

IBM



# Konnektivität Ergänzung

*Version 8*



IBM



# Konnektivität Ergänzung

*Version 8*

**Hinweis**

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die allgemeinen Informationen unter *Bemerkungen* gelesen werden.

- Die IBM Homepage finden Sie im Internet unter: **ibm.com**
- IBM und das IBM Logo sind eingetragene Marken der International Business Machines Corporation.
- Das e-business Symbol ist eine Marke der International Business Machines Corporation
- Infoprint ist eine eingetragene Marke der IBM.
- ActionMedia, LANDesk, MMX, Pentium und ProShare sind Marken der Intel Corporation in den USA und/oder anderen Ländern.
- C-bus ist eine Marke der Corollary, Inc. in den USA und/oder anderen Ländern.
- Java und alle Java-basierenden Marken und Logos sind Marken der Sun Microsystems, Inc. in den USA und/oder anderen Ländern.
- Microsoft Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.
- PC Direct ist eine Marke der Ziff Communications Company in den USA und/oder anderen Ländern.
- SET und das SET-Logo sind Marken der SET Secure Electronic Transaction LLC.
- UNIX ist eine eingetragene Marke der Open Group in den USA und/oder anderen Ländern.
- Marken anderer Unternehmen/Hersteller werden anerkannt.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs  
*IBM Connectivity Supplement*,  
herausgegeben von International Business Machines Corporation, USA

© Copyright International Business Machines Corporation 1993-2004  
© Copyright IBM Deutschland GmbH 2004

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:  
SW TSC Germany  
Kst. 2877  
April 2004

---

# Inhaltsverzeichnis

---

## Teil 1. Manuelles Konfigurieren der Kommunikation . . . . . 1

### Kapitel 1. Manuelles Konfigurieren der TCP/IP-Kommunikation . . . . . 3

Manuelles Konfigurieren der TCP/IP-Kommunikation zwischen DB2 Connect und einem Host- bzw. iSeries-Datenbankserver . . . . .	3
Tasks für die Konfiguration . . . . .	4
Konfigurieren von TCP/IP auf dem DB2 Connect-Server . . . . .	4
Tasks für die TCP/IP-Konfiguration . . . . .	4
Katalogisieren des TCP/IP-Knotens. . . . .	6
Katalogisieren der Datenbank als DCS-Datenbank . . . . .	7
Katalogisieren der Datenbank. . . . .	8
Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver. . . . .	9
Testen der Host- oder iSeries-Verbindung . . . . .	10

### Kapitel 2. Manuelles Konfigurieren der APPC-Kommunikation . . . . . 13

Manuelles Konfigurieren der APPC-Kommunikation zwischen DB2 Connect und einem Host- und iSeries-Datenbankserver . . . . .	13
Tasks für die Konfiguration . . . . .	14
Aktualisieren von APPC-Profilen auf dem DB2 Connect-Server . . . . .	14
Subtasks für die Aktualisierung der APPC-Profile . . . . .	15
Katalogisieren des APPC- oder APPN-Knotens . . . . .	17
Katalogisieren der Datenbank als DCS-Datenbank . . . . .	18
Katalogisieren der Datenbank . . . . .	19
Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver . . . . .	20
Testen der Host- oder iSeries-Verbindung . . . . .	21

---

## Teil 2. Einrichten von Host- oder iSeries-Anwendungsrequestern . . . 23

### Kapitel 3. Einrichten von OS/390- und z/OS-Anwendungsrequestern . . . . . 25

Definieren von DB2 als Anwendungsrequester (OS/390 und z/OS) . . . . .	25
Tasks für die Einrichtung. . . . .	26
Definieren des DB2-Anwendungsrequesters für das lokale System – SNA (OS/390 und z/OS) . . . . .	26
Definieren des DB2-Anwendungsrequesters für das lokale System – TCP/IP (OS/390 und z/OS) . . . . .	29
Definieren der fernen Systeme (OS/390 und z/OS) . . . . .	30

### Kapitel 4. Einrichten von AS/400-Anwendungsrequestern . . . . . 33

Definieren von DB2 als Anwendungsrequester – SNA (iSeries) . . . . .	33
Tasks für die Einrichtung. . . . .	34
Definieren des Anwendungsrequesters für das lokale System – SNA (iSeries) . . . . .	34
Definieren des fernen Systems (iSeries) . . . . .	34
Definieren der SNA-Kommunikation (iSeries) . . . . .	35

### Kapitel 5. Einrichten von VM-Anwendungsrequestern . . . . . 39

Definieren von DB2 als Anwendungsrequester (VM) . . . . .	39
Tasks für die Einrichtung. . . . .	40
Definieren des Anwendungsrequesters für das lokale System (VM). . . . .	40
Definieren von fernen Systemen für den Anwendungsrequester (VM) . . . . .	41
Vorbereiten des Anwendungsrequesters oder Anwendungsservers für die DRDA-Kommunikation (VM) . . . . .	43

---

## Teil 3. Einrichten von Host- oder iSeries-Anwendungsservern . . . . . 45

### Kapitel 6. Einrichten von OS/390- und z/OS-Anwendungsservern . . . . . 47

Definieren von DB2 als Anwendungsserver (OS/390 und z/OS). . . . .	47
Tasks für die Einrichtung. . . . .	47
Definieren des Anwendungsservers für das lokale SNA-Subsystem (OS/390 und z/OS). . . . .	47
Definieren des Anwendungsservers für das lokale TCP/IP-Subsystem (OS/390 und z/OS). . . . .	49

### Kapitel 7. Einrichten von AS/400-Anwendungsservern (SNA) . . . . . 51

Definieren von DB2 als Anwendungsserver – SNA (iSeries). . . . .	51
--	----

### Kapitel 8. Einrichten von AS/400-Anwendungsservern (TCP/IP) . . . . . 53

Herstellen einer Verbindung zu DB2 UDB über TCP/IP (iSeries). . . . .	53
---	----

### Kapitel 9. Einrichten von VSE-Anwendungsservern . . . . . 59

Definieren von DB2 als Anwendungsserver (VSE) . . . . .	59
Tasks für die Einrichtung. . . . .	59
Einrichten von CICS-LU 6.2-Sitzungen (VSE) . . . . .	59
Definieren eines Anwendungsservers (VSE) . . . . .	63
Vorbereiten und Starten des DB2-Anwendungsservers (VSE). . . . .	64

**Kapitel 10. Einrichten von VM-Anwendungsservern . . . . . 67**

Definieren von DB2 als Anwendungsserver (VM). . . 67  
Tasks für die Einrichtung . . . . . 68  
    Definieren des Anwendungsservers (VM) . . . 68

**Teil 4. Konzepte für Host und iSeries . . . . . 71**

**Kapitel 11. Konzepte . . . . . 73**

DB2 für OS/390 und z/OS . . . . . 73  
Weitere Konzepte . . . . . 80  
    Definieren der Kommunikation - SNA (OS/390 und z/OS). . . . . 80  
    Festlegen der RU-Größen und der Nachrichtendosierung (OS/390 und z/OS) . . . . . 80  
DB2 UDB für iSeries . . . . . 81  
DB2 für VM . . . . . 82  
Weitere Konzepte . . . . . 92  
    Definieren der Kommunikation – Anwendungsrequester (VM) . . . . . 92  
    Festlegen der RU-Größen und der Nachrichtendosierung (VM) . . . . . 93  
DB2 für VSE . . . . . 94

**Kapitel 12. Sicherheitsüberlegungen für Anwendungsserver . . . . . 99**

Sicherheitsüberlegungen für Anwendungsserver (OS/390 und z/OS) . . . . . 99  
Weitere Konzepte . . . . . 99  
    Herkunftsüberprüfung (OS/390 und z/OS). . . 99  
    Endbenutzernamen - Anwendungsserver (OS/390 und z/OS) . . . . . 100  
    Netzwerksicherheit - Anwendungsserver (OS/390 und z/OS) . . . . . 102  
    Sicherheit des Datenbankmanagers - Anwendungsserver (OS/390 und z/OS) . . . 103  
    Sicherheitssystem - Anwendungsserver (OS/390 und z/OS) . . . . . 105  
Sicherheitsüberlegungen für Anwendungsserver (iSeries) . . . . . 105  
Sicherheitsüberlegungen für Anwendungsserver (VM) . . . . . 108  
Sicherheitsüberlegungen für Anwendungsserver (VSE) . . . . . 112

**Kapitel 13. Sicherheitsüberlegungen für Anwendungsrequester . . . . . 115**

Sicherheitsüberlegungen für Anwendungsrequester (OS/390 und z/OS) . . . . . 115  
Weitere Konzepte . . . . . 115  
    Endbenutzernamen - Anwendungsrequester (OS/390 und z/OS) . . . . . 115  
    Netzwerksicherheit - Anwendungsrequester (OS/390 und z/OS) . . . . . 119  
    Sicherheit des Datenbankmanagers - Anwendungsrequester (OS/390 und z/OS). . . . . 120  
    Sicherheitssystem - Anwendungsrequester (OS/390 und z/OS) . . . . . 121

Sicherheitsüberlegungen für Anwendungsrequester (iSeries) . . . . . 122  
Erteilen und Entziehen von Berechtigungen: . . . 124  
Sicherheitsüberlegungen für Anwendungsrequester (VM) . . . . . 124

**Kapitel 14. Datendarstellung . . . . . 129**

Datendarstellung (OS/390 und z/OS) . . . . . 129  
Datendarstellung (iSeries) . . . . . 129  
Datendarstellung (VM) . . . . . 132

**Teil 5. Referenz für Host und iSeries . . . . . 137**

**Kapitel 15. Referenz . . . . . 139**

Mit dem Konfigurationsassistenten konfigurierbare Produkte für die APPC-Kommunikation . . . . . 139  
Prüfliste zum Aktivieren eines DB2-Anwendungsservers (VSE) . . . . . 139  
Prüfliste zum Aktivieren eines DB2-Anwendersrequesters (VM) . . . . . 141  
Arbeitsblatt für TCP/IP-Parameterwerte . . . . . 141  
TCP/IP-Parameterwerte zum Katalogisieren von Datenbanken . . . . . 143  
Arbeitsblatt für APPC-Parameterwerte . . . . . 144  
Schlüsselwörter der VTAM-Anweisung APPL von DB2 Connect . . . . . 146

**Teil 6. Anhänge und Schlussteil . . . . . 149**

**Anhang A. Technische Informationen zu DB2 Universal Database . . . . . 151**

DB2-Dokumentation und Hilfe . . . . . 151  
    Aktualisierungen der DB2-Dokumentation . . 151  
DB2 Information - Unterstützung. . . . . 152  
DB2 Information - Unterstützung: Installations-szenarios . . . . . 153  
Installation von 'DB2 Information - Unterstützung' mit dem DB2-Installationsassistenten (UNIX) . . 155  
Installation von 'DB2 Information - Unterstützung' mit dem DB2-Installationsassistenten (Windows) . 158  
Aufrufen von 'DB2 Information - Unterstützung' 160  
Aktualisieren der auf Ihrem Computer oder Intranet-Server installierten Komponente 'DB2 Information - Unterstützung' . . . . . 161  
Anzeigen von Themen in der gewünschten Sprache in 'DB2 Information - Unterstützung' . . . . . 162  
DB2-Dokumentation in PDF-Format und gedrucktem Format . . . . . 163  
    DB2-Kerninformationen . . . . . 163  
    Verwaltungsinformationen . . . . . 164  
    Informationen zur Anwendungsentwicklung 165  
    Informationsmanagement . . . . . 165  
    Informationen zu DB2 Connect . . . . . 166  
    Einführungsinformationen . . . . . 166  
    Lernprogramminformationen . . . . . 166  
    Informationen zu Zusatzkomponenten . . . . 167  
    Release-Informationen . . . . . 167  
Drucken von DB2-Büchern mit PDF-Dateien . . . 168

Bestellen gedruckter DB2-Bücher . . . . .	169
Aufrufen der Kontexthilfe über ein DB2-Tool . . .	170
Aufrufen der Hilfe für Nachrichten über den Befehlszeilenprozessor . . . . .	171
Aufrufen der Hilfe für Befehle über den Befehls- zeilenprozessor . . . . .	171
Aufrufen der Hilfe für den SQL-Status über den Befehlszeilenprozessor . . . . .	172
DB2-Lernprogramme . . . . .	172
Informationen zur Fehlerbehebung in DB2 . . .	173
Eingabehilfen . . . . .	174
Tastatureingabe und Navigation . . . . .	174
Eingabehilfen für Bildschirme . . . . .	174
Kompatibilität mit Unterstützungseinrichtungen	175
Dokumentation im behindertengerechten For- mat. . . . .	175

Syntaxdiagramme in der Schreibweise mit Trenn- zeichen . . . . .	175
Common Criteria-Zertifizierung von DB2 Universal Database-Produkten . . . . .	177

<b>Anhang B. Bemerkungen . . . . .</b>	<b>179</b>
Marken . . . . .	181

<b>Index . . . . .</b>	<b>183</b>
------------------------	------------

<b>Kontaktaufnahme mit IBM . . . . .</b>	<b>189</b>
Produktinformationen . . . . .	189



---

## **Teil 1. Manuelles Konfigurieren der Kommunikation**



---

# Kapitel 1. Manuelles Konfigurieren der TCP/IP-Kommunikation

---

## Manuelles Konfigurieren der TCP/IP-Kommunikation zwischen DB2 Connect und einem Host- bzw. iSeries-Datenbankserver

Die TCP/IP-Verbindung zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank kann auch manuell konfiguriert werden. In der Regel wird TCP/IP mit Hilfe des Konfigurationsassistenten automatisch konfiguriert.

### Voraussetzungen:

Vor dem manuellen Konfigurieren einer TCP/IP-Verbindung zwischen DB2 Connect und einem Host- oder iSeries-Datenbankserver müssen Sie sicherstellen, dass die folgenden Bedingungen erfüllt sind:

- TCP/IP ist auf dem DB2 Connect-Server und dem Host- oder iSeries-System betriebsbereit
- Sie haben mit Hilfe des Arbeitsblatts für die TCP/IP-Parameterwerte die folgenden TCP/IP-Parameterwerte ermittelt:
  - Hostname (*hostname*) oder IP-Adresse (*ip-adresse*)
  - Name des Verbindungsservices (*svcname*) oder Portnummer/-protokoll (*portnummer/tcp*)
  - Zieldatenbankname (*zieldatenbankname*)
  - Name der lokalen Datenbank (*lokaler-dcs-name*)
  - Knotenname (*knotenname*)

### Vorgehensweise:

Führen Sie die folgenden Schritte aus, um die TCP/IP-Kommunikation zwischen dem DB2 Connect-Server und einer Host- oder iSeries-Datenbank manuell zu konfigurieren:

1. Konfigurieren Sie TCP/IP auf dem DB2 Connect-Server.
2. Katalogisieren Sie den TCP/IP-Knoten.
3. Katalogisieren Sie die Host- oder iSeries-Datenbank als DCS-Datenbank (DCS = Database Connection Service).
4. Katalogisieren Sie die Host- oder iSeries-Datenbank.
5. Binden Sie Dienstprogramme und Anwendungen an den Host- oder iSeries-Datenbankserver.
6. Testen Sie die Host- oder iSeries-Verbindung.

**Anmerkung:** Aufgrund der spezifischen Merkmale des TCP/IP-Protokolls wird TCP/IP möglicherweise nicht sofort über den Ausfall einer Partnerstation auf einer anderen Host- oder iSeries-Maschine informiert. Daher kann manchmal der Eindruck entstehen, dass eine Clientanwendung, die über TCP/IP auf einen fernen DB2-Server zugreift, oder der entsprechende Agent auf dem Server blockiert ist. DB2 verwendet die TCP/IP-Socket-Option `SO_KEEPALIVE`, um zu ermitteln, ob eine Störung aufgetreten ist und die TCP/IP-Verbindung unterbrochen wurde.

**Zugehörige Tasks:**

- „Konfigurieren von TCP/IP auf dem DB2 Connect-Server“ auf Seite 4
- „Katalogisieren des TCP/IP-Knotens“ auf Seite 6
- „Katalogisieren der Datenbank als DCS-Datenbank“ auf Seite 7
- „Katalogisieren der Datenbank“ auf Seite 8
- „Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver“ auf Seite 9
- „Testen der Host- oder iSeries-Verbindung“ auf Seite 10
- „Manuelles Konfigurieren der APPC-Kommunikation zwischen DB2 Connect und einem Host- und iSeries-Datenbankserver“ auf Seite 13

**Zugehörige Referenzen:**

- „Arbeitsblatt für TCP/IP-Parameterwerte“ auf Seite 141

---

## Tasks für die Konfiguration

### Konfigurieren von TCP/IP auf dem DB2 Connect-Server

Das Konfigurieren von TCP/IP auf dem DB2 Connect-Server ist einer der Arbeitsschritte für die Konfiguration der TCP/IP-Kommunikation zwischen einem DB2 Connect-Server und einem Host- oder iSeries-Datenbankserver.

**Vorgehensweise:**

Führen Sie die folgenden Schritte aus, um TCP/IP auf dem DB2 Connect-Server zu konfigurieren:

- Lösen Sie die IP-Adresse des lokalen Hostsystems auf.
- Aktualisieren Sie die Datei `services`.

Nach dem Ausführen dieser Schritte können Sie den TCP/IP-Knoten katalogisieren.

**Zugehörige Tasks:**

- „Auflösen der IP-Adresse des lokalen Host- oder iSeries-Systems“ auf Seite 4
- „Aktualisieren der Datei 'services'“ auf Seite 5
- „Katalogisieren des TCP/IP-Knotens“ auf Seite 6

## Tasks für die TCP/IP-Konfiguration

### Auflösen der IP-Adresse des lokalen Host- oder iSeries-Systems

Das Auflösen der IP-Adresse des lokalen Host- oder iSeries-Systems ist einer der Arbeitsschritte für die Konfiguration der TCP/IP-Kommunikation zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank. Der DB2 Connect-Server muss die Adresse des Host- oder iSeries-Systems, mit dem er kommunizieren soll, kennen.

**Anmerkung:** Falls in Ihrem Netzwerk ein Namensserver eingesetzt wird oder falls Sie die IP-Adresse (*ip-adresse*) des Host- oder iSeries-Servers direkt angeben wollen, können Sie sofort mit dem Katalogisieren des TCP/IP-Knotens fortfahren.

Falls in Ihrem Netzwerk kein Namensserver eingesetzt wird, können Sie direkt einen Hostnamen angeben, der der IP-Adresse (*ip-adresse*) des Host- oder iSeries-Systems in der lokalen Datei `hosts` zugeordnet ist.

Wenn ein UNIX-Client unterstützt werden soll, der Network Information Services (NIS) verwendet, und in Ihrem Netzwerk kein Domänennamensserver (DNS) eingesetzt wird, müssen Sie die Datei `hosts` auf dem NIS-Hauptserver entsprechend anpassen.

*Tabelle 1. Speicherposition der lokalen Dateien "hosts" und "services"*

Betriebssystem	Verzeichnis
Windows 98	windows
Windows NT und Windows 2000	winnt\system32\drivers\etc
UNIX	/etc

### Vorgehensweise:

Verwenden Sie zum Auflösen der IP-Adresse des lokalen Host- oder iSeries-Systems einen Texteditor und fügen Sie der Datei `hosts` des DB2 Connect-Servers einen Eintrag für den Hostnamen des Host- oder iSeries-Systems hinzu.

Beispiel:

```
9.21.15.235    nyx    # Hostadresse für nyx
```

Hierbei gilt Folgendes: *9.21.15.235* ist die *ip-adresse*, *nyx* ist der *hostname* und *# ...* ist ein Kommentar, der den Eintrag beschreibt.

Befindet sich das Host- oder iSeries-System nicht in der selben Domäne wie der DB2 Connect-Server, müssen Sie einen vollständig qualifizierten Domänennamen, wie beispielsweise *nyx.spifnet.ibm.com*, angeben. Hierbei steht *spifnet.ibm.com* für den Domänennamen.

Der nächste Konfigurationsschritt ist das Katalogisieren des TCP/IP-Knotens.

### Zugehörige Tasks:

- „Manuelles Konfigurieren der TCP/IP-Kommunikation zwischen DB2 Connect und einem Host- bzw. iSeries-Datenbankserver“ auf Seite 3
- „Katalogisieren des TCP/IP-Knotens“ auf Seite 6
- „Aktualisieren der Datei 'services'“ auf Seite 5

### Aktualisieren der Datei 'services'

Das Aktualisieren der Datei `services` ist einer der Arbeitsschritte für die Konfiguration von TCP/IP auf dem DB2 Connect-Server. Überspringen Sie diesen Schritt, wenn der TCP/IP-Knoten mit Hilfe einer Portnummer (*portnummer*) katalogisiert werden soll. Bearbeiten Sie die Datei `services` des DB2 Connect-Servers und fügen Sie ihr Angaben zum Namen des Verbindungsservices sowie der Portnummer des fernen Hosts, zu dem eine Verbindung hergestellt werden soll, hinzu.

### Vorgehensweise:

Öffnen Sie die Datei `services` des DB2 Connect-Servers mit einem Texteditor. Fügen Sie dieser Datei eine Zeile mit dem Namen des Verbindungsservices und

der Portnummer des fernen Hosts, zu dem eine Verbindung hergestellt werden soll, hinzu. Diese Datei befindet sich im selben Verzeichnis wie die lokale Datei `hosts`.

Beispiel:

```
host1 3700/tcp # DB2-Port für den Verbindungsservice
```

Hierbei ist `host1` der Name des Verbindungsservices, `3700` ist die Portnummer der Verbindung, `tcp` ist das Kommunikationsprotokoll und `#` ist das Kommentarzeichen, das dem Kommentar, der den Eintrag beschreibt, vorausgestellt ist.

Die auf dem DB2 Connect-Server verwendete Portnummer muss mit der auf dem Hostsystem verwendeten Portnummer übereinstimmen. Stellen Sie außerdem sicher, dass Sie keine Portnummer angeben, die bereits von einem anderen Prozess verwendet wird. Wenn ein UNIX-Client unterstützt werden soll, der Network Information Services (NIS) verwendet, müssen Sie auf dem NIS-Hauptserver die Datei `services` entsprechend anpassen.

Der nächste Konfigurationsschritt ist das Katalogisieren des TCP/IP-Knotens.

**Zugehörige Tasks:**

- „Katalogisieren des TCP/IP-Knotens“ auf Seite 6

## Katalogisieren des TCP/IP-Knotens

Das Katalogisieren des TCP/IP-Knotens ist einer der Arbeitsschritte für die Konfiguration der TCP/IP-Kommunikation zwischen DB2 Connect und einem Host- oder iSeries-Datenbankserver. Sie müssen einen Eintrag zum Knotenverzeichnis des DB2 Connect-Servers hinzufügen, um den fernen Knoten zu beschreiben. Dieser Eintrag gibt den ausgewählten Aliasnamen (*knotenname*), den Hostnamen (*hostname*) (oder die *ip-adresse*) und den Servicenamen (*svcname*) (oder die *portnummer*) an, die der Client für den Zugriff auf den fernen Host verwendet.

**Voraussetzungen:**

Eine Benutzer-ID mit der Berechtigung SYSADM (Systemverwaltung) oder SYSC-TRL (Systemsteuerung). Ist die Option `catalog_noauth` auf `ON` gesetzt, können Sie sich auch ohne diese Berechtigungsstufen am System anmelden.

**Vorgehensweise:**

Führen Sie die folgenden Schritte aus, um den TCP/IP-Knoten zu katalogisieren:

1. Unter UNIX müssen Sie zunächst die Exemplarumgebung konfigurieren und den DB2-Befehlszeilenprozessor aufrufen. Führen Sie die Startprozedur wie folgt aus:

```
. INSTHOME/sql1lib/db2profile    (für Bash, Bourne oder Korn-Shell)
source INSTHOME/sql1lib/db2cshrc (für C-Shell)
```

Hierbei steht `INSTHOME` für das Ausgangsverzeichnis des Exemplars.

