

IBM<sup>®</sup>



# Supliment de conectivitate

*Versiunea 8*



IBM<sup>®</sup>



# Supliment de conectivitate

*Versiunea 8*

Înainte de a folosi aceste informații și produsul la care se referă, aveți grijă să citiți informațiile din *Observații*.

Acest document conține informații de proprietar ale IBM. Este furnizat pe baza contractului de licență și este protejat de legea privind copyright-ul. Informațiile din această publicație nu conțin nici o garanție pentru produs și nici o declarație din acest manual nu trebuie să fie interpretată în acest sens.

Puteți comanda publicații IBM online sau prin reprezentantul IBM local.

- Pentru a comanda publicații online, vizitați Centrul de informare IBM, la [www.ibm.com/shop/publications/order](http://www.ibm.com/shop/publications/order)
- Pentru a lua legătura cu reprezentantul IBM local, vizitați IBM Directory of Worldwide Contacts, la [www.ibm.com/planetwide](http://www.ibm.com/planetwide)

Pentru a comanda publicații DB2 de la DB2 Marketing and Sales în Statele Unite sau Canada, sunați la 1-800-IBM-4YOU (426-4968).

Atunci când trimiteți informații la IBM, acordați IBM-ului dreptul neexclusiv de a utiliza sau folosi acele informații în orice mod considerat adecvat, fără ca aceasta să implice vreo obligație față de dumneavoastră.

© Copyright International Business Machines Corporation 1993-2004. Toate drepturile rezervate.

---

# Cuprins

## Partea 1. Configurarea manuală a comunicațiilor . . . . . 1

### Capitolul 1. Configurarea manuală a comunicațiilor TCP/IP . . . . . 3

Configurarea manuală a comunicațiilor TCP/IP dintre DB2 Connect și un server de bază de date gazdă sau iSeries . . . . .	3
Task-uri de configurare . . . . .	4
Configurarea TCP/IP pe serverul DB2 Connect . . . . .	4
Task-uri de configurare TCP/IP . . . . .	4
Catalogarea nodului TCP/IP . . . . .	6
Catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS) . . . . .	7
Catalogarea bazei de date . . . . .	7
Asocierea utilităților și aplicațiilor la gazdă sau server de baze de date iSeries . . . . .	9
Testarea conexiunii gazdei sau a iSeries . . . . .	9

### Capitolul 2. Configurarea manuală a comunicațiilor APPC . . . . . 11

Configurarea manuală a comunicațiilor APPC dintre DB2 Connect și un server de bază de date gazdă sau iSeries . . . . .	11
Task-uri de configurare . . . . .	12
Actualizarea profilurilor APPC pe serverul DB2 Connect . . . . .	12
Subtask-uri de actualizare a profilurilor APPC . . . . .	12
Catalogarea nodului APPC sau APPN . . . . .	14
Catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS) . . . . .	15
Catalogarea bazei de date . . . . .	16
Asocierea utilităților și aplicațiilor la gazdă sau server de baze de date iSeries . . . . .	17
Testarea conexiunii gazdei sau a iSeries . . . . .	18

## Partea 2. Setarea solicitanților de aplicații gazdă sau iSeries . . . . . 21

### Capitolul 3. Setarea solicitanților de aplicații OS/390 sau z/OS . . . . . 23

Instalarea DB2 ca un solicitant de aplicații (OS/390 și z/OS) . . . . .	23
Task-uri de setare . . . . .	24
Definirea solicitantului de aplicații DB2 la sistemul local – SNA (OS/390 and z/OS) . . . . .	24
Definirea solicitantului de aplicații DB2 la sistemul local – TCP/IP (OS/390 și z/OS) . . . . .	26
Definirea sistemelor de la distanță (OS/390 și z/OS) . . . . .	27

### Capitolul 4. Setarea solicitanților de aplicații AS/400 . . . . . 29

Instalarea DB2 ca un solicitant de aplicații – SNA (iSeries) . . . . .	29
Task-uri de setare . . . . .	29

Definirea cererii de tip aplicație DB2 pentru sistemul local – SNA (iSeries) . . . . .	29
Definirea sistemului de la distanță (iSeries) . . . . .	30
Definirea comunicațiilor SNA (iSeries) . . . . .	31

### Capitolul 5. Setarea solicitanților de aplicații VM . . . . . 35

Setarea pentru DB2 ca un solicitant de aplicație (VM) . . . . .	35
Task-uri de setare . . . . .	35
Definirea solicitantului de aplicație la sistemul local (VM) . . . . .	35
Definirea sistemelor de la distanță pentru solicitantul de aplicație (VM) . . . . .	37
Pregătirea solicitantului de aplicație sau a serverului de aplicație pentru comunicațiile DRDA (VM) . . . . .	38

## Partea 3. Setarea serverelor de aplicații gazdă sau iSeries . . . . . 41

### Capitolul 6. Setarea serverelor de aplicații OS/390 sau z/OS . . . . . 43

Instalarea DB2 ca un server de aplicații (OS/390 și z/OS) . . . . .	43
Task-uri de setare . . . . .	43
Definirea serverului de aplicații la subsistemul SNA (OS/390 și z/OS) . . . . .	43
Definirea serverului de aplicații la subsistemul TCP/IP (OS/390 și z/OS) . . . . .	45

### Capitolul 7. Setarea serverelor de aplicații AS/400 (SNA) . . . . . 47

Instalarea DB ca un server de aplicații folosind SNA (iSeries) . . . . .	47
--	----

### Capitolul 8. Setarea serverelor de aplicații AS/400 (TCP/IP) . . . . . 49

Conectarea la DB2 UDB folosind TCP/IP (iSeries) . . . . .	49
---	----

### Capitolul 9. Setarea serverelor de aplicații VSE . . . . . 55

Instalarea DB2 ca un server de aplicații (VSE) . . . . .	55
Task-uri de setare . . . . .	55
Stabilirea sesiunilor CICS LU 6.2 (VSE) . . . . .	55
Definirea unui server de aplicații (VSE) . . . . .	59
Pregătirea și pornirea serverului de aplicație DB2 (VSE) . . . . .	59

### Capitolul 10. Setarea serverelor de aplicații VM . . . . . 61

Instalarea DB2 ca un server de aplicații (VM) . . . . .	61
Task-uri de setare . . . . .	61
Definirea serverului de aplicații (VM) . . . . .	61

## Partea 4. Concepte gazdă și iSeries 65

### Capitolul 11. Concepte . . . . . 67

DB2 pentru OS/390 și z/OS . . . . .	67
Subconcepte . . . . .	72
Definirea comunicațiilor - SNA (OS/390 și z/OS) . . . . .	72
Setarea mărimilor RU și a pasului (OS/390 și z/OS) . . . . .	73
DB2 UDB pentru iSeries . . . . .	74
DB2 pentru VM . . . . .	74
Subconcepte . . . . .	83
Definirea solicitantului de aplicație de comunicații— . . . . .	83
Setare dimensiuni și ritm RU (VM) . . . . .	84
DB2 pentru VSE . . . . .	84

### Capitolul 12. Considerații de securitate pentru servere de aplicații . . . . . 89

Considerații de securitate pentru serverele de aplicații (OS/390 și z/OS) . . . . .	89
Subconcepte . . . . .	89
Verificarea provenienței (Come-From)(OS/390 and z/OS) . . . . .	89
Nume utilizator oprire - server aplicație (OS/390 și z/OS) . . . . .	89
Securitate rețea - server aplicație (OS/390 și z/OS) . . . . .	92
Securitate manager bază de date - server aplicație (OS/390 și z/OS) . . . . .	93
Subsistem securitate - server aplicație (OS/390 și z/OS) . . . . .	94
Considerații de securitate pentru servere de aplicații (iSeries) . . . . .	94
Considerații de securitate pentru serverele de aplicații (VM) . . . . .	97
Considerații de securitate pentru serverele de aplicație (VSE) . . . . .	100

### Capitolul 13. Considerații de securitate pentru solicitanți de aplicații . . . . . 103

Considerații de securitate pentru solicitanții de aplicații (OS/390 și z/OS) . . . . .	103
Subconcepte . . . . .	103
Nume utilizatori oprire - solicitant aplicație (OS/390 și z/OS) . . . . .	103
Securitate rețea - solicitant aplicație (OS/390 și z/OS) . . . . .	106
Securitate manager bază de date - solicitant de aplicație (OS/390 și z/OS) . . . . .	108
Subsistem de securitate - solicitant de aplicație (OS/390 și z/OS) . . . . .	108
Considerații de securitate pentru utilizatorii aplicației (iSeries) . . . . .	109
Acordarea și revocarea autorității (iSeries) . . . . .	111
Considerente de securitate pentru solicitanții de aplicații (VM) . . . . .	111

### Capitolul 14. Reprezentarea datelor 117

Reprezentarea datelor (OS/390 și z/OS) . . . . .	117
Reprezentarea datelor (iSeries) . . . . .	117
Reprezentarea datelor (VM) . . . . .	120

## Partea 5. Referință gazdă și iSeries 123

## Capitolul 15. Referință. . . . . 125

Produsele de comunicații APPC configurate folosind CA . . . . .	125
Listă de verificări pentru activarea unui server aplicație DB2 (VSE) . . . . .	125
Listă de verificări pentru activarea unui solicitant de aplicații DB2 (VM) . . . . .	126
Tabela cu valorile parametrilor TCP/IP . . . . .	127
Valorile parametrului TCP/IP pentru catalogarea bazelor de date . . . . .	128
Tabelul valorilor parametrilor APPC . . . . .	128
Cuvintele cheie ale instrucțiunii DB2 Conectare (Connect) VTAM APPL . . . . .	131

## Partea 6. Anexe. . . . . 135

### Anexa A. Informații tehnice DB2 Universal Database . . . . . 137

Privire generală asupra informațiilor tehnice DB2 Universal Database . . . . .	137
Categoriile de informații tehnice DB2 . . . . .	137
Tipărirea cărților DB2 folosind fișierele PDF . . . . .	143
Comanda cărților DB2 tipărite . . . . .	144
Accesarea ajutorului online . . . . .	144
Invocarea ajutorului pentru mesaje din linia de comandă . . . . .	145
Invocarea ajutorului pentru comenzi din linia de comandă . . . . .	146
Invocarea ajutorului pentru instrucțiunea SQL din linia de comandă (Windows) . . . . .	146
Apelarea Centrului de informare DB2 . . . . .	147
Actualizarea documentației HTML instalată pe mașina dumneavoastră . . . . .	147
Informații online de depanare DB2 . . . . .	148
Accesibilitatea . . . . .	149
Introducerea de la tastatură și navigarea . . . . .	149
Ecran accesibil . . . . .	149
Răspunsuri de alertare alternative . . . . .	149
Compatibilitate cu tehnologiile de asistare . . . . .	150
Documentație accesibilă . . . . .	150
Îndrumare DB2 . . . . .	150
Centru de informare DB2 pentru subiecte . . . . .	151
Instalarea Centrului de informare DB2 (UNIX) . . . . .	151
Instalarea Centrului de informare DB2 (Windows) . . . . .	152
Configurarea browser-ului să afișeze informațiile în limba preferată . . . . .	152
Diagrame de sintaxă zecimal cu puncte . . . . .	152
Certificare Common Criteria pentru produsele DB2 Universal Database . . . . .	154

### Anexa B. Observații. . . . . 157

Mărci comerciale. . . . .	159
---------------------------	-----

## Index . . . . . 161

## Contactarea IBM . . . . . 165

Informații despre produs . . . . .	165
------------------------------------	-----

---

## Partea 1. Configurarea manuală a comunicațiilor





---

# Capitolul 1. Configurarea manuală a comunicațiilor TCP/IP

---

## Configurarea manuală a comunicațiilor TCP/IP dintre DB2 Connect și un server de bază de date gazdă sau iSeries

Puteți configura manual conexiunea TCP/IP între un server DB2 Connect și o bază de date gazdă sau iSeries. În mod normal, TCP/IP este configurat automat folosind Asistentul de configurare (CA - Configuration Assistant).

### Cerințe preliminare:

Înainte de a configura manual o conexiune TCP/IP între DB2 Connect și o gazdă sau un server de baze de date iSeries, asigurați-vă că:

- TCP/IP este funcțional pe serverul DB2 Connect și pe gazda sau sistemul iSeries.
- Ați identificat valorile următorilor parametri, folosind tabela de configurare a valorilor parametrilor TCP/IP
  - Nume gazdă (*hostname*) sau Adresă IP (*ip\_address*)
  - Numele serviciului de conexiune (*svccname*) sau Numărul portului/Protocolul (*port\_number/tcp*)
  - Numele bazei de date destinație (*target\_dbname*)
  - Numele bazei de date locale (*local\_dcsname*)
  - Numele nodului (*node\_name*)

### Procedură:

Pentru configurarea manuală a comunicațiilor TCP/IP între serverul dumneavoastră DB2 Connect și o gazdă sau o bază de date iSeries

1. Configurarea TCP/IP pe serverul DB2 Connect .
2. Catalogați nodul TCP/IP.
3. Catalogați gazda sau baza de date iSeries ca un serviciu de conexiune bază de date (Database Connection Service) (DCS) .
4. Catalogați gazda sau baza de date iSeries < .
5. Asociați utilitățile și aplicațiile la gazda sau serverul de baze de date iSeries.
6. Testați gazda sau conexiunea iSeries .

**Notă:** Datorită caracteristicilor protocolului TCP/IP, se poate ca TCP/IP să nu fie imediat anunțat de o defectare a partenerului pe o altă gazdă sau iSeries. Ca rezultat, o aplicație a clientului ce accesează un server DB2 la distanță utilizând TCP/IP sau agentul corespunzător de la server poate câteodată să apară blocată. DB2 folosește opțiunea socketului SO\_KEEPALIVE al TCP/IP pentru a detecta când s-a produs o defectare și conexiunea TCP/IP s-a întrerupt.

### Task-uri înrudite:

- “Configurarea TCP/IP pe serverul DB2 Connect” la pagina 4
- “Catalogarea nodului TCP/IP” la pagina 6
- “Catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS)” la pagina 7
- “Catalogarea bazei de date” la pagina 7

- “Asocierea utilităților și aplicațiilor la gazdă sau server de baze de date iSeries” la pagina 9
- “Testarea conexiunii gazdei sau a iSeries” la pagina 9
- “Configurarea manuală a comunicațiilor APPC dintre DB2 Connect și un server de bază de date gazdă sau iSeries” la pagina 11

**Referințe înrudite:**

- “Tabela cu valorile parametrilor TCP/IP” la pagina 127

## Task-uri de configurare

### Configurarea TCP/IP pe serverul DB2 Connect

Configurarea TCP/IP pe un server DB2 Connect este o parte a unei operații mai ample de configurare a comunicațiilor TCP/IP între un server DB2 Connect și o gazdă sau un server de baze de date iSeries.

**Procedură:**

Pentru configurarea TCP/IP pe serverul DB2 Connect:

- Rezolvați adresa IP locală a sistemului gazdă.
- Actualizați fișierul de servicii.

Acum puteți cataloga nodul TCP/IP.

**Task-uri înrudite:**

- “Rezolvarea adresei IP a gazdei locale sau a sistemului iSeries” la pagina 4
- “Actualizarea fișierului de servicii” la pagina 5
- “Catalogarea nodului TCP/IP” la pagina 6

## Task-uri de configurare TCP/IP

### Rezolvarea adresei IP a gazdei locale sau a sistemului iSeries

Rezolvarea adresei IP a gazdei locale sau a sistemului iSeries este o parte dintr-o operație mai amplă de configurare a comunicațiilor TCP/IP între un server DB2 Connect și o gazdă sau o bază de date iSeries. Serverul DB2 Connect trebuie să știe adresa gazdei sau a sistemului iSeries cu care încearcă să stabilească aceste comunicații.

**Notă:** Dacă rețeaua dumneavoastră are un server de nume sau dacă intenționați să specificați în mod direct adresa IP (*adresa\_ip*) a gazdei sau a serverului iSeries, puteți continua prin catalogarea nodului TCP/IP.

Dacă nu există un server de nume în rețeaua dumneavoastră, puteți specifica în mod direct un nume gazdă care se mapează pe adresa IP (*adresa\_ip*) a gazdei sau sistemului iSeries în fișierul local de gazde.

Dacă intenționați acordați suport unui client UNIX care utilizează Servicii de informare rețea (Network Information Services) (NIS) și nu utilizați în rețeaua dumneavoastră un server nume domeniu, trebuie să actualizați fișierul de gazde ce se găsește pe serverul master NIS.

*Tabela 1. Locația fișierelor de gazde locale și servicii*

Sistem de operare	Director
Windows 98	windows

Tabela 1. Locația fișierelor de gazde locale și servicii (continuare)

Sistem de operare	Director
Windows NT și Windows 2000	winnt\system32\drivers\etc
UNIX	/etc

### Procedură:

Pentru rezolvarea adresei IP a gazdei locale sau a sistemului iSeries, folosiți un editor de texte pentru a adăuga o intrare în fișierul de gazde al serverului DB2 Connect cu numele gazdă al sistemului iSeries sau al gazdei.

De exemplu:

```
9.21.15.235    nyx    # host address for nyx
```

unde *9.21.15.235* reprezintă *adresa\_ip*, *nyx* reprezintă *numele gazdă* și *#* reprezintă un comentariu ce descrie intrarea.

Dacă gazda sau sistemul iSeries nu se află în același domeniu ca și serverul DB2 Connect, trebuie să furnizați un domeniu complet determinat cum ar fi *nyx.spifnet.ibm.com*, unde *spifnet.ibm.com* reprezintă numele domeniului.

Următorul pas este catalogarea nodului TCP/IP.

### Task-uri înrudite:

- “Configurarea manuală a comunicațiilor TCP/IP dintre DB2 Connect și un server de bază de date gazdă sau iSeries” la pagina 3
- “Catalogarea nodului TCP/IP” la pagina 6
- “Actualizarea fișierului de servicii” la pagina 5

## Actualizarea fișierului de servicii

Actualizarea fișierului de servicii este o parte a unei operații mai ample de configurare a TCP/IP pe un server DB2 Connect. Săriți peste acest pas dacă intenționați să catalogați un nod TCP/IP utilizând un număr de port (*număr\_port*). Trebuie să actualizați fișierul de servicii al serverului DB2 Connect pentru a adăuga numele serviciului de conexiune și numărul portului ale gazdei de la distanță la care vreți să vă conectați.

### Procedură:

Pentru actualizarea fișierului de servicii, folosiți un editor de texte pentru a adăuga numele serviciului de conexiune și numărul portului ale gazdei de la distanță în fișierul de servicii al serverului DB2 Connect. Acest fișier se află în același director ca și fișierul de gazde locale.

De exemplu:

```
gazdă1 3700/tcp # port serviciu conexiune DB2
```

unde *gazdă1* reprezintă numele serviciului de conexiune, *3700* reprezintă numărul portului de conexiune, *tcp* reprezintă protocolul dumneavoastră de comunicație și *#* reprezintă un comentariu ce descrie intrarea.

Numărul portului folosit pe serverul DB2 Connect trebuie să fie același cu numărul portului folosit pe sistemul gazdă. De asemenea, asigurați-vă că nu ați specificat un număr de port care să fie utilizat de orice alt proces. Dacă intenționați să acordați suport unui client UNIX care

utilizează Servicii de informare rețea (Network Information Services) (NIS), trebuie să actualizați fișierul de servicii ce se găsește pe serverul master NIS.

Următorul pas este catalogarea nodului TCP/IP.

**Task-uri înrudite:**

- “Catalogarea nodului TCP/IP” la pagina 6

## Catalogarea nodului TCP/IP

Catalogarea nodului TCP/IP este o parte a unei operații mai ample de configurare a comunicațiilor între DB2 Connect și o gazdă sau un server de baze de date iSeries. Trebuie să adăugați o intrare în directorul de noduri al serverului DB2 Connect pentru a descrie nodul de la distanță. Această intrare specifică aliasul ales (*nume\_nod*), *numele\_gazdei* (sau *adresa\_ip*) și *numele\_serviciului* (sau *numărul\_portului*) pe care îl va utiliza clientul pentru a accesa gazda de la distanță.

**Cerințe preliminare:**

Un utilizator cu autoritate de Administrator de sistem (System Administrative) (SYSADM) sau de Controller de sistem (System Controller) (SYSCTRL) authority. De asemenea, vă puteți înregistra în sistem și fără aceste nivele de autoritate dacă aveți opțiunea *catalog\_fără\_ autorizare* setată ON.

**Procedură:**

Pentru a cataloga un nod TCP/IP:

1. Pe UNIX, trebuie să setați instanța de mediu și să invocați procesorul de linie de comandă al DB2. Rulați scripturile de pornire după cum urmează:

```
. INSTHOME/sql1lib/db2profile (pentru bash, Bourne sau Korn shell)
source INSTHOME/sql1lib/db2cshrc (pentru C shell)
```

unde *INSTHOME* este directorul acasă al instanței.

2. Catalogarea nodului:

```
catalogarea nodului tcpip nume_nod la distanță [nume_gazdă|adresă_ip]
server [nume_serviciu|număr_port]
terminate
```

De exemplu, pentru a cataloga gazda de la distanță *nyx* pe nodul numit *nod\_db2*, folosind numele serviciului *gazdă1*:

```
catalog tcpip node nod_db2 remote nyx server gazdă1
terminate
```

Pentru a cataloga un server la distanță cu adresa IP *9.21.15.235* pe nodul numit *nod\_db2*, folosind portul numărul *3700*:

```
catalog tcpip node nod_db2 remote 9.21.15.235 server 3700
terminate
```

Pentru a schimba valorile care au fost setate prin comanda **catalog node**:

1. Rulați comanda **uncatalog node** în procesorul de comenzi linie după cum urmează:

```
db2 uncatalog node nume_nod
```

2. Recatalogați nodul cu valorile pe care doriți să le folosiți.

Următorul pas este să catalogați baza de date ca o bază de date DCS.

**Task-uri înrudite:**

- “Configurarea TCP/IP pe serverul DB2 Connect” la pagina 4
- “Catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS)” la pagina 7

**Referințe înrudite:**

- “CATALOG TCPIP NODE Command” în *Command Reference*

## Catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS)

Catalogarea bazei de date ca o bază de date de servicii conexiune(Database Connection Service) (DCS) este o parte a unei operații mai ample de configurare a comunicațiilor între un server DB2 Connect și o gazdă sau o bază de date iSeries. Baza de date de la distanță trebuie catalogată ca o bază de date DCS, astfel încât DB2 Connect să poată asigura accesul la ea.

**Cerințe preliminare:**

Un identificator de utilizator cu autoritate de Administrator de sistem (System Administrative) (SYSADM) sau Controller de sistem (System Controller) (SYSCTRL).

**Procedură:**

Pentru a cataloga baza de date de la distanță ca o bază de date DCS:

```
catalog dcs db nume_dcs_locală as nume_db_destinație
terminate
```

unde:

- *nume\_dcs\_locală* reprezintă numele local al gazdei sau baza de date iSeries.
- *nume\_db\_destinație* reprezintă numele gazdei sau baza de date iSeries.

De exemplu, pentru a face *ny* numele local al bazei de date pentru DB2 Connect, pentru gazda de la distanță sau baza de date iSeries numită *newyork*:

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

Următorul pas este catalogarea bazei de date.

**Task-uri înrudite:**

- “Catalogarea nodului TCP/IP” la pagina 6
- “Catalogarea bazei de date” la pagina 7
- “Catalogarea nodului APPC sau APPN” la pagina 14

**Referințe înrudite:**

- “CATALOG DCS DATABASE Command” în *Command Reference*

## Catalogarea bazei de date

Catalogarea bazei de date este o parte dintr-o operație mai amplă de configurare a comunicațiilor între un server DB2 Connect și o gazdă sau o bază de date iSeries. Înainte ca o aplicație a clientului să poată accesa o bază de date de la distanță, baza de date trebuie catalogată pe nodul gazdei sau al sistemului iSeries și pe toate nodurile DB2 Connect care se vor conecta la ea.

Când creați o bază de date, ea este automat catalogată pe sistemul gazdă sau iSeries cu un alias de bază de date (*alias\_bază\_de\_date*), același cu numele bazei de date(*nume\_bază\_de\_date*). Informația din directorul bazei de date, împreună cu informația din directorul nodului este folosită de serverul DB2 Connect pentru a stabili o conexiune cu gazda de la distanță sau baza de date iSeries.

#### Cerințe preliminare:

- Un identificator de utilizator cu autoritate de Administrator de sistem(System Administrative) (SYSADM) sau Controler de sistem (System Controller) (SYSCTRL).
- Identificați următorii parametri:
  - Numele bazei de date (*nume\_bază\_de\_date*)
  - Aliasul bazei de date (*alias\_bază\_de\_date*)
  - Numele nodului (*nume\_nod*)

#### Procedură:

Pentru a cataloga o bază de date pe un serve DB2 Connect:

1. Pe UNIX, setați instanța de mediu și invocați procesorul de linie de comandă al DB2. Rulați scripturile de pornire după cum urmează:

```
. INSTHOME/sql1lib/db2profile (pentru bash, Bourne sau Korn shell)
source INSTHOME/sql1lib/db2cshrc (pentru C shell)
```

unde *INSTHOME* este directorul acasă al instanței.

2. Catalogarea bazei de date:

```
catalog database nume_bază_de_date as alias_bază_de_date at
node nume_nod authentication valoare_aut
```

De exemplu, pentru a cataloga baza de date DCS cunoscută *ny* astfel încât să aibă aliasul *locallocalny*, pe nodul *nod\_db2*, introduceți următoarele comenzi:

```
catalog database ny as localny at node nod_db2
authentication dcs
terminate
```

Pentru a schimba valorile care au fost setate prin comanda **catalog** *bază\_de\_date*:

- a. Rulați comanda **uncatalog** *bază\_de\_date* în procesorul de comenzo linie după cum urmează:

```
uncatalog database alias_bază_de_date
```

- b. Recatalogați baza de date cu valorile pe care doriți să le folosiți.

Următorul pas este să asociați utilitarele și aplicațiile la serverul de baze de date.

#### Task-uri înrudite:

- “Catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS)” la pagina 7
- “Asocierea utilitărelor și aplicațiilor la gazdă sau server de baze de date iSeries” la pagina 9

#### Referințe înrudite:

- “CATALOG DATABASE Command” în *Command Reference*

## Asocierea utilităților și aplicațiilor la gazdă sau server de baze de date iSeries

Asocierea utilităților și aplicațiilor la gazdă sau server de baze de date iSeries este o parte dintr-o operație mai amplă de configurare a comunicațiilor între un server DB2 Connect și o gazdă sau o bază de date iSeries. După terminarea pașilor de configurare a serverului DB2 Connect pentru a comunica cu gazda sau sistemul iSeries, trebuie să asociați utilitățile și aplicațiile la gazda sau serverul de baze de date iSeries.

### Cerințe preliminare:

Un identificator de utilizator cu autoritate BINDADD.

### Procedură:

Pentru a asocia utilitățile și aplicațiile la gazdă sau server de baze de date iSeries:

```
connect to alias_db user id_utilizator using parolă
bind cale_director_asociere@ddcsmvs.lst blocking all sqlerror continue
messages mvs.msg grant public
connect reset
```

De exemplu:

```
connect to NYC3 user Identificatorul_dvs. using Parola_dvs
bind cale_director_asociere@ddcsmvs.lst blocking all sqlerror continue
messages mvs.msg grant public
connect reset
```

unde *cale\_director\_asociere* reprezintă directorul unde pot fi găsite fișierele cu extensia .lst. De exemplu, pe Windows, calea este de obicei \SQLLIB\BND\.

Următorul pas este să testați gazda sau conexiunea iSeries.

### Concepte înrudite:

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

### Task-uri înrudite:

- “Catalogarea bazei de date” la pagina 7
- “Testarea conexiunii gazdei sau a iSeries” la pagina 9

### Referințe înrudite:

- “BIND Command” în *Command Reference*

## Testarea conexiunii gazdei sau a iSeries

Testarea conexiunii gazdei sau a iSeries este o parte dintr-o operație mai amplă de configurare a comunicațiilor între un server DB2 Connect și o gazdă sau o bază de date iSeries. După ce ați terminat configurarea serverului DB2 Connect pentru comunicațiile cu gazda sau iSeries, trebuie să testați conexiunea pe o bază de date de la distanță.

### Cerințe preliminare:

- Va trebui să vă conectați la o bază de date de la distanță pentru a testa conexiunea.
- Valorile pentru *id\_utilizator* și *parolă* trebuie să fie valide pentru sistemul pe care sunt autentificate. Implicit, autentificarea se face la gazdă sau la serverul de baze de date iSeries.

### Procedură:

Testarea conexiunii gazdei sau iSeries a dumneavoastră:

1. Porniți managerul bazei de date introducând comanda **db2start** pe gazda sau serverul de baze de date iSeries (dacă nu a fost deja pornit).
2. Conectarea la baza de date de la distanță:

```
connect to alias_bază_de_date user id_utilizator using parolă
```

De exemplu, introduceți următoarea comandă :

```
connect to nyc3 user id_utilizator using parola
```

Autentificarea pentru conexiunea la bazele de date gazde se setează în timpul configurării DB2Connect.

Dacă această conexiune s-a realizat cu succes, veți primi un mesaj ce conține numele bazei de date la care v-ați conectat. Acum sunteți capabil să extrageți date din acea bază de date.

De exemplu, pentru a extrage o listă a tuturor numelor de tabele menționate în sistem, introduceți următoarea comandă SQL:

```
select tablename from syscat.tables
```

După ce ați terminat utilizarea conexiunii la baza de date, introduceți comanda **db2 connect reset** pentru a to opri conexiune la baza de date.

### Task-uri înrudite:

- “Asocierea utilităților și aplicațiilor la gazdă sau server de baze de date iSeries” la pagina 9



---

## Capitolul 2. Configurarea manuală a comunicațiilor APPC

---

### Configurarea manuală a comunicațiilor APPC dintre DB2 Connect și un server de bază de date gazdă sau iSeries

Puteți configura manual conexiunea APPC între un server DB2 Connect și o bază de date gazdă sau iSeries. Majoritatea comunicațiilor APPC pot fi configurate automat, folosind Asistentul de configurare (CA - Configuration Assistant).

**Notă:** Ar trebui să aveți în vedere trecerea către TCP/IP, deoarece SNA s-ar putea să nu mai fie suportat pe edițiile viitoare ale DB2 Connect. SNA necesită cunoștințe semnificative de configurare și chiar procesul de configurare în sine se poate dovedi pasibil de erori. TCP/IP este simplu de configurat, are costuri de întreținere reduse și furnizează performanțe superioare.

#### Cerințe preliminare:

- APPC este funcțional pe serverul DB2 Connect și pe gazda sau sistemul iSeries.
- Identificați valorile parametrilor găsiți în tabela cu valorile parametrilor APPC.

#### Restricții:

Protocolul SNA nu este suportabil de versiunea 8.1 a DB2 Connect ce rulează pe platforme Windows64-biți (XP 64-bit și servere .NET 64-bit).

#### Procedură:

Pentru a seta manual un server DB2 Connect pentru a utiliza comunicațiile APPC cu o gazdă sau un server de baze de date iSeries:

1. Actualizați profilele APPC pe serverul DB2 Connect.
2. Catalogați nodul APPC sau APPN.
3. Catalogați gazda sau baza de date iSeries ca o bază de date de servicii conexiune (Database Connection Service) (DCS) .
4. Catalogați gazda sau baza de date iSeries.
5. Asociați utilitățile și aplicațiile la gazda sau serverul de baze de date iSeries.
6. Testați gazda sau conexiunea iSeries .

#### Task-uri înrudite:

- “Actualizarea profilelor APPC pe serverul DB2 Connect” la pagina 12
- “Catalogarea nodului APPC sau APPN” la pagina 14
- “Catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS)” la pagina 7
- “Catalogarea bazei de date” la pagina 7
- “Asocierea utilităților și aplicațiilor la gazdă sau server de baze de date iSeries” la pagina 9
- “Testarea conexiunii gazdei sau a iSeries” la pagina 9
- “Configurarea manuală a comunicațiilor TCP/IP dintre DB2 Connect și un server de bază de date gazdă sau iSeries” la pagina 3

#### Referințe înrudite:

- “Tabelul valorilor parametrilor APPC” la pagina 128

---

## Task-uri de configurare

### Actualizarea profilelor APPC pe serverul DB2 Connect

Actualizarea profilelor APPC pe serverul DB2 Connect este o parte a unei operații mai ample de configurare a comunicațiilor APPC pe gazda sau sistemul iSeries pentru DB2 Connect.

#### Procedură:

Pentru configurarea comunicațiilor APPC pe DB2 Connect ca să acceseze o gazdă sau un server de baze de date iSeries de la distanță, trebuie să actualizați profilele APPC corespunzătoare pentru setările rețelei dumneavoastră:

- Configurarea unui client SNA API pentru Serverul de comunicații rețea IBM (IBM eNetwork Communications Server) pentru Windows
- Configurarea serverului Microsoft SNA
- Configurarea clientului Microsoft SNA
- Configurarea Serverului de comunicații rețea IBM pentru AIX
- Configurarea Bull SNA pentru AIX
- Configurarea SNAPLus2 pentru HP-UX

Următorul pas este catalogarea nodului APPC sau APPN

#### Task-uri înrudite:

- “Configurare Client SNA API pentru Serverul Comunicații IBM eNetwork pentru Windows” la pagina 12
- “Configurare Server Microsoft SNA” la pagina 13
- “Configurare Client Microsoft SNA” la pagina 13
- “Configurare Server Comunicații IBM eNetwork pentru AIX” la pagina 13
- “Configurare Bull SNA pentru AIX” la pagina 14
- “Configurare SNAPLus2 pentru HP-UX” la pagina 14
- “Catalogarea nodului APPC sau APPN” la pagina 14

#### Referințe înrudite:

- “Produsele de comunicații APPC configurate folosind CA” la pagina 125

## Subtask-uri de actualizare a profilelor APPC

### Configurare Client SNA API pentru Serverul Comunicații IBM eNetwork pentru Windows

Suportul următor a fost retras din DB2 Enterprise Server Edition (ESE) pentru Windows și UNIX Versiunea 8 și din DB2 Connect Enterprise Edition (EE) pentru Windows și UNIX Versiunea 8:

- Capacitatea de comitere în două faze folosind SNA. Aplicațiile care necesită comitere în două faze trebuie să utilizeze conectivitatea TCP/IP. Comiterea în două faze folosind TCP/IP către o gazdă sau server de baze de date iSeries a fost disponibilă pentru mai multe ediții. Gazde sau aplicații iSeries care necesită suport pentru comitere în două faze pot folosi noua capacitate a suport comitere în două faze TCP/IP din DB2 ESE Versiunea .

- Aplicațiile nu mai pot accesa un server DB2 UDB ESE pe UNIX sau Windows sau un server DB2 Connect EE folosind SNA. Aplicațiile pot încă să acceseze gazde sau servere de baze de date iSeries folosind SNA dar folosind doar comitere într-o singură fază.

**Task-uri înrudite:**

- “Catalogarea nodului APPC sau APPN” la pagina 14

## **Configurare Server Microsoft SNA**

Suportul următor a fost retras din DB2 Enterprise Server Edition (ESE) pentru Windows și UNIX Versiunea 8 și din DB2 Connect Enterprise Edition (EE) pentru Windows și UNIX Versiunea 8:

- Capacitatea de comitere în două faze folosind SNA. Aplicațiile care necesită comitere în două faze trebuie să utilizeze conectivitatea TCP/IP. Comiterea în două faze folosind TCP/IP către o gazdă sau server de baze de date iSeries a fost disponibilă pentru mai multe ediții. Gazde sau aplicații iSeries care necesită suport pentru comitere în două faze pot folosi noua capacitate a suport comitere în două faze TCP/IP din DB2 ESE Versiunea .
- Aplicațiile nu mai pot accesa un server DB2 UDB ESE pe UNIX sau Windows sau un server DB2 Connect EE folosind SNA. Aplicațiile pot încă să acceseze gazde sau servere de baze de date iSeries folosind SNA dar folosind doar comitere într-o singură fază.

**Task-uri înrudite:**

- “Configurare Client Microsoft SNA” la pagina 13
- “Configurarea manuală a comunicațiilor APPC dintre DB2 Connect și un server de bază de date gazdă sau iSeries” la pagina 11
- “Catalogarea nodului APPC sau APPN” la pagina 14

## **Configurare Client Microsoft SNA**

Suportul următor a fost retras din DB2 Enterprise Server Edition (ESE) pentru Windows și UNIX Versiunea 8 și din DB2 Connect Enterprise Edition (EE) pentru Windows și UNIX Versiunea 8:

- Capacitatea de comitere în două faze folosind SNA. Aplicațiile care necesită comitere în două faze trebuie să utilizeze conectivitatea TCP/IP. Comiterea în două faze folosind TCP/IP către o gazdă sau server de baze de date iSeries a fost disponibilă pentru mai multe ediții. Gazde sau aplicații iSeries care necesită suport pentru comitere în două faze pot folosi noua capacitate a suport comitere în două faze TCP/IP din DB2 ESE Versiunea .
- Aplicațiile nu mai pot accesa un server DB2 UDB ESE pe UNIX sau Windows sau un server DB2 Connect EE folosind SNA. Aplicațiile pot încă să acceseze gazde sau servere de baze de date iSeries folosind SNA dar folosind doar comitere într-o singură fază.

**Task-uri înrudite:**

- “Configurare Server Microsoft SNA” la pagina 13
- “Catalogarea nodului APPC sau APPN” la pagina 14

## **Configurare Server Comunicații IBM eNetwork pentru AIX**

Suportul următor a fost retras din DB2 Enterprise Server Edition (ESE) pentru Windows și UNIX Versiunea 8 și din DB2 Connect Enterprise Edition (EE) pentru Windows și UNIX Versiunea 8:

- Capacitatea de comitere în două faze folosind SNA. Aplicațiile care necesită comitere în două faze trebuie să utilizeze conectivitatea TCP/IP. Comiterea în două faze folosind TCP/IP către o gazdă sau server de baze de date iSeries a fost disponibilă pentru mai multe

ediții. Gazde sau aplicații iSeries care necesită suport pentru comitere în două faze pot folosi noua capacitate a suport comitere în două faze TCP/IP din DB2 ESE Versiunea .

- Aplicațiile nu mai pot accesa un server DB2 UDB ESE pe UNIX sau Windows sau un server DB2 Connect EE folosind SNA. Aplicațiile pot încă să acceseze gazde sau servere de baze de date iSeries folosind SNA dar folosind doar comitere într-o singură fază.

**Task-uri înrudite:**

- “Configurarea manuală a comunicațiilor APPC dintre DB2 Connect și un server de bază de date gazdă sau iSeries” la pagina 11
- “Catalogarea nodului APPC sau APPN” la pagina 14

## **Configurare Bull SNA pentru AIX**

Suportul următor a fost retras din DB2 Enterprise Server Edition (ESE) pentru Windows și UNIX Versiunea 8 și din DB2 Connect Enterprise Edition (EE) pentru Windows și UNIX Versiunea 8:

- Capacitatea de comitere în două faze folosind SNA. Aplicațiile care necesită comitere în două faze trebuie să utilizeze conectivitatea TCP/IP. Comiterea în două faze folosind TCP/IP către o gazdă sau server de baze de date iSeries a fost disponibilă pentru mai multe ediții. Gazde sau aplicații iSeries care necesită suport pentru comitere în două faze pot folosi noua capacitate a suport comitere în două faze TCP/IP din DB2 ESE Versiunea .
- Aplicațiile nu mai pot accesa un server DB2 UDB ESE pe UNIX sau Windows sau un server DB2 Connect EE folosind SNA. Aplicațiile pot încă să acceseze gazde sau servere de baze de date iSeries folosind SNA dar folosind doar comitere într-o singură fază.

## **Configurare SNAPLus2 pentru HP-UX**

Suportul următor a fost retras din DB2 Enterprise Server Edition (ESE) pentru Windows și UNIX Versiunea 8 și din DB2 Connect Enterprise Edition (EE) pentru Windows și UNIX Versiunea 8:

- Capacitatea de comitere în două faze folosind SNA. Aplicațiile care necesită comitere în două faze trebuie să utilizeze conectivitatea TCP/IP. Comiterea în două faze folosind TCP/IP către o gazdă sau server de baze de date iSeries a fost disponibilă pentru mai multe ediții. Gazde sau aplicații iSeries care necesită suport pentru comitere în două faze pot folosi noua capacitate a suport comitere în două faze TCP/IP din DB2 ESE Versiunea .
- Aplicațiile nu mai pot accesa un server DB2 UDB ESE pe UNIX sau Windows sau un server DB2 Connect EE folosind SNA. Aplicațiile pot încă să acceseze gazde sau servere de baze de date iSeries folosind SNA dar folosind doar comitere într-o singură fază.

**Task-uri înrudite:**

- “Configurarea manuală a comunicațiilor APPC dintre DB2 Connect și un server de bază de date gazdă sau iSeries” la pagina 11
- “Catalogarea nodului APPC sau APPN” la pagina 14

## **Catalogarea nodului APPC sau APPN**

Catalogarea nodului APPC sau APPN este o parte a unei operații mai ample de configurare a comunicațiilor APPC pe gazdă pentru DB2 Connect. Trebuie să adăugați o intrare în directorul de noduri al serverului DB2 Connect pentru a descrie nodul de la distanță.

În majoritatea cazurilor, veți adăuga o intrare de nod APPC în directorul de noduri. Pentru Windows 32-bit operating systems, puteți alege să adăugați o intrare de nod APPN, dacă nodul dumneavoastră SNA local a fost setat ca un nod APPN.

### Cerințe preliminare:

Un identificator de utilizator cu autoritate de Administrator de sistem(System Administrative) (SYSADM) sau Controller de sistem (System Controller) (SYSCTRL). De asemenea, vă puteți înregistra în sistem și fără aceste nivele de autoritate dacă aveți opțiunea `catalog_fără_ autorizare` setată ON.

### Procedură:

Catalogarea nodului:

1. Pe UNIX, setați instanța de mediu și invocați procesorul de linie de comandă al DB2. Rulați scripturile de pornire după cum urmează:

```
. INSTHOME/sql1lib/db2profile (pentru bash, Bourne sau Korn shell)
source INSTHOME/sql1lib/db2cshrc (pentru C shell)
```

unde *INSTHOME* este directorul acasă al instanței.

2. Pentru catalogarea unui nod APPC, specificați aliasul ales (*nume\_nod*), Numele destinației simbolice (*nume\_dest\_simbolică*) tipul de securitate APPC *tip\_securitate*) pe care îl va utiliza clientul pentru conexiunea APPC. Introduceți următoarele comenzi:

```
catalog "appc node nume_nod remote nume_dest_simbolică
security tip_securitate"
terminate
```

Parametrul *nume\_dest\_simbolică* este sensibil la majuscule și trebuie să fie identic cu numele destinației simbolice pe care l-ați definit anterior.

De exemplu, pentru a cataloga un server de baze de date de la distanță cu numele destinației simbolice *DB2CPIC* pe nodul *nod\_db2*, folosind tipul de securitate APPC *program*, introduceți următoarele comenzi :

```
catalog appc node nod_db2 remote DB2CPIC security program
terminate
```

3. Pentru catalogarea unui nod APPN, specificați aliasul ales (*nume\_nod*), identificatorul rețelei ( **9** ), partenerul LU de la distanță ( **4** ), numele programului de tranzacție ( **17** ), modul ( **15** ) și tipul de securitate. Introduceți următoarele comenzi, înlocuind cu propriile dumneavoastră valori:

```
catalog "appn node nod_db2 network SPIFNET remote NYM2DB2
tpname QCNTEDDM mode IBMRDB security PROGRAM"
terminate
```

Următorul pas este catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS).

### Task-uri înrudite:

- “Catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS)” la pagina 7

## Catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS)

Catalogarea bazei de date ca o bază de date de servicii conexiune(Database Connection Service) (DCS) este o parte a unei operații mai ample de configurare a comunicațiilor între un server DB2 Connect și o gazdă sau o bază de date iSeries. Baza de date de la distanță trebuie catalogată ca o bază de date DCS, astfel încât DB2 Connect să poată asigura accesul la ea.

### Cerințe preliminare:

Un identificator de utilizator cu autoritate de Administrator de sistem (System Administrative) (SYSADM) sau Controller de sistem (System Controller) (SYSCTRL).

**Procedura:**

Pentru a cataloga baza de date de la distanță ca o bază de date DCS:

```
catalog dcs db nume_dcs_locală as nume_db_destinație
terminate
```

unde:

- *nume\_dcs\_locală* reprezintă numele local al gazdei sau baza de date iSeries.
- *nume\_db\_destinație* reprezintă numele gazdei sau baza de date iSeries.

De exemplu, pentru a face *ny* numele local al bazei de date pentru DB2 Connect, pentru gazda de la distanță sau baza de date iSeries numită *newyork*:

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

Următorul pas este catalogarea bazei de date.

**Task-uri înrudite:**

- “Catalogarea nodului TCP/IP” la pagina 6
- “Catalogarea bazei de date” la pagina 7
- “Catalogarea nodului APPC sau APPN” la pagina 14

**Referințe înrudite:**

- “CATALOG DCS DATABASE Command” în *Command Reference*

## Catalogarea bazei de date

Catalogarea bazei de date este o parte dintr-o operație mai amplă de configurare a comunicațiilor între un server DB2 Connect și o gazdă sau o bază de date iSeries. Înainte ca o aplicație a clientului să poată accesa o bază de date de la distanță, baza de date trebuie catalogată pe nodul gazdei sau al sistemului iSeries și pe toate nodurile DB2 Connect care se vor conecta la ea.

Când creați o bază de date, ea este automat catalogată pe sistemul gazdă sau iSeries cu un alias de bază de date (*alias\_bază\_de\_date*), același cu numele bazei de date (*nume\_bază\_de\_date*). Informația din directorul bazei de date, împreună cu informația din directorul nodului este folosită de serverul DB2 Connect pentru a stabili o conexiune cu gazda de la distanță sau baza de date iSeries.

**Cerințe preliminare:**

- Un identificator de utilizator cu autoritate de Administrator de sistem (System Administrative) (SYSADM) sau Controller de sistem (System Controller) (SYSCTRL).
- Identificați următorii parametri:
  - Nume bază de date (*database\_name*)
  - Aliasul bazei de date (*alias\_bază\_de\_date*)
  - Nume nod (*node\_name*)

**Procedura:**

Pentru a cataloga o bază de date pe un serve DB2 Connect:

1. Pe UNIX, setați instanța de mediu și invocați procesorul de linie de comandă al DB2. Rulați scripturile de pornire după cum urmează:

```
. INSTHOME/sqllib/db2profile    (pentru bash, Bourne sau Korn shell)
source INSTHOME/sqllib/db2cshrc (pentru C shell)
```

unde *INSTHOME* este directorul acasă al instanței.

2. Catalogarea bazei de date:

```
catalog database nume_bază_de_date as alias_bază_de_date at
node nume_nod authentication valoare_aut
```

De exemplu, pentru a cataloga baza de date DCS cunoscută *ny* astfel încât să aibă aliasul *locallocalny*, pe nodul *nod\_db2*, introduceți următoarele comenzi:

```
catalog database ny as localny at node nod_db2
authentication dcs
terminate
```

Pentru a schimba valorile care au fost setate prin comanda **catalog** *bază\_de\_date*:

- a. Rulați comanda **uncatalog** *bază\_de\_date* în procesorul de comenzi linie după cum urmează:

```
uncatalog database alias_bază_de_date
```

- b. Recatalogați baza de date cu valorile pe care doriți să le folosiți.

Următorul pas este să asociați utilitățile și aplicațiile la serverul de baze de date.

#### Task-uri înrudite:

- “Catalogarea bazei de date ca o bază de date de servicii conexiune (Database Connection Service) (DCS)” la pagina 7
- “Asocierea utilităților și aplicațiilor la gazdă sau server de baze de date iSeries” la pagina 9

#### Referințe înrudite:

- “CATALOG DATABASE Command” în *Command Reference*

## Asocierea utilităților și aplicațiilor la gazdă sau server de baze de date iSeries

Asocierea utilităților și aplicațiilor la gazdă sau server de baze de date iSeries este o parte dintr-o operație mai amplă de configurare a comunicațiilor între un server DB2 Connect și o gazdă sau o bază de date iSeries. După terminarea pașilor de configurare a serverului DB2 Connect pentru a comunica cu gazda sau sistemul iSeries, trebuie să asociați utilitățile și aplicațiile la gazda sau serverul de baze de date iSeries.

#### Cerințe preliminare:

Un identificator de utilizator cu autoritate BINDADD.

#### Procedura:

Pentru a asocia utilitățile și aplicațiile la gazdă sau server de baze de date iSeries:

```
connect to alias_db user id_utilizator using parolă
bind cale_director_asociere@ddcsmvs.lst blocking all sqlerror continue
messages mvs.msg grant public
connect reset
```

De exemplu:



```
connect to NYC3 user Identificatorul_dvs. using Parola_dvs
bind cale_director_asociere@ddcsmvs.1st blocking all sqlerror continue
messages mvs.msg grant public
connect reset
```

unde *cale\_director\_asociere* reprezintă directorul unde pot fi găsite fișierele cu extensia .1st. De exemplu, pe Windows, calea este de obicei \SQLLIB\BND\.

Următorul pas este să testați gazda sau conexiunea iSeries.

#### Concepte înrudite:

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

#### Task-uri înrudite:

- “Catalogarea bazei de date” la pagina 7
- “Testarea conexiunii gazdei sau a iSeries” la pagina 9

#### Referințe înrudite:

- “BIND Command” în *Command Reference*

## Testarea conexiunii gazdei sau a iSeries

Testarea conexiunii gazdei sau a iSeries este o parte dintr-o operație mai amplă de configurare a comunicațiilor între un server DB2 Connect și o gazdă sau o bază de date iSeries. După ce ați terminat configurarea serverului DB2 Connect pentru comunicațiile cu gazda sau iSeries, trebuie să testați conexiunea pe o bază de date de la distanță.

#### Cerințe preliminare:

- Va trebui să vă conectați la o bază de date de la distanță pentru a testa conexiunea.
- Valorile pentru *id\_utilizator* și *parolă* trebuie să fie valide pentru sistemul pe care sunt autentificate. Implicit, autentificarea se face la gazdă sau la serverul de baze de date iSeries.

#### Procedura:

Testarea conexiunii gazdei sau iSeries a dumneavoastră:

1. Porniți managerul bazei de date introducând comanda **db2start** pe gazda sau serverul de baze de date iSeries (dacă nu a fost deja pornit).
2. Conectarea la baza de date de la distanță:

```
connect to alias_bază_de_date user id_utilizator using parolă
```

De exemplu, introduceți următoarea comandă :

```
connect to nyc3 user id_utilizator using parola
```

Autentificarea pentru conexiunea la bazele de date gazde se setează în timpul configurării DB2Connect.

Dacă această conexiune s-a realizat cu succes, veți primi un mesaj ce conține numele bazei de date la care v-ați conectat. Acum sunteți capabil să extrageți date din acea bază de date.

De exemplu, pentru a extrage o listă a tuturor numelor de tabele menționate în sistem, introduceți următoarea comandă SQL:

```
select tablename from syscat.tables
```



După ce ați terminat utilizarea conexiunii la baza de date, introduceți comanda **db2 connect reset** pentru a to opri conexiune la baza de date.

**Task-uri înrudite:**

- “Asocierea utilitatelor și aplicațiilor la gazdă sau server de baze de date iSeries” la pagina 9



---

## **Partea 2. Setarea solicitanților de aplicații gazdă sau iSeries**



---

## Capitolul 3. Setarea solicitanților de aplicații OS/390 sau z/OS

---

### Instalarea DB2 ca un solicitant de aplicații (OS/390 și z/OS)

DB2 pentru OS/390 și z/OS implementează suportul pentru solicitantul de aplicații DRDA ca o parte integrantă a facilităților de date distribuite (Distributed Data Facility) (DDF) ale DB2 pentru OS/390 și z/OS. DDF poate fi oprit independent din facilitățile locale de gestiune a bazei de date de pe DB2 pentru OS/390 și z/OS, dar nu poate rula în absența suportului local pentru gestiunea bazei de date al DB2 pentru OS/390 și z/OS.

