONE (brak domyślnego identyfikatora użytkownika) oraz parametr lub wartość określającą chronione miejsce na *NO.

SECURITY=NONE

Serwer aplikacji nie oczekuje identyfikatora 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 identyfikatora użytkownika, tak więc powinny mieć własny podsystem w przypadku zwykłych sytuacji, gdy aplikacjom DRDA® nie jest potrzebny domyślny identyfikator użytkownika.

Metodę grupowania przychodzących żądań uruchomienia zadania w jednym identyfikatorze użytkownika opisano w sekcji Nazwy użytkowników. Ta metoda nie sprawdza identyfikatora użytkownika wysłanego z requestera aplikacji. Zadanie serwera aplikacji jest uruchamiane z domyślnym identyfikatorem użytkownika i użytkownik, który zainicjował połączenie na serwerze aplikacji, ma prawa dostępu serwera aplikacji, nawet jeśli wysłany identyfikator użytkownika ma ograniczoną autoryzację. Jest to zrealizowane przez zdefiniowanie serwera aplikacji jako miejsca niechronionego, podanie domyślnego identyfikatora użytkownika w pozycji dotyczącej komunikacji w podsystemie iSeries i skonfigurowanie requestera aplikacji do wysyłania identyfikatora użytkownika tylko podczas trwania połączenia. Jeśli wysyłane jest hasło, zamiast domyślnego identyfikatora użytkownika używany jest towarzyszący hasłu identyfikator użytkownika.

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

System iSeries oferuje także opcję zabezpieczającą 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 możliwa jest ochrona kontrolowana przez system na podstawie obiektów.

Ochrona sieci TCP/IP:

Użycie komendy **CRTDDMTCPA** umożliwia określenie, czy serwer będzie akceptował żądania połączenia TCP/IP bez hasła.

Ochrona menedżera bazy danych:

Cała ochrona jest realizowana za pośrednictwem funkcji ochrony systemu OS/400®.

Ochrona systemu:

System iSeries nie zawiera zewnętrznego podsystemu ochrony. Cała ochrona jest realizowana przez funkcję ochrony systemu OS/400, która jest integralną częścią systemu operacyjnego. System operacyjny steruje uprawnieniami do wszystkich obiektów w systemie, łącznie z programami, pakietami, tabelami, widokami i kolekcjami.

Serwer aplikacji steruje autoryzacją dotyczącymi obiektów, które się w nim znajdują. Ochrona obiektów zależy od identyfikatora użytkownika, który rozpoczął zadanie serwera aplikacji. Ten identyfikator użytkownika jest określony w sposób opisany w sekcji Nazwy użytkowników.

Zarządzanie ochroną obiektów może być realizowane 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 można używać w odniesieniu do dowolnego obiektu w systemie. Instrukcje GRANT i REVOKE działają tylko dla obiektów SQL: tabel, widoków i pakietów. Aby zmienić autoryzację dla innych obiektów, takich jak programy czy kolekcje, należy użyć komend GRTOBJAUT i RVKOBJAUT.

Kiedy obiekty są tworzone w systemie, otrzymują one autoryzację domyślną. Identyfikator użytkownika, który tworzy tabele, widoki i pakiety, ma wszystkie uprawnienia. Pozostałe identyfikatory użytkownika (publiczne) mają takie same uprawnienia, jak inni dysponują w odniesieniu do kolekcji lub bibliotek, w których obiekt został utworzony.

Uprawnienia do obiektów, do których odwołują się statyczne lub dynamiczne instrukcje w pakiecie, są sprawdzane w czasie wykonywania 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 może korzystać z tabeli.

Więcej informacji na temat ochrony systemu można znaleźć w sekcji *OS/400 Security - Reference*.

Zadania pokrewne:

• “Nadawanie i odbieranie uprawnień (iSeries)” na stronie 117

Zagadnienia związane z ochroną w serwerach aplikacji (dla systemu VM)

Gdy requester aplikacji przekierowuje żądanie rozproszonej bazy danych do serwera aplikacji DB2® for VM, należy uwzględnić następujące zagadnienia związane z ochroną:

- nazwa użytkownika
- parametry ochrony sieci
- ochrona menedżera bazy danych
- ochrona wymuszona przez zewnętrzny podsystem ochrony

Nazwy użytkowników:

Zarówno w wypadku języka SQL, jak i jednostek logicznych LU 6.2 użytkownicy otrzymują identyfikatory użytkowników o długości od 1 do 8 bajtów. Identyfikator użytkownika musi być unikalny w obrębie systemu operacyjnego, lecz nie musi być unikalny w całej sieci SNA.

Aby wyeliminować konflikty nazw, program DB2 for VM może opcjonalnie korzystać z funkcji konwersji identyfikatorów użytkowników dostępnej w systemie AVS, przy czym muszą być spełnione następujące warunki:

- Serwer aplikacji DB2 for VM musi być uruchamiany w środowisku VM/ESA®.
- Przychodzące żądania połączeń muszą być kierowane przez bramę AVS.
- Requester aplikacji partnerskiej musi używać opcji ochrony konwersacji SECURITY=SAME (w terminologii SNA znanej również jako *already verified* - sprawdzona uprzednio).

Jeśli połączenie jest kierowane do serwera przez system AVS przy użyciu opcji SECURITY=SAME, to wymagana jest konwersja identyfikatora użytkownika AVS. Wydana z poziomu komputera AVS komenda AGW ADD USERID musi zapewnić uwierzytelnienie ze strony systemu ochrony w stosunku do użytkowników łączących się z określonej zdalnej jednostki logicznej lub bramy AVS. Musi istnieć odwzorowanie dla wszystkich przychodzących jednostek logicznych i identyfikatorów użytkowników, którzy łączą się używając opcji 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 autoryzowania przychodzących (sprawdzonych uprzednio) identyfikatorów użytkowników na lokalnym komputerze 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 system AVS za pomocą komendy AGW STOP. Wszystkie autoryzacje ID użytkowników zostają wyzerowane.
- Należy usunąć identyfikator użytkownika za pomocą komendy AGW DELETE USERID.

Przykład identycznych identyfikatorów użytkowników w różnych miastach przedstawia, w jaki sposób funkcja konwersji 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 systemu 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 administrator DBA musi użyć komendy VM GRANT, 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 Montreal, nie korzysta z uprawnień nadanych użytkownikowi JONES w systemie Montreal.

Opis komend AVS obsługujących konwersję identyfikatorów użytkowników można znaleźć w podręczniku *VM/ESA Connectivity Planning, Administration, and Operation*.

Ochrona w sieci:

Jednostka logiczna LU 6.2 udostępnia trzy główne opcje zabezpieczające sieci:

- ochrona na poziomie sesji
- ochrona na poziomie konwersacji
- szyfrowanie.

Serwer aplikacji DB2 for VM korzysta z ochrony na poziomie sesji w taki sam sposób, jak requester aplikacji DB2 for VM.

Requester aplikacji może wysyłać sprawdzony uprzednio 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 ich poprawność za pomocą katalogu VM na hoście serwera aplikacji. Jeśli sprawdzanie poprawności nie powiedzie 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: Program DB2 for VM nie umożliwia szyfrowania, ponieważ system VM/ESA nie obsługuje szyfrowania.

Ochrona menedżera bazy danych:

Serwer aplikacji DB2 for VM sprawdza, czy identyfikator użytkownika określony przez system VM ma uprawnienie CONNECT, aby uzyskać dostęp do bazy danych, a następnie odrzuca połączenie, jeśli go nie ma.

Jako właściciel zasobów 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 system 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 kontroluje dwie klasy obiektów:

- **Pakiety:** Indywidualni użytkownicy posiadają uprawnienia do tworzenia, wymieniania i uruchamiania pakietów za pomocą instrukcji GRANT programu DB2 for VM. Gdy użytkownik tworzy pakiet, automatycznie uzyskuje uprawnienia do uruchamiania lub wymieniania tego pakietu. Inni użytkownicy mający specjalne uprawnienia do uruchamiania pakietu na serwerze aplikacji DB2 for VM za pomocą instrukcji GRANT EXECUTE. Uprawnienie RUN można nadawać użytkownikom indywidualnym lub wszystkim (PUBLIC), co umożliwia wszystkim użytkownikom uruchomienie pakietu.

  Gdy aplikacja jest przetwarzana wstępnie w systemie 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 wstępnego przetwarzania aplikacji. Autor pakietu musi mieć uprawnienia 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, 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 dane systemu DB2 for VM za pomocą 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. 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, produkt VTAM® wywołuje podsystem ochrony w celu wymiany weryfikacji partnerskiej jednostki logicznej. Decyzja o weryfikacji partnerskiej 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 identyfikatora użytkownika i hasła wysłanego z requestera aplikacji. Jeśli podsystemem ochrony jest narzędzie RACF® i brakuje profilu systemu RACF, narzędzie RACF przeprowadza sprawdzenie poprawności. Jeśli w systemie istnieje profil RACF, na przykład RACFPROF, aby zażądać sprawdzenia poprawności przez system RACF, należy użyć następujących instrukcji:

```
RALTER VMXEVENT RACFPROF DELMEM (APPCPWVL/NOCTL

RALTER VMXEVENT RACFPROF ADDMEM (APPCPWVL/CTL

SETEVENT REFRESH RACFPROF
```

Pojęcia pokrewne:

- “DB2 for VM” na stronie 77
- “Zagadnienia związane z ochroną w requesterach aplikacji (dla systemu VM)” na stronie 118

Zadania pokrewne:

- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemu VM)” na stronie 63

Zagadnienia związane z ochroną w serwerach aplikacji (dla systemu VSE)

Ochrona komunikacji międzysystemowej na serwerze aplikacji DB2® for VSE zależy od ustawień programu CICS®. System CICS udostępnia kilka poziomów ochrony:

- Ochrona czasu wiązania.

  Implementacja CICS sprawdzania między jednostkami logicznymi na poziomie sesji SNA LU 6.2. W architekturze LU 6.2 implementacja ochrony czasu wiązania jest opcjonalna. Można ją udostępnić po stronie serwera aplikacji, podając wartość BINDPASSWORD w komendzie CEDA DEFINE CONNECTION podczas definiowania połączenia z requesterem aplikacji. W requesterze aplikacji partnerska jednostka logiczna obsługująca go musi również zapewnić ochronę czasu wiązania i używać tego samego hasła do sprawdzenia partnerskiej jednostki logicznej.

Można użyć ochrony czasu wiązania, aby uniemożliwić nieautoryzowanym systemom zdalnym uruchomienie (powiązanie) sesji z systemem 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.

- Ochrona użytkownika.

  Implementacja CICS ochrony na poziomie konwersacji SNA LU 6.2 zapewnia sprawdzanie użytkownika.

  Ochrona użytkownika oznacza sprawdzanie poprawności identyfikatora użytkownika w tabeli logowania CICS (DFHSNT) przed zaakceptowaniem żądania uruchomienia konwersacji. Na przykład requestery aplikacji DRDA niezdefiniowane w tabeli logowania CICS 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 w komendzie CEDA DEFINE CONNECTION. Istnieją trzy poziomy ochrony podłączenia:

  – LOCAL. Poziom nieobsługiwany przez architekturę DRDA.
  – IDENTIFY. Odpowiednik SECURITY=SAME (lub uprzednie sprawdzenie) w terminologii LU 6.2. W wypadku tego poziomu ochrony CICS “ufa” systemowi zdalnemu w zakresie sprawdzania jego użytkowników, zanim pozwoli im przydzielić konwersację z serwerem DB2 for VSE. W procesie logowania się do systemu CICS wymagany jest tylko identyfikator użytkownika. Jeśli jednak przekazywane jest również hasło, system CICS wykonuje logowanie do systemu przy użyciu hasła.
  – VERIFY. Odpowiednik SECURITY=PGM w terminologii LU 6.2. W wypadku tego poziomu ochrony system CICS oczekuje od zdalnego systemu, że nadeśle on zarówno ID, jak i hasło użytkownika podczas przydzielania konwersacji i odrzuci połączenie, jeśli hasło nie zostało dostarczone.

- Obowiązkowe szyfrowanie na poziomie sesji SNA LU 6.2. Nieobsługiwane.

Ponieważ serwer aplikacji jest odpowiedzialny za zarządzanie zasobami baz danych, narzuca on mechanizmy ochrony sieci, które musi zapewniać requester aplikacji. Na przykład w wypadku 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. 23 na stronie 106:

```
: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 23. Przykładowa pozycja katalogu CMS Communication Directory.

Ochrona menedżera bazy danych:

Konwersja identyfikatorów użytkownika nie jest obsługiwana przez serwer aplikacji VSE. System CICS używa identyfikatora użytkownika przesłanego bezpośrednio z requestera.

Transakcja AXE po uruchomieniu przez requester aplikacji pobiera identyfikator użytkownika z systemu CICS i przesyła go do serwera DB2 for VSE. Aby ustawić wymagany poziom uprawnień użytkownika do zasobów bazy danych, należy zaktualizować identyfikator użytkownika w katalogu SYSTEM.SYSUSERAUTH produktu DB2 for VSE.

Serwer aplikacji DB2 for VSE sprawdza, czy identyfikator użytkownika określony przez system CICS ma uprawnienie CONNECT umożliwiające uzyskanie dostępu do bazy danych i odrzuca połączenie, jeśli użytkownik nie ma właściwych uprawnień.

Jako właściciel zasobów bazy danych, serwer aplikacji DB2 for VSE steruje funkcjami ochrony bazy danych dla obiektów SQL znajdujących się na serwerze aplikacji DB2 for VSE. Dostęp do obiektów zarządzanych przez system DB2 for VSE jest realizowany przy użyciu zestawu uprawnień, które są nadawane użytkownikom przez administratora systemu DB2 for VSE lub właściciela określonego obiektu. Serwer aplikacji DB2 for VSE kontroluje dwie klasy obiektów:

- **Pakiety:** Indywidualni użytkownicy posiadają uprawnienia do tworzenia, wymieniania i uruchamiania pakietów za pomocą instrukcji GRANT programu DB2 for VSE. Gdy użytkownik tworzy pakiet, automatycznie uzyskuje uprawnienia do uruchamiania lub wymieniania tego pakietu. Inni użytkownicy mający specjalne uprawnienia 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 systemie 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.

Opis uprawnień dostępu do serwera aplikacji dla zdalnych requesterów aplikacji można znaleźć w podręczniku *DB2 Server for VSE System Administration*.

Informacje na temat sposobu udostępnienia ochrony połączenia można znaleźć w podręczniku *CICS on Open Systems: Intercommunication Guide*.

Pojęcia pokrewne:

- "Program DB2 for VSE" na stronie 88

Zadania pokrewne:

- "Konfigurowanie programu DB2 jako serwera aplikacji (dla systemu VSE)" na stronie 57

Rozdział 13. Zagadnienia dotyczące ochrony requesterów aplikacji

Zagadnienia związane z ochroną w requesterach aplikacji (dla systemów OS/390 i z/OS)

Jeśli system zdalny przetwarza rozproszoną bazę danych na rzecz aplikacji SQL, musi on spełniać wymogi dotyczące ochrony requestera aplikacji, serwera aplikacji i łączącej ich sieci. Wymagania te należą do co najmniej jednej z następujących kategorii:

- Nazwy użytkowników
- Ochrona sieci
- Ochrona menedżera baz danych
- Podsystem ochrony

Pojęcia pokrewne:

- "DB2 for OS/390 and z/OS" na stronie 69
- "Zagadnienia związane z ochroną w serwerach aplikacji (dla systemów OS/390 i z/OS)" na stronie 93

Zadania pokrewne:

- "Konfigurowanie programu DB2 jako requestera aplikacji (dla systemów OS/390 i z/OS)" na stronie 23

Pojęcia podrzędne

Nazwy użytkowników - requester aplikacji (dla systemów OS/390 i z/OS)

W systemach OS/390® i z/OS™ nazwom użytkowników są przypisane *identyfikatory użytkowników* zawierające od 1 do 8 znaków. Wartość identyfikatora użytkownika musi być unikalna w danym systemie OS/390 i z/OS, 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 ci dwaj użytkownicy to ta sama osoba, to konflikt nie wystąpi. Jeśli natomiast JONES w DALLAS jest inną osobą niż JONES w NEWYORK, sieć SNA (i, co za tym idzie, systemy obsługujące rozproszone bazy danych w sieci) nie są w stanie rozróżnić tych użytkowników. Jeśli nie zostanie to zmienione, JONES w systemie DALLAS będzie korzystać z uprawnień nadanych użytkownikowi JONES w systemie NEWYORK.

Aby wyeliminować konflikty nazewnictwa, program DB2® obsługuje konwersję nazw użytkowników. Jeśli aplikacja po stronie requestera aplikacji DB2 formułuje żądanie dotyczące rozproszonej bazy danych, program DB2 wykonuje konwersję nazwy, o ile baza danych komunikacji zawiera wymaganie wykonania *konwersji nazwy wychodzącej*. Jeśli wybrana zostanie konwersja nazwy wychodzącej, program DB2 wymusi przesłanie hasła przy każdym żądaniu wychodzącym dotyczącym rozproszonej bazy danych.

Konwersja nazw wychodzących w programie DB2 jest uaktywniana przez ustawienie kolumny USERNAMES w tabeli SYSIBM.LUNAMES lub SYSIBM.IPNAMES na wartość

© Copyright IBM Corp. 1993-2004

'O' lub 'B'. Jeśli kolumna ta ma wartość 'O', dla żądań wychodzących jest wykonywana konwersja nazw użytkowników. Jeśli ma ona wartość 'B', konwersja nazw użytkowników jest wykonywana zarówno dla żądań przychodzących, jak i dla wychodzących.

Ponieważ autoryzacja w programie DB2 zależy zarówno od identyfikatora użytkownika, jak i identyfikatora użytkownika DB2 właściciela planu i pakietu, proces konwersji nazwy użytkownika jest wykonywany dla identyfikatora użytkownika, identyfikatora właściciela planu oraz identyfikatora właściciela pakietu. [4]Proces konwersji nazw przeszukuje tabelę SYSIBM.SYSUSERNAMES w następującej kolejności, aby wyszukać wiersz, który jest zgodny z jednym z następujących wzorców (TYPE.AUTHID.LINKNAME):

1. O.AUTHID.LINKNAME — reguła konwersji dla określonego użytkownika do określonego systemu partnerskiego.
2. O.AUTHID.blank — reguła konwersji dla określonego użytkownika do dowolnego systemu partnerskiego.
3. O.blank.LINKNAME — reguła konwersji dla dowolnego użytkownika do określonego systemu partnerskiego.

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

Rozważmy przykład omawiany wcześniej. Użytkownikowi JONES z systemu NEWYORK należy nadać inną nazwę (NYJONES), gdy JONES wysyła żądanie dotyczące rozproszonej bazy danych do systemu DALLAS. Załóżmy, że aplikacja używana przez użytkownika JONES jest własnością DSNPLAN (właściciel planu DB2) i nie należy wykonywać translacji identyfikatora użytkownika, gdy jest on przesyłany do DALLAS. Instrukcje SQL, których należy użyć, aby określić reguły konwersji nazwy w bazie danych komunikacji, przedstawiono na Rys. 24.