2. Katalogisieren Sie den Knoten wie folgt:

```
catalog tcpip node knotenname remote [hostname|ip-adresse]
server [svcname|portnummer]
terminate
```

Geben Sie zum Beispiel zum Katalogisieren des fernen Hosts *nyx* auf dem Knoten *db2node* unter Verwendung des Servicenamens *host1* die folgenden Befehle ein:

```
catalog tcpip node db2node remote nyx server host1
terminate
```

Geben Sie zum Katalogisieren des fernen Servers mit der IP-Adresse *9.21.15.235* auf dem Knoten *db2node* unter Verwendung der Portnummer *3700* die folgenden Befehle ein:

```
catalog tcpip node db2node remote 9.21.15.235 server 3700
terminate
```

Führen Sie die folgenden Schritte aus, um Werte zu ändern, die mit dem Befehl **catalog node** definiert wurden:

1. Führen Sie im Befehlszeilenprozessor den Befehl **uncatalog node** wie folgt aus:  
`db2 uncatalog node knotenname`
2. Katalogisieren Sie den Knoten erneut und verwenden Sie die gewünschten Werte.

Der nächste Konfigurationsschritt ist das Katalogisieren der Datenbank als DCS-Datenbank.

#### Zugehörige Tasks:

- „Konfigurieren von TCP/IP auf dem DB2 Connect-Server“ auf Seite 4
- „Katalogisieren der Datenbank als DCS-Datenbank“ auf Seite 7

#### Zugehörige Referenzen:

- „CATALOG TCPIP NODE Command“ in *Command Reference*

## Katalogisieren der Datenbank als DCS-Datenbank

Das Katalogisieren der Datenbank als DCS-Datenbank (DCS = Database Connection Service) ist einer der Arbeitsschritte für die Konfiguration der Kommunikation zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank. Die ferne Datenbank muss als DCS-Datenbank katalogisiert werden, damit DB2 Connect den Zugriff auf diese Datenbank zur Verfügung stellen kann.

#### Voraussetzungen:

Eine Benutzer-ID mit der Berechtigung SYSADM (Systemverwaltung) oder SYSCTRL (Systemsteuerung).

#### Vorgehensweise:

Führen Sie die folgenden Befehle aus, um die ferne Datenbank als DCS-Datenbank zu katalogisieren:

```
catalog dcs db lokaler-dcs-name as zieldatenbankname
terminate
```

Hierbei gilt Folgendes:

- *lokaler-dcs-name* steht für den lokalen Namen der Host- oder iSeries-Datenbank.
- *zieldatenbankname* steht für den Namen der Host- oder iSeries-Datenbank.

Geben Sie beispielsweise die folgenden Befehle ein, um die lokale DB2 Connect-Datenbank *ny* als ferne Host- oder iSeries-Datenbank *newyork* zu katalogisieren:

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

Der nächste Konfigurationsschritt ist das Katalogisieren der Datenbank.

**Zugehörige Tasks:**

- „Katalogisieren des TCP/IP-Knotens“ auf Seite 6
- „Katalogisieren der Datenbank“ auf Seite 8
- „Katalogisieren des APPC- oder APPN-Knotens“ auf Seite 17

**Zugehörige Referenzen:**

- „CATALOG DCS DATABASE Command“ in *Command Reference*

## Katalogisieren der Datenbank

Das Katalogisieren der Datenbank ist einer der Arbeitsschritte für die Konfiguration der Kommunikation zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank. Bevor eine Clientanwendung auf eine ferne Datenbank zugreifen kann, muss die Datenbank auf dem Host- oder iSeries-Systemknoten und auf allen DB2 Connect-Serverknoten, die eine Verbindung zu dieser Datenbank herstellen, katalogisiert werden.

Wenn Sie eine Datenbank erstellen, wird sie automatisch auf der Host- oder iSeries-Maschine katalogisiert. Dabei ist der Aliasname der Datenbank (*aliasname-der-datenbank*) mit dem Datenbanknamen (*datenbankname*) identisch. Die Informationen im Datenbankverzeichnis werden zusammen mit den Informationen im Knotenverzeichnis auf dem DB2 Connect-Server verwendet, um eine Verbindung zur fernen Host- oder iSeries-Datenbank herzustellen.

**Voraussetzungen:**

- Eine Benutzer-ID mit der Berechtigung SYSADM (Systemverwaltung) oder SYSCTRL (Systemsteuerung).
- Identifizieren Sie die folgenden Parameter:
  - Datenbankname (*datenbankname*)
  - Aliasname der Datenbank (*aliasname-der-datenbank*)
  - Knotenname (*knotenname*)

**Vorgehensweise:**

Führen Sie die folgenden Schritte aus, um eine Datenbank auf dem DB2 Connect-Server zu katalogisieren:

1. Unter UNIX müssen Sie zunächst die Exemplarumgebung konfigurieren und den DB2-Befehlszeilenprozessor aufrufen. Führen Sie die Startprozedur wie folgt aus:

```
. INSTHOME/sql1lib/db2profile    (für Bash, Bourne oder Korn-Shell)
source INSTHOME/sql1lib/db2cshrc (für C-Shell)
```

Hierbei steht *INSTHOME* für das Ausgangsverzeichnis des Exemplars.

2. Katalogisieren Sie die Datenbank wie folgt:

```
catalog database datenbankname as aliasname-der-datenbank at
node knotenname authentication auth_wert
```

Geben Sie beispielsweise die folgenden Befehle ein, um die bei DCS bekannte Datenbank *ny* so zu katalogisieren, dass sie den Aliasnamen der lokalen Datenbank *localny* auf dem Knoten *db2node* besitzt:

```
catalog database ny as localny at node db2node  
authentication dcs  
terminate
```

Führen Sie die folgenden Schritte aus, um Werte zu ändern, die mit dem Befehl **catalog database** definiert wurden:

a. Führen Sie den Befehl **uncatalog database** im Befehlszeilenprozessor wie folgt aus:

```
uncatalog database aliasname-der-datenbank
```

b. Katalogisieren Sie die Datenbank erneut und verwenden Sie die gewünschten Werte.

Der nächste Konfigurationsschritt ist das Binden von Dienstprogrammen und Anwendungen an den Datenbankserver.

#### **Zugehörige Tasks:**

- „Katalogisieren der Datenbank als DCS-Datenbank“ auf Seite 7
- „Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver“ auf Seite 9

#### **Zugehörige Referenzen:**

- „CATALOG DATABASE Command“ in *Command Reference*

## **Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver**

Das Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver ist einer der Arbeitsschritte für die Konfiguration der Kommunikation zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank. Nach dem Ausführen der Schritte zum Konfigurieren des DB2 Connect-Servers für die Kommunikation mit dem Host- oder iSeries-System müssen Sie die Dienstprogramme und Anwendungen auf dem Host- oder iSeries-Datenbankserver binden.

**Voraussetzungen:**

Eine Benutzer-ID mit der Berechtigung BINDADD.

**Vorgehensweise:**

Führen Sie die folgenden Befehle aus, um die Dienstprogramme und Anwendungen an den Host- oder iSeries-Datenbankserver zu binden:

```
connect to aliasname-der-datenbank user benutzer-id using kennwort
bind bindepfad_verz@ddcsmvs.lst blocking all sqlerror continue
messages mvs.msg grant public
connect reset
```

**Beispiel:**

```
connect to NYC3 user meinebenutzer-id using meinkennwort
bind bindepfad_verz@ddcsmvs.lst blocking all sqlerror continue
messages mvs.msg grant public
connect reset
```

Hierbei steht *bindepfad\_verz* für das Verzeichnis, in dem sich die .lst-Dateien befinden. Unter Windows lautet dieser Pfad in der Regel \SQLLIB\BND\.

Der nächste Konfigurationsschritt ist das Testen der Host- oder iSeries-Verbindung.

**Zugehörige Konzepte:**

- „Binden von Dienstprogrammen an die Datenbank“ in *Systemverwaltung: Implementierung*

**Zugehörige Tasks:**

- „Katalogisieren der Datenbank“ auf Seite 8
- „Testen der Host- oder iSeries-Verbindung“ auf Seite 10

**Zugehörige Referenzen:**

- „BIND Command“ in *Command Reference*

## Testen der Host- oder iSeries-Verbindung

Das Testen der Host- oder iSeries-Verbindung ist einer der Arbeitsschritte für die Konfiguration der Kommunikation zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank. Wenn die Konfiguration des DB2 Connect-Servers für die Host- oder iSeries-Kommunikation abgeschlossen ist, müssen Sie die Verbindung mit Hilfe einer fernen Datenbank testen.

**Voraussetzungen:**

- Zum Testen der Verbindung wird eine Verbindung zu einer fernen Datenbank hergestellt.
- Die Werte für *benutzer-id* und *kennwort* müssen für das System, auf dem sie authentifiziert werden, zulässig sein. Standardmäßig erfolgt die Authentifizierung auf dem Host- oder iSeries-Datenbankserver.

### Vorgehensweise:

Gehen Sie wie folgt vor, um die Host- oder iSeries-Verbindung zu testen:

1. Starten Sie den Datenbankmanager durch Eingabe des Befehls **db2start** auf dem Host- oder iSeries-Datenbankserver (wenn er nicht bereits gestartet ist).
2. Stellen Sie mit dem folgenden Befehl eine Verbindung zur fernen Datenbank her:

```
connect to aliasname-der-datenbank user benutzer-id using kennwort
```

Geben Sie zum Beispiel den folgenden Befehl ein:

```
connect to nyc3 user benutzer-id using kennwort
```

Die Authentifizierung für die Verbindung mit Hostdatenbanken wird während der Konfiguration von DB2 Connect eingerichtet.

Wurde die Verbindung erfolgreich hergestellt, wird der Name der Datenbank, mit der die Verbindung besteht, in einer Nachricht angezeigt. Von dieser Datenbank können nun Daten abgerufen werden.

Geben Sie beispielsweise den folgenden SQL-Befehl ein, um eine Liste aller Tabellennamen abzurufen, die in der Systemkatalogtabelle aufgeführt sind:

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

Wenn Sie die Datenbankverbindung nicht mehr benötigen, geben Sie den Befehl **db2 connect reset** ein, um die Datenbankverbindung zu beenden.

### Zugehörige Tasks:

- „Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver“ auf Seite 9



---

## Kapitel 2. Manuelles Konfigurieren der APPC-Kommunikation

---

### Manuelles Konfigurieren der APPC-Kommunikation zwischen DB2 Connect und einem Host- und iSeries-Datenbankserver

Die APPC-Verbindung zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank kann auch manuell konfiguriert werden. Die APPC-Kommunikation kann meistens mit Hilfe des Konfigurationsassistenten automatisch konfiguriert werden.

**Anmerkung:** Sie sollten in Erwägung ziehen, TCP/IP als Verbindungsprotokoll zu verwenden, da SNA in künftigen Releases von DB2 Connect möglicherweise nicht mehr unterstützt wird. Für die Konfiguration von SNA ist wesentlich mehr technisches Wissen erforderlich, und beim Konfigurationsprozess treten häufig Fehler auf. TCP/IP ist leicht zu konfigurieren, erfordert weniger Aufwand für die Verwaltung und bietet bessere Leistung.

#### Voraussetzungen:

- APPC muss auf dem DB2 Connect-Server und dem Host- oder iSeries-System unterstützt werden.
- Die auf dem Arbeitsblatt für APPC-Parameterwerte eingetragenen Werte müssen zur Verfügung stehen.

#### Einschränkungen:

Das SNA-Protokoll wird von DB2 Connect Version 8.1 auf Windows 64-Bit-Plattformen (XP 64-Bit und .NET Server 64-Bit) nicht unterstützt.

#### Vorgehensweise:

Führen Sie die folgenden Schritte aus, um einen DB2 Connect-Server manuell für die APPC-Kommunikation mit einem Host- oder iSeries-Datenbankserver zu konfigurieren:

1. Aktualisieren Sie die APPC-Profile auf dem DB2 Connect-Server.
2. Katalogisieren Sie den APPC- oder APPN-Knoten.
3. Katalogisieren Sie die Host- oder iSeries-Datenbank als DCS-Datenbank (DCS = Database Connection Service).
4. Katalogisieren Sie die Host- oder iSeries-Datenbank.
5. Binden Sie Dienstprogramme und Anwendungen an den Host- oder iSeries-Datenbankserver.
6. Testen Sie die Host- oder iSeries-Verbindung.

#### Zugehörige Tasks:

- „Aktualisieren von APPC-Profilen auf dem DB2 Connect-Server“ auf Seite 14
- „Katalogisieren des APPC- oder APPN-Knotens“ auf Seite 17
- „Katalogisieren der Datenbank als DCS-Datenbank“ auf Seite 7
- „Katalogisieren der Datenbank“ auf Seite 8

- „Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver“ auf Seite 9
- „Testen der Host- oder iSeries-Verbindung“ auf Seite 10
- „Manuelles Konfigurieren der TCP/IP-Kommunikation zwischen DB2 Connect und einem Host- bzw. iSeries-Datenbankserver“ auf Seite 3

**Zugehörige Referenzen:**

- „Arbeitsblatt für APPC-Parameterwerte“ auf Seite 144

---

## Tasks für die Konfiguration

### Aktualisieren von APPC-Profilen auf dem DB2 Connect-Server

Das Konfigurieren von APPC-Profilen auf dem DB2 Connect-Server ist einer der Arbeitsschritte für die Konfiguration der ACCP-Kommunikation auf dem Host- oder iSeries-System für DB2 Connect.

**Vorgehensweise:**

Um die DB2 Connect-APPC-Kommunikation für den Zugriff auf einen fernen Host- oder iSeries-Datenbankserver zu konfigurieren, müssen Sie die für Ihre Netzwerkkonfiguration relevanten APPC-Profile konfigurieren. Führen Sie hierzu die entsprechenden Schritte aus der folgenden Liste aus:

- Konfigurieren Sie einen SNA-API-Client für IBM eNetwork Communications Server für Windows.
- Konfigurieren Sie Microsoft SNA Server.
- Konfigurieren Sie Microsoft SNA Client.
- Konfigurieren Sie IBM eNetwork Communications Server für AIX.
- Konfigurieren Sie Bull SNA für AIX.
- Konfigurieren Sie SNAPplus2 für HP-UX.

Der nächste Konfigurationsschritt ist das Katalogisieren des APPC- oder APPN-Knotens.

**Zugehörige Tasks:**

- „Konfigurieren eines SNA-API-Clients für IBM eNetwork Communications Server für Windows“ auf Seite 15
- „Konfigurieren von Microsoft SNA Server“ auf Seite 15
- „Konfigurieren von Microsoft SNA Client“ auf Seite 16
- „Konfigurieren von IBM eNetwork Communications Server für AIX“ auf Seite 16
- „Konfigurieren von Bull SNA für AIX“ auf Seite 16
- „Konfigurieren von SNAPplus2 für HP-UX“ auf Seite 17
- „Katalogisieren des APPC- oder APPN-Knotens“ auf Seite 17

**Zugehörige Referenzen:**

- „Mit dem Konfigurationsassistenten konfigurierbare Produkte für die APPC-Kommunikation“ auf Seite 139

## Subtasks für die Aktualisierung der APPC-Profile

### Konfigurieren eines SNA-API-Clients für IBM eNetwork Communications Server für Windows

Die folgende Unterstützung ist für DB2 Enterprise Server Edition (ESE) für Windows und UNIX Version 8 sowie DB2 Connect Enterprise Edition (EE) für Windows und UNIX Version 8 nicht mehr verfügbar:

- Funktionalität für zweiphasige Festschreibung mit SNA. Anwendungen, für die die zweiphasige Festschreibung erforderlich ist, müssen die TCP/IP-Konnektivität verwenden. Die zweiphasige Festschreibung unter Verwendung einer TCP/IP-Verbindung zu einem Host- oder iSeries-Datenbankserver ist bereits seit einigen Releases verfügbar. Host- oder iSeries-Anwendungen, für die die Unterstützung der zweiphasigen Festschreibung erforderlich ist, können die neue Funktionalität der Unterstützung für die zweiphasige Festschreibung mit TCP/IP innerhalb von DB2 ESE Version 8 verwenden.
- Anwendungen können keine SNA-Verbindungen mehr verwenden, um auf einen DB2 UDB ESE-Server unter UNIX oder Windows bzw. einen DB2 Connect EE-Server zuzugreifen. Anwendungen können weiterhin mit SNA auf Host- oder iSeries-Datenbankserver zugreifen, können aber nur die einphasige Festschreibung verwenden.

#### Zugehörige Tasks:

- „Katalogisieren des APPC- oder APPN-Knotens“ auf Seite 17

### Konfigurieren von Microsoft SNA Server

Die folgende Unterstützung ist für DB2 Enterprise Server Edition (ESE) für Windows und UNIX Version 8 sowie DB2 Connect Enterprise Edition (EE) für Windows und UNIX Version 8 nicht mehr verfügbar:

- Funktionalität für zweiphasige Festschreibung mit SNA. Anwendungen, für die die zweiphasige Festschreibung erforderlich ist, müssen die TCP/IP-Konnektivität verwenden. Die zweiphasige Festschreibung unter Verwendung einer TCP/IP-Verbindung zu einem Host- oder iSeries-Datenbankserver ist bereits seit einigen Releases verfügbar. Host- oder iSeries-Anwendungen, für die die Unterstützung der zweiphasigen Festschreibung erforderlich ist, können die neue Funktionalität der Unterstützung für die zweiphasige Festschreibung mit TCP/IP innerhalb von DB2 ESE Version 8 verwenden.
- Anwendungen können keine SNA-Verbindungen mehr verwenden, um auf einen DB2 UDB ESE-Server unter UNIX oder Windows bzw. einen DB2 Connect EE-Server zuzugreifen. Anwendungen können weiterhin mit SNA auf Host- oder iSeries-Datenbankserver zugreifen, können aber nur die einphasige Festschreibung verwenden.

#### Zugehörige Tasks:

- „Konfigurieren von Microsoft SNA Client“ auf Seite 16
- „Manuelles Konfigurieren der APPC-Kommunikation zwischen DB2 Connect und einem Host- und iSeries-Datenbankserver“ auf Seite 13
- „Katalogisieren des APPC- oder APPN-Knotens“ auf Seite 17

## Konfigurieren von Microsoft SNA Client

Die folgende Unterstützung ist für DB2 Enterprise Server Edition (ESE) für Windows und UNIX Version 8 sowie DB2 Connect Enterprise Edition (EE) für Windows und UNIX Version 8 nicht mehr verfügbar:

- Funktionalität für zweiphasige Festschreibung mit SNA. Anwendungen, für die die zweiphasige Festschreibung erforderlich ist, müssen die TCP/IP-Konnektivität verwenden. Die zweiphasige Festschreibung unter Verwendung einer TCP/IP-Verbindung zu einem Host- oder iSeries-Datenbankserver ist bereits seit einigen Releases verfügbar. Host- oder iSeries-Anwendungen, für die die Unterstützung der zweiphasigen Festschreibung erforderlich ist, können die neue Funktionalität der Unterstützung für die zweiphasige Festschreibung mit TCP/IP innerhalb von DB2 ESE Version 8 verwenden.
- Anwendungen können keine SNA-Verbindungen mehr verwenden, um auf einen DB2 UDB ESE-Server unter UNIX oder Windows bzw. einen DB2 Connect EE-Server zuzugreifen. Anwendungen können weiterhin mit SNA auf Host- oder iSeries-Datenbankserver zugreifen, können aber nur die einphasige Festschreibung verwenden.

### Zugehörige Tasks:

- „Konfigurieren von Microsoft SNA Server“ auf Seite 15
- „Katalogisieren des APPC- oder APPN-Knotens“ auf Seite 17

## Konfigurieren von IBM eNetwork Communications Server für AIX

Die folgende Unterstützung ist für DB2 Enterprise Server Edition (ESE) für Windows und UNIX Version 8 sowie DB2 Connect Enterprise Edition (EE) für Windows und UNIX Version 8 nicht mehr verfügbar:

- Funktionalität für zweiphasige Festschreibung mit SNA. Anwendungen, für die die zweiphasige Festschreibung erforderlich ist, müssen die TCP/IP-Konnektivität verwenden. Die zweiphasige Festschreibung unter Verwendung einer TCP/IP-Verbindung zu einem Host- oder iSeries-Datenbankserver ist bereits seit einigen Releases verfügbar. Host- oder iSeries-Anwendungen, für die die Unterstützung der zweiphasigen Festschreibung erforderlich ist, können die neue Funktionalität der Unterstützung für die zweiphasige Festschreibung mit TCP/IP innerhalb von DB2 ESE Version 8 verwenden.
- Anwendungen können keine SNA-Verbindungen mehr verwenden, um auf einen DB2 UDB ESE-Server unter UNIX oder Windows bzw. einen DB2 Connect EE-Server zuzugreifen. Anwendungen können weiterhin mit SNA auf Host- oder iSeries-Datenbankserver zugreifen, können aber nur die einphasige Festschreibung verwenden.

### Zugehörige Tasks:

- „Manuelles Konfigurieren der APPC-Kommunikation zwischen DB2 Connect und einem Host- und iSeries-Datenbankserver“ auf Seite 13
- „Katalogisieren des APPC- oder APPN-Knotens“ auf Seite 17

## Konfigurieren von Bull SNA für AIX

Die folgende Unterstützung ist für DB2 Enterprise Server Edition (ESE) für Windows und UNIX Version 8 sowie DB2 Connect Enterprise Edition (EE) für Windows und UNIX Version 8 nicht mehr verfügbar:

- Funktionalität für zweiphasige Festschreibung mit SNA. Anwendungen, für die die zweiphasige Festschreibung erforderlich ist, müssen die TCP/IP-Konnektivität verwenden.

tät verwenden. Die zweiphasige Festschreibung unter Verwendung einer TCP/IP-Verbindung zu einem Host- oder iSeries-Datenbankserver ist bereits seit einigen Releases verfügbar. Host- oder iSeries-Anwendungen, für die die Unterstützung der zweiphasigen Festschreibung erforderlich ist, können die neue Funktionalität der Unterstützung für die zweiphasige Festschreibung mit TCP/IP innerhalb von DB2 ESE Version 8 verwenden.

- Anwendungen können keine SNA-Verbindungen mehr verwenden, um auf einen DB2 UDB ESE-Server unter UNIX oder Windows bzw. einen DB2 Connect EE-Server zuzugreifen. Anwendungen können weiterhin mit SNA auf Host- oder iSeries-Datenbankserver zugreifen, können aber nur die einphasige Festschreibung verwenden.

## Konfigurieren von SNAPLus2 für HP-UX

Die folgende Unterstützung ist für DB2 Enterprise Server Edition (ESE) für Windows und UNIX Version 8 sowie DB2 Connect Enterprise Edition (EE) für Windows und UNIX Version 8 nicht mehr verfügbar:

- Funktionalität für zweiphasige Festschreibung mit SNA. Anwendungen, für die die zweiphasige Festschreibung erforderlich ist, müssen die TCP/IP-Konnektivität verwenden. Die zweiphasige Festschreibung unter Verwendung einer TCP/IP-Verbindung zu einem Host- oder iSeries-Datenbankserver ist bereits seit einigen Releases verfügbar. Host- oder iSeries-Anwendungen, für die die Unterstützung der zweiphasigen Festschreibung erforderlich ist, können die neue Funktionalität der Unterstützung für die zweiphasige Festschreibung mit TCP/IP innerhalb von DB2 ESE Version 8 verwenden.
- Anwendungen können keine SNA-Verbindungen mehr verwenden, um auf einen DB2 UDB ESE-Server unter UNIX oder Windows bzw. einen DB2 Connect EE-Server zuzugreifen. Anwendungen können weiterhin mit SNA auf Host- oder iSeries-Datenbankserver zugreifen, können aber nur die einphasige Festschreibung verwenden.

### Zugehörige Tasks:

- „Manuelles Konfigurieren der APPC-Kommunikation zwischen DB2 Connect und einem Host- und iSeries-Datenbankserver“ auf Seite 13
- „Katalogisieren des APPC- oder APPN-Knotens“ auf Seite 17

## Katalogisieren des APPC- oder APPN-Knotens

Das Katalogisieren des APPC- oder APPN-Knotens ist einer der Arbeitsschritte für die Konfiguration der APPC-Kommunikation auf dem Host für DB2 Connect. Sie müssen einen Eintrag zum Knotenverzeichnis des DB2 Connect-Servers hinzufügen, um den fernen Knoten zu beschreiben.