Când DB2 pentru OS/390 și z/OS acționează ca un solicitant de aplicații, el poate conecta aplicații ce rulează pe sistem la baza de date universală de la distanță DB2 pentru OS/390 și z/OS, DB2 UDB pentru iSeries servere de baze de date DB2 Server for VSE & VM care implementează funcții ale serverului de aplicații DRDA.

Solicitantul de aplicații trebuie să fie capabil să accepte valori RDB\_NAME și să translateze aceste valori în SNA NETID.LUNAME sau valori de adrese TCP/IP. DB2 pentru OS/390 și z/OS folosește baza de date de comunicații a DB2 pentru OS/390 și z/OS (Communications Database) (CDB) pentru a înregistra RDB\_NAME și parametrii de rețea corespunzători. CDB permite solicitantului de aplicații DB2 pentru OS/390 and z/OS să transmită informația necesară către serverul de comunicații când face cereri către baze de date distribuite atât peste conexiuni SNA, cât și peste conexiuni.

#### Procedură:

O mare parte din procesarea într-un mediu al unei baze de date distribuită necesită schimbul de mesaje cu alte locații din rețeaua dumneavoastră. Pentru ca această procesare să se realizeze corect, trebuie să faceți următoarele:

1. Definiți solicitantul de aplicații DB2 la sistemul local (SNA) sau definiți solicitantul de aplicații DB2 la sistemul local (TCP/IP)
2. Definiți sistemele de la distanță

#### Concepte înrudite:

- “Reprezentarea datelor (OS/390 și z/OS)” la pagina 117
- “Considerații de securitate pentru solicitanții de aplicații (OS/390 și z/OS)” la pagina 103
- “DB2 pentru OS/390 și z/OS” la pagina 67

#### Task-uri înrudite:

- “Definirea solicitantului de aplicații DB2 la sistemul local – SNA (OS/390 and z/OS)” la pagina 24
- “Definirea solicitantului de aplicații DB2 la sistemul local – TCP/IP (OS/390 și z/OS)” la pagina 26
- “Definirea sistemelor de la distanță (OS/390 și z/OS)” la pagina 27
- “Instalarea DB2 ca un server de aplicații (OS/390 și z/OS)” la pagina 43

---

## Task-uri de setare

### Definirea solicitantului de aplicații DB2 la sistemul local – SNA (OS/390 and z/OS)

Definirea sistemului local este o parte a unei operații mai ample de instalare a DB2 pentru OS/390 și z/OS ca un server de aplicații. Fiecărui program din rețeaua SNA i se asignează un NETID și un nume LU, astfel încât solicitantul de aplicații DB2 pentru OS/390 și z/OS al dumneavoastră trebuie să aibă o valoare NETID.LUNAME (asignată prin VTAM) când se conectează în rețea. Deoarece solicitantul de aplicații DB2 pentru OS/390 și z/OS este în sistemul local de gestiune a bazei de date al DB2 pentru OS/390 și z/OS solicitantul de aplicații trebuie de asemenea să aibă un RDB\_NAME. În publicațiile DB2 pentru OS/390 și z/OS, DB2 pentru OS/390 și z/OS se referă la RDB\_NAME ca la un nume de *locație*.

#### Procedură:

Pentru definirea solicitantului de aplicații DB2 pentru OS/390 și z/OS către rețeaua SNA:

1. Alegeți un nume LU pentru sistemul dumneavoastră DB2 pentru OS/390 și z/OS. NETID-ul pentru sistemul dumneavoastră DB2 pentru OS/390 și z/OS este obținut automat de la VTAM când pornește DDF.
2. Definiți numele LU și numele locației în *setul de date bootstrap* al DB2 pentru OS/390 și z/OS (BSDS). (DB2 pentru OS/390 și z/OS limitează numele locației la 16 caractere.)
3. Înregistrați numele LU ales cu VTAM creând o definiție VTAM APPL.
4. Asigurați-vă că securitatea extinsă este setată pe YES.

#### Configurarea DDF BSDS:

DB2 pentru OS/390 și z/OS citește BSDS în timpul procesărilor ce se fac la pornire pentru a obține parametrii de instalare ai sistemului. Una din înregistrările memorate în BSDS este numită *înregistrarea DDF*, deoarece conține informația folosită de DDF pentru a se conecta la VTAM. Această informație constă din următoarele:

- Numele locației pentru sistemul DB2 pentru OS/390 și z/OS
- Numele LU pentru sistemul DB2 pentru OS/390 și z/OS
- Parola folosită când sistemul DB2 pentru OS/390 și z/OS se conectează la VTAM

Puteți livra informația DDF BSDS către DB2 pentru OS/390 și z/OS în două moduri:

- Folosiți panoul de instalare DDF - DSNTIPR când instalați pentru prima dată DB2 pentru OS/390 și z/OS pentru a furniza informația DDF BSDS necesară. Mulți dintre parametrii de instalare nu sunt discutați aici, deoarece este mai important de știut cum se conectează DB2 pentru OS/390 și z/OS la VTAM. Figura 1 la pagina 25 arată cum se folosește panoul de instalare pentru a înregistra numele locației NEW\_YORK3, numele LU NYM2DB2 și parola PSWDBD1 în BSDS al DB2 pentru OS/390 și z/OS.

```

                                DISTRIBUTED DATA FACILITY
=> _
Enter data below (introduceți date mai jos):

1 DDF STARTUP OPTION  ==> AUTO      NO, AUTO sau COMMAND
2 DB2 LOCATION NAME   ==> NEW_YORK3 Numele pe care îl folosesc alte DB2 pentru a referi
                                acest DB2
3 DB2 NETWORK LUNAME  ==> NYM2DB2  Numele folosit de VTAM pentru a referi acest DB2
4 DB2 NETWORK PASSWORD ==> PSWDBD1  Parola pentru aplicații VTAM ale DB2
5 RLST ACCESS ERROR   ==> NOLIMIT  NOLIMIT, NORUN sau 1-5000000
6 RESYNC INTERVAL     ==> 3        Minute între perioadele de resincronizare
7 DDF THREADS         ==> ACTIVE    (ACTIVE or INACTIVE) Starea
                                unui fir de execuție de accesare a bazei de date care comite
                                sau întoarce și nu conține nici un zăvor de baze de date sau
                                .
8 DB2 GENERIC LUNAME  ==>          Nume LU VTAM generic pentru acest subsistem DB2
                                sau grup ce partajează date
9 IDLE THREAD TIMEOUT ==> 120      0 sau secunde până când firul de execuție dormind de pe
                                ACTIVE va fi terminat (0-9999)
10 EXTENDED SECURITY   ==> YES      Permite schimbarea parolei și a descrierii
                                codurilor de eroare de securitate. YES sau NO.
PRESS: ENTER to continue RETURN to exit HELP for more information

```

Figura 1. Panoul de instalare al DB2 pentru OS/390 și z/OS DSNTIPR

- Dacă DB2 pentru OS/390 și z/OS este deja instalat, puteți folosi utilitarul de schimbare a jurnalului de inventar (DSNJU003) pentru actualizarea informației din BSDS.

Figura 2 arată cum să actualizați BSDS cu numele locației *NEW\_YORK3*, numele LU *NYM2DB2* și parola *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
//

```

Figura 2. Exemplu de definire a setului de date de bootstrap (DDF) (for VTAM)

Când se pornește DDF (fie automat la pornirea DB2 pentru OS/390 și z/OS, fie prin comanda `START DDF` a DB2 pentru OS/390 și z/OS), el se conectează la VTAM, transmițând numele LU și parola către VTAM. VTAM recunoaște sistemul DB2 pentru OS/390 și z/OS verificând numele LU și parola (dacă este necesară o parolă VTAM) cu valorile definite în declarațiile VTAM APPL ale DB2 pentru OS/390 și z/OS. Parola VTAM este folosită pentru a verifica dacă DB2 pentru OS/390 și z/OS este autorizată să folosească numele LU specificat pe sistemul VTAM. Parola VTAM nu se transmite prin rețea și nu este folosită pentru a conecta alte sisteme din rețea la DB2 pentru OS/390 și z/OS.

Dacă VTAM nu cere o parolă, omiteți PASSWORD= cuvânt\_cheie în utilitarul de schimbare a jurnalului de inventaron. Absența cuvântului cheie indică faptul că nu este necesară o parolă VTAM.

### Înregistrați numele LU ales cu VTAM creând o definiție VTAM APPL:

După ce definiți numele LU VTAM și parola către DB2 pentru OS/390 și z/OS, trebuie să înregistrați aceste valori cu VTAM. VTAM folosește declarațiile APPL pentru a defini nume LU locale. Figura 3 arată o definiție exemplu pentru numele LU *NYM2DB2*.

```

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

```

Figura 3. Exemplu de definiție VTAM APPL pentru DB2 pentru OS/390 și z/OS

#### Task-uri înrudite:

- “Definirea solicitantului de aplicații DB2 la sistemul local – TCP/IP (OS/390 și z/OS)” la pagina 26
- “Definirea sistemelor de la distanță (OS/390 și z/OS)” la pagina 27

#### Referințe înrudite:

- “Cuvintele cheie ale instrucțiunii DB2 Conectare (Connect) VTAM APPL” la pagina 131

## Definirea solicitantului de aplicații DB2 la sistemul local – TCP/IP (OS/390 și z/OS)

### Procedură:

Pentru definirea comunicațiilor TCP/IP cu DB2 pentru OS/390 și z/OS:

1. Comunicațiile TCP/IP trebuie să fie active atât pe DB2 pentru OS/390 și z/OS, cât și pe sistemul partener.
2. Trebuie alocate două numere de port TCP/IP de către administratorul dumneavoastră de rețea. În mod implicit, DB2 pentru OS/390 și z/OS folosește numărul de port 446 pentru conexiuni la baze de date și numărul de port 5001 pentru cereri de resincronizare (ce se comit în două faze)



3. Serverul de aplicații de la distanță sau solicitantul de aplicații trebuie să folosească aceleași numere de port (sau nume de servicii) ca și DB2 pentru OS/390 și z/OS.
4. Asigurați-vă că opțiunea de securitate deja verificată a TCP/IP este setată pe YES.
5. BSDS al DB2 pentru OS/390 și z/OS trebuie să includă parametri suplimentari. Figura 4 evidențiază parametrii suplimentari necesari pentru activarea comunicațiilor 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=nome,PORT=446,RESPORT=5001
/*
//*

```

Figura 4. Exemplu de definire a setului de date de bootstrap (DDF) (for TCP/IP)

#### Task-uri înrudite:

- “Definirea solicitantului de aplicații DB2 la sistemul local – SNA (OS/390 and z/OS)” la pagina 24
- “Definirea sistemelor de la distanță (OS/390 și z/OS)” la pagina 27

## Definirea sistemelor de la distanță (OS/390 și z/OS)

Când o aplicație DB2 pentru OS/390 și z/OS cere date de la un sistem de la distanță, ea caută în tabelele bazei de date de comunicații (Communications Database) (CDB) pentru a găsi informații despre sistemul de la distanță. Baza de date de comunicații (CDB) este un grup de tabele SQL gestionate administratorul sistemului DB2 pentru OS/390 și z/OS.

#### Procedură:

Ca administrator al DB2 pentru OS/390 și z/OS, puteți folosi SQL pentru a insera linii în CDB pentru a descrie fiecare partener DRDA potențial.

Referințe la căutarea de informații în CDB, incluzând:

- Numele LU și TPN (pentru conexiuni SNA)
- Informații despre adresa TCP/IP (necesare numai pentru conexiuni SNA TCP/IP de ieșire)
- Informații de securitate a rețelei solicitate de site-ul de la distanță
- Limitele sesiunii și numele modurilor folosite pentru comunicarea cu site-ul de la distanță (pentru conexiunea SNA)

### **Completarea cu informații a bazei de date de comunicații:**

Nu este necesară nici o actualizare a Bazei de date de comunicații (CDB) dacă veți folosi numai conexiuni TCP/IP de intrare la baze de date, deci dacă intenționați să folosiți DB2 pentru OS/390 și z/OS numai ca un server TCP/IP, nu aveți nevoie să completați CDB și vor fi folosite valori implicite. Totuși, dacă veți folosi conexiuni SNA de intrare, trebuie să furnizați cel puțin o singură linie goală în SYSIBM.LUNAMES.

De exemplu, pentru a permite ca cereri de conectare la baza de date SNA să fie acceptate de la orice DB2 Connect LU de intrare, folosiți o comandă SQL cum ar fi:

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

Când veți folosi DB2 pentru OS/390 și z/OS ca un solicitant, CDB trebuie să fie întotdeauna actualizat. Va trebui să inserați linii în tabela SYSIBM.LOCATIONS și fie în tabela SYSIBM.LUNAMES (pentru conexiuni SNA), fie în tabela SYSIBM.IPNames (pentru conexiuni TCP/IP).

Mai departe, dacă doriți să controlați cerințele de securitate de intrare sau translatarea la intrare a identificatorilor utilizator pentru conexiuni SNA, pot fi necesare actualizări suplimentare ale CDB.

În *DB2 for OS/390 Administration Guide* se discută mai detaliat cerințele pentru actualizarea tabelelor CDB. După ce completați CDB, puteți scrie interogări care accesează date de pe sistemul de la distanță. De asemenea, *DB2 for OS/390 Installation Guide* furnizează mai departe informații despre actualizarea CDB.

### **Tratarea cererilor de către Baza de date de comunicații:**

Când se trimite o cerere, DB2 pentru OS/390 și z/OS folosește coloana LINKNAME a tabelii catalogului SYSIBM.LOCATIONS pentru a determina ce protocol de rețea să folosească pentru conexiunile de ieșire la baza de date. Pentru a primi cereri VTAM, trebuie să alegeți un LUNAME în panoul de instalare DSNTIPR al DB2 pentru OS/390 și z/OS. Pentru a primi cereri TCP/IP, trebuie să selectați un port DRDA și un port de resincronizare în panoul de instalare DSNTIP5 al DB2 pentru OS/390 și z/OS. TCP/IP folosește numărul de port al serverului pentru a transmite cererile din rețea către subsistemul DB2 corect.

Dacă valoarea din coloana LINKNAME este găsită în tabela SYSIBM.IPNames, TCP/IP este folosit pentru conexiuni DRDA. Dacă valoarea este găsită în tabela SYSIBM.LUNAMES, este folosit SNA. Dacă același nume se găsește atât în SYSIBM.LUNAMES, cât și în SYSIBM.IPNames, este folosit TCP/IP pentru conectarea la locația respectivă.

**Notă:** Un solicitant nu se poate conecta la o locație dată folosind ambele protocoale (SNA și TCP/IP). De exemplu, dacă SYSIBM.LOCATIONS al dumneavoastră specifică un LINKNAME (fie LU1) și dacă LU1 este definit în ambele tabele (SYSIBM.IPNames și SYSIBM.LUNAMES), atunci doar TCP/IP este protocolul folosit pentru conectarea la LU1 a acestui solicitant.

### **Task-uri înrudite:**

- “Definirea solicitantului de aplicații DB2 la sistemul local – SNA (OS/390 and z/OS)” la pagina 24
- “Definirea solicitantului de aplicații DB2 la sistemul local – TCP/IP (OS/390 și z/OS)” la pagina 26

---

## Capitolul 4. Setarea solicitanților de aplicații AS/400

---

### Instalarea DB2 ca un solicitant de aplicații – SNA (iSeries)

---

Sistemul iSeries implementează suportul pentru solicitantul de aplicații (application requester) (AR) DRDA ca o parte integrantă a sistemului de operare OS/400. Deoarece suportul pentru solicitantul de aplicații este o parte a sistemului de operare OS/400, el este activ ori de câte ori sistemul de operare este activ.

#### Procedură:

Solicitantul de aplicații (AR) trebuie să fie capabil de a accepta un nume al unei baze de date distribuită și să îl translateze în parametrii rețelei. Sistemul iSeries utilizează directorul de baze de date relaționale pentru a înregistra nume de baze de date relaționale și parametrii lor de rețea corespunzători. Acest director îi permite solicitantului de aplicații al iSeries să transmită informațiile de rețea necesare stabilirii comunicațiilor într-o rețea de baze de date distribuite.

O mare parte din procesarea ce se face într-un mediu de baze de date distribuite cere să facă schimburi de mesaje cu alte locații din rețea. Când DB2 UDB pentru iSeries acționează ca un solicitant de aplicații (AR), el se poate conecta la orice server de aplicații care suportă DRDA. Pentru ca solicitantul de aplicații DB2 UDB pentru iSeries să furnizeze accesul la baze de date distribuite:

- Definirea solicitantului de aplicații DB2 pentru iSeries la sistemul local
- Definirea sistemului de la distanță
- Definirea comunicațiilor SNA

#### Concepte înrudite:

- “Reprezentarea datelor (iSeries)” la pagina 117
- “Considerații de securitate pentru utilizatorii aplicației (iSeries)” la pagina 109
- “DB2 UDB pentru iSeries” la pagina 74
- “Conectarea la DB2 UDB folosind TCP/IP (iSeries)” la pagina 49

#### Task-uri înrudite:

- “Definirea cererii de tip aplicație DB2 pentru sistemul local – SNA (iSeries)” la pagina 29
- “Definirea sistemului de la distanță (iSeries)” la pagina 30
- “Definirea comunicațiilor SNA (iSeries)” la pagina 31
- “Instalarea DB ca un server de aplicații folosind SNA (iSeries)” la pagina 47

---

### Task-uri de setare

#### Definirea cererii de tip aplicație DB2 pentru sistemul local – SNA (iSeries)

Fiecare solicitant de aplicație din rețeaua bazei de date distribuite trebuie să aibă o intrare în Directorul de Bază de Date Relațională (Relational Database Directory) propriu pentru baza de date relațională proprie și una pentru fiecare bază de date relațională de la distanță pe care

AR o accesează. Orice sistem iSeries din rețeaua de bază de date distribuită care se comportă doar ca un server aplicație trebuie să aibă o intrare în directorul de bază de date distribuită proprie pentru baza de date relațională locală.

#### **Procedură:**

Pentru a defini sistemul local se numește baza de date locală prin adăugarea unei intrări cu un nume de locație de la distanță de \*LOCAL la directorul bazei de date relaționale. Pentru aceasta se folosește comanda Adăugare Intrare în Directorul de Bază de Date Relațională (Add Relational Database Directory Entry) (ADDRDBDIRE). Următorul exemplu arată comanda ADDRDBDIRE, unde numele bazei de date din AR este ROCHESTERDB:

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

În ultima versiune a OS/400, RDB-ul local denumește intrarea prin creare în mod automat dacă acesta nu există deja atunci când este cerut. Numele sistemului din atributele de rețea va fi folosit ca nume al RDB-ului local.

#### **Task-uri înrudite:**

- “Definirea sistemului de la distanță (iSeries)” la pagina 30

## **Definirea sistemului de la distanță (iSeries)**

Fiecare server aplicație din rețeaua bazei de date distribuită trebuie să aibă de asemenea o intrare locală în propriul director RDB. În plus, o intrare pentru fiecare bază de date de la distanță trebuie să fie prezentă în directorul RDB al fiecărui solicitant de aplicație.

#### **Procedură:**

Pentru definirea bazelor de date de la distanță în baza de date locală:

- Se adaugă o intrare pentru fiecare bază de date de la distanță în directorul de bază de date relațională folosind comanda ADDRDBDIRE sau comanda WRKRDBDIRE.

Pentru comunicațiile SNA informația care se poate specifica include:

- Numele bazei de date de la distanță
- Numele locației de la distanță a bazei de date
- Numele locației locale
- Numele modului folosit pentru stabilirea comunicațiilor
- Identificatorul de rețea de la distanță
- Numele dispozitivului folosit pentru comunicații
- Numele programului de tranzacție al bazei de date de la distanță

În cele mai multe cazuri singurele informații necesare sunt numele bazei de date de la distanță și numele locației de la distanță<sup>1</sup> al bazei de date. Atunci când numele locației de la distanță este specificat, valorile implicite sunt folosite pentru parametrii rămași. Sistemul selectează un dispozitiv folosind numele locației de la distanță.

Dacă mai mult de o descriere de dispozitiv conține același nume de locație de la distanță și o descriere de dispozitiv anume este necesară, atunci valorile pentru numele de locație locală și identificatorul de rețea de la distanță al intrării din directorul bazei de date relaționale ar trebui să se potrivească cu valorile descrierilor de dispozitiv. Selecția descrierilor de dispozitiv poate fi complicată dacă același nume de locație de la distanță este folosit în mai mult de o descriere

---

1. “Nume Locație” în OS/400 este sinonim cu “Nume LU” în VTAM. “Numele locației de la distanță” înseamnă “partener sau nume al LU de la distanță”.

de dispozitiv. A se folosi nume de locații de la distanță unice pentru fiecare descriere de dispozitiv pentru a se evita confuzia. Numele programului de tranzacție al bazei de date de la distanță are ca valoare implicită numele programului de tranzacție implicit DRDA de X'07F6C4C2'.

Informațiile legate de comunicații din directorul de bază de date relațională sunt folosite pentru stabilirea unei conversații cu sistemul de la distanță.

**Task-uri înrudite:**

- “Definirea comunicațiilor SNA (iSeries)” la pagina 31
- “Definirea cererii de tip aplicație DB2 pentru sistemul local – SNA (iSeries)” la pagina 29

## Definirea comunicațiilor SNA (iSeries)

Sistemul iSeries permite de asemenea configurații avansate de comunicații (APPC) de tipul program-cu-program, care nu furnizează suport pentru rutarea în rețea. O bază de date distribuită iSeries lucrează cu oricare configurație.

Suportul pentru Orice rețea (AnyNet) de pe iSeries permite aplicațiilor APPC să ruleze peste rețelele TCP/IP. Exemplele din secțiunea următoare includ DDM, Systems Network Architecture Distribution Services (Servicii de distribuție a arhitecturii rețelelor de sisteme), Alerte și 5250 Display Station Pass-Through. Aceste aplicații, împreună cu DRDA, pot rula neschimbate peste rețele TCP/IP cu câteva configurări adiționale. Pentru a specifica suportul pentru orice rețea AnyNet, specificați \*ANYNW pentru parametrul LINKTYPE al comenzii CRTCTLAPPC.

**Procedură:**

APPN furnizează suport de interconectare în rețea care permite sistemului iSeries să participe și să controleze o rețea de sisteme fără să solicite suport de rețea, furnizat în mod tradițional de un sistem specializat în aceasta (un mainframe). Pentru configurarea unui sistem iSeries pentru suport APPN.

1. Definiți atributele rețelei folosind comanda de schimbare a atributelor rețelei (CHGNETA).

Atributele rețelei conțin:

- Numele sistemului local
- Numele sistemului din rețeaua APPN
- Identificatorul din rețeaua locală
- Tipul nodului de rețea
- Numele serverelor de rețea folosite de sistemul iSeries, dacă mașina este un nod terminal
- Punctele de control ale rețelei, dacă iSeries este un nod terminal

2. Creați descrierea de linie.

Descrierea de linie descrie linia de conexiune fizică și protocolul ce asigură legătura de date ce vor fi folosite între sistemul iSeries și rețea. Folosiți următoarele comenzi pentru a crea descrieri de linii:

- Creați descriere de linie (Ethernet) (CRTLINETH)
- Creați descriere de linie (SDLC) (CRTLINS DLC)
- Creați descriere de linie (token ring) (CRTLINTRN)
- Creați descriere de linie (X.25) (CRTLINX25)

3. Creați descrieri controlere.

Descrierea controler descrie sistemele alăturate din rețea. Indicați folosirea suportului APPN specificând APPN (\*YES) când creați descrierea controler. Folosiți următoarele comenzi pentru a crea descrieri controler:

- Creați descriere controler (APPC) (CRTCTLAPPC)
- Creați descriere controler (SNA HOST) (CRTCTLHOST)

Dacă parametrul AUTOCRTCTL dintr-o descriere de linie token-ring sau Ethernet este setat la \*YES, atunci se creează automat o descriere controler când sistemul primește o cerere de pornire a unei sesiuni peste o linie token-ring sau Ethernet.

#### 4. Creați o descriere de clasă-de-serviciu.

Folosiți descrierea unei clase-de-serviciu pentru a selecta rutele de comunicație (grupuri de transmisie) și pentru a da prioritatea transmisiei. Cinci descrieri de clase-de-serviciu sunt furnizate de către sistem:

##### **#CONNECT**

Clasa de serviciu implicită.

##### **#BATCH**

O clasă de serviciu pentru joburi batch.

##### **#BATCHSC**

La fel ca #BATCH, cu excepția faptului că este necesară o securitate la nivelul legăturii de date sau cel puțin o rețea cu comutare de pachete. În rețelele cu comutare de pachete, datele nu urmează întotdeauna aceeași cale prin rețea.

##### **#INTER**

O clasă de serviciu ajustată pentru comunicații interactive.

##### **#INTERSC**

La fel ca #INTER, cu excepția faptului că este necesară o securitate la nivelul legăturii de date sau cel puțin o rețea cu comutare de pachete.

Creați alte descrieri de clase-de-serviciu folosind comanda de creare a claselor-de-serviciu (CRTCOSD).

#### 5. Creați o descriere de mod.

Descrierea mod dă caracteristicile sesiunii și numărul de sesiuni care pot fi folosite pentru negocierea valorilor permise între locația locală și cea de la distanță. Descrierea mod indică de asemenea clasa-de-serviciu care este folosită pentru conversație. Câteva moduri predefinite sunt livrate împreună cu sistemul:

##### **BLANK**

Numele de mod implicit specificat în atributele rețelei când se livrează sistemul.

##### **#BATCH**

Un mod ajustat pentru joburi batch.

##### **#BATCHSC**

La fel ca #BATCH, cu excepția faptului că descrierea de clasă-de-serviciu asociată necesită o securitate la nivelul legăturii de date sau cel puțin o rețea cu comutare de pachete.

##### **#INTER**

Un mod ajustat pentru comunicații interactive.

##### **#INTERSC**

La fel ca #INTER, cu excepția faptului că descrierea de clasă-de-serviciu asociată necesită o securitate la nivelul legăturii de date sau cel puțin o rețea cu comutare de pachete.

##### **IBMRDB**

Un mod ajustat pentru comunicații DRDA.

Pot fi create alte descrieri mod folosind comanda de creare descriere mod (CRTMODD).

6. Creați descrierile dispozitivelor.

Descrierea dispozitivului furnizează caracteristicile conexiunii logice între sistemul local și cel de la distanță. Nu trebuie să creați manual descrieri de dispozitiv dacă sistemul iSeries rulează pe o gazdă cu APPN și ca o unitate logică independentă (LU). Sistemul iSeries creează automat descrierea dispozitivului și o atașează descrierii controler corespunzătoare în momentul stabilirii sesiunii. Dacă sistemul iSeries este un LU dependent, atunci trebuie să creați manual descrierile de dispozitiv folosind comanda de creare descriere dispozitiv (CRTDEVAPPC). În descrierea dispozitivului, specificați APPN(\*YES) pentru a indica faptul că se folosește APPN.

7. Creați listele de locații APPN.

Dacă sunt necesare locații locale suplimentare (numite LU pe alte sisteme) sau caracteristici speciale ale locațiilor de la distanță pentru APPN, atunci trebuie să creați lista de locații APPN. Numele locației locale este numele punctului de control specificat în atributele rețelei. Dacă aveți nevoie de locații suplimentare pentru sistemul iSeries, este necesară o listă locală de locații APPN. Un exemplu de caracteristică specială a unei locații de la distanță este dacă locația de la distanță se află într-o altă rețea decât cea în care se află locația locală. Dacă există condițiile, este necesară o listă a locațiilor de la distanță. Creați listele de locații APPN folosind comanda de creare a listei de configurații (CRTCFGL).

8. Activați comunicațiile.

Puteți activa descrierile comunicației folosind comanda de schimbare a configurației (VRYCFG) sau comanda de lucru cu starea configurației (WRKCFGSTS). Dacă descrierile de linie sunt activate, atunci controlerele și dispozitivele atașate acelei linii sunt de asemenea activate. Comanda WRKCFGSTS este de asemenea utilă pentru vizualizarea stării fiecărei conexiuni.

9. Dimensiunile RU și sincronizarea

Dimensiunile RU și sincronizarea sunt controlate de valori specificate în descrierea mod. Când creați descrierea mod, sunt furnizate valori implicite pentru dimensiunea RU și sincronizare. Valorile implicite sunt o estimare iSeries pentru majoritatea mediilor, inclusiv pentru baze de date distribuite. Dacă pentru dimensiunea RU se ia valoarea implicită, sistemul iSeries estimează cea mai bună valoare de folosit. Când sistemul iSeries comunică cu un alt sistem care suportă sincronizare adaptabilă, atunci valorile de sincronizare specificate sunt doar un punct de pornire. Sincronizarea este ajustată de fiecare sistem, în funcție de capacitatea sistemului de a trata datele trimise către el. Pentru sisteme care nu suportă sincronizare adaptabilă, valorile de sincronizare sunt negociate la pornirea sesiunii și rămân aceleași de-a lungul întregii sesiuni.

**Note:**

1. Descrierea controler este echivalentă cu macrourele unității fizice (PU) din Programul IBM de control al rețelei și Metoda de acces la telecomunicații virtuale (Network Control Program and Virtual Telecommunications Access Method) (NCP/VTAM).
2. Descrierea dispozitiv este echivalentă cu macrourele unității logice (LU) a NCP/VTAM. Descrierea de dispozitiv conține informație similară cu cea memorată în profilul LU al partenerului din Communications Manager/2 1.1.
3. Descrierea mod este echivalentă cu tabelele de mod NCP/VTAM și de profilul Communications Manager Transmission Service Mode.

**Task-uri înrudite:**

- “Definirea cererii de tip aplicație DB2 pentru sistemul local – SNA (iSeries)” la pagina 29
- “Definirea sistemului de la distanță (iSeries)” la pagina 30





---

## Capitolul 5. Setarea solicitanților de aplicații VM

---

### Setarea pentru DB2 ca un solicitant de aplicație (VM)

DB2 pentru VM implementează suportul pentru solicitantul de aplicație DRDA ca parte integrală pentru adaptorul de resursă care se află pe mașina virtuală a utilizatorului final cu aplicația. Utilizatorul poate folosi suportul de apelare aplicație chiar și atunci când mașina virtuală pentru database managers local nu este activă. Se poate activa suportul de apelare aplicație DRDA rulând SQLINIT EXEC cu protocol(auto) sau cu protocol(drda).

#### Procedură:

Atunci când DB2 pentru VM joacă rol de solicitant de aplicație, poate conecta la orice DB2 pentru serverul de aplicație VM sau pentru orice alt server care suportă arhitectura DRDA. Pentru DB2, pentru ca solicitantul de aplicație VM să furnizeze acces la baza de date distribuită, este necesar ca utilizatorul să cunoască cum să facă următoarele:

- Acest solicitant de aplicație trebuie să fie capabil să accepte RDB\_valorile NAME și să le transforme pe acestea în valori SNA NETID.LUNAME. DB2 pentru VM utilizează Directorul de comunicații CMS pentru a cataloga numele RDB\_ și parametri de rețea corespunzători lor. Directorul de comunicații permite solicitantului aplicației să transmită informațiile SNA cerute la VTAM atunci când se returnează cererile bazei de date distribuită.

O mare parte a procesării într-un mediu bază de date distribuită necesită mesaje pentru a fi schimbate cu alte locații din rețea. Pentru a realiza acest proces în mod corect, se urmăresc următorii pași:

1. Se definește solicitantul de aplicație la sistemul local
2. Se definesc sistemele de la distanță pentru solicitantul de aplicație
3. Se pregătește solicitantul de aplicație sau serverul de aplicație pentru comunicațiile DRDA

#### Concepte înrudite:

- “DB2 pentru VM” la pagina 74
- “Considerente de securitate pentru solicitanții de aplicații (VM)” la pagina 111

#### Task-uri înrudite:

- “Definirea solicitantului de aplicație la sistemul local (VM)” la pagina 35
- “Definirea sistemelor de la distanță pentru solicitantul de aplicație (VM)” la pagina 37
- “Pregătirea solicitantului de aplicație sau a serverului de aplicație pentru comunicațiile DRDA (VM)” la pagina 38
- “Instalarea DB2 ca un server de aplicații (VM)” la pagina 61

---

### Task-uri de setare

#### Definirea solicitantului de aplicație la sistemul local (VM)

Definirea solicitantului de aplicație DB2 pentru VM la sistemul local este parte a task-ului mai mare de setare a DB2 pentru VM ca un solicitant de aplicație. Solicitantul de aplicație DB2 pentru VM și serverul de aplicație DB2 pentru VM sunt independenți unul de altul.

Solicitantul de aplicație DB2 pentru VM direcționează cereri de conexiune direct la serverele de aplicație de la distanță sau locale. Totuși, nu se definește singur ca țintă pentru cererile de conexiune internă. Numai serverul de aplicație DB2 pentru VM poate accepta (sau respinge) cererile de conexiune internă. De aceea, aplicantul de aplicație DB2 pentru VM nu identifică un nume RDB\_NAME și TPN pentru el însuși, așa cum face DB2 pentru OS/390 și pentru z/OS.

**Procedură:**

Se definește solicitantul de aplicație DB2 pentru VM la rețeaua SNA după cum urmează:

1. Se definește nume de gateway AVS utilizând instrucțiunile de definiție VTAM APPL.

Solicitantul de aplicație trebuie să definească nume de gateway (de exemplu, numele LU) pentru a ruta cererile destinate în rețea. Figura 5 arată un exemplu pentru aceasta. Aceste instrucțiuni se aplă pe mașina virtuală VTAM. Atunci când VTAM pornește, gateway-urile sunt identificate în rețea, dar nu sunt activate până când se pornește mașina virtuală de control AVS. Fiecare mașină virtuală AVS poate defini gateway-uri multiple pe un host VM.

```

          VBUILD TYPE=APPL
*****
*
*   Definiție de gateway pentru Sistemul Toronto DB2 pentru VM   *
*
*****
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

```

Figura 5. Exemplu de o Definiție gateway AVS

2. Activarea gateway-ului.

Activarea gateway-ului este realizată de la mașina virtuală AVS care operează pe aceeași gazdă (sau alte gazde în cadrul aceleiași colecții TSAF) ca și solicitantul de aplicație DB2 pentru VM. Se include o comandă AGW ACTIVATE GATEWAY GLOBAL în profilul mașinii AVS sau se emite această comandă în mod interactiv de la consola mașină AVS pentru a activa automat gateway-ul de fiecare dată când AVS pornește.

3. Se folosește comanda AGW CNOS pentru a negocia numărul de sesiuni între gateway și fiecare din partenerii săi LU.

Se asigură că valoarea MAXCONN din directorul CP pentru mașina gateway AVS este destul de mare pentru a suporta numărul total de sesiuni cerut.

Se emite comanda AGW DEACTIVE GATEWAY de la mașina virtuală AVS pentru a dezactiva gateway-ul. Definiția gateway-ului rămâne. Gateway-ul poate fi activat din nou în orice moment folosind comanda AGW ACTIVATE GATEWAY GLOBAL.

4. Asigurați-vă că VTAM NETID este definit la DB2 pentru VM DBMS în timpul instalării.

NETID pentru gazdă (sau alte gazde din cadrul aceleiași colecții TSAF) unde solicitantul de aplicație se află este furnizat de VTAM când cererea intră în rețea. NETID este

memorat în fișierul CMS SNA NETID și se află în discul de producție DB2 pentru VM accesat de solicitantul de aplicație. Solicitantul de aplicație folosește acest NETID pentru generarea de LUWID care circulă cu fiecare conversație.

**Task-uri înrudite:**

- “Definirea sistemelor de la distanță pentru solicitantul de aplicație (VM)” la pagina 37
- “Pregătirea solicitantului de aplicație sau a serverului de aplicație pentru comunicațiile DRDA (VM)” la pagina 38

## Definirea sistemelor de la distanță pentru solicitantul de aplicație (VM)

Definirea sistemelor de la distanță pentru solicitantul de aplicație VM este parte a unui task mai mare de setare a DB2 pentru VM ca un solicitant de aplicație. Utilizatorul poate defini sistemele de la distanță prin înregistrarea numelor LU care activează VTAM pentru a localiza destinația de rețea dorită. Atunci când AVS pornește, se identifică numele de gateway globale (numele LU) disponibile pentru rutarea cererilor SQL din rețea la VTAM. Un nume de gateway trebuie să fie unic în cadrul setului numelor LU recunoscute de sistemul VTAM local, astfel încât toate cererile din cadrul rețelei, sau în afara acesteia sunt rutate la numele LU corespunzător. Acesta este cel mai bun mod de a asigura unicitatea numelui gateway-ului prin rețeaua utilizator. Acest lucru simplifică procesul definiției resursă VTAM.

Atunci când o aplicație DB2 pentru VM cere date de la un sistem de la distanță, DB2 pentru VM caută Directorul comunicații CMS pentru următoarele informații legate la sistemul de la distanță:

- Numele gateway-ului (numele local LU)
- Numele LU de la distanță
- TPN de la distanță
- Nivelul de securitate pentru conversație cerut de serverul de aplicație
- ID-ul utilizatorului care identifică solicitantul de aplicație la serverul de aplicație
- Parola care autorizează solicitantul de aplicație la serverul de aplicație
- Numele de mod care descrie caracteristicile de sesiune pentru a utiliza la comunicarea cu serverul de aplicație
- RDB\_NAME

**Procedură:**

CMS Communications Directory este un fișier CMS cu tipul de fișier NAMES, care este creat și administrat de un administrator de sistem DB2 pentru VM.

Ca administrator, se poate folosi XEDIT pentru a crea acest fișier și pentru a adăuga intrările dorite pentru a identifica orice potențial partener DRDA. Fiecare intrare din director este un set de taguri și valorile lor asociate. Figura 6 la pagina 38 arată o intrare exemplu. Atunci când se face o căutare, cheia de căutare este comparată cu valoarea tagului dbname :a fiecărei intrări din fișier până când este găsită o potrivire sau până când este atins sfârșitul de fișier. În exemplul din Figura 6 la pagina 38, managerul de vânzări din Toronto dorește să creeze un raport lunar al vânzărilor pentru ramura Montreal prin accesarea datelor de la distanță de la baza de date 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

```

Figura 6. O intrare exemplu într-o CMS Communications Directory

Tagul tpn: identifică numele de program de tranzacție tpn care activează serverul de aplicație. Prima parte a tagului luname : identifică gateway-ul AVS (local LU) utilizat pentru a câștiga acces la rețeaua SNA. A doua parte identifică numele de la distanță LU. Tagul modename :identifică modul VTAM care definește caracteristicile sesiunilor alocate între LU-urile local și de la distanță. Dimensiunea unității de cerere (RU), ritmul și clasa de serviciu (COS) sunt exemple de asemenea caracteristici. Tagul de securitate :security indică nivelul de securitate care va fi folosit la conversația care conectează aplicația apelatoare la serverul de aplicație.

CMS Communications Directory este accesibil pe un disc de sistem public la toți apelatorii de aplicație într-un sistem VM particular. Orice program sau produs care cere acces de la distanță prin VTAM poate utiliza CMS Communications Directory.

Utilizatorul poate accesa două nivele pentru CMS Communications Directory: nivelul-sistem și nivelul-utilizator. De exemplu, utilizatorul poate crea un director de nivel-sistem pe un disc sistem public accesibil la toți apelatorii de aplicație într-un sistem particular VM. Utilizatorul poate de asemenea crea propriul director de nivel-utilizator pentru a suprascrie intrări existente sau pentru a introduce noi intrări care nu apar în directorul de nivel-sistem. Directorul de nivel-utilizator este primul căutat și în cazul în care căutarea eșuează, atunci este căutat directorul de nivel-sistem. Directorul de nivel-sistem este o extensie a directorului de nivel-utilizator; este căutat numai dacă valorile nu sunt găsite în directorul de nivel utilizator.

Fiecare din aceste directoare este identificat aplicației și este activat cu ajutorul comenzii CMS SET COMDIR. De exemplu, utilizatorul poate folosi următoarea secvență de comandă pentru a identifica amândouă directoarele, de nivel-sistem și de nivel-utilizator (pe minidiscurile A, respectiv S), dar se alege să se activeze numai directorul de nivel-sistem pentru căutări:

```

SET COMDIR FILE SYSTEM SCOMDIR NAMES S

SET COMDIR FILE USER UCOMDIR NAMES A

SET COMDIR OFF USER

```

**Task-uri înrudite:**

- “Definirea solicitantului de aplicație la sistemul local (VM)” la pagina 35
- “Pregătirea solicitantului de aplicație sau a serverului de aplicație pentru comunicațiile DRDA (VM)” la pagina 38

## Pregătirea solicitantului de aplicație sau a serverului de aplicație pentru comunicațiile DRDA (VM)

Pregătirea lui DB2 pentru solicitantul de aplicație sau pentru serverul de aplicație este o parte din marea operație de setare a lui DB2 pentru VM ca un solicitant de aplicație sau ca un server de aplicație. Solicitantul de aplicație DB2 pentru VM sau serverul de aplicație ar putea să nu aibă suportul pentru DRDA deja instalat.

**Procedură:**

Pentru pregătirea lui DB2 pentru solicitantul de aplicație VM sau serverul de aplicație pentru comunicațiile de tip DRDA:

1. Se folosește exec-ul ARISDBMA pentru instalarea suportului DRDA:
  - Se folosește "ARISDBMA DRDA(ARAS=Y)" dacă se instalează suportul pentru solicitant și pentru server.
  - Se folosește "ARISDBMA DRDA(AR=Y)" dacă se instalează suportul doar pentru solicitant.
  - Se folosește "ARISDBMA DRDA(AS=Y)" dacă se instalează suportul doar pentru server.
2. Se reconstruiește DB2 pentru VM ARISQLLD LOADLIB.

Pentru mai multe informații a se vedea "Folosirea unui Mediu DRDA" din cartea *DB2 Server for VM System Administration*.



---

## **Partea 3. Setarea serverelor de aplicații gazdă sau iSeries**





---

## Capitolul 6. Setarea serverelor de aplicații OS/390 sau z/OS

---

### Instalarea DB2 ca un server de aplicații (OS/390 și z/OS)

Suportul pentru serverul de aplicații în DB2 pentru OS/390 și z/OS îi permite acestuia să acționeze ca un server pentru DRDA solicitanții de aplicații.

#### Procedură:

Pentru instalarea DB2 pentru OS/390 și z/OS ca un server de aplicații:

1. Definiți serverul de aplicații la subsistemul SNA local.
2. Definiți serverul de aplicații la subsistemul TCP/IP local.

#### Concepte înrudite:

- “Reprezentarea datelor (OS/390 și z/OS)” la pagina 117
- “DB2 pentru OS/390 și z/OS” la pagina 67
- “Considerații de securitate pentru serverele de aplicații (OS/390 și z/OS)” la pagina 89

#### Task-uri înrudite:

- “Definirea serverului de aplicații la subsistemul SNA (OS/390 și z/OS)” la pagina 43
- “Definirea serverului de aplicații la subsistemul TCP/IP (OS/390 și z/OS)” la pagina 45
- “Instalarea DB2 ca un solicitant de aplicații (OS/390 și z/OS)” la pagina 23

---

### Task-uri de setare

#### Definirea serverului de aplicații la subsistemul SNA (OS/390 și z/OS)

Pentru ca serverul de aplicații să primească cereri pentru baze de date distribuite, el trebuie definit la Communications Manager local și să aibă un RDB\_NAME unic. Discuția următoare se referă la conexiunile SNA.

#### Procedură:

Pentru definirea serverului de aplicații la subsistemul SNA:

1. Selectați numele LU și RDB\_NAME ce vor fi folosite de gazda serverului de aplicații DB2 UDB. RDB\_NAME pe care îl alegeți pentru DB2 UDB pe gazdă trebuie livrat tuturor utilizatorilor finali și solicitanților de aplicații care cer conectarea la serverul de aplicații.
2. Înregistrați valoarea NETID.LUNAME pentru gazda serverului de aplicații DB2 UDB la fiecare solicitant de aplicații ce solicită accesul, astfel încât solicitantul de aplicații să poată ruta cereri SNA către gazda serverului DB2 UDB. Acest lucru este valabil chiar și în cazuri în care solicitantul de aplicații este capabil de a realiza rutare dinamică în rețea, deoarece solicitantul de aplicații trebuie să cunoască NETID.LUNAME, înainte de a putea fi folosită rutarea dinamică în rețea.
3. Furnizați valoarea TPN implicită('X'07F6C4C2') a DRDA fiecărui solicitant de aplicații, deoarece gazda DB2 UDB utilizează în mod automat această valoare.

4. Creați o intrare în tabela de moduri a VTAM pentru fiecare nume de mod cerut de un solicitant de aplicații. Aceste intrări descriu dimensiunile RU, dimensiunea ferestrei de sincronizare și clasa de servicii pentru fiecare nume de mod.
5. Definiți limitele sesiunii pentru solicitantul de aplicații care se conectează cu serverul de aplicații DB2 pentru OS/390 și z/OS. Declarația VTAM APPL definește limitele implicite ale sesiunii pentru toți partenerii sistemului. Dacă doriți să stabiliți valori implicite pentru un anumit partener, puteți folosi tabela SYSIBM.LUMODES a bazei de date de comunicații (CDB).
6. Creați intrări în gazda DB2 UDB CDB pentru a identifica solicitanții de aplicații cărora li se permite conectarea la gazda serverului de aplicații DB2 UDB. Metodele de bază pentru definirea intrărilor CDB pentru solicitanții de aplicații din rețea sunt:
  - a. Puteți insera o linie în SYSIBM.LUNAMES care furnizează valori implicite de folosit pentru orice LU care nu este descris explicit în CDB (linia implicită conține spații în coloana LUNAME). Această metodă vă permite să definiți atribute specifice pentru unele LU din rețeaua dumneavoastră o dată cu stabilirea de valori implicite pentru toți ceilalți.  
  
De exemplu, puteți permite sistemului DALLAS (o altă gazdă de sistem DB2 UDB) să trimită cereri pentru baze de date distribuite deja verificate (LU 6.2 SECURITY=SAME), solicitând totodată sistemelor database manager să trimită parole. În continuare, s-ar putea să nu doriți să înregistrați câte o intrare în CDB pentru fiecare sistem database manager, mai ales dacă este vorba despre un număr mare de astfel de sisteme. Figura 7 arată cum poate fi folosit CDB pentru a specifica SECURITY=SAME pentru sistemul din DALLAS, impunând totodată SECURITY=PGM pentru toți ceilalți solicitanți.

```

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', ' ');

```

Figura 7. Stabilirea valorilor implicite pentru conexiunile solicitanților de aplicații (SNA)

- b. Puteți folosi CDB pentru a autoriza în mod individual fiecare solicitant de aplicații din rețea, configurând CDB în unul din aceste moduri:
  - Nu înregistrați o linie implicită în SYSIBM.LUNAMES. Când linia implicită (linia ce conține un nume LU gol) nu este prezentă, gazda DB2 UDB solicită o linie în SYSIBM.LUNAMES care să conțină numele LU pentru fiecare solicitant de aplicații care încearcă să se conecteze. Dacă nu se găsește linia potrivită în CDB, se refuză accesul solicitantului de aplicații.
  - Înregistrați o linie implicită în SYSIBM.LUNAMES care să specifice că este cerută o verificare a provenienței (coloana USERNAMES setată la 'I' sau 'B'). Aceasta face gazda DB2 UDB să limiteze accesul solicitanților de aplicații și utilizatorilor finali identificați în tabela SYSIBM.USERNAMES. S-ar putea să doriți folosirea acestei metode dacă regulile dumneavoastră de traducere a numelor solicită o linie cu un nume LU neînscris în SYSIBM.LUNAMES, dar nu doriți ca DB2 pentru OS/390 și z/OS să folosească această linie pentru a permite accese neautorizate la serverul de aplicații DB2 UDB.

În Figura 8 la pagina 45, nici o linie nu conține blaturi în coloana LUNAME și deci gazda DB2 UDB refuză accesul tuturor LU, cu excepția LUDALLAS sau 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', ' ');

```

Figura 8. Identificarea Conexiunilor individuale ale solicitanților de aplicații (SNA)

**Task-uri înrudite:**

- “Definirea serverului de aplicații la subsistemul TCP/IP (OS/390 și z/OS)” la pagina 45

## Definirea serverului de aplicații la subsistemul TCP/IP (OS/390 și z/OS)

Pentru ca serverul de aplicații să primească cereri pentru baze de date distribuite prin conexiuni TCP/IP, el trebuie să fie definit la subsistemul TCP/IP local și să aibă un RDB\_NAME unic. Adicional, DB2 pentru OS/390 și z/OS Bootstrap Dataset trebuie să includă parametrii necesari și s-ar putea să fie nevoie să faceți actualizări în baza de date de comunicații a DB2 pentru OS/390 și z/OS (Communications Database) (CDB).

Nu sunt necesare actualizări CDB dacă veți folosi numai conexiuni de intrare către baze de date, deci dacă intenționați să folosiți DB2 pentru OS/390 și z/OS numai ca server, nu este nevoie să completați CDB și pot fi folosite valori implicite. Urmează un exemplu simplu despre cum se face actualizarea SYSIBM.IPNAMES.

**Procedură:**

Dacă doriți să permiteți intrari de cereri de conectare la baze de date pentru noduri TCP/IP, puteți folosi o astfel de comandă SQL pentru actualizarea acestei tabel:

```

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

```

Pentru informații despre instalarea TCP/IP la serverul de aplicații, vedeți *DB2 for OS/390 Installation Guide*.

**Task-uri înrudite:**

- “Definirea serverului de aplicații la subsistemul SNA (OS/390 și z/OS)” la pagina 43



---

## Capitolul 7. Setarea serverelor de aplicații AS/400 (SNA)

---

### Instalarea DB ca un server de aplicații folosind SNA (iSeries)

Suportul pentru serverul de aplicații de pe sistemul iSeries îi permite acestuia să acționeze ca un server pentru solicitanții de aplicații DRDA. Solicitantul de aplicații conectat la baza de date universală DB2 (UDB) pentru serverul de aplicații iSeries poate fi orice client care suportă protocoale DRDA.

Solicitantului de aplicații i se permite să acceseze tabele memorate local la serverul de aplicații DB2 UDB pentru iSeries. Solicitantul de aplicații trebuie să creeze un pachet la serverul de aplicații DB2 UDB pentru iSeries, înainte de a se putea rula orice instrucțiune SQL. Serverul de aplicații DB2 UDB pentru iSeries folosește pachetul ce conține declarațiile SQL ale aplicației în momentul rulării programului.

#### **Procedură:**

Pentru a procesa cereri către baze de date distribuite pe serverul de aplicații iSeries, trebuie să numiți baza de date a serverului de aplicații în directorul RDB. Pentru comunicații SNA trebuie să definiți sistemul pentru server de aplicații și să setați dimensiunile și sincronizările unităților de cerere și răspuns.

#### **Numirea bazei de date a serverului de aplicații:**

Numiți baza de date a serverului de aplicații (localizată la serverul de aplicații) în același mod în care identificați baza de date a solicitantului de aplicații (localizată la solicitantul de aplicații). Utilizați comanda Aduagă intrare în directorul bazei de date relaționale (ADDRDBDIRE) și specificați \*LOCAL drept locația de la distanță.

#### **Definirea serverului de aplicații către rețea:**

Pentru accesare folosind SNA, definirea serverului de aplicații către rețea este identică precum definirea solicitantului de aplicații către rețea. Trebuie să creați descriptori de linie, de controler, de dispozitiv și de mod pentru a defini atât serverul de aplicații, cât și solicitantul de aplicații care trimit cereri.