```
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 24. Instrukcje SQL dla konwersji nazw wychodzących (SNA).

Wynikowe tabele bazy danych komunikacji przedstawiono na Rys. 25 na stronie 111.

4. Jeśli żądanie jest wysyłane do serwera DB2, konwersja nazwy jest także wykonywana dla właściciela pakietu i właściciela planu. Nazwy właściciela planu i właściciela pakietu nie są nigdy związane z hasłem.

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 25. Konwersja nazw wychodzących.

Rys. 26 przedstawia prostszy przykład połączenia z serwerem aplikacji DRDA® DB2 for OS/390 and z/OS 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 26. Instrukcje SQL konwersji nazw wychodzących (prosty przykład dla architektury SNA).

Rys. 27 na stronie 112 przedstawia prostszy przykład połączenia z serwerem aplikacji DRDA DB2 for OS/390 and z/OS przy użyciu połączenia TCP/IP.

```
-- DB2 dla 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 27. Instrukcje SQL konwersji nazw wychodzących (prosty przykład dla protokołu TCP/IP).

Pojęcia pokrewne:

- “Zagadnienia związane z ochroną w requesterach aplikacji (dla systemów OS/390 i z/OS)” na stronie 109

Ochrona sieci - requester aplikacji (dla systemów OS/390 i z/OS)

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

- Ochrona na poziomie sesji, sterowana przez parametr VERIFY w instrukcji VTAM® APPL.
- Ochrona na poziomie konwersacji sterowana przez zawartość tabeli SYSIBM.SYSLUNAMES.
- Szyfrowanie danych, obsługiwane tylko przez system VTAM 3.4 i późniejsze wydania systemu VTAM.

Serwer aplikacji jest odpowiedzialny za zarządzanie zasobami baz danych i dlatego decyduje on, które opcje zabezpieczające sieci są wymagane od requestera aplikacji. Należy zapisać

wymagania dotyczące ochrony na poziomie konwersacji każdego serwera aplikacji w tabeli SYSIBM.LUNAMES, ustawiając w kolumnie USERNAMES wartości odzwierciedlające wymagania serwera aplikacji.

Możliwe opcje ochrony konwersacji SNA:

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

Ponieważ program DB2® dopasowuje konwersję nazwy użytkownika do ochrony konwersacji wychodzącej, nie pozwala on na użycie opcji SECURITY=SAME, gdy konwersja 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, program DB2 uzyskuje hasło użytkownika z dwóch różnych źródeł:

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

  Rys. 28 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 użytkownicy 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 28. Wysyłanie haseł do miejsc zdalnych.

- Hasła zaszyfrowane są wysyłane do miejsc zdalnych, jeśli kolumna ENCRYPTPSWDS tabeli SYSIBM.SYSLUNAMES zawiera wartość 'Y'. Hasła zaszyfrowane są pobierane z narzędzia RACF® (lub produktu będącego jego odpowiednikiem) i mogą być interpretowane jedynie przez inny system DB2. Podczas komunikowania z systemem innym niż DB2 nie należy ustawiać kolumny ENCRYPTPSWDS na wartość 'Y'.

  Program DB2 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 konwersji nazw, musi utworzyć wiersze w tabeli SYSIBM.SYSUSERNAMES, które spowodują wysłanie nazw bez konwersji. Wykonanie instrukcji przedstawionych na Rys. 29 na stronie 114 pozwala na wysłanie żądań do LUDALLAS i LUNYC bez translacji nazwy użytkownika (identyfikatorów 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 29. Wysyłanie haseł zaszyfrowanych do systemów zdalnych.

SECURITY=NONE
Opcja ta nie jest obsługiwana przez architekturę DRDA, dlatego program DB2 jej nie obsługuje.

Pojęcia pokrewne:

- “Zagadnienia związane z ochroną w requesterach aplikacji (dla systemów OS/390 i z/OS)” na stronie 109

Ochrona menedżera bazy danych - requester aplikacji (dla systemów OS/390 i z/OS)

Jednym ze sposobów zapewnienia przez requester aplikacji ochrony w rozproszonej bazie danych jest konwersja nazw połączeń przychodzących. Aby sterować dostępem do każdego serwera aplikacji, można użyć konwersji nazw wychodzących na podstawie tożsamości użytkownika wysyłającego żądanie i aplikacji wysyłającej żądanie. Inne sposoby używane przez requester aplikacji DB2® w celu ochrony systemu rozproszonego:

Wiązanie aplikacji zdalnych
Użytkownicy wiążą aplikacje zdalne na serwerze aplikacji, wykorzystując komendę DB2 BIND PACKAGE. Program DB2 nie ogranicza użycia komendy BIND PACKAGE na requesterze. Użytkownik nie może jednak użyć pakietu zdalnego, dopóki pakiet ten nie zostanie włączony do planu DB2. Program DB2 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 DB2 GRANT.

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

Wykonywanie aplikacji zdalnych
Aby użytkownik programu DB2 mógł uruchomić zdalną aplikację, musi mieć uprawnienia do uruchamiania planu DB2 związanego z aplikacją. Właścicielowi planu DB2 nadawane są automatycznie uprawnienia do jego uruchomienia. Używając instrukcji DB2 GRANT EXECUTE, można nadać innym użytkownikom uprawnienia do uruchamiania planu. W ten sposób właściciel aplikacji obsługującej rozproszone bazy danych może kontrolować korzystanie z aplikacji dla każdego użytkownika osobno.

Pojęcia pokrewne:

- “Zagadnienia związane z ochroną w requesterach aplikacji (dla systemów OS/390 i z/OS)” na stronie 109

Podsystem ochrony - requester aplikacji (dla systemów OS/390 i z/OS)

Zewnętrznym podsystemem ochrony systemów MVS™ jest narzędzie RACF® lub inne produkty, które obsługują interfejs kompatybilny z narzędziem RACF. Requester aplikacji DB2® nie ma bezpośrednich odwołań do zewnętrznego podsystemu ochrony, z wyjątkiem obsługi hasła szyfrowanego. Zewnętrzny podsystem ochrony jest jednak wykorzystywany pośrednio w requesterze aplikacji w następujących sytuacjach:

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

Pojęcia pokrewne:

- "Zagadnienia związane z ochroną w requesterach aplikacji (dla systemów OS/390 i z/OS)" na stronie 109

Uwagi dotyczące ochrony w requesterach aplikacji (dla systemu iSeries)

Jeśli system zdalny przetwarza rozproszoną bazę danych na rzecz aplikacji SQL, musi on spełniać wymogi dotyczące ochrony requestera aplikacji, serwera aplikacji i łączącej ich sieci. Wymagania te należą do co najmniej jednej z następujących kategorii:

- nazwy użytkowników
- parametry ochrony sieci
- ochrona menedżera bazy danych
- ochrona narzucona przez mechanizmy ochronne systemu iSeries™

Nazwy użytkowników:

W systemach iSeries użytkownicy są przypisani do identyfikatorów użytkowników zawierających od 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 konwersja nazw wychodzących zmieniająca identyfikator użytkownika.

Jednak system iSeries nie dokonuje konwersji 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 iSeries. USER to poprawny identyfikator na serwerze aplikacji, a USING to odpowiadające mu hasło użytkownika.

Ochrona w sieci:

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

- ochrona na poziomie sesji, kontrolowana za pomocą parametru LOCPWD komendy CRTDEVAPPC
- ochrona na poziomie konwersacji, kontrolowana przez system operacyjny OS/400®
- szyfrowanie (nieobsługiwane w systemie operacyjnym 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 i dlatego decyduje on, które opcje zabezpieczające sieci są wymagane od requestera aplikacji. Administrator ochrony systemu iSeries musi sprawdzić wymagania ochrony każdego serwera aplikacji, aby nie przewyższały one wymagań obsługiwanych przez requester aplikacji iSeries.

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 iSeries.

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 iSeries.

SECURITY=NONE
: Opcja nieobsługiwana, jeśli system iSeries jest requesterem aplikacji.

Ochrona menedżera bazy danych:

System iSeries nie zawiera zewnętrznego podsystemu ochrony. Cała ochrona jest realizowana za pośrednictwem systemu OS/400.

Ochrona systemu:

System operacyjny OS/400 steruje autoryzacją dla wszystkich obiektów w systemie, łącznie 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 iSeries. 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: nadawanie uprawnienia do obiektów (Grant Object Authority - GRTOBJAUT) i odbieranie uprawnienia do obiektów (Revoke Object Authority - RVKOBJAUT). Komendy te działają w odniesieniu do dowolnego obiektu w systemie. Instrukcje GRANT i REVOKE działają tylko dla obiektów SQL: tabel, widoków i pakietów. Aby zmienić autoryzację dla innych obiektów, takich jak programy czy kolekcje, należy użyć komend GRTOBJAUT i RVKOBJAUT.

Podczas tworzenia obiektów jednocześnie są tworzone autoryzacje domyślne. Domyślnie użytkownik, który utworzy tabele, widoki i programy, ma wszystkie uprawnienia.

Więcej informacji na temat ochrony systemu można znaleźć w podręczniku *OS/400 Security - Reference*.

Pojęcia pokrewne:

- "Uwagi związane z ochroną w serwerach aplikacji (dla systemu iSeries)" na stronie 99
- "Program DB2 UDB for iSeries" na stronie 77

Zadania pokrewne:

- "Konfigurowanie programu DB2 jako requestera aplikacji – SNA (dla systemu iSeries)" na stronie 31
- "Nadawanie i odbieranie uprawnień (iSeries)" na stronie 117

Nadawanie i odbieranie uprawnień (iSeries)

Procedura postępowania:

Aby nadać użytkownikowi USER1 uprawnienie *USE do programu PGMA, w systemie iSeries należy wprowadzić komendę:

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

Aby odebrać to samo uprawnienie:

```
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) służących 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 iSeries 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 umożliwia tworzenie pakietów.

Komenda powodująca odebranie tego uprawnienia:

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

Pojęcia pokrewne:

- "Uwagi związane z ochroną w serwerach aplikacji (dla systemu iSeries)" na stronie 99
- "Uwagi dotyczące ochrony w requesterach aplikacji (dla systemu iSeries)" na stronie 115
- "Program DB2 UDB for iSeries" na stronie 77

Zagadnienia związane z ochroną w requesterach aplikacji (dla systemu VM)

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

- nazwy użytkowników
- parametry ochrony sieci
- ochrona menedżera bazy danych
- ochrona wymuszona przez zewnętrzny podsystem ochrony

Nazwy użytkowników:

Zarówno w wypadku języka SQL, jak i jednostek logicznych LU 6.2 użytkownicy otrzymują identyfikatory użytkowników o długości od 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 ci dwaj użytkownicy to ta sama osoba, to konflikt nie wystąpi. Jednak jeśli JONES w systemie TORONTO nie jest tą samą osobą co JONES w systemie MONTREAL, sieć SNA (i konsekwentnie systemy rozproszonych baz danych wewnątrz tej sieci) nie może odróżnić użytkownika JONES w systemie TORONTO od użytkownika JONES w systemie MONTREAL. Jeśli nie podejmie się żadnych kroków zapobiegawczych, użytkownik JONES w systemie TORONTO będzie mógł używać uprawnień nadanych użytkownikowi JONES w systemie MONTREAL i odwrotnie.

Aby wyeliminować konflikty nazewnictwa, program DB2® for VM obsługuje konwersję nazw użytkowników. System nie wymusza jednak konwersji identyfikatorów użytkowników. Jeśli wymagana jest konwersja wymuszona przez system, należy się upewnić, że właściwa konwersja nazw przychodzących wykonywana jest na serwerze aplikacji.

Konwersja nazw wychodzących jest wykonywana przy użyciu katalogu komunikacji CMS. Pozycja w katalogu komunikacji CMS musi zawierać wpis :security.PGM. W tym przypadku odpowiednie wartości w znacznikach :userid i :password przepływają do miejsca zdalnego (serwera aplikacji) w żądaniu połączenia.

Utworzenie pozycji pokazanej na Rys. 30 na stronie 119 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 eliminowana zostaje 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 30. Konwersja nazw wychodzących.

Ochrona w sieci:

Po wybraniu nazwy użytkownika reprezentującej requester aplikacji w punkcie zdalnym (serwer aplikacji), requester aplikacji musi dostarczyć wymagane informacje dotyczące ochrony sieci LU 6.2. Jednostka logiczna LU 6.2 dostarcza trzy główne mechanizmy ochrony sieci:

- ochrona na poziomie sesji, określona przy użyciu parametru VERIFY w instrukcji APPL VTAM®
- ochrona na poziomie konwersacji, określona w katalogu komunikacji CMS
- 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.

Architektura DRDA® obsługuje następujące opcje ochrony na poziomie konwersacji SNA:

SECURITY=SAME

Znana także jako sprawdzona uprzednio 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 określona wartość :security.SAME. Jeśli użytkownik korzysta z tej opcji, konwersja wychodzącej nazwy użytkownika nie jest wykonywana. Identyfikator użytkownika wysyłany do zdalnego miejsca DRDA jest identyfikatorem logowania użytkownika CMS. Znacznik :userid w katalogu komunikacji CMS jest ignorowany w przypadku występowania wartości :security.SAME.

SECURITY=PGM

Ta opcja powoduje, że zarówno identyfikator użytkownika, jak i hasło są wysyłane do zdalnego systemu (serwera aplikacji) celem sprawdzenia. Ta opcja ochrony jest używana, gdy wpis :security.PGM jest podany w pozycji Katalog komunikacji CMS requestera aplikacji. Gdy ta opcja jest używana, przeprowadzana jest konwersja wychodzącej nazwy użytkownika.

DB2 for VM nie obsługuje szyfrowania haseł. Hasło może zostać podane w znaczniku :password lub może być przechowywane w pozycji katalogu CP użytkownika używającego instrukcji katalogu APPCPASS. Instrukcja APPCPASS zalecana jest, gdy następuje konieczność zwiększenia ochrony hasła. Jeśli hasło nie zostało podane na pozycji Katalog komunikacji CMS, to na pozycji katalogu systemu użytkownika (VM) poszukiwana jest instrukcja APPCPASS.

Instrukcja APPCPASS:

System VM udostępnia instrukcję APPCPASS w celu zwiększenia poziomu ochrony identyfikatora użytkownika i hasła, używanych przez requester aplikacji do łączenia się z serwerem aplikacji. Instrukcja APPCPASS jest elastyczna i pozwala przechowywać informacje ochrony na jeden z następujących sposobów:

- **Identyfikator użytkownika i hasło:** W tym przypadku znaczniki :userid i :password w katalogu komunikacji CMS muszą być puste.
- **Tylko identyfikator użytkownika:** W tym przypadku znacznik :userid w katalogu komunikacji CMS musi być pusty, a znacznik :password musi zawierać hasło użytkownika.
- **Tylko hasło:** W tym przypadku znacznik :password w katalogu komunikacji CMS musi być pusty, a znacznik :userid musi zawierać identyfikator użytkownika.

Rys. 31 ilustruje przypadek, w którym identyfikator użytkownika jest przechowywany w katalogu komunikacyjnym użytkownika, a hasło w pozycji katalogu użytkownika VM. W pozycji katalogu komunikacyjnego identyfikator użytkownika ma wartość MTLSOU, ale 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 31. Przykład pozycji katalogu komunikacyjnego bez hasła.

Gdy system APPC/VM inicjuje połączenie między requesterem aplikacji i serwerem aplikacji używając konwersacji SECURITY=PGM, odczytuje wartości znaczników :userid i :password i przekazuje je do serwera aplikacji. Jeśli co najmniej jeden z nich jest pusty, system APPC/VM szuka brakujących informacji w pozycji katalogu użytkownika VM. W takim przypadku instrukcja APPCPASS w pozycji katalogu VM powinna mieć następującą postać:

```
APPCPASS TORGATE MTLGATE MTLSOU Q6VBN8XP
```

Instrukcja ta mówi systemowi APPC/VM, że użytkownik (requester aplikacji) żądający połączenia przez (lokalną) bramę AVS TORGATE, partnerską jednostkę logiczną nazwaną MTLGATE i identyfikator 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 na poziomie konwersacji i instrukcji APPCPASS można znaleźć w podręczniku *VM/ESA Connectivity Planning, Administration, and Operation*.

Ochrona menedżera bazy danych:

Jako część ogólnej struktury rozproszonej bazy danych w architekturze DRDA, requester aplikacji może brać udział w kontrolowaniu, którzy użytkownicy mogą tworzyć żądania rozproszonej bazy danych. W programie DB2 for VM requester aplikacji może brać udział w ochronie rozproszonej bazy danych na trzy sposoby:

Konwersja wychodzących nazw użytkowników
Konwersji wychodzących nazw użytkowników można używać do kontrolowania dostępu do określonego requestera aplikacji na podstawie identyfikacji użytkownika tworzącego żądanie. Program DB2 for VM próbuje przeprowadzić translację nazwy użytkownika przed wysłaniem żądania do miejsca zdalnego. Najlepszym sposobem jest jednak sprawdzanie przez serwer aplikacji pochodzenia i wykonywanie konwersji nazw przychodzących, ponieważ użytkownicy requestera aplikacji VM mogą za pomocą katalogu CMS User Communications Directory przesłonić konwersję nazw wychodzących.