In den meisten Fällen wird dem Knotenverzeichnis ein Eintrag für einen APPC-Knoten hinzugefügt. Unter 32-Bit-Windows-Betriebssystemen können Sie alternativ dazu einen Eintrag für einen APPN-Knoten hinzufügen, wenn Ihr lokaler SNA-Knoten als APPN-Knoten definiert wurde.

### Voraussetzungen:

Eine Benutzer-ID mit der Berechtigung SYSADM (Systemverwaltung) oder SYSC-TRL (Systemsteuerung). Ist die Option `catalog_noauth` auf `ON` gesetzt, können Sie sich auch ohne diese Berechtigungsstufen am System anmelden.

## Vorgehensweise:

Führen Sie die folgenden Schritte aus, um den Knoten zu katalogisieren:

1. Unter UNIX müssen Sie zunächst die Exemplarumgebung konfigurieren und den DB2-Befehlszeilenprozessor aufrufen. Führen Sie die Startprozedur wie folgt aus:

```
. INSTHOME/sql1lib/db2profile    (für Bash, Bourne oder Korn-Shell)
source INSTHOME/sql1lib/db2cshrc (für C-Shell)
```

Hierbei steht *INSTHOME* für das Ausgangsverzeichnis des Exemplars.

2. Geben Sie zum Katalogisieren eines APPC-Knotens den ausgewählten Aliasnamen (*knotenname*), den symbolischen Bestimmungsnamen (*symbolischer-bestimmungsname*) und die APPC-Sicherheitseinstufung (*sicherheitseinstufung*) an, die der Client für die APPC-Verbindung verwendet. Geben Sie die folgenden Befehle ein:

```
catalog "appc node knotenname remote symbolischer-bestimmungsname
        security sicherheitseinstufung"
terminate
```

Beim Parameter *symbolischer-bestimmungsname* muss die Groß-/Kleinschreibung beachtet werden. Zudem muss dieser Parameter *genau* mit dem Wert des symbolischen Bestimmungsnamens übereinstimmen, den Sie zuvor festgelegt haben.

Geben Sie zum Beispiel zum Katalogisieren des fernen Datenbankservers mit dem symbolischen Bestimmungsnamen *DB2CPIC* auf dem Knoten *db2node* unter Verwendung der APPC-Sicherheitseinstufung *program* die folgenden Befehle ein:

```
catalog appc node db2node remote DB2CPIC security program
terminate
```

3. Geben Sie zum Katalogisieren eines APPN-Knotens den Aliasnamen (*knotenname*), die Netzwerk-ID (**9**), den Namen der fernen Partner-LU (**4**), den Transaktionsprogrammnamen (**17**), den Modus (**15**) und die Sicherheitseinstufung an. Geben Sie die folgenden Befehle ein, wobei Sie Ihre eigenen Werte einsetzen müssen:

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

Der nächste Konfigurationsschritt ist das Katalogisieren der Datenbank als DCS-Datenbank (DCS = Database Connection Service).

### Zugehörige Tasks:

- „Katalogisieren der Datenbank als DCS-Datenbank“ auf Seite 7

## Katalogisieren der Datenbank als DCS-Datenbank

Das Katalogisieren der Datenbank als DCS-Datenbank (DCS = Database Connection Service) ist einer der Arbeitsschritte für die Konfiguration der Kommunikation zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank. Die ferne Datenbank muss als DCS-Datenbank katalogisiert werden, damit DB2 Connect den Zugriff auf diese Datenbank zur Verfügung stellen kann.

**Voraussetzungen:**

Eine Benutzer-ID mit der Berechtigung SYSADM (Systemverwaltung) oder SYSCTRL (Systemsteuerung).

**Vorgehensweise:**

Führen Sie die folgenden Befehle aus, um die ferne Datenbank als DCS-Datenbank zu katalogisieren:

```
catalog dcs db lokaler-dcs-name as zieldatenbankname
terminate
```

Hierbei gilt Folgendes:

- *lokaler-dcs-name* steht für den lokalen Namen der Host- oder iSeries-Datenbank.
- *zieldatenbankname* steht für den Namen der Host- oder iSeries-Datenbank.

Geben Sie beispielsweise die folgenden Befehle ein, um die lokale DB2 Connect-Datenbank *ny* als ferne Host- oder iSeries-Datenbank *newyork* zu katalogisieren:

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

Der nächste Konfigurationsschritt ist das Katalogisieren der Datenbank.

**Zugehörige Tasks:**

- „Katalogisieren des TCP/IP-Knotens“ auf Seite 6
- „Katalogisieren der Datenbank“ auf Seite 8
- „Katalogisieren des APPC- oder APPN-Knotens“ auf Seite 17

**Zugehörige Referenzen:**

- „CATALOG DCS DATABASE Command“ in *Command Reference*

## Katalogisieren der Datenbank

Das Katalogisieren der Datenbank ist einer der Arbeitsschritte für die Konfiguration der Kommunikation zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank. Bevor eine Clientanwendung auf eine ferne Datenbank zugreifen kann, muss die Datenbank auf dem Host- oder iSeries-Systemknoten und auf allen DB2 Connect-Serverknoten, die eine Verbindung zu dieser Datenbank herstellen, katalogisiert werden.

Wenn Sie eine Datenbank erstellen, wird sie automatisch auf der Host- oder iSeries-Maschine katalogisiert. Dabei ist der Aliasname der Datenbank (*aliasname-der-datenbank*) mit dem Datenbanknamen (*datenbankname*) identisch. Die Informationen im Datenbankverzeichnis werden zusammen mit den Informationen im Knotenverzeichnis auf dem DB2 Connect-Server verwendet, um eine Verbindung zur fernen Host- oder iSeries-Datenbank herzustellen.

**Voraussetzungen:**

- Eine Benutzer-ID mit der Berechtigung SYSADM (Systemverwaltung) oder SYSCTRL (Systemsteuerung).
- Identifizieren Sie die folgenden Parameter:
  - Datenbankname (*datenbankname*)
  - Aliasname der Datenbank (*aliasname-der-datenbank*)

- Knotenname (*knotenname*)

### Vorgehensweise:

Führen Sie die folgenden Schritte aus, um eine Datenbank auf dem DB2 Connect-Server zu katalogisieren:

1. Unter UNIX müssen Sie zunächst die Exemplarumgebung konfigurieren und den DB2-Befehlszeilenprozessor aufrufen. Führen Sie die Startprozedur wie folgt aus:

```
. INSTHOME/sql1lib/db2profile    (für Bash, Bourne oder Korn-Shell)
source INSTHOME/sql1lib/db2cshrc (für C-Shell)
```

Hierbei steht *INSTHOME* für das Ausgangsverzeichnis des Exemplars.

2. Katalogisieren Sie die Datenbank wie folgt:

```
catalog database datenbankname as aliasname-der-datenbank at
node knotenname authentication auth_wert
```

Geben Sie beispielsweise die folgenden Befehle ein, um die bei DCS bekannte Datenbank *ny* so zu katalogisieren, dass sie den Aliasnamen der lokalen Datenbank *localny* auf dem Knoten *db2node* besitzt:

```
catalog database ny as localny at node db2node
authentication dcs
terminate
```

Führen Sie die folgenden Schritte aus, um Werte zu ändern, die mit dem Befehl **catalog database** definiert wurden:

- a. Führen Sie den Befehl **uncatalog database** im Befehlszeilenprozessor wie folgt aus:

```
uncatalog database aliasname-der-datenbank
```

- b. Katalogisieren Sie die Datenbank erneut und verwenden Sie die gewünschten Werte.

Der nächste Konfigurationsschritt ist das Binden von Dienstprogrammen und Anwendungen an den Datenbankserver.

### Zugehörige Tasks:

- „Katalogisieren der Datenbank als DCS-Datenbank“ auf Seite 7
- „Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver“ auf Seite 9

### Zugehörige Referenzen:

- „CATALOG DATABASE Command“ in *Command Reference*

## Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver

Das Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver ist einer der Arbeitsschritte für die Konfiguration der Kommunikation zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank. Nach dem Ausführen der Schritte zum Konfigurieren des DB2 Connect-Servers für die Kommunikation mit dem Host- oder iSeries-System müssen Sie die Dienstprogramme und Anwendungen auf dem Host- oder iSeries-Datenbankserver binden.

**Voraussetzungen:**

Eine Benutzer-ID mit der Berechtigung BINDADD.

**Vorgehensweise:**

Führen Sie die folgenden Befehle aus, um die Dienstprogramme und Anwendungen an den Host- oder iSeries-Datenbankserver zu binden:

```
connect to aliasname-der-datenbank user benutzer-id using kennwort
bind bindepfad_verz@ddcsmvs.lst blocking all sqlerror continue
messages mvs.msg grant public
connect reset
```

**Beispiel:**

```
connect to NYC3 user meinebenutzer-id using meinkennwort
bind bindepfad_verz@ddcsmvs.lst blocking all sqlerror continue
messages mvs.msg grant public
connect reset
```

Hierbei steht *bindepfad\_verz* für das Verzeichnis, in dem sich die .lst-Dateien befinden. Unter Windows lautet dieser Pfad in der Regel \SQLLIB\BND\.

Der nächste Konfigurationsschritt ist das Testen der Host- oder iSeries-Verbindung.

**Zugehörige Konzepte:**

- „Binden von Dienstprogrammen an die Datenbank“ in *Systemverwaltung: Implementierung*

**Zugehörige Tasks:**

- „Katalogisieren der Datenbank“ auf Seite 8
- „Testen der Host- oder iSeries-Verbindung“ auf Seite 10

**Zugehörige Referenzen:**

- „BIND Command“ in *Command Reference*

## Testen der Host- oder iSeries-Verbindung

Das Testen der Host- oder iSeries-Verbindung ist einer der Arbeitsschritte für die Konfiguration der Kommunikation zwischen einem DB2 Connect-Server und einer Host- oder iSeries-Datenbank. Wenn die Konfiguration des DB2 Connect-Servers für die Host- oder iSeries-Kommunikation abgeschlossen ist, müssen Sie die Verbindung mit Hilfe einer fernen Datenbank testen.

**Voraussetzungen:**

- Zum Testen der Verbindung wird eine Verbindung zu einer fernen Datenbank hergestellt.
- Die Werte für *benutzer-id* und *kennwort* müssen für das System, auf dem sie authentifiziert werden, zulässig sein. Standardmäßig erfolgt die Authentifizierung auf dem Host- oder iSeries-Datenbankserver.

### Vorgehensweise:

Gehen Sie wie folgt vor, um die Host- oder iSeries-Verbindung zu testen:

1. Starten Sie den Datenbankmanager durch Eingabe des Befehls **db2start** auf dem Host- oder iSeries-Datenbankserver (wenn er nicht bereits gestartet ist).
2. Stellen Sie mit dem folgenden Befehl eine Verbindung zur fernen Datenbank her:

```
connect to aliasname-der-datenbank user benutzer-id using kennwort
```

Geben Sie zum Beispiel den folgenden Befehl ein:

```
connect to nyc3 user benutzer-id using kennwort
```

Die Authentifizierung für die Verbindung mit Hostdatenbanken wird während der Konfiguration von DB2 Connect eingerichtet.

Wurde die Verbindung erfolgreich hergestellt, wird der Name der Datenbank, mit der die Verbindung besteht, in einer Nachricht angezeigt. Von dieser Datenbank können nun Daten abgerufen werden.

Geben Sie beispielsweise den folgenden SQL-Befehl ein, um eine Liste aller Tabellennamen abzurufen, die in der Systemkatalogtabelle aufgeführt sind:

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

Wenn Sie die Datenbankverbindung nicht mehr benötigen, geben Sie den Befehl **db2 connect reset** ein, um die Datenbankverbindung zu beenden.

### Zugehörige Tasks:

- „Binden von Dienstprogrammen und Anwendungen an den Host- oder iSeries-Datenbankserver“ auf Seite 9

---

## **Teil 2. Einrichten von Host- oder iSeries-Anwendungsreques- tern**



---

## Kapitel 3. Einrichten von OS/390- und z/OS-Anwendungsrequestern

---

### Definieren von DB2 als Anwendungsrequester (OS/390 und z/OS)

DB2 für OS/390 und z/OS implementiert die Unterstützung für den DRDA-Anwendungsrequester als integralen Bestandteil der Distributed Data Facility (DDF) von DB2 für OS/390 und z/OS. DDF kann unabhängig von den lokalen Funktionen für die Verwaltung von Datenbanken unter DB2 für OS/390 und z/OS gestoppt werden; DDF kann jedoch nicht ohne lokale Unterstützung für die Verwaltung von Datenbanken unter DB2 für OS/390 und z/OS ausgeführt werden.

Wenn DB2 für OS/390 und z/OS als Anwendungsrequester fungiert, kann die Verbindung zwischen auf dem System ausgeführten Anwendungen und fernen Datenbankservern unter DB2 Universal Database für OS/390 und z/OS, DB2 UDB für iSeries und DB2 Server für VSE & VM hergestellt werden, die die DRDA-Anwendungsserverfunktion implementieren.

Der Anwendungsrequester muss in der Lage sein, RDB\_NAME-Werte entgegenzunehmen und in SNA-NETID.LUNAME-Werte oder TCP/IP-Adresswerte umzuwandeln. DB2 für OS/390 und z/OS verwendet die Kommunikationsdatenbank (Communications Database - CDB) von DB2 für OS/390 und z/OS zum Registrieren der RDB\_NAME-Werte und ihrer entsprechenden Netzwerkparameter. Mit der Kommunikationsdatenbank kann der Anwendungsrequester unter DB2 für OS/390 und z/OS die erforderlichen Informationen an den Communications Server übergeben, wenn Anforderungen für verteilte Datenbanken über SNA- bzw. TCP/IP-Verbindungen abgesetzt werden.

#### Vorgehensweise:

Für viele Verarbeitungsprozesse in einer verteilten Datenbankumgebung ist der Austausch von Nachrichten mit anderen Netzwerkstandorten erforderlich. Damit diese Verarbeitungsprozesse korrekt ausgeführt werden können, müssen Sie die folgenden Schritte ausführen:

1. Definieren Sie den DB2-Anwendungsrequester für das lokale System (SNA) oder definieren Sie den DB2-Anwendungsrequester für das lokale System (TCP/IP).
2. Definieren Sie die fernen Systeme.

#### Zugehörige Konzepte:

- „Datendarstellung (OS/390 und z/OS)“ auf Seite 129
- „Sicherheitsüberlegungen für Anwendungsrequester (OS/390 und z/OS)“ auf Seite 115
- „DB2 für OS/390 und z/OS“ auf Seite 73

#### Zugehörige Tasks:

- „Definieren des DB2-Anwendungsrequesters für das lokale System – SNA (OS/390 und z/OS)“ auf Seite 26
- „Definieren des DB2-Anwendungsrequesters für das lokale System – TCP/IP (OS/390 und z/OS)“ auf Seite 29

- „Definieren der fernen Systeme (OS/390 und z/OS)“ auf Seite 30
- „Definieren von DB2 als Anwendungsserver (OS/390 und z/OS)“ auf Seite 47

---

## Tasks für die Einrichtung

### Definieren des DB2-Anwendungsrequesters für das lokale System – SNA (OS/390 und z/OS)

Das Definieren des lokalen Systems ist einer der Arbeitsschritte für die Einrichtung von DB2 für OS/390 und z/OS als Anwendungsserver. Jedem Programm im SNA-Netzwerk werden eine Netzwerk-ID (NETID) und ein LU-Name zugeordnet, d. h. der Anwendungsrequester unter DB2 für OS/390 und z/OS muss einen (durch VTAM zugeordneten) NETID.LUNAME-Wert aufweisen, wenn die Verbindung zum Netzwerk hergestellt wird. Da der Anwendungsrequester unter DB2 für OS/390 und z/OS in das lokale Datenbankverwaltungssystem von DB2 für OS/390 und z/OS integriert ist, muss der Anwendungsrequester auch über einen RDB\_NAME-Wert verfügen. In den Veröffentlichungen zu DB2 für OS/390 wird der RDB\_NAME als *Standortname* bezeichnet.

#### Vorgehensweise:

Gehen Sie wie folgt vor, um den Anwendungsrequester unter DB2 für OS/390 und z/OS im SNA-Netzwerk zu definieren:

1. Wählen Sie einen LU-Namen für das System unter DB2 für OS/390 und z/OS aus. Die NETID des Systems unter DB2 für OS/390 und z/OS wird beim Starten von DDF von VTAM automatisch abgerufen.
2. Definieren Sie den LU-Namen und Standortnamen im *Bootstrap Data Set* (BSDS) von DB2 für OS/390 und z/OS. (Unter DB2 für OS/390 und z/OS ist die Länge des Standortnamens auf 16 Zeichen beschränkt.)
3. Erstellen Sie eine VTAM-APPL-Definition, um den ausgewählten LU-Namen bei VTAM zu registrieren.
4. Stellen Sie sicher, dass die Option für erweiterte Sicherheit (Extended Security) auf YES gesetzt ist.

#### Konfigurieren des DDF-BSDS:

Während des Startvorgangs liest DB2 für OS/390 und z/OS den BSDS, um Parameter der Systeminstallation abzurufen. Einer der im BSDS gespeicherten Datensätze ist der so genannte *DDF-Datensatz*, weil er die von DDF verwendeten Informationen zur Verbindungsherstellung zu VTAM enthält. Dabei handelt es sich um folgende Informationen:

- Der Standortname für das System mit DB2 für OS/390 und z/OS
- Der LU-Name für das System mit DB2 für OS/390 und z/OS
- Das bei der Verbindungsherstellung vom System mit DB2 für OS/390 und z/OS zu VTAM verwendete Kennwort

Sie können DB2 für OS/390 und z/OS die DDF-BSDS-Informationen auf die folgenden beiden Arten zur Verfügung stellen:

- Stellen Sie die erforderlichen DDF-BSDS-Informationen bei der Erstinstallation von DB2 für OS/390 und z/OS mit Hilfe der DDF-Installationsanzeige DSNTIPR bereit. Viele der Installationsparameter werden hier nicht erläutert, weil es wichtiger ist, das Verfahren zum Herstellen einer Verbindung zwischen DB2 für

OS/390 und z/OS und VTAM zu kennen. In Abb. 1 wird dargestellt, wie Sie mit Hilfe der Installationsanzeige den Standortnamen NEW\_YORK3, den LU-Namen NYM2DB2 und das Kennwort PSWDBD1 im BSDS von DB2 für OS/390 und z/OS eintragen können.

```

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

```

Abbildung 1. Installationsanzeige DSNTIPR von DB2 für OS/390 und z/OS

- Ist DB2 für OS/390 und z/OS bereits installiert, können Sie die Informationen im BSDS mit dem Dienstprogramm zum Ändern des Protokollinventars (DSN-JU003) aktualisieren.

In Abb. 2 wird dargestellt, wie der BSDS mit dem Standortnamen NEW\_YORK3, dem LU-Namen NYM2DB2 und dem Kennwort PSWDBD1 aktualisiert wird.

```

//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
/*

```

Abbildung 2. Beispiel für BSDS-DDF-Definition (für VTAM)

Beim Starten von DDF (entweder automatisch beim Starten von DB2 für OS/390 und z/OS oder durch den Befehl START DDF von DB2 für OS/390 und z/OS) wird die Verbindung zu VTAM hergestellt, wobei der LU-Name und das Kennwort an VTAM übergeben werden.

VTAM erkennt das System mit DB2 für OS/390 und z/OS, indem es den LU-Namen und das Kennwort (sofern ein VTAM-Kennwort erforderlich ist) anhand der in der VTAM-Anweisung APPL von DB2 für OS/390 und z/OS definierten Werte überprüft. Mit dem VTAM-Kennwort wird überprüft, ob DB2 für OS/390 und z/OS berechtigt ist, den angegebenen LU-Namen auf dem VTAM-System zu verwenden. Das VTAM-Kennwort wird nicht über das Netzwerk übertragen, und es wird nicht zur Herstellung einer Verbindung zwischen anderen Systemen im Netzwerk und DB2 für OS/390 und z/OS verwendet.

Ist für VTAM kein Kennwort erforderlich, müssen Sie das Schlüsselwort `PASS-WORD=` im Dienstprogramm zum Ändern des Protokollinventars übergehen. Das Fehlen des Schlüsselworts gibt an, dass kein VTAM-Kennwort erforderlich ist.

**Erstellen einer VTAM-APPL-Definition, um den ausgewählten LU-Namen bei VTAM zu registrieren:**

Nach dem Definieren des LU-Namens und Kennworts von VTAM für DB2 für OS/390 und z/OS müssen Sie diese Werte in VTAM registrieren. VTAM verwendet die Anweisung APPL, um lokale LU-Namen zu definieren. In Abb. 3 wird eine Beispielformatdefinition für den LU-Namen `NYM2DB2` dargestellt.

```

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

```

Abbildung 3. VTAM-APPL-Beispielformatdefinition für DB2 für OS/390 und z/OS

**Zugehörige Tasks:**

- „Definieren des DB2-Anwendungsrequesters für das lokale System – TCP/IP (OS/390 und z/OS)“ auf Seite 29
- „Definieren der fernen Systeme (OS/390 und z/OS)“ auf Seite 30

**Zugehörige Referenzen:**

- „Schlüsselwörter der VTAM-Anweisung APPL von DB2 Connect“ auf Seite 146

## Definieren des DB2-Anwendungsrequesters für das lokale System – TCP/IP (OS/390 und z/OS)

### Vorgehensweise:

Damit die TCP/IP-Kommunikation mit DB2 für OS/390 und z/OS definiert werden kann, müssen die folgenden Bedingungen erfüllt sein:

1. Die TCP/IP-Kommunikation muss für das System mit DB2 für OS/390 und z/OS und auf dem Partnersystem aktiviert sein.
2. Der Netzwerkadministrator muss zwei geeignete TCP/IP-Portnummern zuordnen. DB2 für OS/390 und z/OS verwendet standardmäßig die Portnummer 446 für Datenbankverbindungen und die Portnummer 5001 für Resynchronisationsanforderungen (zweiphasige Festschreibung).
3. Der ferne Anwendungsserver bzw. Anwendungsrequester muss die gleichen Portnummern (bzw. Servicenamen) wie DB2 für OS/390 und z/OS verwenden.
4. Stellen Sie sicher, dass die Option für bereits überprüfte TCP/IP-Sicherheit auf YES gesetzt ist.
5. Der BSDS von DB2 für OS/390 und z/OS muss zusätzliche Parameter enthalten. In Abb. 4 werden diese für die Aktivierung der TCP/IP-Kommunikation erforderlichen zusätzlichen Parameter dargestellt.

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

Abbildung 4. Beispiel für BSDS-DDF-Definition (für TCP/IP)

### Zugehörige Tasks:

- „Definieren des DB2-Anwendungsrequesters für das lokale System – SNA (OS/390 und z/OS)“ auf Seite 26
- „Definieren der fernen Systeme (OS/390 und z/OS)“ auf Seite 30

## Definieren der fernen Systeme (OS/390 und z/OS)

Wenn eine Anwendung unter DB2 für OS/390 und z/OS Daten von einem fernen System anfordert, sucht sie in den Tabellen der Kommunikationsdatenbank (Communications Database - CDB) nach Informationen zum fernen System. Die Kommunikationsdatenbank ist eine Gruppe von SQL-Tabellen, die vom Systemadministrator von DB2 für OS/390 und z/OS verwaltet wird.

### Vorgehensweise:

Der Systemadministrator von DB2 für OS/390 und z/OS kann mit Hilfe von SQL Zeilen mit Beschreibungen aller potenziellen DRDA-Partner in die Kommunikationsdatenbank einfügen.