Numele programului de tranzacție folosit pentru a porni o bază de date de pe un server de aplicații iSeries este valoarea DRDA implicită X'07F6C4C2'. Acest nume al programului de tranzacție este definit în sistemul iSeries pentru a porni serverul de aplicații. Parametrul corespunzător pentru conexiuni TCP/IP, când acest protocol este suportat de DB2 UDB pentru iSeries, este portul. DB2 UDB pentru iSeries va folosi întotdeauna bine-cunoscutul port DRDA 446 ca un server.

#### **Setarea dimensiunilor RU și a sincronizării:**

Definirile rețelei trebuie revăzute pentru a determina impactul rețelei bazei de date distribuită asupra rețelei deja existente. Aceste considerații sunt aceleași pentru serverul de aplicații și pentru solicitantul de aplicații.

#### **Concepte înrudite:**

- “Considerații de securitate pentru servere de aplicații (iSeries)” la pagina 94
- “DB2 UDB pentru iSeries” la pagina 74

**Task-uri înrudite:**

- “Configurarea TCP/IP pe serverul DB2 Connect” la pagina 4
- “Instalarea DB2 ca un solicitant de aplicații – SNA (iSeries)” la pagina 29

---

## Capitolul 8. Setarea serverelor de aplicații AS/400 (TCP/IP)

---

### Conectarea la DB2 UDB folosind TCP/IP (iSeries)

Această topică furnizează un sumar al informațiilor conținute în *DB2 for AS/400 Distributed Database Programming*, care vă arată cum să setați DB2<sup>®</sup> UDB pentru iSeries:

- Ca un solicitant de aplicație DRDA<sup>®</sup> folosind comunicații TCP/IP de ieșire
- Ca un server de aplicații DRDA folosind comunicații TCP/IP de ieșire.

Principiile sunt aceleași ca și acelea descrise în Setarea lui DB2 UDB pentru iSeries<sup>™</sup> ca un solicitant de aplicație folosind SNA<sup>™</sup> și "Setarea lui DB2 UDB pentru iSeries ca un server de aplicații folosind SNA", dar pașii de configurare ai comunicării sunt mult mai simplii.

#### Note:

1. Pentru comunicațiile DRDA folosind TCP/IP numărul portului implicit pentru conexiunile bazei de date este 446.
2. Implementarea DB2 Universal Database for AS/400 Versiunii 4 Eliberarea 2 nu suportă o comitere în două faze (unități de lucru distribuite) peste comunicațiile TCP/IP.

#### Sumar al informațiilor pentru DB2 UDB pentru iSeries:

Cartea *DB2 for AS/400 Distributed Database Programming* conține următoarele secțiuni care ar trebui să le citiți și care se referă la:

- Procesarea Bazei de Date Relaționale Distribuite
- Suportul DRDA și CDRA.
- Configurarea unei Rețele de Comunicații folosind TCP/IP
- Securitatea DRDA folosind TCP/IP
- Gestiunea Managementului pentru DRDA Folosită cu TCP/IP
- Setarea Serverului TCP/IP
- Gestiunea unui Server TCP/IP
- Factori care Afectează Blocarea pentru DRDA
- Manipularea Eșecurilor de Cerere de Conexiune pentru TCP/IP
- Pornirea unui Job de Serviciu pentru un Server TCP/IP
- Accesul la Platforme-Distribuite Folosind DRDA.

Suplimentar veți mai avea nevoie de a ști:

- Numărul portului TCP/IP și informațiile de nume al gazdei pentru server și pentru solicitant.
- CCSID și informația de pagină de cod pentru server și pentru solicitant.
- ID-ul de utilizator și informațiile de parolă necesare la executarea conexiunilor pe baza de date.

#### Considerații de setare pentru serverul DB2 UDB pentru iSeries DRDA TCP/IP:

Setarea serverului TCP/IP DB2 UDB pentru iSeries DRDA asigură faptul că serverul a fost pornit. Comanda CL pentru pornirea serverului DRDA (de asemenea cunoscut și ca server DDM) este :

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

Serverul DRDA poate fi de asemenea pornit folosind comanda Pornire Server TCP/IP (Start TCP/IP Server) (STRTCPSVR) fără parametrii sau cu \*ALL specificată pentru parametrul lui SERVER. Serverul DRDA va fi în mod automat pornit la pornirea TCP/IP dacă această comandă CL a fost emisă:

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

Oricine poate verifica faptul că serverul a fost pornit prin emiterea următoarei comenzi CL:

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

Această comandă va arăta o listă derulantă de joburi. Dacă derulați în jos aproximativ o pagină ar trebui să vedeți două linii care conțin următoarele informații:

```
— QRWTLSTN  QUSER      BATCH  ACTIVE
— QRWTSRVR  QUSER      PJ      ACTIVE
```

(Ar putea exista apariții repetate ale liniei QRWTSRVR, în funcție de câte joburi pe serverul de prestart sunt active)

Prezența liniei QRWTLSTN indică faptul că jobul care ascultă pentru cererile de conexiune de tip DRDA și DDM este activ. Acest job abandonează munca pentru jobul(urile) de tip QRWTSRVR pe măsură ce cererile de conexiune sunt primite.

O altă posibilitate de verificare a faptului că serverul DRDA a fost pornit este de a emite comanda STRTCPSVR SERVER(\*DDM). A se căuta mesajele 'încă active ale serverului DDM TCP/IP'.

Numele jobului de prestart folosit pentru o conexiune particulară poate fi găsit prin emiterea unei comenzi DSPLOG precum:

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

unde timpul specificat este mai timpuriu decât cel la care conexiune a fost făcută. Aceasta va genera o listă derulantă de intrări din istoricul de loguri. A se căuta pentru o intrare precum aceasta care va conține numele jobului serverului:

```
DDM job 039554/QUSER/QRWTSRVR care face service utilizatorului SRR pe data 03/30/01 la 15:57:38.
```

Acest nume de job este folosit pentru căutarea în istoricul de joburi pentru joburi încă active. Este de asemenea folosit de a porni un job de serviciu pe joburile încă-active pentru problema determinării sau pentru a vedea mesajele optimizatorului de interogare. Un exemplu de comandă CL pentru pornirea unui job de serviciu folosind informațiile descrise mai sus ar fi:

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

Pentru a pune jobul de serviciu în modul depanare se execută comanda STRDBG:

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

În anumite situații serverul DRDA salvează istoricul de joburi ale jobului de prestart înainte de a recicla jobul și de a șterge istoricul de joburi. Aceasta se întâmplă atunci când o defecțiune serioasă a fost detectată sau atunci când jobul s-a terminat în timp ce era servit (folosind comanda STRSRVJOB).

Pentru găsirea istoricului de joburi salvat după ce jobul s-a terminat se emite următoarea comandă:

```
WRKJOB userid/QPRTJOB
```

unde ID-ul utilizatorului este numele ID-ului de utilizator de sub care conexiunea a fost efectuată (SSR în exemplul de deasupra).



Aceasta va afișa o listă de joburi dintre care unul poate fi selectat sau un meniu de opțiuni pentru un singur job. Alegeți opțiunea 4, 'Gestiunea fișierelor grupate' pentru găsirea istoricului de joburi salvat. Acesta va fi acela cu numele de fișier QPJOBLOG în cazul în care sunt mai multe fișiere grupate. Opțiunea 5 vă permite vizualizarea fișierului de istoric de joburi.

Un exemplu de tip de mesaje ale optimizatorului de interogare pe care le-ați putea vedea în istoricul de joburi atunci când jobul a fost rulat sub depanare este următorul:

```

CPI4329   Informații   00   03/30/01  16:14:57  QQQIMPLE
          QSYS          3911   QSQOPEN   QSYS      09C4
Mesaj . . . . : Accesul la secvența de ajungere a fost efectuat pentru fișierul TBL2.
Cauza . . . . : Accesul la secvența de ajungere a fost folosit pentru selectarea
înregistrărilor din membrul TBL2 al fișierului TBL2 din librăria SR. Dacă fișierul TBL2
din librăria SR este un fișier logic atunci membrul TBL2 al fișierului fizic
TBL2 din librăria SR este fișierul actual din care înregistrările
sunt selectate. Un nume de fișier *N pentru fișier indică faptul că acesta este un
fișier temporar. Restaurare . . . : Folosirea unei căi de acces poate
îmbunătăți performanța interogării dacă selectarea înregistrării este
specificată. Dacă o cale de acces nu există, s-ar putea să vreți să
creați una ale cărei câmpuri cele mai din stânga se potrivesc în selectarea
înregistrării. Potrivirea mai multor câmpuri cheie în calea de acces cu
câmpurile din selecția înregistrării va îmbunătăți
performanța. În cazul general, pentru a forța utilizarea unei căi de acces deja existente
se specifică ordinea prin câmpurile care se potrivesc cu câmpurile cheie cele mai din stânga
ale căii de acces. Pentru mai multe informații a se face referire la cartea Programarea lui
iSeries SQL.

```

Figura 9. Un exemplu de mesaj al optimizatorului de interogare

### Considerații de setare pentru clientul DB2 UDB pentru iSeries DRDA TCP/IP:

Considerațiile principale pentru folosirea lui DB2 UDB pentru iSeries ca un solicitant de aplicație DRDA (AR) peste TCP/IP este, împotriva considerațiilor de securitate discutate în următoarea secțiune, adăugarea unei intrări în directorul RDB pentru serverul de aplicații de la distanță. Aceasta se realizează într-o manieră similară cu ceea ce a fost descris în capitolul precedent asupra folosirii comunicațiilor de tip SNA. Cu toate acestea, în ciuda faptului că parametrii APPC precum numele LU de la distanță și numele programului de tranzacție, există doi parametri TCP/IP: numele gazdei de la distanță sau adresa IP și numărul portului sau numele serviciului. Cel de-al doilea element al parametrului de locație de la distanță poate fi specificat ca \*SNA (valoarea implicită) sau ca \*IP (pentru a indica faptul că conexiunea va fi efectuată folosind TCP/IP).

### Condiderații de securitate pentru folosirea lui DRDA peste TCP/IP:

DRDA peste TCP/IP nativ nu folosește serviciile de securitate ale comunicațiilor OS/400® și concepte precum dispozitive de comunicații, moduri, atribute de locații sigure și nivele de securitate a conversației care sunt asociate cu comunicațiile APPC. Prin urmare, setarea securității pentru TCP/IP este chiar diferită.

Două tipuri de mecanisme de securitate sunt suportate de către implementarea curentă a lui DB2 UDB pentru iSeries al lui DRDA peste TCP/IP:

1. Doar ID-ul utilizatorului
2. ID-ul utilizatorului cu parola

Pentru un server de aplicații DB2 UDB pentru iSeries (AS), securitatea implicită este ID de utilizator cu parolă. Pe măsură ce sistemul este instalat, cererile de conectare TCP/IP de ieșire trebuie să aibă o parolă care însoțește ID-ul utilizatorului sub care jobul serverului va fi rulat.

Comanda CHGDDMTCPA poate fi folosită pentru specificarea faptului că parola nu este necesară. Pentru efectuarea acestei schimbări, se introduce CHGDDMTCPA PWDRQD(\*NO). Trebuie să aveți autoritatea specială \*IOSYSCFG pentru folosirea acestei comenzi.

Pentru un solicitant de aplicație DB2 UDB pentru iSeries (AR), există două metode care pot fi folosite pentru trimiterea unei parole împreună cu ID-ul utilizatorului asupra cererilor de conectare TCP/IP. În absența ambelor, doar un ID de utilizator va fi trimis.

Prima metodă de trimitere a unei parole este de a folosi forma USER/USING a instrucțiunii SQL CONNECT. Sintaxa este:

```
CONNECT TO rdbname USER userid USING 'parolă'
```

unde cuvintele cu litere mici reprezintă parametrii de conectare corespunzători. Într-un program care folosește SQL încorporat, valorile ID-ului utilizatorului și ale parolei pot fi conținute în variabile gazdă.

Un alt mod prin care o parolă poate fi furnizată pentru trimiterea unei cereri de conexiune peste TCP/IP este prin folosirea unei intrări de autorizare a serverului. Asociată cu fiecare profil de utilizator de pe sistem este o listă de autorizații de pe server. Implicit lista este goală, dar cu comanda ADDSVRAUTE, intrări pot fi adăugate. Atunci când o conexiune DRDA peste TCP/IP este încercată. DB2 UDB pentru iSeries verifică lista de autorizații de pe server pentru profilul utilizatorului sub care jobul client rulează. Dacă o potrivire este găsită între numele RDB din instrucțiunea CONNECT și numele SERVER din intrarea de autorizare, parametrul USERID asociat din intrare este folosit pentru ID-ul utilizatorului de conexiune. Dacă un parametru PASSWORD este stocat în intrare, acea parolă este de asemenea trimisă în cererea de conectare.

Pentru ca o parolă să fie stcată folosind comanda ADDSVRAUTE, valoarea sistemului QRETSVRSEC trebuie să fie setată la '1'. Implicit, valoarea este '0'. Pentru efectuarea schimbării se introduce:

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

Sintaxa comenzii ADDSVRAUTE este:

```
ADDSVRAUTE USRPRF(profil-utilizator) SERVER(rdbname) USRID(userid) PASSWORD(parolă)
```

Parametrul USRPRF specifică profilul utilizatorului sub care jobul solicitantului de aplicație rulează. Parametrul SERVER specifică numele RDB de la distanță, și parametrul USRID specifică profilul utilizatorului sub care jobul serverului va rula. Parametrul PASSWORD specifică parola pentru profilul utilizatorului de pe server.

**Notă:** Este foarte important faptul că numele RDB din parametrul SERVER trebuie să fie specificat cu litere mari.

Dacă parametrul USRPRF este omis, acesta va fi setat la valoarea implicită de profil al utilizatorului sub care comanda ADDSVRAUTE este rulată. Dacă parametrul USRID este omis, acesta va lua ca valoare implicită valoarea parametrului USRPRF. Dacă parametrul PASSWORD este omis sau dacă valoarea lui QRETSVRSEC este 0, nici o parolă nu va fi stocată în intrare. Și atunci când o încercare de conexiune este efectuată folosind intrarea, mecanismul de securitate folosit va fi doar ID-ul utilizatorului.

Comanda RMVSVRAUTE poate înlătura o intrare de autorizare a serverului și comanda CHGSVRAUTE poate schimba intrarea. A se vedea *AS/400 Referințe de Comenzi* pentru descrieri complete ale acestor comenzi.

Dacă o intrare de autorizare pe server există pentru o RDB și forma USER/USING a instrucțiunii CONNECT este de asemenea folosită, ultima are precedență.

**Concepte înrudite:**

- “Reprezentarea datelor (iSeries)” la pagina 117
- “Considerații de securitate pentru servere de aplicații (iSeries)” la pagina 94
- “Considerații de securitate pentru utilizatorii aplicației (iSeries)” la pagina 109
- “DB2 UDB pentru iSeries” la pagina 74

**Task-uri înrudite:**

- “Instalarea DB ca un server de aplicații folosind SNA (iSeries)” la pagina 47
- “Instalarea DB2 ca un solicitant de aplicații – SNA (iSeries)” la pagina 29



---

## Capitolul 9. Setarea serverelor de aplicații VSE

---

### Instalarea DB2 ca un server de aplicații (VSE)

Suportul de server de aplicații în DB2 pentru VSE permite DB2 pentru VSE să acționeze ca un server pentru solicitanții de aplicații DRDA. Solicitantul de aplicații conectat la un server de aplicații DB2 pentru VSE poate fi unul din următorii:

- Un solicitant DB2 pentru VM
- Un solicitant DB2 Universal Database for z/OS and OS/390
- Un solicitant DB2
- Un solicitant DB2 UDB Database pentru iSeries
- Orice solicitant de aplicații din familia DB2, inclusiv DB2 CONNECT sau orice alt produs care suportă protocoale DRDA Application Requester protocols - se pot conecta la un server de aplicații DB2 pentru VSE.

#### Procedură:

Pentru stabilirea conexiunii rețelei la serverul de aplicații VSE:

1. Stabiliți sesiuni CICS LU 6.2 la sistemul de la distanță
2. Definiți un server de aplicații VSE
3. Pregătiți și porniți serverul de aplicații DB2 pentru VSE

#### Concepte înrudite:

- “Considerații de securitate pentru serverele de aplicație (VSE)” la pagina 100
- “DB2 pentru VSE” la pagina 84

#### Task-uri înrudite:

- “Stabilirea sesiunilor CICS LU 6.2 (VSE)” la pagina 55
- “Definirea unui server de aplicații (VSE)” la pagina 59
- “Pregătirea și pornirea serverului de aplicație DB2 (VSE)” la pagina 59

#### Referințe înrudite:

- “Listă de verificări pentru activarea unui server aplicație DB2 (VSE)” la pagina 125

---

### Task-uri de setare

#### Stabilirea sesiunilor CICS LU 6.2 (VSE)

Stabilirea sesiunilor CICS LU 6.2 este o parte a unei operații mai ample de setare a DB2 pentru VSE ca un server de aplicații. Serverul de aplicații DB2 pentru VSE comunică cu solicitantul său de aplicații prin legături CICS LU 6.2. Partițiile CICS folosite pentru acest scop trebuie să aibă legături LU 6.2 către sistemele de la distanță cu solicitanții de aplicații.

#### Procedură:

Pentru stabilirea unei sesiuni CICS LU 6.2:

1. Instalați modulele necesare pentru ISC.

Trebuie să includeți în sistemul dumneavoastră următoarele module, folosind SIT sau înlocuiri în inițializare:

- Programele de interfață EXEC (specificați EXEC=YES sau lăsați setată valoarea implicită).
- Programele de comunicație intersistem (specificați ISC=YES).
- Programul de control terminal generat de DFHSG PROGRAM=TCP. O versiune ce specifică ACCMETH=VTAM, CHNASSY=YES și VTAMDEV=LUTYPE6 este necesară.

## 2. Instalați Suportul de repornire și resincronizare CICS

Dacă Suportul de repornire și resincronizare CICS nu a fost activat la instalarea sistemului CICS, trebuie să actualizați următoarele tabele CICS pentru a activa capacitatea CICS de repornire și resincronizare :

DFHJCT	Tabela de control a jurnalului (Journal Control Table)  Un jurnal folosit de sistemul CICS trebuie definit în DFHJCT, specificând JFILEID=SYSTEM într-un macro DFHJCT TYPE=ENTRY.
DFHPCT	Tabelul de control al programului (Program Control Table)  Pentru a genera intrarea DFHPCT, în scopul utilizării capacității CICS de repornire și resincronizare, introduceți:  DFHPCT TYPE=GROUP, FN=RMI
DFHPPT	Tabela de procesare a programului  Pentru generarea intrării DFHPPT în scopul utilizării Capacității CICS de repornire și resincronizare, introduceți:  DFHPPT TYPE=GROUP, FN=RMI
DFHSIT	Tabela de inițializare a sistemului.  Macro-ul DFHSIT trebuie să includă parametrii JCT. Specificați JCT=YES sau JCT=(jj<,...>) unde jj este valoarea parametrului SUFFIX specificat în macro-ul DFHJCT TYPE=INITIAL , ce definește setul de jurnale cu date de înregistrare a sistemului CICS.

Figura 10. Tabelele de actualizat pentru activarea capacității de repornire și resincronizare

## 3. Definiți CICS către VTAM pentru VSE.

Pentru a suporta conexiuni LU 6.2, CICS trebuie definit către VTAM pentru VSE ca un nod important de aplicații VTAM. Nodul important al aplicației codat în declarația VTAM APPL este APPLID pentru partiția CICS specificată în SIT de parametrul APPLID. Este numele LU folosit de VTAM (și de aici folosit de partenerii de comunicații CICS ) pentru identificarea sistemului CICS. Vedeți Figura 11 la pagina 57.

```

          VBUILD TYPE=APPL
*****
*
*   Definiție LU pentru sistemul Toronto VSE SQL/DS
*
*****
VSEGATE  APPL  ACBNAME=VSEGATE,
           AUTH=(ACQ,SPO,VPACE),
           APPC=NO,
           SONSCIP=YES,
           ESA=30
           MODTAB=RDBMODES,
           PARSESS=YES,
           VPACING=0

```

Figura 11. Exemplu de definiție VTAM APPL pentru CICS

**AUTH=(ACQ,SPO,VPACE)**

ACQ permite lui CICS să obțină sesiuni LU 6.2.

SPO permite lui CICS să emită comanda MODIFY nume\_vtam USERVAR.

VPACE permite sincronizarea fluxurilor intersistem.

**ESA=30**

Această opțiune specifică numărul de unități adresabile de rețea cu care CICS poate stabili sesiuni. Acest număr trebuie să includă numărul total de sesiuni paralele pentru acest sistem CICS.

**PARSESS=YES**

Specifică suportul de sesiune paralelă LUTYPE6.

**SONSCIP=YES**

Specifică suportul pentru notificarea expirării sesiunii (SON). SON permite CICS, în anumite cazuri, recuperarea unei sesiuni eșuate fără a fi necesară intervenția operatorului.

**APPC=NO**

Aceasta este necesară pentru a lăsa CICS să utilizeze macro-uri VTAM. CICS nu lansează macroinstrucțiuni APPCCMD.

**Notă:** SYNCLVL=SYNCPT nu este necesar, din moment ce nu s-a specificat APPC=NO. CICS gestionează toate punctele de sincronizare SYNCPT pe nivele de activitate pentru unități de lucru distribuite.

4. Definiți legături către sistemele de la distanță folosind protocolul LU 6.2.

a. Definiți toate LU de la distanță către CICS.

Definiți toți LU de la distanță folosind comanda CEDA DEFINE CONNECTION online-ul de definire a resurselor (RDO):

- Specificați numele LU de la distanță în parametrul NETNAME parameter.
- Specificați PROTOCOL=APPC pentru a vă asigura că se folosesc protocoale LU6.2.
- Specificați AUTOCONNECT=YES și INSERVICE=YES astfel încât conexiunea, când este instalată, să fie pusă în funcțiune automat, iar sesiunile să fie obținute automat.
- Specificați nivelul de securitate al conversației folosind parametrul ATTACHSEC. ATTACHSEC=IDENTIFY este nivelul minim de securitate cerut de DRDA.
- Specificați nivelul de securitate al sesiunii folosind parametrul BINDPASSWORD. Valoarea implicită este securitate nulă la nivel de sesiune.

- b. Definiți grupuri de sesiuni LU 6.2 cu sistemul de la distanță.
- Pentru fiecare conexiune definită mai sus, definiți grupul de sesiuni paralele pentru fiecare legătură folosind comanda CEDA DEFINE SESSIONS:
- Specificați numele conexiunii (definită mai sus) în parametrul CONNECTION.
  - Specificați tabela VTAM pentru modul de logare în parametrul MODENAME.
  - Utilizați parametrul MAXIMUM pentru a specifica:
    - Numărul maxim de sesiuni
    - Numărul maxim de sesiuni care vor fi suportate drept câștigători ai concurenței.
- Specificați valorile folosite de software-ul de comunicații solicitant de aplicații DRDA.

**Notă:** Definirea unui număr mare pentru dimensiunea de trimis (SENDsize) și dimensiunea de primit(RECEIVESize) ar putea îmbunătăți rata de transmisie, totuși, va fi de asemenea necesar mai mult spațiu virtual de stocare de la un capăt la altul al rețelei. Dimensiunea de 4 kiloocteți este suportată nivelele rețelei SNA. De aceea, la configurarea serverului DRDA, setați dimensiunile buffere-lor de trimitere și recepție la 4 kiloocteți. Când conexiunile pot fi făcute cu succes de la utilizatorii de la distanță, ajustați acești parametri pentru a determina valoarea optimă.

- c. Definiți identificatorul utilizator și parola către CICS
- Definiți toți utilizatorii în tabela de înregistrare CICS (DFHSNT). Puteți testa validitatea unui identificator utilizator, realizând o logare CESN la un terminal CICS. Înregistrarea locală trebuie să se facă cu succes.
- d. Definiți modulele de încărcare (fazele) către CICS folosind comanda CEDA DEFINE PROGRAM:
- 1) ARICAXED - tranzacția AXE
  - 2) ARICDIRD - directorul DBNAME și rutina de căutare
  - 3) ARICDAXD - programul de tratare a tranzacției DAXP și DAXT
  - 4) ARICDEBD - handlerul de activare a suportului CICS TRUE
  - 5) ARICDRAD - însuși CICS TRUE
  - 6) ARICDR2 - blocul de control DR2DFLT

Pentru fiecare din acestea, trebuie specificată opțiunea LANGUAGE=ASSEMBLER.

- e. Pentru fiecare TPN specificat de solicitantul de aplicații, definiți o tranzacție AXE folosind comanda CEDA DEFINE TRANSACTION:
- Pentru specificarea TPN, folosiți parametrul TRANSACTION
  - Pentru specificarea fazei, folosiți PROGRAM=ARICAXED
  - Pentru specificarea unui al doilea nume hexazecimal al tranzacției, folosiți parametrul XTRANID.
- În acest timp, definiți de asemenea tranzacțiile DAXP și DAXT , specificând PROGRAM=ARICDAXD.

*CICS on Open Systems: Intercommunication Guide* conține detalii despre definirea și stabilirea de legături CICS LU 6.2 cu sisteme de la distanță.

#### **Task-uri înrudite:**

- “Definirea unui server de aplicații (VSE)” la pagina 59



## Definirea unui server de aplicații (VSE)

Definirea unui server de aplicații VSE este o parte a unei operații mai ample de instalare a DB2 pentru VSE ca un server de aplicații.

### Procedură:

Pentru definirea unui server de aplicații VSE:

1. Actualizați directorul DBNAME al DB2 pentru VSE.

Adăugați o intrare în directorul DBNAME pentru fiecare tranzacție definită mai sus folosind comanda CEDA DEFINE TRANSACTION. Cu sesiunea LU 6.2 stabilită, un solicitant de aplicații de la distanță poate porni o conversație cu serverul de aplicații DB2 pentru VSE. Face acest lucru alocând o conversație LU 6.2 cu serverul de aplicații, specificând un TPN (numele programului de tranzacție). Acest TPN trebuie să fie identificatorul tranzacției CICS ce indică tranzacția AXE responsabilă de rutarea cererilor sau de la serverul DB2 pentru VSE. Acest TPN trebuie să fie în directorul DBNAME al DB2 pentru VSE mapat la serverul DB2 pentru VSE astfel încât să fie accesat de solicitantul de aplicații. Administratorul bazei de date DB2 pentru VSE este responsabil de actualizarea directorului DBNAME, precum și de informarea utilizatorilor de la distanță asupra mapării TPN-către-server.

Atât TPN, cât și numele serverului corespunzător (numele bazei de date - așa cum e definit în directorul DBNAME), trebuie să fie identificați către solicitantul de aplicații:

- Solicitantul de aplicații folosește TPN pentru inițierea tranzacției router AXE.
  - Solicitantul de aplicații vede numele serverului din fluxul inițial DRDA drept numele bazei de date destinație. Serverul DB2 pentru VSE folosește acest nume de server pentru a verifica dacă solicitantul de aplicații accesează serverul corect. O nepotrivire în numele serverului refuză accesul solicitantului de aplicații la server, iar solicitantul de aplicații termină conversația.
2. Folosiți procedura ARISBDID pentru a construi și asambla directorul DBNAME (membru ARISDIRD.A).

Pentru mai multe informații, vedeți *DB2 Server for VSE System Administration* și *DB2 Server for VSE & VM Database Administration*.

### Task-uri înrudite:

- “Stabilirea sesiunilor CICS LU 6.2 (VSE)” la pagina 55
- “Pregătirea și pornirea serverului de aplicație DB2 (VSE)” la pagina 59

## Pregătirea și pornirea serverului de aplicație DB2 (VSE)

Pregătirea și pornirea serverului de aplicație DB2 pentru VSE este o parte a taskului mai mare de setare a lui DB2 pentru VSE ca un server de aplicație.

### Procedură:

Pentru pregătirea și pornirea serverului de aplicație DB2 pentru VSE

1. Tranzacția AXE menține un istoric de erori care este o coadă de stocare temporară CICS numită ARIAXELG. Acest istoric de erori conține mesaje de eroare înregistrând probleme de comunicare și terminări anormale ale sesiunilor DRDA. Se definește acest istoric ca “recuperabil” folosind CICS TST.
2. Se rulează procedura ARIS342D pentru a instala suportul pentru serverul de aplicație DRDA.

3. Dacă este necesar se emite tranzacția DAXP pentru specificarea parolei și a limbajului implicite care vor fi folosite atunci când suportul CICS TRUE este activat pentru un server specific. A se vedea manualul *DB2 Server for VSE & VM Operation* pentru mai multe detalii.
4. Se pornește DB2 pentru VSE cu parametrii DBNAME, RMTUSERS și SYNCNT:
  - DBNAME folosit trebuie să fie definit în directorul DBNAME.
  - Parametrul RMTUSERS trebuie să nu fie zero.
  - Se specifică SYNCNT=Y pentru a activa suportul pentru unitatea de lucru distribuită.
5. Toți utilizatorii de la distanță trebuie să fie autorizați de către serverul DB2 pentru VSE cu diferite nivele de autorizare.

#### **Determinarea problemei:**

- Dacă solicitantul de aplicație a reușit în găsirea partenerilor săi CICS cu un TPN valid (TPN definit în directorul DBNAME) atunci o tranzacție AXE este pornită. Contorul de folosire asupra programului ARICAXED este incrementat cu unu (verificat prin emiterea lui CEMT I PR(ARICAXED) ).
- Pentru asigurarea faptului că un ID de utilizator de la distanță este stabilit în tabela de semnare CICS se execută o semnare locală folosind tranzacția CESN cu ID-ul de utilizator al utilizatorului de la distanță și parola. Semnarea locală trebuie să aibă succes.
- Atunci când serverul DB2 pentru VSE rulează și o aplicație execută pentru prima dată activitate a unității de lucru distribuită DRDA-2, suportul TRUE asupra unui server va fi activat în mod automat. A se observa mesajul ARI0187I, care indică faptul că suportul TRUE a fost activat cu succes. Cu toate acestea dacă mesajul ARI0190E apare, ceea ce indică faptul că o eroare a apărut în timpul activării lui TRUE a se observa mesajele de eroare de dinainte de la consolă.
- Dacă programul aplicație DRDA propriu primește cod viabil X'08063426' sau X'FFFE0101', aceasta ar putea fi un semn că CICS rulează în afara sesiunii. CICS poate rămâne fără sesiuni dacă toate sesiunile sunt fie în folosire, fie programate spre a fi de ieșire, dar UNBIND nu a fost încă completată. CICS poate rămâne fără sesiuni dacă există multe tranzacții de intrare concurente care sunt de durată scurtă. În acest caz creșterea numărului de sesiuni specificate în parametrul CEDA DEFINE SESSIONS MAXIMUM pentru numărarea sesiunilor care sunt programate spre a fi UNBINDed, dar UNBIND nu a fost încă completată.

#### **Task-uri înrudite:**

- “Stabilirea sesiunilor CICS LU 6.2 (VSE)” la pagina 55
- “Definirea unui server de aplicații (VSE)” la pagina 59

---

## Capitolul 10. Setarea serverelor de aplicații VM

---

### Instalarea DB2 ca un server de aplicații (VM)

Suportul de server de aplicații în DB2 pentru VM permite DB2 pentru VM să acționeze ca un server pentru solicitanții de aplicații DRDA. Solicitantul de aplicații conectat la un server de aplicații DB2 pentru VM poate fi unul din următorii:

- Un solicitant DB2 pentru VM
- Un solicitant DB2 Universal Database for z/OS and OS/390
- Un solicitant DB2 Universal Database pentru iSeries
- Un solicitant DB2 for AIX
- Orice solicitant de aplicații din familia DB2, inclusiv DB2 CONNECT sau orice alt produs care suportă protocoale DRDA Application Requester protocols - se pot conecta la un server de aplicații DB2 pentru VM.

Pentru orice solicitant de aplicații conectat la un server de aplicații DB2 pentru VM, serverul de aplicații DB2 pentru VM permite solicitantului de aplicații să acceseze obiecte de tip bază de date (cum ar fi tabele) memorate local la serverul de aplicații DB2 pentru VM. Solicitantul de aplicații trebuie să creeze un pachet ce va conține declarațiile SQL ale aplicațiilor la serverul de aplicații DB2 pentru VM înainte de a se putea stabili conexiunea.

#### Procedură:

Pentru procesarea cererilor de baze de date distribuite de la serverul de aplicații DB2 pentru VM:

1. Definiți serverul de aplicații
2. Pregătiți solicitantul de aplicații DB2 pentru VM sau serverul de aplicații

#### Concepte înrudite:

- “Cosiderații de securitate pentru serverele de aplicații (VM)” la pagina 97
- “DB2 pentru VM” la pagina 74
- “Reprezentarea datelor (VM)” la pagina 120

#### Task-uri înrudite:

- “Definirea serverului de aplicații (VM)” la pagina 61
- “Pregătirea solicitantului de aplicație sau a serverului de aplicație pentru comunicațiile DRDA (VM)” la pagina 38
- “Setarea pentru DB2 ca un solicitant de aplicație (VM)” la pagina 35

---

### Task-uri de setare

#### Definirea serverului de aplicații (VM)

Definirea serverului de aplicații este o parte a unei operații mai ample de instalare a DB2 pentru VM ca un server de aplicații. Pentru ca serverul de aplicații să primească cereri de la baze de date distribuite, definiți serverul de aplicații la subsistemul local de comunicații și alocați-i un nume RDB\_unic. Numele RDB\_ este furnizat de SQLSTART EXEC ca parametru al DBNAME.

## Procedură:

Pentru definirea serverului de aplicații:

1. Definiți serverul de aplicații DB2 pentru VM în rețeaua SNA după ce selectați numele de gateway și RDB\_NAME pentru serverul de aplicații DB2 pentru VM. Numele RDB\_NAME pe care îl alegeți pentru DB2 pentru VM trebuie să fie livrat tuturor utilizatorilor (solicitanții de aplicații) care ar putea solicita conectarea la serverul de aplicații DB2 pentru VM.

Identificatorul de rețea (NETID) este definit în VTAM ca un parametru de inițializare și toate cererile distribuite de la solicitanții de aplicații sunt rutate corect către el. Serverul de aplicații DB2 pentru VM nu setează identificatorul de rețea (NETID).

Serverul de aplicații DB2 pentru VM nu determină care gateway trebuie folosit pentru rutarea cererilor distribuite sosite de la solicitantul de aplicații. Întotdeauna, acest lucru este controlat de solicitantul de aplicații. În cazul unui solicitant de aplicații DB2 pentru VM, CMS Communications Directory îi specifică utilizarea :luname și :etichete tpn

Pentru ca serverul de aplicații DB2 pentru VM să suporte unități distribuite de activități productive, solicitantul de aplicații trebuie să selecteze un gateway AVS gateway care a fost definit către VTAM folosind parametrul SYNCLVL=SYNCPT. Asigurați-vă că gateway-ul AVS a fost definit pentru a suporta unități de lucru distribuite.

2. Creați un server de recuperare CRR, utilizat pentru gestionarea unităților de lucru distribuite pentru serverul de aplicații DB2 pentru VM pe acest sistem VM. Pentru a face aceasta, parcurgeți pașii de post-instalare - pentru încărcarea grupurilor de fișiere și a serverelor furnizate de IBM. Aceasta include definirea unui server CRR (VMSERVER) și a unui grup de fișiere CRR (VMSYSR). Asigurați-vă că la pornirea serverului de recuperare CRR, este specificat un nume LUNAME, egal cu numele unui gateway AVS pentru care s-a specificat SYNCLVL=SYNCPT.
3. Asigurați-vă că directorul CP pentru mașina - server de aplicații are o declarație IUCV \*IDENT. Aceasta identifică serverul ca o resursă globală.
4. Creați o intrare în tabelul cu nume de moduri VTAM pentru fiecare nume de mod pe care îl cere un solicitant de aplicații. Aceste intrări descriu caracteristicile sesiunii, cum ar fi dimensiuneaRU, numărul de pași și clasa de servicii pentru un anumit nume de mod.
5. Definiți limitele sesiunii pentru solicitanții de aplicații care se conectează la serverul de aplicații DB2 pentru VM. Declarația APPL din VTAM definește limite de sesiune implicite pentru toate sistemele partenere. Pentru a stabili valori implicite unice pentru un anumit partener, folosiți comanda AGW CNOS de pe mașina virtuală AVS ce rulează pe site-ul serverului de aplicații. (De obicei, limitele sesiunii sunt cerute de solicitantul de aplicații.)

După alegerea dimensiunilor RU, a limitelor sesiunii și a numărului de pași, considerați impactul pe care îl au aceste valori pe grupul (pool) VTAM IOBUF pool.

## Maparea numelui serverului la o RESID:

Un identificator de resursă (resource ID) (RESID) este termenul folosit de VM pentru numele unui program de tranzacție. În mediul VM, este de obicei definit ca un nume alfanumeric cu o lungime de până la 8 octeți. În mod normal, definiți un identificator de resursă (RESID) identic cu numele serverului, pentru a menține administrarea facilă. Figura 12 la pagina 63 arată un exemplu de fișier cu nume RESID.

Vedeți "Exemplu de intrare director de comunicații fără parolă" în *Considerații de securitate pentru solicitanții de aplicații (VM)* - subiectul despre intrările din directorul de comunicații care definește acest nume\_bază\_de\_date și identificatorul de resursă (RESID) (ca TPN). Dacă numele serverului de aplicații nu poate fi același ca identificatorul de resursă (RESID), atunci

serverul de aplicații DB2 pentru VM utilizează un fișier NUME IDENTIFICATORI RESURSE (NAMES RESID) pentru a furniza maparea.

```
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
```

Figura 12. Exemplu de fișier cu nume de identificatori de resurse

Această mapare este necesară dacă:

- Folosiți un identificator de resursă (RESID) diferit de numele serverului
- Folosiți un nume de server mai lung de 8 octeți
- Folosiți un identificator de resursă (RESID) cu o valoare hexazecimală pe 4 octeți, cum ar fi valoarea implicită DRDA TPN X'07F6C4C2'

În timpul instalării, în mod implicit se utilizează numele serverului specificat pe SQLDBINS EXEC ca identificator de resursă (RESID). Pentru a crea o intrare de mapare în fișierul RESID NAMES, specificați parametrul RESDI pe SQLDBINS.

Când porniți baza de date folosind SQLSTART DB(server\_num),DB2 pentru VM caută identificatorul de resursă (RESID) corespunzător și înfrmează VM că aceasta este resursa pe care VM o are de controlat. Dacă nu se găsește o intrare în fișierul RESID NAMES, DB2 pentru VM presupune că identificatorul de resursă (RESID) este chiar numele serverului și anunță acest lucru către VM.

Pentru informații suplimentare despre pașii post-instalării serverelor livrate de IBM și pool-uri de fișiere, vedeți *VM/ESA Installation Guide*.

Pentru informații suplimentare despre "Utilizarea mediului DRDA", vedeți cartea *DB2 Server for VM System Administration*.

#### Concepte înrudite:

- "Cosiderații de securitate pentru serverele de aplicații (VM)" la pagina 97
- "Reprezentarea datelor (VM)" la pagina 120



---

## Partea 4. Concepte gazdă și iSeries





---

## Capitolul 11. Concepte

---

### DB2 pentru OS/390 și z/OS

Bazele de date universale DB2 (UDB)<sup>®</sup> pentru OS/390<sup>®</sup> și z/OS<sup>™</sup> sunt reprezentate de sistemul de management de baze de date relaționale IBM<sup>®</sup> pentru DB2 pentru OS/390 și de sistemele z/OS. Figura 13 la pagina 68 apată un sistem OS/390 sau un sistem z/OS rulând o singură copie de DB2 UDB pentru OS/390 și z/OS. Este posibil să se ruleze copii multiple pentru DB2 UDB pentru OS/390 și pentru z/OS pe un singur sistem. Pentru a identifica copiii de DB2 pentru OS/390 și pentru z/OS în cadrul unui sistem dat (sau copii de DB2 pentru OS/390 și pentru z/OS dintr-un complex JES), fiecărui sistem DB2 îi este dat un nume de subsistem, un șir unic de 1 până la 4 caractere în cadrul complexului JES.

#### Apelanții de aplicație:

Solicitantul de aplicație conectat la un server de aplicații DB2 pentru OS/390 sau z/OS poate fi:

- Un solicitant DB2 pentru OS/390 sau pentru z/OS
- DB2 Connect
- O bază de date universală DB2<sup>™</sup> Versiunea server pentru companii cu suport de conectare DB2<sup>™</sup> activat.
- Un solicitant Versiunea 2DB2 care poate rula pe AIX, HP-UX, OS/2, Solaris, Windows<sup>®</sup> 3.1, Windows 3.11 for Workgroups, Windows 95 sau pe Windows NT, ca și pe Macintosh, SCO, SGI sau SINIX. Serviciile de conexiune baze de date distribuite<sup>®</sup> (DDCS) Versiunea gateway multi-utilizator 2.3, Versiunea single-utilizat or 2.3 și Versiunea DDCS 2.4 pentru Windows furnizează această funcție.
- Un solicitant DB2 UDB pentru iSeries<sup>™</sup>
- Un solicitant DB2 for VM
- Orice produs care suportă DRDA protocoalele de apelare de aplicație

#### Serverele de aplicație:

Serverele de aplicație DB2 pentru OS/390 și pentru z/OS suportă acces de bază de date după cum urmează:

- Solicitantul de aplicație este permis să acceseze tabele memorate la serverul de aplicație DB2 pentru OS/390 și pentru z/OS. Solicitantul de aplicație trebuie să creeze un pachet la serverul de aplicație DB2 pentru OS/390 și z/OS înainte ca aplicație să poată să fie rulată. Serverul de aplicație DB2 pentru OS/390 și z/OS utilizează pachetul pentru a localiza, la momentul execuției, instrucțiunile SQL ale aplicației.
- Solicitantul de aplicație poate informa serverul de aplicație DB2 pentru OS/390 și z/OS că accesul trebuie să fie restricționat la activitățile numai citire în cazul în care DRDA conexiunea la serverul solicitant nu suportă procesul de comitere în două faze. De exemplu, un solicitant DDCS V2R3 cu un început CICS<sup>®</sup> ar informa aplicația DB2 Universal Database for z/OS and OS/390 că actualizările nu sunt permise.
- De asemenea, solicitantul de aplicație poate fi permis să acceseze tabelele memorate la alte sisteme DB2 pentru OS/390 și z/OS din rețea utilizând accesul directat-sistem. Accesul directat-sistem permite solicitantului de aplicație să realizeze conexiuni la sisteme de baze de date multiple într-o singură unitate de lucru.

#### Spețiile de adrese OS/390 și z/OS:

În Figura 13, numele de subsistem pentru DB2 pentru OS/390 și pentru z/OS este xxxx. Trei dintre numele de spațiu de adresă pentru OS/390 și z/OS sunt prefixate de numele de subsistem DB2 pentru OS/390 și z/OS. Aceste trei spații de adresă compune produsul DB2 pentru OS/390 și z/OS.

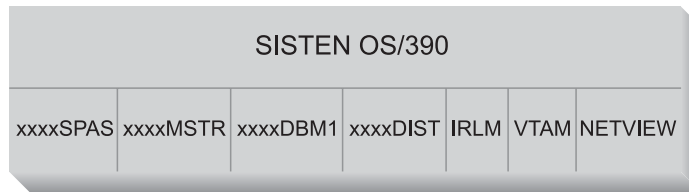


Figura 13. Spațiile de adresă OS/390 și z/OS folosite de DB2 pentru OS/390 și z/OS

Figura 13 arată spațiile de adresare OS/390 și z/OS implicate în procesare bazelor de date distribuite cu DB2 pentru OS/390 și z/OS. Aceste spații de adresare lucrează împreună pentru a permite utilizatorilor de DB2 pentru OS/390 și z/OS să acceseze baze de date relaționale locale și să comunice cu sistemele iSeries sau gazdă de la distanță. Scopul fiecărui spațiu de adresare este după cum urmează:

**xxxxSPAS**

Spațiu de adresare proceduri de memorare DB2.

**xxxxMSTR**

Spațiul de adresare servicii de sistem pentru produsul DB2 pentru OS/390 și z/OS este responsabil de deschiderea și închiderea DB2 pentru OS/390 și z/OS și controlează accesul local la DB2 pentru OS/390 și z/OS.

**xxxxDBM1**

Spațiul de adresare servicii bază de date este responsabil de accesarea bazelor de date relaționale controlate de DB2 pentru OS/390 și z/OS. Acesta este locul unde ieșirea și intrarea la resursele de bază de date sunt realizate în numele programelor de aplicație SQL.

**xxxxDIST**

Porțiunea din DB2 pentru OS/390 și z/OS care furnizează capacități de daze de date distribuite; de asemenea cunoscută ca *Facilitate de date distribuite* (DDF). Atunci când este primită o cerere la o bază de date distribuită, DDF trimite cererea la xxxxDBM1, astfel încât operațiile de I/O de bază de date apelată pot să fie realizate.

**IRLM** Managerul de glocare folosit de DB2 pentru OS/390 și de z/OS pentru a controla accesul la resursele bazei de date.

**VTAM®**

Serverul de comunicații IBM pentru funcțiile pentru OS/390 și pentru z/OS SNA(VTAM). DDF poate utiliza SNA sau TCP/IP pentru a realiza comunicații de baze de date distribuită în numele DB2 pentru OS/390 și z/OS. În această diagramă nu este arătat nici un spațiu de adresare pentru TCP/IP.

**NETVIEW**

Produsul punctul central de management al rețelei de pe sistemele OS/390 și z/OS. Atunci când apar erori în timpul procesării bazei de date distribuită, informațiile de eroare înregistrări DDF (de asemenea cunoscute ca alarme) din baza de date monitor hardware NetView®. Administratorii de sistem pot folosi NetView pentru a examina erorile memorate în baza de date monitor hardware sau furnizează proceduri de comandă automate pentru a fi invocate atunci când condițiile de alarmă sunt înregistrate.

NetView poate de asemenea să fie folosit pentru a diagnostica erorile de comunicație VTAM.

### Facilitățile de atașare OS/390 și z/OS:

Figura 13 la pagina 68 nu prezintă nici un program de aplicație SQL. Atunci când un program de aplicație folosește DB2 pentru a emite instrucțiuni SQL, programul de aplicație trebuie să se atașeze la produsul DB2 pentru OS/390 și z/OS în unul din următoarele moduri:

**TSO** Job-urile batch și utilizatorii finali legați la TSO sunt conectați la DB2 UDB pentru OS/390 și z/OS prin facilitățile de atașare TSO. Aceasta este tehnica utilizată pentru a conecta SPUFI și multe aplicații QMF™ la DB2 pentru OS/390 și z/OS.

#### CICS/ESA®

Atunci când o aplicație CICS/ESA emite apeluri SQL, produsul CICS/ESA utilizează interfața de atașare CICS pentru a ruta cereri SQL la DB2 pentru OS/390 și z/OS.

#### IMS/ESA®

Tranzacțiile ce rulează sub controlul IMS/ESA utilizează interfața de atașare IMS™ pentru a transmite instrucțiuni SQL la DB2 pentru OS/390 și z/OS pentru procesare.

**DDF** Facilitatea de date distribuite este responsabilă pentru conectarea aplicațiilor distribuite la DB2 pentru OS/390 și z/OS.

**CAF** Apelarea facilității de atașare permite subsistemelor care pot fi scrise de utilizator să se conecteze direct la DB2 pentru OS/390 și z/OS.

### Conexiunile bază de date distribuită:

DRDA® definește tipuri de funcții de sistem management de bază de date distribuită. DB2 pentru OS/390 și z/OS suportă unitate de lucru de la distanță. Cu unitate de lucru de la distanță, un program de aplicație care se execută în unul din sisteme poate accesa date la o DBMS de la distanță utilizând SQL furnizat de acel DBMS de la distanță.

DB2 pentru OS/390 și z/OS suportă de asemenea unități de lucru distribuite. Cu unitate de lucru distribuită, un program de aplicație care se execută într-un sistem, poate accesa date la DBMS-uri de la distanță folosind SQL furnizat de DBMS-uri de la distanță.

Așa cum se arată în Figura 14 la pagina 70, DB2 pentru OS/390 și z/OS suportă trei configurații de conexiuni de bază de date distribuită utilizând două metode de acces:

**[1] Acces sistem-directat** (de asemenea cunoscut ca utilizând *protocolul privat DB2 pentru OS/390 și z/OS*) permite un solicitant DB2 pentru OS/390 și z/OS să se conecteze la unul sau la mai multe servere DB2 pentru OS/390 și z/OS. Conexiunea realizată între solicitantul DB2 pentru OS/390 și z/OS și server nu aderă la protocoalele definite în DRDA și nu poate fi folosită pentru a conecta produsele non-DB2 pentru OS/390 și z/OS la DB2 pentru OS/390 și z/OS. Acest tip de conexiune este realizată prin codarea nume de trei-părți sau aliasuri în aplicație.

**[2] Accesul directat-aplicație** permite un solicitant DB2 pentru OS/390 și z/OS sau un solicitant non-DB2 pentru OS/390 și z/OS cum ar fi DB2 Connect pentru a se conecta la unul sau mai multe servere de aplicație DB2 pentru OS/390 și z/OS sau non-DB2 pentru OS/390 și z/OS cum ar fi Baza de date universală DB2 și DB2 UDB pentru iSeries folosind protocoalele DRDA. Numărul de servere de aplicație care pot fi conectate la solicitantul de aplicație la un moment de timp depinde de nivelul pentru DB2 pentru OS/390 și z/OS al solicitantului de aplicație. Acest tip de conexiune este realizată prin codarea instrucțiunilor SQL CONNECT din aplicație.

**[3] Accesese directate-aplicație și cele directate-sistem** pot fi folosite împreună pentru a realiza conexiunile. Utilizatorul nu se poate conecta utilizând DRDA și memorarea directată-sistem în același fir de execuție.

Termenul *server secundar* descrie sisteme care acționează ca servere la serverul de aplicație.

Dacă toate sistemele dintr-o configurație suportă comitere fază-dublă, atunci unitatea de lucru distribuită este suportată. (citire din mai multe locuri și actualizare în mai multe locuri). În cazul în care nu toate sistemele suportă comitere fază dublă, actualizările din cadrul unei unități de lucru sunt sau restricționate la un singur loc care nu suportă comitere fază dublă sau subșetel la subșeturi de locuri care suportă comitere fază dublă.