Przetwarzanie wstępne aplikacji
Użytkownicy przetwarzają wstępnie aplikacje dla określonego serwera aplikacji, korzystając z komendy SQLPREP EXEC programu DB2 for VM lub z komendy RELOAD PACKAGE programu narzędziowego Database Service Utility (DBSU). DB2 for VM nie ogranicza używania tych usług. Gdy dany użytkownik przetwarza wstępnie aplikację, on właśnie jest właścicielem pakietu wynikowego.

Wykonywanie aplikacji
Aby użytkownik programu 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 GRANT EXECUTE programu DB2 for VM. 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 narzędzie RACF® lub produkt będący jego odpowiednikiem, który zapewnia zgodność interfejsu z narzędziem 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 przez system VTAM do sprawdzania poprawności tożsamości nazwy zdalnej jednostki logicznej.

Pojęcia pokrewne:
- “Zagadnienia związane z ochroną w serwerach aplikacji (dla systemu VM)” na stronie 101
- “DB2 for VM” na stronie 77

Zadania pokrewne:
- “Konfigurowanie programu DB2 jako requestera aplikacji (dla systemu VM)” na stronie 37

Rozdział 14. Reprezentacja danych

Reprezentacja danych (dla systemów OS/390 i z/OS)

Program DB2® jest dostarczany z identyfikatorem domyślnie instalowanego kodowanego zestawu znaków (CCSID) równym 500. To ustawienie domyślne może być niepoprawne dla danej instalacji.

Podczas instalowania programu DB2 należy zmienić identyfikator CCSID na CCSID znaków generowanych i wysyłanych do programu DB2 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 generowała nieprawidłowe wyniki.

Należy sprawdzić, czy podsystem DB2 ma możliwość dokonywania konwersji identyfikatora CCSID każdego serwera aplikacji do instalacyjnego identyfikatora CCSID podsystemu DB2. Program DB2 zawiera tabele konwersji dla większości popularnych kombinacji identyfikatorów CCSID źródła i obiektu docelowego, ale nie dla każdej możliwej kombinacji. Jeśli zaistnieje taka konieczność, można dodać pozycje do zestawu dostępnych tabel konwersji i procedur konwersji.

Więcej informacji na temat konwersji znaków w programach DB2 UDB for OS/390 and z/OS zawiera podręcznik *DB2 Universal Database™ for OS/390® and z/OS™ Administration Guide*.

Pojęcia pokrewne:

- “DB2 for OS/390 and z/OS” na stronie 69
- “Conversion of character data” w podręczniku *Quick Beginnings for DB2 Connect Enterprise Edition*

Zadania pokrewne:

- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemów OS/390 i z/OS)” na stronie 45
- “Konfigurowanie programu DB2 jako requestera aplikacji (dla systemów OS/390 i z/OS)” na stronie 23

Reprezentacja danych (dla systemu iSeries)

Produkty obsługujące architekturę DRDA® automatycznie wykonują wszystkie niezbędne konwersje po stronie serwera aplikacji. Aby tak się działo, wartość CCSID serwera aplikacji musi być obsługiwana przez requester aplikacji w celu przeprowadzenia konwersji.

Dostarczona domyślna wartość identyfikatora CCSID dla systemu OS/400® wynosi 65535; można ją także przedstawić jako X'FFFF'. Ta wartość domyślna nie jest zgodna z innymi produktami IBM®. Identyfikator CCSID systemu może zostać wyświetlony za pomocą komendy CL DSPSYSVAL QCCSID. Może on zostać zmieniony za pomocą komendy CHGSYSVAL. Na przykład: CHGSYSVAL QCCSID VALUE(37). Wartość CCSID w systemie może również zostać przesłonięta wartością CCSID związaną z zadaniem serwera DRDA. Ten identyfikator CCSID może zostać ustawiony za pomocą komendy CL CHGUSRPRF. Na przykład: CHGUSRPRF MYUSERID CCSID(37).

© Copyright IBM Corp. 1993-2004

Serwery aplikacji:

W przypadku serwera aplikacji ważny jest identyfikator CCSID skojarzony z:

Obsługiwanym zadaniem w podsystemie komunikacyjnym
Identyfikator CCSID obsługiwanego zadania musi być zgodny 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 programu DB2® UDB for iSeries™ należy się wpisać do systemu i użyć komendy Zmień profil użytkownika (Change User Profile - CHGUSRPRF) w celu przypisania akceptowalnej wartości identyfikatora CCSID do profilu użytkownika zadania, które będzie obsługiwało żądania DRDA.

Kolekcjami SQL
Kolekcja SQL składa się z obiektu biblioteki 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 niedające się wyświetlić lub zniekształcone dane albo requester aplikacji wyświetli 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 zmiany zadania (Change Job - CHGJOB). Do zmiany wartości identyfikatora CCSID profilu użytkownika dla kolejnych zadań należy użyć komendy zmiany profilu użytkownika (Change User Profile - CHGUSRPRF). Aby uzyskać aktualny identyfikator CCSID w programie CL, należy użyć komendy pobierania atrybutów zadania (Retrieve Job Attributes - RTVJOBA). W trybie interaktywnym należy użyć komendy pracy z zadaniem (Work with Job - WRKJOB) i wybrać na ekranie pracy z zadaniem opcję 2 wyświetlania atrybutów definicji zadania (Display Job Definition Attributes).

Tabelami SQL i innymi plikami programu DB2 UDB for iSeries dostępnymi w sieci DRDA
Tabela SQL odpowiada plikowi fizycznemu programu DB2 UDB 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 niezgodne z requesterem aplikacji. Głównym źródłem niezgodności 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.

Requestery aplikacji:

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, obsługa zarządzania pracą pobiera identyfikator CCSID z wartości systemowej QCCSID. Początkowo wartość systemowa QCCSID wynosi CCSID 65535. Użycie wartości 65535 jako identyfikatora CCSID zadania podczas prób

połączenia z programem 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 systemu iSeries, z którym realizowane jest połączenie.

Identyfikator CCSID zadania można zmienić za pomocą komendy zmiany zadania (Change Job - CHGJOB). Do zmiany wartości identyfikatora CCSID profilu użytkownika dla kolejnych zadań należy użyć komendy zmiany profilu użytkownika (Change User Profile - CHGUSRPRF). Do sprawdzenia, jaki identyfikator CCSID został w rzeczywistości przypisany do zadania w programie języka CL, należy użyć komendy pobierania atrybutów zadania (Retrieve Job Attributes - RTVJOBA), aby uzyskać aktualny identyfikator CCSID. W trybie interaktywnym należy użyć komendy pracy z zadaniem (Work with Job - WRKJOB) i wybrać na ekranie pracy z zadaniem opcję 2 wyświetlania 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 (niekoniecznie jest to identyfikator CCSID tego zadania). Przed programem DB2 for AS/400® V3R1 domyślny był identyfikator CCSID zadania, którego wartością była często liczba 65535 i który był niepoprawny dla architektury DRDA. Domyślny identyfikator CCSID zadania nigdy nie wynosi 65535 i dlatego stanowi lepszy wybór jako identyfikator CCSID plików fizycznych dostępnych za pośrednictwem architektury DRDA.

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

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

- Pliki logiczne zostały zdefiniowane na podstawie pliku fizycznego. W takim przypadku można:
  1. Zapisać 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 kopiowania pliku (Copy File - CPYF).
- Formaty rekordu są współużytkowane w systemie OS/400 w wersji wcześniejszej niż wersja 3 wydanie 1.

Pojęcia pokrewne:

- "Program DB2 UDB for iSeries" na stronie 77
- "Conversion of character data" w podręczniku *Quick Beginnings for DB2 Connect Enterprise Edition*

Zadania pokrewne:

- "Konfigurowanie programu DB2 jako serwera aplikacji przy użyciu architektury SNA (dla systemu iSeries)" na stronie 49
- "Konfigurowanie programu DB2 jako requestera aplikacji – SNA (dla systemu iSeries)" na stronie 31

Reprezentacja danych (dla systemu VM)

Do instalacji należy wybrać najodpowiedniejszy domyślny parametr CHARNAME i identyfikator CCSID. Używanie odpowiednich wartości zapewnia integralność reprezentacji danych znakowych i redukuje obciążenie wydajności związane z konwersją identyfikatorów CCSID.

Serwery aplikacji:

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. Dzieje się tak dlatego, że znaki CP/CS 37/697 odpowiadają identyfikatorowi CCSID równemu 37, który z kolei odpowiada wartości CHARNAME równej ENGLISH.

Aby wyeliminować zbędną konwersję identyfikatorów 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 tych celów:

- Serwer aplikacji ma mniej niż pięć lokalnych requesterów aplikacji (dla requesterów aplikacji parametr protokołu byłby ustawiony na wartość 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 znaków CP/CS 37/697. Zdalne requestery aplikacji korzystają z identyfikatora CCSID równego 285.

  Jeśli domyślnie parametr CHARNAME serwera aplikacji ma wartość ENGLISH, utrzymuje to integralność danych dla lokalnych requesterów aplikacji, lecz powoduje obciążenie wydajności związane z konwersją identyfikatorów CCSID dla wszystkich zdalnych requesterów aplikacji.

  Jeśli domyślnie parametr CHARNAME serwera aplikacji jest ustawiony na wartość UK_ENGLISH, pozwala to uniknąć nadmiernego obciążenia wydajności związanego z konwersją identyfikatorów CCSID dla wszystkich zdalnych requesterów, 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. Więcej szczegółowych informacji na ten temat można znaleźć w podręczniku *DB2 Server for VM System Administration*.

W przypadku nowo zainstalowanej bazy danych parametr CHARNAME serwera aplikacji ma wartość INTERNATIONAL, a domyślny identyfikator CCSID wynosi 500. Prawdopodobnie *nie* jest to prawidłowe ustawienie dla używanego systemu. Domyślną wartością parametru CHARNAME dla systemu migrowanego jest ENGLISH, a domyślny identyfikator CCSID wynosi 37.

Requestery aplikacji:

Requester aplikacji musi mieć ustawione odpowiednie wartości domyślne CHARNAME i CCSID. Dobranie poprawnych wartości zapewnia integralność reprezentacji danych znakowych i redukuje obciążenie wydajności związane z konwersją identyfikatorów CCSID.

Na przykład, jeśli posiadany requester aplikacji DB2 for VM został wygenerowany przy użyciu strony kodowej 37 i zestawu znaków 697(CP/CS 37/697) dla znaków US ENGLISH, requester aplikacji powinien ustawić wartość domyślną parametru CHARNAME na ENGLISH. Dzieje się tak dlatego, że znaki CP/CS 37/697 odpowiadają identyfikatorowi CCSID równemu 37, który z kolei odpowiada wartości CHARNAME równej ENGLISH.

Domyślną wartością parametru CHARNAME nowo zainstalowanego lub migrowanego systemu jest INTERNATIONAL, a identyfikator CCSID wynosi 500. Prawdopodobnie *nie* jest to prawidłowe ustawienie dla wartości używanej instalacji. Aby wyświetlić wartości bieżących domyślnych identyfikatorów CCSID, należy użyć następującej komendy:

```
SQLINIT QUERY
```

Odpowiednia wartość identyfikatora 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:

- Zaktualizuj tabelę konwersji identyfikatorów CCSID serwera aplikacji, aby obsługiwał on konwersję między domyślnym identyfikatorem CCSID requestera aplikacji i domyślnym identyfikatorem CCSID serwera aplikacji (zapoznaj się z podręcznikami produktów serwera aplikacji, aby znaleźć szczegółowe informacje dotyczące dodawania obsługi konwersji CCSID).
- Zmień domyślny identyfikator CCSID requestera aplikacji na identyfikator 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 zestawu znaków CP/CS 37/697. Serwer aplikacji nie obsługuje konwersji z zestawu CCSID 37, lecz obsługuje konwersję z zestawu CCSID 285 (jest to CHARNAME UK-ENGLISH dla SQL/DS).

    Jeśli requester aplikacji został zmieniony, aby mógł używać domyślnego ustawienia parametru CHARNAME równego UK-ENGLISH (i identyfikatora CCSID równego 285), nie zostanie zachowana integralność danych. Jeśli serwer aplikacji chce wyświetlić np. znak funta brytyjskiego (£), 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.

Prawidłowa wartość identyfikatora CCSID dla serwera aplikacji może być jedną z wartości nieobsługiwanych przez tabele konwersji requestera aplikacji. W takim przypadku należy nawiązać połączenie, wykonując jedną z następujących czynności:

- Zaktualizuj tabelę konwersji CCSID requestera aplikacji, aby mogła obsługiwać konwersję między domyślnym identyfikatorem CCSID serwera aplikacji i domyślnym identyfikatorem CCSID requestera aplikacji. (Zapoznaj się z podręcznikami produktów serwera aplikacji. Znajdują się w nich szczegółowe informacje dotyczące dodawania obsługi konwersji CCSID). Tabela ta jest używana przy tworzeniu pliku CMS ARISSTR MACRO, który jest stosowany przez requester aplikacji do obsługi konwersji identyfikatorów CCSID.
- Zmień domyślny identyfikator CCSID serwera aplikacji. Czynność ta powinna zostać wykonana, jeśli tylko jest to możliwe, przy czym trzeba 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.

Więcej szczegółowych informacji na ten temat można znaleźć w podręczniku *DB2 Server for VM System Administration*.

Pojęcia pokrewne:

- “DB2 for VM” na stronie 77
- “Program DB2 for VSE” na stronie 88
- “Conversion of character data” w podręczniku *Quick Beginnings for DB2 Connect Enterprise Edition*

Zadania pokrewne:

- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemu VM)” na stronie 63
- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemu VSE)” na stronie 57
- “Konfigurowanie programu DB2 jako requestera aplikacji (dla systemu VM)” na stronie 37

Część 5. Informacje dodatkowe dla hosta i systemu iSeries

© Copyright IBM Corp. 1993-2004

Rozdział 15. Informacje dodatkowe

Produkty komunikacyjne APPC, które można skonfigurować przy użyciu Asysty podczas konfigurowania

Komunikacja APPC w wielu przypadkach może być skonfigurowana automatycznie za pomocą Asysty podczas konfigurowania. Poniższa tabela zawiera listę produktów, które mogą być konfigurowane za pomocą Asysty podczas konfigurowania:

Tabela 4. Produkty, które można skonfigurować za pomocą Asysty podczas konfigurowania

Produkty	Platforma	Konfigurowanie za pomocą Asysty podczas konfigurowania?
IBM Personal Communications V4.2 i wersje nowsze	Systemy Windows 98, Windows NT i Windows 2000	Tak
IBM Communications Server (serwer)	Windows NT i Windows 2000	Tak
IBM Communications Server (klient)	Systemy Windows 98, Windows NT i Windows 2000	Nie
RUMBA	Systemy Windows 98, Windows NT i Windows 2000	Tak
Microsoft SNA (serwer)	Windows NT i Windows 2000	Nie
Microsoft SNA (klient)	Systemy Windows 98, Windows NT i Windows 2000	Nie

Zadania pokrewne:

- “Ręczne konfigurowanie komunikacji APPC między programem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries” na stronie 11
- “Aktualizowanie profili APPC na serwerze DB2 Connect” na stronie 12

Lista kontrolna włączania serwera aplikacji DB2 (dla systemu VSE)

Poniższa lista kontrolna podsumowuje kroki niezbędne do włączenia requestera aplikacji DRDA. Założono, że system VSE 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. Zainstaluj obsługę CICS ISC i obsługę restartowania resynchronizacji.
2. Zdefiniuj system CICS dla VTAM for VSE.
3. Zasembluj tabelę VTAM LOGMODE z pozycją IBMRDB.
4. Zasembluj tabelę logowania do systemu CICS ze wszystkimi zdefiniowanymi identyfikatorami i hasłami użytkowników zdalnych.
5. Uruchom system CICS z odpowiednimi informacjami SIT:
   - ISC=YES,
   - TST=YES, ARIAXELG zdefiniowany jako RECOVERABLE w DFHTST i zasemblowany,
   - APPLID=nazwa jednostki logicznej (jak została zdefiniowana w instrukcji VTAM APPL).

© Copyright IBM Corp. 1993-2004

6. Zdefiniuj systemy zdalne dla systemu 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, np. o nazwie IBMG. Zainstaluj grupę za pomocą komendy CEDA INSTALL GROUP(IBMG).
7. Zaktualizuj katalog DBNAME (ARISDIRD.A):
   - Zdefiniuj wszystkie nazwy TPN dla systemu CICS znajdujące się w tym katalogu. Nazwy TPN niezdefiniowane dla systemu CICS są bezużyteczne.
   - Zdefiniuj wszystkie serwery aplikacji DB2 for VSE DRDA w tym katalogu z poprawną nazwą TPN.
8. Uruchomi procedurę ARISBDID, aby zasemblować zaktualizowany katalog DBNAME.
9. Przygotuj serwer DB2 for VSE:
   - Uruchom procedurę ARIS342D, aby zainstalować obsługę DRDA.
   - Jeśli aplikacje online DB2 for VSE (na przykład ISQL) są uruchamiane z partycji CICS, nadaj uprawnienie do planowania identyfikatorowi CICS APPLID podanemu w tabeli CICS SIT.
   - Nadaj uprawnienia wszystkim użytkownikom zdalnym.
10. Jeśli jest to konieczne, uruchom transakcję DAXP CICS.
11. Uruchom programu DB2 for VSE z odpowiednim parametrem RMTUSERS i opcjonalnie z parametrami DBNAME i SYNCPNT.
12. Należy przygotować aplikacje na serwerze aplikacji DRDA VSE.