Verweise auf die Kommunikationsdatenbank suchen unter anderem nach folgenden Informationen:

- LU-Name und TPN (für SNA-Verbindungen)
- TCP/IP-Adressinformationen (nur für abgehende TCP/IP-SNA-Verbindungen erforderlich)
- Vom fernen Standort benötigte Informationen zur Netzwerksicherheit
- Zum Übertragen von Daten an ferne Standorte verwendete Sitzungsbegrenzungen und Modusnamen (für SNA-Verbindungen)

### Eintragen von Werten in die Kommunikationsdatenbank:

Aktualisierungen der Kommunikationsdatenbank sind nicht erforderlich, wenn Sie die TCP/IP-Datenbankverbindungen nur für eingehende Anforderungen verwenden; wenn DB2 für OS/390 und z/OS nur als TCP/IP-Server verwendet werden soll, müssen Sie daher keine Werte in der Kommunikationsdatenbank eintragen. Statt dessen können die Standardwerte verwendet werden. Wenn jedoch SNA-Verbindungen für eingehende Anforderungen verwendet werden sollen, müssen Sie mindestens eine leere Zeile in der Tabelle SYSIBM.LUNAMES bereitstellen.

Damit beispielsweise Anforderungen für SNA-Datenbankverbindungen von einer beliebigen ankommenden LU von DB2 Connect akzeptiert werden, müssen Sie einen SQL-Befehl wie den folgenden verwenden:

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

Wenn Sie DB2 für OS/390 und z/OS als Requester verwenden, müssen Sie die Kommunikationsdatenbank auf jeden Fall aktualisieren. Dabei müssen Zeilen in die Tabelle SYSIBM.LOCATIONS und entweder in die Tabelle SYSIBM.LUNAMES (für SNA-Verbindungen) oder die Tabelle SYSIBM.IPNAMES (für TCP/IP-Verbindungen) eingefügt werden.

Wenn Sie bei SNA-Verbindungen die Sicherheitsvoraussetzungen oder die Namensumsetzung für eingehende Anforderungen steuern wollen, sind unter Umständen zusätzliche Kommunikationsdatenbankaktualisierungen erforderlich.

Ausführlichere Informationen zu den Voraussetzungen für das Aktualisieren von Kommunikationsdatenbanktabellen finden Sie im Handbuch *DB2 for OS/390 Administration Guide*. Nach dem Eintragen der Werte in die Kommunikationsdatenbank können Sie Abfragen schreiben, die auf Daten ferner Systeme zugreifen. Das Handbuch *DB2 for OS/390 Installation Guide* enthält außerdem weitere Informationen zum Aktualisieren der Kommunikationsdatenbank.

### **Anforderungsverarbeitung durch die Kommunikationsdatenbank:**

Wenn DB2 für OS/390 und z/OS eine Anforderung sendet, verwendet es die Spalte LINKNAME der Katalogtabelle SYSIBM.LOCATIONS, um das für abgehende Datenbankverbindungen verwendete Netzwerkprotokoll zu ermitteln. Um VTAM-Anforderungen empfangen zu können, müssen Sie in der Installationsanzeige DSNTIPR von DB2 für OS/390 und z/OS einen LUNAME-Wert auswählen. Um TCP/IP-Anforderungen empfangen zu können, müssen Sie in der Installationsanzeige DSNTIP5 von DB2 für OS/390 und z/OS einen DRDA-Port und einen Resynchronisationsport auswählen. TCP/IP verwendet die Portnummer des Servers, um Netzwerkanforderungen an das korrekte DB2-Subsystem zu übergeben.

Wird der Wert in der Spalte LINKNAME der Tabelle SYSIBM.IPNAMES gefunden, wird für DRDA-Verbindungen TCP/IP verwendet. Wird der Wert in der Tabelle SYSIBM.LUNAMES gefunden, wird SNA verwendet. Wird der gleiche Name in beiden Tabellen (SYSIBM.LUNAMES und SYSIBM.IPNAMES) gefunden, wird zum Herstellen der Verbindung zum Standort TCP/IP verwendet.

**Anmerkung:** Ein Requester kann die Verbindung zu einem bestimmten Standort nicht unter Verwendung beider Protokolle (SNA und TCP/IP) herstellen. Wenn beispielsweise in der Tabelle SYSIBM.LOCATIONS für LINKNAME der Wert LU1 angegeben ist und LU1 in den Tabellen SYSIBM.IPNAMES und SYSIBM.LUNAMES definiert ist, wird zum Herstellen der Verbindung zu LU1 von diesem Requester aus nur das TCP/IP-Protokoll verwendet.

### **Zugehörige Tasks:**

- „Definieren des DB2-Anwendungsrequesters für das lokale System – SNA (OS/390 und z/OS)“ auf Seite 26
- „Definieren des DB2-Anwendungsrequesters für das lokale System – TCP/IP (OS/390 und z/OS)“ auf Seite 29



---

## Kapitel 4. Einrichten von AS/400-Anwendungsrequestern

---

### Definieren von DB2 als Anwendungsrequester – SNA (iSeries)

Das iSeries-System implementiert die Unterstützung für den DRDA-Anwendungsrequester als integralen Bestandteil des Betriebssystems OS/400. Da die Unterstützung für Anwendungsrequester Teil des Betriebssystems OS/400 ist, ist sie immer aktiv, wenn das Betriebssystem aktiv ist.

#### Vorgehensweise:

Der Anwendungsrequester muss in der Lage sein, den Namen einer relationalen Datenbank entgegenzunehmen und in Netzwerkparameter umzusetzen. Das iSeries-System verwendet das Verzeichnis für relationale Datenbanken zum Registrieren der Namen relationaler Datenbanken und der dazugehörigen Netzwerkparameter. Dieses Verzeichnis ermöglicht dem iSeries-Anwendungsrequester das Übergeben der erforderlichen Netzwerkinformationen, um die Kommunikation in einem Netzwerk mit verteilten Datenbanken herzustellen.

Für viele Verarbeitungsprozesse in einer verteilten Datenbankumgebung ist der Austausch von Nachrichten mit anderen Netzwerkstandorten erforderlich. Wenn DB2 UDB für iSeries als Anwendungsrequester fungiert, kann es eine Verbindung zu jedem Anwendungsserver herstellen, der DRDA unterstützt. Damit der Anwendungsrequester unter DB2 UDB für iSeries den Zugriff auf verteilte Datenbanken zur Verfügung stellen kann, müssen Sie die folgenden Schritte ausführen:

- Definieren Sie den Anwendungsrequester unter DB2 für iSeries für das lokale System
- Definieren Sie das ferne System
- Definieren Sie die SNA-Kommunikation

#### Zugehörige Konzepte:

- „Datendarstellung (iSeries)“ auf Seite 129
- „Sicherheitsüberlegungen für Anwendungsrequester (iSeries)“ auf Seite 122
- „DB2 UDB für iSeries“ auf Seite 81
- „Herstellen einer Verbindung zu DB2 UDB über TCP/IP (iSeries)“ auf Seite 53

#### Zugehörige Tasks:

- „Definieren des Anwendungsrequesters für das lokale System – SNA (iSeries)“ auf Seite 34
- „Definieren des fernen Systems (iSeries)“ auf Seite 34
- „Definieren der SNA-Kommunikation (iSeries)“ auf Seite 35
- „Definieren von DB2 als Anwendungsrequester – SNA (iSeries)“ auf Seite 51

---

## Tasks für die Einrichtung

### Definieren des Anwendungsrequesters für das lokale System – SNA (iSeries)

Jeder Anwendungsrequester im Netzwerk mit verteilten Datenbanken muss in seinem Verzeichnis relationaler Datenbanken einen Eintrag für die eigene lokale relationale Datenbank und je einen Eintrag für jede ferne relationale Datenbank haben, auf die der Anwendungsrequester zugreift. Jedes iSeries-System im Netzwerk mit verteilten Datenbanken, das nur als Anwendungsserver fungiert, muss im eigenen Verzeichnis relationaler Datenbanken einen Eintrag für die lokale relationale Datenbank haben.

#### Vorgehensweise:

Benennen Sie zum Definieren des lokalen Systems die lokale Datenbank, indem Sie einen Eintrag mit dem Namen \*LOCAL als Name der fernen Station zum Verzeichnis relationaler Datenbanken hinzufügen. Verwenden Sie dazu den Befehl zum Hinzufügen eines Eintrags im Verzeichnis relationaler Datenbanken (ADDRDBDIRE). Das folgende Beispiel stellt den Befehl ADDRDBDIRE dar, in dem ROCHESTERDB als Datenbankname des Anwendungsrequesters angegeben wird:

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

In den neusten Versionen von OS/400 wird der Eintrag für den Namen der lokalen RDB bei Bedarf automatisch erstellt, wenn er nicht bereits vorhanden ist. Als lokaler RDB-Name wird der Systemname in den Netzwerkattributen verwendet.

#### Zugehörige Tasks:

- „Definieren des fernen Systems (iSeries)“ auf Seite 34

### Definieren des fernen Systems (iSeries)

Für jeden Anwendungsserver im Netzwerk mit verteilten Datenbanken muss auch ein lokaler Eintrag im RDB-Verzeichnis vorhanden sein. Darüber hinaus muss im RDB-Verzeichnis der einzelnen Anwendungsrequester ein Eintrag für jede ferne Datenbank bestehen.

#### Vorgehensweise:

Führen Sie die folgenden Schritte aus, um die fernen Datenbanken für die lokale Datenbank zu definieren:

- Verwenden Sie den Befehl ADDRDBDIRE bzw. WRKRDBDIRE, um einen Eintrag für jede ferne Datenbank zum Verzeichnis relationaler Datenbanken hinzuzufügen. Bei Verwendung der SNA-Kommunikation können Sie folgende Informationen angeben:
  - Name der fernen Datenbank
  - Name des fernen Standorts der Datenbank
  - Name des lokalen Standorts
  - Name des zum Herstellen der Kommunikation verwendeten Modus
  - Ferne Netzwerk-ID
  - Name der für die Kommunikation verwendeten Einheit
  - Name des Transaktionsprogramms der fernen Datenbank

In den meisten Fällen sind nur der Name der fernen Datenbank und der Name des fernen Standorts<sup>1</sup> der Datenbank erforderlich. Wird nur der Name des fernen Standorts angegeben, werden für die übrigen Parameter Standardwerte verwendet. Das System wählt eine Einheitenbeschreibung aus, die den Namen der fernen Datenbank enthält.

Wenn der selbe Name für einen fernen Standort in mehreren Einheitenbeschreibungen vorkommt und eine bestimmte Beschreibung erforderlich ist, sollten die Werte für den lokalen Standort und die ferne Netzwerk-ID in dem Eintrag im Verzeichnis relationaler Datenbanken mit den Werten in der Einheitenbeschreibung übereinstimmen. Das Auswählen von Einheitenbeschreibungen kann kompliziert werden, wenn der selbe Name für einen fernen Standort in mehreren Einheitenbeschreibungen verwendet wird. Verwenden Sie in jeder Einheitenbeschreibung eindeutige Namen für ferne Standorte, um Verwechslungen zu vermeiden. Als Transaktionsprogrammname der fernen Datenbank wird standardmäßig der DRDA-Standard-Transaktionsprogrammname X'07F6C4C2' verwendet.

Die Informationen zur Kommunikation im Verzeichnis relationaler Datenbanken werden zum Einrichten eines Dialogs mit dem fernen System verwendet.

#### **Zugehörige Tasks:**

- „Definieren der SNA-Kommunikation (iSeries)“ auf Seite 35
- „Definieren des Anwendungsrequesters für das lokale System – SNA (iSeries)“ auf Seite 34

## **Definieren der SNA-Kommunikation (iSeries)**

Das iSeries-System ermöglicht auch Konfigurationen für APPC (Advanced Program-to-Program Communications), die keine Unterstützung für die Weiterleitung im Netzwerk bereitstellen. Eine verteilte iSeries-Datenbank kann mit jeder der beiden Konfigurationen betrieben werden.

Die AnyNet-Unterstützung auf dem iSeries-System ermöglicht das Ausführen von APPC-Anwendungen über TCP/IP-Netzwerke (TCP/IP - Transmission Control Protocol/Internet Protocol). Die Beispiele in den nachfolgenden Abschnitten umfassen DDM, SNA-Verteilungsservices (Systems Network Architecture Distribution Services), Alerts und 5250 Datensichtgerätsdurchgriff. Diese Anwendungen können zusammen mit DRDA nach einigen zusätzlichen Konfigurationsschritten unverändert über TCP/IP-Netzwerke ausgeführt werden. Geben Sie für die AnyNet-Unterstützung den Wert \*ANYNW im Parameter LINKTYPE des Befehls CRTCTLAPPC ein.

#### **Vorgehensweise:**

APPN stellt eine Unterstützung für den Netzwerkbetrieb zur Verfügung, mit deren Hilfe das iSeries-System an einem Netzwerk aus Systemen teilnehmen und dieses steuern kann, ohne dass die Netzwerkunterstützung erforderlich ist, die normalerweise von einem Großrechnersystem implementiert wird. Führen Sie die folgenden Schritte aus, um ein iSeries-System für die APPN-Unterstützung zu konfigurieren:

1. Verwenden sie den Befehl zum Ändern der Netzwerkattribute (CHGNETA), um die Netzwerkattribute zu definieren.

---

1. „Standortname“ in OS/400 ist gleich bedeutend mit „LU-Name“ in VTAM. „Name des fernen Standorts“ bedeutet „Name der Partner-LU oder der fernen LU“.

Zu den Netzwerkattributen gehören:

- Der Name des lokalen Systems
- Der Name des Systems im APPN-Netzwerk
- Die Kennung (ID) des lokalen Netzwerks
- Der Netzwerkknotentyp
- Die Namen der vom iSeries-System verwendeten Netzwerkserver, wenn die Maschine ein Endknoten ist
- Die Netzwerksteuerpunkte, wenn das iSeries-System ein Endknoten ist

2. Erstellen Sie die Leitungsbeschreibung.

Die Leitungsbeschreibung beschreibt die physische Verbindungsleitung und das Datenübertragungsprotokoll, die zwischen dem iSeries-System und dem Netzwerk verwendet werden sollen. Verwenden Sie zum Erstellen von Leitungsbeschreibungen die folgenden Befehle:

- Leitungsbeschreibung erstellen (Ethernet) (CRTLINETH)
- Leitungsbeschreibung erstellen (SDLC) (CRTLINS DLC)
- Leitungsbeschreibung erstellen (Token-Ring) (CRTLINTRN)
- Leitungsbeschreibung erstellen (X.25) (CRTLINX25)

3. Erstellen Sie Controllerbeschreibungen.

Die Controllerbeschreibung beschreibt die benachbarten Systeme im Netzwerk. Weisen Sie beim Erstellen der Controllerbeschreibung auf die Verwendung der APPN-Unterstützung hin, indem Sie APPN(\*YES) angeben. Verwenden Sie zum Erstellen von Controllerbeschreibung die folgenden Befehle:

- Controllerbeschreibung erstellen (APPC) (CRTCTLAPPC)
- Controllerbeschreibung erstellen (SNA-HOST) (CRTCTHHOST)

Wird der Parameter AUTOCRTCTL einer Token-Ring- oder Ethernet-Leitungsbeschreibung auf \*YES gesetzt, wird automatisch eine Controllerbeschreibung erstellt, wenn das System über die Token-Ring- oder Ethernet-Leitung eine Sitzungsstartanforderung empfängt.

4. Erstellen Sie eine Serviceklassenbeschreibung.

Die Serviceklassenbeschreibung wird zum Auswählen der Kommunikationsverbindungswege (Übertragungsgruppen) und zur Vergabe von Übertragungsprioritäten verwendet. Das System stellt die folgenden fünf Serviceklassenbeschreibungen zur Verfügung:

**#CONNECT**

Die Standardserviceklasse.

**#BATCH**

Eine Serviceklasse für Stapeljobs.

**#BATCHSC**

Entspricht #BATCH, jedoch ist mindestens die Datenübertragungssicherheit eines Netzwerks mit Paketvermittlung erforderlich. In paketvermittelten Netzwerken nehmen Daten nicht immer den selben Weg durch das Netzwerk.

**#INTER**

Eine Serviceklasse, die auf interaktive Kommunikation abgestimmt ist.

**#INTERSC**

Entspricht #INTER, jedoch ist mindestens die Datenübertragungssicherheit eines Netzwerks mit Paketvermittlung erforderlich.

Weitere Serviceklassen können mit dem Befehl zum Erstellen von Serviceklassen (CRTCOSD) erstellt werden.

5. Erstellen Sie eine Modusbeschreibung.

Die Modusbeschreibung gibt die Kenndaten der Sitzung an sowie die Anzahl der Sitzungen, die zum Vereinbaren der zulässigen Werte zwischen dem lokalen und dem fernen Standort verwendet werden können. Die Modusbeschreibung verweist außerdem auf die Serviceklasse, die für den Datenaustausch verwendet wird. Im Lieferumfang des Systems sind die folgenden vordefinierten Modi enthalten:

**BLANK**

Der werkseitig in den Netzwerkattributen angegebene Standardmodusname.

**#BATCH**

Ein auf Stapeljobs abgestimmter Modus.

**#BATCHSC**

Entspricht #BATCH, jedoch ist für die zugeordnete Serviceklassenbeschreibung mindestens die Datenübertragungssicherheit eines Netzwerks mit Paketvermittlung erforderlich.

**#INTER**

Ein auf interaktive Kommunikation abgestimmter Modus.

**#INTERSC**

Entspricht #INTER, jedoch ist für die zugeordnete Serviceklassenbeschreibung mindestens die Datenübertragungssicherheit eines Netzwerks mit Paketvermittlung erforderlich.

**IBMRDB**

Ein auf DRDA-Kommunikation abgestimmter Modus.

Weitere Modusbeschreibungen können mit dem Befehl zum Erstellen von Modusbeschreibungen (CRTMODD) erstellt werden.

6. Erstellen Sie Einheitenbeschreibungen.

Die Einheitenbeschreibung gibt die Kenndaten der logischen Verbindung zwischen dem lokalen und dem fernen System an. Sie müssen Einheitenbeschreibungen nicht manuell erstellen, wenn das iSeries-System in Verbindung mit einem Hostsystem mit APPN und als unabhängige logische Einheit (LU) ausgeführt wird. Das iSeries-System erstellt die Einheitenbeschreibung automatisch und ordnet sie der entsprechenden Controllerbeschreibung zu, wenn die Sitzung eingerichtet wird. Ist das iSeries-System eine abhängige LU, müssen Sie die Einheitenbeschreibungen mit dem Befehl zum Erstellen von Einheitenbeschreibungen (CRTDEVAPPC) manuell erstellen. Geben Sie in der Einheitenbeschreibung den Wert APPN(\*YES) an, um anzuzeigen, dass APPN verwendet wird.

7. Erstellen Sie APPN-Standortlisten.

Sind für APPN zusätzliche lokale Standorte (in anderen Systemen als LUs bezeichnet) oder spezielle Kenndaten für ferne Standorte erforderlich, müssen Sie APPN-Standortlisten erstellen. Der Name des lokalen Standorts ist der in den Netzwerkattributen angegebene Steuerpunktname. Wenn Sie zusätzliche Standorte für das iSeries-System benötigen, ist eine Liste lokaler APPN-Standorte erforderlich. Ein Beispiel für einen fernen Standort mit speziellen Kenndaten liegt vor, wenn der ferne Standort sich in einem anderen Netzwerk befindet als der lokale Standort. Unter diesen Bedingungen ist eine Liste ferner APPN-Standorte erforderlich. APPN-Standortlisten werden mit dem Befehl zum Erstellen von Konfigurationslisten (CRTCFGL) erstellt.

8. Aktivieren Sie die Kommunikation (vary on).  
Zum Aktivieren der Beschreibungen für die Kommunikation können Sie den Befehl zum An-/Abhängen der Konfiguration (VRYCFG) oder den Befehl zum Arbeiten mit dem Konfigurationsstatus (WRKCFGSTS) verwenden. Sind die Leitungsbeschreibungen aktiviert, sind die mit dieser Leitung verbundenen Controllern und Einheiten ebenfalls aktiviert. Mit dem Befehl WRKCFGSTS kann außerdem der Status jeder Verbindung angezeigt werden.
9. RU-Größe und Nachrichtendosierung.  
RU-Größe und Nachrichtendosierung werden durch Werte gesteuert, die in der Modusbeschreibung angegeben sind. Wenn Sie die Modusbeschreibung erstellen, werden Standardwerte für die RU-Größe und Nachrichtendosierung bereitgestellt. Die Standardwerte sind ein iSeries-Schätzwert für die meisten Umgebungen (einschließlich einer verteilten Datenbank). Wird der Standardwert für die RU-Größe übernommen, schätzt das iSeries-System den besten Wert. Kommuniziert das iSeries-System mit einem anderen System, das angepasste Nachrichtendosierung unterstützt, sind die angegebenen Nachrichtendosierungswerte nur vorläufige Anfangswerte. Die Nachrichtendosierung wird von jedem System entsprechend seiner Fähigkeiten zum Verarbeiten der empfangenen Daten angepasst. Für Systeme, die keine angepasste Nachrichtendosierung unterstützen, werden die Nachrichtendosierungswerte zu Beginn der Sitzung festgelegt und bleiben für die Dauer der Sitzung unverändert.

**Anmerkungen:**

1. Die Controllerbeschreibung entspricht den NCP/VTAM-PU-Makros (IBM Network Control Program/Virtual Telecommunications Access Method Physical Unit Macros).
2. Die Einheitenbeschreibung entspricht dem NCP/VTAM-LU-Makro. Die Einheitenbeschreibung enthält ähnliche Informationen wie die, die im Partner-LU-Profil von Communications Manager Version 2 1.1 gespeichert sind.
3. Die Modusbeschreibung entspricht den NCP/VTAM-Modustabellen und dem Übertragungsservice-Modusprofil von Communications Manager.

**Zugehörige Tasks:**

- „Definieren des Anwendungsrequesters für das lokale System – SNA (iSeries)“ auf Seite 34
- „Definieren des fernen Systems (iSeries)“ auf Seite 34

---

## Kapitel 5. Einrichten von VM-Anwendungsrequestern

---

### Definieren von DB2 als Anwendungsrequester (VM)

DB2 für VM implementiert die Unterstützung für DRDA-Anwendungsrequester als integralen Bestandteil des Ressourcenadapters, der sich zusammen mit der Anwendung auf der virtuellen Maschine des Endbenutzers befindet. Sie können die Unterstützung für Anwendungsrequester auch verwenden, wenn die virtuelle Maschine des lokalen Datenbankmanagers nicht aktiv ist. Die Unterstützung für den DRDA-Anwendungsrequester kann aktiviert werden, indem SQLINIT EXEC mit "protocol(auto)" oder "protocol(drda)" ausgeführt wird.

#### Vorgehensweise:

Wenn DB2 für VM als Anwendungsrequester fungiert, kann eine Verbindung zu einem Anwendungsserver unter DB2 für VM oder zu jedem anderen Server-Produkt, das die DRDA-Architektur unterstützt, hergestellt werden. Sie müssen die folgenden Punkte beachten, damit der Anwendungsrequester unter DB2 für VM den Zugriff auf verteilte Datenbanken zur Verfügung stellen kann:

- Der Anwendungsrequester muss in der Lage sein, RDB\_NAME-Werte entgegenzunehmen und in SNA NETID.LUNAME-Werte umzuwandeln. DB2 für VM verwendet das CMS-Kommunikationsverzeichnis, um die RDB\_NAME-Werte und ihre zugehörigen Netzwerkparameter zu katalogisieren. Mit Hilfe des Kommunikationsverzeichnisses kann der Anwendungsrequester beim Absetzen von Anforderungen für verteilte Datenbanken die erforderlichen SNA-Informationen an VTAM übermitteln.

Für viele Verarbeitungsprozesse in einer verteilten Datenbankumgebung ist der Austausch von Nachrichten mit anderen Netzwerkstandorten erforderlich. Für die korrekte Durchführung dieses Prozesses sind die folgenden Schritte erforderlich:

1. Definieren Sie den Anwendungsrequester für das lokale System.
2. Definieren Sie ferne Systeme für den Anwendungsrequester.
3. Bereiten Sie den Anwendungsrequester oder Anwendungsserver für die DRDA-Kommunikation vor.