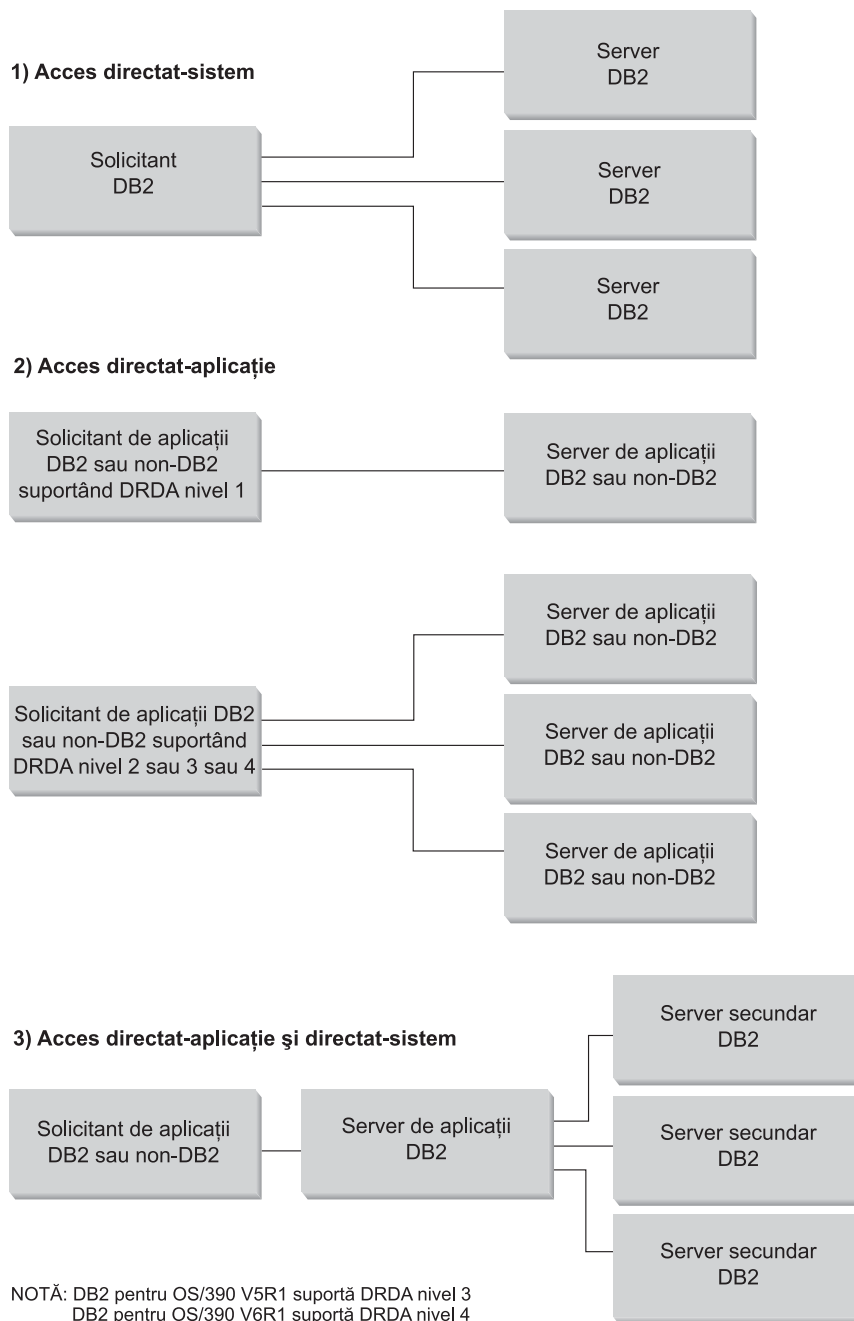


Figura 14. Conexiunile distribuite DB2 pentru OS/390 și z/OS

Tabela 2 la pagina 71 compară tipurile de conexiune de bază de date distribuită DB2 pentru OS/390 și z/OS.

Tabela 2. Comparație de Conexiuni distribuite DB2 pentru OS/390 și z/OS

[1] Acces directat-sistem	[2] Acces directat-aplicație (cu toate sistemele având comitere fază dublă)	[3] Accese directate-sistem și directate aplicație
Toți partenerii trebuie să fie sisteme DB2 pentru OS/390 și z/OS	Poate interconecta oricare două DRDA sisteme	Solicitantul de aplicație poate fi orice sistem DRDA; serverele trebuie să fie sisteme DB2 pentru OS/390 și z/OS
Se poate conecta în mod direct la mulți parteneri	Se poate conecta în mod direct la mulți parteneri	Solicitantul de aplicație se conectează direct la serverele de aplicație; serverele de aplicație se pot conecta la mai multe servere secundare DB2 pentru OS/390 și z/OS
Orice aplicație SQL poate avea conversații multiple cu fiecare server	Fiecare aplicație SQL are o conversație cu fiecare server	Aplicația SQL are o conversație cu fiecare server; serverul de aplicație DB2 pentru OS/390 și z/OS poate realiza multe conversații la fiecare server pentru aplicație
Poate accesa amândouă resursele, de la distanță și locale într-un scop comitere	Poate accesa amândouă resursele, locale și de la distanță, într-un singur scop comitere	Solicitantul de aplicație și serverul de aplicație pot accesa date locale și de la distanță
Interogări mai eficiente la interogările mari și interogări concurente multiple	Mai eficient la instrucțiunile SQL care sunt executate de puține ori într-un scop de comitere	Conexiunea solicitant aplicație - server aplicație se comportă ca [2]; conexiunile server secundar se comportă ca [1]
Poate suporta SQL static sau dinamic, dar serverul leagă dinamic SQL static prima dată când se execută într-un scop comitere	Poate emite SQL static sau dinamic	Solicitantul de aplicație și serverul de aplicație poate emite SQL static sau dinamic; serverele secundare suportă SQL static sau dinamic, dar leagă dinamic SQL static prima dată când este executat într-un scop comitere
Limitat la instrucțiunile SQL INSERT, DELETE și UPDATE și la instrucțiunile care suportă SELECT	Poate folosi orice instrucțiune suportată de sistemul care execută instrucțiunea	Serverele de aplicație suportă orice SQL; serverele secundare suportă numai DML SQL (de exemplu, CREATE sau ALTER)

### Intensificări de securitate suplimentare:

#### Coduri de securitate extinse

Până la Versiunea 5.1 DB2 UDB pentru OS/390, cererile de conectare care furnizează ID-uri utilizator sau parole puteau eșua cu codul motiv 0 SQL30082, dar cu nici o altă indicație despre ce ar putea fi greșit. DB2 UDB pentru OS/390 Versiunea 5.1 a introdus o intensificare care furnizează suport pentru codurile de securitate extinse. Specificarea securității extinse va furniza diagnosticări suplimentare, cum ar fi (PAROLĂ EXPIRATĂ) suplimentar la codul motiv.

Pentru a exploata acest lucru, parametrul de instalare pentru securitate extinsă DB2 Universal Database for z/OS and OS/390 ZPARM ar trebui setat la valoarea YES. Se utilizează panoul de instalare DB2 Universal Database for z/OS and OS/390 DSN6SYSP pentru a seta EXTSEC=YES. De asemenea puteți folosi panoul DDF 1 (DSNTIPR) pentru a seta acest parametru. Valoarea implicită este EXTSEC=NO. În cazul unei parole expirate, Windows, UNIX și aplicațiile web care utilizează DB2 Connect vor primi mesajul de eroare SQL01404.

#### Securitatea TCP/IP deja verificată

Dacă se dorește furnizarea de suport pentru opțiunea de securitate DB2 Universal Database AUTHENTICATION=CLIENT, atunci se utilizează panoul de instalare DB2 Universal Database for z/OS and OS/390 DSNTIP4 (panoul DDF 2) pentru a seta securitatea deja verificată TCP/IP la YES.

#### Desktop ODBC și Java™ securitate de aplicație

Aplicațiile stație de lucru ODBC și Java utilizează SQL dinamic. Acest lucru poate

crea motive de îngrijorare asupra securității în unele instalări. DB2 Universal Database for z/OS and OS/390 introduce o nouă opțiune de legare DYNAMICRULES(BIND) care permite execuția lui SQL dinamic sub autorizarea ori a deținătorului, ori a celui care a legat.

DB2 Universal Database și DB2 Connect furnizează un nou parametru de configurare CLI/ODBC CURRENTPACKAGESET în fișierul de configurare DB2CLI.INI. Acesta ar trebui setat la un nume de schemă care ar trebui să aibă privilegiile corespunzătoare. O instrucțiune SQL schemă SET CURRENT PACKAGESET va fi emisă automat după fiecare conectare pentru aplicație.

Se folosește Managerul ODBC pentru a actualiza DB2CLI.INI.

### **Support pentru schimbarea parolei**

Dacă o instrucțiune SQL CONNECT returnează un mesaj indicând că parola ID-ului utilizatorului a expirat, cu DB2 Connect este posibil să se modifice parola fără a semna la TSO. Prin DRDA, DB2 Universal Database for z/OS and OS/390 se poate modifica parola pentru utilizator.

Vechia parolă împreună cu noua parolă și parola de verificare trebuie furnizate de utilizator. Dacă securitatea specificată la serverul DB2 Connect Enterprise Edition este DCS, atunci o cerere de modificare a parolei este setată la serverul de bază de date DB2 Universal Database for z/OS and OS/390. Dacă securitatea specificată este SERVER atunci parola de pe serverul Conectare DB2 este modificată.

Un beneficiu suplimentar este că o definiție LU separată nu este cerută.

### **Concepte înrudite:**

- “Reprezentarea datelor (OS/390 și z/OS)” la pagina 117
- “Considerații de securitate pentru solicitantii de aplicații (OS/390 și z/OS)” la pagina 103
- “Considerații de securitate pentru serverele de aplicații (OS/390 și z/OS)” la pagina 89

### **Task-uri înrudite:**

- “Instalarea DB2 ca un server de aplicații (OS/390 și z/OS)” la pagina 43
- “Instalarea DB2 ca un solicitant de aplicații (OS/390 și z/OS)” la pagina 23
- “Setarea mărimilor RU și a pasului (OS/390 și z/OS)” la pagina 73

---

## **Subconcepte**

### **Definirea comunicațiilor - SNA (OS/390 și z/OS)**

VTAM este Communications Manager pentru sisteme OS/390 și z/OS. VTAM acceptă comenzi LU 6.2 de la DB2 pentru OS/390 și z/OS și convertește aceste comenzi în fluxuri de date LU 6.2 pe care la puteți transmite în cadrul rețelei.

#### **Procedură:**

Pentru ca VTAM să comunice cu aplicațiile partenere definite în CDB alDB2 pentru OS/390 și z/OS, trebuie să furnizați către VTAM următoarele informații:

- Numele LU pentru fiecare server.

Când DB2 pentru OS/390 și z/OS comunică cu VTAM, DB2 are permisiunea de a transmite către VTAM numai un nume LU (nu NETID.LUNAME) pentru identificarea destinației dorite. Acest nume LU trebuie să fie unic în cadrul numelor LU cunoscute de sistemul VTAM local, pentru a permite VTAM să determine atât NETID, cât și numele LU din valoarea numelui LU transmisă de DB2 pentru OS/390 și z/OS. Când numele LU sunt

unice în cadrul întregii rețele SNA a unei întreprinderi, se simplifică foarte mult procesul de definire a resurselor VTAM. Totuși, se poate ca acest lucru să nu fie întotdeauna posibil. Dacă numele LU din rețelele dumneavoastră SNA nu sunt unice, trebuie să folosiți translatarea numelor LU a VTAM pentru a construi combinația corectă NETID.LUNAME pentru un nume LU care nu este unic. Acest proces este descris în "Translatarea numelor resurselor" ("Resource Name Translation") din *VTAM Network Implementation Guide*.

Amplasarea și sintaxa definițiilor VTAM folosite pentru definirea de nume LU de la distanță sunt puternic dependente de modul în care sistemul de la distanță este conectat din punct de vedere logic și fizic la sistemul VTAM local.

- Dimensiunea RU, dimensiunea ferestrei de sincronizare și clasa de servicii pentru fiecare nume de mod. Creați câte o intrare în tabela de moduri a VTAM pentru fiecare nume de mod specificat în CDB. De asemenea, trebuie să definiți IBMRDB și IBMDB2LM.
- Profilele VTAM și RACF pentru algoritmul de verificare LU, dacă intenționați să folosiți verificarea LU a partenerului.

**Concepte înrudite:**

- "DB2 pentru OS/390 și z/OS" la pagina 67

## Setarea mărimilor RU și a pasului (OS/390 și z/OS)

Intrările din modul de tabelă VTAM pe care le-ați definit specifică mărimile RU și numărul de pas. Eșuarea în a defini aceste valori în mod corect poate avea un impact negativ asupra tuturor aplicațiilor VTAM.

**Procedură:**

După alegerea mărimilor RU, a limitelor sesiunilor și a numerelor de pas este extrem de important să se considere impactul pe care aceste valori îl pot avea asupra rețelelor VTAM deja existente. Ar trebui să revedeți următoarele articole atunci când instalați un nou sistem de bază de date distribuită:

- Pentru conexiunile VTAM se verifică dacă parametrul MAXBFRU este destul de mare astfel încât acesta să poată trata mărimea RU proprie plus cei 29 de octeți VTAM adăugați pentru antetul de cerere SNA și antetul de transmisie. MAXBFRU este măsurată în unități de 4K octeți, așa încât MAXBFRU trebuie să fie de cel puțin 2 pentru a acomoda o RU de 4K.
- Pentru conexiunile NCP trebuie să se asigure faptul că MAXDATA este destul de mare astfel încât să poată trata mărimea RU plus 29 de octeți. Dacă specificați o mărime de 4K, MAXDATA trebuie să fie de cel puțin 4125.

Dacă specificați parametrul NCP MAXBFRU se selectează o valoare care poate acomoda mărimea RU plus 29 de octeți. Pentru NCP, parametrul MAXBFRU definește numărul de buffere VTAM I/O care pot fi folosite pentru reținerea lui PIU. Dacă se alege o mărime a bufferului IOBUF de 441, MAXBFRU=10 procesează un RU de 4K în mod corect deoarece  $10 \times 441$  este mai mare decât  $4096 + 29$ .

- *DRDA Ghid de Conectivitate* descrie cum se calculează impactul pe care baza de date distribuită proprie îl are asupra grupului VTAM IOBUF. Dacă folosiți prea multe resurse ale grupului IOBUF performanța lui VTAM este degradată pentru toate aplicațiile VTAM.

**Concepte înrudite:**

- "DB2 pentru OS/390 și z/OS" la pagina 67



---

## DB2 UDB pentru iSeries

OS/400 conține sistemele DB2<sup>®</sup> UDB pentru iSeries, sistemul IBM iSeries de management al bazei de date relaționale<sup>®</sup>. DB2 Universal Database for AS/400 Versiunea 4.2 a introdus suport pentru comunicațiile DRDA<sup>®</sup> utilizând TCP/IP.

Programul licențiat OS/400<sup>®</sup> Versiunea 2 Livrarea 1 Modificarea 1 a sprijinit unitatea de lucru de la distanță DRDA și OS/400 Versiunea 3 Livrarea 1 a adăugat suport pentru unitatea de lucru distribuită DRDA (DUOW). Acest suport este parte a sistemului de operare OS/400. Acest lucru înseamnă că nu aveți nevoie de Managerul de interogare DB2 UDB pentru iSeries și de programele licențiate Kit de dezvoltare SQL pentru a utiliza suportul DRDA sau pentru a rula programele cu instrucțiuni SQL înglobate.

### Concepte înrudite:

- “Reprezentarea datelor (iSeries)” la pagina 117
- “Considerații de securitate pentru servere de aplicații (iSeries)” la pagina 94
- “Considerații de securitate pentru utilizatorii aplicației (iSeries)” la pagina 109

### Task-uri înrudite:

- “Instalarea DB ca un server de aplicații folosind SNA (iSeries)” la pagina 47
- “Instalarea DB2 ca un solicitant de aplicații – SNA (iSeries)” la pagina 29

---

## DB2 pentru VM

SQL/DS<sup>™</sup> (DB2 pentru VM) Versiunea 3 Ediția 5 furnizează DRDA<sup>®</sup> server de aplicație unitate de lucru de la distanță și suportul de solicitant de aplicație pentru sistemele VM.

Fiecare DB2<sup>®</sup> pentru managerul de bază de date VM poate dirija una sau mai multe baze de date (în același timp) și este tipic referită după numele bazei de date pe care o dirijează în mod curent. Acest nume de bază de date relațională este unic în cadrul unui set de rețele SNA interconectate.

SQL/DS (DB2 pentru VM) Versiunea 3 Livrarea 5 furnizează server de aplicație DRDA unitate de lucru de la distanță și suport de solicitant de aplicație pentru sistemele VM. SQL/DS (DB2 pentru VSE) Versiunea 3 Livrarea 5 furnizează suport de server de aplicație unitate de lucru de la distanță DRDA pentru sistemele VSE.

În plus la aceasta, DB2 pentru VSE & VM Versiunea 5 Livrarea 1 furnizează suport de server de aplicație unitate de lucru distribuită DRDA pentru amândouă sistemele, VM și VSE. Accentul acestui capitol este în primul rând asupra conectării sistemelor VM DB2 pentru VSE & VM pentru a nu se confunda cu sistemele DRDA de la distanță. Pentru mai multe informații asupra conectării a două sisteme VM DB2 pentru VSE & se va face referire la următoarele manuale:

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

### Procesarea bazelor de date distribuite - componente DRDA și VM:

Diferite componente DRDA și VM implicate în procesarea bazelor de date distribuite sunt descrise mai jos. Aceste componente permit DB2 for VM database managers pentru a accesa bazele de date relaționale locale și să comunice cu sistemele DRDA de la distanță în rețeaua SNA.



**AVS** Suportul APPC/VTAM (AVS) este o componentă VM care permit aplicațiilor VM să acceseze rețeaua SNA. Furnizează funcția de unitate logică (LU) așa cum este definită de SNA. O LU este referită ca *gateway* în mediile VM. AVS rulează într-un sistem control de grup ca o aplicație VTAM®. Convertește apelurile macro APPC/VM în apeluri macro APPC/VTAM și invers. APPC/VM folosește AVS pentru a ruta și pentru a transla șirurile de date. AVS permite cererilor DB2 pentru VM să fie rutate între sistemul local VM și locațiile de la distanță SNA. AVS trebuie să fie utilizat oricând aplicațiile DB2 pentru VM sau bazele de date co munică cu bazele de date non-DB2 pentru VM sau cu aplicațiile.

Pe partea unui solicitant de aplicație, un utilizator trebuie să fie autorizat să se conecteze printr-un gateway AVS înainte ca cererile să fie trimise. De partea serverului de aplicație, gateway-ul AVS de primire trebuie de asemenea să fie autorizat să se conecteze la mașina server DB2 pentru VM înainte ca AVS să poată să trimită cererile utilizatorului. Autorizarea este făcută prin furnizarea instrucțiunilor de control director IUCV corespunzător pe mașina utilizatorului, mașina bază de date și pe mașinile AVS de trimitere și de recepționare. Pentru detalii asupra cum să se facă acest lucru, se face referire la manualul *VM/ESA Connectivity Planning, Administration, and Operation*.

### **APPC/VM**

APPC/VM este nivelul API de asamblare VM care furnizează un subset pentru setul de funcție LU 6.2 așa cum este definit de SNA. În termeni practici, furnizează verbele LU 6.2 care permit aplicațiilor DB2 pentru VM să se conecteze și să proceseze în managerii bază de date de la distanță și locali. Verbele LU 6.2 suportate de APPC/VM sunt listate în manualul *VM/ESA CP Programming Services*.

### **Directorul de comunicații**

Directorul de comunicații este un fișier CMS NAMES care servește un anumit rol în realizarea conversațiilor APPC între un solicitant de aplicație VM local și un server de aplicație. Directorul furnizează informațiile necesare pentru rutarea și stabilirea unei conversații APPC cu serverul destinație. Aceste informații conțin elemente cum ar fi numele LU, TPN, securitatea, numele de mod, ID-ul de utilizator, parola și numele bazei de date.

DB2 pentru VM utilizează tag-ul COMDIR :dbname pentru a rezolva RDB\_NAME la datele sale de rutare corespondente.

Acest fișier special și funcția lui de comunicație sunt descrise în manualul *VM/ESA Connectivity Planning, Administration, and Operation*.

**CRR** Recuperarea de resursă coordonată (CRR) este o facilitate VM care coordonează comiterea sau backout-ul pentru actualizările resurselor protejate. Programele de aplicație distribuite, în cooperare cu CRR, utilizează conversații protejate pentru a asigura integritatea de resursă de tranzacție distribuită.

### **Server de recuperare CRR**

Serverul de recuperare CRR este o componentă pentru CRR și rulează în propria mașină virtuală. Este responsabil pentru realizarea punctului de sincronizare prin log-are și funcțiilor de resincronizare.

**GCS** Sistemul de control de grup este o componentă VM care consistă din:

- Un segment partajat care rulează într-o mașină virtuală
- Un supervisor de mașină virtuală care leagă multe mașini între ele într-un grup și supraveghează operațiile acestora
- O interfață între următoarele produse de program:
  - Metoda de acces telecomunicații virtuale (VTAM)
  - Suportul APPC/VTAM (AVS)

- Subsistemul de comunicații spool de la distanță (RSCS)
- Programul de control (CP)

GCS supraveghează execuția aplicațiilor VTAM cum ar fi AVS într-un mediu VM. Mașinile virtuale care rulează sub supravegherea GCS nu utilizează CMS.

#### **Adaptor de resursă**

Adaptorul de resursă este porțiunea din DB2 pentru VM logic care se aplă în mașina dumneavoastră virtuală și permite aplicațiilor să ceară acces la serverul DB2 pentru VM. Funcția solicitant de aplicație DRDA este integrată în adaptorul de resursă.

**TSAF** Facilitatea de acces servicii transparente este o componentă VM care furnizează suport de comunicații între sistemele VM interconectate. Într-o colecție TSAF pot participa până la opt sisteme VM, care pot fi considerate analoge unei rețele locale VM (sau unui WAN). Fiecare sistem participant VM trebuie să aibe o mașină virtuală TSAF în operație. În cadrul unei colecții TSAF, toate ID-urile de utilizator și toate ID-urile de resursă sunt unice.

DB2 pentru VM utilizează TSAF pentru a ruta cereri de bază de date distribuită la alte mașini DB2 pentru VM în cadrul colecției TSAF. Dacă sistemul local VM nu are o mașină virtuală AVS, atunci DB2 pentru VM utilizează TSAF pentru a ruta cereri DRDA la un sistem VM care are o mașină virtuală AVS. AVS permite cererii să fie dirijată la alte colecții TSAF și sisteme non-DB2 pentru VM.

O colecție TSAF este văzută ca una sau mai multe unități logice într-o rețea SNA. Resursele definite ca globale în cadrul unei colecții TSAF pot fi accesate de programele de la distanță APPC care se află oriunde în colecție.

Tipic, o colecție TSAF operează într-un mod de sine stătător, independent de VTAM și de rețeaua SNA. Totuși, acesta poate opera cu AVS și VTAM pentru a face ca resursele sale globale să fie accesibile de programele de la distanță APPC care rezidă oriunde în rețeaua SNA. Acest lucru cere ca o mașină AVS și o mașină VTAM să opereze pe unul sau mai mulți membri TSAF. TSAF este descris în manualul VM/ESA® *VM/ESA Connectivity Planning, Administration, and Operation*.

**VTAM** Metoda de acces la telecomunicațiile virtuale furnizează suportul de comunicații de rețea pentru conectivitate. DB2 pentru VM utilizează serviciile VTAM prin AVS pentru a ruta conexiuni și cereri la sistemele de la distanță DRDA. VTAM este folosit *numai* pentru cereri de la distanță care accesează rețeaua SNA.

#### **\*IDENT**

AVS și TSAF folosesc numele de program de tranzacție (TPN) pentru a ruta cereri între sistemele VM care sunt conectate prin TSAF și AVS. TPN poate fi un TPN înregistrat SNA sau un nume alfanumeric valid. VM face referire la valoarea TPN ca un ID de resursă. Pentru ca un server DB2 pentru VM să fie accesibil la sistemele de la distanță DRDA, systems, serverul DB2 pentru VM utilizează serviciul sistem VM IDENTIFY (\*IDENT) pentru a se defini ca managerul unui ID de resursă globală (TPN). După ce serverul este identificat ca o resursă globală, TSAF și AVS pot ruta cereri DRDA la serverul DB2 pentru VM, dacă TPN-ul recepți onat se potrivește cu ID-ul resursei.

Așa cum se arată în Figura 15 la pagina 77, o aplicație VM trebuie să treacă prin crearea de aplicație DB2 pentru VM (adaptare resursă) pentru a accesa bază de date server de aplicație DB2 pentru VM sau DRDA application server database. O bază de date server de aplicație DB2 pentru VM poate primi cereri SQL pentru orice cerere de aplicație DB2 pentru VM sau DRDA.

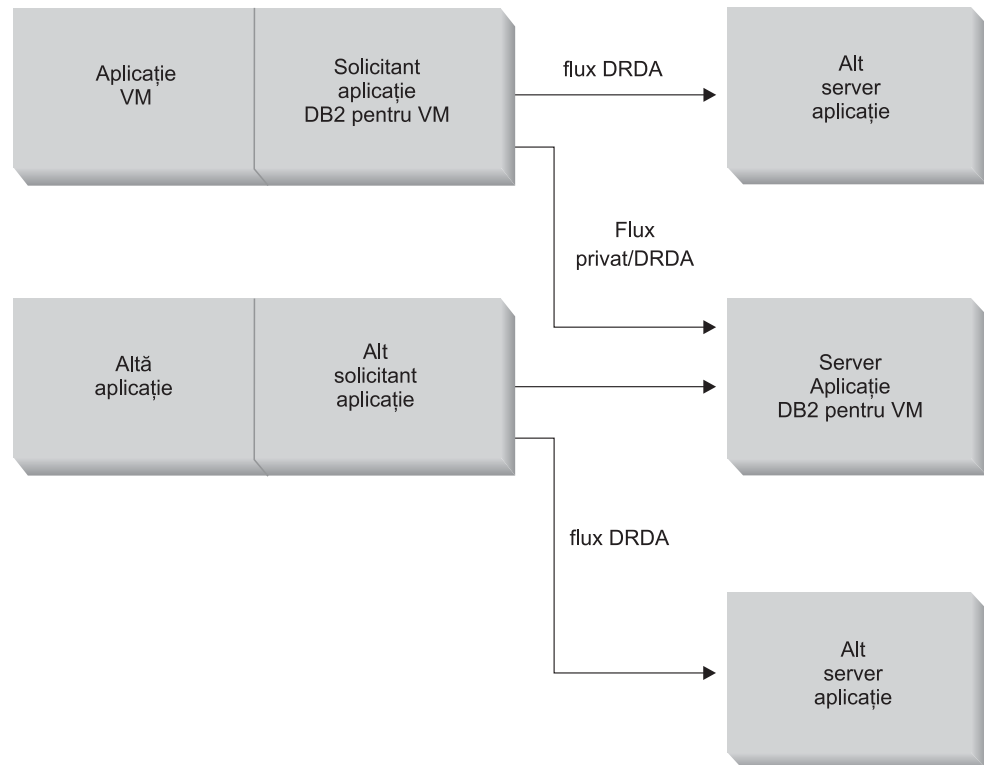


Figura 15. Solicitantul DB2 pentru aplicația VM și serverul de aplicație

### Opțiuni pentru preprocesarea sau rularea unei aplicații:

DB2 pentru VM suportă trei opțiuni de procesare pe comanda **sqlinit** care permite utilizatorului și administratorului bazei de date să activeze suportul bază de date distribuită. Utilizatorul poate specifica una din următoarele opțiuni SQLINIT înaintea preprocesării sau rulării aplicației:

#### PROTOCOL(SQLDS)

Cere utilizarea protocolului privat SQLDS. Aceasta este o opțiune implicită. Poate fi folosită între un solicitant de aplicație DB2 pentru VM și server, într-un mediu de la distanță sau local. Serverul de aplicație DB2 pentru VM presupune că solicitantul folosește aceleași CCSID-uri ca și serverul. Valorile implicite CCSID<sup>2</sup> setate de solicitant prin SQLINIT sunt ignorate și nu este asociat nici o LU 6.2 LUWID cu conversația. Dacă se utilizează numai sisteme DB2 pentru VM și aceeași valoare CCSID este peste tot, atunci aceasta este cea mai eficientă opțiune.

#### PROTOCOL(AUTO)

Apelează Solicitantul de aplicație DB2 pentru VM pentru a găsi dacă serverul de aplicație este ca un sistem sau nu. Apoi selectează automat utilizarea protocolului privat SQLDS pentru un sistem asemănător sau protocolul DRDA pentru un sistem care nu este asemănător. Poate fi utilizat printre sistemele asemănătoare (locale și de la distanță) și printre cele neasemănătoare. În cazul în care serverul de aplicație nu este setat cu PROTOCOL=SQLDS, atunci solicitantul de aplicație și serverul pot avea valori implicite CCSID diferite. Cererile și răspunsurile sunt convertite în mod corespunzător. AUTO este opțiunea recomandată pentru oricare din următoarele cazuri:

2. În DB2 pentru VM, solicitantul de aplicație și serverul de aplicație specifică valoarea implicită CCSID prin specificarea unei opțiuni CHARNAME pentru SQLINIT și respectiv pentru SQLSTART. CHARNAME este un nume simbolic care este mapat intern la CCSID-urile corespunzătoare

- Dacă este nevoie să se acceseze amândouă tipurile de sistem, asemănătoare și neasemănătoare
- Dacă valorile implicite CCSID sunt diferite la solicitant și la server (și opțiunea protocol PROTOCOL pentru serverul de aplicație nu este SQLDS)
- Dacă este nevoie de un LU 6.2 LUWID asociat cu fiecare conversație astfel încât ut ilizatorul să poată întoarce ușor o sarcină la starea ei inițială. Acest lucru este util dacă de administrează multe sisteme de la distanță DB2 pentru VM în rețeaua de bază de date distribuită a utilizatorului.

### PROTOCOL(DRDA)

Forțează solicitantul de aplicație DB2 pentru VM să utilizeze numai protocolul DRDA p entru a comunica cu serverul de aplicație. Utilizatorul poate folosi această opțiune între sistemele asemănătoare (locale și de la distanță) și între sistemele neasemănătoare. În cazul în care serverul de aplicație este un sistem asemănător, atunci protocolul DRDA est e utilizat între două sisteme DB2 pentru VM. Solicitantul de aplicație și serverul de aplicație pot avea valori implicite CCSID diferite. Cererile și răspunsurile sunt convertite în mod corespunzător. Utilizatorul poate folosi această opțiune între două sisteme DB2 pentru VM pentru a testa sau pentru aplicații specifice în care utilizarea protocolului DRDA ar putea furniza o mai bună transmisie datorită utilizării unui buffer cu dimensiunea mai mare pentru transmisie și recepție de date.

Tabela 3 compară caracteristicile funcționale ale opțiunilor de procesare SQLINIT pentru solicitantul de aplicație DB2 pentru VM.

Tabela 3. Compararea Operațiilor de procesare SQLINIT pentru solicitantul de aplicație DB2 pentru VM

[SQLDS]	[AUTO]	[DRDA]
Amândoi partenerii trebuie să fie sisteme DB2 pentru VM	Se conectează la orice sistem DRDA	Se conectează la orice sistem DRDA
Poate comunica cu partenerul local prin TSAF sau AVS/VTAM	Poate comunica cu un sistem DB2 pentru VM local sau cu un sistem de la distanță DB2 pentru VM prin TSAF sau AVS. Cu un sistem diferit, trebuie comunicat prin AVS.	Poate comunica cu un sistem DB2 pentru VM local sau cu un sistem de la distanță DB2 pentru VM prin TSAF sau AVS. Cu un sistem diferit, trebuie comunicat prin AVS.
Suportă SQL static, dinamic și extins	Suportă SQL static, dinamic și extins	Suportă dinamic SQL static, dinamic și extins <sup>3</sup>
Valorile CCSID definite de SQLINIT pentru solicitantul de aplicație sunt ignorate de server ul de aplicație DB2 pentru VM	Valorile CCSID definite de SQLINIT pentru solicitantul de aplicație sunt onorate de serverul de aplicație DB2 pentru VM și este realizată o conversație caracteristică (dacă serverul de aplicație este setat la AUTO)	CCSID-urile definite de SQLINIT pentru solicitantul de aplicație sunt onorate de serverul de aplicație DB2 pentru VM și este realizată o conversație corespunzătoare
Dimensiunea de bloc de 8K fixată; apelul OPEN nu returnează nici un rând; solicitantul de aplicație trebuie să închidă cursorul în mod explicit	DB2 pentru VM la DB2 pentru VM: metoda SQLDS; toate celelalte: metoda DRDA	Dimensiunea de bloc variabilă de la 1K la 32K; împachetare de date mai compactată; apelul OPEN returnează un singur bloc de rânduri; serverul de aplicație poate să închidă cursorul în mod implicit salvând solicitantul de aplicație de la a trimite un apel CLOSE
Se poate utiliza INSERT și PUT pentru cursor pentru a insera un bloc de rânduri la un moment dat utilizând dimensiunea de blocuri fixată de 8K	DB2 pentru VM la DB2 pentru VM: metoda SQLDS; toate celelalte: metoda DRDA	Operațiile PUT sunt convertite în inserări de rânduri simple regulate și se trimite un singur rând la un moment dat

3. SQL dinamic extins este suportat cu fluxuri DRDA prin convertirea în instrucțiuni dinamice sau statice. Aplicarea unor restricții.

Tabela 3. Compararea Operațiilor de procesare SQLINIT pentru solicitantul de aplicație DB2 pentru VM (continuare)

[SQLDS]	[AUTO]	[DRDA]
Toate comenzile DB2 pentru VM unice sunt suportate	DB2 pentru VM la DB2 pentru VM: metoda SQLDS; toate celelalte: metoda DRDA	Comenzile de operator DB2 pentru VM, unele instrucțiuni DB2 pentru VM și unele comenzi ISQL și DBSU nu sunt suportate (A se vedea <i>DB2 Server for VSE &amp; VM SQL Reference</i> ).
LUID nu este suportat	LUID este suportat	LUID este suportat

### Opțiunile pentru pornirea mașinii server bază de date:

Această secțiune descrie diferite opțiuni pentru pornirea Mașinii server bază de date.

#### Parametrul PROTOCOL:

Administratorul bazei de date poate specifica una din următoarele opțiuni pentru parametrul PROTOCOL atunci când se pornește mașina server bază de date.

#### SQLDS

Opțiunea implicită și recomandată în cazul în care serverul de aplicație necesită să furnizeze suport numai pentru apelanții de aplicație DB2 pentru VM sau apelanții de aplicație DB2 pentru VSE luând avantajele de la resursele partajate VSE. Serverul de aplicație utilizează numai fluxul privat (SQLDS).

Serverul de aplicație este sensibil la opțiunea de procesare selectată de solicitantul de aplicație. În cazul în care un solicitant DB2 pentru VM specifică PROTOCOL(SQLDS), procesarea asupra serverului DB2 pentru VM continuă normal cu fluxuri private. În cazul în care solicitantul DB2 pentru VM specifică PROTOCOL(AUTO), atunci serverul DB2 pentru VM notifică solicitantul să schimbe fluxurile private. Nu este schimbată nici o informație CCSID între solicitantul de aplicație și serverul de aplicație. Serverul de aplicație presupune că CCSID-urile solicitant de aplicație sunt aceleași ca CCSID-urile server de aplicație. Dacă solicitantul DB2 pentru VM specifică PROTOCOL(DRDA), atunci conversația este terminată. Dacă solicitantul de aplicație, altul decât DB2 pentru VSE & VM încearcă să acceseze serverul DB2 pentru VM, atunci conversația este terminată.

**AUTO** Opțiunea recomandată dacă serverul The recommended option if the application server needs to provide support for both the private protocol and the DRDA protocol. Apelanții de aplicație DB2 pentru VM care specifică PROTOCOL(SQLDS) sau PROTOCOL(AUTO) comunică în fluxul privat. Pentru solicitantul de aplicație care specifică SQLDS, nici o informație CCSID nu este schimbată și serverul de aplicație presupune că CCSID-urile de solicitant de aplicație sunt aceleași ca CCSID-urile serverului de aplicație. Pentru un solicitant care specifică AUTO, informațiile CCSID sunt schimbate și conversația CCSID pentru cereri și răspunsuri este făcută corespunzător. Fluxul DRDA este cerut de alți apelanți decât DB2 for VM, sau de orice apelanți DB2 pentru VM care specifică PROTOCOL(DRDA).

#### Parametrul SYNCPOINT:

Acest parametru specifică dacă un manager punct de sincronizare (SPM) va fi folosit sau nu pentru a coordona citirea multi-site DRDA-2, activitatea de unitate de lucru distribuită scriere multi-site.

Dacă este specificat Y, atunci serverul va folosi un manager punct de sincronizare, dacă acest lucru este posibil, pentru a coordona comiterile fază dublă și activitatea de resincronizare. Dacă este specificat N, atunci serverul de aplicație nu va utiliza un SPM pentru a realiza

comiteri fază dublă. Dacă este specificat N, atunci serverul de aplicație este limitat unități de lucru distribuitecitere multi-site, scriere single-site și poate fi singurul site de scriere. Dacă Y este specificat, dar serverul de aplicație găsește că un manager punct de sincronizare nu este disponibil, atunci serverul va opera ca și când N a fost specificat.

Implicit este SYNCNT=Y atunci când PROTOCOL=AUTO. Atunci când PROTOCOL=SQLDS, parametrul SYNCNT este setat la N.

#### Exemplu de flux de comunicații pentru solicitant de aplicație:

Următorul exemplu arată cum fiecare componentă joacă un rol în realizarea comunicațiilor între un solicitant de aplicație VM și un server de la distanță DRDA. Figura 16 arată cum solicitantul de aplicație se conectează la AVS și utilizează VTAM pentru a accesa rețeaua SNA. Accesul la resursele de la distanță nu este rutat prin serverul de aplicație DB2 pentru VM.

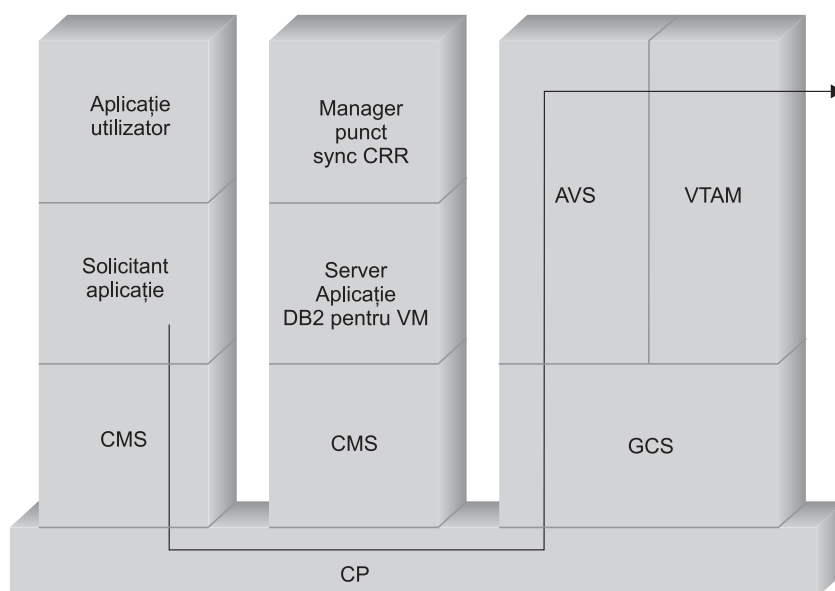


Figura 16. Cererea de acces la o resursă de la distanță

Se presupune că un solicitant de aplicație DB2 pentru VM care operează într-o colecție TSAF este cel care trebuie să acceseze datele de la distanță dirijate de un server de aplicație DRDA. Prin definiție, acest lucru implică o mașină TSAF care operează pe o gazdă locală VM unde se află solicitantul de aplicație. De asemenea, o componentă AVS și o mașină VTAM operează pe un sistem VM în această colecție TSAF. AVS și VTAM pot de asemenea să se găsească pe același sistem ca solicitantul de aplicație Server de aplicație.

După ce mașina VTAM pornește, aceasta definește gateway-ul local AVS la rețeaua SNA și activează una sau mai multe sesiuni pentru a le utiliza mai târziu pentru realizarea conversățiilor.

După ce pornește mașina AVS, aceasta negociază limitele sesiunii între gateway-ul local AVS și LU-urile potențial partener.

Serverul de aplicație poate să fie sau să nu fie activ. Operatorul trebuie să îl pornească înainte de a putea procesa cereri de la o aplicație asemănătoare sau neasemănătoare Solicitantului de aplicație.

Solicitantul de aplicație emite o instrucțiune APPC/VM CONNECT pentru a realiza o conversație LU cu serverul de aplicație. Funcția CONNECT utilizează Directorul de comunicații CMS pentru a rezolva numele de bază de date relațională în numele lui LU asociat și TPN-ul care cuprinde adresa Serverului de aplicație din rețeaua SNA. Directorul de comunicații CMS determină de asemenea nivelul de securitate de conversație și cuvintele de securitate, cum ar fi ID-ul utilizatorului și parola, pentru a trece la site-ul de la distanță pentru scopuri de autorizare. Dacă SECURITY=PGM este folosit, atunci solicitantul de aplicație trebuie să treacă un ID de utilizator și o parolă la serverul de aplicație. Utilizatorul poate specifica ID-ul de utilizator și parola în Directorul de comunicații CMS sau în înregistrarea APPCPASS definită cu directorul CP al utilizatorului de aplicație. Dacă SECURITY=SAME este utilizat, atunci numai ID-ul de logare VM pentru utilizatorul solicitant de aplicație este trimis la serverul de aplicație și nu este cerută nici o parolă suplimentară.

De exemplu, dacă folosiți SECURITY=SAME, gazda verifică dacă o mașină AVS operează local. Dacă aceasta nu operează, atunci gazda realizează o conexiune între solicitantul de aplicație și mașina locală TSAF. Mașina locală TSAF alege celelalte mașini TSAF din colecția TSAF pentru mașina AVS și apoi realizează o conexiune la aceasta.

Componenta AVS din colecția TSAF convertește cererea de conexiune APPC/VM la apelul lui de funcție echivalent APPC/VTAM. AVS utilizează apoi o sesiune existentă sau alocă o nouă sesiune între gateway-ul său (LU) și LU-ul de la distanță. AVS realizează apoi o conversație cu LU-ul de la distanță și trimite numele de LU, TPN-ul, nivelul de securitate și ID-ul utilizatorului. Dacă LU-ul de la distanță este de asemenea un sistem VM, atunci sesiunea și conversația sunt mânuite de componenta AVS care rulează pe acel sistem.

#### Exemplu de flux de comunicații server de aplicație:

Următorul exemplu arată cum fiecare componentă joacă un rol în realizarea comunicațiilor între un solicitant aplicație de la distanță și un server DB2 pentru VM DRDA local. Figura 17 arată că VTAM rutează conexiunea internă la gateway-ul specific AVS și apoi la serverul de aplicație.

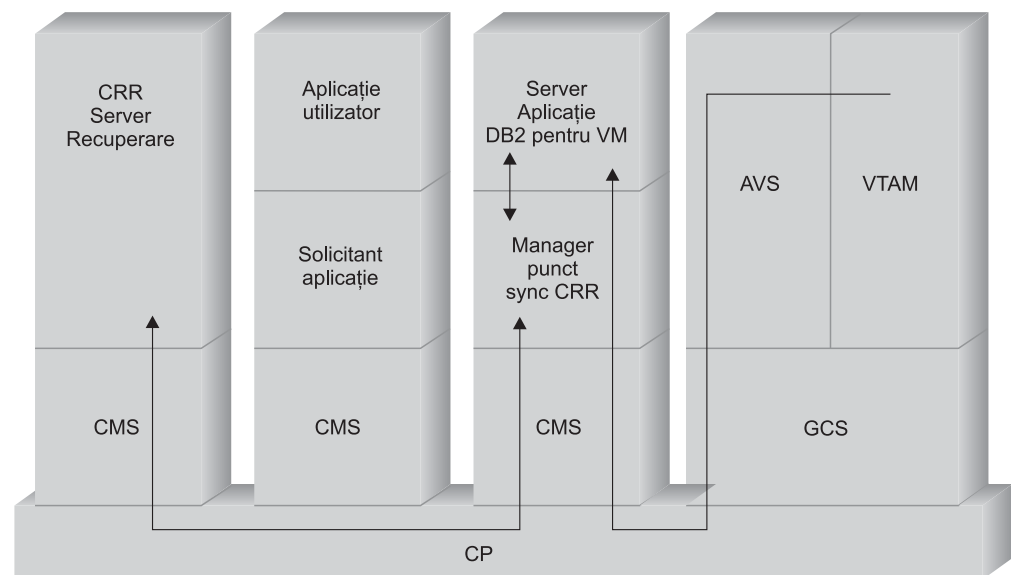


Figura 17. Câștigarea accesului la o resursă de la distanță

Se presupune că un server de aplicație DB2 pentru VM operează într-o colecție TSAF. Prin definiție, acest lucru implică că o mașină TSAF operează pe gazda locală VM unde se află serverul de aplicație. De asemenea, o componentă AVS și o mașină VTAM operează pe un



sistem VM în această colecție TSAF. AVS și VTAM pot de asemenea să se găsească pe același sistem ca solicitantul de aplicație Server de aplicație.

După ce mașina VTAM pornește, aceasta definește gateway-ul local AVS la rețeaua SNA și activează una sau mai multe sesiuni pentru a le utiliza mai târziu pentru realizarea conversațiilor.

După ce pornește mașina AVS, aceasta negociază limitele sesiunii între gateway-ul local AVS și LU-urile potențial partener.

Serverul de aplicație poate să fie sau să nu fie activ. Operatorul trebuie să îl porească înainte de a putea procesa cereri de la un Solicitant de aplicație asemănător sau neasemănător. După ce serverul de aplicație pornește, acesta utilizează serviciul \*IDENT pentru a înregistra ID-ul de resursă care se descurcă cu sistemul VM gazdă. Fiecare înregistrare creează o intrare într-o tabelă de resursă internă menținută de sistemul VM.

După ce componenta AVS locală realizează sesiunea cu LU-ul partenerului său, atunci acceptă conversația și trimite TPN-ul, ID-ul de utilizator și parola la gazda VM pentru validare. VM caută pentru TPN în tabela de resurse internă. Această tabelă conține o intrare pentru fiecare ID de resursă înregistrat prin serviciul de sistem \*IDENT. În cazul în care căutarea TPN este cu succes, atunci VM validează ID-ul de utilizator și parola cu directorul corespunzător, sau RACF® sau un produs de securitate similar. În cazul în care validarea este cu succes, atunci AVS realizează o conexiune la serverul de aplicație și trimite ID-ul de utilizator pentru scopuri de autorizare bază de date.

În cazul în care căutarea de tabelă nu este cu succes, atunci AVS relaționează că TPN-ul trebuie să se găsească într-un alt sistem VM în colecția TSAF și realizează o conexiune la mașina locală TSAF, trimițându-i ID-ul utilizatorului, parola și TPN. Mașina TSAF alege celelalte mașini TSAF din colecția TSAF. Dacă una din aceste mașini cunoaște existența TPN-ului din tabela de resursă proprie, atunci mașina TSAF locală se conectează la mașina de la distanță TSAF și îi trimite ID-ul utilizatorului și parola pentru a fi verificată cu directorul său VM. Dacă validarea este cu succes, mașina TSAF de la distanță se conectează la Serverul de aplicație și trimite ID-ul utilizator pentru autorizarea de bază de date.

În cazul în care solicitantul de aplicație dorește să beneficieze de suportul de unitate de lucru distribuită DRDA, atunci realizează o conversație protejată (cum ar fi SYNCLEVEL=SYNCPT) cu serverul de aplicație DB2 pentru VM. Înainte ca CMS să prezinte conexiunea la DB2 pentru VM, creează o unitate de lucru CMS pentru conversația protejată de pe mașina DB2 pentru VM. DB2 pentru VM utilizează apoi această unitate de lucru CMS oricând realizează lucru pentru a pelant. Atunci când DB2 pentru VM începe să lucreze pentru solicitant, înregistrează această unitate de lucru CMS cu managerul punct de sincronizare CRR. Apoi, atunci când DB2 primește o indicație "apelare comitere" sau o indicație "apelare întoarcere" pe conversația protejată, atunci cere managerului punct de sincronizare CRR să comită sau să întoarcă unitatea de lucru. Managerul punct de sincronizare CRR dirijează apoi comiterea sau întoarcerea, cerând Serverului de recuperare CRR să realizeze punctul de sincronizare logându-se atunci când este necesar.

Depinzând de complexitatea rutării pentru conexiune, conversația APPC între solicitantul de aplicație și serverul de aplicație poate implica sisteme suplimentare. Oricum, toate conexiunile intermediare sunt dirijate de VM și sunt transparente pentru solicitantul de aplicație sau pentru aplicația utilizator. Interfața APPC/VM lasă serverele de aplicație DB2 pentru VM să comunice cu programele de aplicație APPC care se află în:

- Același sistem VM
- Sistem VM diferit
- Sistem VM dintr-o rețea SNA care are AVS și VTAM în rulare



- Sistem VM dintr-o colecție TSAF diferită care are AVS și VTAM în rulare
- Sistem non-VM într-o rețea SNA care suportă protocolul LU 6.2
- Sistem non-IBM dintr-o rețea SNA care suportă protocolul LU 6.2

**Concepte înrudite:**

- “Cosiderații de securitate pentru serverele de aplicații (VM)” la pagina 97
- “Reprezentarea datelor (VM)” la pagina 120
- “Considerente de securitate pentru solicitantii de aplicații (VM)” la pagina 111
- “DB2 pentru VSE” la pagina 84

**Task-uri înrudite:**

- “Instalarea DB2 ca un server de aplicații (VM)” la pagina 61
- “Setarea pentru DB2 ca un solicitant de aplicație (VM)” la pagina 35

**Referințe înrudite:**

- “Listă de verificări pentru activarea unui solicitant de aplicații DB2 (VM)” la pagina 126

## Subconcepte

### Definirea solicitantului de aplicație de comunicații—

În mediul VM, o combinație de componente realizează managementul de comunicație. Componentele implicate în comunicație, printre care nu cele ca sistemele DRDA, sunt APPC/VM, Directorul de comunicații CMS, TSAF, AVS și VTAM.

APPC/VM reprezintă nivelul-asamblare API LU 6.2 pe care îl utilizează solicitantul de aplicație DB2 pentru VM pentru a cere servicii de comunicație. CMS Communications Directory furnizează informațiile de securitate și de rutare pentru sistemul partener distribuit. AVS activează gateway-ul și translatează fluxurile APPC/VM din afara rețelei în fluxuri APPC/VTAM și încadrează fluxurile APPC/VTAM în fluxuri APPC/VM.

APPC/VM, TSAF și AVS se bazează pe Directorul de comunicații CMS, pe VTAM și pe \*IDENT pentru a ruta cererile spre partenerul DRDA corespunzător.

Pentru ca VTAM să comunice cu aplicațiile partener identificate în Directorul de comunicații CMS, utilizatorul trebuie să furnizeze următoarele informații:

1. Să definească la VTAM numele LU pentru fiecare solicitant de aplicație și pentru fiecare server de aplicație. Locul și sintaxa acestor definiții depinde de cum este conectat logic și fizic sistemul de la distanță la sistemul VTAM.
2. Creați o intrare în tabela mod VTAM pentru fiecare nume mod specificat în Directorul de comunicații CMS. Aceste intrări descriu dimensiunea unității de cerere (RU), plasare dimensiune fereastră și clasa de servicii pentru un anumit nume de mod.
3. Dacă utilizatorul intenționează să utilizeze verificarea LU partener (securitate de nivel-sesiune), atunci se furnizează profilele RACF și VTAM (sau altele echivalente) pentru algoritmul de verificare.

**Considerații de limită sesiune AVS:**

Atunci când un solicitant de aplicație folosește AVS pentru a comunica cu un server de aplicație de la distanță, o conexiune este inițializată. Dacă această conexiune cauzează depășirea limitei de sesiune stabilită, atunci AVS suspendă conexiunea la o stare de așteptare până când o sesiune devine disponibilă. Atunci când o sesiune devine disponibilă, AVS alocă

conexiunea în așteptare la o sesiune și controlul este returnat aplicației utilizatorului. Pentru a evita această situație, se planifică pentru o utilizare de vârf prin mărirea limitei de sesiune pentru a permite unele conexiuni suplimentare. Asigurați-vă că valoarea MAXCONN din directorul CP de pe mașina AVS este destul de mare pentru a suporta o utilizare de vârf de către conexiunile APPC/VM.

**Concepte înrudite:**

- “DB2 pentru VM” la pagina 74

## Setare dimensiuni și ritm RU (VM)

Intrările definite în tabelul mod VTAM<sup>®</sup> specifică numerele dimensiuni și ritm pentru unitate de cerere (RU). Eșecul în definirea corectă a acestor valori poate avea un efect advers asupra tuturor aplicațiilor VTAM.