Pojęcia pokrewne:

- “Program DB2 for VSE” na stronie 88

Zadania pokrewne:

- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemu VSE)” na stronie 57

Lista kontrolna włączania requestera aplikacji DB2 (dla systemu 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 kompletne.

1. Zdefiniuj lokalną bramę AVS dla systemu VTAM.
2. Zainstaluj obsługę DRDA w requesterze aplikacji DB2 for VM, używając programu ARISDBMA.
3. Ustaw katalog komunikacyjny CMS i dodaj wszystkie niezbędne instrukcje APPCPASS do katalogu VM na komputerze aplikacji. Aby włączyć katalog komunikacyjny, należy użyć komendy SET COMDIR CMS.
4. Uruchom system VTAM i AVS, aby aplikacje VM mogły zdalnie komunikować się przez sieć SNA.
5. Uruchom program SQLINIT i określ parametry DBNAME, PROTOCOL i CHARNAME, aby wskazać domyślną bazę danych, protokół i identyfikatory CCSID, które mają być używane.
6. Należy przygotować aplikacje na serwerze zdalnym.

Pojęcia pokrewne:

- "DB2 for VM" na stronie 77

Zadania pokrewne:

- "Konfigurowanie programu DB2 jako requestera aplikacji (dla systemu VM)" na stronie 37

Arkusz wartości parametrów TCP/IP

Podczas przechodzenia przez poszczególne etapy konfigurowania w celu zapisania wymaganych wartości należy skorzystać z kolumny *Wartość użytkownika* w poniższej tabeli.

Tabela 5. Wartości TCP/IP wymagane po stronie serwera DB2 Connect

Parametr	Opis	Wartość przykładowa	Wartość użytkownika
Nazwa hosta • Nazwa hosta (*nazwa_hosta*) lub • Adres IP (*adres_ip*)	Zastosuj wartość *nazwa_hosta* lub *adres_ip* zdalnego hosta. Aby ustalić wartość tego parametru: • W celu uzyskania wartości parametru *nazwa_hosta* skontaktuj się z administratorem sieci. • W celu uzyskania wartości parametru *adres_ip* skontaktuj się z administratorem sieci lub wpisz komendę **ping** *nazwa_hosta*.	nyx lub 9.21.15.235	
Nazwa usługi • Nazwa usługi połączeń (*nazwa_usługi*) lub • Numer portu/protokół (*numer_portu/tcp*)	Wartości wymagane w pliku services. Nazwa usługi połączenia jest ustaloną arbitralnie nazwą oznaczającą numer portu połączeniowego po stronie klienta (*numer_portu*). Numer portu dla serwera DB2 Connect i numer portu, na który jest odwzorowywany parametr *svcename* w pliku usług na serwerze bazy danych, muszą być takie same (parametr *svcename* znajduje się w pliku konfiguracyjnym menedżera bazy danych na komputerze hosta). Wartość ta nie może być używana przez żadną inną aplikację i musi być unikalna w pliku usług. Na platformach UNIX wartość ta musi być zwykle większa lub równa 1024. Aby poznać wartości stosowane podczas konfigurowania systemu hosta, należy skontaktować się z administratorem bazy danych.	host1 lub 3700/tcp	

Tabela 5. Wartości TCP/IP wymagane po stronie serwera DB2 Connect (kontynuacja)

Parametr	Opis	Wartość przykładowa	Wartość użytkownika
Nazwa docelowej bazy danych (*nazwa_docelowej_bazy_danych*)	Nazwa bazy danych w formie znanej w systemie hosta lub iSeries. • Jeśli nawiązuje się połączenie z programem DB2 UDB for OS/390 and z/OS, należy użyć nazwy położenia. • Jeśli nawiązuje się połączenie z programem DB2 UDB dla systemu iSeries, należy użyć lokalnej nazwy RDB. • Jeśli nawiązuje się połączenie z programem DB2 dla systemu VM lub VSE, należy użyć wartości dbname.	newyork	
Nazwa lokalnej bazy danych (*lokalna_nazwa_dcs*)	Pseudonim lokalny ustalony arbitralnie, który ma być używany przez serwer DB2 Connect reprezentujący zdalną bazę danych hosta lub systemu iSeries.	ny	
Nazwa węzła (*nazwa_węzła*)	Lokalny alias lub pseudonim opisujący węzeł, gdzie znajduje się baza danych, z którą ma zostać nawiązane połączenie. Można wybrać dowolną nazwę; jednak wszystkie wartości nazw węzłów w ramach lokalnego katalogu węzłów muszą być unikalne.	węzeł_db2	

Zadania pokrewne:

- "Ręczne konfigurowanie komunikacji TCP/IP między programem DB2 Connect a serwerem bazy danych hosta i systemu iSeries" na stronie 3

Wartości parametrów TCP/IP używane przy wpisywaniu baz danych do katalogu

Wypełnij kolumnę *Wartość użytkownika* w poniższym arkuszu.

Tabela 6. Arkusz: Wartości parametrów używane przy wpisywaniu baz danych do katalogu.

Parametr	Opis	Wartość przykładowa	Wartość użytkownika
Nazwa bazy danych (*nazwa_bazy_danych*)	Lokalna nazwa bazy danych DCS (*lokalna_nazwa_dcs*) *zdalnej* bazy danych, określona podczas wpisywania katalogu bazy danych DCS do katalogu, na przykład ny.	ny	
Alias bazy danych (*alias_bazy_danych*)	Arbitralny lokalny pseudonim zdalnej bazy danych. Jeśli alias nie zostanie podany, domyślnie zostanie użyty alias identyczny z nazwą bazy danych (*nazwa_bazy_danych*). Nazwę tą należy stosować, gdy następuje połączenie z bazą danych z poziomu klienta.	lokalny	

Tabela 6. Arkusz: Wartości parametrów używane przy wpisywaniu baz danych do katalogu. (kontynuacja)

Parametr	Opis	Wartość przykładowa	Wartość użytkownika
Nazwa węzła (*nazwa_węzła*)	Należy użyć tej samej wartości dla nazwy węzła (*nazwa_węzła*), przy użyciu której wpisano węzeł do katalogu.	węzeł_db2	

Zadania pokrewne:

- “Ręczne konfigurowanie komunikacji TCP/IP między programem DB2 Connect a serwerem bazy danych hosta i systemu iSeries” na stronie 3
- “Wpisywanie bazy danych do katalogu” na stronie 7

Arkusz wartości parametrów APPC

Przed skonfigurowaniem serwera DB2 Connect administrator hosta lub administrator systemu iSeries i administrator sieci lokalnej powinni wypełnić kopie tego arkusza dla *każdej* bazy danych hosta lub systemu iSeries, z którymi będą nawiązywane połączenia.

Po wypełnieniu pozycji w kolumnie *Wartość użytkownika* można użyć arkusza roboczego do skonfigurowania komunikacji APPC dla programu DB2 Connect. Podczas konfiguracji należy zastąpić wartości przykładowe występujące w instrukcjach własnymi wartościami z arkusza. Liczby w prostokątach (na przykład **1**) służą do określenia związku instrukcji konfiguracyjnych z wartościami z arkusza.

Wartości z arkusza i instrukcje konfiguracyjne dostarczają przykładowych wartości wymaganych parametrów konfiguracyjnych. W wypadku innych parametrów można użyć domyślnych wartości programu komunikacyjnego. Jeśli konfiguracja danej sieci różni się od konfiguracji w instrukcjach, należy skontaktować się z administratorem sieci w celu uzyskania poprawnych wartości.

W instrukcjach dotyczących konfiguracji symbol ***** oznacza pozycje, które należy zmienić, lecz nie mają one swej reprezentacji w arkuszu.

Tabela 7. Arkusz planowania połączeń hosta i serwera iSeries

Nr	Nazwa na serwerze DB2 Connect	Nazwa sieci lub systemu VTAM	Wartość przykładowa	Wartość użytkownika
Elementy sieci po stronie serwera bazy danych hosta lub systemu iSeries				
1	Nazwa hosta	Nazwa sieci lokalnej	SPIFNET	
2	Nazwa partnerskiej jednostki logicznej	Nazwa aplikacji	NYM2DB2	
3	Identyfikator sieci		SPIFNET	
4	Nazwa węzła partnerskiego	Nazwa lokalnego punktu kontrolnego lub punktu SSCP	NYX	
5	Nazwa docelowej bazy danych (*nazwa_docelowej_bazy_danych*)	**OS/390 lub z/OS:** NAZWA MIEJSCA **VM/VSE:** DBNAME **iSeries:** Nazwa relacyjnej bazy danych	NEWYORK	

Tabela 7. Arkusz planowania połączeń hosta i serwera iSeries (kontynuacja)

Nr	Nazwa na serwerze DB2 Connect	Nazwa sieci lub systemu VTAM	Wartość przykładowa	Wartość użytkownika
6	Nazwa połączenia lub nazwa trybu		IBMRDB	
7	Nazwa połączenia		LINKHOST	
8	Adres sieci zdalnej lub sieci LAN	Adres adaptera lokalnego lub adres docelowy	400009451902	
Elementy sieci po stronie serwera DB2 Connect				
9	Identyfikator sieci lub identyfikator sieci LAN		SPIFNET	
10	Nazwa lokalnego punktu kontrolnego		NYX1GW	
11	Nazwa lokalnej jednostki logicznej		NYX1GW0A	
12	Alias lokalnej jednostki logicznej		NYX1GW0A	
13	Identyfikator węzła lub węzła lokalnego	ID BLK	071	
14		ID NUM	27509	
15	Nazwa trybu		IBMRDB	
16	Symboliczna nazwa docelowa		DB2CPIC	
17	Nazwa zdalnego programu transakcyjnego		**OS/390 lub z/OS:** X'07'6DB ('07F6C4C2') lub DB2DRDA **VM/VSE:** AXE dla VSE. Nazwa bazy danych DB2 for VM lub X'07'6DB ('07F6C4C2') for VM **iSeries:** X'07'6DB ('07F6C4C2') lub QCNTEDDM	
Pozycje katalogu DB2 po stronie serwera DB2 Connect				
18	Nazwa węzła		węzeł_db2	
19	Ochrona		program	
20	Nazwa lokalnej bazy danych (*lokalna_nazwa_dcs*)		ny	

Dla każdego serwera wypełnij kopię arkusza w sposób następujący:

1. Dla *identyfikatora sieci* określ nazwę sieci dla hosta i serwerów DB2 Connect (1 , 3 i 9). Zwykle wartości te są takie same. Na przykład SPIFNET.
2. Dla *nazwy partnerskiej jednostki logicznej* (2) określ nazwę aplikacji (APPL) VTAM dla OS/390, z/OS, VSE lub VM. Określ nazwę lokalnego punktu CP dla systemu iSeries.
3. Dla *nazwy węzła partnerskiego* (4) określ nazwę punktu SSCP dla OS/390, z/OS, VM lub VSE. Określ nazwę lokalnego punktu kontrolnego dla systemu iSeries.
4. Dla *nazwy bazy danych* (5) określ nazwę bazy danych hosta i systemu iSeries. Jest to nazwa *LOCATION NAME* dla systemu OS/390 lub z/OS, *DBNAME* dla systemu VM lub VSE albo nazwa relacyjnej bazy danych (RDB) dla systemu iSeries.

5. Dla *nazwy trybu* (6 i 15) zazwyczaj wystarczy użyć wartości domyślnej IBMDRB.
6. Dla *adresu sieci zdalnej* (8) - określ adres kontrolera lub adres lokalnego adaptera docelowego hosta lub systemu iSeries.
7. Określ *nazwę lokalnego punktu kontrolnego* (10) serwera DB2 Connect. Jest ona zwykle identyczna z nazwą jednostki fizycznej systemu.
8. Określ *nazwę lokalnej jednostki logicznej*, która ma zostać użyta przez DB2 Connect (11). Jeśli korzystasz z menedżera punktów synchronizacji (SPM) do zarządzania aktualizacjami na wielu serwerach (z zatwierdzaniem dwufazowym), lokalna jednostka logiczna powinna być jednostką logiczną używaną dla menedżera SPM. W tym wypadku ta jednostka logiczna nie może być również jednostką logiczną punktu kontrolnego.
9. Jako *alias lokalnej jednostki logicznej* (12) zwykle używana jest nazwa identyczna z nazwą lokalnej jednostki logicznej (11).
10. Dla *identyfikatora węzła lokalnego* lub *identyfikatora węzła* (13 i 14) - podaj wartości IDBLK i IDNUM serwera DB2 Connect. Wartość domyślna powinna być poprawna.
11. Wybierz odpowiednią wartość dla *symbolicznej nazwy docelowej* (16).
12. Dla *nazwy programu transakcyjnego (TP)* (zdalnego) (17) użyj wartości domyślnych znajdujących się w arkuszu.
13. Pozostałe pozycje (od 18 do 21) wstaw teraz niewypełnione.

Zadania pokrewne:

- “Ręczne konfigurowanie komunikacji APPC między programem DB2 Connect a serwerem bazy danych hosta lub systemu iSeries” na stronie 11

Parametry instrukcji APPL systemu VTAM programu DB2 Connect

W instrukcji APPL VTAM dostępnych jest wiele parametrów. Parametry omawiane w tym podręczniku odpowiadają tytułom tematów.

LUDBD1

System VTAM używa etykiety instrukcji APPL jako nazwy jednostki logicznej. 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 określona w instrukcji APPL VTAM, ponieważ wszystkie aplikacje VTAM są automatycznie przypisywane do identyfikatora 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).

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

DMINWNL=10

Liczba sesji, dla których zwycięzcą rywalizacji jest ten system. Parametr DMINWNL zawiera wartość domyślną dla przetwarzania żądania CNOS, lecz można go przesłonić dla dowolnego partnera, dodając wiersz do tabeli SYSIBM.LUMODES w bazie danych komunikacji.

DMINWNR=10

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

DSESLIM=20

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

Jeśli partner nie może obsługiwać liczby sesji podanej w parametrach DSESLIM, DMINWNL lub DMINWNR, proces CNOS negocjuje nową wartość dla tych parametrów, która jest akceptowalna 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 programu DB2.

PRTCT=PSWDBD1

Określa hasło VTAM, które ma być użyte, gdy program DB2 próbuje łączyć się z systemem VTAM. Jeśli parametr PRTCT został pominięty, hasło nie jest wymagane i należy pominąć parametr PASSWORD= w programie narzędziowym obsługującym wykaz protokołu zmian programu DB2.

SECACPT=ALREADYV

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

- 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 niezawierające żadnych informacji dotyczących ochrony). Program DB2 odrzuca żądania DRDA zawierające specyfikację SECURITY=NONE.

Najlepiej zawsze podawać wartość SECACPT=ALREADYV, ponieważ poziom ochrony konwersacji SNA dla każdego partnera DB2 jest pobierany z bazy danych komunikacji programu DB2 (kolumna USERSECURITY tabeli SYSIBM.LUNAMES). Parametr SECACPT=ALREADYV zapewnia największą elastyczność w wyborze wartości dla parametru USERSECURITY.

VERIFY=NONE

Identyfikuje poziom ochrony sesji SNA (weryfikację partnerskiej jednostki logicznej) wymagany przez ten system DB2. Wartość NONE oznacza, że weryfikacja partnerskiej jednostki logicznej nie jest wymagana.

W programie DB2 nie ma ograniczeń w wyborze wartości dla parametru VERIFY. W sieci niezaufanej zaleca się ustawienie wartości VERIFY=REQUIRED. Ustawienie VERIFY=REQUIRED powoduje, że system VTAM odrzuca partnerów, którzy nie mogą wykonać weryfikacji partnerskiej jednostki logicznej. Jeśli zostanie

wybrane ustawienie VERIFY=OPTIONAL, system 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 program DB2 jest w stanie obsługiwać zatwierdzanie dwufazowe. System VTAM korzysta z tych informacji, aby przekazać partnerowi, że zatwierdzanie dwufazowe jest możliwe. Podanie tego parametru powoduje, że program DB2 automatycznie używa dwufazowego zatwierdzania, jeśli tylko partner jest w stanie je obsłużyć.

ATNLOSS=ALL
Wskazuje, że program DB2 musi być każdorazowo informowany o zakończeniu sesji VTAM. Umożliwia to wykonywanie przez program DB2 resynchronizacji SNA, gdy jest to potrzebne.

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

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

Pojęcia pokrewne:

- “Podsystem ochrony - serwer aplikacji (dla systemów OS/390 i z/OS)” na stronie 98
- “Ochrona sieci - serwer aplikacji (dla systemów OS/390 i z/OS)” na stronie 96
- “Ochrona sieci - requester aplikacji (dla systemów OS/390 i z/OS)” na stronie 112
- “Podsystem ochrony - requester aplikacji (dla systemów OS/390 i z/OS)” na stronie 115

Zadania pokrewne:

- “Konfigurowanie programu DB2 jako serwera aplikacji (dla systemów OS/390 i z/OS)” na stronie 45
- “Konfigurowanie programu DB2 jako requestera aplikacji (dla systemów OS/390 i z/OS)” na stronie 23

Część 6. Dodatki i uzupełnienia

© Copyright IBM Corp. 1993-2004

Dodatek A. Informacje techniczne dotyczące programu DB2 Universal Database

Centrum informacyjne DB2

Centrum informacyjne DB2® zapewnia dostęp do wszystkich informacji potrzebnych do pełnego wykorzystania możliwości programów z rodziny DB2, takich jak DB2 Universal Database™, DB2 Connect™, DB2 Information Integrator i DB2 Query Patroller™. Centrum informacyjne DB2 zapewnia także dostęp do informacji związanych z podstawowymi funkcjami i komponentami DB2, takimi jak replikacja, opracowywanie danych i rozszerzenia DB2.