#### Zugehörige Konzepte:

- „DB2 für VM“ auf Seite 82
- „Sicherheitsüberlegungen für Anwendungsrequester (VM)“ auf Seite 124

#### Zugehörige Tasks:

- „Definieren des Anwendungsrequesters für das lokale System (VM)“ auf Seite 40
- „Definieren von fernen Systemen für den Anwendungsrequester (VM)“ auf Seite 41
- „Vorbereiten des Anwendungsrequesters oder Anwendungsservers für die DRDA-Kommunikation (VM)“ auf Seite 43
- „Definieren von DB2 als Anwendungsserver (VM)“ auf Seite 67

## Tasks für die Einrichtung

### Definieren des Anwendungsrequesters für das lokale System (VM)

Das Definieren des Anwendungsrequesters unter DB2 für VM für das lokale System ist einer der Arbeitsschritte für die Einrichtung von DB2 für VM als Anwendungsrequester. Der Anwendungsrequester unter DB2 für VM und der Anwendungsserver unter DB2 für VM sind voneinander unabhängig. Der Anwendungsrequester unter DB2 für VM leitet Verbindungsanforderungen direkt an lokale oder ferne Anwendungsserver weiter. Er definiert sich jedoch nicht selbst als Ziel für eingehende Verbindungsanforderungen. Nur der Anwendungsserver unter DB2 für VM kann eingehende Verbindungsanforderungen annehmen (oder zurückweisen). Daher identifiziert der Anwendungsrequester unter DB2 für VM im Unterschied zu DB2 für OS/390 und z/OS keine eigenen RDB\_NAME-Werte und Transaktionsprogrammnamen.

#### Vorgehensweise:

Definieren Sie den Anwendungsrequester unter DB2 für VM im SNA-Netzwerk wie folgt:

1. Verwenden Sie APPL-Definitionsanweisungen für VTAM, um AVS-Gatewaynamen zu definieren.

Der Anwendungsrequester benötigt definierte Gatewaynamen (z. B. die LU-Namen), damit er abgehende Anforderungen an das Netzwerk weiterleiten kann. In Abb. 5 wird ein Beispiel hierfür dargestellt. Diese Anweisungen befinden sich auf der virtuellen VTAM-Maschine. Beim Starten von VTAM werden die Gateways gegenüber dem Netzwerk identifiziert; sie werden jedoch erst aktiviert, wenn die für die Steuerung zuständige virtuelle AVS-Maschine gestartet wird. Jede virtuelle AVS-Maschine kann auf einem VM-Host mehrere Gateways definieren.

```
          VBUILD TYPE=APPL
*****
*
* Gatewaydefinition für System mit DB2 für VM Toronto      *
*
*****
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
```

Abbildung 5. Beispiel für eine AVS-Gatewaydefinition

2. Aktivieren Sie den Gateway.

Die Gatewayaktivierung wird von der virtuellen AVS-Maschine aus durchgeführt, die auf dem selben Host wie der Anwendungsrequester unter DB2 für VM (oder auf einem anderen Host im selben TSAF-Verbund) ausgeführt wird. Fügen Sie einen Befehl AGW ACTIVATE GATEWAY GLOBAL in das Profil der AVS-Maschine ein oder setzen Sie diesen Befehl interaktiv über die Konsole der AVS-Maschine ab, damit der Gateway bei jedem Start der AVS-Maschine aktiviert wird.

3. Verwenden Sie den Befehl AGW CNOS, um die Anzahl der Sitzungen zwischen dem Gateway und jeder seiner Partner-LUs zu vereinbaren.

Stellen Sie sicher, dass der Wert für MAXCONN im Benutzerverzeichnis der AVS-Gatewaymaschine groß genug ist, um die Gesamtzahl der erforderlichen Sitzungen zu unterstützen.

Setzen Sie den Befehl AGW DEACTIVE GATEWAY auf der virtuellen AVS-Maschine ab, um den Gateway zu inaktivieren. Die Gatewaydefinition bleibt erhalten. Der Gateway kann mit dem Befehl AGW ACTIVATE GATEWAY GLOBAL jederzeit erneut aktiviert werden.

4. Stellen Sie sicher, dass die VTAM-NETID während der Installation für das Datenbankverwaltungssystem von DB2 für VM definiert wird.

Die NETID für den Host, auf dem sich der Anwendungsrequester befindet (oder für andere Hosts im selben TSAF-Verbund), wird von VTAM bereitgestellt, sobald die Anforderung in das Netzwerk gelangt. Die NETID wird in der CMS-Datei SNA NETID gespeichert und befindet sich auf der Produktionsplatte von DB2 für VM, auf die der Anwendungsrequester zugreift. Der Anwendungsrequester verwendet diese NETID zum Generieren der LUWID, die bei jedem Datenaustausch mit übertragen wird.

#### Zugehörige Tasks:

- „Definieren von fernen Systemen für den Anwendungsrequester (VM)“ auf Seite 41
- „Vorbereiten des Anwendungsrequesters oder Anwendungsservers für die DRDA-Kommunikation (VM)“ auf Seite 43

## Definieren von fernen Systemen für den Anwendungsrequester (VM)

Das Definieren von fernen Systemen für den Anwendungsrequester ist einer der Arbeitsschritte für die Einrichtung von DB2 für VM als Anwendungsrequester. Sie müssen die fernen Systeme definieren, indem Sie die LU-Namen registrieren, die VTAM das Suchen der gewünschten Netzwerkzieladresse ermöglichen. Beim Starten identifiziert AVS die globalen Gatewaynamen (LU-Namen), die zum Weiterleiten von SQL-Anforderungen über das Netzwerk an VTAM zur Verfügung stehen. Ein Gatewayname muss innerhalb der Gruppe von LU-Namen, die vom lokalen VTAM-System erkannt werden, eindeutig sein, damit eingehende und abgehende Anforderungen an den richtigen LU-Namen weitergeleitet werden. Dies ist das beste Verfahren, um die Eindeutigkeit von Gatewaynamen im Benutzernetzwerk sicherzustellen. Außerdem vereinfacht es den Definitionsprozess für VTAM-Ressourcen.

Wenn eine Anwendung unter DB2 für VM Daten von einem fernen System anfordert, sucht DB2 für VM im Kommunikationsverzeichnis von CMS nach den folgenden Informationen, die sich auf das ferne System beziehen:

- Gatewayname (Name der lokalen LU)
- Name der fernen LU

- Name des fernen Transaktionsprogramms (TPN)
- Erforderliche Dialogsicherheitsstufe für den Anwendungsserver
- Benutzer-ID zum Identifizieren des Anwendungsrequesters auf dem Anwendungsserver
- Kennwort, das den Anwendungsrequester zum Zugriff auf den Anwendungsserver berechtigt
- Modusname, der die Sitzungskenndaten für die Verbindung mit dem Anwendungsserver beschreibt
- RDB\_NAME

### Vorgehensweise:

Das CMS Communications Directory ist eine CMS-Datei mit dem Dateityp NAMES, die von einem Systemadministrator für DB2 für VM erstellt und verwaltet wird.

Als Administrator können Sie diese Datei mit XEDIT erstellen und die gewünschten Einträge zum Identifizieren aller potenziellen DRDA-Partner hinzufügen. Jeder Verzeichniseintrag besteht aus einer Reihe von Kennungen mit den zugeordneten Werten. In Abb. 6 wird ein Beispieleintrag dargestellt. Beim Ausführen eines Suchvorgangs wird der Suchbegriff mit dem Wert der Kennung :dbname jedes Eintrags der Datei verglichen, bis eine Übereinstimmung gefunden oder das Ende der Datei erreicht wird. Im Beispiel in Abb. 6 möchte der Verkaufsmanager in Toronto einen monatlichen Verkaufsbericht für die Geschäftsstelle in Montreal durch Fernzugriff auf die Datenbank MONTREAL\_SALES erstellen.

```

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

```

Abbildung 6. Beispieleintrag in einem CMS Communications Directory

Die Kennung :tpn identifiziert den Namen des Transaktionsprogramms, durch das der Anwendungsserver aktiviert wird. Der erste Teil der Kennung :luname gibt den AVS-Gateway (die lokale LU) an, über den auf das SNA-Netzwerk zugegriffen wird. Der zweite Teil gibt den Namen der fernen LU an. Die Kennung :modename gibt den VTAM-Modus an, der die Kenndaten der zwischen den lokalen und fernen LUs zugeordneten Sitzungen definiert. Beispiele für diese Kenndaten sind die Größe der Anforderungseinheit (Request Unit, RU), die Nachrichtendosierung und die Serviceklasse (Class of Service, COS). Die Kennung :security gibt die Sicherheitsstufe an, die für den Dialog zwischen Anwendungsrequester und Anwendungsserver verwendet werden soll.

Das CMS Communications Directory befindet sich auf einem öffentlichen Systemdatenträger, auf den alle Anwendungsrequester in einem bestimmten VM-System zugreifen können. Jedes Programm oder Produkt, das Fernzugriff über VTAM benötigt, kann das CMS Communications Directory verwenden.

Sie können auf zwei Ebenen des CMS Communications Directory zugreifen: die Systemebene und die Benutzerebene. Sie können beispielsweise auf Systemebene ein Verzeichnis auf einem öffentlichen Systemdatenträger erstellen, auf das alle Anwendungsrequester in einem bestimmten VM-System zugreifen können. Außerdem können Sie auf Benutzerebene ein eigenes Verzeichnis erstellen, um vorhandene Einträge zu überschreiben oder neue Einträge hinzuzufügen, die in dem Verzeichnis auf Systemebene nicht enthalten sind. Das Verzeichnis auf Benutzerebene wird zuerst durchsucht. Bleibt die Suche erfolglos, wird anschließend das Verzeichnis auf Systemebene durchsucht. Das Verzeichnis auf Systemebene ist eine Erweiterung des Verzeichnisses auf Benutzerebene. Es wird nur durchsucht, wenn die gesuchten Werte im Verzeichnis auf Benutzerebene nicht gefunden werden.

Jedes dieser Verzeichnisse wird gegenüber der Anwendung identifiziert und durch den CMS-Befehl SET COMDIR aktiviert. Sie können beispielsweise mit der folgenden Befehlsfolge sowohl das Verzeichnis auf Systemebene als auch das Verzeichnis auf Benutzerebene (auf den Miniplatten S bzw. A) identifizieren, jedoch nur das Verzeichnis auf Systemebene für Suchvorgänge aktivieren:

```
SET COMDIR FILE SYSTEM SCOMDIR NAMES S
```

```
SET COMDIR FILE USER UCOMDIR NAMES A
```

```
SET COMDIR OFF USER
```

#### **Zugehörige Tasks:**

- „Definieren des Anwendungsrequesters für das lokale System (VM)“ auf Seite 40
- „Vorbereiten des Anwendungsrequesters oder Anwendungsservers für die DRDA-Kommunikation (VM)“ auf Seite 43

## **Vorbereiten des Anwendungsrequesters oder Anwendungsservers für die DRDA-Kommunikation (VM)**

Das Vorbereiten des Anwendungsrequesters oder Anwendungsservers unter DB2 für VM ist einer der Arbeitsschritte für die Einrichtung von DB2 für VM als Anwendungsrequester oder Anwendungsserver. Für den Anwendungsrequester oder Anwendungsserver unter DB2 für VM ist möglicherweise keine DRDA-Unterstützung installiert.

#### **Vorgehensweise:**

Führen Sie die folgenden Schritte aus, um den Anwendungsrequester oder Anwendungsserver unter DB2 für VM für die DRDA-Kommunikation vorzubereiten:

1. Verwenden Sie die ausführbare Datei ARISDBMA wie folgt, um die DRDA-Unterstützung zu installieren:
  - Verwenden Sie "ARISDBMA DRDA(ARAS=Y)", wenn Sie die Unterstützung für den Requester und den Server installieren.
  - Verwenden Sie "ARISDBMA DRDA(AR=Y)", wenn Sie die Unterstützung lediglich für den Requester installieren.
  - Verwenden Sie "ARISDBMA DRDA(AS=Y)", wenn Sie die Unterstützung lediglich für den Server installieren.
2. Erstellen Sie ARISQLLD LOADLIB für DB2 für VM erneut.

Weitere Informationen finden Sie im Abschnitt "Using a DRDA Environment" im Handbuch *DB2 Server for VM System Administration*.



---

### **Teil 3. Einrichten von Host- oder iSeries-Anwendungsservern**



---

## Kapitel 6. Einrichten von OS/390- und z/OS-Anwendungsservern

---

### Definieren von DB2 als Anwendungsserver (OS/390 und z/OS)

Die Unterstützung für Anwendungsserver in DB2 für OS/390 und z/OS ermöglicht es, DB2 als Server für DRDA-Anwendungsrequester einzusetzen.

#### Vorgehensweise:

Führen Sie die folgenden Schritte aus, um DB2 für OS/390 und z/OS als Anwendungsserver zu definieren:

1. Definieren Sie den Anwendungsserver für das lokale SNA-Subsystem.
2. Definieren Sie den Anwendungsserver für das lokale TCP/IP-Subsystem.

#### Zugehörige Konzepte:

- „Datendarstellung (OS/390 und z/OS)“ auf Seite 129
- „DB2 für OS/390 und z/OS“ auf Seite 73
- „Sicherheitsüberlegungen für Anwendungsserver (OS/390 und z/OS)“ auf Seite 99

#### Zugehörige Tasks:

- „Definieren des Anwendungsservers für das lokale SNA-Subsystem (OS/390 und z/OS)“ auf Seite 47
- „Definieren des Anwendungsservers für das lokale TCP/IP-Subsystem (OS/390 und z/OS)“ auf Seite 49
- „Definieren von DB2 als Anwendungsrequester (OS/390 und z/OS)“ auf Seite 25

---

### Tasks für die Einrichtung

#### Definieren des Anwendungsservers für das lokale SNA-Subsystem (OS/390 und z/OS)

Damit der Anwendungsserver Anforderungen für verteilte Datenbanken empfangen kann, muss er für den lokalen Kommunikationsmanager definiert sein und über einen eindeutigen RDB\_NAME-Wert verfügen. Die folgenden Erläuterungen beziehen sich auf SNA-Verbindungen.

#### Vorgehensweise:

Gehen Sie wie folgt vor, um den Anwendungsserver für das SNA-Subsystem zu definieren:

1. Wählen Sie den vom DB2 UDB-Anwendungsserver auf dem Host zu verwendenden LU-Namen und RDB\_NAME-Wert aus. Der für DB2 UDB auf dem Host gewählte RDB\_NAME-Wert muss allen Endbenutzern und Anwendungsrequestern bereitgestellt werden, für die eine Verbindung zum Anwendungsserver erforderlich ist.

2. Registrieren Sie den Wert für NETID.LUNAME für den DB2 UDB-Anwendungsserver auf dem Host bei allen Anwendungsrequestern, die Zugriff erfordern, damit der Anwendungsrequester SNA-Anforderungen an den DB2 UDB-Server auf dem Host weiterleiten kann. Dies gilt auch für Fälle, in denen der Anwendungsrequester dynamische Netzwerkweiterleitung ausführen kann, weil der Anwendungsrequester den Wert für NETID.LUNAME kennen muss, bevor dynamische Netzwerkweiterleitung verwendet werden kann.
3. Stellen Sie den Standard-DRDA-TPN (X'07F6C4C2') für die einzelnen Anwendungsrequester bereit, da DB2 UDB auf dem Host diesen Wert automatisch verwendet.
4. Erstellen Sie für jeden von einem Anwendungsrequester angeforderten Modusnamen einen Eintrag in der VTAM-Modustabelle. Diese Einträge beschreiben die RU-Größe, die Größe des Nachrichtendosierungsfensters und die Serviceklasse für die einzelnen Modusnamen.
5. Definieren Sie Sitzungsbegrenzungen für die Anwendungsrequester, die eine Verbindung zu dem Anwendungsserver unter DB2 für OS/390 und z/OS herstellen. Die VTAM-Anweisung APPL definiert Standardwerte für die Sitzungsbegrenzungen aller Partnersysteme. Verwenden Sie zum Definieren eindeutiger Standardwerte für einen bestimmten Partner die Tabelle SYSIBM.LUMODES der Kommunikationsdatenbank (CDB).
6. Erstellen Sie Einträge in der CDB von DB2 UDB auf dem Host, mit denen identifiziert wird, für welche Anwendungsrequester die Verbindung zum DB2 UDB-Anwendungsserver auf dem Host zugelassen werden soll. Zum Definieren der CDB-Einträge für die Anwendungsrequester im Netzwerk stehen die folgenden beiden grundlegenden Vorgehensweisen zur Verfügung:
  - a. Sie können eine Zeile in die Tabelle SYSIBM.LUNAMES einfügen, die die Standardwerte für eine in der Kommunikationsdatenbank nicht explizit beschriebene LU bereitstellt (die Standardzeile enthält in der Spalte LUNAME Leerzeichen). Diese Vorgehensweise ermöglicht das Definieren spezifischer Attribute für einige der LUs in Ihrem Netzwerk und gleichzeitig das Bereitstellen von Standardwerten für alle anderen LUs.

Beispielsweise können Sie dem System DALLAS (einem weiteren DB2 UDB-System auf dem Host) die Berechtigung erteilen, bereits überprüfte Anforderungen für verteilte Datenbanken zu senden (LU 6.2 SECURITY=SAME); von Systemen mit Datenbankmanagern hingegen das Senden von Kennwörtern anfordern. Außerdem ist es unter Umständen günstiger, in der Kommunikationsdatenbank nicht für alle Systeme mit Datenbankmanagern Einträge vorzunehmen, vor allem wenn es sich um viele Systeme handelt. In Abb. 7 wird dargestellt, wie die Kommunikationsdatenbank zur Angabe von SECURITY=SAME für das System DALLAS und von SECURITY=PGM für alle anderen Requester verwendet werden kann.

```

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', ' ');

```

Abbildung 7. Festlegen von Standardwerten für Anwendungsrequester-Verbindungen (SNA)

- b. Mit der Kommunikationsdatenbank (CDB) können Sie Berechtigungen für die einzelnen Anwendungsrequester im Netzwerk individuell erteilen.

Konfigurieren Sie dazu die Kommunikationsdatenbank auf eine der folgenden Arten:

- Stellen Sie sicher, dass die Tabelle SYSIBM.LUNAMES keine Standardzeile enthält. Wenn die Standardzeile (die Zeile mit einem leeren LU-Namen) fehlt, ist für DB2 UDB auf dem Host erforderlich, dass für jeden Anwendungsrequester, der eine Verbindungsherstellung versucht, eine Zeile mit dem LU-Namen in die Tabelle SYSIBM.LUNAMES aufgenommen wird. Wenn in der Kommunikationsdatenbank keine übereinstimmende Zeile gefunden wird, wird dem Anwendungsrequester der Zugriff verweigert.
- Tragen Sie in der Tabelle SYSIBM.LUNAMES eine Standardzeile ein, die angibt, dass eine Herkunftsüberprüfung erforderlich ist (Spalte USERNAMES auf 'I' oder 'B' gesetzt). Hierdurch beschränkt DB2 UDB auf dem Host den Zugriff auf Anwendungsrequester und Endbenutzer, die in der Tabelle SYSIBM.USERNAMES identifiziert sind. Diese Vorgehensweise empfiehlt sich, wenn Ihre Regeln für die Umsetzung für Namen eine Zeile mit einem leeren LU-Namen in der Tabelle SYSIBM.LUNAMES erfordern, DB2 für OS/390 und z/OS diese Zeile jedoch nicht zum Erteilen des unbeschränkten Zugriffs auf den DB2 UDB-Anwendungsserver auf dem Host verwenden soll.

In Abb. 8 enthält keine Zeile in der Spalte LUNAME Leerzeichen, d. h. DB2 UDB auf dem Host verweigert allen LUs außer LUDALLAS bzw. LUNYC den Zugriff.

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

Abbildung 8. Angeben individueller Anwendungsrequester-Verbindungen (SNA)

#### Zugehörige Tasks:

- „Definieren des Anwendungsservers für das lokale TCP/IP-Subsystem (OS/390 und z/OS)“ auf Seite 49

## Definieren des Anwendungsservers für das lokale TCP/IP-Subsystem (OS/390 und z/OS)

Damit der Anwendungsserver Anforderungen für verteilte Datenbanken über TCP/IP-Verbindungen empfangen kann, muss er für das lokale TCP/IP-Subsystem definiert sein und über einen eindeutigen RDB\_NAME-Wert verfügen. Zudem muss der BSDS (Bootstrap Dataset) von DB2 für OS/390 und z/OS die erforderlichen Parameter enthalten, und Sie müssen unter Umständen die Kommunikationsdatenbank von DB2 für OS/390 und z/OS aktualisieren.

Aktualisierungen der Kommunikationsdatenbank sind nicht erforderlich, wenn Sie die TCP/IP-Datenbankverbindungen nur für eingehende Anforderungen verwenden; wenn DB2 für OS/390 und z/OS nur als TCP/IP-Server verwendet werden soll, müssen Sie daher keine Werte in der Kommunikationsdatenbank eintragen. Statt dessen können die Standardwerte verwendet werden. Es folgt ein einfaches Beispiel für die Aktualisierung der Tabelle SYSIBM.IPNAMES.

**Vorgehensweise:**

Wenn Sie Anforderungen für Datenbankverbindungen für eingehende Anforderungen für TCP/IP-Knoten zulassen wollen, können Sie einen SQL-Befehl wie den folgenden verwenden, um diese Tabelle zu aktualisieren:

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

Informationen zum Konfigurieren von TCP/IP auf dem Anwendungsserver finden Sie im Handbuch *DB2 for OS/390 Installation Guide*.

**Zugehörige Tasks:**

- „Definieren des Anwendungsservers für das lokale SNA-Subsystem (OS/390 und z/OS)“ auf Seite 47

---

## Kapitel 7. Einrichten von AS/400-Anwendungsservern (SNA)

---

### Definieren von DB2 als Anwendungsserver – SNA (iSeries)

Die Anwendungsserver-Unterstützung des iSeries-Systems ermöglicht die Verwendung des iSeries-Systems als Server für DRDA-Anwendungsrequester. Der Anwendungsrequester, der mit einem Anwendungsserver unter DB2 Universal Database (UDB) für iSeries verbunden ist, kann ein beliebiger Client sein, der DRDA-Protokolle unterstützt.

Der Anwendungsrequester kann auf Tabellen zugreifen, die lokal auf dem Anwendungsserver unter DB2 UDB für iSeries gespeichert sind. Damit SQL-Anweisungen ausgeführt werden können, muss der Anwendungsrequester zuvor ein Paket auf dem Anwendungsserver unter DB2 UDB für iSeries erstellen. Der Anwendungsserver unter DB2 UDB für iSeries verwendet das Paket mit den SQL-Anweisungen der Anwendung bei der Programmausführung.

#### **Vorgehensweise:**

Zur Verarbeitung von Anforderungen für verteilte Datenbanken auf dem iSeries-Anwendungsserver müssen Sie die Anwendungsserverdatenbank im RDB-Verzeichnis benennen. Für die SNA-Kommunikation müssen Sie das Anwendungsserversystem definieren und die Größe und Nachrichtendosierung für Anforderungs- und Antworteinheiten festlegen.

#### **Benennen der Anwendungsserverdatenbank:**

Das Benennen der Anwendungsserverdatenbank (am Standort des Anwendungsservers) erfolgt auf die gleiche Weise wie das Identifizieren der Anwendungsrequesterdatenbank (am Standort des Anwendungsrequesters). Verwenden Sie dazu den Befehl zum Hinzufügen eines Eintrags im Verzeichnis relationaler Datenbanken (ADDRDBDIRE) und geben Sie als fernen Standort \*LOCAL an.

#### **Definieren des Anwendungsservers im Netzwerk:**

Beim Zugriff über SNA ist der Vorgang zum Definieren des Anwendungsservers im Netzwerk identisch mit dem Vorgang zum Definieren des Anwendungsrequesters im Netzwerk. Sie müssen Leitungs-, Controller-, Einheiten- und Modusbeschreibungen erstellen, um sowohl den Anwendungsserver als auch den Anwendungsrequester, der die Anforderungen sendet, zu definieren.