După alegerea numerelor dimensiuni unitate de cerere (RU), limite sesiune și ritm considerați posibilul impact al acestor valori asupra rețelei SNA existente. Ar trebui să revedeți următoarele elemente când instalați un sistem bază de date distribuită nou:

- Pentru conexiuni VTAM CTC, verificați că parametrul MAXBFRU este destul de mare pentru a gestiona dimensiunea RU plus cei 29 de bytes pe care îi adaugă VTAM pentru antetele cerere SNA și transmisie. MAXBFRU este măsurat în unități de 4K bytes, deci MAXBFRU trebuie să fie cel puțin 2 pentru acomodarea cu un RU de 4K.
- Pentru conexiuni NCP, fiți siguri că MAXDATA este destul de mare pentru a gestiona dimensiunea RU plus 29 bytes. Dacă specificați o dimensiune RU de 4K, MAXDATA trebuie să fie cel puțin 4125.

Dacă specificați parametrul NCP MAXBFRU, alegeți o valoare care să se acomodeze cu dimensiunea RU plus 29 bytes. Pentru NCP, parametrul MAXBFRU definește numărul bufferelor I/O VTAM care pot reține PIU. Dacă alegeți o dimensiune buffer IOBUF de 441, MAXBFRU=10 procesează un RU de 4K corect, deoarece  $10 \cdot 441$  este mai mare decât  $4096 + 29$ .

- *DRDA<sup>®</sup> Ghid conectivitate* descrie cum să estimați impactul bazei de date distribuite asupra pool-ului VTAM IOBUF. Dacă folosiți prea mult din resursele pool-ului IOBUF, performanța VTAM este degradată pentru toate aplicațiile VTAM.

**Concepte înrudite:**

- “DB2 pentru VM” la pagina 74

---

## DB2 pentru VSE

SQL/DS<sup>™</sup> (DB2 pentru VSE) Versiune 3 Ediție 5 oferă DRDA<sup>®</sup> unitate la distanță suportului server pentru lucrul cu aplicații pentru sisteme VSE.

În mediul de operare VSE/ESA<sup>™</sup>, DB2<sup>®</sup> pentru VSE oferă funcția server aplicație într-un mediu DRDA. Funcția solicitant aplicație nu este furnizată. Diversele DB2-uri pentru VSE și componente VSE implicate în procesarea distribuită a bazelor de date sunt descrise în această secțiune. Aceste componente permit sistemului de gestiune a bazei de date DB2 pentru VSE să comunice cu solicitanți de aplicații DRDA la distanță într-o rețea SNA.

### CICS(ISC)

Componenta intersistem Sistemul de control al informațiilor despre clienți (CICS) oferă funcțiile SNA LU 6.2 (APPC) pentru serverul aplicație DB2 pentru VSE.

### CICS(SPM)

Componenta gestiune punct sync CICS<sup>®</sup> este integrată în suportul unitate de lucru

distribuit DB2 pentru VSE DRDA. Funcționează ca un participant punct sync și este responsabil cu coordonarea activității comitere în doua faze la un sistem VSE/ESA.

### CICS(TRUE)

Ieșirea utilizator legat de task CICS este o interfață folosită de tranzacția AXE pentru a comunica cu managerul punct sync CICS.

### ACF/VTAM®

CICS(ISC) folosește VTAM® pentru VSE pentru a stabili sau lega sesiuni LU-la-LU cu sisteme la distanță. DB2 pentru VSE folosește conversații de bază LU 6.2 pe parcursul acestor sesiuni pentru a comunica cu solicitanții de aplicații DRDA la distanță.

### AXE

Tranzacția APPC-XPCC-Exchange este o tranzacție CICS activată de solicitantul de aplicație DRDA la distanță. Ea rutează șirul de date DRDA între solicitantul de aplicație la distanță și serverul aplicație DB2 pentru VSE folosind suportul CICS LU 6.2 și funcțiile VSE XPCC.

### Directorul DBNAME

Directorul DBNAME (nume bază de date) mapează o cerere de intrare pentru alocare ea conversației la un server aplicație predeterminat identificat de TPN-ul de intrare. Vedeți *Ghid de administrare a sistemului SQL/DS pentru VSE* pentru detalii suplimentare.

### XPCC

Controlul comunicație partiție încrucișată este interfața macro VSE care oferă transferul de date dintre partiții VSE.

### Exemplu flux de comunicații server aplicație:

Figura 18 arată cum fiecare componentă joacă un rol în stabilirea comunicațiilor dintre serverul aplicație DB2 pentru VSE și solicitantul de aplicație la distanță.

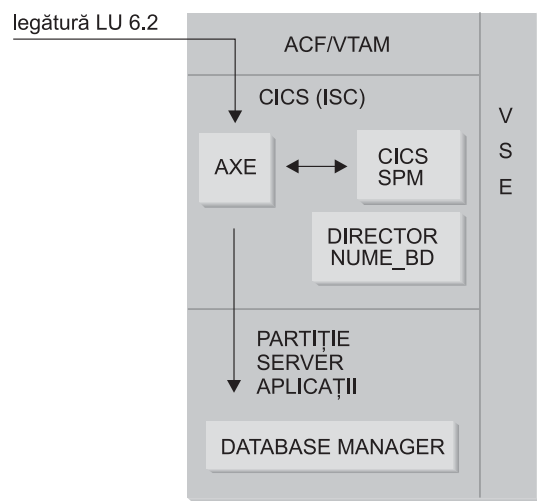


Figura 18. Dobândirea accesului la serverul aplicație

Solicitantul de aplicație emite un verb ALLOCATE cu un nume LU specific și nume program tranzacție (TPN) pentru stabilirea unei conversații LU 6.2 cu serverul aplicație. Numele LU este folosit pentru rutarea cererii ALLOCATE prin VTAM spre CICS. După primirea verbului ALLOCATE, CICS verifică dacă o tranzacție AXE este definită cu acel TPN și efectuează o deschidere sesiune CICS. Dacă nivelul de securitate al conversației pentru conexiunea CICS este VERIFY ID-ul utilizator și parola sunt așteptate de la solicitantul de aplicație și sunt folosite în această deschidere de sesiune.

Taboul deschidere de sesiune CICS (DFHSNT) trebuie să fie actualizat cu ID-ul și parola acestui utilizatorului ca să poată fi acceptată conexiunea. Dacă nivelul de securitate este setat la IDENTIFY, numai ID-ul utilizator este cerut, și CICS încredințează verificarea securității sistemului la distanță. Dacă verificarea securității decurge cu succes, CICS pornește tranzacția AXE pentru a ruta cereri și răspunsuri între solicitantul aplicație și serverul aplicație. TPN-ul folosit de solicitantul aplicație trebuie de asemenea să aibă o intrare definită în directorul DB2 pentru VSE DBNAME care trimite la un server operațional DB2 pentru VSE din sistemul VSE.

Dacă solicitantul aplicație dorește să folosească suportul unității de lucru distribuit specifică un SYNCLVL al SYNCPT la verbul APPC ALLOCATE. Când tranzacția AXE a început, ea interoghează CICS pentru a determina SYNCLVL-ul conversației. Dacă el este SYNCPT, face următoarele:

- Dacă este necesar, tranzacția AXE activează suportul TRUE astfel încât să poată comunica cu managerul punct sync CICS.
- Înregistrează unitatea logică de lucru cu managerul punct sync CICS.

#### **Limitări server aplicație:**

Spre deosebire de VM-ul complementar, serverul aplicație DB2 pentru VSE acceptă fluxurile DRDA de la solicitanți aplicație la distanță. Protocoalele private nu sunt suportate. Ca efect, solicitanții aplicație VM nu pot accesa un server VSE cu PROTOCOL=SQLDS. Serverul DRDA DB2 pentru VSE nu poate ruta cereri de la solicitanți aplicație la distanță la un server DB2 pentru VM folosind partajarea oaspete VSE. Astfel de cereri ar trebui trimise direct la serverul DRDA DB2 pentru VM.

#### **Parametri pornire server aplicație:**

##### **Parametrul RMTUSERS**

Administratorul bazei de date poate specifica parametrul RMTUSERS la pornirea serverului aplicație pentru a seta numărul maxim de solicitanți aplicație la distanță cărora li se permite conectarea la server. Acesta este similar valorii MAXCONN din directorul VM al mașinei server bază de date DB2 pentru VM. Acest parametru ajută la echilibrarea lucrului între procesarea locală și la distanță.

Când valoarea RMTUSERS este mai mare decât numărul agenților DB2 pentru VSE disponibili (definit de NCUSER), unii utilizatori la distanță trebuie să aștepte ca un agent DB2 pentru VSE să se ocupe de cererea lor. În mod normal un agent DB2 pentru VSE este reassignat unui utilizator în așteptare la sfârșitul unei unități logice de lucru (LUW). Serverul aplicație DB2 pentru VSE suportă acces privilegiat care permite unui utilizator la distanță să păstreze un agent DB2 pentru VSE LUW-uri multiple până la sfârșitul conversației.

##### **Parametrul SYNCPT**

Acest parametru specifică dacă un manager punct sync (SPM) va fi sau nu folosit pentru coordonarea activității unității de lucru distribuit de citire multi-site, scriere multi-site.

Dacă Y este specificat, serverul va folosi un manager punct sync, dacă este posibil, pentru coordonarea comiterilor în două faze și activității de resincronizare. Dacă N este specificat, serverul aplicație nu va folosi un SPM pentru a realiza comiteri în două faze. Dacă N este specificat, serverul este limitat la unități de lucru distribuit de citire multi-site, scriere multi-site și poate fi în stare de scriere unică. Dacă Y este specificat, dar serverul aplicație găsește că un SPM nu este disponibil, atunci serverul va funcționa ca și cum ar fi fost specificat N.

Valoarea implicită este SYNCPT=Y când RMTUSERS este mai mare sau egal cu zero. Când RMTUSERS=0, parametrul SYNCPT este setat la N.

**Task-uri înrudite:**

- “Instalarea DB2 ca un server de aplicații (VSE)” la pagina 55



---

## Capitolul 12. Considerații de securitate pentru servere de aplicații

---

### Considerații de securitate pentru serverele de aplicații (OS/390 și z/OS)

Atunci când o cerere aplicație rutează o cerere de bază de date distribuită către serverele de aplicații DB2<sup>®</sup> pentru OS/390<sup>®</sup> și z/OS<sup>™</sup> următoarele considerente de securitate ar putea fi implicate:

- Verificare De-La-Cine (Come-from checking)
- Nume de utilizatori terminali (End user names)
- Securitate de rețea (Network security)
- Securitate a managerului de bază de date (Database manager security)
- Subsistem de securitate (Security subsystem)

**Concepte înrudite:**

- “Considerații de securitate pentru solicitantii de aplicații (OS/390 și z/OS)” la pagina 103
- “DB2 pentru OS/390 și z/OS” la pagina 67

**Task-uri înrudite:**

- “Instalarea DB2 ca un server de aplicații (OS/390 și z/OS)” la pagina 43

---

### Subconcepte

#### Verificarea provenienței (Come-From)(OS/390 and z/OS)

Când aplicația gazdă de pe server primește un nume de utilizator terminal de la aplicația solicitantă, serverul de aplicații poate restricționa numele utilizatorilor terminali primite de la un anumit solicitant de aplicații. Acest lucru este realizat prin utilizarea verificării *provenienței*. Verificarea provenienței permite serverului de aplicații să specifice ca un identificator de utilizator dat să poată fi folosit doar de anumiți parteneri.

De exemplu, serverul de aplicații poate să-i restricționeze lui JONES “accesul\_doar\_din” DALLAS. Dacă un alt solicitant de aplicații (altul decât DALLAS) încearcă să trimită numele JONES către serverul de aplicații, atunci serverul de aplicații poate refuza, deoarece numele nu a venit din locația corectă a rețelei.

Sistemul dumneavoastră gazdă implementează verificarea provenienței ca o parte a translării numelor utilizatorilor terminali, care este descrisă în secțiunea următoare.

**Notă:** Intrarea și verificarea provenienței nu sunt realizate pentru cereri de intrare TCP/IP.

**Concepte înrudite:**

- “Considerații de securitate pentru serverele de aplicații (OS/390 și z/OS)” la pagina 89

#### Nume utilizator oprire - server aplicație (OS/390 și z/OS)

ID-ul utilizator transmis de solicitantul de aplicație ar putea să nu fie unic în întreaga rețea SNA. Serverul aplicație DB2<sup>®</sup> ar putea avea nevoie să efectueze translarea numelui de intrare pentru a crea nume utilizatori oprire unice în întreaga rețea SNA. Similar, serverul aplicație

DB2 ar putea fi nevoit să efectueze translații nume de ieșire pentru a oferi un nume utilizator oprire unic pentru serverele secundare implicate în aplicație.

Translația numelui de intrare este activată prin setarea coloanei USERNAMES din SYSIBM.LUNAMES sau tabelul SYSIBM.IPNAMES la 'I' (translație de intrare) sau 'B' (translație de intrare și de ieșire). Când translația numelui de intrare este în aplicare, DB2 translatează ID-ul utilizator trimis de solicitantul de aplicație și numele deținătorului de plan DB2 (dacă solicitantul de aplicație este alt sistem DB2).

Dacă solicitantul de aplicație trimite un ID-utilizator și verbul APPC ALLOCATE, ID-ul și parola sunt validate înainte ca ID-ul utilizator să fie tradus. Coloana PASSWORD din SYSIBM.USERNAMES nu este folosită pentru validarea parolei. În loc de aceasta, ID-ul și parola utilizatorului sunt prezentate sistemului de securitate extern (RACF sau un produs echivalent-RACF) pentru validare.

Când ID-ul utilizator de intrare cu verbul ALLOCATE este verificat, DB2 are ieșiri autorizate pe care le puteți folosi pentru a oferi o listă de AUTHID-uri secundare și pentru a realiza verificări de securitate adiționale. Vedeți *DB2 for OS/390 Administration Guide* pentru detalii.

Procesul de translație a numelui de intrare caută un rând în tabelul SYSIBM.USERNAMES, care trebuie să se potrivească unui model arătat în următoarea listă (TYPE.AUTHID.LINKNAME):

1. I.AUTHID.LINKNAME—Un utilizator oprire specific de la un solicitant de aplicație specific.
2. I.AUTHID.blank—Un utilizator oprire specific de la orice solicitant de aplicație specific
3. I.blank.LINKNAME—Orice utilizator oprire specific de la un solicitant de aplicație specific

Dacă nu este găsit nici un rând, accesul la distanță este refuzat. Dacă este găsit un rând, accesul la distanță este permis și numele utilizatorului oprire este schimbat la valoarea oferită în coloana NEWAUTHID, cu o valoare a NEWAUTHID spațiu indicând că numele este neschimbat. Orice verificări autorizării resurse DB2 (de exemplu, privilegiile tabel SQL) făcute de DB2 sunt realizate pe numele utilizator oprire traduse, mai degrabă decât pe numele utilizator originale.

Când serverul aplicație DB2 primește un nume utilizator oprire de la un solicitant de aplicație, mai multe obiective pot fi realizate prin folosirea capacității de translație nume de intrare DB2:

- Puteți schimba un nume utilizator oprire pentru a-l face unic. De exemplu, următoarele instrucțiuni SQL translatează numele utilizator oprire JONES din solicitantul de aplicație NEWYORK (LUNAME LUNYC) într-un nume diferit (NYJONES).

```
INSERAȚI ÎN SYSIBM.LUNAMES
(LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
MODESELECT, USERNAMES)
VALORI ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INSERAȚI ÎN SYSIBM.USERNAMES
(TIP, AUTHID, LINKNAME, NEWAUTHID, PAROLA)
VALORI ('I', 'JONES', 'LUNYC', 'NYJONES', ' ');
```

Figura 19. Schimbarea unui nume utilizator oprire pentru a-l face unic

- Puteți modifica numele utilizator oprire astfel încât un întreg grup de utilizatori oprire să fie reprezentat de un singur nume. De exemplu, ați putea vrea să reprezentați toți utilizatorii



din solicitantul de aplicație NEWYORK (LUNAME LUNYC) cu numele utilizator NYUSER. Aceasta vă permite să oferiți privilegiile SQL numelui NYUSER și să controlați accesul SQL oferit utilizatorilor din NEWYORK.

```

INERATAI ÎN SYSIBM.LUNAMES
  (LUNAME, SYSMODENAME, SECURITY_IN, ENCRYPTPSWDS,
   MODESELECT, USERNAMES)
  VALORI ('LUNYC', ' ', 'A', 'N', 'N', 'I');
INERATAI ÎN SYSIBM.USERNAMES
  (TIP, AUTHID, LINKNAME, NEWAUTHID, PAROLA)
  VALORI ('I', ' ', 'LUNYC', 'NYUSER', ' ');

```

Figura 20. Schimbarea unui nume utilizator astfel încât un grup de utilizatori oprire sunt reprezentați printr-un singur nume

- Puteți restricționa numele utilizator oprire transmise de un solicitant de aplicație particular. Această folosire a translației numelui utilizator oprire realizează întoarcerea din verificare.. De exemplu, instrucțiunile SQL care urmează permit numai SMITH și JONES ca nume utilizator oprire din solicitantul de aplicație NEWYORK. Oricărui alt nume îi este refuzat accesul deoarece nu este listat în tabelul 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', ' ', ' ');

```

Figura 21. Restricționarea numelor utilizator oprire transmise de un solicitant de aplicație

- Puteți restricționa solicitantii de aplicații cărora li se permite conectarea la serverul aplicație DB2. Aceasta este o altă caracteristică a întoarcerii din verificare. Următorul exemplu acceptă orice nume utilizator oprire trimis de solicitantul de aplicație NEWYORK (LUNYC) sau de solicitantul de aplicație CHICAGO (LUCHI). Altor solicitanți de aplicații le este refuzat accesul, deoarece rândul implicit SYSIBM.LUNAMES specifică translația numelui de intrare pentru toate cererile de intrare.

```

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', ' ', ' ');

```

Figura 22. Restricționarea solicitanților de aplicație cărora li se permite conectarea

#### Concepte înrudite:

- “Considerații de securitate pentru serverele de aplicații (OS/390 și z/OS)” la pagina 89

## Securitate rețea - server aplicație (OS/390 și z/OS)

Pentru conexiuni SNA, LU 6.2 oferă 3 caracteristici de securitate a rețelei majore:

- Nivel securitate-sesiune
- Nivel securitate-conversație
- Criptare

Singura considerație despre securitatea rețelei ramasă este nivelul securitate-conversație SNA. Unele aspecte ale nivelului de securitate-conversație sunt unice pentru un server aplicație DB2<sup>®</sup>. Vedeți *DB2 for OS/390 Administration Guide* pentru mai multe detalii. Serverul aplicație DB2 joacă două roluri distincte în securitatea rețelei:

- Ca solicitant către servere secundare, serverul aplicație DB2 este responsabil pentru emiterea cererilor APPC care conțin parametrii nivel securitate-conversație SNA ceruți de serverele secundare. Serverul aplicație DB2 folosește coloana NUMEUTILIZATORI din tabelul SYSIBM.LUNAMES și tabelul SYSIBM.USERNAMES pentru a defini cerințele de nivel de securitate a conversației SNA pentru fiecare server secundar.
- Ca server pentru solicitantul de aplicație, serverul aplicație DB2 dictează cerințele de nivel de securitate a conversației SNA pentru solicitantul de aplicație. DB2 folosește coloana USERSECURITY a tabelului SYSIBM.LUNAMES pentru a determina securitatea conversației cerute de fiecare solicitant de aplicație din rețea. Următoarele valori sunt folosite în coloana USERSECURITY:

**C** Aceasta arată că DB2 cere solicitantului de aplicație să trimită un ID și o parolă a utilizatorului (LU 6.2 SECURITY=PGM) cu fiecare cerere bază de date distribuită. Dacă coloana ENCRYPTPSWDS din SYSIBM.LUNAMES conține 'Y', DB2 presupune că parola este deja în format criptat RACF<sup>®</sup> (așa ceva este posibil doar pentru un solicitant de aplicație DB2). Dacă coloana ENCRYPTPSWDS nu conține 'Y', DB2 așteaptă parola în sformatul standard LU 6.2 (reprezentare caracter EBCDIC). În fiecare caz, DB2 trece ID-ul și parola utilizatorului subsistemului de securitate pentru validare. Trebuie să aveți un subsistem de securitate care oferă verificarea ID-ului și parolei utilizatorului APPC de exemplu, RACF are capacitatea să verifice ID-urile și parolelele utilizatorilor APPC. Dacă subsistemul de securitate respinge perechea ID-parolă utilizator, accesul la baza de date distribuită este refuzat.

### Orice altă valoare

Aceasta arată că solicitantului de aplicație îi este permis să trimită ori un ID utilizator deja verificat (LU 6.2 SECURITY=SAME) ori un ID și o parolă utilizator (LU 6.2 SECURITY=PGM). Dacă un ID și o parolă utilizator sunt trimise, DB2 le procesează așa cum este descris pentru 'C' mai jos. Dacă cererea conține numai un ID utilizator, subsistemul de securitate este chemat pentru a autentifica utilizatorul doar dacă tabelul sysusernames este folosit pentru a gestiona ID-urile utilizator de intrare.

Dacă o violare a securității este descoperită, LU 6.2 cere serverului aplicație DB2 să returneze codul sens securitate SNA ('080F6051'X) către solicitantul de aplicație. Deoarece acest cod sens nu descrie cauza eșecului, DB2 oferă două metode pentru a înregistra cauza violărilor de securitate distribuită:

- Un mesaj DSNL030I este produs, care oferă solicitantului LUWID și un cod motiv Db2 care descrie eșecul. DSNL030I include de asemenea AUTHID, dacă este cunoscută, care a fost trimisă de la cererea de aplicație care a fost respinsă.
- O alertă este înregistrată în baza de date monitor hardware NETVIEW, care conține aceleași informații oferite în mesajul DSNL030I.

### Concepte înrudite:

- “Construcții de securitate pentru serverele de aplicații (OS/390 și z/OS)” la pagina 89

## Securitate manager bază de date - server aplicație (OS/390 și z/OS)

Ca deținător al resurselor bazei de date, serverul aplicație DB2<sup>®</sup> controlează funcțiile de securitate ale bazei de date pentru obiecte SQL care se află la serverul aplicație DB2. Accesul la obiecte gestionate de DB2 este controlat prin privilegii, care sunt oferite utilizatorilor de administratorul DB2 sau de deținătorii de obiecte individuale. Cele două clase de bază de obiecte pe care le controlează serverul aplicație DB2 sunt:

- Utilizatorii oprire **Pachete**— Individual sunt autorizați să creeze, înlocuiască și rula pachete cu comanda DB2 GRANT. Când un utilizator oprire deține un pachet, acel utilizator poate rula sau înlocui automat pachetul. Alți utilizatori oprire trebuie autorizați în mod specific să ruleze un pachet la serverul aplicație DB2 cu comanda GRANT. USE poate fi oferit utilizatorilor oprire individuali sau celor PUBLIC, ceea ce permite tuturor utilizatorilor oprire să ruleze pachetul.

Când o aplicație este legată de DB2, pachetul conține instrucțiunile tSQL conținute în programul aplicație. Aceste instrucțiuni SQL sunt clasificate ca:

### SQL static

SQL static înseamnă că instrucțiunea SQL și obiectele SQL referențiate de instrucțiune sunt cunoscute la momentul în care aplicația este asociată DB2. Persoana care creează pachetul trebuie să aibă autorizarea să execute fiecare din instrucțiunile SQL static conținute în pachet.

Când utilizatorilor oprire li se oferă autorizația de a executa un pachet, ei au automat autorizație să execute fiecare din instrucțiunile SQL static conținute în pachet. Astfel, utilizatorii oprire nu au nevoie de vreun privilegiu tabel DB2 dacă pachetul pe care îl execută conține numai instrucțiuni SQL static.

### SQL Dinamic

SQL Dinamic descrie o instrucțiune SQL care nu este cunoscută până când programul se execută. Cu alte cuvinte, instrucțiunea SQL este construită de program și asociată dinamic lui DB2 cu instrucțiunea SQL PREPARE. Când un utilizator oprire execută o instrucțiune SQL dinamic, utilizatorul trebuie să aibă privilegiile tabel cerute pentru a executa instrucțiunea SQL. Deoarece instrucțiunea SQL nu este cunoscută la momentul creerii planului sau pachetului, utilizatorului oprire nu-i este oferită automat autorizația cerută de deținătorul pachetului.

- **Obiecte SQL**— Acestea sunt tabele, vizualizări, sinonime sau aliasuri. Utilizatorilor DB2 le pot fi oferite diferite nivele de autorizație pentru a crea, șterge sau citi obiecte SQL individuale. Această autorizație este cerută pentru a asocia instrucțiunile SQL static sau pentru a executa instrucțiuni SQL dinamic.

Când creați un pachet, opțiunea DEZACTIVARE/ACTIVARE vă permite să controlați care tip de conexiune DB2 poate rula pachetul. Puteți folosi rutinele de ieșire securitate RACF<sup>®</sup> și DB2 pentru a permite selectiv utilizatorilor oprire să folosească DDF. Puteți folosi RLF pentru a specifica limitele pentru timpul procesor pentru asocieri la distanță și execuții SQL dinamic.

Construcții un pachet DB2 numit MYPKG, care este deținut de JOE. JOE poate permite lui SAL să execute pachetul emițând instrucțiunea DB2 GRANT USE. Când SAL execută pachetul, se întâmplă următoarele:

- DB2 verifică dacă lui SAL i s-a oferit autorizația USE pentru pachet.
- SAL poate emite orice instrucțiune SQL static din pachet deoarece JOE avea privilegiile obiect SQL cerute pentru a crea pachetul.

- Dacă pachetul are instrucțiuni SQL dinamic, SAL trebuie să aibă privilegiile tabel SQL proprii. De exemplu, SAL nu poate emite `SELECT * FROM JOE.TABLE5` decât dacă îi este acordat acces la citire pentru `JOE.TABLE5`.

**Concepte înrudite:**

- “Considerații de securitate pentru serverele de aplicații (OS/390 și z/OS)” la pagina 89

## Subsistem securitate - server aplicație (OS/390 și z/OS)

Folosirea serverului aplicație DB2<sup>®</sup> de către subsistemul de securitate (RACF sau produs echivalent RACF) depinde de cum definiți funcția de translație nume intrare din tabelul `SYSIBM.LUNAMES`:

- Dacă specificați 'I' sau 'B' pentru coloana `NUMEUTILIZATORI`, translația numelui de intrare este activă, și DB2 presupune că administratorul DB2 folosește translația numelui de intrare pentru a realiza o parte din obligațiile de securitate ale sistemului. Subsistemul de securitate extern este chemat doar dacă solicitantul de aplicație trimite o cerere conținând ID-ul utilizator și parola (`SECURITY=PGM`). Trebuie să aveți un subsistem de securitate care oferă APPC verificarea ID-ului utilizator și parolei; de exemplu, RACF<sup>®</sup> are capacitatea să verifice ID-urile și parolele utilizatorilor APPC.

Dacă cererea de la solicitantul de aplicație conține numai un ID utilizator (`SECURITY=SAME`), sistemul de securitate extern nu este chemat deloc, deoarece regulile de translație a numelui de intrare definesc căror utilizatori li se permite conectarea la serverul aplicație DB2.

- Dacă specificați altceva decât 'I' sau 'B' pentru coloana `NUMEUTILIZATORI`, următoarele verificări subsistem securitate sunt făcute:
  - Când o cerere bază de date distribuită este primită de la solicitantul de aplicație, DB2 cheamă sistemul de securitate extern pentru a valida ID-ul utilizatorului oprire (și parola dacă este oferită).
  - Sistemul de securitate extern este chemat pentru a verifica că utilizatorul oprire este autorizat să se conecteze la subsistemul DB2.
- În fiecare caz, o ieșire autorizație este condusă pentru a oferi o listă de ID-uri autorizații secundară.

Pentru informații suplimentare, vedeți *DB2 UDB pentru OS/390<sup>®</sup> și z/OS<sup>™</sup> Ghid administrație*.

**Concepte înrudite:**

- “Considerații de securitate pentru serverele de aplicații (OS/390 și z/OS)” la pagina 89

---

## Considerații de securitate pentru servere de aplicații (iSeries)

Când un solicitant de aplicații rutează o cerere pentru o bază de date distribuită către serverul de aplicații iSeries<sup>™</sup>, pot fi implicate următoarele măsuri de securitate:

- Numele utilizatorului final
- Parametrii de securitate ai rețelei
- Securitatea gestionării bazei de date
- Securitatea iSeries

**Numele utilizatorilor finali:**

Solicitantul de aplicații trimite un identificator utilizator către serverul de aplicații pentru prelucrări legate de securitate. Jobul ce rulează pe serverul de aplicații iSeries utilizează acest identificator utilizator sau, în unele situații, un identificator utilizator implicit.

Serverul de aplicații iSeries nu furnizează translatarea intrărilor de identificatori utilizator pentru rezolvarea conflictelor dintre identificatorii utilizator care nu sunt unici sau grupuri de utilizatori multipli sub un singur identificator. Fiecare identificator utilizator trimis de la un solicitant de aplicații trebuie să existe (să se regăsească) pe serverul de aplicații. O metodă de grupare a cererilor de intrare într-un singur identificator utilizator, cu pierderea unei securități, este specificarea unui identificator utilizator implicit într-o intrare de comunicație în subsistemul care tratează cererile de pornire a joburilor de la distanță. Vedeți descrierile ADDGMNE și CHGGMNE în *AS/400 CL Reference*.

### **Securitatea rețelei SNA:**

LU 6.2 furnizează trei caracteristici importante pentru securitatea rețelei:

- Scuritatea la nivel de sesiune
- Scuritate la nivel de conversație
- Criptarea (care nu este suportată de sistemul iSeries)

Serverul de aplicații DB2<sup>®</sup> UDB pentru iSeries folosește securitatea la nivel de sesiune în exact aceeași manieră ca și solicitantul de aplicații DB2 UDB pentru iSeries.

Serverul de aplicații controlează nivelele de conversație SNA utilizate pentru conversație. Parametrul SECURELOC din descrierea dispozitivului APPC sau valoarea locației sigure din lista de locații de la distanță de pe APPN<sup>®</sup> determină ce este acceptat de la solicitantul de aplicații pentru conversație.

Opțiunile de securitate a conversației SNA sunt:

#### **SECURITY=SAME**

De asemenea cunoscută și drept securitate deja verificată. Numai identificatorul utilizator al utilizatorului aplicației este cerut de serverul de aplicații. Nu se trimite nici o parolă. Pentru a folosi acest nivel de securitate la serverul de aplicații, setați parametrul SECURELOC în descrierea dispozitivului APPC la valoarea \*YES sau setați valoarea locației sigure din lista de locații de pe APPN de la distanță la valoarea \*YES.

#### **SECURITY=PGM**

Face ca atât identificatorul utilizator, cât și parola să fie necesare de serverul de aplicații pentru validare. Pentru a folosi acest nivel de securitate a conversației la serverul de aplicații, setați identificatorul utilizator implicit din intrarea subsistemului de comunicații iSeries la valoarea \*NONE (nici un identificator utilizator implicit) și setați parametrul SECURELOC sau valoarea locației sigure la \*NO.

#### **SECURITY=NONE**

Un server de aplicații nu așteaptă un identificator utilizator sau o parolă. Conversația este permisă utilizându-se un profil utilizator implicit pe serverul de aplicații. Pentru a folosi această opțiune, specificați un profil utilizator implicit în directorul de comunicații al subsistemului și specificați \*NO pentru parametrul SECURELOC sau pentru valoarea locației sigure.

SNA/DS (SNA Servicii Distribuite) necesită un identificator utilizator implicit, deci SNA/DS ar trebui să aibă propriul său subsistem pentru cazul normal în care nu doriți un identificator utilizator implicit pentru aplicațiile DRDA<sup>®</sup>.

O metodă pentru gruparea cererilor de intrare de pornire a joburilor într-un singur identificator utilizator a fost menționată în subiectul Numele utilizatorilor finali (End User Names). Această metodă nu verifică identificatorul utilizator trimis de solicitantul de aplicații. Jobul serverului de aplicații este pornit sub un identificator utilizator implicit și utilizatorul care inițiază conexiunea de la serverul de aplicații are acces la serverul de aplicații chiar dacă identificatorul utilizator trimis are autorizare restrânsă. Aceasta se realizează definind serverul de aplicații ca pe o locație nesigură, specificând un identificator utilizator implicit în intrările subsistemului de comunicații al iSeries și configurând solicitantul de aplicații să trimită un identificator utilizator numai în timpul procesului de conectare. Dacă se trimite o parolă, identificatorul utilizator care o însoțește este folosit în locul identificatorului utilizator implicit.

Intrările subsistemului de comunicații iSeries sunt diferențiate prin dispozitivul și numele modului folosite pentru pornirea conversației. Prin asignarea de identificatori de utilizatori diferiți la diferite perechi dispozitiv/mod, utilizatorii pot fi grupați după cum comunică ei cu serverul de aplicații.

Sistemul iSeries oferă de asemenea o opțiune de securitate a rețelei care este folosită numai pentru baze de date distribuite și pentru gestiunea distribuită a fișierelor. Un atribut de rețea pentru aceste tipuri de accesare a sistemului există fie dacă refuză toate încercările de accesare, fie dacă permite ca securitatea să fie controlată de sistem după principiul obiect-cu-obiect.

#### **Securitatea rețelei TCP/IP:**

Folosind comanda **CRTDDMTCPA** , puteți specifica dacă un server va accepta cereri de conectare TCP/IP fără parolă.

#### **Securitatea gestiunii bazei de date:**

Întreaga securitate este tratată prin funcția de securitate OS/400® .

#### **Securitatea sistemului:**

Sistemul iSeries nu are un subsistem de securitate extern. Întreaga securitate este asigurată de funcția de securitate a OS/400 care este o parte integrantă a sistemului de operare. Sistemul de operare controlează autorizarea la toate obiectele din sistem, inclusiv programe, pachete, tabele, vizualizări și colecții.

Serverul de aplicații controlează autorizarea la obiecte rezidente pe serverul de aplicații. Controlul securității pentru aceste obiecte se bazează pe identificatorul utilizator care pornește jobul pe serverul de aplicații. Acest identificator utilizator se determină după cum s-a descris în subiectul Numele utilizatorilor finali.

Securitatea obiectelor poate fi gestionată prin folosirea comenzilor CL de autorizare a obiectelor sau prin declarațiile SQL GRANT și REVOKE. Comenzile CL de autorizare a obiectelor includ Acordă autoritate obiectului (GRTOBJAUT) și Revocă autoritatea obiectului (RVKOBJAUT). Folosiți aceste comenzi CL pentru orice obiect din sistem. Folosiți declarațiile GRANT și REVOKE numai pentru următoarele obiecte SQL: tabele, vizualizări și pachete. Dacă este nevoie să schimbați autorizarea altor obiecte, cum ar fi programe sau colecții, folosiți comenzile GRTOBJAUT și RVKOBJAUT.

La crearea obiectelor pe sistem, li se acordă o autorizare implicită. Identificatorului utilizator care crează tabele, vizualizări și pachete i se dă autoritate totală. Tuturor celorlalți identificatori utilizatori (publicului) li se dă aceeași autoritate pe care o au asupra colecției sau bibliotecii în care se crează obiectul.

Autoritatea asupra obiectelor referite prin declarații statice sau dinamice conținute în pachet este verificată în momentul rulării pachetului. Dacă creatorul pachetului nu are autorizare asupra obiectelor de referință, atunci se returnează mesaje de avertizare când se crează pachetul. În momentul execuției, utilizatorul ce execută pachetul adoptă autoritatea creatorului pachetului. Dacă creatorul pachetului este autorizat asupra unui tabel, dar același utilizator ce rulează pachetul nu este autorizat, utilizatorul adoptă autoritatea creatorului pachetului și are permisiunea de folosire a tabelului respectiv.

Pentru informații suplimentare despre securitatea sistemului, vedeți *OS/400 Security - Reference*.

**Task-uri înrudite:**

- “Acordarea și revocarea autorității (iSeries)” la pagina 111

---

## Cosiderații de securitate pentru serverele de aplicații (VM)

Când un solicitant de aplicații rulează o cerere pentru o bază de date distribuită către serverul de aplicații DB2<sup>®</sup> pentru VM, se pot aplica următoarele măsuri de securitate:

- Numele utilizatorului final
- Parametrii de securitate ai rețelei
- Securitatea gestionării bazei de date
- Securitatea impusă de un subsistem de securitate extern

**Numele utilizatorilor finali:**

Atât în SQL, cât și în LU 6.2, utilizatorii finali li se alocă un identificator de utilizator format dintr-un număr de unu până la 8 octeți. Acest identificator de utilizator trebuie să fie unic în interiorul unui anumit sistem de operare, dar nu e necesar să fie unic în cadrul întregii rețele SNA. Pentru a elimina aceste conflicte de numire, DB2 pentru VM are opțiunea de a utiliza funcția de traducere a identificatorului de utilizator, funcție furnizată de AVS, dar numai cu îndeplinirea următoarelor condiții:

- Serverul de aplicații DB2 pentru VM trebuie să ruleze într-un mediu VM/ESA<sup>®</sup>.
- Cererea de conexiune de intrare trebuie să fie rutată printr-un gateway AVS.
- Solicitantul de aplicații al partenerului trebuie să utilizeze conversația SECURITY=SAME (cunoscută și sub denumirea *deja verificat* în terminologia SNA).

Dacă o conexiune este rutată către un server prin AVS folosindu-se opțiunea SECURITY=SAME, atunci este necesară traducerea identificatorilor de utilizatori AVS. Comanda AGW Aduagă identificator utilizator (ADD USERID), emisă de pe mașina AVS, trebuie să furnizeze permisiunea de securitate intențiilor de conectare ale utilizatorilor ce vin de la un anumit LU de la distanță sau de la un anumit gateway AVS. Trebuie să existe o mapare pentru toate intrările LU și pentru toți identificatorii de utilizatori care se conectează folosind același sistem de securitate (SECURITY=SAME). Comanda este flexibilă; puteți accepta toți identificatorii de utilizatori de la un anumit LU sau de la toți LU de la distanță în general. Sau, puteți accepta numai o anumită mulțime de identificatori de utilizatori de la un anumit LU.

Puteți folosi comanda AGW Aduagă identificator utilizator (ADD USERID) pentru a autoriza intrarea (deja verificată) a identificatorilor de utilizatori la mașina locală AVS, nerealizându-se nici o validare la gazdă. Aceasta înseamnă că identificatorul autorizat nu este obligatoriu să existe la gazdă, dar conexiunea este acceptată oricum.

Pentru schimbarea autorizării AVS curente a unui identificator de utilizator sunt două metode:



- Opriți AVS, folosind comanda AGW STOP. Aceasta anulează în întregime autorizarea identificatorilor de utilizatori.
- Ștergeți identificatorul de utilizator, folosind comanda AGW DELETE USERID.

Ca exemplu, cazul unor identificatori utilizator identici în orașe diferite arată cum poate funcția de translatare AVS să rezolve un conflict de denumire. Se presupune că există un utilizator cu identificatorul JONES în sistemul din Toronto și un alt utilizator cu același identificator se găsește în sistemul din Montreal. Dacă JONES din Montreal vrea să acceseze date din sistemul din Toronto, acțiunile următoare întreprinse la sistemul din Toronto elimină conflictul de denumire și îl împiedică pe JONES din Montreal să beneficieze de privilegiile acordate lui JONES pentru sistemul din Toronto:

1. Operatorul AVS trebuie să se folosească de comanda AGW ADD USERID pentru translatarea identificatorului utilizatorului din Montreal într-un identificator utilizator local. De exemplu, dacă operatorul lansează AGW ADD USERID MTLGATE JONES MONTJON, atunci utilizatorul din Montreal este cunoscut drept MONTJON în interiorul sistemului din Toronto. Dacă toți ceilalți utilizatori din Montreal au permisiunea de a se conecta (prin LU MTLGATE de la distanță) și sunt cunoscuți local prin identificatorii lor de utilizatori de la distanță, atunci operatorul trebuie să lanseze comanda AGW ADD USERID MTLGATE \* =. Comenzile AVS pot fi de asemenea adăugate profilului AVS astfel încât să fie executate automat la pornirea AVS.
2. DBA trebuie să utilizeze comanda GRANT a DB2 pentru VM, pentru a acorda un set de privilegii special pentru identificatorii utilizator translați, în acest caz particular MONTJON.

Aceste acțiuni pot fi realizate de asemenea și la sistemul din Montreal pentru a se asigura faptul că JONES din Toronto nu folosește privilegiile acordate lui JONES din Montreal, atunci când JONES din Toronto accesează date la distanță din sistemul din Montreal.

Comenzile AVS care permit translatarea identificatorilor utilizator sunt descrise în *VM/ESA Connectivity Planning, Administration, and Operation*.

### **Securitatea rețelei:**

LU 6.2 furnizează trei caracteristici importante pentru securitatea rețelei:

- Scuritatea la nivel de sesiune
- Scuritate la nivel de conversație
- Criptare

Serverul de aplicații DB2 pentru VM utilizează securitatea la nivel de sesiune în același mod ca și solicitantii de aplicații DB2 pentru VM.

Solicitantul de aplicații poate trimite fie un identificator utilizator deja verificat (SECURITY=SAME), fie un identificator utilizator și o parolă (SECURITY=PGM). Dacă se trimite un identificator utilizator și o parolă, atunci CP, RACF sau un echivalent le validează cu directorul VM din gazda serverului de aplicații. Dacă validarea eșuează, cererea de conectare este refuzată; altfel, este acceptată. Dacă cererea conține numai un identificator de utilizator, DB2 pentru VM acceptă cererea fără validarea identificatorului de utilizator.

**Notă:** DB2 pentru VM nu furnizează capacitatea de criptare, deoarece VM/ESA nu suportă criptare.

### **Securitatea gestiunii bazei de date:**



Serverul de aplicații DB2 pentru VM verifică dacă identificatorul utilizator dat de VM are autorizarea CONNECT pentru accesarea bazei de date și apoi refuză conexiunea, dacă identificatorul utilizator nu are autorizarea.

Ca proprietar al reurselor bazei de date, serverul de aplicații DB2 pentru VM controlează funcțiile de securitate a bazei de date pentru obiecte SQL ce se află la serverul de aplicații DB2 for VM. Accesul la obiecte gestionate de DB2 pentru VM este controlat printr-un set de privilegii, care sunt acordate utilizatorilor de către administratorul sistemului DB2 pentru VM sau de proprietarul unui anumit obiect. Serverul de aplicații DB2 pentru VM controlează două clase de obiecte:

- **Pachete:** Utilizatorii finali individuali sunt autorizați să creeze, să înlocuiască și să ruleze pachete ce au declarația DB2 pentru VM - GRANT Când un utilizator final crează un pachet, atunci acel utilizator este automat autorizat să ruleze sau să înlocuiască un pachet. Ceilalți utilizatori finali trebuie să fie autorizați explicit pentru a rula un pachet la serverul de aplicații DB2 pentru VM, prin declarația GRANT EXECUTE. Dreptul de rulare(RUN) poate fi acordat individual utilizatorilor finali sau tuturor (PUBLIC), care permite tuturor utilizatorilor finali să ruleze pachetul.

Când o aplicație este preprocesată pe DB2 pentru VM, pachetul conține declarațiile SQL din programul aplicație. Aceste declarații SQL sun clasificate astfel:

- **SQL statice:** Aceasta înseamnă că declarațiile SQL și obiectele SQL referite sunt în momentul în care aplicația este preprocesată. Creatorul pachetului trebuie să aibă autoritatea de a executa fiecare declarație statică SQL din pachet.

Când unui utilizator final i se acordă dreptul de execuție a unui pachet, utilizatorul final are automat autoritatea de execuție a fiecărei declarații stactice SQL conținută în pachet. Totuși, utilizatorii finali nu au nevoie de nici o tabelă de drepturi DB2 for VM dacă pachetul conține numai declarații SQL statice.

- **SQL dinamice:** Acestea descriu o declarație SQL care nu este cunoscută până când pachetul este rulat. Declarația SQL este construită de către program preprocesată dinamic către DB2 pentru VM cu declarația SQL PREPARE sau declarația EXECUTE IMMEDIATE. Când un utilizator final rulează o declarație SQL dinamică, utilizatorul trebuie să aibă tabela de privilegii necesară pentru execuția declarației SQL. Din cauză că declarația SQL nu este cunoscută când se crează pachetul, utilizatorului final nu i se dă automat autoritatea necesară de către proprietarul pachetului.

- **Obiecte SQL:** Acestea pot fi tabele, vizualizări și sinonime. Utilizatorilor DB2 pentru VM li se pot acorda diverse nivele de autorizare pentru crearea, ștergerea, schimbarea sau citirea de obiecte SQL individuale. Această autorizare este necesară pentru preprocesarea declarațiilor SQL statice sau pentru execuția declarațiilor SQL dinamice.

#### Subsistemul de securitate:

Utilizarea acestui subsistem de către serverul de aplicații DB2 pentru VM este opțională. Dacă serverul de aplicații are nevoie să identifice numele LU al solicitantului de aplicații, VTAM<sup>®</sup> apelează subsistemul de securitate pentru a realiza schimbul necesar verificării LU al partenerului. Decizia de realizare a verificării LU al partenerului este luată în funcție de valoarea specificată de parametrul VERIFY din instrucțiunea APPL a VTAM pentru acel gateway pe care serverul de aplicații DB2 pentru VM îl folosește pentru a primi intrări de cereri pentru baze de date distribuite.

Subsistemul de securitate poate fi apelat, de asemenea, și de CP pentru validarea identificatorului utilizator și a parolei trimise de solicitantul de aplicații. Dacă subsistemul de securitate este RACF<sup>®</sup> și nu aveți un profil de sistem RACF, atunci validarea este realizată de RACF. Dacă aveți un profil de sistem RACF, de exemplu RACFPROF, folosiți următoarele instrucțiuni pentru a cere această validare de la RACF:

RALTER VMXEVENT RACFPROF DELMEM (APPCPWL/NOCTL

RALTER VMXEVENT RACFPROF ADDMEM (APPCPWL/CTL

SETEVENT REFRESH RACFPROF

#### Concepte înrudite:

- “DB2 pentru VM” la pagina 74
- “Considerente de securitate pentru solicitanții de aplicații (VM)” la pagina 111

#### Task-uri înrudite:

- “Instalarea DB2 ca un server de aplicații (VM)” la pagina 61

---

## Conșiderații de securitate pentru serverele de aplicație (VSE)

Serverul de aplicații DB2<sup>®</sup> pentru VSE depinde de CICS<sup>®</sup> pentru securitatea de comunicație intersistem. CICS oferă câteva nivele de securitate:

- Securitate la-legare

Implementarea CICS verificării LU-la-LU a nivelului de sesiune SNA LU 6.2.

Implementarea securității la legare este opțională în arhitectura LU 6.2. Pe partea serverului de aplicație aceasta poate fi activată prin furnizarea unei BINDPASSWORD în comanda CEDA DEFINE CONNECTION la definirea conexiunii cu solicitantul de aplicație. Pe partea solicitantului de aplicație, LU-ul partenerului care servește solicitantul de aplicație trebuie de asemenea să suporte securitate la legare și să folosească aceeași parolă pentru verificarea LU-ului partenerului.

Se poate folosi securitate la legare pentru oprirea sistemelor de la distanță neautorizate de a stabili (lega) sesiuni cu CICS.

- Securitate de legătură

Securitatea de legătură poate fi folosită pentru limitarea sistemului de la distanță (și proprii solicitanți aplicație DRDA<sup>®</sup> rezidenți) de a atașa doar un anumit set de tranzații AXE.

De exemplu, se pot defini două tranzații AXE: AXE2 cu cheia de securitate 2, și AXE3 cu cheia de securitate 3. Solicitanților de aplicație din sistemul de la distanță li se pot asigna un operator de securitate de 3 (de exemplu, folosind parametrul OPERSECURITY în comanda CEDA DEFINE SESSION), permițând acestora atașarea doar a lui AXE3. AXE3 ar putea să nuaibă acces privilegiat la server în timp ce AXE2 are acces privilegiat.

- Securitate de utilizator

Implementarea CICS a securității la nivel de conversie de tip SNA LU 6.2 cu furnizarea verificării la terminal utilizator.

Securitatea de utilizator validează ID-ul utilizatorului cu tabela de semnături CICS (DFHSNT) înainte de a accepta o cerere de pornire a conversației. De exemplu, solicitanților de aplicație DRDA care nu sunt definiți în tabela de semnături CICS nu le este permisă atașarea unei tranzații AXE de pornire a conversației cu serverul DB2 pentru VSE. Nivelul de securitate la nivel utilizator pentru un sistem de la distanță poate fi selectat în comanda CEDA DEFINE CONNECTION folosind parametrul ATTACHSEC. Cele trei nivele de atașare a securității sunt:

- LOCAL. Nu este suportat de către DRDA.
- IDENTIFY. Este echivalent cu SECURITY=SAME (sau deja-verificat) în terminologia LU 6.2. Cu acest nivel de securitate, CICS “are încredere” în sistemul de la distanță pentru verificarea propriilor utilizatori înainte de a permite acestora alocarea conversației cu serverul DB2 pentru VSE. Doar ID-ul de utilizator este cerut pentru procesul de semnare CICS. Cu toate acestea, dacă parola este deja transmisă, CICS execută înregistrarea cu parolă.

- VERIFY. Este echivalent cu SECURITY=PGM în terminologia LU 6.2. Cu acest nivel de securitate CICS așteaptă ca sistemul aflat la distanță să transmită atât ID-ul de utilizator cât și parola la alocarea conversației și refuză conexiunea dacă o parolă nu este furnizată.
- Criptografia obligatorie la nivel de sesiune SNA LU 6.2. Nu este suportată.

Deoarece serverul de aplicație este responsabil pentru obligativitatea resurselor bazei de date, acesta este cel care dictează care mecanisme de securitate a rețelei trebuie să furnizeze solicitantul de aplicație. De exemplu, cu un solicitant de aplicație DB2 pentru VM trebuie să înregistrați cerințele de securitate la nivel de conversație ale serverului de aplicație în directorul de comunicații a solicitantului de aplicație prin setarea valorii corespunzătoare :etichetei de securitate, precum în Figura 23:

```

:nick.VSE1      :tpn.TOR3
                 :luname.TORGATE VSEGATE
                 :modename.IBMRDB
                 :security.PGM
                 :userid.SALESMGR
                 :password.PROFIT
                 :dbname.TORONT03