Poniżej wymieniono funkcje Centrum informacyjnego DB2 dostępne w wypadku korzystania z przeglądarek Mozilla 1.0 lub nowszych albo Microsoft® Internet Explorer 5.5 lub nowszych. Niektóre funkcje wymagają włączenia obsługi języka JavaScript™:

Elastyczne opcje instalacji

Użytkownik może określić metodę wyświetlania dokumentacji DB2, wybierając opcję, która najlepiej odpowiada jego potrzebom:

- Aby mieć łatwy dostęp do zawsze aktualnej dokumentacji, należy korzystać z niej bezpośrednio w Centrum informacyjnym DB2 w serwisie WWW firmy IBM® pod adresem: http://publib.boulder.ibm.com/infocenter/db2help/
- Aby zmniejszyć nakład pracy związany z przeprowadzaniem aktualizacji i ograniczyć ruch do sieci intranet, można zainstalować dokumentację DB2 na jednym serwerze intranetowym.
- Aby zwiększyć elastyczność działania i zmniejszyć zależność od połączeń sieciowych, można zainstalować dokumentację programu DB2 na komputerze lokalnym.

Wyszukiwanie

Wszystkie tematy Centrum informacyjnego DB2 można przeszukiwać, wprowadzając szukany zwrot w polu tekstowym **Szukaj**. Aby znaleźć tekst dokładnie odpowiadający szukanemu tekstowi, należy umieścić wyszukiwane słowa w cudzysłowie; można też zawęzić obszar wyszukiwania, korzystając ze znaków zastępczych (*, ?) i operatorów boolowskich (AND, NOT, OR).

Spis treści uporządkowany według zadań

Tematy w dokumentacji DB2 można znaleźć, korzystając z jednego spisu treści. Spis treści jest zorganizowany przede wszystkim według typów wykonywanych zadań, ale zawiera także takie pozycje jak przegląd produktu, informacje dodatkowe, indeks i glosariusz.

- Przeglądy produktów opisują związki między dostępnymi produktami z rodziny DB2, funkcje oferowane przez te produkty i najnowsze informacje dotyczące każdego z nich.
- Kategorie zadań, takie jak instalacja, administracja i projektowanie, zawierają tematy umożliwiające szybkie wykonanie zadań i lepsze zrozumienie związanych z nimi zagadnień.
- Informacje dodatkowe zawierają między innymi tematy dotyczące składni instrukcji i komend, pomoc dotyczącą komunikatów i parametrów konfiguracyjnych.

Wskazywanie bieżącego tematu w spisie treści

Istnieje możliwość wskazania w spisie treści pozycji odpowiadającej wyświetlanemu

© Copyright IBM Corp. 1993-2004

aktualnie tematowi. W tym celu należy kliknąć przycisk **Odśwież/Pokaż bieżący temat** w ramce spisu treści lub przycisk **Pokaż w spisie treści** w ramce zawartości. Funkcja ta jest przydatna, kiedy użytkownik kliknął kilka odsyłaczy do tematów pokrewnych, znajdujących się w kilku plikach, lub otworzył temat z listy wyników wyszukiwania.

Indeks Dostęp do całej dokumentacji można uzyskać z poziomu indeksu. Indeks jest uporządkowany alfabetycznie według haseł.

Glosariusz
Definicje terminów używanych w dokumentacji DB2 można znaleźć w glosariuszu. Glosariusz jest uporządkowany alfabetycznie według terminów.

Zintegrowane informacje w językach narodowych
Informacje w Centrum informacyjnym DB2 są wyświetlane w języku określonym jako preferowany w ustawieniach używanej przeglądarki. Jeśli nie istnieje przetłumaczona wersja określonego tematu w języku wybranym przez użytkownika, temat ten wyświetlany jest w Centrum informacyjnym DB2 w języku angielskim.

Informacje techniczne dotyczące serwerów iSeries™ można znaleźć w Centrum informacyjnym IBM eServer™ iSeries pod adresem: www.ibm.com/eserver/iseries/infocenter/.

Zadania pokrewne:

- "Aktualizowanie Centrum informacyjnego DB2 zainstalowanego na komputerze lokalnym lub serwerze intranetowym" na stronie 149

Instalowanie Centrum informacyjnego DB2 przy użyciu Kreatora instalacji DB2 (UNIX)

Istnieją następujące trzy metody uzyskiwania dostępu do dokumentacji produktu DB2: w serwisie WWW firmy IBM, na serwerze intranetowym lub na komputerze lokalnym. Domyślnie produkty DB2 uzyskują dostęp do dokumentacji DB2 z poziomu serwisu WWW firmy IBM. Aby korzystać z dokumentacji DB2 na serwerze intranetowym lub na własnym komputerze, należy zainstalować dokumentację z dysku CD *Centrum informacyjne DB2*. Przy użyciu Kreatora instalacji DB2 można zdefiniować preferencje instalacji i zainstalować Centrum informacyjne DB2 na komputerze działającym pod kontrolą systemu operacyjnego UNIX.

Wymagania wstępne:

Ta sekcja zawiera listę wymagań dotyczących sprzętu, systemów operacyjnych, oprogramowania i komunikacji, których spełnienie jest niezbędne do zainstalowania Centrum informacyjnego DB2 na komputerach z systemem UNIX.

- **Wymagania dotyczące sprzętu**
  Wymagany jest jeden z następujących procesorów:
  - PowerPC (AIX)
  - HP 9000 (HP-UX)
  - Intel 32–bitowy (Linux)
  - komputery Solaris UltraSPARC (Środowisko Operacyjne Solaris)
- **Wymagania dotyczące systemu operacyjnego**
  Wymagany jest jeden z następujących systemów operacyjnych:
  - IBM AIX 5.1 (dla procesora PowerPC)
  - HP-UX 11i (dla procesora HP 9000)

  - Red Hat Linux 8.0 (dla 32–bitowego procesora Intel)
  - SuSE Linux 8.1 (dla 32–bitowego procesora Intel)
  - Sun Solaris, wersja 8 (dla komputerów UltraSPARC ze Środowiskiem Operacyjnym Solaris)

  Uwaga: Centrum informacyjne DB2 może zostać uruchomione w systemach operacyjnych UNIX obsługujących klientów DB2. Dlatego zalecane jest uzyskiwanie dostępu do Centrum informacyjnego DB2 w serwisie WWW firmy IBM lub zainstalowanie Centrum informacyjnego DB2 i korzystanie z niego na serwerze intranetowym.

- **Wymagania dotyczące oprogramowania**
  - Obsługiwana jest następująca przeglądarka:
    - Mozilla, wersja 1.0 lub nowsza
- Kreator instalacji DB2 to instalator z graficznym interfejsem użytkownika. Do uruchomienia Kreatora instalacji DB2 na danym komputerze wymagana jest implementacja oprogramowania X Window System umożliwiającego prezentację graficznego interfejsu użytkownika. Przed uruchomieniem Kreatora instalacji DB2 należy upewnić się, że terminal został poprawnie zdefiniowany. Na przykład w wierszu komend wprowadź następującą komendę:

  ```
  export DISPLAY=9.26.163.144:0.
  ```
- **Wymagania dotyczące komunikacji**
  - TCP/IP

Procedura:

Aby zainstalować Centrum informacyjne DB2 przy użyciu Kreatora instalacji DB2:

1. Zaloguj się w systemie.
2. Włóż i podłącz w systemie dysk CD Centrum informacyjne DB2.
3. Przejdź do katalogu, w którym jest podłączony dysk CD, wpisując następującą komendę:

   ```
   cd /cd
   ```

   gdzie */cd* oznacza punkt podłączenia dysku CD.
4. Wprowadź komendę **./db2setup**, aby uruchomić Kreatora instalacji DB2.
5. Zostanie otwarte okno Wyrzutnia konfiguracji programu IBM DB2. Aby przejść bezpośrednio do instalacji Centrum informacyjnego DB2, kliknij opcję **Instalacja produktu**. Informacje o wykonywaniu pozostałych kroków procedury można znaleźć w pomocy elektronicznej. Aby wywołać pomoc elektroniczną, kliknij opcję **Pomoc**. Aby zakończyć instalację w dowolnym momencie, można kliknąć przycisk **Anuluj**.
6. Na stronie **Wybierz produkt, który chcesz zainstalować** kliknij przycisk **Dalej**.
7. Na stronie **Witamy w Kreatorze instalacji DB2** kliknij przycisk **Dalej**. Kreator instalacji DB2 przeprowadzi użytkownika przez proces instalacji programu.
8. Aby kontynuować instalację, trzeba zaakceptować warunki umowy licencyjnej. Na stronie **Umowa licencyjna** wybierz opcję **Akceptuję postanowienia umowy licencyjnej** i kliknij przycisk **Dalej**.
9. Na stronie **Wybierz działanie instalacyjne** wybierz opcję **Zainstaluj Centrum informacyjne DB2 na tym komputerze**. Aby użyć pliku odpowiedzi do zainstalowania Centrum informacyjnego DB2 na tym komputerze lub innych komputerach w dogodnym momencie w przyszłości, wybierz opcję **Zapisz ustawienia w pliku odpowiedzi**. Kliknij przycisk **Dalej**.

10. Na stronie **Wybierz języki do zainstalowania** wybierz języki, w których ma być zainstalowane Centrum informacyjne DB2. Kliknij przycisk **Dalej**.
11. Na stronie **Określ port Centrum informacyjnego DB2** skonfiguruj Centrum informacyjne DB2 pod kątem komunikacji przychodzącej. Kliknij przycisk **Dalej**, aby kontynuować instalację.
12. Na stronie **Początek kopiowania plików** dokonaj przeglądu wybranych opcji instalacji. Aby zmienić dowolne ustawienia, kliknij przycisk **Wstecz**. Kliknij przycisk **Instaluj**, aby skopiować pliki Centrum informacyjnego DB2 na komputer lokalny.

Centrum informacyjne DB2 można także zainstalować przy użyciu pliku odpowiedzi.

Protokoły instalacji db2setup.his, db2setup.log i db2setup.err domyślnie znajdują się w katalogu /tmp.

W pliku db2setup.log przechwytywane są wszystkie informacje dotyczące instalacji produktu DB2, w tym informacje o błędach. W pliku db2setup.his zapisywane są wszystkie instalacje produktów DB2 na danym komputerze. Program DB2 dopisuje plik db2setup.log do pliku db2setup.his. W pliku db2setup.err przechwytywane są wszystkie błędy zwracane przez środowisko Java, na przykład wyjątki oraz informacje o pułapkach.

Po zakończeniu instalacji Centrum informacyjne DB2 będzie zainstalowane w jednym z następujących katalogów, zależnie od typu używanego systemu operacyjnego UNIX:

- AIX: /usr/opt/db2_08_01
- HP-UX: /opt/IBM/db2/V8.1
- Linux: /opt/IBM/db2/V8.1
- Środowisko Operacyjne Solaris: /opt/IBM/db2/V8.1

Zadania pokrewne:

- "Instalowanie Centrum informacyjnego DB2 przy użyciu Kreatora instalacji DB2 (Windows)" na stronie 146

Instalowanie Centrum informacyjnego DB2 przy użyciu Kreatora instalacji DB2 (Windows)

Istnieją następujące trzy metody uzyskiwania dostępu do dokumentacji produktu DB2: w serwisie WWW firmy IBM, na serwerze intranetowym lub na komputerze lokalnym. Domyślnie produkty DB2 uzyskują dostęp do dokumentacji DB2 umieszczonej w serwisie WWW firmy IBM. Aby korzystać z dokumentacji DB2 na serwerze intranetowym lub na własnym komputerze, należy zainstalować dokumentację DB2 z dysku CD *Centrum informacyjne DB2*. Korzystając z Kreatora instalacji DB2, można określić preferencje dotyczące instalacji i zainstalować Centrum informacyjne DB2 na komputerze z systemem operacyjnym Windows.

Wymagania wstępne:

Ta sekcja zawiera listę wymagań dotyczących sprzętu, systemów operacyjnych, oprogramowania i komunikacji, których spełnienie jest niezbędne do zainstalowania Centrum informacyjnego DB2 na komputerach z systemem Windows.

- **Wymagania dotyczące sprzętu**

  Wymagany jest jeden z następujących procesorów:

  – komputery 32-bitowe: procesor Pentium lub kompatybilny z Pentium
- **Wymagania dotyczące systemu operacyjnego**

Wymagany jest jeden z następujących systemów operacyjnych:

– Windows 2000
– Windows XP

Uwaga: Centrum informacyjne DB2 może zostać uruchomione w systemach operacyjnych Windows obsługujących klientów DB2. Dlatego zalecane jest uzyskiwanie dostępu do Centrum informacyjnego DB2 w serwisie WWW firmy IBM lub zainstalowanie Centrum informacyjnego DB2 i korzystanie z niego na serwerze intranetowym.

- **Wymagania dotyczące oprogramowania**
  – Obsługiwane są następujące przeglądarki:
    - Mozilla, wersja 1.0 lub nowsza
    - Internet Explorer, wersja 5.5 lub 6.0 (wersja 6.0 dla systemu Windows XP)
- **Wymagania dotyczące komunikacji**
  – TCP/IP

Ograniczenia:

- Aby zainstalować Centrum informacyjne DB2, trzeba mieć konto z uprawnieniami administratora.

Procedura:

Aby zainstalować Centrum informacyjne DB2 przy użyciu Kreatora instalacji DB2:

1. Zaloguj się w systemie, używając konta zdefiniowanego w celu zainstalowania Centrum informacyjnego DB2.
2. Włóż dysk CD do napędu. Jeśli opcja automatycznego uruchamiania jest włączona, zostanie otwarta Wyrzutnia instalacji programu IBM DB2.
3. Kreator instalacji DB2 określi język systemu i uruchomi program instalacyjny w tym języku. Aby uruchomić program instalacyjny w języku innym niż angielski lub w przypadku gdy program instalacyjny nie uruchamia się automatycznie, można uruchomić Kreatora instalacji DB2 ręcznie.

   Aby ręcznie uruchomić Kreatora instalacji DB2:

   a. Kliknij przycisk **Start** i wybierz opcję **Uruchom**.
   b. W polu **Otwórz** wpisz następującą komendę:

      ```
      x:\setup.exe /i dwuliterowy identyfikator języka
      ```

      gdzie *x:* reprezentuje napęd dysków CD, a *dwuliterowy identyfikator języka* reprezentuje język, w którym ma zostać uruchomiony program instalacyjny.
   c. Kliknij przycisk **OK**.
4. Zostanie otwarte okno Wyrzutnia instalacji programu IBM DB2. Aby przejść bezpośrednio do instalacji Centrum informacyjnego DB2, kliknij opcję **Instalacja produktu**. Informacje o wykonywaniu pozostałych kroków procedury można znaleźć w pomocy elektronicznej. Aby wywołać pomoc elektroniczną, kliknij opcję **Pomoc**. Aby zakończyć instalację w dowolnym momencie, można kliknąć przycisk **Anuluj**.
5. Na stronie **Wybierz produkt, który chcesz zainstalować** kliknij przycisk **Dalej**.
6. Na stronie **Witamy w Kreatorze instalacji DB2** kliknij przycisk **Dalej**. Kreator instalacji DB2 przeprowadzi użytkownika przez proces instalacji programu.
7. Aby kontynuować instalację, trzeba zaakceptować warunki umowy licencyjnej. Na stronie **Umowa licencyjna** wybierz opcję **Akceptuję postanowienia umowy licencyjnej** i kliknij przycisk **Dalej**.

8. Na stronie **Wybierz działanie instalacyjne** wybierz opcję **Zainstaluj Centrum informacyjne DB2 na tym komputerze**. Aby użyć pliku odpowiedzi do zainstalowania Centrum informacyjnego DB2 na tym komputerze lub innych komputerach w dogodnym momencie w przyszłości, wybierz opcję **Zapisz ustawienia w pliku odpowiedzi**. Kliknij przycisk **Dalej**.
9. Na stronie **Wybierz języki do zainstalowania** wybierz języki, w których ma być zainstalowane Centrum informacyjne DB2. Kliknij przycisk **Dalej**.
10. Na stronie **Określ port Centrum informacyjnego DB2** skonfiguruj Centrum informacyjne DB2 pod kątem komunikacji przychodzącej. Kliknij przycisk **Dalej**, aby kontynuować instalację.
11. Na stronie **Początek kopiowania plików** dokonaj przeglądu wybranych opcji instalacji. Aby zmienić dowolne ustawienia, kliknij przycisk **Wstecz**. Kliknij przycisk **Instaluj**, aby skopiować pliki Centrum informacyjnego DB2 na komputer lokalny.

Centrum informacyjne DB2 można zainstalować przy użyciu pliku odpowiedzi. Można także użyć komendy **db2rspgn** do wygenerowania pliku odpowiedzi na podstawie istniejącej instalacji.

Informacje na temat błędów napotkanych podczas instalacji można znaleźć w plikach db2.log i db2wi.log, które znajdują się w katalogu 'Moje dokumenty'\DB2LOG\. Położenie katalogu 'Moje dokumenty' zależy od ustawień na danym komputerze.

W pliku db2wi.log przechwytywane są najnowsze informacje dotyczące instalacji produktu DB2. W pliku db2.log przechwytywana jest historia instalacji produktów DB2.

Zadania pokrewne:

- "Instalowanie Centrum informacyjnego DB2 przy użyciu Kreatora instalacji DB2 (UNIX)" na stronie 144

Uruchamianie Centrum informacyjnego DB2

Centrum informacyjne DB2 zapewnia dostęp do wszystkich informacji potrzebnych do pełnego wykorzystania możliwości produktów DB2, takich jak DB2 Universal Database, DB2 Connect, DB2 Information Integrator i DB2 Query Patroller, dla systemów operacyjnych Linux, UNIX i Windows.