Als Transaktionsprogrammname zum Starten einer iSeries-Anwendungsserverdatenbank wird der DRDA-Standardwert X'07F6C4C2' verwendet. Dieser Transaktionsprogrammname ist innerhalb des iSeries-Systems zum Starten des Anwendungsservers definiert. Wenn TCP/IP von DB2 UDB für iSeries unterstützt wird, ist der entsprechende Parameter für TCP/IP-Verbindungen der Port. DB2 UDB für iSeries verwendet immer den standardmäßigen DRDA-Port 446 als Server.

### **Festlegen von RU-Größe und Nachrichtendosierung:**

Die Netzwerkdefinitionen müssen überprüft werden, um festzustellen, ob das Netzwerk mit verteilten Datenbanken Auswirkungen auf das vorhandene Netzwerk hat. Dabei gelten für Anwendungsserver und Anwendungsrequester die selben Überlegungen.

### **Zugehörige Konzepte:**

- „Sicherheitsüberlegungen für Anwendungsserver (iSeries)“ auf Seite 105
- „DB2 UDB für iSeries“ auf Seite 81

### **Zugehörige Tasks:**

- „Konfigurieren von TCP/IP auf dem DB2 Connect-Server“ auf Seite 4
- „Definieren von DB2 als Anwendungsrequester – SNA (iSeries)“ auf Seite 33

---

## Kapitel 8. Einrichten von AS/400-Anwendungsservern (TCP/IP)

---

### Herstellen einer Verbindung zu DB2 UDB über TCP/IP (iSeries)

In diesem Abschnitt sind die im Handbuch *DB2 for AS/400 Distributed Database Programming* enthaltenen Informationen zusammengefasst. In diesem Handbuch wird beschrieben, wie DB2<sup>®</sup> UDB für iSeries mit einer der folgenden Konfigurationen eingerichtet wird:

- Als DRDA<sup>®</sup>-Anwendungsrequester, der abgehende TCP/IP-Kommunikation verwendet
- Als DRDA-Anwendungsserver, der eingehende TCP/IP-Kommunikation verwendet

Die Prinzipien entsprechen denjenigen, die in den Abschnitten "Definieren von DB2 als Anwendungsrequester – SNA (iSeries)" und "Definieren von DB2 als Anwendungsserver – SNA (iSeries)" beschrieben sind. Die Schritte zur Konfiguration der Kommunikation sind jedoch viel einfacher.

#### Anmerkungen:

1. Bei DRDA-Kommunikation über TCP/IP ist die Standardportnummer für Datenbankverbindungen 446.
2. Die Implementierung von DB2 Universal Database für AS/400 Version 4 Release 2 unterstützt die zweiphasige Festschreibung (verteilte Arbeitseinheit) über TCP/IP-Kommunikation nicht.

#### Zusammenfassung der Informationen zu DB2 UDB für iSeries:

Das Handbuch *DB2 for AS/400 Distributed Database Programming* enthält die folgenden Abschnitte, auf die Sie sich beziehen sollten:

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

Außerdem müssen Sie folgende Angaben kennen:

- TCP/IP-Portnummer und Host-Name für den Server und den Requester
- ID für codierten Zeichensatz (CCSID) und Codepage für den Server und den Requester
- Beim Herstellen von Datenbankverbindungen die erforderliche Benutzer-ID und das erforderliche Kennwort

## Überlegungen zum Einrichten des DRDA-TCP/IP-Servers unter DB2 UDB für iSeries:

Durch das Einrichten des DRDA-TCP/IP-Servers unter DB2 UDB für iSeries wird sichergestellt, dass der Server gestartet wurde. Der CL-Befehl zum Starten des DRDA-Servers (auch als DDM-Server bezeichnet) lautet:

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

Zum Starten des DRDA-Servers können Sie den Befehl zum Starten des TCP/IP-Servers (STRTCPSVR) auch ohne Parameter angeben oder \*ALL für den Parameter SERVER angeben. Der DRDA-Server wird nach dem Absetzen des folgenden CL-Befehls beim Start von TCP/IP automatisch gestartet:

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

Sie können prüfen, ob der Server gestartet wurde, indem Sie den folgenden CL-Befehl absetzen:

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

Durch diesen Befehl wird eine Jobliste mit Blätterfunktion angezeigt. Wenn Sie ungefähr eine Seite vorblättern, werden zwei Zeilen mit den folgenden Informationen angezeigt:

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

(Die Zeile QRWTSRVR kommt eventuell mehrfach vor, je nachdem, wie viele vorab gestartete Server-Jobs aktiv sind.)

Das Vorkommen der Zeile QRWTLSTN gibt an, dass der Job, der auf DRDA- und DDM-Verbindungsanforderungen wartet, aktiv ist. Dieser Job teilt dem bzw. den QRWTSRVR-Job(s) Arbeit zu, wenn Verbindungsanforderungen empfangen werden.

Sie können auch prüfen, ob der DRDA-Server gestartet wurde, indem Sie den Befehl STRTCPSVR SERVER(\*DDM) absetzen und auf die Nachricht 'DDM TCP/IP Server ist bereits aktiv' warten.

Der Name des vorab gestarteten Jobs für eine bestimmte Verbindung kann durch das Absetzen eines DSPLOG-Befehls abgerufen werden. Beispiel:

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

Dabei muss die angegebene Zeit vor der Verbindungsherstellung liegen. Durch diesen Befehl wird eine Liste der Systemprotokolleinträge mit Blätterfunktion angezeigt. Suchen Sie nach einem Eintrag, der den Namen des Server-Jobs enthält, z. B.:

```
DDM job 039554/QUSER/QRWTSRVR servicing user SRR on 03/30/01 at 15:57:38.
```

Mit diesem Jobnamen kann das Jobprotokoll der momentan aktiven Jobs durchsucht werden. Darüber hinaus können Sie mit diesem Jobnamen einen Wartungsjob für momentan aktive Jobs zum Zweck der Fehlerbestimmung starten oder Nachrichten des Abfrageoptimierungsprogramms aufrufen. Beispiel eines CL-Befehls zum Starten eines Wartungsjobs unter Verwendung der obigen Informationen:

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

Führen Sie den Befehl STRDBG aus, um für den gewarteten Job den Fehlerbehebungsmodus zu aktivieren:

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

In bestimmten Situationen sichert der DRDA-Server das Jobprotokoll des vorab gestarteten Jobs, bevor der Job erneut gestartet und das Jobprotokoll gelöscht wird. Dazu kommt es, wenn ein schwer wiegender Fehler festgestellt wurde oder wenn das Jobende während der Wartung (mit dem Befehl STRSRVJOB) erreicht wurde.

Setzen Sie den folgenden Befehl ab, um das gesicherte Jobprotokoll nach dem Jobende zu suchen:

```
WRKJOB benutzer-id/QPRTJOB
```

Hierbei ist benutzer-id der Name der Benutzer-ID, unter der die Verbindung hergestellt wurde (im obigen Beispiel SRR).

Hierdurch wird eine Liste mit Jobs, aus der Sie einen Job auswählen können, oder ein Auswahlmenü für einen einzelnen Job angezeigt. Wählen Sie Option 4, 'Mit Spool-Dateien arbeiten' aus, um das gesicherte Jobprotokoll zu suchen. Falls mehrere gespoolte Dateien vorhanden sind, ist dies das Protokoll mit dem Dateinamen QPJOBLOG. Mit Option 5 können Sie die Jobprotokolldatei anzeigen.

Beispiel für die Art von Nachrichten des Abfrageoptimierungsprogramms, die in einem Server-Jobprotokoll auftreten können, wenn der Job im Fehlerbehebungsmodus ausgeführt wurde:

```
CPI4329      Information  00   03/30/01  16:14:57  QQQIMPLE
              QSYS       3911   QSQOPEN   QSYS      09C4
Nachricht . . . : Zugriff nach Eingangsfolge für Datei TBL2 verwendet.
Ursache . . . . : Der Zugriffspfad nach Eingangsfolge wurde verwendet,
                  um Sätze aus Teildatei TBL2 der Datei TBL2 in Bibliothek SR auszuwählen.
                  Handelt es sich bei Datei TBL2 in Bibliothek SR um eine logische Datei,
                  ist Teildatei TBL2 der physischen Datei TBL2 in Bibliothek SR die
                  tatsächliche Datei, aus der Sätze ausgewählt werden. Der Dateiname *N
                  für die Datei zeigt an, dass es sich um eine temporäre Datei handelt.
Fehlerbeseitigung . . . : Die Verwendung eines Zugriffspfads kann die
                  Leistung der Abfrage verbessern, wenn Satzauswahl angegeben ist. Besteht
                  kein Zugriffspfad, empfiehlt es sich, einen Zugriffspfad zu erstellen,
                  dessen links angeordneten Schlüsselfelder mit einem der Felder in der
                  Satzauswahl übereinstimmen. Die Übereinstimmung weiterer Schlüsselfelder
                  im Zugriffspfad mit Feldern in der Satzauswahl führt zu einer höheren
                  Leistung. Normalerweise kann die erzwungene Verwendung eines bestehenden
                  Zugriffspfads erreicht werden, indem eine Sortierung nach Feldern angegeben
                  wird, die mit den links angeordneten Schlüsselfeldern dieses Zugriffspfads
                  übereinstimmen. Weitere Informationen enthält das Handbuch "DB2 for iSeries
                  SQL Programming".
```

Abbildung 9. Beispielnachricht des Abfrageoptimierungsprogramms:

### Überlegungen zum Einrichten des DRDA-TCP/IP-Clients unter DB2 UDB für iSeries:

Der Hauptgrund für den Einsatz von DB2 UDB für iSeries als DRDA-Anwendungsrequester über TCP/IP ist neben den im folgenden Abschnitt dargestellten Sicherheitsüberlegungen das Hinzufügen eines RDB-Verzeichniseintrags für den fernen Anwendungsserver. Dies geschieht auf ähnliche Weise wie im vorherigen Kapitel zur Verwendung der SNA-Kommunikation beschrieben.

Anstelle von APPC-Parametern wie dem fernen LU-Namen und dem Transaktionsprogrammnamen werden jedoch zwei TCP/IP-Parameter verwendet, und zwar der Name des fernen Hosts bzw. die IP-Adresse sowie die Portnummer bzw. der Servicenamen. Das zweite Element des Parameters für den fernen Standort kann als \*SNA (Standardwert) oder als \*IP (Verbindung verwendet TCP/IP) angegeben werden.

### **Sicherheitsüberlegungen zur Verwendung von DRDA über TCP/IP:**

DRDA über eigenständige TCP/IP-Verbindungen verwendet keine OS/400®-Kommunikationssicherheitservices und -konzepte wie Datenübertragungseinheiten, Modi, Standortschutzattribute und Dialogsicherheitsstufen, die der APPC-Kommunikation zugeordnet sind. Daher muss die Sicherheit für TCP/IP anders eingerichtet werden.

Von der aktuellen DB2 UDB für iSeries-Implementierung von DRDA über TCP/IP werden die folgenden beiden Arten von Sicherheitsmechanismen unterstützt:

1. Nur Benutzer-ID
2. Benutzer-ID mit Kennwort

Bei einem Anwendungsserver unter DB2 UDB für iSeries wird als Standard-sicherheitsmodus die Benutzer-ID mit Kennwort verwendet. Bleibt die Installationseinstellung des Systems unverändert, müssen eingehende TCP/IP-Verbindungsanforderungen über ein Kennwort verfügen müssen, das der Benutzer-ID zugeordnet ist, unter der der Serverjob ausgeführt werden soll. Mit dem Befehl CHGDDMTCPA kann angegeben werden, dass das Kennwort nicht erforderlich ist. Nehmen Sie diese Änderung durch Eingabe von CHGDDMTCPA PWDRQD(\*NO) vor. Sie müssen über die Sonderberechtigung \*IOSYSCFG verfügen, um diesen Befehl verwenden zu können.

Für einen Anwendungsrequester unter DB2 UDB für iSeries stehen zwei Methoden zur Verfügung, die verwendet werden können, um bei TCP/IP-Verbindungsanforderungen zusammen mit der Benutzer-ID ein Kennwort zu senden. Fehlen beide Methoden, wird nur die Benutzer-ID verwendet.

Bei der ersten Methode wird das Kennwort unter Verwendung des Formats USER/USING der SQL-Anweisung CONNECT gesendet. Die Syntax lautet wie folgt:

```
CONNECT TO rdbname USER benutzer-id USING 'kennwort'
```

Hierbei stellen die Wörter in Kleinbuchstaben die entsprechenden Verbindungsparameter dar. In einem Programm, das eingebettetes SQL verwendet, können die Werte für die Benutzer-ID und das Kennwort in Hostvariablen enthalten sein.

Bei der anderen Methode zum Bereitstellen eines Kennworts, das beim Anfordern der Verbindung über TCP/IP gesendet werden soll, wird ein Serverberechtigungs-eintrag verwendet. Jedem Benutzerprofil auf dem System ist eine Serverberechtigungsliste zugeordnet. Die Liste ist standardmäßig leer; mit dem Befehl ADDSVRAUTE können jedoch Einträge hinzugefügt werden. Beim Versuch, eine DRDA-Verbindung über TCP/IP herzustellen, durchsucht DB2 UDB für iSeries die Serverberechtigungsliste nach dem Benutzerprofil, unter dem der Clientjob ausgeführt wird.

Wird eine Übereinstimmung zwischen dem RDB-Namen in der Anweisung CONNECT und dem SERVER-Namen in einem Berechtigungseintrag gefunden, wird der zugehörige Parameter USRID des Eintrags als Verbindungsbenutzer-ID verwendet. Falls in dem Eintrag ein Parameter PASSWORD gespeichert ist, wird dieses Kennwort bei der Verbindungsanforderung ebenfalls gesendet.

Damit ein Kennwort mit dem Befehl ADDSVRAUTE gespeichert werden kann, muss der Systemwert QRETSVRSEC auf '1' gesetzt sein. Der Standardwert ist '0'. Geben Sie den folgenden Befehl ein, um die Änderung auszuführen:

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

Die Syntax des Befehls ADDSVRAUTE lautet wie folgt:

```
ADDSVRAUTE USRPRF(benutzerprofil) SERVER(rdbname) USRID(benutzer-id) PASSWORD(kennwort)
```

Der Parameter USRPRF gibt das Benutzerprofil an, unter dem der Anwendungsrequesterjob ausgeführt wird. Der Parameter SERVER gibt den Namen der fernen relationalen Datenbank an, und der Parameter USRID gibt das Benutzerprofil an, unter dem der Serverjob ausgeführt wird. Der Parameter PASSWORD gibt das Kennwort für das Benutzerprofil auf dem Server an.

**Anmerkung:** Es ist sehr wichtig, dass der RDB-Name im Parameter SERVER in Großbuchstaben angegeben wird.

Wird der Parameter USRPRF übergangen, wird er standardmäßig auf das Benutzerprofil gesetzt, unter dem der Befehl ADDSVRAUTE ausgeführt wird. Wird der Parameter USRID übergangen, nimmt er standardmäßig den Wert des Parameters USRPRF an. Wird der Parameter PASSWORD übergangen oder ist der Wert für QRETSVRSEC '0', wird im Eintrag kein Kennwort gespeichert. Wird in diesem Fall versucht, eine Verbindung mit Hilfe des Eintrags herzustellen, wird als Sicherheitsmechanismus nur die Benutzer-ID verwendet.

Mit dem Befehl RMVSVRAUTE kann ein Serverberechtigungseintrag entfernt werden; mit dem Befehl CHGSVRAUTE kann ein solcher Eintrag geändert werden. Eine vollständige Beschreibung dieser Befehle finden Sie im Handbuch *AS/400 Command Reference*.

Ist ein Serverberechtigungseintrag für eine relationale Datenbank (RDB) vorhanden und wird außerdem das Format USER/USING der Anweisung CONNECT verwendet, hat das Format USER/USING der Anweisung CONNECT Vorrang.

#### **Zugehörige Konzepte:**

- „Datendarstellung (iSeries)“ auf Seite 129
- „Sicherheitsüberlegungen für Anwendungsserver (iSeries)“ auf Seite 105
- „Sicherheitsüberlegungen für Anwendungsrequester (iSeries)“ auf Seite 122
- „DB2 UDB für iSeries“ auf Seite 81

#### **Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsserver – SNA (iSeries)“ auf Seite 51
- „Definieren von DB2 als Anwendungsrequester – SNA (iSeries)“ auf Seite 33



---

## Kapitel 9. Einrichten von VSE-Anwendungsservern

---

### Definieren von DB2 als Anwendungsserver (VSE)

Die Anwendungsserver-Unterstützung von DB2 für VSE ermöglicht die Verwendung von DB2 für VSE als Server für DRDA-Anwendungsrequester. Folgende Anwendungsrequester können mit einem Anwendungsserver unter DB2 für VSE verbunden werden:

- Requester unter DB2 für VM
- Requester unter DB2 Universal Database für z/OS und OS/390
- Requester unter DB2
- Requester unter DB2 UDB für iSeries
- Alle Anwendungsrequester der DB2-Produktfamilie (einschließlich DB2 CONNECT) sowie jedes andere Produkt, das die Protokolle für DRDA-Anwendungsrequester unterstützt und eine Verbindung zu einem Anwendungsserver unter DB2 für VSE herstellen kann

#### Vorgehensweise:

Führen Sie die folgenden Schritte aus, um die Netzwerkverbindung zum VSE-Anwendungsserver herzustellen:

1. Richten Sie CICS-LU 6.2-Sitzungen mit den fernen Systemen ein
2. Definieren Sie einen VSE-Anwendungsserver
3. Bereiten Sie den Anwendungsserver unter DB2 für VSE vor und starten Sie ihn

#### Zugehörige Konzepte:

- „Sicherheitsüberlegungen für Anwendungsserver (VSE)“ auf Seite 112
- „DB2 für VSE“ auf Seite 94

#### Zugehörige Tasks:

- „Einrichten von CICS-LU 6.2-Sitzungen (VSE)“ auf Seite 59
- „Definieren eines Anwendungsservers (VSE)“ auf Seite 63
- „Vorbereiten und Starten des DB2-Anwendungsservers (VSE)“ auf Seite 64

#### Zugehörige Referenzen:

- „Prüfliste zum Aktivieren eines DB2-Anwendungsservers (VSE)“ auf Seite 139

---

## Tasks für die Einrichtung

### Einrichten von CICS-LU 6.2-Sitzungen (VSE)

Das Einrichten von CICS-LU 6.2-Sitzungen ist einer der Arbeitsschritte für die Einrichtung von DB2 für VSE als Anwendungsserver. Der Anwendungsserver unter DB2 für VSE kommuniziert über CICS-LU 6.2-Verbindungen mit seinem Anwendungsrequester. Die für diesen Zweck verwendete CICS-Partition muss über LU 6.2-Verbindungen zu den fernen Systemen verfügen, auf denen sich die Anwendungsrequester befinden.

## Vorgehensweise:

Führen Sie die folgenden Schritte aus, um eine CICS LU 6.2-Sitzung einzurichten:

1. Installieren Sie die für ISC (Intersystem Communication) erforderlichen Module.

Sie müssen folgende Module mit Hilfe von SIT oder durch Überschreiben der während der Initialisierung festgelegten Werte in Ihr System aufnehmen:

- Die EXEC-Schnittstellenprogramme (geben Sie EXEC=YES an oder akzeptieren Sie den Standardwert)
- Die systemübergreifenden Kommunikationsprogramme (geben Sie ISC=YES an)
- Das durch DFHSG PROGRAM=TCP generierte Workstation-Steuerprogramm (eine Version mit den Angaben ACCMETH=VTAM, CHNASSY=YES und VTAMDEV=LUTYPE6 ist erforderlich)

2. Installieren Sie Unterstützung für die CICS-Funktion zur Neustartresynchronisation (CICS Restart Resynchronization).

Wenn die CICS-Funktion zur Neustartresynchronisation bei der Installation des CICS-Systems nicht installiert wurde, müssen Sie die folgenden CICS-Tabellen aktualisieren, um die CICS-Funktion zur Neustartresynchronisation (CICS Restart Resynchronization) zu aktivieren:

DFHJCT	Journalsteuertabelle
	Ein Journal für das CICS-Systemprotokoll muss in DFHJCT unter Angabe von JFILEID=SYSTEM in einem Makro DFHJCT TYPE=ENTRY definiert werden.
DFHPCT	Programmsteuerungstabelle
	Geben Sie Folgendes ein, um den DFHPCT-Eintrag für CICS-Neustartresynchronisation zu generieren:
	DFHPCT TYPE=GROUP, FN=RMI
DFHPPT	Verarbeitungsprogrammtabelle
	Geben Sie Folgendes ein, um den DFHPPT-Eintrag für CICS-Neustartresynchronisation zu generieren:
	DFHPPT TYPE=GROUP, FN=RMI
DFHSIT	Systeminitialisierungstabelle
	Das Makro DFHSIT muss den Parameter JCT enthalten. Geben Sie JCT=YES bzw. JCT=(jj<,...>) an. Dabei ist jj der Parameterwert für SUFFIX aus dem Makro DFHJCT TYPE=INITIAL, das die Journaldatei des CICS-Systemprotokolls definiert.

Abbildung 10. Tabellen, die aktualisiert werden müssen, um die CICS-Funktion zur Neustartresynchronisation zu aktivieren

3. Definieren Sie CICS für VTAM für VSE.

Damit LU 6.2-Verbindungen unterstützt werden, muss CICS gegenüber VTAM für VSE als ein VTAM-Anwendungshauptknoten definiert werden. Der in der VTAM-Anweisung APPL codierte Name des Anwendungshauptknotens ist die APPLID für die in SIT durch den Parameter APPLID angegebene CICS-Partition. Dies ist der von VTAM (und deshalb auch von den CICS-

Kommunikationspartnern) zum Identifizieren des CICS-Systems verwendete LU-Name. Weitere Informationen finden Sie in Abb. 11.

```

          VBUILD TYPE=APPL
*****
*
*   LU-Definition für VSE SQL/DS-System in Toronto
*
*****
VSEGATE APPL ACBNAME=VSEGATE,
          AUTH=(ACQ,SPO,VPACE),
          APPC=NO,
          SONSCIP=YES,
          ESA=30
          MODTAB=RDBMODES,
          PARSESS=YES,
          VPACING=0

```

Abbildung 11. VTAM-APPL-Beispieldefinition für CICS

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

ACQ ermöglicht CICS das Anfordern von LU 6.2-Sitzungen.

SPO ermöglicht CICS das Absetzen des Befehls MODIFY vtamname USERVAR.

VPACE ermöglicht die Nachrichtendosierung für die systemübergreifenden Datenflüsse.

**ESA=30**

Diese Option gibt die Anzahl netzwerkadressierbarer Einheiten an, mit denen CICS Sitzungen herstellen kann. Die angegebene Anzahl muss die Gesamtzahl paralleler Sitzungen für dieses CICS-System mit einschließen.

**PARSESS=YES**

Gibt die Unterstützung für LUTYPE6-Parallelsitzungen an.

**SONSCIP=YES**

Gibt die Unterstützung für Sitzungsausfallhinweise (Session Outage Notification, SON) an. SON ermöglicht CICS in bestimmten Fällen, eine fehlgeschlagene Sitzung ohne Eingreifen eines Bedieners wiederherzustellen.

**APPC=NO**

Dies ist erforderlich, damit CICS VTAM-Makros verwenden kann. CICS setzt keine APPCCMD-Makroinstruktionen ab.

**Anmerkung:** SYNCLVL=SYNCPT ist nicht erforderlich, da APPC=NO angegeben ist. CICS verwaltet alle SYNCPT-Aktivitäten auf Synchronisationspunktebene für verteilte Arbeitseinheiten.

4. Definieren Sie Verbindungen zu fernen Systemen mit dem LU 6.2-Protokoll.

a. Definieren Sie alle fernen LUs für CICS.

Definieren Sie alle fernen LUs mit Hilfe des Befehls CEDA DEFINE CONNECTION in RDO (Ressource Definition Online). Gehen Sie hierzu wie folgt vor:

- Geben Sie den fernen LU-Namen im Parameter NETNAME an.
- Geben Sie PROTOCOL=APPC an, um sicherzustellen, dass LU 6.2-Protokolle verwendet werden.