Unde: TOR3      - ID-ul tranzacției AXE mapată pe baza de date TORONT03.
      TORGATE   - Gateway de tip VM/APPC.
      VSEGATE   - Partiție APPLID a CICS/VSE® care servește ca gateway
                 pentru TORONT03.
      SALESMGR/PROFIT - USERID/PASSWORD definită în DFHSNT din
                 VSEGATE, și autorizată în TORONT03
      TORONT03  - Numele specificat în parametrul de pornire DBNAME atunci când
                 serverul de aplicație a DB2 pentru VSE a fost pornit (sau
                 numele bazei de date implicite determinată de către DBNAME
                 Director este DBNAME dacă a fost omis la pornire).

```

Figura 23. Exemplu de intrare în Directorul de Comunicații CMS

### Securitate a managerului de bază de date:

Translatarea ID-ului utilizator nu este suportată de către serverul de aplicație VSE. CICS folosește ID-ul utilizatorului transmis direct de la solicitant.

După pornirea de către un solicitant de aplicație, tranzacția AXE extrage ID-ul utilizatorului din CICS și îl transmite către serverul de tip DB2 pentru VSE. Pentru setarea nivelului cerut al autorității utilizatorului asupra resurselor bazei de date trebuie să actualizați ID-ul utilizatorului în catalogul de DB2 pentru VSE numit SYSTEM.SYSUSERAUTH.

Serverul de aplicație DB2 pentru VSE verifică dacă ID-ul utilizatorului dat de către CICS are autoritatea de CONNECT pentru accesarea bazei de date și respinge conexiunea dacă nu există această autoritate.

Ca proprietar al resurselor bazei de date, serverul de aplicație DB2 pentru VSE controlează funcțiile de securitate a bazei de date pentru obiectele de tip SQL care sunt rezidente pe serverul de aplicație de tip DB2 pentru VSE. Accesul la obiecte gestionate de către DB2 pentru VSE este controlat printr-un set de privilegii, care sunt acordate de către administratorul de sistem DB2 pentru VSE sau de către proprietarul acelui obiect particular. Serverul de aplicație de tip DB2 pentru VSE controlează două clase de obiecte:

- **Pachete:** Utilizatorii terminali individuali sunt autorizați pentru crearea, înlocuirea și rularea pachetelor cu instrucțiunea de tip DB2 pentru VSE GRANT. Atunci când un utilizator terminal crează un pachet, acel utilizator este în mod automat autorizat pentru a rula sau a înlocui un pachet. Alți utilizatori terminali trebuie să fie autorizat în mod specific

pentru a rula un pachet pe serverul de aplicație DB2 pentru VSE cu instrucțiunea GRANT. Privilegiul RUN poate fi acordat utilizatorilor terminali individuali sau către cei de tip PUBLIC, ceea ce permite tuturor utilizatorilor terminali rularea pachetului.

Atunci când o aplicație este preprocesată pe DB2 pentru VSE, pachetul conține instrucțiunile SQL conținute în programul aplicație. Aceste instrucțiuni SQL sunt clasificate ca:

- **SQL Static:** Aceasta înseamnă că instrucțiunea SQL și obiectele SQL referite de către instrucțiune sunt cunoscute la momentul când aplicația este preprocesată. Creatorul pachetului trebuie să aibă autoritatea de execuție a fiecărei instrucțiuni SQL statice din pachet.

Atunci când unui utilizator terminal îi este acordat privilegiul de execuție a pachetului, acel utilizator în mod automat are autoritatea de execuție a fiecărei instrucțiuni SQL statice conținute în pachet. Deci, utilizatorii terminali nu au nevoie de oricare privilegii ale tabeli DB2 pentru VSE dacă pachetul conține doar instrucțiuni SQL statice.

- **SQL dinamic:** Descrie o instrucțiune SQL care nu este cunoscută până când pachetul este rulat. Instrucțiunea SQL este construită de către program și este preprocesată dinamic în DB2 pentru VSE cu instrucțiunea SQL PREPARE sau cu instrucțiunea EXECUTE IMMEDIATE. Atunci când un utilizator terminal rulează o instrucțiune SQL dinamică, utilizatorul trebuie să aibă privilegiile tabeli necesare pentru execuția instrucțiunii SQL. Deoarece instrucțiunea SQL nu este cunoscută atunci când pachetul este creat, utilizatorului terminal nu îi este dat în mod automat autoritatea cerută de către proprietarul pachetului.

- **Obiecte SQL:** Acestea pot fi tabele, vederi și sinonime. Utilizatorilor DB2 pentru VSE le pot fi acordate diverse nivele de autoritate pentru crearea, ștergerea, schimbarea sau citirea obiectelor SQL individuale. Această autoritate este necesară pentru preprocesarea instrucțiunilor SQL statice sau pentru execuția instrucțiunilor SQL dinamice.

A se vedea cartea *DB2 Server for VSE System Administration* pentru o descriere a accesului privilegiat la serverul de aplicație de către solicitanții de aplicație de la distanță.

A se vedea *CICS on Open Systems: Intercommunication Guide* pentru cum se activează securitatea de legătură.

#### **Concepte înrudite:**

- “DB2 pentru VSE” la pagina 84

#### **Task-uri înrudite:**

- “Instalarea DB2 ca un server de aplicații (VSE)” la pagina 55

---

## Capitolul 13. Considerații de securitate pentru solicitanții de aplicații

---

### Considerații de securitate pentru solicitanții de aplicații (OS/390 și z/OS)

Când un sistem de la distanță realizează procesări asupra bazelor de date distribuite în numele unei aplicații SQL, el trebuie să fie capabil de a satisface cerințele de securitate ale solicitantului de aplicații, ale serverului de aplicații și ale rețelei care le conectează. Aceste cerințe se regăsesc în una sau mai multe din categoriile următoare:

- Numele utilizatorilor finali
- Securitatea rețelei
- Securitatea gestionării bazei de date
- Subsistemul de securitate

#### Concepte înrudite:

- “DB2 pentru OS/390 și z/OS” la pagina 67
- “Considerații de securitate pentru serverele de aplicații (OS/390 și z/OS)” la pagina 89

#### Task-uri înrudite:

- “Instalarea DB2 ca un solicitant de aplicații (OS/390 și z/OS)” la pagina 23

---

### Subconcepte

#### Nume utilizatori oprire - solicitant aplicație (OS/390 și z/OS)

Pe sistemele OS/390® și z/OS™, utilizatorilor oprire le este asignat un *ID utilizator* de 1 până la 8 caractere. Această valoare a ID-ului utilizator trebuie să fie unică în interiorul unui sistem particular OS/390 și z/OS, dar posibil ne-unic în rețea.

De exemplu, poate exista un utilizator numit JONES pe sistemul NEWYORK, și un alt utilizator numit JONES pe sistemul DALLAS. Dacă acești doi utilizatori sunt aceeași persoană, nu există nici un conflict. Totuși, dacă JONES din DALLAS este altul decât JONES din NEWYORK, rețeaua SNA network (și în consecință sistemele baza de date distribuită din rețea) nu pot distinge între JONES din NEWYORK și JONES din DALLAS. Dacă nu corecți această situație, JONES din DALLAS poate folosi privilegiile oferite lui JONES la sistemul NEWYORK.

Pentru a elimina conflictele de numire, DB2® oferă suport pentru translație nume utilizator oprire. Când o aplicație la solicitantul de aplicație DB2 face o cerere bază de date distribuită, DB2 efectuează translația numelui dacă baza de date comunicații specifică faptul că *translația nume ieșire* este necesară. Dacă translația nume ieșire este selectată, DB2 impune întotdeauna ca o parolă să fie trimisă cu fiecare cerere bază de date distribuită de ieșire.

Translația numelui de ieșire în DB2 este activată prin setarea coloanei USERNAMES din SYSIBM.LUNAMES sau tabelul SYSIBM.IPNames la valoarea 'O' sau 'B'. Dacă USERNAMES este setat la 'O', translația nume utilizator oprire este efectuată pentru cereri de ieșire. Dacă USERNAMES este setat la 'B', translația nume utilizator oprire este efectuată și pentru cererile de intrare și pentru cele de ieșire.

Deoarece autorizația DB2 depinde de ID-ul utilizatorului oprire și de cel al deținătorului DB2 pentru plan sau pachet, procesul de translație al numelui utilizator oprire este efectuat pentru ID-ul utilizator al utilizatorului oprire, ID-ul utilizator al deținătorului de plan și ID-ul utilizator al deținătorului de pachet.<sup>4</sup>Procesul de translație caută în tabelul SYSIBM.USERNAMES în următoarea secvență pentru a găsi un rând care să se potrivească cu unul din următoarele modele (TYPE.AUTHID.LINKNAME):

1. O.AUTHID.LINKNAME—O regulă de translație pentru un utilizator oprire specific către un sistem partener specific.
2. O.AUTHID.blank—O regulă de translație pentru un utilizator oprire specific către orice sistem partener.
3. O.blank.LINKNAME—O regulă de translație pentru orice utilizator oprire specific către un sistem partener specific.

Dacă nu este găsit nici un rând potrivit, DB2 respinge cererea bază de date distribuită. Dacă un rând este găsit, valoarea din coloana NEWAUTHID este folosită ca ID autorizație. (Un valoare NEWAUTHID spațiu indică faptul că numele original este folosit fără translație.)

Luați în considerare exemplul discutat mai devereme. Vreți să dați lui JONES din NEWYORK un nume diferit (NYJONES) când JONES face cereri bază de date distribuită la DALLAS. În exemplu, presupuneți că aplicația folosită de JONES este deținută de DSNPLAN (deținătorul de plan DB2), și nu aveți nevoie să translați acest ID-utilizator când acesta este trimis la DALLAS. Instrucțiunile SQL necesare pentru a oferi regulile de translație a numelui în CDB sunt arătate în Figura 24.

```

INSERT INTO SYSIBM.LUNAMES
  (LUNAME, SYSMODENAME, SECURITY_OUT, ENCRYPTPSWDS, MODESELECT, USERNAMES)
VALUES ('LUDALLAS', ' ', 'A', 'N', 'N', '0');
INSERT INTO SYSIBM.LOCATIONS
  (LOCATION, LINKNAME, LINKATTR)
VALUES ('DALLAS', 'LUDALLAS', '');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('0', 'JONES', 'LUDALLAS', 'NYJONES', 'JONESPWD');
INSERT INTO SYSIBM.USERNAMES
  (TYPE, AUTHID, LINKNAME, NEWAUTHID, PASSWORD)
VALUES ('0', 'DSNPLAN', 'LUDALLAS', ' ', 'PLANPWD');

```

Figura 24. SQL pentru Translație nume de ieșire (SNA)

Tabelele CDB rezultate sunt arătate în Figura 25 la pagina 105:

4. Dacă cererea este trimisă la un server DB2, translația numelui este de asemenea efectuată pentru deținătorul de pachet și deținătorul de plan. Numele deținătorilor de pachet și plan nu au niciodată parole asociate lor.

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				
TIP	AUTHID	LINKNAME	NEWAUTHID	PAROLĂ
0	JONES	LUDALLAS	NYJONES	JONESPWD
0	DSNPLAN	LUDALLAS		PLANPWD

Figura 25. Translație nume de ieșire

Figura 26 arată un exemplu mai simplu pentru conectarea la DB2 pentru OS/390 și z/OS DRDA<sup>®</sup> AS folosind o conexiune 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');

```

Figura 26. SQL pentru Translație nume de ieșire (exemplu simplu pentru SNA).

Figura 27 la pagina 106 arată un exemplu simplu pentru conectarea la DB2 pentru OS/390 și z/OS DRDA AS folosind o conexiune TCP/IP.

```

-- DB2 pentru 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')
;

```

Figura 27. SQL pentru Translație nume de ieșire (exemplu simplu pentru TCP/IP).

#### Concepte înrudite:

- “Considerații de securitate pentru solicitanții de aplicații (OS/390 și z/OS)” la pagina 103

## Securitate rețea - solicitant aplicație (OS/390 și z/OS)

După ce solicitantul de aplicație selectează numele utilizator oprire pentru a reprezenta aplicația la distanță, solicitantul de aplicație trebuie să ofere informațiile de securitate a rețelei LU 6.2 cerute. LU 6.2 oferă trei caracteristici de securitate a rețelei majore:

- Nivel securitate-sesiune, care este controlat de cuvântul cheie VERIFY prin instrucțiunea APPL VTAM®.
- Nivel securitate-conversație, care este controlat de conținutul tabelului SYSIBM.SYSLUNAMES.
- Criptarea datelor, care este suportată numai pentru edițiile VTAM 3.4 sau mai noi ale VTAM.

Deoarece serverul aplicație este responsabil pentru gestiunea resurselor bazei de date, serverul aplicație dictează care caracteristici de securitate a rețelei sunt cerute de la solicitantul de aplicație. Trebuie să înregistrați cerințele nive de securitate-conversație ale fiecărui server aplicație în tabelul SYSIBM.SYSLUNAMES prin setarea coloanei USERNAMES a tabelului SYSIBM.SYSLUNAMES să reflecte cerințele serverului aplicație.



Opțiunile de securitate a conversației SNA sunt:

### **SECURITY=SAME**

Aceasta este de asemenea cunoscută ca securitatea deja-verificată deoarece doar ID-ul utilizator al utilizatorului oprire este trimis către sistemul la distanță (nu se transmite nici o parolă). Folosiți acest nivel de securitate al conversației când coloana USERNAMES din SYSIBM.SYSLUNAMES nu conține 'O' sau 'B'.

Deoarece DB2<sup>®</sup> leagă translația numelui utilizator de securitatea conversației de ieșire, el nu vă permite să folosiți SECURITY=SAME când translația nume utilizator oprire de ieșire este activată.

### **SECURITY=PGM**

Aceasta cauzează trimiterea ID-ului și parolei utilizator la sistemul la distanță pentru validare. Folosiți această opțiune de securitate când coloana USERNAMES din tabelul SYSIBM.SYSLUNAMES conține ori 'O' ori 'B'.

În funcție de opțiunile specificate în tabelul SYSIBM.SYSLUNAMES DB2 obține parola utilizatorului oprire din două surse diferite:

- Parolele necriplate sunt obținute din coloana PASSWORD din tabelul SYSIBM.SYSUSERNAMES. DB2 extrage parolele din tabelul SYSIBM.SYSUSERNAMES când coloana ENCRYPTPSWDS din SYSIBM.SYSLUNAMES nu este setată la 'Y'. Parolele obținute din această sursă pot fi transmise către orice server aplicație DRDA.

Figura 28 definește parole pentru SMITH și JONES. Coloana LUNAME din exemplu conține spații, deci aceste parole sunt folosite pentru orice sistem la distanță SMITH ori JONES care încearcă accesul.

```
INSERAȚI ÎN SYSIBM.SYSUSERNAMES
(TIP, AUTHID, LUNAME, NEWAUTHID, PAROLĂ)
VALORI ('O', 'JONES', ' ', ' ', 'JONESPWD');
INSERAȚI ÎN SYSIBM.SYSUSERNAMES
(TIP, AUTHID, LUNAME, NEWAUTHID, PAROLĂ)
VALORI ('O', 'SMITH', ' ', ' ', 'SMITHPWD');
```

Figura 28. Trimiterea parolelor către Site-uri la distanță

- Parolele criplate sunt trimise la site-ul la distanță când coloana ENCRYPTPSWDS din SYSIBM.SYSLUNAMES conține 'Y'. Parolele criplate sunt extrase din RACF<sup>®</sup> (sau un produs echivalent RACF), și pot fi interpretate numai de un alt sistem DB2. La comunicarea cu un sistem non-DB2, nu setați ENCRYPTPSWDS la valoarea 'Y'.

DB2 caută în tabelul SYSIBM.SYSUSERNAMES pentru a determina ID-ul utilizator (valoare NEWAUTHID) pentru transmiterea către sistemul la distanță. Acest nume translatat este folosit pentru extragerea parolei RACF. Dacă nu doriți să translați nume, trebuie să creați rânduri în SYSIBM.SYSUSERNAMES care va face ca numele să fie trimise fără translatare. Figura 29 la pagina 108 permite cererilor să fie trimise la LUDALLAS și LUNYC fără translatarea numelui utilizatorului oprire (ID utilizator).

```

INSERAȚI ÎN SYSIBM.SYSUSERNAMES
(TIP, AUTHID, LUNAME, NEWAUTHID, PAROLĂ)
VALORI ('0', ' ', 'LUNYC', ' ', ' ');
INSERAȚI ÎN SYSIBM.SYSUSERNAMES
(TIP, AUTHID, LUNAME, NEWAUTHID, PAROLĂ)
VALORI ('0', ' ', 'LUDALLAS', ' ', ' ');

```

Figura 29. Trimitere parole criptate către Site-uri la distanță.

#### SECURITY=NONE

Această opțiune nu este suportată de DRDA, deci DB2 nu are rezerve pentru această opțiune de securitate.

#### Concepte înrudite:

- “Considerații de securitate pentru solicitanții de aplicații (OS/390 și z/OS)” la pagina 103

## Securitate manager bază de date - solicitant de aplicație (OS/390 și z/OS)

Un mod în care solicitantul de aplicație poate participa la securitatea bazei de date distribuite este prin translația numelor. Puteți folosi translația numelui de intrare pentru a controla accesul la fiecare server aplicație, bazându-vă pe identitatea utilizatorului oprire care face cererea și a aplicației care face cererea. Alte moduri în care solicitantul de aplicație DB2® contribuie la securitatea sistemului distribuit sunt:

#### Legarea aplicațiilor la distanță

Utilizatorii oprire leagă aplicații la distanță pe serverul aplicație cu comanda DB2 BIND PACKAGE command. DB2 nu restricționează folosirea comenzii BIND PACKAGE la solicitant. Totuși, un utilizator oprire nu poate folosi un pachet la distanță până când pachetul este inclus într-un plan DB2. DB2 restricționează folosirea comenzii BIND PLAN. Un utilizator oprire nu poate adăuga pachetul la distanță la un plan decât dacă i se oferă privilegiile BIND sau BINDADD cu instrucțiunea DB2 GRANT.

WCând legați un pachet, folosiți opțiunea ACTIVARE/DEZACTIVARE pentru a specifica dacă pachetul va fi folosit de TSO, CICS/ESA, IMS/ESA, sau un subsistem DB2 la distanță.

#### Executare aplicații la distanță

Pentru ca utilizatorul oprire DB2 să ruleze o aplicație la distanță, el trebuie să aiba autorizație să ruleze planul DB2 asociat cu acea aplicație. Deținătorul de plan DB2 are în mod automat autorizația să ruleze planul. Altor utilizatori oprire li se poate oferi autorizația să ruleze planul cu instrucțiunea DB2 GRANT EXECUTE. În acest fel, deținătorul unei aplicații bază de date distribuite poate controla folosirea aplicației pentru fiecare utilizator.

#### Concepte înrudite:

- “Considerații de securitate pentru solicitanții de aplicații (OS/390 și z/OS)” la pagina 103

---

## Subsistem de securitate - solicitant de aplicație (OS/390 și z/OS)

Subsistemul de securitate extern pe sistemele MVS™ este oferit de RACF® și alte produse care oferă o interfață compatibile RACF. Solicitantul de aplicație DB2® nu are apeluri directe către subsistemul de securitate extern, cu excepția suportului parolei criptate. Totuși, subsistemul de securitate extern este folosit indirect la solicitantul de aplicație în următoarele situații:

- Produsul responsabil pentru atașarea utilizatorului oprire la DB2 folosește subsistemul de securitate extern pentru a valida identitatea utilizatorului oprire (ID utilizator și parolă). Aceasta se întâmplă înainte ca utilizatorul oprire să fie atașat la DB2. Așa cum este declarat anterior, CICS/ESA, TSO, și IMS/ESA<sup>®</sup> sunt exemple de produse care atașează utilizatori oprire la DB2.
- Dacă folosiți un nivel de securitate-sesiune SNA (prin cuvântul cheie VERIFY în instrucțiunea APPL DB2 VTAM<sup>®</sup>), subsistemul de securitate extern este invocat de VTAM pentru a valida identitatea sistemului la distanță.

#### **Concepte înrudite:**

- “Considerații de securitate pentru solicitanții de aplicații (OS/390 și z/OS)” la pagina 103

---

## **Considerații de securitate pentru utilizatorii aplicației (iSeries)**

Atunci când un sistem de la depărtare produce procesare de bază de date distribuită în numele unei aplicații SQL, acesta trebuie să fie capabil să satisfacă cerințele de securitate ale unui solicitant al aplicației, pentru un server de aplicație și pentru rețeaua care le conectează. Aceste cerințe aparțin uneia sau mai multor categorii care urmează:

- Nume de utilizatori finali
- Parametri de securitate a rețelei
- Securitate pentru manager bază de date
- Securitate forțată de securitatea iSeries<sup>™</sup>

#### **Nume de utilizatori finali:**

Pe sistemele iSeries, utilizatorilor finali le sunt atașate un ID utilizator de la 1 la 10 caractere, acest ID fiind unic pe acel sistem, dar nu neapărat unic în cadrul rețelei. Acest ID utilizator este cel dat sistemului de la distanță atunci când conexiunea este realizată între două baze de date. Pentru a evita conflictele între ID-urile utilizatorilor pe sistemele din rețea, translatarea numelui de la distanță este deseori folosită pentru a modifica ID-ul utilizatorului pentru a rezolva conflictul înainte ca acesta să fie trimis în rețea.

Totuși, sistemul iSeries nu furnizează nici o translatare de nume de la distanță pentru a rezolva eventualele conflicte la server. Aceste conflicte trebuie rezolvate la serverul de aplicație, în cazul în care nu se folosesc clauzele suplimentare USER și USING în instrucțiunea iSeries SQL CONNECT statement. USER este un ID valid pe serverul de aplicație și USING este parola corespunzătoare pentru utilizator.

#### **Securitatea rețelei:**

După ce solicitantul aplicației selectează numele de utilizatori finali pentru a reprezenta aplicația de la distanță, trebuie apoi să furnizeze informațiile de securitate de rețea LU 6.2 cerute. LU 6.2 furnizează trei mari caracteristici de securitate a rețelei:

- Securitate nivel-sesiune, controlată de cuvântul cheie LOCPWD în comanda CRTDEVAPP
- Securitate nivel-conversație, controlată de sistemul de operare OS/400<sup>®</sup>
- Criptarea, care nu e suportată pe sistemul de operare OS/400

Securitatea la nivel-sesiune este furnizată prin verificare LU-la-LU. Fiecare LU are o cheie care trebuie să se potrivească cu cheia de la LU-ul de la distanță. Cheia se specifică la cuvântul cheie LOCPWD la comanda CRTDEVAPP.

Pentru că serverul de aplicație este responsabil pentru dirijarea resurselor bazei de date, serverul aplicație dictează care caracteristici de securitate a rețelei sunt cerute pentru solicitantul aplicației. Administratorul cu securitatea iSeries trebuie să verifice cerințele de securitate pentru fiecare server de aplicație astfel încât să nu ceară mai mult decât suportă solicitantul de aplicație iSeries.

Următoarele sunt posibile opțiuni de securitate conversație SNA:

#### **SECURITY=SAME**

De asemenea cunoscută ca securitate deja verificată. Este trimis numai ID-ul utilizator al unui utilizator de aplicație la un sistem de la distanță. Nu este trimisă nici o parolă. Înainte de AS/400® Versiunea 2 Livrarea 2 Modificarea 0, acest nivel de securitate de conversație a fost singurul nivel suportat de un solicitant de aplicație iSeries.

#### **SECURITY=PGM**

Cauzează trimiterea ID-ului utilizatorului și parola aplicației să fie trimisă la sistemul de la distanță pentru validare. Înaintea versiunii 2, ediția 2, modificarea 0, AS/400, această opțiune de securitate nu a fost suportată de solicitantul de aplicație iSeries.

#### **SECURITY=NONE**

Nu este suportată atunci când iSeries este un solicitant de aplicație iSeries.

#### **Securitate manager bază de date:**

Sistemul iSeries nu are un subsistem de securitate extern. Toată securitatea este mânăuită prin sistemul de operare OS/400.

#### **Securitate de sistem:**

Sistemul de operare OS/400 controlează autorizarea la toate obiectele de pe sistem, incluzând programe, pachete, tabele, vederi și colecții.

Solicitantul aplicației controlează autorizarea la obiectele care sunt implicate de solicitantul aplicației. Securitatea pentru obiecte de pe serverul de aplicație este controlată la serverul de aplicație, pe baza căruia este trimis ID-ul utilizatorului de la solicitantul aplicației. ID-ul utilizator trimis la serverul de aplicație este asociat cu utilizatorul aolantului aplicației iSeries sau ID-ul utilizator dat în clauza USER a instrucțiunii iSeries SQL CONNECT. De exemplu, CONNECT TO *numerd* USER *ID utilizator* USING *parolă*.

Securitatea obiectelor poate fi dirijată folosind comenzile CL de autoritate obiect sau cu instrucțiunile SQL GRANT și REVOKE. Comenzile de autoritate CL obiect includ Garantare autoritate obiect (GRTOBJAUT) și Revocare autoritate obiect (RVKOBJAUT). Aceste comenzi lucrează pe orice obiect de pe sistem. Instrucțiunile GRANT și REVOKE lucrează numai pe obiectele SQL: tabele, vizualizări și pachete. Dacă este nevoie să se modifice autorizarea pentru alte obiecte cum ar fi programe sau colecții, se utilizează comenzile GRTOBJAUT și RVKOBJAUT.

Atunci când sunt create obiecte, le sunt date o autorizație implicită. Implicit, creatorul unei tabele, vizualizări sau al unui program are toate autorizările pe aceste obiecte. De asemenea, implicit, public este dată aceeași autorizare pe acele obiecte ca cea pe care acestea o au în librăria de obiecte sau în colecție.

Pentru mai multe informații asupra securității de sistem, a se vedea *OS/400 Security - Reference*.

#### **Concepte înrudite:**

- “Considerații de securitate pentru servere de aplicații (iSeries)” la pagina 94
- “DB2 UDB pentru iSeries” la pagina 74

**Task-uri înrudite:**

- “Instalarea DB2 ca un solicitant de aplicații – SNA (iSeries)” la pagina 29
- “Acordarea și revocarea autorității (iSeries)” la pagina 111

## Acordarea și revocarea autorității (iSeries)

**Procedură:**

Pentru acordarea autorității \*USE utilizatorului USER1 d a programa PGMA pe un sistem iSeries:

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

Pentru a revoca aceeași autoritate:

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

\*PGM identifică tipul obiectului din acest exemplu ca un program. \*SQLPKG este folosit pentru a opera asupra unui pachet, \*LIB este folosită pentru o colecție și \*FILE este folosită pentru o tabelă.

GRTOBJAUT și RVKOBJAUT pot fi de asemenea folosite pentru a preveni utilizatorii de la a crea programe și pachete. Atunci când autoritatea este revocată de la oricare comandă CRTSQLxxx (unde xxx = RPG, C, CBL, FTN sau PLI) folosită pentru crearea programelor, un utilizator nu mai poate crea programe. Dacă autoritatea este revocată asupra comenzii CRTSQLPKG utilizatorul nu mai poate crea pachete pornind de la solicitantul de aplicație sau de la serverul de aplicație.

De exemplu, se introduce următoarea comandă pe un sistem iSeries pentru a acorda autoritatea \*USE utilizatorului USER1 asupra comenzii CRTSQLPKG:

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

Aceasta afectează execuția crtsqlpkg asupra solicitantului de aplicație. Pe serverul de aplicație această comandă permite crearea de pachete.

Comanda pentru a revoca aceeași autoritate este:

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

**Concepte înrudite:**

- “Considerații de securitate pentru servere de aplicații (iSeries)” la pagina 94
- “Considerații de securitate pentru utilizatorii aplicației (iSeries)” la pagina 109
- “DB2 UDB pentru iSeries” la pagina 74

## Considerente de securitate pentru solicitanții de aplicații (VM)

Atunci când un sistem aflat la distanță execută procesare pe baze de date distribuite în numele unei aplicații SQL, acesta trebuie să poată fi în măsură să satisfacă cerințele de securitate ale unui server de aplicații, ale solicitantului de aplicație și ale rețelei care le conectează. Aceste cerințe cad într-una sau mai multe dintre următoarele categorii:

- Nume de utilizator terminal
- Parametrii de securitate a rețelei

- Securitatea managerului de bază de date
- Securitate impusă de către un subsistem de securitate extern

#### Nume de utilizatori terminali:

Atât în SQL cât și în LU 6.2, utilizatorilor terminali le sunt asignate ID-uri de utilizator de 1-până la 8- caractere. Această valoare a ID-ului de utilizator trebuie să fie unică într-un sistem de operare patricular, dar nu este necesară unică în rețeaua SNA.

De exemplu, poate exista un utilizator numit JONES în sistemul TORONTO și un alt utilizator numit JONES în sistemul MONTREAL. Dacă acești doi utilizatori sunt aceeași persoană, nu există nici un conflict. Cu toate acestea, dacă JONES din TORONTO nu este aceeași persoană ca și JONES din MONTREAL, rețeaua SNA (și implicit sistemele de baze de date distribuite din cadrul acelei rețele) nu pot distinge între JONES din TORONTO și JONES din MONTREAL. Dacă nici un pas nu este luat pentru prevenirea acestei situații, JONES din TORONTO poate folosi privilegiile acordate lui JONES din MONTREAL și vice versa.

Pentru a elimina conflictele de nume, DB2<sup>®</sup> pentru VM furnizează suport pentru translatarea de nume de utilizator terminal. Cu toate acestea, sistemul nu impune translatarea ID-urilor utilizator. Dacă translatarea impusă de sistem este necesară, ar trebui să vă asigurați că transtarea de intrare corespunzătoare este realizată pe serverul de aplicație.

*Translatarea de ieșire* este realizată folosind CMS Communications Directory. O intrare în CMS Communications Directory trebuie să specifice :security.PGM. În acest caz, valorile corespunzătoare din etichetele :userid și :parolă curg către site-ul de la distanță (serverul de aplicație) din cererea de conexiune.

Prin crearea intrării din Figura 30, utilizatorul cu ID-ul JONES de pe sistemul local (TORONTO) este mapat pe ID-ul de utilizator JONEST atunci când acesta se conectează la serverul de aplicație MONTREAL\_SALES\_DB de pe sistemul MONTREAL. În acest fel ambiguitatea de ID-uri de utilizator este eliminată.

```

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

```

Figura 30. Translatarea de Nume de Ieșire

#### Securitatea rețelei:

Prin selectarea numelui de utilizator terminal care reprezintă cererea de aplicație de pe sistemul de la distanță (serverul de aplicație), solicitantul de aplicație trebuie să furnizeze informațiile de securitate a rețelei LU 6.2 necesare. LU 6.2 furnizează trei mecanisme de securitate a rețelei majore:

- Securitatea de nivel sesiune, specificată folosind parametrul VERIFY al instrucțiunii VTAM<sup>®</sup> APPL.
- Securitatea de nivel conversație, specificată în CMS Communications Directory.
- Criptarea.

Deoarece serverul de aplicație este responsabil pentru gestiunea resurselor bazei de date, serverul de aplicație este cel care dictează pe care mecanisme de securitate a rețelei solicitantul de aplicație trebuie să le furnizeze. Trebuie să înregistrați cerințele de securitate ale serverului de aplicație în directorul de comunicații ale solicitantului de aplicație prin setarea valorii corespunzătoare a etichetei de securitate .:

Opțiunile de securitate ale nivelului conversație SNA suportate de către DRDA® sunt:

#### **SECURITY=SAME**

Aceasta este de asemenea cunoscută și ca securitate deja-verificată deoarece doar ID-urile de utilizatori terminali sunt trimise către sistemul de la distanță. Parola nu este trimisă. Acest nivel de securitate a conversației este folosit atunci când :security.SAME este specificată în directorul de comunicații al solicitantului de aplicație pentru acel server de aplicație. Atunci când această opțiune este folosită, translatarea numelui de utilizator terminal de ieșire nu este executată. ID-ul de utilizator trimis către site-ul DRDA de la distanță este ID-ul de logare al utilizatorului CMS. Eticheta :userid din CMS Communications Directory este ignorată pentru :security.SAME.

#### **SECURITY=PGM**

Această opțiune cauzează ca atât ID-ul utilizatorului terminal cât și parola să fie trimise către sistemul de la distanță (serverul de aplicație) pentru validare. Această opțiune de securitate este folosită atunci când :security.PGM este specificată în intrarea CMS Communications Directory a solicitantului de aplicație. Atunci când această opțiune este folosită, translatarea numelui de utilizator terminal de ieșire este executată.

DB2 pentru VM nu suportă criptarea parolei. Parola poate fi specificată în eticheta :parolă sau poate fi stocată în intrarea directorului CP al utilizatorului terminal folosind o instrucțiune a directorului APPCPASS. Instrucțiunea APPCPASS este recomandată dacă doriți maximizarea securității parolei. Dacă parola nu este specificată în intrarea CMS Communications Directory, intrarea directorului (VM) de sistem al utilizatorului este cău tată pentru o instrucțiune APPCPASS.

#### **Instrucțiunea APPCPASS:**

VM furnizează instrucțiunea APPCPASS pentru maximizarea securității ID-ului de utilizator și a parolei folosite de către solicitantul de aplicație pentru conectarea la un server de aplicație. APPCPASS este flexibilă în aceea că vă permite stocarea informațiilor de securitate într-unul dintre următoarele moduri:

- **ID utilizator și parolă:** În acest caz etichetele :userid și :parolă din CMS Communications Directory trebuie să fie setate la spațiu liber.
- **Doar ID utilizator:** În acest caz eticheta :userid din CMS Communications Directory trebuie să fie setată la spațiu liber și eticheta :parolă trebuie să fie setată la parola utilizatorului.
- **Doar parolă:** În acest caz eticheta :parolă din CMS Communications Directory trebuie să fie setată la spațiu liber și eticheta :userid trebuie să fie setată la ID-ul utilizatorului.

Figura 31 la pagina 114 ilustrează cazul în care ID-ul utilizatorului este stocat în directorul de comunicații al utilizatorului și parola este stocată în intrarea directorului VM al utilizatorului. În intrarea directorului de comunicații ID-ul utilizatorului este setat la MTLSSOU, dar parola nu este setată. Parola este stocată în intrarea directorului VM al utilizatorului.



```
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
```

Figura 31. Exemplu de o intrare în directorul de comunicații fără o parolă

Atunci când APPC/VM inițiază conexiunea între solicitantul de aplicație și serverul de aplicație folosind conversația SECURITY=PGM, acesta citește valorile etichetelor :userid și :parolă și le transmite către serverul de aplicație. Dacă una dintre aceste etichete este setată la spațiu liber, acesta caută intrarea directorului VM al utilizatorului pentru informațiile lipsă. În acest caz trebuie să aveți o instrucțiune APPCPASS în intrarea directorului VM după cum urmează:

```
APPCPASS TORGATE MTLGATE MTLYOU Q6VBN8XP
```

Această instrucțiune spune lui APPC/VM faptul că utilizatorul (solicitantul de aplicație) care solicită conexiunea prin poarta (gateway) TORGATE a AVS (local), partenerul LU numit MTLGATE, și ID-ul de utilizator MTLYOU ar trebui să trimită parola Q6VBN8XP către serverul de aplicație. Utilizatorul este cunoscut prin aceste două bucăți de identificare de pe serverul de aplicație.

Plasarea instrucțiunii APPCPASS în directorul VM nu este o operație a utilizatorului terminal. Utilizatorul terminal trebuie să plaseze o cerere cu programatorul de sistem VM pentru a realiza acest lucru.

Pentru mai multe informații despre securitatea de nivel conversație și pentru instrucțiunea APPCPASS a se face referire la *VM/ESA Connectivity Planning, Administration, and Operation*.

**Securitatea managerului de bază de date:**

Ca parte a cadrului de lucru a securității bazei de date distribuite generale din DRDA, solicitantul de aplicație poate juca un rol în controlarea căror utilizatori terminali le sunt permisi execuția cererilor de baze de date distribuite. În DB2 pentru VM, solicitantul de aplicație poate participa la securitatea bazei de date distribuite în trei moduri:

**Translatarea numelui de utilizator de ieșire**

Se poate folosi translatarea numelui de utilizator de ieșire pentru controlarea accesului la un server de aplicație particular, bazându-ne pe identitatea utilizatorului terminal care execută cererea. DB2 pentru VM încearcă translatarea numelui de utilizator terminal înainte de trimiterea cererii către site-ul de la distanță. Cu toate acestea, cea mai bună metodă este de a pune serverul de aplicație să execute verificarea sursei și a translatării de intrare, deoarece utilizatorii solicitanți de aplicație VM pot în cele din urmă să suprascrie translatarea de ieșire cu propriul Director de Comunicații al Utilizatorului CMS.

**Preprocesarea aplicației**

Aplicațiile de la distanță de preprocesare a utilizatorilor terminali către un server de aplicație particular prin folosirea lui DB2 pentru VM SQLPREP EXEC sau a comenzii Utilitarului de Servicii a Bazei de Date (Database Service Utility) (DBSU)



RELOAD PACKAGE. DB2 pentru VM nu restricționează utilizarea acestor servicii. Atunci când un utilizator terminal procesează o aplicație, acel utilizator este cel care deține pachetul rezultat.

#### **Execuția de aplicație**

Pentru ca utilizatorul terminal al DB2 pentru VM să ruleze o aplicație de la distanță, utilizatorul terminal trebuie să aibă autoritatea asupra site-ului de la distanță (server de aplicație) pentru rularea pachetului de la distanță asociat cu aplicația particulară. Creatorul (proprietarul) pachetului este în mod automat autorizat să ruleze pachetul. Alți utilizatori terminali pot obține autoritatea de a rula pachetul cu instrucțiunea de execuție a DB2 pentru VM GRANT. În acest mod, proprietarul unei aplicații de bază de date distribuită poate controla utilizarea aplicației pe baze de utilizator-la-utilizator.

#### **Subsistemul de securitate:**

Subsistemul de securitate extern de pe sistemul VM este furnizat fie de către RACF® sau alți producători echivalenți care furnizează o interfață compatibilă cu RACF. Solicitantul de aplicație al DB2 pentru VM nu interferează direct cu subsistemul de securitate extern. Subsistemul de securitate extern nu este folosit pentru a furniza parole pentru securitatea de nivel conversație. Dacă alegeți folosirea securității de nivel sesiune, subsistemul de securitate extern este apelat de către VTAM pentru validarea identității numelui LU de la distanță în timpul verificării LU a partenerilor.

#### **Concepte înrudite:**

- “Cosiderații de securitate pentru serverele de aplicații (VM)” la pagina 97
- “DB2 pentru VM” la pagina 74

#### **Task-uri înrudite:**

- “Setarea pentru DB2 ca un solicitant de aplicație (VM)” la pagina 35



---

## Capitolul 14. Reprezentarea datelor

---

### Reprezentarea datelor (OS/390 și z/OS)

DB2<sup>®</sup> este livrat cu un set de caractere instalat implicit (CCSID). Această valoare implicită nu este probabil corectă pentru instalarea dumneavoastră.

La instalarea DB2, trebuie să setați instalarea CCSID la CCSID al caracterelor generate și trimise către DB2 de către dispozitivele de intrare din site-ul dumneavoastră. Acest CCSID (set de caractere implicit) este în general determinat de limba națională pe care o folosiți. Dacă instalarea CCSID nu este corectă, conversia caracterelor va produce rezultate incorecte.

Asigurați-vă că subsistemul dumneavoastră DB2 are abilitatea de a converti CCSID (setul de caractere implicit) de la oricare server de aplicații către CCSID (setul de caractere) instalat pe subsistemul DB2 al dumneavoastră. DB2 furnizează tabele de conversie pentru cele mai comune combinații de CCSID (seturi de caractere) sursă și destinație, dar nu pentru toate combinațiile posibile. Puteți adăuga mulțimii tabelor de conversie disponibile tabelele și rutinele de conversie de care aveți nevoie.

Vedeți *Ghidul de administrare al bazelor de date universale DB2™ pentru OS/390® și z/OS™* pentru mai multe informații despre DB2 UDB pentru conversia de caractere la OS/390 și z/OS.

#### Concepte înrudite:

- “DB2 pentru OS/390 și z/OS” la pagina 67
- “Conversion of character data” în *Quick Beginnings for DB2 Connect Enterprise Edition*

#### Task-uri înrudite:

- “Instalarea DB2 ca un server de aplicații (OS/390 și z/OS)” la pagina 43
- “Instalarea DB2 ca un solicitant de aplicații (OS/390 și z/OS)” la pagina 23

---

### Reprezentarea datelor (iSeries)

Produsele ce suportă DRDA<sup>®</sup> realizează automat orice conversie necesară la serverul de aplicații. Pentru a se întâmpla acest lucru, valoarea CCSID a serverului de aplicații trebuie să fie o valoare suportabilă de către solicitantul de aplicații pentru conversație.

Valoarea CCSID livrată implicit pentru OS/400<sup>®</sup> este 65535, referită de asemenea și ca X'FFFF'. Această valoare implicită nu este compatibilă cu toate celelalte produse IBM<sup>®</sup>. Sistemul CCSID poate fi afișat prin comanda CL DSPSYSVAL QCCSID. Poate fi schimbată prin comanda CHGSYSVAL. De exemplu, CHGSYSVAL QCCSID VALUE(37). CCSID-ul sistemului poate fi de asemenea înlocuit de CCSID-ul asociat cu serverul de joburi DRDA. CCSID poate fi setat prin comanda CL CHGUSRPRF. De exemplu, CHGUSRPRF MYUSERID CCSID(37).

#### Servere de aplicații:

Pe un server de aplicații, trebuie să aveți în vedere CCSID-ul asociat cu:

#### Jobul de servire în subsistemul de comunicații

CCSID-ul jobului de servire al dumneavoastră trebuie să fie compatibil cu

solicitantul de aplicații. Acest CCSID este stabilit de profilul utilizatorului al identificadorului de utilizator care solicită conexiunea. Suportul pentru controlul funcționării al OS/400 inițializează CCSID-ul jobului la CCSID-ul din profilul utilizatorului. Dacă în profilul utilizatorului nu există un CCSID, suportul de control al funcționării ia CCSID-ul (QCCSID) din valoarea sistemului. Valoarea de sistem QCCSID este inițial setată la CCSID 65535.

Înainte de inițierea unei cereri către DB2® UDB pentru iSeries™, trebuie să vă înregistrați și să schimbați profilul utilizatorului (Change User Profile) (CHGUSRPRF) pentru a asigura valoarea CCSID acceptabilă profilului utilizator al jobului care va servi cererea DRDA.

### **Colecții SQL**

O colecție SQL constă într-o bibliotecă de obiecte OS/400, un jurnal, un receptor jurnal și, opțional, un dicționar de date IDDU, dacă este specificată clauza WITH DATA DICTIONARY în declarația CREATE COLLECTION. Fișierele fizice și logice folosite pentru unele din aceste obiecte recurg implicit la CCSID-ul jobului din momentul creării. Dacă interogați dicționarul de date sau catalogul de pe un solicitant de aplicații care nu suportă valoarea CCSID-ul acestor fișiere, s-ar putea să vedeți date ne-afișabile sau distorsionate. Sau s-ar putea ca solicitantul de aplicații să emită un mesaj care să spună că valoarea CCSID nu este suportată. Pentru corectarea acestui lucru, trebuie să creați o nouă colecție SQL cu o valoare CCSID de job acceptabilă pentru celălalt sistem.

CCSID-ul jobului poate fi schimbat folosind comanda Change Job (CHGJOB). Sau pentru joburile următoare, folosiți comanda de schimbare a profilului utilizatorului (Change User Profile) (CHGUSRPRF) pentru a schimba valoarea CCSID a profilului utilizatorului. Într-un program CL, folosiți comanda de extragere a atributelor jobului (Retrieve Job Attributes) (RTVJOBA) pentru a obține CCSID-ul jobului curent. În mod interactiv, folosiți comanda de lucru cu jobul (Work with Job) (WRKJOB) și selectați opțiunea 2, Afișează atributele de definiție ale jobului pe displayul comenzii Work with Job.

### **Tabele SQL și alte fișiere DB2 UDB pentru iSeries accesate prin DRDA**

Un tabel SQL corespunde unui fișier fizic DB2 UDB pentru iSeries conținut într-o bibliotecă cu același nume ca și colecția dumneavoastră. Coloanele unui tabel corespund de asemenea câmpurilor de definiție dintr-un fișier fizic. Valorile CCSID pentru tabele sau coloane ale tabelului pot să nu fie compatibile cu solicitantul de aplicații. O sursă importantă de incompatibilități CCSID în versiunile OS/400 înainte de Versiunea 3 Release 1 era faptul că multe fișiere și tabele SQL erau etichetate cu valoarea CCSID 65535 implicit. În Versiunea 3 Release 1 și realizările următoare, CCSID-urile acestor fișiere se schimbă automat la unele valori mai potrivite.

### **Solicitanții de aplicații:**

Pe un solicitant de aplicații, trebuie să aveți în vedere CCSID-ul asociat cu:

#### **Jobul solicitant**

Suportul pentru control funcționare al OS/400 inițializează CCSID-ul jobului la CCSID-ul din profilul utilizatorului. Dacă valoarea CCSID din profilul utilizatorului este \*SYSVAL, suportul de control al funcționării ia CCSID-ul din valoarea sistemului - QCCSID. Valoarea de sistem QCCSID este inițial setată la 65535. Folosirea valorii 65535 pentru CCSID-ul joburilor ce servesc pentru încercări de conectare de la DB2 Universal Database™ va duce la eșuarea încercărilor de conectare. Schimbarea valorii sistem QCCSID afectează întregul sistem, de aceea acțiunea recomandată este schimbarea CCSID-ul din profilul utilizatorului pentru jobul sub care rulează jobul server. Setati CCSID-ul din profilul utilizatorului la o

valoare corespunzătoare. De exemplu, folosiți CCSID 37 pentru US English. În general, alegerea corectă este să folosiți identificatorul implicit al setului de caractere pentru iSeries la care vă conectați.

CCSID-ul jobului poate fi schimbat folosind comanda (Change Job) (CHGJOB). Sau pentru joburile următoare folosiți comanda de schimbare a profilului utilizatorului (Change User Profile) (CHGUSRPRF) pentru a schimba valoarea CCSID din profilul utilizatorului. Pentru a vedea care CCSID este funcțional pentru un job, într-un program CL, folosiți comanda de extragere a atributelor jobului (Retrieve Job Attributes) (RTVJOBA) pentru a obține CCSID-ul jobului curent. În mod interactiv, folosiți comanda de lucru cu jobul (Work with Job) (WRKJOB) și selectați opțiunea 2, Afișează atributele de definiție ale jobului pe displayul comenzii Work with Job.

### **Baza de date cu fișierele fizice al bazei de date**

Fișierele fizice recurg în mod implicit la CCSID-ul jobului implicit (care poate fi diferit de CCSID-ul jobului) în momentul creării fișierului dacă nu se specifică explicit în comada de creare fișier fizic (Create Physical File) (CRTPF) sau de creare fișier fizic sursă (Source Physical File) (CRTSRCPF). Înainte de DB2 pentru AS/400® V3R1, valoarea implicită era CCSID-ul jobului, care era adesea 65535 și necorespunzătoare pentru utilizare DRDA. CCSID-ul implicit al jobului nu este niciodată 65535 și de aceea este o alegere mai bună pentru CCSID-ul fișierelor fizice accesate prin DRDA.

Puteți folosi comanda de afișare a descrierii fișierului (DSPFD) pentru a vedea CCSID-ul unui fișier sau comanda de afișare a descrierii câmpurilor unui fișier (DSPFFD) pentru vizualizarea CCSID-urile câmpurilor unui fișier.

Folosiți comanda de schimbare a unui fișier fizic (Change Physical File) (CHGPF) pentru a schimba CCSID-ul unui fișier fizic. Un fișier fizic nu poate fi întotdeauna schimbat dacă există una sau mai multe din următoarele condiții:

- Fișiere logice sunt definite peste fișiere fizice. În acest caz, este nevoie să faceți următoarele:
  1. Salvați fișierele logice și fizice, împreună cu căile lor de acces.
  2. Tipăriți o listă de autorizări pentru fișierele logice (DSPOBJAUT).
  3. Ștergeți fișierele logice.
  4. Schimbați fișierele fizice.
  5. Restaurați fișierele fizice și logice împreună cu căile lor de acces peste fișierele fizice schimbate.
  6. Acordați autorizări private fișierelor logice (vedeți lista tipărită).
- Fișierelor și câmpurilor li se alocă explicit o valoare CCSID. Pentru a schimba un fișier fizic cu CCSID asignat la nivel de câmp, creați din nou fișierul fizic și copiați datele în noul fișier folosind parametrul FMTOPT(\*MAP) în comanda de copiere fișier (CPYF).
- Formatele înregistrărilor sunt partajate într-o versiune a OS/400 înainte de versiunea Version 3 Release 1.

### **Concepte înrudite:**

- “DB2 UDB pentru iSeries” la pagina 74
- “Conversion of character data” în *Quick Beginnings for DB2 Connect Enterprise Edition*

### **Task-uri înrudite:**

- “Instalarea DB ca un server de aplicații folosind SNA (iSeries)” la pagina 47
- “Instalarea DB2 ca un solicitant de aplicații – SNA (iSeries)” la pagina 29

---

## Reprezentarea datelor (VM)

Trebuie să alegeți cele mai corespunzătoare valori implicite CHARNAME și CCSID pentru instalarea proprie. Folosirea valorilor celor mai corespunzătoare asigură integritatea reprezentării datelor de tip caracter și reduce regia de performanță asociată cu conversia CCSID.

### Servere de aplicații:

De exemplu, dacă DB2-ul propriu<sup>®</sup> pentru serverul de aplicație VM este accesat doar de către utilizatori locali ai căror controllere de terminal sunt generate cu pagina de cod 37 și setul de caractere 697 (CP/CS 37/697) pentru caracterele US ENGLISH atunci ar trebui să setați valoarea implicită CHARNAME a serverului de aplicație la valoarea de ENGLISH. Aceasta deoarece CP/CS 37/697 corespunde lui CCSID de valoare 37, care corespunde lui CHARNAME de valoare ENGLISH.

Pentru eliminarea conversiei CCSID nenecesare se alege o valoare implicită CCSID a serverului de aplicație astfel încât aceasta să fie aceeași cu valoarea lui CCSID a solicitantului de aplicație care accesează serverul de aplicație propriu cel mai des.

Ceea ce urmează este un exemplu a cum aceste două scopuri pot fi situate în conflict:

- Un server de aplicație are mai puțin de cinci solicitanți de aplicație care sunt locali (pentru solicitanții de aplicație VM parametrul protocolului ar trebui să fie setat la SQL/DS) și mulți (în jur de 100) solicitanți de aplicație care accesează serverul de aplicație folosind protocolul DRDA<sup>®</sup>. Solicitanții de aplicație locali au controllere care sunt definite cu CP/CS 37/697. Solicitanții de aplicație de la distanță folosesc CCSID 285.

Dacă valoarea implicită CHARNAME a serverului de aplicație este setată la valoarea de ENGLISH, aceasta ține integritatea datelor pentru solicitanții de aplicație locali, dar regia de conversie CCSID crește pentru toți solicitanții de aplicație de la distanță.

Dacă valoarea implicită CHARNAME a serverului de aplicație este setată la valoarea de UK-ENGLISH, aceasta împiedică creșterea regiei de conversie CCSID pentru toți solicitanții de aplicație de la distanță, dar cauzează probleme de integritate a datelor pentru solicitanții de aplicație locali—anumite caractere nu sunt afișate corect în solicitanții de aplicație locali; de exemplu, un semn de liră Britanică este afișat ca un semn de tip dolar.

Pentru afișarea valorii curente a CCSID-ului sistemului se interoghează tabela SYSTEM.SYSOPTIONS. Valoarea implicită CCSID a serverului de aplicație este de obicei valoarea de CCSIDMIXED. Dacă această valoare este zero, atunci valoarea implicită CCSID a sistemului este valoarea de CCSIDSBCS. Valorile CHARNAME, CCSIDSBCS, CCSIDMIXED și CCSIDGRAPHIC din această tabelă sunt actualizate la valorile folosite ca valori implicite ale sistemului de fiecare dată când baza de date este pornită. Valorile din această tabelă ar putea să nu fie întotdeauna valorile implicite ale sistemului. Un utilizator cu autoritatea DBA ar putea să fi schimbat aceste valori, chiar dacă aceasta nu este ceva recomandat. Pentru schimbarea valorii implicite CCSID a serverului de aplicație trebuie să specificați parametrul CHARNAME al SQLSTART EXEC data viitoare când serverul de aplicație este pornit. A se vedea manualul *DB2 Server for VM System Administration* pentru informații mai detaliate.

Pentru o bază de date nou instalată, valoarea implicită CHARNAME a serverului de aplicație este valoarea INTERNATIONAL și valoarea implicită CCSID a serverului de aplicație este 500. Aceasta este cel mai probabil *ne* corectă pentru sistemul propriu. Valoarea implicită CHARNAME pentru un sistem migrat este valoarea ENGLISH și valoarea implicită CCSID este 37.

### Solicitanți de aplicație:

Un solicitant de aplicație trebuie să aibă valoarea implicită CHARNAME corespunzătoare și valorile CCSID. Alegerea valorilor corecte asigură integritatea reprezentării datelor de tip caracter și reduce regia de performanță asociată cu conversia CCSID.

De exemplu, dacă solicitantul de aplicație propriu DB2 pentru VM este generat cu pagina de cod 37 și setul de caractere 697(CP/CS 37/697) pentru caracterele US ENGLISH atunci solicitantul de aplicație ar trebui să seteze valoarea implicită CHARNAME la valoarea de ENGLISH. Aceasta se întâmplă deoarece CP/CS 37/697 corespunde cu un CCSID de 37, care corespunde lui CHARNAME cu valoarea ENGLISH.