Centrum informacyjne DB2 można wywołać z jednego z następujących miejsc:

- komputery z zainstalowanym klientem lub serwerem DB2 UDB
- serwer intranetowy lub komputer lokalny z zainstalowanym Centrum informacyjnym DB2
- serwis WWW firmy IBM

Wymagania wstępne:

Przed wywołaniem Centrum informacyjnego DB2 należy wykonać następujące czynności:

- *Opcjonalnie*: Skonfiguruj przeglądarkę do wyświetlania tematów w preferowanym języku
- *Opcjonalnie*: Skonfiguruj klienta DB2 do korzystania z Centrum informacyjnego DB2 zainstalowanego na komputerze lokalnym lub serwerze intranetowym

Procedura:

Aby wywołać Centrum informacyjne DB2 na komputerze, na którym zainstalowany jest klient lub serwer DB2 UDB:

- W menu Start (w systemie operacyjnym Windows): Kliknij kolejno opcje: **Start ⟶ Programy ⟶ IBM DB2 ⟶ Informacje ⟶ Centrum informacyjne**.
- W wierszu komend:
  - W systemie operacyjnym Linux lub UNIX wpisz komendę **db2icdocs**.
  - W systemie operacyjnym Windows wpisz komendę **db2icdocs.exe**.

Aby przy użyciu przeglądarki WWW otworzyć Centrum informacyjne DB2 zainstalowane na serwerze intranetowym lub komputerze lokalnym:

- Otwórz stronę WWW pod adresem http://<nazwa-hosta>:<numer-portu>/, gdzie <nazwa-hosta> to nazwa hosta, a <numer-portu> to numer portu, na którym dostępne jest Centrum informacyjne DB2.

Aby w przeglądarce WWW otworzyć Centrum informacyjne DB2 dostępne w serwisie WWW firmy IBM:

- Otwórz stronę WWW pod adresem: publib.boulder.ibm.com/infocenter/db2help/.

Pojęcia pokrewne:

- "Centrum informacyjne DB2" na stronie 143

Zadania pokrewne:

- "Konfiguracja przeglądarki w celu umożliwienia wyświetlania tematów pomocy w preferowanym języku" na stronie 150
- "Wywoływanie pomocy kontekstowej z poziomu narzędzia DB2" na stronie 157
- "Aktualizowanie Centrum informacyjnego DB2 zainstalowanego na komputerze lokalnym lub serwerze intranetowym" na stronie 149
- "Wywoływanie pomocy dotyczącej komunikatów przy użyciu procesora wiersza komend" na stronie 158
- "Wywoływanie pomocy dotyczącej komend przy użyciu procesora wiersza komend" na stronie 158
- "Wywoływanie pomocy dotyczącej stanu SQL przy użyciu procesora wiersza komend" na stronie 159

Aktualizowanie Centrum informacyjnego DB2 zainstalowanego na komputerze lokalnym lub serwerze intranetowym

Centrum informacyjne DB2 dostępne pod adresem http://publib.boulder.ibm.com/infocenter/db2help/ jest okresowo aktualizowane o nową lub zmienioną dokumentację. Firma IBM może także udostępnić aktualizacje Centrum informacyjnego DB2, które mogą zostać pobrane i zainstalowane na komputerze lokalnym lub na serwerze intranetowym. Zaktualizowanie Centrum informacyjnego DB2 nie powoduje zaktualizowania produktów klienta lub serwera DB2.

Wymagania wstępne:

Wymagany jest komputer podłączony do Internetu.

Procedura:

Aby zaktualizować Centrum informacyjne DB2 zainstalowane na komputerze lokalnym lub serwerze intranetowym:

1. Otwórz Centrum informacyjne DB2 dostępne w serwisie WWW firmy IBM pod adresem: http://publib.boulder.ibm.com/infocenter/db2help/

2. Na stronie powitania, w sekcji Downloads pod nagłówkiem Service and Support kliknij odsyłacz **DB2 Universal Database Documentation**.
3. Sprawdź, czy zainstalowane lokalnie Centrum informacyjne DB2 jest nieaktualne, porównując poziom najnowszego obrazu dokumentacji z poziomem dokumentacji, która jest zainstalowana na komputerze lokalnym. Poziom zainstalowanej dokumentacji można sprawdzić na stronie powitania Centrum informacyjnego DB2.
4. Jeśli dostępna jest nowsza wersja Centrum informacyjnego DB2, pobierz najnowszy obraz *Centrum informacyjnego DB2* odpowiedni dla używanego systemu operacyjnego.
5. Aby zainstalować najnowszy obraz *Centrum informacyjnego DB2*, postępuj zgodnie z instrukcjami dostępnymi na stronie WWW.

Zadania pokrewne:

- "Kopiowanie plików z dysku CD-ROM z dokumentacją HTML programu DB2 na serwer WWW" w podręczniku *DB2 Personal Edition - Krótkie wprowadzenie*

Informacje pokrewne:

- "Dokumentacja DB2 w postaci plików PDF i w postaci drukowanej" na stronie 151

Konfiguracja przeglądarki w celu umożliwienia wyświetlania tematów pomocy w preferowanym języku

Centrum informacyjne DB2 wyświetla tematy pomocy w przeglądarce w języku określonym w preferencjach przeglądarki. Jeśli dany temat nie został przetłumaczony na preferowany język, tekst wyświetlany jest w języku angielskim.

Procedura postępowania:

Aby wyświetlać tematy pomocy w preferowanym języku w przeglądarce WWW Internet Explorer:

1. W programie Internet Explorer kliknij kolejno opcje: **Narzędzia** —> **Opcje internetowe** —> **Języki**. Zostanie otwarte okno Preferencje językowe.
2. Sprawdź, czy na liście języków jako pierwszy wyświetlany jest preferowany język.
   - Aby dodać do listy nowy język, kliknij przycisk **Dodaj**.
   - Aby przenieść język do góry listy, zaznacz język i klikaj przycisk **Przenieś w górę** do momentu, aż język będzie wyświetlony jako pierwszy na liście.

Aby wyświetlać tematy pomocy w preferowanym języku w przeglądarce WWW Mozilla:

1. W programie Mozilla wybierz kolejno opcje **Edit** (Edycja) —> **Preferences** (Preferencje) —> **Languages** (Języki). W oknie Preferences (Preferencje) zostanie wyświetlony panel Languages (Języki).
2. Sprawdź, czy na liście języków jako pierwszy wyświetlany jest preferowany język.
   - Aby dodać do listy nowy język, kliknij przycisk **Add...** (Dodaj), aby wybrać język w oknie Add Languages (Dodaj język).
   - Aby przenieść język do góry listy, zaznacz język i klikaj przycisk **Move Up** (Przenieś w górę) do momentu, aż język będzie wyświetlony jako pierwszy na liście.

Dokumentacja DB2 w postaci plików PDF i w postaci drukowanej

W poniższych tabelach dostępne są oficjalne tytuły podręczników, numery zamówień i nazwy plików PDF. Aby zamówić podręcznik w postaci drukowanej, trzeba znać oficjalny tytuł podręcznika. Aby wydrukować plik PDF, trzeba znać nazwę danego pliku PDF.

Dokumentacja programu DB2 uporządkowana jest według następujących kategorii:

- Podstawowe informacje o DB2
- Informacje administracyjne
- Informacje o projektowaniu aplikacji
- Informacje o inteligentnej analizie danych
- Informacje o DB2 Connect
- Informacje instalacyjne i konfiguracyjne
- Kursy
- Informacje o komponentach opcjonalnych
- Uwagi do wydania

W poniższych tabelach dostępne są informacje potrzebne do zamówienia poszczególnych podręczników z biblioteki DB2 w postaci drukowanej, do wydrukowania lub wyświetlenia odpowiadających im plików PDF. Pełny opis każdego podręcznika z biblioteki DB2 jest dostępny w serwisie IBM Publications Center pod adresem: www.ibm.com/shop/publications/order

Podstawowe informacje o programie DB2

Podręczniki te zawierają podstawowe informacje dla wszystkich użytkowników programu DB2. Informacje te są przydatne zarówno dla programistów, administratorów baz danych, jak i dla użytkowników programu DB2 Connect, DB2 Warehouse Manager lub innych produktów z rodziny DB2.

Tabela 8. Podstawowe informacje o programie DB2

Nazwa	Numer zamówienia	Nazwa pliku PDF
IBM DB2 Universal Database - Command Reference	SC09-4828	db2n0x81
IBM DB2 Universal Database Glosariusz	Brak numeru	db2t0x81
IBM DB2 Universal Database Komunikaty, tom 1	GC85-0061 (niedostępny w postaci drukowanej)	db2m1x81
IBM DB2 Universal Database Komunikaty, tom 2	GC85-0062 (niedostępny w postaci drukowanej)	db2m2x81
IBM DB2 Universal Database Co nowego	SC85-0060	db2q0x81

Informacje administracyjne

Podręczniki te zawierają informacje potrzebne do wydajnego projektowania, implementowania i obsługiwania baz danych, hurtowni danych i systemów stowarzyszonych DB2.

Tabela 9. Informacje administracyjne

Nazwa	Numer zamówienia	Nazwa pliku PDF
IBM DB2 Universal Database Administration Guide: Planning	SC09-4822	db2d1x81
IBM DB2 Universal Database Administration Guide: Implementation	SC09-4820	db2d2x81
IBM DB2 Universal Database Administration Guide: Performance	SC09-4821	db2d3x81
IBM DB2 Universal Database Administrative API Reference	SC09-4824	db2b0x81
IBM DB2 Universal Database Data Movement Utilities Guide and Reference	SC09-4830	db2dmx81
IBM DB2 Universal Database Data Recovery and High Availability Guide and Reference	SC09-4831	db2hax81
IBM DB2 Universal Database Data Warehouse Center Administration Guide	SC27-1123	db2ddx81
IBM DB2 Universal Database SQL Reference, Volume 1	SC09-4844	db2s1x81
IBM DB2 Universal Database SQL Reference, Volume 2	SC09-4845	db2s2x81
IBM DB2 Universal Database System Monitor Guide and Reference	SC09-4847	db2f0x81

Informacje o projektowaniu aplikacji

Podręczniki te zawierają informacje przeznaczone przede wszystkim dla twórców aplikacji i programistów pracujących z programem DB2 Universal Database (DB2 UDB). Są to między innymi informacje o obsługiwanych językach i kompilatorach, a także dokumentacja interfejsów programistycznych umożliwiających dostęp do programu DB2 UDB, takich jak osadzony SQL, ODBC, JDBC, SQLj i CLI. Jeśli używane jest Centrum informacyjne DB2, możliwe jest także uzyskanie dostępu do kodu źródłowego przykładowych programów w wersji HTML.

Tabela 10. Informacje o projektowaniu aplikacji

Nazwa	Numer zamówienia	Nazwa pliku PDF
IBM DB2 Universal Database Application Development Guide: Building and Running Applications	SC09-4825	db2axx81
IBM DB2 Universal Database Application Development Guide: Programming Client Applications	SC09-4826	db2a1x81
IBM DB2 Universal Database Application Development Guide: Programming Server Applications	SC09-4827	db2a2x81

Tabela 10. Informacje o projektowaniu aplikacji (kontynuacja)

Nazwa	Numer zamówienia	Nazwa pliku PDF
IBM DB2 Universal Database Call Level Interface Guide and Reference, Volume 1	SC09-4849	db2l1x81
IBM DB2 Universal Database Call Level Interface Guide and Reference, Volume 2	SC09-4850	db2l2x81
IBM DB2 Universal Database Data Warehouse Center Application Integration Guide	SC27-1124	db2adx81
IBM DB2 XML Extender Administration and Programming	SC27-1234	db2sxx81

Informacje o inteligentnej analizie danych

Podręczniki te zawierają informacje opisujące sposób korzystania z komponentów usprawniających opracowywanie danych i zwiększających możliwości analityczne programu DB2 Universal Database.

Tabela 11. Informacje o inteligentnej analizie danych

Nazwa	Numer zamówienia	Nazwa pliku PDF
IBM DB2 Warehouse Manager Standard Edition Information Catalog Center Administration Guide	SC27-1125	db2dix81
IBM DB2 Warehouse Manager Standard Edition Installation Guide	GC85-0083	db2idx81
IBM DB2 Warehouse Manager Standard Edition Managing ETI Solution Conversion Programs with DB2 Warehouse Manager	SC18-7727	iwhe1mstx80

Informacje o programie DB2 Connect

Do tej kategorii należą informacje opisujące metody uzyskiwania dostępu do danych na serwerach typu mainframe i serwerach dla przedsiębiorstw przy użyciu programu DB2 Connect Enterprise Edition lub DB2 Connect Personal Edition.

Tabela 12. Informacje o programie DB2 Connect

Nazwa	Numer zamówienia	Nazwa pliku PDF
Połączenia z DB2 - suplement	Brak numeru	db2h1x81
IBM DB2 Connect Quick Beginnings for DB2 Connect Enterprise Edition	GC09-4833	db2c6x81
IBM DB2 Connect Personal Edition Krótkie wprowadzenie	GC85-0057	db2c1x81
IBM DB2 Connect Podręcznik użytkownika	SC85-0058	db2c0x81

Informacje instalacyjne i konfiguracyjne

Do tej kategorii należą informacje przydatne podczas instalowania i konfigurowania serwerów, klientów i innych produktów DB2.

Tabela 13. Informacje instalacyjne i konfiguracyjne

Nazwa	Numer zamówienia	Nazwa pliku PDF
IBM DB2 Universal Database: Klienci DB2 - Krótkie wprowadzenie	GC85-0056 (niedostępny w postaci drukowanej)	db2itx81
IBM DB2 Universal Database: Serwery DB2 - Krótkie wprowadzenie	GC85-0082	db2isx81
IBM DB2 Universal Database: DB2 Personal Edition Krótkie wprowadzenie	GC85-0100	db2i1x81
IBM DB2 Universal Database: Instalowanie i konfigurowanie - suplement	GC85-0059 (niedostępny w postaci drukowanej)	db2iyx81
IBM DB2 Universal Database Quick Beginnings for DB2 Data Links Manager	GC09-4829	db2z6x81

Kursy

Kursy wprowadzają użytkownika w funkcje i właściwości programu DB2 i przedstawiają sposoby wykonywania rozmaitych zadań.

Tabela 14. Kursy

Nazwa	Numer zamówienia	Nazwa pliku PDF
Business Intelligence Tutorial: Introduction to the Data Warehouse	Brak numeru	db2tux81
Business Intelligence Tutorial: Extended Lessons in Data Warehousing	Brak numeru	db2tax81
Information Catalog Center Tutorial	Brak numeru	db2aix81
Video Central for e-business Tutorial	Brak numeru	db2twx81
Kurs Visual Explain	Brak numeru	db2tvx81

Informacje o komponentach opcjonalnych

Do tej kategorii należą informacje opisujące sposób korzystania z opcjonalnych komponentów programu DB2.

Tabela 15. Informacje o komponentach opcjonalnych

Nazwa	Numer zamówienia	Nazwa pliku PDF
IBM DB2 Cube Views Guide and Reference	SC18–7298	db2aax81

Tabela 15. Informacje o komponentach opcjonalnych (kontynuacja)

Nazwa	Numer zamówienia	Nazwa pliku PDF
IBM DB2 Query Patroller Guide: Installation, Administration and Usage Guide	GC09–7658	db2dwx81
IBM DB2 Spatial Extender and Geodetic Extender User's Guide and Reference	SC27-1226	db2sbx81
IBM DB2 Universal Database Data Links Manager Administration Guide and Reference	SC27-1221	db2z0x82
DB2 Net Search Extender Administration and User's Guide **Uwaga:** Wersja HTML tego dokumentu *nie* jest instalowana z dysku CD-ROM z dokumentacją w formacie HTML.	SH12-6740	Nie dotyczy

Uwagi do wydania

Uwagi do wydania zawierają dodatkowe informacje dotyczące konkretnego wydania danego produktu lub poziomu pakietu poprawek. Obejmują one także zestawienia aktualizacji dokumentacji wprowadzonych w poszczególnych wydaniach, aktualizacjach i pakietach poprawek.

Tabela 16. Uwagi do wydania

Nazwa	Numer zamówienia	Nazwa pliku PDF
Uwagi do wydania DB2	Patrz: Uwaga.	Patrz: Uwaga.
Uwagi dotyczące instalowania programu DB2	Dostępny tylko na dysku CD-ROM produktu.	Niedostępne.

Uwaga: Uwagi do wydania dostępne są:

- w postaci plików XHTML i plików tekstowych na dyskach CD z produktem,
- w postaci plików PDF na dysku CD z dokumentacją PDF.

Ponadto fragmenty Uwag do wydania dotyczące *znanych problemów i metod ich obejścia* oraz *niezgodności między wersjami* są także dostępne w Centrum informacyjnym DB2.

Aby wyświetlić Uwagi do wydania w postaci pliku tekstowego na platformach z systemem UNIX, należy otworzyć plik Release.Notes. Plik ten znajduje się w katalogu DB2DIR/Readme/*%L*, gdzie *%L* oznacza ustawienia narodowe, a DB2DIR oznacza:

- W systemach operacyjnych AIX: /usr/opt/db2_08_01
- We wszystkich pozostałych systemach operacyjnych UNIX: /opt/IBM/db2/V8.1

Zadania pokrewne:

- "Drukowanie książek z biblioteki DB2 w formacie pliku PDF" na stronie 156
- "Zamawianie drukowanych książek z biblioteki DB2" na stronie 156
- "Wywoływanie pomocy kontekstowej z poziomu narzędzia DB2" na stronie 157

Drukowanie książek z biblioteki DB2 w formacie pliku PDF

Podręczniki DB2 można drukować z plików PDF znajdujących się na dysku CD o nazwie *Dokumentacja DB2 w formacie PDF*. Korzystając z programu Adobe Acrobat Reader, można wydrukować całą książkę lub tylko wybrane strony.