- Geben Sie AUTOCONNECT=YES und INSERVICE=YES an, damit die installierte Verbindung automatisch hergestellt wird und die Sitzungen automatisch angefordert werden.
  - Geben Sie die Sicherheit auf Dialogebene mit dem Parameter ATTACHSEC an. ATTACHSEC=IDENTIFY ist die für DRDA erforderliche minimale Sicherheitsstufe.
  - Geben Sie die Sicherheit auf Sitzungsebene mit dem Parameter BIND-PASSWORD an. Standardmäßig wird keine Sicherheit auf Sitzungsebene verwendet.
- b. Definieren Sie LU 6.2-Sitzungsgruppen im fernen System.

Für jede der oben definierte Verbindungen müssen mit Hilfe des Befehls CEDA DEFINE SESSIONS Gruppen mit Parallelsitzungen für jede Verbindung zur fernen LU definiert werden. Gehen Sie hierzu wie folgt vor:

- Geben Sie den oben definierten Namen der Verbindung im Parameter CONNECTION an.
- Geben Sie den Eintrag für die VTAM-Anmeldemodustabelle im Parameter MODENAME an.
- Geben Sie mit dem Parameter MAXIMUM Folgendes an:
  - Maximale Anzahl der Sitzungen
  - Maximale Anzahl der Sitzungen, die als Konfliktgewinner unterstützt werden sollen

Geben Sie die von der Kommunikationssoftware der DRDA-Anwendungsrequester verwendeten Werte an.

**Anmerkung:** Das Angeben eines höheren Werts für SENDSize und RECEIvesize verbessert möglicherweise die Datenübertragungsgeschwindigkeit, erfordert aber auch mehr virtuellen Speicher im Netzwerk. 4 KB ist die von allen Schichten im SNA-Netzwerk unterstützte Größe. Stellen Sie daher die Größe des Send- und Empfangspuffers beim Konfigurieren des DRDA-Servers auf 4 KB ein. Passen Sie diese Parameter nach der erfolgreichen Herstellung von Verbindungen seitens ferner Benutzer an den optimalen Wert an.

- c. Definieren Sie Benutzer-IDs und Kennwörter für CICS.

Definieren Sie alle Benutzer in der CICS-Anmeldetabelle (DFHSNT). Prüfen Sie die Gültigkeit einer Benutzer-ID durch Ausführen einer CESN-Anmeldung auf einer CICS-Workstation. Die lokale Anmeldung muss erfolgreich verlaufen.

- d. Definieren Sie die Lademodule (Phasen) für CICS mit dem Befehl CEDA DEFINE PROGRAM:

- 1) ARICAXED - AXE-Transaktion
- 2) ARICDIRD - Verzeichnis DBNAME und Suchroutine
- 3) ARICDAXD - Transaktionsroutinen DAXP und DAXT
- 4) ARICDEBD - Verarbeitungsroutine für Unterstützung von CICS TRUE
- 5) ARICDRAD - CICS TRUE selbst
- 6) ARICDR2 - DR2DFLT-Steuerblock

Für jedes dieser Module muss die Option LANGUAGE=ASSEMBLER angegeben werden.

- e. Definieren Sie für jeden vom Anwendungsrequester angegebenen TPN (Transaktionsprogrammnamen) mit dem Befehl CEDA DEFINE TRANSACTION eine Transaktion AXE:

- Geben Sie den TPN mit dem Parameter TRANSACTION an.
- Geben Sie die Phase mit PROGRAM=ARICAXED an.
- Geben Sie einen zweiten hexadezimalen Transaktionsnamen mit dem Parameter XTRANID an.

Definieren Sie zugleich durch Angabe von PROGRAM=ARICDAXD die Transaktionen DAXP und DAXT.

Ausführliche Informationen zum Definieren und Einrichten von CICS-LU 6.2-Verbindungen zu fernen Systemen finden Sie im Handbuch *CICS on Open Systems: Intercommunication Guide*.

#### Zugehörige Tasks:

- „Definieren eines Anwendungsservers (VSE)“ auf Seite 63

## Definieren eines Anwendungsservers (VSE)

Das Definieren eines Anwendungsservers ist einer der Arbeitsschritte für die Einrichtung von DB2 für VSE als Anwendungsserver.

#### Vorgehensweise:

Führen Sie die folgenden Schritte aus, um einen VSE-Anwendungsserver zu definieren:

1. Aktualisieren Sie das Verzeichnis DBNAME von DB2 für VSE.

Fügen Sie dem Verzeichnis DBNAME für jede der oben definierten Transaktionen mit dem Befehl CEDA DEFINE TRANSACTION einen Eintrag hinzu. Nachdem die LU 6.2-Sitzungen eingerichtet sind, kann ein ferner Anwendungsrequester einen Dialog mit dem Anwendungsserver unter DB2 für VSE starten. Dazu wird dem Anwendungsserver ein LU 6.2-Dialog unter Angabe eines TPN (Transaktionsprogrammnamens) zugeordnet. Dieser TPN muss die CICS-Transaktions-ID der Transaktion AXE sein, die für die Weiterleitung von Anforderungen zum oder vom Server unter DB2 für VSE zuständig ist. Der TPN muss sich in demjenigen Verzeichnis DBNAME von DB2 für VSE befinden, das dem Server von DB2 für VSE zugeordnet ist, auf den der Anwendungsrequester zugreifen soll. Der Administrator der Datenbank unter DB2 für VSE ist für das Aktualisieren des Verzeichnisses DBNAME und das Benachrichtigen der fernen Benutzer über die TPN-Serverzuordnung zuständig.

Sowohl der TPN als auch der dazugehörige Servername (der im Verzeichnis DBNAME definierte Datenbankname) müssen für den Anwendungsrequester identifiziert werden:

- Der Anwendungsrequester verwendet den TPN zum Initialisieren der AXE-Router-Transaktion.
  - Der Anwendungsrequester gibt den Server-Namen im einleitenden DRDA-Datenfluss als Zieldatenbanknamen an. Der Server unter DB2 für VSE verwendet diesen Server-Namen, um sicherzustellen, dass der Anwendungsrequester auf den richtigen Server zugreift. Bei einer Abweichung von Server-Namen erhält der Anwendungsrequester keinen Zugriff auf den Server, und der Anwendungsrequester beendet den Dialog.
2. Verwenden Sie die Prozedur ARISBDID zum Erstellen und Assemblieren des Verzeichnisses DBNAME (Member ARISDIRD.A).

Weitere Informationen finden Sie in den Handbüchern *DB2 Server for VSE System Administration* und *DB2 Server for VSE & VM Database Administration*.

**Zugehörige Tasks:**

- „Einrichten von CICS-LU 6.2-Sitzungen (VSE)“ auf Seite 59
- „Vorbereiten und Starten des DB2-Anwendungsservers (VSE)“ auf Seite 64

## Vorbereiten und Starten des DB2-Anwendungsservers (VSE)

Das Vorbereiten und Starten des Anwendungsservers unter DB2 für VSE ist einer der Arbeitsschritte für die Einrichtung von DB2 für VSE als Anwendungsserver.

**Vorgehensweise:**

Gehen Sie wie folgt vor, um den Anwendungsserver unter DB2 für VSE vorzubereiten und zu starten:

1. Die Transaktion AXE verwaltet ein Fehlerprotokoll in Form einer CICS Temporary Storage Queue mit dem Namen ARIAXELG. Dieses Fehlerprotokoll enthält hilfreiche Fehlermeldungen mit Angaben zu Kommunikationsproblemen und abnormalen Beendigungen der DRDA-Sitzungen. Definieren Sie dieses Protokoll mit CICS TST als wiederherstellbar (recoverable).
2. Führen Sie die Prozedur ARIS342D aus, um die Unterstützung für DRDA-Anwendungsserver zu installieren.
3. Setzen Sie (falls erforderlich) die Transaktion DAXP ab, um die Standardwerte für das Kennwort und die Sprache anzugeben, die verwendet werden, wenn die Unterstützung für CICS TRUE für einen bestimmten Server aktiviert ist. Weitere Informationen hierzu finden Sie im Handbuch *DB2 Server for VSE & VM Operation*.
4. Starten Sie DB2 für VM mit den Parametern DBNAME, RMTUSERS und SYNCPNT. Hierbei gilt Folgendes:
  - Der verwendete DBNAME muss im Verzeichnis DBNAME definiert sein.
  - Der Parameter RMTUSERS muss ungleich Null sein.
  - Geben Sie SYNCPNT=Y an, um die Unterstützung für verteilte Arbeitseinheiten zu aktivieren.
5. Allen fernem Benutzern müssen vom Server unter DB2 für VSE unterschiedliche Berechtigungsstufen erteilt worden sein.

**Fehlerbestimmung:**

- Wenn der Anwendungsrequester seine Partner-CICS über einen gültigen TPN (definiert im Verzeichnis DBNAME) erreicht hat, wird eine Transaktion AXE gestartet. Der Auslastungszähler im Programm ARICAXED wird um eins erhöht (Überprüfung durch Ausführen von CEMT I PR(ARICAXED) ).
- Führen Sie eine lokale Anmeldung mit der Transaktion CESN unter Verwendung von Benutzer-ID und Kennwort des fernem Benutzers aus, um sicherzustellen, dass in der CICS-Anmeldetabelle eine ferne Benutzer-ID eingerichtet ist. Die lokale Anmeldung muss erfolgreich verlaufen.
- Wenn der Server unter DB2 für VSE aktiv ist und eine Anwendung zuerst Funktionen auf verteilten DRDA-2-Arbeitseinheiten ausführt, wird Unterstützung für TRUE auf einem Server automatisch aktiviert. Sie werden mit der Nachricht ARI0187I darüber informiert, dass die Unterstützung für TRUE erfolgreich aktiviert wurde. Wird allerdings die Nachricht ARI0190E angezeigt, die auf einen Fehler beim Aktivieren von TRUE hinweist, wurden bereits vorher auf der Konsole Fehlermeldungen angezeigt, die Sie sich noch einmal ansehen sollten.

- Wenn das DRDA-Anwendungsprogramm den Prüfcode X'08063426' oder X'FFFE0101' empfängt, weist dies eventuell darauf hin, dass von CICS keine weiteren Sitzungen zur Verfügung gestellt werden können. Dazu kann es kommen, wenn alle Sitzungen entweder im Gebrauch sind oder aufgelöst werden sollen, UNBIND aber noch nicht beendet wurde. CICS kann keine weiteren Sitzungen zur Verfügung stellen, wenn zu viele gleichzeitig ablaufende Transaktionen mit kurzer Dauer ankommen. Erhöhen Sie in diesem Fall die Anzahl der im Parameter MAXIMUM des Befehls CEDA DEFINE SESSIONS angegebenen Sitzungen, um die Sitzungen zu berücksichtigen, die aufgelöst werden sollen, für die jedoch UNBIND noch nicht beendet wurde.

**Zugehörige Tasks:**

- „Einrichten von CICS-LU 6.2-Sitzungen (VSE)“ auf Seite 59
- „Definieren eines Anwendungsservers (VSE)“ auf Seite 63



---

## Kapitel 10. Einrichten von VM-Anwendungsservern

---

### Definieren von DB2 als Anwendungsserver (VM)

Die Unterstützung für Anwendungsserver in DB2 für VM ermöglicht es, DB2 für VM als Server für DRDA-Anwendungsrequester einzusetzen. Die folgenden Anwendungsrequester können mit einem Anwendungsserver unter DB2 für VM verbunden werden:

- Requester unter DB2 für VM
- Requester unter DB2 Universal Database für z/OS und OS/390
- Requester unter DB2 Universal Database für iSeries
- Requester unter DB2 für AIX
- Jeder Anwendungsrequester der DB2-Produktfamilie, wie beispielsweise DB2 Connect, und jedes andere Produkt, das die Protokolle für DRDA-Anwendungsrequester unterstützt, kann eine Verbindung zu einem Anwendungsserver unter DB2 für VM herstellen

Jedem mit einem Anwendungsserver unter DB2 für VM verbundenen Anwendungsrequester ermöglicht der Anwendungsserver unter DB2 für VM den Zugriff auf Datenobjekte (z. B. Tabellen), die lokal auf dem Anwendungsserver unter DB2 für VM gespeichert sind. Der Anwendungsrequester muss auf dem Anwendungsserver unter DB2 für VM ein Paket erstellen, das die SQL-Anweisungen der Anwendung enthält, bevor die Verbindung hergestellt werden kann.

#### Vorgehensweise:

Führen Sie die folgenden Schritte aus, um verteilte Datenbankanforderungen vom Anwendungsserver unter DB2 für VM zu verarbeiten:

1. Definieren Sie den Anwendungsserver.
2. Bereiten Sie den Anwendungsrequester oder Anwendungsserver unter DB2 für VM vor.

#### Zugehörige Konzepte:

- „Sicherheitsüberlegungen für Anwendungsserver (VM)“ auf Seite 108
- „DB2 für VM“ auf Seite 82
- „Datendarstellung (VM)“ auf Seite 132

#### Zugehörige Tasks:

- „Definieren des Anwendungsservers (VM)“ auf Seite 68
- „Vorbereiten des Anwendungsrequesters oder Anwendungsservers für die DRDA-Kommunikation (VM)“ auf Seite 43
- „Definieren von DB2 als Anwendungsrequester (VM)“ auf Seite 39

---

## Tasks für die Einrichtung

### Definieren des Anwendungsservers (VM)

Das Definieren des Anwendungsservers ist einer der Arbeitsschritte für die Einrichtung von DB2 für VM als Anwendungsserver. Damit der Anwendungsserver Anforderungen für verteilte Datenbanken empfangen kann, müssen Sie ihn für das lokale Kommunikationssystem definieren und ihm einen eindeutigen Wert für RDB\_NAME zuordnen. RDB\_NAME wird in der Prozedur SQLSTART EXEC als Parameter DBNAME angegeben.

#### Vorgehensweise:

Führen Sie die folgenden Schritte aus, um den Anwendungsserver zu definieren:

1. Definieren Sie den DB2 für VM-Anwendungsserver für das SNA-Netzwerk, nachdem Sie den Gatewaynamen und den Wert für RDB\_NAME für den Anwendungsserver unter DB2 für VM ausgewählt haben. Der für DB2 für VM ausgewählte RDB\_NAME muss allen Benutzern (Anwendungsrequestern) mitgeteilt werden, die möglicherweise eine Verbindung zu diesem Anwendungsserver unter DB2 für VM herstellen wollen.

Der Wert für NETID wird gegenüber VTAM als Startparameter definiert, und alle verteilten Anforderungen vom Anwendungsrequester werden korrekt an diese NETID weitergeleitet. Der Anwendungsserver unter DB2 für VM legt die NETID nicht fest.

Der Anwendungsserver unter DB2 für VM legt nicht fest, welches Gateway zum Weiterleiten eingehender verteilter Anforderungen des Anwendungsrequesters verwendet wird. Dies wird stets vom Anwendungsrequester gesteuert. Für einen Anwendungsrequester unter DB2 für VM werden diese Angaben im CMS Communications Directory durch die Kennungen :luname und :tpn festgelegt.

Der Anwendungsrequester muss einen AVS-Gateway auswählen, der mit dem Parameter SYNCLVL=SYNCPT für VTAM definiert wurde, damit der Anwendungsserver unter DB2 für VM verteilte Arbeitseinheiten unterstützen kann. Stellen Sie sicher, dass der AVS-Gateway für die Unterstützung verteilter Arbeitseinheiten definiert wurde.

2. Erstellen Sie auf dem VM-System einen CRR Recovery Server zum Verwalten verteilter Arbeitseinheiten für Anwendungsserver unter DB2 für VM. Führen Sie hierzu die Schritte aus, um die von IBM gelieferten Server und Dateipools nach der Installation zu laden. Zu diesen Schritten gehört das Definieren eines CRR-Servers (VMSERVR) und eines CRR-Dateipools (VMSYSR). Stellen Sie sicher, dass beim Starten des CRR Recovery Servers ein LUNAME angegeben wird, der dem Namen eines AVS-Gateways entspricht, für den SYNCLVL=SYNCPT angegeben wurde.
3. Stellen Sie sicher, dass das Benutzerverzeichnis für die Anwendungsservermaschine eine IUCV-Anweisung \*IDENT enthält. Durch diese Anweisung wird der Server als globale Ressource identifiziert.
4. Erstellen Sie in der VTAM-Modusnamentabelle für jeden Modusnamen, der von einem Anwendungsrequester angefordert wird, einen Eintrag. Diese Einträge beschreiben die Sitzungskenndaten wie RU-Größe, Nachrichtendosierungszähler und Serviceklasse für einen bestimmten Modusnamen.
5. Definieren Sie Sitzungsbegrenzungen für die Anwendungsrequester, die eine Verbindung zu dem Anwendungsserver unter DB2 für VM herstellen. Die VTAM-Anweisung APPL definiert Standardwerte für die Sitzungsbegrenzungen

aller Partnersysteme. Verwenden Sie zum Definieren eindeutiger Standardwerte für einen bestimmten Partner den Befehl AGW CNOS auf der virtuellen AVS-Maschine, die am Standort des Anwendungsservers läuft. (Sitzungsbegrenzungen werden normalerweise vom Anwendungsrequester angefordert.)

Bedenken Sie beim Auswählen der RU-Größe, der Sitzungsbegrenzungen und der Nachrichtendosierungszähler, welche Auswirkungen diese Werte auf den VTAM-Pool IOBUF haben.

### Zuordnen des Servernamens zu einer RESID:

*Ressourcen-ID* (RESID) ist die VM-Bezeichnung für den Transaktionsprogrammnamen. In der VM-Umgebung wird dafür im Allgemeinen ein alphanumerischer Name mit einer Länge von bis zu 8 Byte definiert. In der Regel wird eine RESID definiert, die mit dem Servernamen identisch ist, um die Systemverwaltung zu vereinfachen. In Abb. 12 wird eine Beispieldatei RESID NAMES dargestellt.

Im Abschnitt "Beispieleintrag im Kommunikationsverzeichnis ohne definiertes Kennwort" des Themas *Sicherheitsüberlegungen für Anwendungsrequester* finden Sie den Kommunikationsverzeichniseintrag, in dem dieser Wert für dbname und diese RESID (als TPN) definiert sind. Wenn der Name des Anwendungsservers nicht mit der RESID identisch sein kann, verwendet der Anwendungsserver unter DB2 für VM die Datei RESID NAMES zur Zuordnung der Namen.

```
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
```

Abbildung 12. Beispieldatei RESID NAMES

Diese Zuordnung ist erforderlich, wenn Sie:

- eine RESID verwenden, die sich vom Servernamen unterscheidet
- einen Servernamen verwenden, der länger als 8 Zeichen ist
- eine RESID mit einem 4 Byte langen hexadezimalen Wert verwenden (z. B. den DRDA-Standard-TPN X'07F6C4C2')

Bei der Installation wird standardmäßig der Servername verwendet, der in der Prozedur SQLDBINS EXEC als RESID angegeben ist. Wenn Sie einen Zuordnungseintrag in der Datei RESID NAMES erstellen wollen, geben Sie den Parameter RESID in der Prozedur SQLDBINS an.

Wenn Sie die Datenbank mit SQLSTART DB(servername) starten, fragt DB2 für VM die entsprechende RESID ab und informiert das VM-System darüber, dass diese Ressource von VM gesteuert werden soll. Wird in der Datei RESID NAMES kein Eintrag gefunden, geht DB2 für VM davon aus, dass die RESID mit dem Servernamen identisch ist, und weist VM entsprechend an.

Weitere Informationen zu den Schritten, mit denen die von IBM gelieferten Server und Dateipools nach der Installation geladen werden, finden Sie im Handbuch *VM/ESA Installation Guide*.

Weitere Informationen zum Verwenden einer DRDA-Umgebung finden Sie im Handbuch *DB2 Server for VM System Administration*.

**Zugehörige Konzepte:**

- „Sicherheitsüberlegungen für Anwendungsserver (VM)“ auf Seite 108
- „Datendarstellung (VM)“ auf Seite 132

---

## **Teil 4. Konzepte für Host und iSeries**



---

## Kapitel 11. Konzepte

---

### DB2 für OS/390 und z/OS

DB2<sup>®</sup> Universal Database (UDB) für OS/390<sup>®</sup> und z/OS<sup>™</sup> ist das IBM<sup>®</sup> Verwaltungssystem für relationale Datenbanken für Systeme unter DB2 für OS/390 und z/OS. In Abb. 13 auf Seite 74 wird ein OS/390- oder z/OS-System dargestellt, auf dem ein einzelnes Exemplar von DB2 UDB für OS/390 und z/OS ausgeführt wird. Es ist auch möglich, mehrere Exemplare von DB2 UDB für OS/390 und z/OS auf einem einzelnen System auszuführen. Zur Identifikation der Exemplare von DB2 für OS/390 und z/OS auf einem bestimmten System (bzw. von Exemplaren von DB2 für OS/390 und z/OS innerhalb eines JES-Komplexes) wird jedem DB2-System ein Subsystemname zugeordnet. Hierbei handelt es sich um eine 1 bis 4 Zeichen lange eindeutige Zeichenfolge innerhalb eines JES-Komplexes.

#### Anwendungsrequester:

Die folgenden Anwendungsrequester können mit einem Anwendungsserver unter DB2 für OS/390 und z/OS verbunden werden:

- Requester unter DB2 für OS/390 oder z/OS
- DB2 Connect
- DB2 Universal Database<sup>™</sup> Enterprise Server Edition mit aktivierter Unterstützung für DB2 Connect<sup>™</sup>
- Requester mit DB2 Version 2, der unter AIX, HP-UX, OS/2, Solaris, Windows<sup>®</sup> 3.1, Windows 3.11 für Workgroups, Windows 95 oder Windows NT sowie Macintosh, SCO, SGI oder SINIX ausgeführt werden kann. Distributed Database Connection Services<sup>®</sup> (DDCS) Mehrbenutzer-Gateway Version 2.3, DDCS Einzelplatz-System Version 2.3 und DDCS für Windows Version 2.4 stellen diese Funktion bereit
- Requester unter DB2 UDB für iSeries<sup>™</sup>
- Requester unter DB2 für VM
- Jedes andere Produkt, das die Protokolle für DRDA-Anwendungsrequester unterstützt

#### Anwendungsserver:

Die Anwendungsserver unter DB2 für OS/390 und z/OS unterstützen den Datenbankzugriff wie folgt:

- Der Anwendungsrequester kann auf Tabellen zugreifen, die auf dem Anwendungsserver unter DB2 für OS/390 und z/OS gespeichert sind. Bevor die Anwendung ausgeführt werden kann, muss der Anwendungsrequester auf dem Anwendungsserver unter DB2 für OS/390 und z/OS ein Paket erstellen. Dieses Paket wird vom Anwendungsserver unter DB2 für OS/390 und z/OS verwendet, um die SQL-Anweisungen der Anwendung während der Ausführung zu lokalisieren.
- Der Anwendungsrequester kann den Anwendungsserver unter DB2 für OS/390 und z/OS anweisen, den Zugriff nur für Lesevorgänge zu ermöglichen, wenn die DRDA-Verbindung zwischen Requester und Server den zweiphasigen Festschreibeprozess nicht unterstützt. Beispielsweise würde ein Requester

unter DDCS Version 2 Release 3 mit einer CICS-Front-End-Anwendung den Anwendungsserver unter DB2 für OS/390 und z/OS darüber informieren, dass Aktualisierungen nicht zulässig sind.

- Der Anwendungsrequester kann auch berechtigt werden, mit Hilfe von systemgesteuertem Zugriff auf Tabellen zuzugreifen, die auf anderen Systemen mit DB2 für OS/390 und z/OS im Netzwerk gespeichert sind. Systemgesteuerter Zugriff ermöglicht dem Anwendungsrequester, Verbindungen zu mehreren Datenbanksystemen in einer einzelnen Arbeitseinheit herzustellen.

#### Adressräume von OS/390 und z/OS:

In Abb. 13 ist der Name des Subsystems von DB2 für OS/390 und z/OS *xxxx*. Vier der OS/390- und z/OS-Adressraumnamen wird der Name des Subsystems von DB2 für OS/390 und z/OS vorangestellt. Jeder dieser vier Adressräume hat Anteil an der ordnungsgemäßen Funktionsweise von DB2 für OS/390 und z/OS.