Valoarea implicită CHARNAME a unui sistem nou instalat sau a unui migrat este valoarea INTERNATIONAL și cea a lui CCSID este 500. Aceasta probabil *nu* prea corectă pentru instalarea proprie. Pentru a afișa valorile curente implicite ale CCSID-urilor, se folosește următoarea comandă:

```
SQLINIT QUERY
```

Valoarea de CCSID corespunzătoare pentru solicitantul de aplicație poate fi una care nu este suportat de către tablele de conversie de pe serverul de aplicație. Dacă aceasta este situația, se poate stabili conexiunea prin urmarea următoarelor:

- Se are în vedere actualizarea tablei de conversie CCSID a serverului de aplicație pentru suportarea conversiei între valoarea implicită a CCSID a solicitantului de aplicație și valoarea implicită CCSID a serverului de aplicație ( a se face referire la manualele de produs a serverului de aplicație pentru detalii asupra a cum se adaugă suportul de conversie CCSID).
- Se schimbă valoarea implicită CCSID a solicitantului de aplicație la una care este suportată de către serverul de aplicație. Acest lucru ar putea cauza probleme de integritate a datelor și trebuie să aveți în vedere aceste consecințe. Un exemplu de astfel de consecință urmează:
  - Un solicitant de aplicație folosește un controler definit cu CP/CS 37/697. Serverul de aplicație nu suportă o conversie de la CCSID 37, dar suportă o conversie de la CCSID 285 (acesta este valoarea lui CHARNAME de UK-ENGLISH pentru SQL/DS).  
Dacă solicitantul de aplicație este schimbat pentru a folosi o valoare implicită a lui CHARNAME de UK-ENGLISH (și pentru CCSID de 285) atunci integritatea datelor nu va fi menținută. De exemplu, acolo unde un caracter semn de liră Britanică (£) este intenționat de către serverul de aplicație, solicitantul de aplicație afișează un semn dolar (\$). Alte caractere pot fi de asemenea diferite.

Pentru schimbarea valorii CCSID a unui solicitant de aplicație DB2 pentru VM trebuie să specificați parametrul CHARNAME a lui SQLINIT EXEC.

Valoarea de CCSID corespunzătoare pentru serverul de aplicație poate fi una care nu este suportată de către tablele de conversie ale solicitantului de aplicație. Dacă acesta este cazul se poate stabili conexiunea prin urmarea uneia dintre următoarele posibilități:

- Se actualizează tabela de conversie folosită de către solicitantul de aplicație pentru a suporta conversia dintre valoarea implicită de CCSID a serverului de aplicație și valoarea implicită de CCSID a solicitantului de aplicație. Această tabelă este folosită pentru crearea macroului MACRO ARISSTR a fișierului CMS, care este folosit de către solicitantul de aplicație pentru suportul de conversie CCSID.
- Se execută schimbarea valorii implicite de CCSID a serverului de aplicație. Acest lucru ar trebui executat doar dacă este cazul, luând în considerare scopurile alegerii valorii implicite de CCSID a serverului de aplicație. Valoarea implicită de CCSID a serverului de aplicație afectează toți solicitanții de aplicație care se conectează cu acesta, terminalul operator folosit cu serverul de aplicație și datele stocate în tablele pe serverul de aplicație.

A se vedea *DB2 Server for VM System Administration* manualul pentru mai multe informații.

**Concepte înrudite:**

- “DB2 pentru VM” la pagina 74
- “DB2 pentru VSE” la pagina 84
- “Conversion of character data” în *Quick Beginnings for DB2 Connect Enterprise Edition*

**Task-uri înrudite:**

- “Instalarea DB2 ca un server de aplicații (VM)” la pagina 61
- “Instalarea DB2 ca un server de aplicații (VSE)” la pagina 55
- “Setarea pentru DB2 ca un solicitant de aplicație (VM)” la pagina 35



---

## Partea 5. Referință gazdă și iSeries



---

## Capitolul 15. Referință

---

### Produsele de comunicații APPC configurate folosind CA

Asistentul configurare (CA) poate adesea să configureze APPC automat. Următorul tabel listează produsele pe care CA le poate configura:

*Tabela 4. Produse configurate folosind CA*

Produse	Platformă	Configurat de CA?
IBM Personal Communications V4.2 și mai nou	Windows 98, Windows NT și Windows 2000	Da
IBM Communications Server (Server)	Windows NT și Windows 2000	Da
IBM Communications Server (Client)	Windows 98, Windows NT și Windows 2000	Nu
RUMBA	Windows 98, Windows NT și Windows 2000	Da
Microsoft SNA (Server)	Windows NT și Windows 2000	Nu
Microsoft SNA (Client)	Windows 98, Windows NT și Windows 2000	Nu

#### Task-uri înrudite:

- “Configurarea manuală a comunicațiilor APPC dintre DB2 Connect și un server de bază de date gazdă sau iSeries” la pagina 11
- “Actualizarea profilelor APPC pe serverul DB2 Connect” la pagina 12

---

### Listă de verificări pentru activarea unui server aplicație DB2 (VSE)

Următoarea listă de verificări însumează etapele necesare pentru activarea unui server aplicație DRDA, începînd cu presupunerea ca sistemul dumneavoastră VSE este instalat cu ACF/VTAM ca metodă acces teleprocesare și că definițiile VTAM necesare pentru a comunica cu sistemele la distanță, cum sunt definițiile NCP sunt efectuate.

1. Instalați suportul CICS ISC și suportul Resincronizare repornire .
2. Definiți CICS pentru VTAM pentru VSE.
3. Asamblați tabelul VTAM LOGMODE cu intrarea IBMRDB.
4. Asamblați tabelul deschidere sesiune CICS cu toate ID-urile utilizator și parolele definite la distanță.
5. Începeți CICS cu informațiile SIT corecte:
  - ISC=DA
  - TST=DA, ARIAXELG definit ca RECUPERABIL în DFHTST și asamblată
  - APPLID=LU nume (așa cum este definit în declarația VTAM APPL)
6. Definiți sistemele la distanță pentru CICS (se poate folosi RDO):
  - CEDA DEF CONEXIUNE
  - CEDA DEF SESIUNE
  - CEDA DEF PROGRAM
  - CEDA DEF TRANZACȚIE

Aceste declarații ar trebui să aibă toate definițiile sub un grup, de exemplu, numit IBMG. Instalați grupul cu: CEDA INSTALARE GRUP(IBMGM).

7. Actualizați directorul DBNAME (ARISDIRD.A):
  - Definiți toate TNP-urile listate în director pentru CICS. TPN-uri nedefinite pentru CICS nu pot fi folosite.
  - Definiți fiecare DB2 pentru serverul aplicații VSE DRDA în directorul cu un TPN valid.
8. Rulați procedura ARISBDID pentru a asambla directorul DBNAME actualizat.
9. Pregătiți DB2 pentru serverul VSE:
  - Rulați procedura ARIS342D pentru a instala suportul DRDA.
  - Dacă DB2 pentru aplicații VSE online (de exemplu ISQL) sunt rulate din partiții CICS, acordați autorizare de planificare CICS-ului APPLID specificat în tabelul CICS SIT.
  - Acordați autorizare tuturor utilizatorilor la distanță.
10. Dacă este necesar, rulați tranzacția DAXP CICS.
11. Porniți DB2 pentru VSE cu parametrul RMTUSERS corect și, opțional, parametrii DBNAME și SYNCNT.
12. Pregătiți aplicații pe serverul aplicații VSE DRDA.

**Concepte înrudite:**

- “DB2 pentru VSE” la pagina 84

**Task-uri înrudite:**

- “Instalarea DB2 ca un server de aplicații (VSE)” la pagina 55

---

## Listă de verificări pentru activarea unui solicitant de aplicații DB2 (VM)

Următoarea listă de verificări însumează etapele necesare pentru activarea unui solicitant aplicație DRDA, începând cu presupunerea ca sistemul dumneavoastră VM este instalat cu ACF/VTAM ca metodă acces teleprocesare și că definițiile VTAM necesare pentru a comunica cu sistemele la distanță, cum sunt definițiile NCP sunt efectuate.

1. Definiți gateway-ul AVS local pentru VTAM
2. Instalați suport DRDA în Solicitantul aplicații VM pentru DB2 folosind ARISDBMA exec.
3. Setați un director Comunicații CMS și adăugați orice instrucțiuni APPCPASS necesare în directorul VM al mașinei aplicație VM. Folosiți comanda SET COMDIR CMS pentru a activa directorul de comunicație.
4. Porniți VTAM și AVS astfel încât aplicațiile VM să poată comunica la distanță prin rețeaua SNA.
5. Lansați SQLINIT exec și specificați parametrii DBNAME, PROTOCOL și CHARNAME pentru a indica baza de date implicită, protocolul de folosit și CCSID-urile de folosit.
6. Pregătiți aplicațiile pe severul de la distanță.

**Concepte înrudite:**

- “DB2 pentru VM” la pagina 74

**Task-uri înrudite:**

- “Setarea pentru DB2 ca un solicitant de aplicație (VM)” la pagina 35

## Tabela cu valorile parametrilor TCP/IP

În timp ce continuați pașii de configurare, utilizați coloana *Valoarea dumneavoastră* din următorul tabel pentru a înregistra valorile necesare

Tabela 5. Valorile necesare TCP/IP la un server DB2 Connect

Parametru	Descriere	Valoare exemplu	Valoarea dumneavoastră
Numele gazdei • Numele gazdei ( <i>nume_gazdă</i> ) or • Adresa IP ( <i>adresă_ip</i> )	Utilizați <i>nume_gazdă</i> sau <i>adresă_ip</i> a gazdei de la distanță.  Pentru a rezolva acest parametru : • Contactați administratorul dumneavoastră de rețea pentru a obține <i>nume_gazdă</i> . • Contactați administratorul dumneavoastră de rețea pentru a obține <i>adresă_ip</i> sau introduceți comanda <b>ping</b> <i>nume_gazdă</i> .	nyx sau 9.21.15.235	
Numele serviciului • Numele serviciului de conexiune ( <i>nume_serviciu</i> ) sau • Număr port/Protocol ( <i>numar_port/tcp</i> )	Valori cerute în fișierul de servicii .  Numele serviciului de conexiune este un nume arbitrar care reprezintă numărul portului de conexiune ( <i>numar_port</i> ) la client.  Numarul portului pentru serverul DB2 Connect server trebuie să fie același ca numărul portului pe care se mapează parametrul <i>nume_serviciu</i> în fișierul de servicii al gazdei serverului de baze de date. (Parametrul <i>nume_serviciu</i> se află în fișierul manager de configurare a bazei de date al gazdei). Această valoare trebuie să nu fie folosită de nici o altă aplicație și trebuie să fie unică în fișierul de servicii.  Pe platformele UNIX, această valoare trebuie să fie în general 1024 sau mai mult.  Contactați administratorul dumneavoastră de baze de date pentru valorile folosite pentru configurarea sistemului gazdă.	gazdă1 sau 3700/tcp	
Numele bazei de date destinație ( <i>nume_bază_de_date_destinație</i> )	Numele bazei de date cum este cunoscut de către gazdă sau sistem iSeries. • Dacă vă conectați la o DB2 UDB pentru un sistem OS/390 și z/OS system, folosiți numele locației . • Dacă vă conectați la o DB2 UDB pentru sistemul iSeries, folosiți numele local RDB. • Dacă vă conectați la o DB2 pentru un sistem VM sau DB2 pentru un sistem VSE, folosiți <i>nume_bază_de_date</i> .	newyork	

Tabela 5. Valorile necesare TCP/IP la un server DB2 Connect (continuare)

Parametru	Descriere	Valoare exemplu	Valoarea dumneavoastră
Numele bazei de date locale ( <i>nume_bază_de_date_locală</i> )	O poreclă locală arbitrară pentru utilizarea serverului DB2 Connect care reprezintă gazda de la distanță sau baza de date iSeries.	ny	
Numele nodului ( <i>nume_nod</i> )	Un alias local sau o poreclă care descrie nodul la care încercați să vă conectați. Puteți alege orice nume doriți; totuși, toate valorile numelui nodului din directorul local de noduri trebuie să fie unice.	nod_db2	

**Task-uri înrudite:**

- “Configurarea manuală a comunicațiilor TCP/IP dintre DB2 Connect și un server de bază de date gazdă sau iSeries” la pagina 3

## Valorile parametrului TCP/IP pentru catalogarea bazelor de date

Completați coloana *Valoarea dumneavoastră* în următoarea pagină de lucru.

Tabela 6. Pagină de lucru: Valori parametru pentru catalogarea bazelor de date

Paramtru	Descriere	Valoare exemplu	Valoarea dumneavoastră
Nume bază de date ( <i>database_name</i> )	Numele bazei de date DCS locale ( <i>local_dcsname</i> ) al bazei de date la distanță, ați specificat acestea când ați catalogat directorul bază de date DCS, de exemplu, ny.	ny	
Alias bază de date ( <i>database_alias</i> )	O poreclă locală arbitrară pentru baza de date la distanță. Dacă nu oferiți una, valoarea implicită este aceeași cu numele bazei de date ( <i>database_name</i> ). Folosiți acest nume atunci când vă conectați la baza de date de la un client.	localny	
Nume nod ( <i>node_name</i> )	Folosiți aceeași valoare pentru Numele nodului <i>node_name</i> pe care ați folosit-o pentru a cataloga nodul.	db2node	

**Task-uri înrudite:**

- “Configurarea manuală a comunicațiilor TCP/IP dintre DB2 Connect și un server de bază de date gazdă sau iSeries” la pagina 3
- “Catalogarea bazei de date” la pagina 7

## Tabelul valorilor parametrilor APPC

Înainte de configurarea DB2 Connect serverului, cereți administratorului dumneavoastră de gazdă și iSeries, precum și administratorului rețelei locale să completeze copii ale acestui tabel pentru fiecare gazdă sau bază de date iSeries la care vreți să vă conectați.

După ce completați intrările în coloana *Valoarea dvs.*, puteți folosi tabelul la configurarea comunicațiilor APPC pentru DB2 Connect. În timpul procesului de configurare, înlocuiți

valorile exemplu care apar în instrucțiunile de configurare cu valorile din tabel. Folosiți nunerele încasotate (de exemplu, **1**) pentru a corela instrucțiunile de configurare cu valorile din tabel.

Tabelul și instrucțiunile oferă valori sugerate sau exemple pentru parametrii de configurare necesari. Pentru ceilalți parametri, folosiți valorile implicite ale programului de comunicații. În cazul în care configurația rețelei dumneavoastră este diferită de aceste instrucțiuni, consultați administratorul dumneavoastră de rețea pentru valorile corespunzătoare rețelei dumneavoastră.

În instrucțiunile de configurație, simbolul **\*** denotază intrări care trebuie schimbate, dar nu au o reprezentare în tabel.

Tabela 7. Tabelul pentru planificarea gazdei și a conexiunilor serverului iSeries.

Ref.	Numele la serverul DB2 Connect	Rețeaua sau numele VTAM	Valoare exemplu	Valoarea dumneavoastră
<b>Elementele rețelei la gazdă sau la serverul de baze de date iSeries</b>				
<b>1</b>	Numele gazdei	Numele rețelei locale	SPIFNET	
<b>2</b>	Numele partenerului LU	Numele aplicației	NYM2DB2	
<b>3</b>	ID-ul rețelei		SPIFNET	
<b>4</b>	Numele partenerului de nod	Numele CP sau SSCP local	NYX	
<b>5</b>	Numele bazei de date destinație ( <i>nume_bază_de_date_destinație</i> )	<b>OS/390 sau z/OS:</b> NUMELE LOCAȚIEI <b>VM/VSE:</b> NUMELE_BAZEI_DE_DATE <b>iSeries:</b> numele RDB	NEWYORK	
<b>6</b>	Numele legăturii sau al modului		IBMRDB	
<b>7</b>	Numele conexiunii (al legăturii)		LEGĂTURĂ_GAZDĂ	
<b>8</b>	Rețeaua de la distanță sau adresa LAN	Adaptorul local sau adresa destinației	400009451902	
<b>Elementele de rețea la DB2 Connect server</b>				
<b>9</b>	Identificatorul rețelei sau al LAN		SPIFNET	
<b>10</b>	Numele punctului local de control		NYX1GW	
<b>11</b>	Numele local LU		NYX1GW0A	
<b>12</b>	Aliasul LU local		NYX1GW0A	
<b>13</b>	Nodul local sau identificatorul nodului	ID BLK	071	
<b>14</b>		ID NUM	27509	
<b>15</b>	Numele modului		IBMRDB	
<b>16</b>	Numele destinației simbolice		DB2CPIC	

Tabela 7. Tabelul pentru planificarea gazdei și a conexiunilor serverului iSeries. (continuare)

Ref.	Numele la serverul DB2 Connect	Rețeaua sau numele VTAM	Valoare exemplu	Valoarea dumneavoastră
<b>17</b>	Numele programului de tranzacție de la distanță (Remote Transaction) (TP)		<b>OS/390 sau z/OS:</b> X'07'6DB ('07F6C4C2') sau DB2DRDA  <b>VM/VSE:</b> AXE pentru VSE. Numele DB2 pentru VM db sau X'07'6DB ('07F6C4C2') pentru VM  <b>iSeries:</b> X'07'6DB ('07F6C4C2') sau QCNTEDDM	
<b>Intrările de directoare DB2 la DB2 Connect server</b>				
<b>19</b>	Numele nodului		nod_db2	
<b>19</b>	Securitate		program	
<b>20</b>	Numele bazei de date locală <i>nume_bază_de_date_locală</i>		ny	

Pentru fiecare server la care vă conectați, completați câte o copie a tabelului, după cum urmează :

1. Pentru *identificator\_rețea*, determinați numele rețelei atât al gazdei iSeries, cât și al DB2 Connect serverului ( **1** , **3** și **9** ). De obicei, aceste valori vor fi aceleași. De exemplu, SPIFNET.
2. Pentru *numele partenerului LU* ( **2** ), determinați numele aplicației VTAM (APPL) pentru OS/390, z/OS, VSE, sau VM. Determinați numele CP local pentru iSeries.
3. Pentru *numele nodului partenerului* ( **4** ), determinați numele punctului de control al sistemului de servicii (SSCP) pentru OS/390, z/OS, VM, sau VSE. Determinați numele punctului local de control pentru un iSeries.
4. Pentru *numele bazei de date* ( **5** ), determinați numele gazdei și al bazei de date iSeries. Acesta este *NUMELE LOCAȚIEI* pentru OS/390 sau z/OS, *NUMELE BAZEI DE DATE* pentru VM sau VSE sau numele unei baze de date relațională (RDB) pentru iSeries.
5. Pentru *numele modului* ( **6** și **15** ), de obicei cel implicit IBMDRDB este suficient.
6. Pentru *adresa rețelei de la distanță* ( **8** ), determinați adresa controlerului sau adresa adaptorului local al gazdei sau sistemului iSeries destinație.
7. Determinați *numele punctului local de control* ( **10** ) al serverului DB2 Connect. Acesta este de obicei același ca numele PU pentru sistem.
8. Determinați *numele local LU* care DB2 Connect va utiliza ( **11** ). Dacă folosiți un punct manager sincron (SPM) pentru gestionarea actualizărilor multisite (comise în două faze), atunci LU local va trebui să fie LU utilizat pentru SPM. În acest caz, acel LU nu poate să fie și punctul de control LU.
9. Pentru *aliasul LU local* ( **12** ), folosiți de obicei aceeași valoare ca și pentru numele LU local ( **11** ).
10. Pentru *nodul local* sau *identificatorul nodului* ( **13** plus **14** ), determinați IDBLK și IDNUM ale DB2 Connect serverului. Această valoare implicită ar trebui să fie corectă.
11. Pentru *numele destinației simbolice* ( **16** ), alegeți o valoare dorită.
12. Pentru *numele programului de tranzacție* (de la distanță) ( **17** ), folosiți valorile implicite menționate în tabel.



13. Deocamdată, lăsați celelalte articole goale ( **18** to **21** ).

**Task-uri înrudite:**

- “Configurarea manuală a comunicațiilor APPC dintre DB2 Connect și un server de bază de date gazdă sau iSeries” la pagina 11

---

## Cuvintele cheie ale instrucțiunii DB2 Conectare (Connect) VTAM APPL

Multe cuvinte cheie sunt disponibile în instrucțiunea VTAM APPL. Cuvintele cheie discutate aici adresează topici din această carte.

### **LUDBD1**

VTAM folosește eticheta instrucțiunii APPL ca nume al LU. În acest caz numele LU este LUDBD1. Sintaxa lui APPL nu permite spațiu pentru o valoare a NETID.LUNAME completă. Valoarea lui NETID nu este specificată în instrucțiunea VTAM APPL deoarece tuturor aplicațiilor VTAM le sunt în mod automat asignate NETID pentru sistemul VTAM.

### **AUTOSES=1**

Numărul sesiunii câștigătoare a concursului SNA care pornesc în mod automat atunci când o cerere Schimbare Număr al Sesiunii AAPC (APPC Change Number of Sessions) (CNOS) este emisă.

Nu este obligatoriu să porniți în mod automat toate sesiunile APPC între oricare doi parteneri baze de date distribuite. Dacă valoarea lui AUTOSES este mai mică decât limita câștigătorului concursului (DMINWNL), VTAM întârzie sesiunile SNA rămase până când acestea sunt cerute de către o aplicație bază de date distribuită.

### **DMINWNL=10**

Numărul de sesiuni pe care acest sistem se află este câștigătorul concursului. Parametrul DMINWNL este valoarea implicită pentru procesarea CNOS, dar aceasta poate fi înlocuită pentru oricare partener dat prin adăugarea unui rând la tabela SYSIBM.SYSLUMODES din baza de date de comunicații.

### **DMINWNR=10**

Numărul de sesiuni pe care sistemul partener se află este câștigătorul concursului. Parametrul DMINWNR este valoarea implicită pentru procesarea CNOS, dar aceasta poate fi înlocuită pentru oricare partener dat prin adăugarea unui rând la tabela SYSIBM.SYSLUMODES din baza de date de comunicații.

### **DSESLIM=20**

Numărul total de sesiuni (sesiuni câștigătoare și cele care au pierdut) pe care le puteți stabili între DB2 și un alt sistem distribuit pentru un nume de grup mod specific. Parametrul DSESLIM este valoarea implicită pentru procesarea CNOS, dar aceasta poate fi înlocuită pentru oricare partener dat prin adăugarea unui rând la tabela SYSIBM.SYSLUMODES din baza de date de comunicații DB2.

Dacă partenerul nu poate suporta numărul de sesiuni cerute în parametrii DSESLIM, DMINWNL sau DMINWNR procesul CNOS negociază noi valori pentru acești parametri care sunt acceptabile pentru partener.

### **EAS=9999**

O estimare a numărului total de sesiuni pe care acest VTAM LU le necesită.

### **MODETAB=RDBMODES**

Identifică tabela VTAM MODE în care fiecare nume de mod DB2 există.

### **PRTCT=PSWDBD1**

Identifică parola VTAM pentru folosire atunci când DB2 încearcă conectarea la

VTAM. Dacă cuvântul cheie PRTCT este omis, nici o parolă nu este necesară și ar trebui să omiteți cuvântul cheie PASSWORD= din utilitarul de inventariere a istoricului de schimbări ale DB2.

#### **SECACPT=ALREADYV**

Identifică cea mai mare valoare a securității de nivel conversație SNA acceptată de către acest sistem DB2 atunci când primește o cerere de bază de date distribuită din partea unui sistem de la distanță. Cuvântul cheie ALREADYV indică faptul că acest sistem DB2 poate accepta trei opțiuni de securitate a sesiunii SNA din partea altor DRDA sisteme care cer date din partea acestui sistem DB2:

- SECURITY=SAME (o cerere deja-verificată care conține ID-ul utilizatorului solicitant).
- SECURITY=PGM (o cerere conținând ID-ul utilizatorului solicitant și parola).
- SECURITY=NONE (o cerere neconținând nici o informație de securitate). DB2 refuză DRDA cererile care specifică SECURITY=NONE.

Cel mai bine este ca întotdeauna să se specifice SECACPT=ALREADYV, deoarece nivelul de securitate al conversației SNA pentru fiecare partener DB2 este luat din baza de date de comunicații DB2 (coloana USERSECURITY a tabeli SYSIBM.SYSLUNAMES). SECACPT=ALREADYV asigură cea mai mare flexibilitate în selectarea valorilor pentru USERSECURITY.

#### **VERIFY=NONE**

Identifică nivelul de securitate al sesiunii SNA (verificarea LU a partenerului) cerută de către acest sistem DB2. Valoarea NONE indică faptul că verificarea LU a partenerului nu este necesară.

DB2 nu restricționează alegerea pentru cuvântul cheie VERIFY. Într-o rețea nesigură, VERIFY=REQUIRED este recomandată. VERIFY=REQUIRED cauzează VTAM să rejeteze partenerii care nu pot executa verificări LU de parteneri. Dacă alegeți VERIFY=OPTIONAL, VTAM execută verificarea LU a partenerilor doar pentru acei parteneri care furnizează suport.

#### **VPACING=2**

Setează contorul de pași VTAM la 2.

#### **SYNCLVL=SYNCPT**

Indică faptul că DB2 este în stare să suporte comitere în două faze. VTAM folosește această informație pentru informarea partenerului de faptul că comiterea în două faze este disponibilă. Dacă acest cuvânt cheie este folosit, DB2 în mod automat folosește comiterea în două faze dacă partenerul o poate suporta.

#### **ATNLOSS=ALL**

Indică faptul că DB2 are nevoie să fie informat de fiecare dată ce o sesiune VTAM se termină. Aceasta asigură faptul că DB2 efectuează resincronizarea SNA atunci când este necesară.

DSESLIM, DMINWNL și DMINWNR permit stabilirea limitelor implicite de sesiuni VTAM pentru toți partenerii. Pentru partenerii care au cerințe de limită de sesiuni specială tabela SYSIBM.SYSLUMODES poate fi folosită pentru înlocuirea limitelor implicite de sesiuni. De exemplu, dacă doriți să specificați limitele implicite de sesiuni VTAM care sunt corespunzătoare pentru sistemele proprii Windows. Pentru ați parteneri puteți crea rânduri în tabela SYSIBM.SYSLUMODES pentru definirea limitelor de sesiuni dorite. Considerați aceste valori de exemplu:

DSESLIM=4, DMINWNL=0, DMINWNR=4

#### **Concepte înrudite:**

- “Subsistem securitate - server aplicație (OS/390 și z/OS)” la pagina 94

- “Securitate rețea - server aplicație (OS/390 și z/OS)” la pagina 92
- “Securitate rețea - solicitant aplicație (OS/390 și z/OS)” la pagina 106
- “Subsistem de securitate - solicitant de aplicație (OS/390 și z/OS)” la pagina 108

**Task-uri înrudite:**

- “Instalarea DB2 ca un server de aplicații (OS/390 și z/OS)” la pagina 43
- “Instalarea DB2 ca un solicitant de aplicații (OS/390 și z/OS)” la pagina 23



---

## Partea 6. Anexe



---

## Anexa A. Informații tehnice DB2 Universal Database

---

### Privire generală asupra informațiilor tehnice DB2 Universal Database

Informațiile tehnice DB2 Universal Database pot fi obținute în următoarele formate:

- Cărți (formate PDF și tipărite)
- Arbore de subiecte (format HTML)
- Ajustor pentru uneltele DB2 (format HTML)
- Programe eșantion (format HTML)
- Ajustor pentru linia de comandă
- Îndrumare

Această secțiune este privire generală asupra informațiilor tehnice oferite și a modului în care le puteți accesa.

### Categoriile de informații tehnice DB2

Informațiile tehnice DB2 sunt împărțite pe categorii după următoarele titluri:

- Informații nucleu DB2
- Informații administrare
- Informații dezvoltare aplicații
- Informații sistem informațional de afaceri
- Informații DB2 Connect
- Informații de inițiere
- Informații de îndrumare
- Informații componente opționale
- Note privind ediția

Tabelele următoare prezintă, pentru fiecare carte din biblioteca DB2, informațiile necesare pentru a comanda copia tipărită, pentru a tipări sau vizualiza PDF-ul sau pentru a localiza directorul HTML corespunzător cărții. În Centrul de publicații IBM, la [www.ibm.com/shop/publications/order](http://www.ibm.com/shop/publications/order), se găsește câte o descriere completă a fiecărei cărți din biblioteca DB2.

Directorul de instalare al CD-ului cu documentație HTML este diferit pentru fiecare categorie de informații:

`caledhtml/doc/htmlcd/%L/categorie`

unde:

- `caledhtml` este directorul în care este instalat CD-ul cu documentația HTML.
- `%L` este identificatorul de limbă. De exemplu, `en_US`.
- `categorie` este identificatorul de categorie. De exemplu, `core` pentru informații nucleu DB2.

În coloana Nume fișier PDF din următoarele tabele, caracterul din poziția a șasea a numelui de fișier indică versiunea de limbă a cărții. De exemplu, numele de fișier `db2d1e80` identifică versiunea în limba engleză a cărții *Administration Guide: Planning*, iar numele de fișier `db2d1g80` identifică versiunea în germană a aceleiași cărți. Pentru a indica versiunea de limbă, în poziția a șasea a numelui de fișier sunt folosite următoarele caractere:

<b>Limbă</b>	<b>Identificator</b>
Arabă	w
Portugheză braziliană	b
Bulgară	u
Croată	9
Cehă	x
Daneză	d
Olandeză	q
Engleză	e
Finlandeză	y
Franceză	f
Germană	g
Greacă	a
Maghiară	h
Italiană	i
Japoneză	j
Coreeană	k
Norvegiană	n
Poloneză	p
Portugheză	v
Română	8
Rusă	r
Chineză simpl.	c
Slovacă	7
Slovenă	l
Spaniolă	z
Suedează	s
Chineză trad.	t
Turcă	m

**Fără număr format**, indică faptul că respectiva carte este disponibilă numai online, nu și într-o versiune tipărită.

## Informații nucleu DB2

Informațiile din această categorie acoperă subiectele DB2 care sunt fundamentale pentru toți cei ce utilizează DB2. Aceste informații vă sunt utile indiferent dacă sunteți programator, dacă sunteți administrator de bază de date sau dacă lucrați cu DB2 Connect, DB2 Warehouse Manager sau alte produse DB2.

Directorul de instalare pentru această categorie este `doc/htmlcd/%L/core`.

*Tabela 8. Informații nucleu DB2*

<b>Nume</b>	<b>Număr format</b>	<b>Nume fișier PDF</b>
<i>IBM DB2 Universal Database Command Reference</i>	SC09-4828	db2n0x80
<i>IBM DB2 Universal Database Glossary</i>	Fără număr format	db2t0x80
<i>IBM DB2 Universal Database Master Index</i>	SC09-4839	db2w0x80
<i>IBM DB2 Universal Database Message Reference, Volume 1</i>	GC09-4840	db2m1x80
<i>IBM DB2 Universal Database Message Reference, Volume 2</i>	GC09-4841	db2m2x80



Tabela 8. Informații nucleu DB2 (continuare)

Nume	Număr format	Nume fișier PDF
IBM DB2 Universal Database <i>What's New</i>	SC09-4848	db2q0x80

## Informații administrare

Informațiile din această categorie acoperă subiectele necesare pentru activitatea de proiectare, implementare și întreținere a bazelor de date, depozitelor de date și sistemelor federalizate DB2.

Directorul de instalare pentru această categorie este `doc/htmlcd/%L/admin`.

Tabela 9. Informații administrare

Nume	Număr format	Nume fișier PDF
IBM DB2 Universal Database <i>Administration Guide: Planning</i>	SC09-4822	db2d1x80
IBM DB2 Universal Database <i>Administration Guide: Implementation</i>	SC09-4820	db2d2x80
IBM DB2 Universal Database <i>Administration Guide: Performance</i>	SC09-4821	db2d3x80
IBM DB2 Universal Database <i>Administrative API Reference</i>	SC09-4824	db2b0x80
IBM DB2 Universal Database <i>Data Movement Utilities Guide and Reference</i>	SC09-4830	db2dmx80
IBM DB2 Universal Database <i>Data Recovery and High Availability Guide and Reference</i>	SC09-4831	db2hax80
IBM DB2 Universal Database <i>Data Warehouse Center Administration Guide</i>	SC27-1123	db2ddx80
IBM DB2 Universal Database <i>Federated Systems Guide</i>	GC27-1224	db2fpx80
IBM DB2 Universal Database <i>Guide to GUI Tools for Administration and Development</i>	SC09-4851	db2atx80
IBM DB2 Universal Database <i>Replication Guide and Reference</i>	SC27-1121	db2e0x80
IBM DB2 <i>Installing and Administering a Satellite Environment</i>	GC09-4823	db2dsx80
IBM DB2 Universal Database <i>SQL Reference, Volume 1</i>	SC09-4844	db2s1x80
IBM DB2 Universal Database <i>SQL Reference, Volume 2</i>	SC09-4845	db2s2x80
IBM DB2 Universal Database <i>System Monitor Guide and Reference</i>	SC09-4847	db2f0x80

## Informații dezvoltare aplicații

Informațiile din această categorie îi interesează în special pe dezvoltatorii de aplicații sau programatorii care lucrează cu DB2. Veți găsi informații despre limbajele și compilatoarele suportate, precum și documentația necesară pentru a accesa DB2 folosind diversele interfețe de programare suportate, cum ar fi SQL înglobat, ODBC, JDBC, SQLj și CLI. Dacă vizualizați aceste informații online, în format HTML, aveți acces și la un set de programe eșantion DB2.

Directorul de instalare pentru această categorie este [doc/htmlcd/%L/ad](#).

Tabela 10. Informații dezvoltare aplicații

Nume	Număr format	Nume fișier PDF
<i>IBM DB2 Universal Database Application Development Guide: Building and Running Applications</i>	SC09-4825	db2axx80
<i>IBM DB2 Universal Database Application Development Guide: Programming Client Applications</i>	SC09-4826	db2a1x80
<i>IBM DB2 Universal Database Application Development Guide: Programming Server Applications</i>	SC09-4827	db2a2x80
<i>IBM DB2 Universal Database Call Level Interface Guide and Reference, Volume 1</i>	SC09-4849	db211x80
<i>IBM DB2 Universal Database Call Level Interface Guide and Reference, Volume 2</i>	SC09-4850	db212x80
<i>IBM DB2 Universal Database Data Warehouse Center Application Integration Guide</i>	SC27-1124	db2adx80
<i>IBM DB2 XML Extender Administration and Programming</i>	SC27-1234	db2sxx80

## Informații sistem informațional de afaceri

Informațiile din această categorie prezintă modul în care se folosesc componentele care îmbunătățesc capacitățile analitice și de lucru cu depozitele de date DB2 Universal Database.

Directorul de instalare pentru această categorie este [doc/htmlcd/%L/wareh](#).

Tabela 11. Informații sistem informațional de afaceri

Nume	Număr format	Nume fișier PDF
<i>IBM DB2 Warehouse Manager Information Catalog Center Administration Guide</i>	SC27-1125	db2dix80
<i>IBM DB2 Warehouse Manager Installation Guide</i>	GC27-1122	db2idx80

## Informații DB2 Connect

Informațiile din această categorie prezintă modul în care se accesează datele de pe gazdă sau iSeries folosind DB2 Connect Enterprise Edition sau DB2 Connect Personal Edition.

Directorul de instalare pentru această categorie este <doc/htmlcd/%L/conn>.

Tabela 12. Informații DB2 Connect

Nume	Număr format	Nume fișier PDF
<i>APPC, CPI-C, and SNA Sense Codes</i>	Fără număr format	db2apx80
<i>IBM Connectivity Supplement</i>	Fără număr format	db2h1x80
<i>IBM DB2 Connect Quick Beginnings for DB2 Connect Enterprise Edition</i>	GC09-4833	db2c6x80
<i>IBM DB2 Connect Quick Beginnings for DB2 Connect Personal Edition</i>	GC09-4834	db2c1x80
<i>IBM DB2 Connect User's Guide</i>	SC09-4835	db2c0x80

## Informații de inițiere

Informațiile din această categorie sunt utile atunci când instalați și configurați servere, clienți și alte produse DB2.

Directorul de instalare pentru această categorie este <doc/htmlcd/%L/start>.

Tabela 13. Informații de inițiere

Nume	Număr format	Nume fișier PDF
<i>IBM DB2 Universal Database Quick Beginnings for DB2 Clients</i>	GC09-4832	db2itx80
<i>IBM DB2 Universal Database Quick Beginnings for DB2 Servers</i>	GC09-4836	db2isx80
<i>IBM DB2 Universal Database Quick Beginnings for DB2 Personal Edition</i>	GC09-4838	db2i1x80
<i>IBM DB2 Universal Database Installation and Configuration Supplement</i>	GC09-4837	db2iyx80
<i>IBM DB2 Universal Database Quick Beginnings for DB2 Data Links Manager</i>	GC09-4829	db2z6x80

## Informații de îndrumare

Informațiile de îndrumare prezintă caracteristicile DB2 și vă învață cum să realizați diverse operații.

Directorul de instalare pentru această categorie este <doc/htmlcd/%L/tutr>.

Tabela 14. Informații de îndrumare

Nume	Număr format	Nume fișier PDF
<i>Business Intelligence Tutorial: Introduction to the Data Warehouse</i>	Fără număr format	db2tux80
<i>Business Intelligence Tutorial: Extended Lessons in Data Warehousing</i>	Fără număr format	db2tax80

Tabela 14. Informații de îndrumare (continuare)

Nume	Număr format	Nume fișier PDF
<i>Development Center Tutorial for Video Online using Microsoft Visual Basic</i>	Fără număr format	db2tdx80
<i>Information Catalog Center Tutorial</i>	Fără număr format	db2aix80
<i>Video Central for e-business Tutorial</i>	Fără număr format	db2twx80
<i>Visual Explain Tutorial</i>	Fără număr format	db2tvx80

## Informații componente opționale

Informațiile din această categorie prezintă modul în care se lucrează cu componentele DB2 opționale.

Directorul de instalare pentru această categorie este doc/htmlcd/%L/opt.

Tabela 15. Informații componente opționale

Nume	Număr format	Nume fișier PDF
<i>IBM DB2 Life Sciences Data Connect Planning, Installation, and Configuration Guide</i>	GC27-1235	db2lsx80
<i>IBM DB2 Spatial Extender User's Guide and Reference</i>	SC27-1226	db2sbx80
<i>IBM DB2 Universal Database Data Links Manager Administration Guide and Reference</i>	SC27-1221	db2z0x80
<i>IBM DB2 Universal Database Net Search Extender Administration and Programming Guide</i>	SH12-6740	-

**Notă:** Versiunea HTML a acestui document nu se instalează de pe CD-ul cu documentație HTML.

## Note privind ediția

Notele referitoare la ediție conțin informații suplimentare, specifice ediției dumneavoastră de produs și nivelului de FixPak. De asemenea, ele oferă sumare cu actualizările de documentație încorporate în fiecare ediție și FixPak.

Tabela 16. Note privind ediția

Nume	Număr format	Nume fișier PDF	Director HTML
<i>Note privind ediția DB2</i>	Vedeți nota.	Vedeți nota.	doc/prodcd/%L/db2ir  unde %L este identificatorul de limbă.
<i>Note privind ediția DB2 Connect</i>	Vedeți nota.	Vedeți nota.	doc/prodcd/%L/db2cr  unde %L este identificatorul de limbă.
<i>Note privind instalarea DB2</i>	Disponibile numai pe CD-ROM-ul produsului.	Disponibile numai pe CD-ROM-ul produsului.	

**Notă:** Versiunea HTML a notelor privind ediția este disponibilă în Centrul de informare și pe CD-ROM-urile produsului. Pentru a vizualiza fișierul ASCII:

- Pe platformele bazate pe UNIX, vedeți fișierul `Release.Notes`. Acest fișier se află în directorul `DB2DIR/Readme/%L`, unde `%L` reprezintă numele de Locale, iar `DB2DIR` reprezintă:
  - `/usr/opt/db2_08_01` pe AIX
  - `/opt/IBM/db2/V8.1` pe toate celelalte sisteme de operare UNIX
- Pe alte platforme, vedeți fișierul `RELEASE.TXT`. Acest fișier se află în directorul în care este instalat produsul.

**Task-uri înrudite:**

- “Tipărirea cărților DB2 folosind fișierele PDF” la pagina 143
- “Comanda cărților DB2 tipărite” la pagina 144
- “Accesarea ajutorului online” la pagina 144

---

## Tipărirea cărților DB2 folosind fișierele PDF

Puteți tipări cărțile DB2 folosind fișierele PDF de pe CD-ul *DB2 PDF Documentation*. Cu Adobe Acrobat Reader, puteți tipări toată cartea sau numai un anumit interval de pagini.

**Cerințe preliminare:**

Asigurați-vă că aveți Adobe Acrobat Reader. Acesta este disponibil pe site-ul Web Adobe, la [www.adobe.com](http://www.adobe.com)

**Procedura:**

Pentru a tipări o carte DB2 folosind un fișier PDF:

1. Introduceți în unitate CD-ul *DB2 PDF Documentation*. În cazul sistemelor de operare UNIX, montați CD-ul *DB2 PDF Documentation*. Consultați manualul *Quick Beginnings* pentru detalii privind modul în care se montează un CD în sistemele de operare UNIX.
2. Lansați în execuție Adobe Acrobat Reader.
3. Deschideți fișierul PDF din una dintre următoarele locații:
  - În sistemele de operare Windows:  
directorul `x:\doc\limbă`, unde `x` reprezintă litera unității CD-ROM, iar `limbă` reprezintă codul de teritoriu din două caractere care reprezintă limba dumneavoastră (de exemplu, EN pentru English).
  - În sistemele de operare UNIX:  
directorul `/cdrom/doc/%L` de pe CD-ROM, unde `/cdrom` reprezintă punctul de montare a CD-ROM-ului, iar `%L` reprezintă numele dorit pentru Locale.

**Concepte înrudite:**

- “Centru de informare DB2 pentru subiecte” la pagina 151

**Task-uri înrudite:**

- “Comanda cărților DB2 tipărite” la pagina 144

**Referințe înrudite:**

- “Privire generală asupra informațiilor tehnice DB2 Universal Database” la pagina 137

---

## Comanda cărților DB2 tipărite

### Procedura:

Pentru a comanda cărți tipărite:

- Contactați vânzătorul sau reprezentantul IBM autorizat. Pentru a găsi un reprezentant IBM local, verificați directorul cu contacte IBM din lumea întreagă la [www.ibm.com/shop/planetwide](http://www.ibm.com/shop/planetwide)
- Apelați la 1-800-879-2755 în Statele Unite și la 1-800-IBM-4YOU în Canada.
- Vizitați IBM Publications Center la [www.ibm.com/shop/publications/order](http://www.ibm.com/shop/publications/order)

### Task-uri înrudite:

- “Tipărirea cărților DB2 folosind fișierele PDF” la pagina 143

### Referințe înrudite:

- “Privire generală asupra informațiilor tehnice DB2 Universal Database” la pagina 137

---

## Accesarea ajutorului online

Ajutorul online care vine cu componentele toate DB2 este de trei tipuri:

- Ajutor fereastră și caiet (notebook)
- Ajutor linie de comandă
- Ajutor instrucțiuni SQL

Ajutor fereastră sau caiet explică operațiile pe care le puteți realiza într-o fereastră sau caiet și descrie controalele. Acest ajutor are două tipuri:

- Ajutor accesibil de la butonul **Ajutor**
- Infopop-uri

Butonul **Ajutor** vă furnizează acces să aruncați o privire generală și să aflați informații preliminară. Infopop-urile descriu controalele din fereastră sau caiet (notebook). Ajutorul fereastră și caiet sunt disponibile din centrele DB2 și din componentele care au interfețe de utilizator.

Ajutorul de linie de comandă include ajutorul pentru comenzi și ajutorul pentru mesaje. Ajutorul de comenzi explică sintaxa comenzilor în procesorul de linie de comandă. Ajutorul de mesaje descrie cauza unui mesaj de eroare și descrie orice acțiune pe care trebuie să o executați ca răspuns la eroare.

Ajutorul pentru instrucțiuni SQL include ajutorul SQL și ajutorul SQLSTATE. DB2 întoarce o valoare SQLSTATE pentru condiții care pot fi rezultatul unei instrucțiuni SQL. Ajutorul SQLSTATE explică sintaxa pentru instrucțiunile SQL (stările SQL și codurile de clasă).

**Notă:** Ajutorul SQL nu este disponibil pentru sistemele de operare UNIX.

### Procedura:

Pentru a accesa ajutorul online:

- Pentru ajutorul ferestrei și caietului, faceți clic pe **Ajutor** sau faceți clic pe acel control și apoi faceți clic pe **F1**. Dacă caseta de bifare **Afișare automată infopop-uri** de pe pagina **General** a caietului **Setări unelte** este selectată, puteți vedea infopop-ul pentru un control anume ținând cursorul mouse-ului peste el.

- Pentru ajutorul pentru linia de comandă, deschideți procesorul de linie de comandă și introduceți:

– Pentru ajutor comenzi:

`? comandă`

unde *comandă* reprezintă un cuvânt cheie sau întreaga comandă.

De exemplu, `? catalog` afișează ajutorul pentru toate comenzile CATALOG, în timp ce `? catalog database` afișează ajutorul pentru comanda CATALOG DATABASE.

- Pentru ajutor mesaje:

`? XXXnnnnn`

unde *XXXnnnnn* reprezintă un identificator de mesaj valid.

De exemplu, `? SQL30081` afișează un ajutor despre mesajul SQL30081.

- Pentru ajutorul pentru instrucțiunile SQL, deschideți procesor de linie de comandă și introduceți:

– Pentru ajutor SQL:

`? stare_sql` sau `? cod_clasă`

unde *stare\_sql* reprezintă o stare validă SQL din cinci cifre și *cod\_clasă* reprezintă primele două cifre din starea SQL.

De exemplu, `? 08003` afișează ajutor pentru starea SQL 08003, în timp ce `? 08` afișează ajutorul pentru cod clasă 08.

– Pentru ajutor SQLSTATE:

`help instrucțiune`

unde *instrucțiune* reprezintă o instrucțiune SQL.

De exemplu, `help SELECT` afișează ajutorul despre instrucțiunea SELECT.

#### **Task-uri înrudite:**

- “Apelarea Centrului de informare DB2” la pagina 147
- “Invocarea ajutorului pentru mesaje din linia de comandă” la pagina 145
- “Invocarea ajutorului pentru comenzi din linia de comandă” la pagina 146
- “Invocarea ajutorului pentru instrucțiunea SQL din linia de comandă (Windows)” la pagina 146

---

## **Invocarea ajutorului pentru mesaje din linia de comandă**

Ajutorul de mesaje descrie cauza unui mesaj de eroare și descrie orice acțiune pe care trebuie să o executați ca răspuns la eroare.

#### **Procedura:**

Pentru ajutorul pentru mesaj, deschideți procesorul de linie de comandă și introduceți:

`? XXXnnnnn`

unde *XXXnnnnn* reprezintă un identificator de mesaj valid.

De exemplu, `? SQL30081` afișează un ajutor despre mesajul SQL30081.

#### **Task-uri înrudite:**

- “Accesarea ajutorului online” la pagina 144

- “Apelarea Centrului de informare DB2” la pagina 147
- “Invocarea ajutorului pentru comenzi din linia de comandă” la pagina 146
- “Invocarea ajutorului pentru instrucțiunea SQL din linia de comandă (Windows)” la pagina 146

---

## Invocarea ajutorului pentru comenzi din linia de comandă

Ajutorul de comenzi explică sintaxa comenzilor în procesorul de linie de comandă.

### Procedura:

Pentru ajutorul pentru linia de comandă, deschideți procesorul de linie de comandă și introduceți:

```
? comandă
```

unde *comandă* reprezintă un cuvânt cheie sau întreaga comandă.

De exemplu, ? catalog afișează ajutorul pentru toate comenzile CATALOG, în timp ce ? catalog database afișează ajutorul pentru comanda CATALOG DATABASE.

### Task-uri înrudite:

- “Accesarea ajutorului online” la pagina 144
- “Apelarea Centrului de informare DB2” la pagina 147
- “Invocarea ajutorului pentru mesaje din linia de comandă” la pagina 145
- “Invocarea ajutorului pentru instrucțiunea SQL din linia de comandă (Windows)” la pagina 146

---

## Invocarea ajutorului pentru instrucțiunea SQL din linia de comandă (Windows)

Ajutorul pentru instrucțiuni SQL include ajutorul SQL și ajutorul SQLSTATE. DB2 întoarce o valoare SQLSTATE pentru condiții care pot fi rezultatul unei instrucțiuni SQL. Ajutorul SQLSTATE explică sintaxa pentru instrucțiunile SQL (stările SQL și codurile de clasă).

### Restricții:

Ajutorul SQL nu este disponibil pentru sistemele de operare UNIX.

### Procedura:

Pentru ajutorul pentru instrucțiunile SQL, deschideți procesor de linie de comandă și introduceți:

```
? stare_sql sau ? cod_clasă
```

unde *stare\_sql* reprezintă o stare validă SQL din cinci cifre și *cod\_clasă* reprezintă primele două cifre din starea SQL.

De exemplu, ? 08003 afișează ajutor pentru starea SQL 08003, în timp ce ? 08 afișează ajutorul pentru cod clasă 08.

### Task-uri înrudite:

- “Apelarea Centrului de informare DB2” la pagina 147



- “Invocarea ajutorului pentru mesaje din linia de comandă” la pagina 145
- “Invocarea ajutorului pentru comenzi din linia de comandă” la pagina 146

---

## Apelarea Centrului de informare DB2

Centrul de informare DB2 vă oferă acces la toate informațiile de care aveți nevoie pentru a beneficia pe deplin de DB2 Universal Database, DB2 Connect, DB2 Information Integrator și DB2 Query Patroller.

### Cerințe preliminare:

Înainte de a putea invoca Centrul de informare DB2 trebuie să:

- Configurați browser-ul să afișeze informațiile în limba preferată
- *Opțional*: Configurați clientul DB2 să folosească un Centru de informare DB2 instalat local.

### Procedură:

Pentru a apela Centrul de informare DB2 de pe desktop:

- Pentru sistemul de operare Windows: Faceți clic pe **Start** → **Programs** → **IBM DB2** → **Information** → **DB2 Documentation Set**

Pentru a apela Centrul de informare DB2 din linia de comandă :

- Pentru sisteme de operare Linux și UNIX : Lansați comanda **db2help**.
- Pentru sisteme de operare Windows: Lansați comanda **db2docs.exe**.

### Concepte înrudite:

- “Centru de informare DB2 pentru subiecte” la pagina 151

### Task-uri înrudite:

- “Configurarea browser-ului să afișeze informațiile în limba preferată” la pagina 152
- “Accesarea ajutorului online” la pagina 144
- “Actualizarea documentației HTML instalată pe mașina dumneavoastră” la pagina 147
- “Invocarea ajutorului pentru mesaje din linia de comandă” la pagina 145
- “Invocarea ajutorului pentru comenzi din linia de comandă” la pagina 146
- “Invocarea ajutorului pentru instrucțiunea SQL din linia de comandă (Windows)” la pagina 146

---

## Actualizarea documentației HTML instalată pe mașina dumneavoastră

Acum este posibilă actualizarea HTML-urilor instalate de pe CD-ul *DB2 HTML Documentation CD* când sunt disponibile actualizări de la IBM. Acest lucru se poate face în unul din două moduri:

- Folosind Centru de informare (dacă aveți uneltele GUI de administrare DB2 instalate).
- Prin descărcarea și aplicarea unui FixPak de documentație HTML DB2.

**Notă:** Aceasta NU va actualiza codul DB2; va actualiza numai documentația HTML instalată de pe CD-ul *DB2 HTML Documentation CD*.