Wymagania wstępne:

Trzeba mieć zainstalowany program Adobe Acrobat Reader. Program Adobe Acrobat Reader jest dostępny w serwisie WWW firmy Adobe pod adresem: www.adobe.com

Procedura:

Aby wydrukować podręcznik z biblioteki DB2 w formacie pliku PDF:

1. Włóż do napędu dysk CD o nazwie *Dokumentacja DB2 w formacie PDF*. W systemach operacyjnych UNIX: podłącz dysk CD o nazwie Dokumentacja DB2 w formacie PDF. Szczegółowe informacje na temat podłączania dysku CD-ROM w systemach operacyjnych UNIX dostępne są w podręczniku *Krótkie wprowadzenie*.
2. Otwórz plik index.htm. Plik zostanie otwarty w oknie przeglądarki.
3. Kliknij tytuł dokumentu PDF, który chcesz wyświetlić. Plik PDF zostanie otwarty w programie Acrobat Reader.
4. Aby wydrukować dowolny fragment podręcznika, wybierz kolejno opcje: **File (Plik) → Print (Drukuj)**.

Pojęcia pokrewne:

- “Centrum informacyjne DB2” na stronie 143

Zadania pokrewne:

- “Zamawianie drukowanych książek z biblioteki DB2” na stronie 156

Informacje pokrewne:

- “Dokumentacja DB2 w postaci plików PDF i w postaci drukowanej” na stronie 151

Zamawianie drukowanych książek z biblioteki DB2

Jeśli użytkownik woli korzystać z podręczników w wersji drukowanej, może je zamówić na trzy sposoby.

Procedura:

W niektórych krajach lub regionach istnieje możliwość zamówienia podręczników w postaci drukowanej. Informacje o dostępności tej usługi w określonym kraju lub regionie można znaleźć w serwisie WWW IBM Publications. Jeśli istnieje możliwość zamówienia publikacji, można to zrobić w następujący sposób:

- Skontaktuj się z autoryzowanym dealerem lub przedstawicielem handlowym firmy IBM. Lokalnych przedstawicieli firmy IBM można znaleźć w serwisie IBM Worldwide Directory of Contacts pod adresem: www.ibm.com/planetwide
- Zadzwoń pod numer 1-800-879-2755 w Stanach Zjednoczonych lub 1-800-IBM-4YOU w Kanadzie.
- Odwiedź serwis IBM Publications Center pod adresem: http://www.ibm.com/shop/publications/order. W wypadku niektórych krajów zamówienie podręczników w serwisie IBM Publications Center może nie być możliwe.

W chwili udostępnienia produktu DB2 informacje w publikacjach drukowanych odpowiadają dokładnie informacjom w plikach PDF na dysku CD *Dokumentacja DB2 w formacie PDF*. Te same informacje są również dostępne na dysku CD *Centrum informacyjne DB2*. Na dysku CD z Centrum informacyjnym DB2 dostępne są także dodatkowe informacje, które nie są zawarte w podręcznikach w postaci plików PDF (na przykład procedury administracyjne SQL i przykłady HTML). Nie wszystkie podręczniki dostępne na dysku CD z dokumentacją DB2 w formacie PDF mogą zostać zamówione w postaci drukowanej.

Uwaga: Centrum informacyjne DB2 jest aktualizowane częściej niż pliki PDF lub podręczniki drukowane. Aby mieć dostęp do najbardziej aktualnych informacji, należy instalować udostępniane na bieżąco aktualizacje dokumentacji lub korzystać z Centrum informacyjnego DB2 pod adresem: http://publib.boulder.ibm.com/infocenter/db2help/.

Zadania pokrewne:

- "Drukowanie książek z biblioteki DB2 w formacie pliku PDF" na stronie 156

Informacje pokrewne:

- "Dokumentacja DB2 w postaci plików PDF i w postaci drukowanej" na stronie 151

Wywoływanie pomocy kontekstowej z poziomu narzędzia DB2

Pomoc kontekstowa udostępnia informacje o zadaniach lub elementach sterujących związanych z określonym oknem, notatnikiem, kreatorem lub doradcą. Dostęp do pomocy kontekstowej można uzyskać przy użyciu administracyjnych i programistycznych narzędzi DB2 wyposażonych w interfejs graficzny. Istnieją dwa typy pomocy kontekstowej:

- Pomoc dostępna po kliknięciu przycisku **Pomoc** wyświetlanego w każdym oknie lub notatniku.
- Etykietki czyli wywoływane okna informacyjne wyświetlane po umieszczeniu kursora myszy na określonym polu lub elemencie sterującym lub gdy użytkownik wybierze określone pole albo element sterujący w oknie, notatniku, kreatorze lub doradcy, a następnie naciśnie klawisz F1.

Przycisk **Pomoc** umożliwia dostęp do informacji przeglądowych, informacji dotyczących wymagań wstępnych i zadań. Etykietki opisują poszczególne pola i elementy sterujące.

Procedura:

Aby wywołać pomoc kontekstową:

- Aby uzyskać dostęp do pomocy dotyczącej okna lub notatnika, uruchom jedno z narzędzi DB2, a następnie otwórz okno lub notatnik. Kliknij przycisk **Pomoc** wyświetlony w prawym dolnym rogu okna lub notatnika, aby wywołać pomoc kontekstową.

  Dostęp do pomocy kontekstowej można uzyskać także przy użyciu opcji menu **Pomoc** dostępnej w górnej części okna każdego narzędzia DB2.

  Aby wyświetlić pomoc kontekstową w kreatorze lub doradcy, kliknij dostępny na pierwszej stronie odsyłacz Przegląd zadania.
- Aby uzyskać pomoc w postaci etykietek dotyczącą poszczególnych elementów sterujących okna lub notatnika, kliknij odpowiedni element, a następnie naciśnij klawisz **F1**. Wyświetlone zostanie okienko z żółtym tłem zawierające szczegółowe informacje o wybranym elemencie.

  Uwaga: Aby etykietki były wyświetlane po zatrzymaniu kursora myszy nad polem lub elementem sterującym, w notatniku Ustawienia narzędzi, na stronie **Dokumentacja** zaznacz pole wyboru **Automatycznie wyświetlaj etykietki**.

Podobną do etykietek formą pomocy kontekstowej są wywoływane okienka diagnostyczne zawierające reguły wprowadzania danych. Okienka diagnostyczne mają kolor purpurowy i są wyświetlane po wprowadzeniu niepoprawnych lub niewystarczających danych. Wywoływane okienka diagnostyczne mogą zostać wyświetlone w wypadku następujących typów pól:

– pól obowiązkowych
– pól wymagających wprowadzenia danych w określonym formacie, na przykład daty

Zadania pokrewne:

- “Uruchamianie Centrum informacyjnego DB2” na stronie 148
- “Wywoływanie pomocy dotyczącej komunikatów przy użyciu procesora wiersza komend” na stronie 158
- “Wywoływanie pomocy dotyczącej komend przy użyciu procesora wiersza komend” na stronie 158
- “Wywoływanie pomocy dotyczącej stanu SQL przy użyciu procesora wiersza komend” na stronie 159

Wywoływanie pomocy dotyczącej komunikatów przy użyciu procesora wiersza komend

Pomoc dotycząca komunikatów objaśnia przyczyny wygenerowania komunikatu o błędzie i opisuje działania, jakie należy podjąć w odpowiedzi na dany komunikat.

Procedura:

Aby wywołać pomoc dotyczącą komunikatów, otwórz procesor wiersza komend i wpisz:

```
? XXXnnnnn
```

gdzie *XXXnnnnn* reprezentuje poprawny identyfikator komunikatu.

Na przykład: `? SQL30081` wyświetli pomoc dotyczącą komunikatu SQL30081.

Zadania pokrewne:

- “Wywoływanie pomocy kontekstowej z poziomu narzędzia DB2” na stronie 157
- “Uruchamianie Centrum informacyjnego DB2” na stronie 148
- “Wywoływanie pomocy dotyczącej komend przy użyciu procesora wiersza komend” na stronie 158
- “Wywoływanie pomocy dotyczącej stanu SQL przy użyciu procesora wiersza komend” na stronie 159

Wywoływanie pomocy dotyczącej komend przy użyciu procesora wiersza komend

Pomoc dotycząca komend objaśnia składnię komend stosowaną w procesorze wiersza komend.

Procedura:

Aby wywołać pomoc dotyczącą komend, otwórz procesor wiersza komend i wpisz:

```
? komenda
```

gdzie *komenda* reprezentuje parametr lub całą komendę.

Na przykład: ? catalog wyświetla pomoc na temat wszystkich komend CATALOG, a ? catalog database wyświetla pomoc tylko na temat komendy CATALOG DATABASE.

Zadania pokrewne:

- “Wywoływanie pomocy kontekstowej z poziomu narzędzia DB2” na stronie 157
- “Uruchamianie Centrum informacyjnego DB2” na stronie 148
- “Wywoływanie pomocy dotyczącej komunikatów przy użyciu procesora wiersza komend” na stronie 158
- “Wywoływanie pomocy dotyczącej stanu SQL przy użyciu procesora wiersza komend” na stronie 159

Wywoływanie pomocy dotyczącej stanu SQL przy użyciu procesora wiersza komend

Program DB2 Universal Database zwraca wartość SQLSTATE w sytuacji, która mogła zaistnieć na skutek wykonania instrukcji SQL. Pomoc dotycząca wartości SQLSTATE zawiera wyjaśnienia znaczenia stanów SQL i opisy kodów klas stanów SQL.

Procedura:

Aby wywołać pomoc dotyczącą stanów SQL, otwórz procesor wiersza komend i wpisz:

```
? stan sql lub ? kod klasy
```

gdzie *stan sql* reprezentuje poprawny pięciocyfrowy stan SQL, a *kod klasy* reprezentuje pierwsze dwie cyfry stanu SQL.

Na przykład: ? 08003 wyświetla pomoc dotyczącą stanu SQL 08003, a ? 08 wyświetli pomoc dotyczącą kodu klasy 08.

Zadania pokrewne:

- “Uruchamianie Centrum informacyjnego DB2” na stronie 148
- “Wywoływanie pomocy dotyczącej komunikatów przy użyciu procesora wiersza komend” na stronie 158
- “Wywoływanie pomocy dotyczącej komend przy użyciu procesora wiersza komend” na stronie 158

Kursy na temat programu DB2

Kursy na temat programu DB2® pomagają użytkownikowi zapoznać się z różnymi aspektami programu DB2 Universal Database. Na kursy składają się lekcje z instrukcjami typu ″krok po kroku″ obejmujące tematykę projektowania aplikacji, dostrajania efektywności zapytań SQL, pracy z hurtowniami danych, zarządzania metadanymi i opracowywania serwisów WWW za pomocą programu DB2.

Zanim rozpoczniesz:

Kursy w wersji XHTML można wyświetlić w Centrum informacyjnym pod adresem: http://publib.boulder.ibm.com/infocenter/db2help/.

W niektórych lekcjach wykorzystano przykładowe dane lub kod programu. Opisy wymagań wstępnych dla wykonania konkretnych zadań znajdują się w treści poszczególnych kursów.

Kursy na temat programu DB2 Universal Database:

Wybierz nazwę kursu z poniższej listy, aby wyświetlić dany kurs.

Kurs inteligentnej analizy danych: Wprowadzenie do Centrum hurtowni danych
Zadania wprowadzające z zakresu opracowywania danych w Centrum hurtowni danych.

Kurs inteligentnej analizy danych: Lekcje zaawansowanego opracowywania danych hurtowych
Zaawansowane zadania związane z opracowywaniem danych w Centrum hurtowni danych.

Kurs Centrum katalogu informacyjnego
Tworzenie i zarządzanie katalogiem informacyjnym w celu wyszukiwania i korzystania z metadanych w Centrum katalogu informacyjnego.

Kurs Visual Explain
Poprawianie wydajności drogą analizy, optymalizacji i dostrajania instrukcji SQL za pomocą programu Visual Explain.

Informacje dotyczące rozwiązywania problemów z programem DB2

Podczas korzystania z produktów DB2® użytkownik ma do dyspozycji wiele różnych informacji dotyczących diagnozowania i rozwiązywania problemów.

Dokumentacja DB2
Informacje dotyczące rozwiązywania problemów można znaleźć za poednictwem Centrum informacyjnego DB2, a także w podręcznikach dostępnych w postaci plików PDF wchodzących w skład biblioteki DB2. Pełną listę dokumentacji dotyczącej rozwiązywania problemów z programem DB2 można znaleźć w Centrum informacyjnym DB2, w sekcji ″Wsparcie i rozwiązywanie problemów″ w drzewie nawigacyjnym (w panelu znajdującym się w lewej części okna przeglądarki).

Serwis WWW wsparcia technicznego dla programu DB2
W razie wystąpienia problemów i konieczności uzyskania pomocy w znalezieniu prawdopodobnych przyczyn i możliwych rozwiązań, należy odwiedzić serwis WWW wsparcia technicznego dla programu DB2. Serwis ten zawiera odsyłacze do najnowszych publikacji dotyczących programu DB2, not technicznych, raportów APAR (Authorized Program Analysis Report), pakietów poprawek, najnowszej listy wewnętrznych kodów błędów programu DB2 oraz do innych zasobów. Użytkownik może przeszukiwać tę bazę wiedzy, aby znaleźć możliwe rozwiązania określonych problemów.

Serwis WWW wsparcia technicznego dla programu DB2 jest dostępny pod adresem: http://www.ibm.com/software/data/db2/udb/winos2unix/support

DB2 Problem Determination Tutorial Series
Serwis WWW DB2 Problem Determination Tutorial Series (seria kursów dotyczących określania problemów z programem DB2) zawiera informacje pomocne w szybkiej identyfikacji i rozwiązywaniu problemów, które mogą wystąpić podczas pracy z produktami z rodziny DB2. Jeden z kursów opisuje funkcje i narzędzia programu DB2 ułatwiające określanie problemów i zawiera informacje pomocne w podjęciu decyzji, kiedy należy z nich korzystać. W innych kursach omawiane są tematy pokrewne, na przykład określanie problemów dotyczących mechanizmu bazy danych (″Database Engine Problem Determination″), określanie problemów

dotyczących wydajności (″Performance Problem Determination″) i określanie problemów dotyczących aplikacji (″Application Problem Determination″).

Pełny zestaw kursów dotyczących określania problemów związanych z programem DB2 jest dostępny w serwisie WWW wsparcia technicznego dla programu DB2 pod adresem: http://www.ibm.com/software/data/support/pdm/db2tutorials.html

Pojęcia pokrewne:

- “Centrum informacyjne DB2” na stronie 143

Ułatwienia dostępu

Ułatwienia dostępu pomagają użytkownikom niepełnosprawnym fizycznie, na przykład z upośledzeniem ruchowym lub wzrokowym, efektywnie korzystać z oprogramowania. Poniższa lista zawiera opis głównych ułatwień dostępu w produktach DB2®, wersja 8:

- Ze wszystkich funkcji programu DB2 można korzystać za pośrednictwem klawiatury, bez konieczności użycia myszy. Więcej informacji na ten temat można znaleźć w sekcji “Wprowadzanie danych i nawigacja za pomocą klawiatury”.
- Interfejsy użytkownika programu DB2 umożliwiają dostosowanie wielkości i koloru czcionek. Więcej informacji na ten temat można znaleźć w sekcji “Przystępny ekran” na stronie 162.
- Produkty DB2 obsługują ułatwiające dostęp aplikacje korzystające z interfejsu Java™ Accessibility API. Więcej informacji na ten temat można znaleźć w sekcji “Zgodność z rozwiązaniami technicznymi dla niepełnosprawnych” na stronie 162.
- Dokumentacja programu DB2 jest dostępna w przystępnym formacie. Więcej informacji na ten temat można znaleźć w sekcji “Dokumentacja w przystępnym formacie” na stronie 162.

Wprowadzanie danych i nawigacja za pomocą klawiatury

Operowanie programem za pomocą klawiatury

Narzędzia programu DB2 można obsługiwać za pomocą samej klawiatury. Wszystkie operacje, które można wykonać za pomocą myszy, można również wykonać za pomocą pojedynczych klawiszy lub ich kombinacji. Standardowe kombinacje klawiszy używane w systemie operacyjnym są wykorzystywane do wykonania standardowych operacji w systemie operacyjnym.

Więcej informacji o korzystaniu z klawiszy lub kombinacji klawiszy do wykonania określonych operacji można znaleźć w sekcji Skróty i akceleratory klawiszowe: Wspólny interfejs GUI - Pomoc.

Nawigacja przy użyciu klawiatury

Interfejs użytkownika narzędzi DB2 umożliwia nawigację przy użyciu klawiszy lub kombinacji klawiszy.

Więcej informacji o korzystaniu z klawiszy lub kombinacji klawiszy do nawigowania po narzędziach DB2 można znaleźć w sekcji Skróty i akceleratory klawiszowe: Wspólny interfejs GUI - Pomoc.

Miejsce aktywne dla klawiatury

W systemach operacyjnych UNIX® obszar aktywnego okna, w którym obsługiwane są sekwencje klawiszy, jest podświetlony.

Przystępny ekran

W narzędziach DB2 dostępne są funkcje zwiększające dostępność programu dla użytkowników o obniżonej zdolności widzenia. Takim usprawnieniem jest między innymi możliwość dostosowywania właściwości czcionek do indywidualnych potrzeb.

Ustawienia czcionek

Za pomocą notatnika Ustawienia narzędzi można wybrać kolor, rozmiar i rodzaj czcionki tekstu wyświetlanego w menu i oknach dialogowych.

Więcej informacji o określaniu ustawień czcionki można znaleźć w sekcji Zmiana czcionki menu i tekstu: Wspólny interfejs GUI - Pomoc.

Niezależność od kolorów

Zdolność rozróżniania kolorów nie jest potrzebna, aby móc korzystać ze wszystkich funkcji tego produktu.

Zgodność z rozwiązaniami technicznymi dla niepełnosprawnych

Interfejsy narzędzi DB2 zapewniają obsługę interfejsu Java Accessibility API, który pozwala na wykorzystanie razem z produktami DB2 lektorów ekranowych i innych przydatnych technologii.

Dokumentacja w przystępnym formacie

Dokumentacja dotycząca programu DB2 jest dostępna w formacie XHTML 1.0, który jest obsługiwany przez większość przeglądarek WWW. Zastosowanie formatu XHTML umożliwia wyświetlenie dokumentacji zgodnie z preferencjami wyświetlania określonymi w używanej przeglądarce. Ponadto dzięki temu można korzystać z czytników ekranu i innych rozwiązań technicznych dla niepełnosprawnych.

Diagramy składni przedstawione są w postaci dziesiętnej z kropkami. Ten format jest dostępny tylko podczas korzystania z dokumentacji elektronicznej za pomocą lektora ekranowego.

Pojęcia pokrewne:

• “Diagramy składniowe w postaci dziesiętnej z kropkami” na stronie 162

Diagramy składniowe w postaci dziesiętnej z kropkami

Diagramy składni przedstawione w postaci dziesiętnej z kropkami przeznaczone są dla użytkowników uzyskujących dostęp do Centrum informacyjnego przy użyciu lektora ekranowego.

W formacie dziesiętnym z kropkami każdy element składni jest umieszczony w osobnym wierszu. Jeśli co najmniej dwa elementy składni zawsze występują razem (lub zawsze razem są nieobecne), można je umieścić w tym samym wierszu, ponieważ stanowią one jeden złożony element składni.

Każdy wiersz rozpoczyna się numerem w postaci dziesiętnej z kropkami, na przykład: 3, 3.1 lub 3.1.1. Aby usłyszeć te numery poprawnie, trzeba skonfigurować lektora ekranowego tak, aby odczytywał znaki przestankowe. Wszystkie elementy składni o tym samym numerze w postaci dziesiętnej z kropkami (np. wszystkie elementy składni o numerze 3.1) są zamienne i

wykluczają się wzajemnie. Jeśli zostaną odczytane wiersze 3.1 USERID i 3.1 SYSTEMID, oznacza to, że składnia może zawierać element USERID albo SYSTEMID, ale nie oba elementy jednocześnie.

Poziom numeracji w postaci dziesiętnej z kropkami oznacza poziom zagnieżdżenia. Na przykład, jeśli po elemencie składni o numerze w postaci dziesiętnej z kropkami 3 następuje seria elementów składniowych o numerze 3.1, wszystkie elementy składni o numerze 3.1 są podrzędne względem elementu o numerze 3.

Dodatkowe informacje o elementach składni są określane przez słowa i symbole umieszczane po numerach w postaci dziesiętnej z kropkami. Czasami te słowa i symbole mogą występować na początku samego elementu. Aby ułatwić identyfikację, słowa lub symbole będące częścią elementu składni są poprzedzane znakiem ukośnika odwrotnego (\). Aby oznaczyć powtarzalność elementów składni, stosuje się symbol * umieszczony za numerem w postaci dziesiętnej z kropkami. Na przykład, element składni *FILE o numerze 3 ma postać 3 * FILE. Format 3* FILE oznacza, że element składni FILE jest powtarzalny. Format 3* * FILE oznacza, że element składni * FILE jest powtarzalny.

Znaki (np. przecinki) wykorzystywane do oddzielania łańcuchów elementów składnio występują w składni tuż przed oddzielanymi elementami. Znaki te mogą występować w tym samym wierszu, w którym występują poszczególne elementy, lub w osobnym wierszu o tym samym numerze w postaci dziesiętnej z kropkami, co elementy, których dotyczą. Wiersz może zawierać także inne symbole informujące o elementach składni. Na przykład wiersze 5.1*, 5.1 LASTRUN i 5.1 DELETE oznaczają, że w przypadku wielokrotnego użycia elementów składni LASTRUN i DELETE, trzeba oddzielić je przecinkiem. Jeśli znak separatora nie zostanie określony, do oddzielania elementów składni będzie wykorzystywany znak odstępu.

Jeśli element składni jest poprzedzony symbolem %, oznacza to odwołanie zdefiniowane w innym miejscu. Łańcuch następujący po symbolu % to nazwa fragmentu składni, a nie literał. Na przykład wiersz 2.1 %OP1 oznacza odwołanie do osobnego fragmentu składni o nazwie OP1.

Po numerach w postaci dziesiętnej z kropkami mogą występować następujące słowa i symbole:

- ? oznacza opcjonalny element składni. Występujący po numerze w postaci dziesiętnej z kropkami symbol ? oznacza, że wszystkie elementy składni o odpowiadającym mu numerze i wszystkie podrzędne elementy składni są opcjonalne. Jeśli występuje tylko jeden element składni o danym numerze w postaci dziesiętnej z kropkami, symbol ? znajduje się w tym samym wierszu, co element składni (na przykład 5? NOTIFY). Jeśli takich elementów składni jest więcej, symbol ? występuje w osobnym wierszu, a za nim elementy składni, które są opcjonalne. Na przykład, jeśli zostaną odczytane wiersze 5 ?, 5 NOTIFY i 5 UPDATE, oznacza to, że elementy składni NOTIFY i UPDATE są opcjonalne (czyli można wybrać jeden z nich lub nie wybrać żadnego). Symbol ? jest równoważny linii obejścia w diagramach blokowych.
- ! oznacza domyślny element składni. Występujący po numerze w postaci dziesiętnej z kropkami symbol ! z elementem składni oznacza, że element ten jest opcją domyślną wśród wszystkich elementów składni o tym samym numerze. Symbol ! może być przypisany tylko do jednego z elementów składniowych o tym samym numerze. Na przykład, jeśli zostaną odczytane wiersze 2? FILE, 2.1! (KEEP) i 2.1 (DELETE), oznacza to że opcja (KEEP) jest domyślną opcją słowa kluczowego FILE. Jeśli w tym przykładzie zostanie użyte słowo kluczowe FILE bez określenia opcji, zostanie zastosowana domyślna opcja KEEP. Opcja domyślna ma zastosowanie także do kolejnego wyższego numeru w postaci dziesiętnej z kropkami. Jeśli w tym przykładzie zostanie pominięte słowo kluczowe FILE, będzie użyta domyślna wartość FILE(KEEP). Jeśli jednak zostaną odczytane wiersze 2?

FILE, 2.1, 2.1.1! (KEEP) i 2.1.1 (DELETE), domyślna opcja KEEP będzie dotyczyć tylko kolejnego wyższego numeru w postaci dziesiętnej z kropkami, 2.1 (któremu nie przypisano słowa kluczowego), a nie będzie dotyczyć numeru 2? FILE. Jeśli słowo kluczowe FILE zostanie pominięte, nie zostanie użyta żadna wartość.

- * oznacza element składni, który może nie wystąpić wcale lub wystąpić wielokrotnie. Występujący po numerze w postaci dziesiętnej z kropkami symbol * oznacza, że element składni może zostać użyty 0 lub wiele razy (tj. element ten jest opcjonalny i powtarzalny). Na przykład, jeśli zostanie odczytany obszar danych wiersza 5.1*, oznacza to, że można określić jeden obszar danych, wiele obszarów danych lub można wcale nie określać obszaru danych. Jeśli zostaną odczytane wiersze 3*, 3 HOST i 3 STATE, oznacza to, ze można uwzględnić opcję HOST, STATE, obie te opcje lub nie uwzględniać żadnej z nich.

  Uwagi:

  1. Jeśli przy numerze w postaci dziesiętnej z kropkami znajduje się symbol gwiazdki (*) i istnieje tylko jeden element o tym numerze, można powtórzyć ten element więcej niż jeden raz.
  2. Jeśli przy numerze w postaci dziesiętnej z kropkami znajduje się symbol gwiazdki i jest wiele elementów o tym numerze, można użyć kilku elementów z listy, ale każdego z nich tylko raz. W poprzednim przykładzie można wstawić elementy HOST STATE, ale nie można użyć elementów HOST HOST.
  3. Symbol * jest równoznaczny pętli zwrotnej w blokowym diagramie składni.
- + oznacza element składni, który musi wystąpić przynajmniej raz. Występujący po numerze w postaci dziesiętnej z kropkami symbol + oznacza, że element ten musi wystąpić jeden lub kilka razy (tj. musi wystąpić co najmniej raz i jest powtarzalny). Na przykład, jeśli zostanie odczytany obszar danych wiersza 6.1+, oznacza to, że trzeba określić co najmniej jeden obszar danych. Jeśli zostaną odczytane wiersze 2+, 2 HOST i 2 STATE, trzeba określić element HOST, STATE lub oba te elementy. Podobnie jak w przypadku symbolu *, symbol + oznacza, że dany element można powtórzyć tylko wtedy, gdy jest on jedynym elementem o danym numerze w postaci dziesiętnej z kropkami. Symbol +, tak jak symbol *, odpowiada pętli zwrotnej w blokowym diagramie składni.

Informacje pokrewne:

- “How to read the syntax diagrams” w podręczniku *SQL Reference, Volume 2*

Certyfikacja Common Criteria produktów DB2 Universal Database

Program DB2 Universal Database jest oceniany dla potrzeb certyfikacji Common Criteria zgodnie z zasadami poziomu EAL4 (Evaluation Assurance Level 4). Więcej informacji na temat certyfikacji Common Criteria można znaleźć pod adresem: http://niap.nist.gov/cc-scheme/.

Dodatek B. Uwagi

Produktów, usług lub opcji opisywanych w tym dokumencie firma IBM nie musi oferować we wszystkich krajach. 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 ich odpowiednik funkcjonalny, pod warunkiem, że nie narusza to praw własności intelektualnej firmy IBM. Jednakże cała odpowiedzialność za ocenę przydatności i sprawdzenie działania produktu, programu lub usługi pochodzących od producenta innego niż IBM spoczywa na użytkowniku.

IBM może posiadać patenty lub złożone wnioski patentowe na towary i usługi, o których mowa w niniejszej publikacji. 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.

Zapytania dotyczące zestawów znaków dwubajtowych (DBCS) należy kierować do lokalnych działów własności intelektualnej firmy IBM (IBM Intellectual Property Department) lub wysłać je na piśmie na adres:

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 przepisami prawa miejscowego: FIRMA INTERNATIONAL BUSINESS MACHINES CORPORATION DOSTARCZA TĘ PUBLIKACJĘ W TAKIM STANIE, W JAKIM SIĘ ZNAJDUJE “AS IS” BEZ UDZIELANIA JAKICHKOLWIEK GWARANCJI (W TYM TAKŻE RĘKOJMI), WYRAŹNYCH LUB DOMNIEMANYCH, A W SZCZEGÓLNOŚCI DOMNIEMANYCH GWARANCJI PRZYDATNOŚCI HANDLOWEJ ORAZ PRZYDATNOŚCI DO OKREŚLONEGO CELU LUB GWARANCJI, ŻE PUBLIKACJA NIE NARUSZA PRAW OSÓB TRZECICH. Ustawodawstwa niektórych krajów nie dopuszczają zastrzeżeń dotyczących gwarancji wyraźnych lub domniemanych w odniesieniu do pewnych transakcji; w takiej sytuacji powyższe zdanie nie ma zastosowania.

Informacje zawarte w niniejszej publikacji mogą zawierać nieścisłości techniczne lub błędy drukarskie. Informacje te są okresowo aktualizowane, a zmiany te zostaną ujęte w kolejnych wydaniach tej publikacji. IBM zastrzega sobie prawo do wprowadzania ulepszeń i/lub zmian w produktach i/lub programach opisanych w tej publikacji w dowolnym czasie, bez wcześniejszego powiadomienia.

Jakiekolwiek wzmianki na temat stron internetowych nie należących do firmy IBM zostały podane jedynie dla wygody użytkownika i nie oznaczają, że firma IBM w jakikolwiek sposób firmuje te strony. Materiały dostępne na tych stronach nie są częścią materiałów opracowanych dla tego produktu IBM, a użytkownik korzysta z nich na własną odpowiedzialność.

© Copyright IBM Corp. 1993-2004

IBM ma prawo do korzystania i rozpowszechniania informacji przysłanych przez użytkownika w dowolny sposób, jaki uzna za właściwy, bez żadnych zobowiązań wobec ich autora.

Licencjobiorcy tego programu, którzy chcieliby uzyskać informacje na temat programu w celu: (i) wdrożenia wymiany informacji między niezależnie utworzonymi programami i innymi programami (łącznie z tym opisywanym) oraz (ii) wykorzystywania wymienianych informacji, powinni skontaktować się z:

IBM Canada Limited
Office of the Lab Director
8200 Warden Avenue
Markham, Ontario
L6G 1C7
CANADA

Informacje takie mogą być udostępnione, o ile spełnione zostaną odpowiednie warunki, w tym, w niektórych przypadkach, uiszczenie odpowiedniej opłaty.

Licencjonowany program opisany w tym dokumencie oraz wszystkie inne licencjonowane materiały dostępne dla tego programu są dostarczane przez IBM na warunkach określonych w Umowie IBM z Klientem, Międzynarodowej Umowie Licencyjnej IBM na Program lub w innych podobnych umowach zawartych między IBM i 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 być dokonywane 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 powinni we własnym zakresie sprawdzić odpowiednie dane dla ich środowiska.

Informacje dotyczące produktów innych firm zostały uzyskane od dostawców tych produktów z opublikowanych przez nich zapowiedzi lub innych powszechnie dostępnych źródeł. Firma IBM nie testowała 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.

Jakiekolwiek wzmianki na temat kierunków rozwoju firmy IBM mogą ulec zmianie lub anulowaniu bez uprzedzenia i dotyczą jedynie ogólnych celów i założeń.

Publikacja ta może zawierać przykładowe dane i raporty używane w codziennej działalności biznesowej. W celu kompleksowego zilustrowania tej działalności podane przykłady zawierają nazwy osób, firm i ich produktów. Wszystkie te nazwiska/nazwy są fikcyjne i jakakolwiek ich zbieżność z prawdziwymi nazwiskami/nazwami jest całkowicie przypadkowa.

LICENCJA NA PRAWA AUTORSKIE:

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 rozpowszechniania aplikacji zgodnych z aplikacyjnym interfejsem programowym dla tego systemu operacyjnego, dla którego napisane były programy przykładowe. Programy przykładowe nie zostały gruntownie

przetestowane. Firma IBM nie może zatem 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

Następujące nazwy są znakami towarowymi firmy International Business Machines Corporation w Stanach Zjednoczonych i/lub innych krajach i zostały użyte w co najmniej jednym dokumencie z biblioteki DB2:

ACF/VTAM
AISPO
AIX
AIXwindows
AnyNet
APPN
AS/400
BookManager
C Set++
C/370
CICS
Database 2
DataHub
DataJoiner
DataPropagator
DataRefresher
DB2
DB2 Connect
DB2 Extenders
DB2 OLAP Server
DB2 Information Integrator
DB2 Query Patroller
DB2 Universal Database
Distributed Relational Database Architecture
DRDA
eServer
Extended Services
FFST
First Failure Support Technology
IBM
IMS
IMS/ESA
iSeries
LAN Distance
MVS
MVS/ESA
MVS/XA
Net.Data
NetView
OS/390
OS/400
PowerPC
pSeries
QBIC
QMF
RACF
RISC System/6000
RS/6000
S/370
SP
SQL/400
SQL/DS
System/370
System/390
SystemView
Tivoli
VisualAge
VM/ESA
VSE/ESA
VTAM
WebExplorer
WebSphere
WIN-OS/2
z/OS
zSeries

Poniższe nazwy są znakami towarowymi lub zastrzeżonymi znakami towarowymi innych firm i zostały użyte w co najmniej jednym dokumencie z biblioteki DB2:

Microsoft, Windows, Windows NT oraz logo Windows są znakami towarowymi firmy Microsoft Corporation w Stanach Zjednoczonych i/lub innych krajach.

Intel i Pentium są znakami towarowymi firmy Intel Corporation w Stanach Zjednoczonych i/lub innych krajach.

Java i wszystkie znaki towarowe związane z językiem Java są znakami towarowymi firmy Sun Microsystems, Inc. w Stanach Zjednoczonych i/lub innych krajach.

UNIX jest zastrzeżonym znakiem towarowym The Open Group w Stanach Zjednoczonych i innych krajach.

Inne nazwy firm, produktów i usług mogą być znakami towarowymi lub znakami usług innych firm.

Indeks

© Copyright IBM Corp. 1993-2004

E

G

H

I

K

L

M

N

O

P

R

S

T

U

V

W

X

Z

Kontakt z firmą IBM

W celu skontaktowania się z firmą IBM w Stanach Zjednoczonych zadzwoń pod jeden z następujących numerów:

- 1-800-IBM-SERV (1-800-426-7378) - dział obsługi klienta
- 1-888-426-4343 - informacje o dostępnych usługach
- 1-800-IBM-4YOU (426-4968) - dział marketingu i sprzedaży programu DB2

W celu skontaktowania się z firmą IBM w Kanadzie zadzwoń pod jeden z następujących numerów:

- 1-800-IBM-SERV (1-800-426-7378) - dział obsługi klienta
- 1-800-465-9600 - informacje o dostępnych usługach
- 1-800-IBM-4YOU (1-800-426-4968) - dział marketingu i sprzedaży programu DB2

Krajowe lub regionalne przedstawicielstwo firmy IBM można znaleźć w serwisie WWW o nazwie Directory of Worldwide Contacts pod adresem http://www.ibm.com/planetwide

Informacje o produkcie

Informacje dotyczące produktów z rodziny DB2 Universal Database można uzyskać telefonicznie lub w sieci WWW pod adresem http://www.ibm.com/software/data/db2/udb

W tym serwisie dostępne są najnowsze informacje dotyczące biblioteki technicznej, zamawiania podręczników, oprogramowania do pobrania, grup dyskusyjnych i pakietów poprawek, a także najświeższe wiadomości i odsyłacze do zasobów WWW.

Mieszkańcy USA, którzy chcą zamawiać produkty lub uzyskać informacje natury ogólnej mogą dzwonić pod następujące numery telefonów:

- 1-800-IBM-CALL (1-800-426-2255).
- 1-800-879-2755 - zamawianie publikacji.

Informacje o możliwościach kontaktu z firmą IBM poza Stanami Zjednoczonymi dostępne są na stronie serwisu IBM Worldwide pod adresem www.ibm.com/planetwide

© Copyright IBM Corp. 1993-2004

PN: SDB2-CONN-SU