### Procedură:

Pentru a folosi Centrul de informare pentru actualizarea documentației locale:

1. Porniți Centrul de informare DB2 într-unul din următoarele moduri:
  - Din uneltele de administrare grafice, apăsați pe icoana **Information Center** din bara de unelte. Puteți de asemenea să o selectați din meniul **Help**.
  - În linia de comandă, introduceți **db2ic**.
2. Asigurați-vă că mașina are acces la Internet extern; programul de actualizare va descărca, dacă este necesar, ultimul FixPak documentație de pe serverul IBM.
3. Selectați din meniu **Centru de informare** —> **Actualizare documentație locală** pentru a porni actualizarea.
4. Furnizați informațiile de proxy (dacă este necesar) pentru conectarea la Internet extern.

Centrul de informare va descărca și va aplica ultimul FixPak de documentație, dacă există unul disponibil.

Pentru a descărca și aplica FixPak documentație manual:

1. Asigurați-vă că mașina dumneavoastră este conectată la Internet.
2. Deschideți pagina de suport DB2 de la:  
[www.ibm.com/software/data/db2/udb/winos2unix/support](http://www.ibm.com/software/data/db2/udb/winos2unix/support)
3. Urmați legătura de la versiunea 8 și căutați legătura "Documentation FixPaks".
4. Determinați dacă versiunea documentației locale este expirată prin compararea nivelului FixPak de documentație, cu nivelul documentației instalate. Această documentație curentă de pe mașină este la următorul nivel: **DB2 v8.1 GA**.
5. Dacă există disponibilă o versiune de documentație mai recentă, descărcați FixPak-ul aplicabil sistemului de operare. Există un FixPak pentru toate platformele Windows și unul pentru toate platformele UNIX.
6. Aplicarea FixPak-ului:
  - Pentru sistemele de operare Windos: FixPak-ul de documentație este un fișier zip care se extrage singur. Puneți FixPak-ul de documentație într-un director gol și rulați-l. Va crea o comandă **setup** pe care puteți să o rulați pentru instalarea FixPak-ului de documentație.
  - Pentru sistemele de operare Unix: FixPak-ul de documentație este un fișier comprimat tar.Z. Decomprasați și faceți untar la fișier. Va crea un director numit **delta\_install** cu un script numit **installdocfix**. Rulați acest script pentru a instala FixPak-ul de documentație.

#### Task-uri înrudite:

- "Copying files from the DB2 HTML Documentation CD to a Web server" în *Quick Beginnings for DB2 Personal Edition*

#### Referințe înrudite:

- "Privire generală asupra informațiilor tehnice DB2 Universal Database" la pagina 137

---

## Informații online de depanare DB2

Începând cu ediția DB2<sup>®</sup> UDB Versiunea 8, nu va mai exista un *Troubleshooting Guide (Ghid de depanare)*. Informațiile de depanare conținute în acest ghid au fost integrate în publicațiile DB2. Realizând aceasta, putem furniza cea mai nouă informație posibilă. Pentru a găsi informații despre utilitățile și funcțiile de depanare DB2, accesați Centrul de informare DB2 de pe oricare din unelte.

Vedeți site-ul pentru suport online DB2 dacă aveți probleme și deoriți ajutor la găsirea cauzelor și soluțiilor posibile. Site-ul de suport conține o bază de date mare, actualizată

constant de publicații DB2, note tehnice (TechNotes), înregistrări APAR (probleme ale produsului), FixPak-uri și alte resurse. Puteți folosi site-ul de suport pentru a căuta prin această bază de date și să găsiți soluții posibile la problemele dumneavoastră.

Accesați site-ul de suport online la [www.ibm.com/software/data/db2/udb/winos2unix/support](http://www.ibm.com/software/data/db2/udb/winos2unix/support) sau făcând clic pe butonul **Support online** în Centrul de informare DB2. Informațiile care se modifică frecvent, cum ar fi lista de erori interne DB2, sunt acum și ele disponibile pe acest site.

#### **Concepte înrudite:**

- “Centru de informare DB2 pentru subiecte” la pagina 151

---

## **Accesibilitatea**

Caracteristicile de accesibilitate ajută utilizatorii cu handicapuri fizice, cum ar fi o mobilitate redusă sau o vedere limitată, să folosească cu succes produsele de software. Acestea sunt principalele caracteristici de accesibilitate din DB2® Universal Database, Versiunea 8:

- DB2 permite să operați toate caracteristicile folosind tastatura în locul mouse-ului. Vedeți “Introducerea de la tastatură și navigarea”.
- DB2 permite personalizarea dimensiunii și culorii pentru fonturi. Vedeți “Ecran accesibil”.
- DB2 vă permite să primiți răspunsuri de alertare vizuale sau audio. Vedeți “Răspunsuri de alertare alternative”.
- DB2 suportă aplicațiile de accesibilitate care folosesc Java™ Accessibility API. Vedeți “Compatibilitate cu tehnologiile de asistare” la pagina 150.
- DB2 sosește cu documentație care este furnizată într-un format accesibil. Vedeți “Documentație accesibilă” la pagina 150.

## **Introducerea de la tastatură și navigarea**

### **Introducerea de la tastatură**

Puteți opera DB2 Tools folosind numai tastatura. Puteți folosi taste sau combinații de taste pentru a realiza majoritatea operațiilor care pot fi făcute folosind mouse-ul.

### **Focar tastatură**

În sistemele bazate pe UNIX, poziția focarului tastaturii este evidențiată, indicând ce zonă a ferestrei este activă și unde apăsările de taste au efect.

## **Ecran accesibil**

DB2 Tools au caracteristici care îmbunătățesc interfața cu utilizatorul și îmbunătățesc accesibilitatea utilizatorilor cu o vedere mai slabă. Aceste îmbunătățiri de accesibilitate includ suport pentru proprietăți de fonturi personalizabile.

### **Setări fonturi**

DB2 Tools vă permit să selectați culoarea, dimensiunea și fontul pentru textul din meniuri și din ferestrele de dialog, folosind caietul Tools Settings.

### **Fără dependență de culoare**

Nu este nevoie să distingeți între culori pentru a putea folosi oricare din funcțiile din acest produs.

## **Răspunsuri de alertare alternative**

Puteți specifica dacă vreți să primiți alerte prin răspunsuri vizuale sau audio, folosind caietul Tools Settings.

## Compatibilitate cu tehnologiile de asistare

Interfața DB2 Tools suportă API-ul Java Accessibility permițând folosirea de cititoare de ecran și alte tehnologii de asistare folosite de persoane cu handicap.

## Documentație accesibilă

Documentația pentru familia de produse DB2 este disponibilă în format HTML. Aceasta vă permite să vedeți documentația corespunzător cu preferințele setate în browser. Vă permite de asemenea folosirea unui cititor de ecran și alte tehnologii de asistare.

### Concepte înrudite:

- “Diagrame de sintaxă zecimal cu puncte” la pagina 152

---

## Îndrumare DB2

Îndrumările DB2<sup>®</sup> vă ajută să învățați despre diverse aspecte legate de baza de date universală DB2. Îndrumările furnizează lecții cu instrucțiuni pas-cu-pas în arii ce țin de dezvoltarea de aplicații, reglarea performanțelor interogărilor SQL, lucrul cu depozite de date, gestionarea metadatelor și dezvoltarea serviciilor Web folosind DB2.

### Înainte de a începe:

Înainte de a putea accesa aceste îndrumare folosind legăturile de mai jos, trebuie să instalați tutorialele de pe CD-ROM-ul *DB2 HTML Documentation*.

Dacă nu doriți să instalați aceste îndrumare, puteți vedea versiunile HTML ale îndrumarelor direct de pe CD-ul *DB2 HTML Documentation CD*. Versiunile PDF ale acestor îndrumare sunt de asemenea disponibile pe CD-ul *DB2 PDF Documentation CD*.

Unele lecții din îndrumare folosesc exemple de date sau cod. Vedeti fiecare îndrumar pentru o descriere a tuturor cerințelor preliminare pentru operația sa specifică.

### Îndrumările DB2 Universal Database:

Dacă ați instalat îndrumările de pe CD-ROM-ul *DB2 HTML Documentation*, puteți apăsa pe titlul unui îndrumar din lista următoare pentru a vedea acel îndrumar.

#### *Tutorial Business Intelligence: Introducere la Data Warehouse Center*

Realizează operații introductive despre depozitarea datelor folosind Data Warehouse Center.

#### *Business Intelligence Tutorial: Extended Lessons in Data Warehousing*

Realizează operații avansate de depozitare de date folosind Data Warehouse Center. (Nu este furnizat pe CD). Puteți descărca acest îndrumar din secțiunea Descărcare (Downloads) a site-ului web al Business Intelligence Solutions Web de la <http://www.ibm.com/software/data/bi/>.

#### *Tutorial Development Center pentru video online folosind Microsoft<sup>®</sup> Visual Basic*

Construiește diverse componente ale unei aplicații folosind Development Center Add-in pentru Microsoft Visual Basic.

#### *Tutorial centru catalog de informații*

Crează și gestionează un catalog cu informații pentru a localiza și folosi metadate, utilizând Information Catalog Center.

#### *Tutorial Video Central pentru e-business*

Dezvoltă și desfășoară o aplicație avansată DB2 Web Services folosind produse WebSphere<sup>®</sup>.

### *Tutorial Visual Explain*

Analizează, optimizează și ajustează instrucțiuni SQL pentru performanțe mai bune folosind Visual Explain.

---

## Centru de informare DB2 pentru subiecte

Centrul de informare DB2<sup>®</sup> vă oferă acces la toate informațiile de care aveți nevoie pentru a beneficia pe deplin de DB2 Universal Database™, DB2 Connect™ în activitatea dumneavoastră. Centrul de informare DB2 documentează de asemenea caracteristicile și componentele principale DB2 inclusiv replicarea, depozitarea de date, Centrul catalog de informații, Life Sciences Data Connect și extinderile DB2.

Centrul de informare DB2 accesat de la un browser are următoarele caracteristici:

### **Documentație actualizată regulat**

Păstrați-vă subiectele actualizate (up-to-date) descărcând HTML-uri actualizate.

### **Căutare (Search)**

Căutați toate subiectele instalate pe stația dumneavoastră de lucru apăsând **Search** în bara de unelte de navigare.

### **Arborele de navigare integrat**

Localizați orice subiect în biblioteca DB2 dintr-un singur arbore de navigare.

Arborele de navigare este organizat după tipul informației după cum urmează:

- Operațiile furnizează instrucțiuni pas-cu-pas despre cum să atingeți un anumit scop.
- Conceptele furnizează o privire generală a unui subiect.
- Subiectele cu referințe furnizează informații detaliate despre un subiect, inclusiv instrucțiuni și sintaxa comenzilor, mesaje de ajutor, cerințe.

### **Indexul master**

Accesează informațiile din subiecte și din ajutorul pentru unelte dintr-un index master. Indexul este organizat în ordine alfabetică după termenul de indexare.

### **Glosarul master**

Glosarul master definește termenii folosiți în Centrul de informare DB2. Glosarul este organizat în ordine alfabetică după termenul din glosar.

### **Task-uri înrudite:**

- “Actualizarea documentației HTML instalată pe mașina dumneavoastră” la pagina 147

---

## Instalarea Centrului de informare DB2 (UNIX)

### **Cerințe preliminare:**

### **Restricții:**

### **Procedura:**

- 1.
- 2.

### **Task-uri înrudite:**

- “Instalarea Centrului de informare DB2 (Windows)” la pagina 152

---

## Instalarea Centrului de informare DB2 (Windows)

### Cerințe preliminare:

### Restricții:

### Procedura:

- 1.
- 2.

### Task-uri înrudite:

- “Instalarea Centrului de informare DB2 (UNIX)” la pagina 151

---

## Configurarea browser-ului să afișeze informațiile în limba preferată

Când afișați Centrul de informare DB2 în browser, el încearcă să afișeze subiecte în limba specificată în preferințele browser-ului. Dacă un subiect nu a fost tradus în limba preferată, Centrul de informare DB2 afișează subiectul în engleză.

### Procedură:

Pentru a afișa limba preferată în browser-ul web Internet Explorer:

1. În Internet Explorer, faceți clic pe **Tools** → **Internet Options** → butonul **Languages...** Se deschide fereastra Preferințe de limbă.
2. Asigurați-vă că limba preferată este specificată în prima intrare din lista de limbi.
  - Pentru a adăuga o nouă limbă la listă, faceți clic pe butonul **Add...**
  - Pentru a muta o limbă în fruntea listei, selectați limba și faceți clic pe butonul **Move Up** până când limba este prima din listă.

Pentru a afișa subiecte în limba preferată în browser-ul de web Mozilla:

1. În Mozilla, selectați **Edit** → **Preferences** → butonul **Languages**. Este afișat panoul Languages în fereastra Preferences.
2. Asigurați-vă că limba preferată este specificată în prima intrare din lista de limbi.
  - Pentru a adăuga o nouă limbă la listă, faceți clic pe butonul **Add...** pentru a adăuga o limbă din fereastra Add Languages.
  - Pentru a muta o limbă în fruntea listei, selectați limba și faceți clic pe butonul **Move Up** până când limba este prima din listă.

---

## Diagrame de sintaxă zecimal cu puncte

Diagramele de sintaxă sunt disponibile în format zecimal cu puncte, care reprezintă o caracteristică de accesibilitate. Diagramele de sintaxă zecimal cu puncte sunt disponibile numai dacă accesați documentația online folosind un cititor de ecran.

În format zecimal cu puncte, fiecare element de sintaxă este scris într-o linie separată. Dacă unul sau mai multe elemente de sintaxă sunt întotdeauna prezente împreună (sau întotdeauna absente împreună), ele pot apărea în aceeași linie, deoarece pot fi considerate ca un singur element compus de sintaxă.

Fiecare linie începe cu un număr zecimal cu puncte; de exemplu, 3 sau 3.1 sau 3.1.1. Pentru a auzi aceste numere corect, asigurați-vă că cititorul de ecran este setat să citească punctuația.

Toate elementele de sintaxă care au aceleași numere zecimale cu punct (de exemplu, toate elementele de sintaxă care au numărul 3.1) sunt alternative care se exclud mutual. Dacă auziți liniile 3.1 USERID și 3.1 SYSTEMID, știți că sintaxa poate include fie USERID, fie SYSTEMID, dar nu pe amândouă.

Nivelul numerelor zecimale cu punct denotă nivelul imbricării. De exemplu, dacă un element de sintaxă cu numărul zecimal cu punct 3 este urmat de o serie de elemente de sintaxă cu numărul zecimal cu punct 3.1, toate elementele de sintaxă numerotate cu 3.1 sunt subordonate elementului de sintaxă numerotat cu 3.

Unele cuvinte și simboluri sunt folosite lângă numerele zecimale cu punct pentru a adăuga informații despre elementele de sintaxă. Uneori, aceste cuvinte și simboluri pot apărea la începutul fiecărui element. Pentru ușurința identificării, dacă simbolul sau cuvântul este parte a unui element de sintaxă, atunci este precedat de caracterul backslash (\). Simbolul \* poate fi folosit lângă un număr zecimal cu puncte pentru a indica faptul că elementul de sintaxă se repetă. De exemplu, elementul de sintaxă \*FILE cu numărul zecimal cu punct 3 este dat cu formatul 3 \\* FILE. Formatul 3\* FILE indică faptul că elementul de sintaxă FILE se repetă. Formatul 3\* \\* FILE indică faptul că elementul de sintaxă \* FILE se repetă.

Caracterele precum virgula, care sunt folosite pentru a separa șiruri din elementele de sintaxă, sunt arătate în sintaxă chiar înainte de elementele pe care le separă. Aceste caractere pot apărea pe aceeași linie cu fiecare element sau pe o linie separată cu același număr zecimal cu puncte ca și elementele relevante. Linia poate arăta un alt simbol care să dea informații despre elementele de sintaxă. De exemplu, liniile 5.1\*, 5.1 LASTRUN și 5.1 DELETE înseamnă că dacă folosiți mai mult de unul din elementele de sintaxă LASTRUN și DELETE, elementele trebuie să fie separate de o virgulă. Dacă nu se dă nici un separator, se presupune că folosiți un spațiu (blank) pentru a separa fiecare element de sintaxă.

Dacă un element de sintaxă este precedat de un simbol %, această indică o referință care este definită în altă parte. Șirul care urmează simbolului % este mai degrabă numele unui fragment de sintaxă, decât un literal. De exemplu, linia 2.1 %OP1 înseamnă că vă veți referi la fragmentul de sintaxă separat OP1.

Următoarele cuvinte și simboluri sunt folosite lângă numerele zecimale cu punct:

- ? înseamnă un element de sintaxă opțional. Un număr zecimal cu puncte urmat de simbolul ? indică faptul că toate elementele de sintaxă cu un număr zecimal cu puncte corespunzător și toate elementele de sintaxă subordonate sunt opționale. Dacă există numai un element de sintaxă cu un număr zecimal cu puncte simbolul ? este afișat pe aceeași linie ca și elementul de sintaxă, (de exemplu 5? NOTIFY). Dacă există mai mult de un element de sintaxă cu un număr zecimal cu puncte simbolul ? este afișat pe o linie singură, urmat de elementele de sintaxă care sunt opționale. De exemplu, dacă auziți liniile 5 ?, 5 NOTIFY și 5 UPDATE, știți că elementele de sintaxă NOTIFY și UPDATE sunt opționale; adică puteți alege unul sau nici unul dintre ele. Simbolul ? este echivalent cu o linie de ocolire într-o diagramă tip cale ferată.
- ! înseamnă un element de sintaxă implicit. Un număr zecimal cu puncte urmat de simbolul ! și de un element de sintaxă indică faptul că elementul de sintaxă este opțiunea implicită pentru toate elementele de sintaxă care împart același număr zecimal cu puncte. Numai unul din elementele de sintaxă care împart același număr zecimal cu puncte poate specifica un simbol !. De exemplu, dacă auziți liniile 2? FILE, 2.1! (KEEP) și 2.1 (DELETE), știți că (KEEP) este opțiunea implicită pentru cuvântul cheie FILE. În acest exemplu, dacă includeți cuvântul cheie FILE, dar nu specificați o opțiune, se va aplica opțiunea implicită KEEP. O opțiune implicită se va aplica la următorul număr zecimal cu punct mai mare. În acest exemplu, dacă cuvântul cheie FILE este omis, se folosește implicit FILE(KEEP). Dar, dacă auziți liniile 2? FILE, 2.1, 2.1.1! (KEEP) și 2.1.1 (DELETE), opțiunea implicită



KEEP se aplică numai la următorul număr zecimal cu puncte mai mare, 2.1 (care nu are un cuvânt cheie asociat) și nu se aplică la 2? FILE. Nu se folosește nimic dacă este omis cuvântul cheie FILE.

- \* înseamnă un element de sintaxă care poate fi repetat de 0 sau mai multe ori. Un număr zecimal cu puncte urmat de simbolul \* indică faptul că acest element de sintaxă poate fi folosit de 0 sau mai multe ori; adică este opțional și poate fi repetat. De exemplu, dacă auziți linia 5.1\* data area, știți că puteți include mai mult de o data area (zonă de date) sau puteți include nici una. Dacă auziți liniile 3\*, 3 HOST și 3 STATE, știți că puteți include HOST, STATE, ambele împreună sau nimic.

**Note:**

1. Dacă un număr zecimal cu puncte are lângă el un asterisc (\*) și există doar un element cu acest număr zecimal cu punct, puteți repeta același element mai mult decât o dată.
  2. Dacă un număr zecimal cu puncte are lângă el un asterisc și mai multe elemente au acel număr zecimal cu punct, puteți folosi mai mult de un element din listă, dar nu puteți folosi fiecare element mai mult de o singură dată. În exemplu anterior, puteați scrie HOST STATE, dar nu puteați scrie HOST HOST.
  3. Simbolul \* este echivalent cu o buclă într-o diagramă de sintaxă tip cale ferată.
- + înseamnă un element de sintaxă care trebuie inclus o dată sau mai multe ori. Un număr zecimal cu puncte urmat de simbolul + indică faptul că acest element de sintaxă trebuie inclus o dată sau de mai multe ori; adică trebuie inclus cel puțin o dată și poate fi repetat. De exemplu, dacă auziți linia 6.1+ dataarea, trebuie să includeți cel puțin o dataarea (zonă de date). Dacă auziți liniile 2+, 2 HOST și 2 STATE, știți că trebuie să includeți HOST, STATE sau ambele. Ca și pentru simbolul \*, puteți repeta doar un element particular, dacă este singurul element cu acel număr zecimal cu puncte. Simbolul +, ca și simbolul \* este echivalent cu o buclă la o diagramă de sintaxă de tip cale ferată.

**Referințe înrudite:**

- “How to read the syntax diagrams” în *SQL Reference, Volume 2*

---

## Certificare Common Criteria pentru produsele DB2 Universal Database

Pentru Versiunea 8.2, produsele DB2 Universal Database (DB2 UDB) sunt certificate conform cu Common Criteria EAL4. Următoarele produse sunt certificate pe următoarele sisteme de operare.

*Tabela 17. Configurații DB2 Universal Database certificate*

	Windows 2000	Linux SuSE	AIX 5.2	Solaris Operating Environment, 8
Enterprise Server Edition <b>Notă:</b> Nuami mediu cu o singură partiție.	Da	Da	Da	Da
Workgroup Server Edition	Da	Da	Da	Da
Personal Edition	Da	Da	-	-
Express Edition	Da	Da	-	-

**Note:**

1. Configurațiile DB2 UDB sunt certificate Common-Criteria numai pe hardware de 32 de biți. Configurațiile de 64 de biți nu sunt certificate.
2. Configurațiile DB2 UDB pe mediul Linux SuSE sunt certificate Common-Criteria numai pe hardware bazat pe Intel.



Pentru informații despre instalarea și configurarea unui sistem DB2 UDB care se conformează cu Common Criteria EAL4, vedeți următoarele cărți:

- *DB2 Universal Database Common Criteria Certification: Installing DB2 Universal Database Enterprise Server Edition and DB2 Universal Database Workgroup Server Edition*
- *DB2 Universal Database Common Criteria Certification: Installing DB2 Universal Database Personal Edition*
- *DB2 Universal Database Common Criteria Certification: Installing DB2 Universal Database Express Edition*
- *DB2 Universal Database Common Criteria Certification: Administration and User Documentation*

Cărțile sunt disponibile în format PDF în DB2 Information Management Library.

Pentru informații despre Common Criteria, vedeți pagina de bază Common Criteria.



---

## Anexa B. Observații

Este posibil ca IBM poate să nu ofere în toate țările produsele, serviciile și caracteristicile discutate în acest document. Consultați reprezentantul IBM local pentru informații asupra produselor și serviciilor care sunt disponibile curent în zona dumneavoastră. Orice referire la un produs, program sau serviciu IBM nu înseamnă că se afirmă sau se sugerează că doar acel produs, program sau serviciu IBM poate fi folosit. Poate fi folosit în locul lui orice produs, program sau serviciu echivalent funcțional care nu încalcă nici un drept de proprietate intelectuală IBM. Însă este responsabilitatea utilizatorului să evalueze și să verifice funcționarea oricărui produs, program sau serviciu non-IBM.

IBM poate avea brevete sau aplicații în curs de brevetare care să acopere subiectele descrise în acest document. Prin furnizarea acestui document nu vi se oferă nici o licență pentru aceste brevete. Puteți trimite solicitări de licență, în scris, la:

IBM Director of Licensing  
IBM Corporation  
North Castle Drive  
Armonk, NY 10504-1785  
U.S.A.

Pentru întrebări în legătură cu informații de licență pentru DBCS (double-byte), contactați IBM Intellectual Property Department în țara/regiunea dumneavoastră sau trimiteți întrebările în scris la:

IBM World Trade Asia Corporation  
Licensing  
2-31 Roppongi 3-chome, Minato-ku  
Tokyo 106, Japan

**Paragraful următor nu se aplică Marii Britanii sau în alte țări/regiuni în care aceste prevederi sunt incompatibile cu legile locale:** INTERNATIONAL BUSINESS MACHINES CORPORATION OFERĂ ACEASTĂ PUBLICAȚIE “CA ATARE” FĂRĂ NICI UN FEL DE GARANȚIE, EXPRIMATE SAU PRESUPUSE, INCLUZÂND, DAR NELIMITÂNDU-SE LA ELE, GARANȚIILE SUBÎNȚELESE DE NEÎNCĂLCARE A UNUI DREP, DE VANDABILITATE SAU DE POTRIVIRE PENTRU UN ANUMIT SCOP. Unele state nu acceptă declinarea responsabilității în anumite tranzacții pentru garanțiile exprese sau implicite; de aceea această declarație s-ar putea să nu fie aplicabilă pentru dumneavoastră.

Aceste informații pot include inexactități tehnice sau erori de tipărire. În mod periodic se aduc schimbări informației de aici; aceste schimbări vor fi încorporate în ediții noi ale publicației. Se poate ca IBM să aducă îmbunătățiri și/sau schimbări în produsul(produsele) și/sau programul(programele) descrise în această publicație oricând fără aviz.

Orice referire în cadrul acestor informații la situri web altele decât IBM sunt furnizate doar pentru comoditate și nu servesc în nici un caz drept sprijin pentru acele situri web. Materialele de pe acele situri web nu fac parte din materialele pentru acest produs IBM și folosirea acelor situri web o veți face pe propriul dumneavoastră risc.

IBM poate folosi sau distribui orice informație pe care o furnizați în orice mod crede de cuviință fără să-și asume nici o obligație către dumneavoastră.

Licențele acestui program care doresc să obțină informații despre el pentru a da posibilitatea: (i) schimbului de informații între programe create independent și alte programe (inclusiv cel de față) și (ii) folosirea mutuală a informației care s-a schimbat, vor trebui să contacteze:

IBM Canada Limited  
Office of the Lab Director  
8200 Warden Avenue  
Markham, Ontario  
L6G 1C7  
CANADA

Astfel de informații pot fi disponibile, subiect al termenilor și condițiilor corespunzătoare, incluzând în unele cazuri plata unui onorariu.

Programul cu licență descris în acest document și toate materialele cu licență disponibile pentru el sunt furnizate de către IBM în termenii stabiliți de IBM Customer Agreement, IBM International Program License Agreement sau orice acord echivalent.

Orice date despre performanță conținute aici au fost determinate într-un mediu controlat. Prin urmare, rezultatele obținute în alte medii de operare pot varia semnificativ. Unele măsurători se poate să fi fost făcute pe sisteme la nivel de dezvoltare și nu există nici o garanție că aceste măsurători vor fi aceleași pe sistemele disponibile în general. Mai mult, unele măsurători pot fi estimări obținute prin extrapolare. Rezultatele reale pot varia. Utilizatorii acestui document ar trebui să verifice informațiile aplicabile mediului lor de lucru specific.

Informațiile referitoare la produse non-IBM au fost obținute de la furnizorii acelor produse, din anunțurile lor publicate sau alte surse disponibile publicului. IBM nu a testat acele produse și nu poate confirma cu acuratețe performanța, compatibilitatea sau orice alte afirmații referitoare la produse non-IBM. Întrebările despre capacitățile produselor non-IBM ar trebui adresate furnizorilor acelor produse.

Toate declarațiile privind direcția viitoare sau intențiile IBM sunt un subiect ce poate fi schimbat sau retractat fără aviz și reprezintă doar scopuri și obiective.

Aceste informații pot conține exemple de date și rapoarte folosite în operațiile de afaceri zilnice. Pentru a le ilustra cât mai complet cu putință, exemplele includ nume de persoane, companii, mărci și produse. Toate aceste nume sunt fictive și orice asemănare cu numele și adresele folosite de o întreprindere de afaceri reală este o simplă coincidență.

#### LICENȚĂ COPYRIGHTE:

Aceste informații pot conține exemple de programe de aplicații, în limbaj sursă, care ilustrează tehnici de programare pe diferite platforme de operare. Puteți copia, modifica și distribui aceste programe-exemplu în orice formă fără plată către IBM, în scopuri ce țin de dezvoltare, utilizare, marketing sau distribuție de programe de aplicații, în conformitate cu interfața de programare a aplicațiilor pentru platforma de operare pentru care sunt scrise exemplele de programe. Aceste exemple nu au fost testate detaliat în toate condițiile. Prin urmare, IBM nu poate garanta sau implica încrederea în aceste programe, deservirea sau funcționarea lor.

Orice copie sau orice porțiune din aceste programe-exemplu sau orice lucru derivat din ele trebuie să includă un anunț de copyright după cum urmează:

© (Numele companiei dumneavoastră) (year). Părți din acest cod sunt derivate de la IBM Corp. Programe exemplu. © Copyright IBM Corp. *\_introduceți anul sau anii\_*. Toate drepturile sunt rezervate.

---

## Mărci comerciale

Următorii termeni sunt mărci ale International Business Machines Corporation în Statele Unite, în alte țări sau ambele și au fost utilizați în cel puțin unul dintre documentele din biblioteca de documentație DB2 UDB.

ACF/VTAM	LAN Distance
AISPO	MVS
AIX	MVS/ESA
AIXwindows	MVS/XA
AnyNet	Net.Data
APPN	NetView
AS/400	OS/390
BookManager	OS/400
C Set++	PowerPC
C/370	pSeries
CICS	QBIC
Database 2	QMF
DataHub	RACF
DataJoiner	RISC System/6000
DataPropagator	RS/6000
DataRefresher	S/370
DB2	SP
DB2 Connect	SQL/400
DB2 Extenders	SQL/DS
DB2 OLAP Server	System/370
DB2 Query Patroller	System/390
DB2 Universal Database	SystemView
Distributed Relational Database Architecture	Tivoli
DRDA	VisualAge
eServer	VM/ESA
Extended Services	VSE/ESA
FFST	VTAM
First Failure Support Technology	WebExplorer
IBM	WebSphere
IMS	WIN-OS/2
IMS/ESA	z/OS
iSeries	zSeries

Următorii termeni sunt mărci sau mărci înregistrate ale altor companii și au fost utilizați în cel puțin unul dintre documentele din biblioteca de documentație DB2 UDB:

Microsoft, Windows, Windows NT și emblema Windows sunt mărci comerciale ale Microsoft Corporation în Statele Unite, în alte țări sau ambele.

Intel și Pentium sunt mărci ale Intel Corporation în Statele Unite, alte țări sau ambele.

Java și toate mărcile comerciale ce au la bază Java sunt mărci comerciale ale Sun Microsystems, Inc. în Statele Unite, în alte țări sau ambele.

UNIX este o marcă comercială înregistrată a The Open Group în Statele Unite și în alte țări.

Alte nume de companii, produse sau servicii pot fi mărci comerciale sau mărci de servicii ale altora.



# Index

## A

- accesibilitate
  - caracteristici 149
  - diagrame sintaxă zecimal cu puncte 152
- acesare
  - servere gazdă
    - IBM eNetwork Communication Server V5 pentru AIX 13
    - pentru sistemele de operare Windows pe 32 de biți 13
    - SNA API Client 12
- ACF/VTAM 84
- Actualizare
  - documentație HTML 147
- adaptor resursă, VM 74
- ADDRDBDIRE 47
- adresa IP
  - rezolvare 4
- adresă
  - adaptor local 128
  - nume punct de control 128
  - UL local 128
- AIX
  - configurare
    - Bull SNA 14
- ajutor
  - afișare 147, 152
  - online, acesare 144
  - pentru comenzi
    - invocare 146
  - pentru instrucțiuni SQL
    - invocare 146
  - pentru mesaje
    - invocare 145
- ajutor comandă
  - invocare 146
- ajutor instrucțiuni SQL
  - invocare 146
- ajutor mesaj
  - invocare 145
- APPC (Advanced Program-to-Program Communication)
  - Bull SNA 14
  - Communications Server pentru Windows NT SNA Client 12
  - configurare manuală 11
  - configurare utilizând Asistentul de configurare (CA) 125
  - SNAplusLink 13
- APPN (advanced peer-to-peer networking), creare liste de locații 31
- autorizare implicită, iSeries 109
- AVS
  - componentă a VM 74
  - considerații limită de sesiune AVS 83
  - definire poartă, exemplu 35
- AXE 84

## B

- bază de date gazdă
  - testarea conexiunii 9, 18
- bază de date relațională
  - al directorului
    - descriere, OS/400 29
    - informații intrare, iSeries 30
  - subsistem 128
- baze de date
  - catalogare 7, 16
- baze de date relaționale distribuite
  - conexiuni DB2 67
- baze de de date destinație
  - subsistem 128

## C

- catalogare
  - baze de date 7, 16
    - bază de date DCS la distanță 7, 15
    - valori parametri TCP/IP 128
  - nod APPC 14
  - nod TCP/IP 6
- cărți tipărite, comandare 144
- CCSID (identificator set de caractere codat)
  - implicit DB2 117
  - VM
    - afișare curent 120
    - implicit 120
- CDB (bază de date de comunicații) 27
- Centru de informare
  - instalare 151, 152
- Centru de informare DB2 151
  - invocare 147
- CICS (Customer Information Control System)
  - sesiuni CICS LU 6.2
    - instalare 55
    - stabilire pentru VSE 55
- CICS(ISC) 84
- CICS(SPM) 84
- CICS(TRUE) 84
- clasa de serviciu
  - creare 31
  - descriere OS/400 31
- CLI (call level interface)
  - aplicații
    - CURRENTPACKAGESET 67
  - comanda ADDRDBDIRE (add relational database directory entry command) 29
  - comanda ADDSVRAUTE 49
  - comanda CHGNETA 31
  - comanda CRTCFGL 31
  - comanda CRTCOSD 31
  - comanda CRTCTLAPPC 31
  - comanda CRTCTLHOST 31
  - comanda CRTDDMTCPA command 94
  - comanda CRTDEVAPPC 31
  - comanda CRTLINETH 31
  - comanda CRTLINS DLC 31
  - comanda CRTLINTRN 31

- comanda CRTLINX25 31
- comanda CRTMODD 31
- comanda de schimbare atribute de rețea 31
- comanda GRTOBJAUT 94, 111
- comanda RELOAD PACKAGE 111
- comanda RVKOBJAUT
  - autorizarea \*USE 94
  - securitate 111
- comanda SET COMDIR 37
- comanda STRTCPSVR 49
- comanda VRYCFG 31
- comanda WRKCFGSTS 31
- comandare cărți
  - tipărire fișiere PDF 143
- comandare cărți DB2 tipărite 144
- comdir (director de comunicații)
  - CMS 37
  - comanda SET COMDIR 37
  - intrare exemplu 37, 111
  - VM 74
- Communications Server pentru Windows NT SNA Client
  - configurare manuală 12
  - versiunea necesară 12
- comunicații
  - APPC 125
  - director, mediu VM 37, 74
  - exemplu flux VM 74
  - exemplu flux, SQL/DS VSE 84
  - subsistem
    - solicitant de aplicații DB2 72
    - solicitant de aplicații OS/400 31
  - tabele baze de date, DB2
    - SYSIBM.LOCATIONS 27
  - testarea conexiunilor 9, 18
- configurare
  - Bull SNA 14
  - de configurare, schimbarea parolei 67
  - IBM eNetwork Communications Server
    - pentru AIX 13
  - IBM eNetwork Communications Server pentru Windows NT SNA API Client 12
  - iSeries 128
  - liste, creare 31
  - Microsoft SNA Client 13
  - Microsoft SNA Server 13
  - server de aplicații 128
  - server DRDA 128
  - SNAPLUS 13
  - SQLDS 128
  - VM 128
  - VSE 128
- convenții de numire
  - bază de date la distanță, OS/400 47
  - bază de date locală, OS/400 29
- cuvant cheie CURRENTPACKAGESET
  - CLI/ODBC 67

## D

DB2 Connect  
actualizarea profilului APPC 12  
server  
configurare TCP/IP 4

DB2 pentru VM  
privire generală DRDA 74

DB2 Universal Database pentru iSeries 74  
client TCP/IP DRDA  
considerații 49  
setare 49  
conexiuni TCP/IP, setare 30  
Manual Programarea bazelor de date  
distribuite 49  
server TCP/IP DRDA  
considerații 49  
setare 49

DB2 Universal Database pentru OS/390 și  
z/OS 23  
conexiuni baze de date distribuite  
comparație 67  
definirea sistemului local  
TCP/IP 26  
DYNAMICRULES(BIND) 67  
facilități de atașare  
CAF 67  
CICS/ESA 67  
DDF 67  
IMS/ESA 67  
TSO 67  
îmbunătățiri de securitate 67  
coduri de securitate extinse 67  
securitate TCP/IP deja verificată 67  
securitatea aplicațiilor desktop ODBC  
și Java 67  
suport schimbare parolă 67  
numere de porturi 26

DB2 Universal Database pentru VM  
privire generală 74

DB2 Universal Database pentru VSE  
componente de procesare distribuită  
ACF/VTAM 84  
AXE 84  
CICS(ISC) 84  
CICS(SPM) 84  
CICS(TRUE) 84  
Director DBNAME 84  
XPCC 84  
privire generală 84

DB2 Universal Database pentru VSE și VM  
conexiuni gazdă 74

DDF (facilitate de date distribuite) 23  
depanare  
informații online 148  
descriere de controler, creare 31  
descrieri de controler, creare 31  
descrieri mod, creare 31  
diagrame sintaxă zecimal cu puncte  
dimensionare RU  
server de aplicații OS/400 47  
solicitant aplicație 73  
solicitant de aplicații OS/400 31  
solicitant de aplicații SQL/DS 84  
VM 84

Director DBNAME 84  
director de comunicații CMS  
catalogare RDB\_NAME-uri 37

director de comunicații CMS (*continuare*)  
exemplu de intrare 100  
securitate 111  
director nume bază de date 84  
documentație  
afișare 147  
documentație HTML  
actualizare 147

## E

element de rețea DBNAME (VSE sau  
VM) 128  
exemple  
acordarea autorizării, OS/400 111  
comanda ADDRDBDIRE 29  
DB2 pentrusolicitant aplicație și server de  
aplicații VM 74  
definire poartă AVS 35  
fișier de nume RESID, SQL/DS pe  
VM 61  
flux comunicații, SQL/DS VSE 84  
flux de comunicații server de aplicații 74  
flux de comunicații VM 74  
instrucțiune VTAM APPL 24  
intrare director de comunicații CMS 100  
intrări comdir VM 111  
panou de instalare DSNTIPR 24  
traducere nume de ieșire  
SNA 103  
TCP/IP 103

## F

facilitate acces servicii transparent  
(TSAF) 74  
facilități de atașare 67  
fișier de servicii  
actualizare 5  
foaie de lucru valoare parametru  
configurare TCP/IP 127  
foi de lucru  
valoarea parametru  
APPC 128  
foi de lucru LU 128

## G

GCS (group control system) 74

## H

HP-UX  
configurare SNAPplus2 14

## I

IDENT 74  
incapacitate 149  
informații de rețea  
serverul de aplicații SQL/DS VSE  
setare 55  
SON(session outage notification) 55  
solicitant de aplicații OS/400 29  
solicitant de aplicații SQL/DS 35

informații de rețea (*continuare*)  
SQL/DS pe serverul de aplicații VM 61  
instalare  
Centru de informare 151, 152  
instrucțiune APPCPASS 111  
instrucțiunea SET CURRENT  
PACKAGESET 67  
instrucțiuni APPL 24  
invocare  
ajutor comandă 146  
ajutor instrucțiuni SQL 146  
ajutor mesaj 145  
IRLM 67  
iSeries  
DB2 UDB 74  
testarea conexiunii 9, 18

## Î

îndrumare 150  
Îndrumare DB2 150  
înregistrare DDF 24

## L

limite de sesiune  
SQL/DS pe VM 83  
linie  
descrieri, creare 31  
LOCATION NAME (z/OS, OS/390) 128  
locații  
bază de date la distanță, director de  
comunicații CMS 37  
la distanță 106  
legătură la distanță 128  
tranzacție la distanță 128

## M

manager puncte de sincronizare (SPM)  
parametrul SYNCPNT 74  
manageri tranzacții  
foaie de lucru de planificare 128  
Microsoft SNA Client  
configurare 13  
versiunea necesară 13  
Microsoft SNA Server  
configurare 13  
MODEENT 128  
modificare număr de sesiuni (CNOS) 131  
MVS (Multiple Virtual Storage)  
spații de adresă DB2 67

## N

NetView 67  
nume  
partener 128  
UL local 128  
nume destinație simbolică 128  
nume mod 128  
nume punct de control 128  
nume RDB (iSeries) 128  
nume utilizatori finali  
securitate 89



nume utilizatori finali *(continuare)*  
server de aplicații  
OS/400 94  
SQL/DS pe VM 97  
solicitant aplicație  
DB2 103  
OS/400 109  
SQL/DS pe VM 111  
numere de porturi  
DB2 UDB pentru OS/390 și z/OS 26

## O

ODBC (open database connectivity)  
aplicații  
CURRENTPACKAGESET 67  
OS/390  
considerații de securitate 89  
OS/400  
acriarea comunicării 31  
atribute de rețea 31

## P

pachete  
securitate manager de baze de date  
SQL/DS 100  
SQL dinamic 97  
SQL static 97  
securitate server de aplicații DB2 93  
panou de instalare DSNTIPR  
exemplu 24  
parametri BSDS (bootstrap data set)  
actualizare 24, 45  
parametru CHARNAME 74, 111, 120  
parametru RMTUSERS 84  
parametrul PROTOCOL  
opțiuni  
AUTO 74  
SQLDS 74  
parametrul SYNCNT 74, 84  
parole  
suport de modificare (OS/390 și z/OS) 67  
procesor linie de comandă (CLP)  
catalogarea unui nod 6, 14  
protocoale de comunicații  
APPC 11  
protocol privat, OS/390 și z/OS 67  
PU 128

## R

recuperare resurse coordonată (CRR) 74  
reprezentarea datelor  
server de aplicații DB2 94, 117  
server de aplicații OS/400 117  
solicitant de aplicații DB2 117  
solicitant de aplicații SQL/DS 111  
SQL/DS pe serverul de aplicații VM 120  
RESID (ID resursă)  
fișier de nume, SQL/DS pe VM,  
exemple 61  
nume program de tranzacție (TPN) 61  
rețea  
rețea 128  
schimb de mesaje 23

rețea *(continuare)*  
subsistem 128

## S

schimb  
de mesaje, DB2 23  
schimbul de mesaje, DB2 23  
scurtături tastatură  
suport pentru 149  
securitate  
acordare autorizare  
exemplu, iSeries 111  
autorizare implicită  
iSeries 109  
coduri extinse  
OS/390 și z/OS 67  
manager de baze de date  
executare aplicații la distanță 108  
iSeries 94  
legare aplicații la distanță 108  
servere de aplicații VM 97  
nume utilizatori finali  
server de aplicații DB2 89  
servere de aplicații OS/400 94  
servere de aplicații VM 97  
solicitant de aplicații DB2 103  
solicitant de aplicații OS/400 109  
solicitant de aplicații SQL/DS 111  
procesare  
server de aplicații DB2 89  
SQL/DS pe serverul de aplicații  
VM 97  
rețea  
server de aplicații DB2 92  
server de aplicații iSeries 94  
servere de aplicații VM 97  
solicitant de aplicații OS/400 109  
solicitant de aplicații SQL/DS 111  
servere de aplicații  
manager de baze de date DB2 93  
OS/390 89  
SQL/DS pe subsistemul VM 97  
subsistem DB2 94  
z/OS 89  
sistem iSeries 94  
sistem la distanță 103  
solicitanți de aplicații  
manager de baze de date DB2 108  
manager de baze de date OS/400 109  
manager de baze de date  
SQL/DS 111  
OS/390 103  
OS/400 109  
rețea DB2 106  
subsistem DB2 108  
z/OS 103  
subsistem SQL/DS 111  
verificare de-la-cine în DB2 89  
securitate de atașare, nivele 100  
securitate de sistem, OS/400 109  
securitate manager de baze de date  
server de aplicații DB2 93  
solicitant de aplicații DB2 108  
solicitant de aplicații OS/400 109  
solicitant de aplicații SQL/DS  
execuție aplicație 111

securitate manager de baze de date  
*(continuare)*  
solicitant de aplicații SQL/DS  
*(continuare)*  
procesare aplicație 111  
traducere nume de ieșire 111  
SQL/DS pe serverul de aplicații VM 97  
securitate rețea  
DB2 UDB pentru serverul de aplicații  
iSeries 94  
server de aplicații DB2 92  
solicitant de aplicații DB2 106  
solicitant de aplicații SQL/DS 111  
SQL/DS pe serverul de aplicații VM 97  
server CRR (coordinated resource  
recovery) 74  
servere de aplicații  
OS/390 și z/OS 43  
OS/400  
descriere 47  
dimensionare RU 47  
nume utilizatori finali 94  
numire bază de date la distanță 47  
reprezentarea datelor 117  
securitate 94  
setare 47  
reprezentarea datelor 94, 117  
securitate  
manager de baze de date 93  
nume utilizatori finali 89  
rețea 92  
subsistem 94  
securitate manager de baze de date 93  
setare 43  
SNA 43  
SQL/DS VM  
descriere 61  
informații de rețea 61  
nume utilizatori finali 97  
reprezentarea datelor 120  
securitate 97  
setare 61  
traducere nume de intrare 97  
SQL/DS VSE  
descriere 59  
informații de rețea 55  
pornire 59  
securitate 100  
setare 55  
traducere nume de intrare 89  
verificare control de-la-cine 89  
VSE  
limitări 84  
parametru de pornire RMTUSERS 84  
parametru de pornire SYNCNT 84  
servere de baze de date gazdă  
legarea utilitatelor și a aplicațiilor 9, 17  
servere de baze de date iSeries  
legarea utilitatelor și a aplicațiilor 9, 17  
servere secundare  
stabilirea unei conexiuni 67  
sistem control grup (GCS) 74  
sistem local  
definire DB2 (VTAM) 24  
solicitant de aplicații SQL/DS 35

- SNA (Systems Network Architecture)
  - configurare
    - SNAPLus 13
  - configurare manuală
    - Communications Server pentru Windows NT SNA Client 12
    - Microsoft SNA Client 13
- SNAPLus2, configurare pentru HP-UX 14
- solicitanți de aplicații 23, 108
  - conexiuni (SNA) 43
  - definire sistem la distanță 27
  - definiție sistem local (VTAM) 24
  - dimensionare RU 73
  - OS/400
    - definiri de comunicații 31
    - dimensionare RU 31
    - informații de rețea 29
    - securitate 109
    - setare 29
    - transmisie 31
  - reprezentarea datelor 117
  - securitate
    - manager de baze de date 108
    - nume utilizatori finali 103
    - rețea 106
    - subsistem 108
  - SQL/DS VM
    - activare 126
    - considerații limită de sesiune AVS 83
    - definire sistem la distanță 37
    - definire sistem local 35
    - dimensionare RU 84
    - informații de rețea 35
    - reprezentarea datelor 111
    - securitate 111
    - setare 35
    - subsistem de comunicații 83
    - transmisie 84
  - SQL/DS VSE, activare 125
  - subsistem de comunicații 72
  - transmisie 73
- SON (session outage notification) 55
- SQL (Structured Query Language)
  - dinamic 93
  - obiecte
    - securitate DB2 93
    - securitate manager de baze de date SQL/DS 97, 100
  - static 93
- SQL dinamic
  - CURRENTPACKAGESET 67
  - pachete 93, 97, 100
- SQL static
  - pachete 93, 97, 100
- SQL/DS
  - securitate manager de baze de date
    - SQL dinamic 100
    - SQL static 100
  - VM 74
  - VSE 55
- SQLINIT 74
- SSCP 128
- subsistem
  - subsistem 23
- suport APPC/VM 74
- suport APPC/VTAM 74

## T

- tabelă LINKNAME 27
- tabelă LINKNAME DB2 27
- tabelă SYSIBM.LOCATIONS 27
- TCP/IP
  - actualizare
    - fișier de servicii 5
  - bine cunoscutul port 446 pentru DRDA 47
  - configurare
    - foaie de lucru 4
    - server DB2 Connect 127
  - configurare manuală
    - servere de baze de date gazdă 3
    - servere de baze de date iSeries 3
  - foaie de lucru valoare parametru 127
  - securitate
    - considerații DRDA 49
    - iSeries 94
    - verificată 67
  - setare iSeries
    - server de aplicații DRDA 49
    - solicitant aplicație DRDA 49
  - valorile parametrilor pentru catalogare baze de date 128
- tipărire
  - fișiere PDF 143
- tipuri de
  - autentificare
    - CLIENT 67
  - tipuri de conexiuni
    - bază de date distribuită DB2 67
    - SQL/DS pe bază de date distribuită VM 74
- TPN (nume program de tranzacție)
  - implicit DRDA, OS/400 30
  - server de aplicații OS/400 47
  - SQL/DS pe VM RESID (id resursă) 61
  - tabelă DB2 SYSIBM.LOCATIONS 27
- traducere nume de ieșire
  - exemplu 103
  - SNA 103
  - solicitant de aplicații DB2 103
  - solicitant de aplicații SQL/DS 111
  - TCP/IP 103
- traducere nume de intrare
  - servere de aplicații DB2 89
  - SQL/DS pe serverul de aplicații VM 97
- trimitere parole
  - criptată 106
  - necriptată 106
- TSAF (transparent services access facility) 74

## U

- unitate de lucru distribuită
  - acces direcționat aplicație 67
  - acces direcționat sistem 67
- unitate de lucru la distanță
  - tipuri de 67

## V

- verificare control de-la-cine 89

- viteză de transmisie
  - server de aplicații OS/400 47
  - solicitant de aplicații DB2 73
  - solicitant de aplicații OS/400 31
  - solicitant de aplicații SQL/DS 84
- VM
  - adaptor de resursă 74
  - director de comunicații (comdir) 74
  - DRDA
    - componente 74
    - pregătire server de aplicații 38
    - pregătire solicitant aplicație 38
  - intrări de director 111
- VTAM
  - descriere 67
  - DRDA, rol în 74
  - este nume partener UL 128
  - exemplu BSDS 24
  - instrucțiuni APPL
    - exemple DB2 24
    - limite de sesiune implicite 131

## X

- XPCC 84

## Z

- z/OS
  - considerații de securitate 89

---

## Contactarea IBM

În Statele Unite,apelați unul din numerele următoare pentru a contacta IBM:

- 1-800-IBM-SERV (1-800-426-7378) pentru servicii oferite clienților
- 1-888-426-4343 pentru a afla mai multe despre opțiunile de servicii disponibile
- 1-800-IBM-4YOU (426-4968) pentru departamentul DB2 de marketing și vânzări

În Canada, apelați unul din numerele următoare pentru a contacta IBM:

- 1-800-IBM-SERV (1-800-426-7378) pentru servicii oferite clienților
- 1-800-465-9600 pentru a afla mai multe despre opțiunile de servicii disponibile
- 1-800-IBM-4YOU (1-800-426-4968) pentru departamentul DB2 de marketing și vânzări

Pentru a localiza un birou IBM în țara sau regiunea dumneavoastră, verificați repertoarul IBM de contacte internaționale pe web, la [www.ibm.com/planetwide](http://www.ibm.com/planetwide)

---

## Informații despre produs

Informații privind baza de date universală DB2 sunt disponibile fie prin telefon, fie prin World Wide Web la [www.ibm.com/software/data/db2/udb](http://www.ibm.com/software/data/db2/udb)

Acest site conține ultimele informații despre biblioteci tehnice, comandarea de cărți, descărcări pentru clienți, grupuri de știri, FixPaks, știri și legături către resurse web.

Dacă locuiți în U.S.A., atunci puteți suna la unul din următoarele numere:

- 1-800-IBM-CALL (1-800-426-2255) pentru a comanda produse sau pentru a obține informații generale.
- 1-800-879-2755 pentru a comanda publicații.

Pentru informații despre cum puteți contacta IBM în afara Statelor Unite, vizitați pagina IBM Worldwide la [www.ibm.com/planetwide](http://www.ibm.com/planetwide)







Număr parte: SDB2-CONN-SU

Tipărit în Irlanda.

Spine information:



IBM®

Supliment de conectivitate

*Versiunea 8*