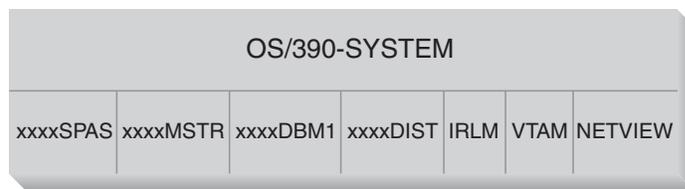


Abbildung 13. Von DB2 für OS/390 und z/OS verwendete OS/390- und z/OS-Adressräume

In Abb. 13 werden die OS/390- und z/OS-Adressräume dargestellt, die an der Verarbeitung für verteilte Datenbanken durch DB2 für OS/390 und z/OS beteiligt sind. Diese Adressräume arbeiten zusammen, um Benutzern von DB2 für OS/390 und z/OS den Zugriff auf lokale relationale Datenbanken und die Kommunikation mit fernen Host- oder iSeries-Systemen zu ermöglichen. Die Verwendung der einzelnen Adressräume wird im Folgenden erklärt:

#### xxxxSPAS

Der Adressraum für gespeicherte DB2-Prozeduren.

#### xxxxMSTR

Der Adressraum des Systemservices von DB2 für OS/390 und z/OS, der für das Starten und Stoppen von DB2 für OS/390 und z/OS sowie die Steuerung des lokalen Zugriffs auf DB2 für OS/390 und z/OS zuständig ist.

#### xxxxDBM1

Der Adressraum des Datenbankservices, der für den Zugriff auf von DB2 für OS/390 und z/OS gesteuerte relationale Datenbanken zuständig ist. Hier wird im Auftrag von SQL-Anwendungsprogrammen die Eingabe in und Ausgabe von Datenbankressourcen ausgeführt.

#### xxxxDIST

Die Komponente von DB2 für OS/390 und z/OS, die Funktionen für verteilte Datenbanken bereitstellt; sie wird auch als *Distributed Data Facility* (DDF) bezeichnet. Wenn eine Anforderung für verteilte Datenbanken empfangen wird, übergibt DDF die Anforderung an *xxxxDBM1*, damit die erforderlichen Datenbank-E/A-Operationen ausgeführt werden können.

**IRLM** Der von DB2 für OS/390 und z/OS verwendete Sperrenmanager (Lock Manager) zum Steuern des Zugriffs auf Datenbankressourcen.

**VTAM<sup>®</sup>**

Funktionen von IBM Communications Server für OS/390 und z/OS (VTAM). DDF kann SNA bzw. TCP/IP verwenden, um die Kommunikation für verteilte Datenbanken im Auftrag von DB2 für OS/390 und z/OS auszuführen. In dieses Diagramm wurde kein Adressraum für TCP/IP aufgenommen.

**NETVIEW**

Das zentrale Alert-Verarbeitungssystem der Netzwerkverwaltung auf OS/390- und z/OS-Systemen. Treten während der Verarbeitung für verteilte Datenbanken Fehler auf, zeichnet DDF Fehlerinformationen (auch als *Alerts* bezeichnet) in der NetView<sup>®</sup>-Datenbank für die Hardwareüberwachung auf. Systemadministratoren können mit NetView die in der Datenbank für die Hardwareüberwachung gespeicherten Fehler überprüfen oder automatische Befehlsprozeduren zur Verfügung stellen, die aufgerufen werden, wenn Alert-Bedingungen aufgezeichnet werden.

NetView kann auch verwendet werden, um die Diagnose von VTAM-Übertragungsfehlern auszuführen.

**Verbindungseinrichtungen für OS/390 und z/OS:**

In Abb. 13 auf Seite 74 werden keine SQL-Anwendungsprogramme dargestellt. Verwendet ein Anwendungsprogramm DB2, um SQL-Anweisungen abzusetzen, muss es auf eine der folgenden Arten eine Verbindung zu DB2 für OS/390 und z/OS herstellen:

**TSO** Für Stapeljobs und an TSO angemeldete Endbenutzer wird über die TSO-Verbindungseinrichtung eine Verbindung zu DB2 für OS/390 und z/OS hergestellt. Mit diesem Verfahren wird die Verbindung von SPUFI-Anwendungen und den meisten QMF<sup>®</sup>-Anwendungen zu DB2 für OS/390 und z/OS hergestellt.

**CICS/ESA<sup>®</sup>**

Wenn eine CICS/ESA-Anwendung SQL-Aufrufe absetzt, verwendet das CICS/ESA-Produkt die CICS-Verbindungsschnittstelle, um SQL-Anforderungen an DB2 für OS/390 und z/OS weiterzuleiten.

**IMS/ESA<sup>®</sup>**

Transaktionen, die unter der Steuerung von IMS/ESA ausgeführt werden, verwenden die IMS<sup>™</sup>-Verbindungsschnittstelle, um SQL-Anweisungen zur Verarbeitung an DB2 für OS/390 und z/OS zu übergeben.

**DDF** DDF (Distributed Data Facility) ist für das Herstellen der Verbindung verteilter Anwendungen zu DB2 für OS/390 und z/OS zuständig.

**CAF** CAF (Call Attachment Facility) ermöglicht benutzerdefinierten Subsystemen die Herstellung einer direkten Verbindung zu DB2 für OS/390 und z/OS.

## Verbindungen verteilter Datenbanken:

DRDA<sup>®</sup> definiert die Funktionsarten des Verwaltungssystems für verteilte Datenbanken. DB2 für OS/390 und z/OS unterstützt ferne Arbeitseinheiten. Durch ferne Arbeitseinheiten kann ein auf einem System ausgeführtes Anwendungsprogramm auf Daten eines fernen Datenbankverwaltungssystems zugreifen. Es verwendet hierzu die vom fernen Datenbankverwaltungssystem bereitgestellten SQL-Anweisungen.

DB2 für OS/390 und z/OS unterstützt auch verteilte Arbeitseinheiten. Durch verteilte Arbeitseinheiten kann ein auf einem System ausgeführtes Anwendungsprogramm auf Daten mehrerer ferner Datenbankverwaltungssysteme zugreifen. Es verwendet hierzu die von den fernen Datenbankverwaltungssystemen bereitgestellten SQL-Anweisungen.

Wie in Abb. 14 auf Seite 77 gezeigt, unterstützt DB2 für OS/390 und z/OS drei Konfigurationen von Verbindungen für verteilte Datenbanken unter Verwendung von zwei Zugriffsmethoden:

[1] *Systemgesteuerter Zugriff* (auch als die Verwendung des *privaten Protokolls von DB2 für OS/390 und z/OS* bezeichnet) ermöglicht einem Requester unter DB2 für OS/390 und z/OS die Verbindung zu einem oder mehreren Servern unter DB2 für OS/390 und z/OS. Die zwischen dem Requester und dem Server unter DB2 für OS/390 und z/OS hergestellte Verbindung hält sich nicht an die in DRDA definierten Protokolle und kann *nur* zum Herstellen von Verbindungen zwischen DB2 für OS/390 und z/OS-Produkten und z/OS und DB2 für OS/390 und z/OS verwendet werden. Diese Art der Verbindung wird durch die Codierung von dreiteiligen Namen oder Aliasnamen in der Anwendung hergestellt.

[2] *Anwendungsgesteuerter Zugriff* ermöglicht einem Requester unter DB2 für OS/390 und z/OS oder unter einem anderen Produkt (wie beispielsweise DB2 Connect) die Verbindung zu einem oder mehreren Anwendungsservern unter DB2 für OS/390 und z/OS oder einem anderen Produkt, wie beispielsweise DB2 Universal Database oder DB2 UDB für iSeries, über DRDA-Protokolle. Die Anzahl der Anwendungsserver, für die jeweils eine Verbindung zum Anwendungsrequester bestehen kann, hängt von der Version von DB2 für OS/390 und z/OS für den Anwendungsrequester ab. Diese Art der Verbindung wird hergestellt, indem SQL-CONNECT-Anweisungen in der Anwendung codiert werden.

[3] Anwendungsgesteuerter und systemgesteuerter Zugriff können gemeinsam verwendet werden, um Verbindungen herzustellen. Sie können eine Verbindung nicht über DRDA und systemgesteuerte Speicherung im gleichen Thread herstellen.

Der Begriff *sekundärer Server* beschreibt Systeme, die für den Anwendungsserver als Server fungieren.

Unterstützen alle Systeme in einer Konfiguration die zweiphasige Festschreibung, werden verteilte Arbeitseinheiten (Lesen und Aktualisieren von auf mehrere Standorte verteilten Daten) unterstützt. Unterstützen nicht alle Systeme die zweiphasige Festschreibung, sind Aktualisierungen innerhalb einer Arbeitseinheit auf einen einzelnen Standort beschränkt, der zweiphasige Festschreibung nicht unterstützt, oder auf die Untergruppe der Standorte, die zweiphasige Festschreibung unterstützen.

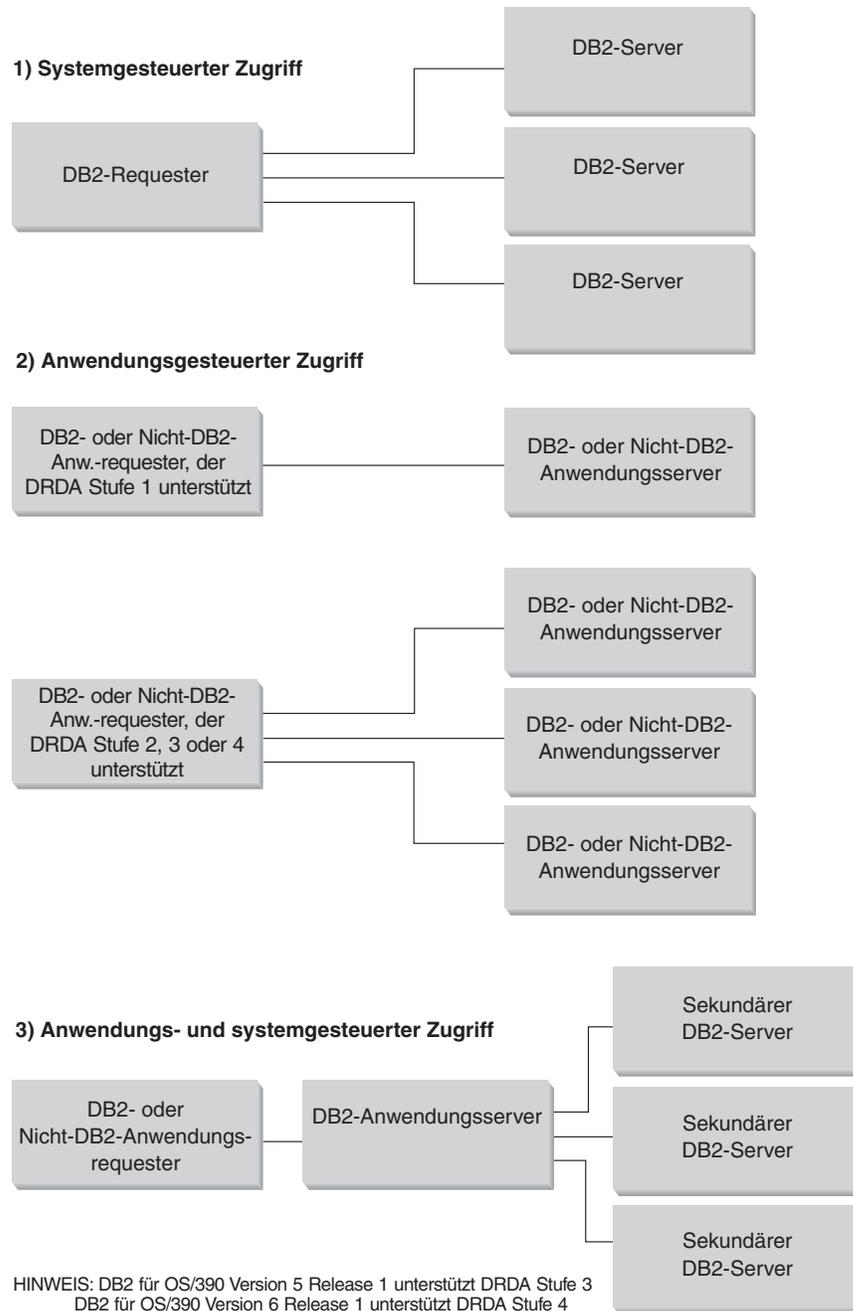


Abbildung 14. Verteilte Verbindungen von DB2 für OS/390 und z/OS

In Tabelle 2 auf Seite 78 werden die verschiedenen Typen der Verbindung von DB2 für OS/390 und z/OS zu verteilten Datenbanken verglichen.

Tabelle 2. Vergleich der Verbindungen von DB2 für OS/390 und z/OS zu verteilten Datenbanken

[1] Systemgesteuerter Zugriff	[2] Anwendungsgesteuerter Zugriff (alle Systeme unterstützen zweiphasige Fest-schreibung)	[3] Anwendungsgesteuerter und system-gesteuerter Zugriff
Alle Partner müssen Systeme mit DB2 für OS/390 und z/OS sein.	Kann Verbindung zwischen zwei DRDA-Systemen herstellen.	Der Anwendungsrequester kann ein beliebiges DRDA-System sein. Server müssen Systeme mit DB2 für OS/390 und z/OS sein.
Kann direkte Verbindung zu vielen Partnern herstellen.	Kann direkte Verbindung zu vielen Partnern herstellen.	Der Anwendungsrequester stellt direkte Verbindungen zu Anwendungsservern her; die Anwendungsserver können direkte Verbindungen zu vielen sekundären Servern unter DB2 für OS/390 und z/OS herstellen.
Jede SQL-Anwendung kann für jeden Server mehrere Dialoge einrichten.	Jede SQL-Anwendung richtet für jeden Server einen Dialog ein.	Die SQL-Anwendung richtet für jeden Server einen Dialog ein. Anwendungsserver unter DB2 für OS/390 und z/OS können für die Anwendung viele Dialoge mit jedem Server herstellen.
Kann sowohl auf lokale als auch auf ferne Ressourcen in einem COMMIT-Bereich zugreifen.	Kann sowohl auf lokale als auch auf ferne Ressourcen in einem COMMIT-Bereich zugreifen.	Anwendungsrequester und Anwendungsserver können auf lokale und ferne Daten zugreifen.
Effektiver bei großen Abfragen und mehreren gleichzeitig ablaufenden Abfragen	Effektiver bei SQL-Anweisungen, die in einem COMMIT-Bereich nicht häufig ausgeführt werden	Verbindungen zwischen Anwendungsrequester und Anwendungsserver verhalten sich wie [2]. Verbindungen zu sekundären Servern verhalten sich wie [1].
Kann statisches oder dynamisches SQL unterstützen; der Server bindet statisches SQL bei der Erstauführung in einem COMMIT-Bereich jedoch dynamisch.	Kann statisches oder dynamisches SQL absetzen.	Anwendungsrequester und Anwendungsserver können statisches oder dynamisches SQL absetzen. Sekundäre Server unterstützen statisches oder dynamisches SQL, binden statisches SQL bei der Erstauführung in einem COMMIT-Bereich jedoch dynamisch.
Auf die SQL-Anweisungen INSERT, DELETE und UPDATE und auf Anweisungen beschränkt, die SELECT unterstützen.	Kann jede Anweisung verwenden, die von dem System, das die Anweisung ausführt, unterstützt wird.	Anwendungsserver unterstützen beliebiges SQL; sekundäre Server unterstützen nur DML-SQL (z. B. CREATE oder ALTER).

### Zusätzliche Sicherheitserweiterungen:

#### Erweiterte Sicherheitscodes

Bis DB2 UDB für OS/390 Version 5.1 konnte es vorkommen, dass Verbindungsanforderungen, die Benutzer-IDs oder Kennwörter angaben, mit SQL30082 Ursachencode 0 fehlschlagen, aber keine andere Nachricht mit Angaben zur Fehlerursache ausgegeben wurde. In DB2 UDB für OS/390 Version 5.1, Version 5.1 wurde eine Erweiterung eingeführt, die Unterstützung für erweiterte Sicherheitscodes zur Verfügung stellt. Durch das Angeben erweiterter Sicherheitscodes werden zusätzliche Diagnoseinformationen, beispielsweise Informationen zu einem abgelaufenen Kennwort zusätzlich zum Ursachencode geliefert.

Um diese Möglichkeiten nutzen zu können, muss der DB2 Universal Database für z/OS und OS/390-Installationsparameter ZPARM für erweiterte Sicherheit auf YES eingestellt werden. Mit der Installationsanzeige DSN6SYSP von DB2 Universal Database für z/OS und OS/390 kann EXTSEC=YES eingestellt werden. Daneben kann auch die DDF-Anzeige 1 (DSNTIPR) verwendet werden. Der Standardwert ist EXTSEC=NO.

Falls das Kennwort nicht mehr gültig ist, wird von Anwendungen für Windows, UNIX und das Web, die mit DB2 Connect arbeiten, die Fehlermeldung SQL01404 empfangen.

#### **Bereits überprüfte TCP/IP-Sicherheit**

Wenn Sie Unterstützung für die Sicherheitsoption AUTHENTICATION=CLIENT von DB2 Universal Database wünschen, geben Sie in der Installationsanzeige DSNTIP4 von DB2 Universal Database für z/OS und OS/390 (DDF-Anzeige 2) mit YES an, dass die TCP/IP-Sicherheit bereits überprüft ist.

#### **Sicherheit für ODBC- und Java™-Anwendungen auf Workstations**

ODBC- und Java-Anwendungen auf Workstations verwenden dynamisches SQL. Dies kann bei einigen Installationen Sicherheitsfragen aufwerfen. DB2 Universal Database für z/OS und OS/390 führt eine neue Bindeoption, DYNAMICRULES(BIND), ein, die die Ausführung von dynamischem SQL unter der Berechtigung des Eigners oder des Binders zulässt.

DB2 Universal Database und DB2 Connect bieten einen neuen CLI/ODBC-Konfigurationsparameter, CURRENTPACKAGESET, in der Konfigurationsdatei DB2CLI.INI. Dieser sollte auf einen Schemanamen eingestellt werden, der die geeigneten Zugriffsrechte hat. Eine SQL-Anweisung SET CURRENT PACKAGESET schema wird automatisch nach jeder Verbindungsherstellung für die Anwendung abgesetzt.

Verwenden Sie den ODBC-Manager, um DB2CLI.INI zu aktualisieren.

#### **Unterstützung für die Änderung des Kennworts**

Gibt eine SQL-Anweisung CONNECT eine Nachricht zurück, die besagt, dass das Kennwort der Benutzer-ID nicht mehr gültig ist, können Sie mit DB2 Connect das Kennwort ändern, ohne sich an TSO anzumelden. Mit Hilfe von DRDA kann DB2 Universal Database für z/OS und OS/390 das Kennwort für Sie ändern.

Der Benutzer muss das alte Kennwort zusammen mit dem neuen Kennwort und dem Prüfkennwort angeben. Wenn die am DB2 Connect Enterprise Edition-Server angegebene Sicherheitseinstufung DCS ist, wird eine Anforderung zum Ändern des Kennworts an den Datenbankserver unter DB2 Universal Database für z/OS und OS/390 gesendet. Wenn die angegebene Sicherheitseinstufung SERVER ist, wird das Kennwort auf dem DB2 Connect-Server geändert.

Ein weiterer Vorteil ist, dass keine separate LU-Definition erforderlich ist.

#### **Zugehörige Konzepte:**

- „Datendarstellung (OS/390 und z/OS)“ auf Seite 129
- „Sicherheitsüberlegungen für Anwendungsrequester (OS/390 und z/OS)“ auf Seite 115
- „Sicherheitsüberlegungen für Anwendungsserver (OS/390 und z/OS)“ auf Seite 99

#### **Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsserver (OS/390 und z/OS)“ auf Seite 47
- „Definieren von DB2 als Anwendungsrequester (OS/390 und z/OS)“ auf Seite 25
- „Festlegen der RU-Größen und der Nachrichtendosierung (OS/390 und z/OS)“ auf Seite 80

---

## Weitere Konzepte

### Definieren der Kommunikation - SNA (OS/390 und z/OS)

VTAM ist der Kommunikationsmanager für OS/390- und z/OS-Systeme. VTAM nimmt LU 6.2-Verben von DB2 für OS/390 und z/OS entgegen und wandelt diese Verben in LU 6.2-Datenströme um, die über das Netzwerk übertragen werden können.

#### Vorgehensweise:

Damit VTAM mit den in der Kommunikationsdatenbank von DB2 für OS/390 und z/OS angegebenen Partneranwendungen kommunizieren kann, müssen Sie VTAM die folgenden Informationen zur Verfügung stellen:

- Die LU-Namen für alle Server.

Wenn DB2 für OS/390 und z/OS mit VTAM kommuniziert, darf DB2 für OS/390 und z/OS nur einen LU-Namen (nicht NETID.LUNAME) an VTAM übergeben, um den gewünschten Zielstandort anzugeben. Dieser LU-Name muss innerhalb der auf dem lokalen VTAM-System bekannten LU-Namengruppe eindeutig sein, damit VTAM die NETID und den LU-Namen aus dem von DB2 für OS/390 und z/OS übergebenen Wert für den LU-Namen ermitteln kann. Wenn LU-Namen im SNA-Netzwerk eines Unternehmens eindeutig sind, vereinfacht dies den VTAM-Ressourcendefinitionsprozess enorm. Dies ist jedoch nicht immer möglich. Sind LU-Namen innerhalb des SNA-Netzwerks nicht eindeutig, müssen Sie die VTAM-LU-Umsetzung für Namen verwenden, um die korrekte NETID.LUNAME-Kombination für einen nicht eindeutigen LU-Namen zu erstellen. Dieser Prozess wird im Abschnitt "Resource Name Translation" des Handbuchs *VTAM Network Implementation Guide* beschrieben.

Platzierung und Syntax der VTAM-Definitionen zum Definieren der fernen LU-Namen hängen stark davon ab, wie das ferne System logisch und physisch mit dem lokalen VTAM-System verbunden ist.

- RU-Größe, Größe des Nachrichtendosierungsfensters und Serviceklasse für jeden Modusnamen. Erstellen Sie in der VTAM-Modustabelle für jeden in der Kommunikationsdatenbank angegebenen Modusnamen einen Eintrag. Sie müssen auch IBMRDB und IBMDB2LM definieren.
- Die VTAM- und RACF-Profile für den LU-Prüfungsalgorithmus, wenn Sie die Partner-LU-Prüfung verwenden wollen.

#### Zugehörige Konzepte:

- „DB2 für OS/390 und z/OS“ auf Seite 73

### Festlegen der RU-Größen und der Nachrichtendosierung (OS/390 und z/OS)

Die in der VTAM-Modustabelle von Ihnen definierten Einträge geben die RU-Größe und die Nachrichtendosierungszähler an. Fehlende oder fehlerhafte Definitionen für diese Werte können sich nachteilig auf alle VTAM-Anwendungen auswirken.

### Vorgehensweise:

Bedenken Sie bei der Wahl der RU-Größen, Sitzungsbegrenzungen und Nachrichtendosierungszähler, welche Auswirkungen diese Werte auf das vorhandene VTAM-Netzwerk haben können. Überprüfen Sie beim Installieren eines neuen verteilten Datenbanksystems die folgenden Punkte:

- Stellen Sie für VTAM-CTC-Verbindungen sicher, dass der Parameterwert für MAXBFRU groß genug ist, um Ihre RU-Größe plus der 29 Byte, die VTAM als SNA-Anforderungs- und Übertragungskopf hinzufügt, zu verarbeiten. MAXBFRU wird in Einheiten von 4 KB gemessen, d. h. der Wert für MAXBFRU muss mindestens 2 betragen, um eine RU-Größe von 4 KB zu unterstützen.
- Stellen Sie für NCP-Verbindungen sicher, dass der Wert für MAXDATA groß genug ist, um Ihre RU-Größe plus 29 Byte zu verarbeiten. Wenn Sie als RU-Größe 4 KB angegeben haben, muss der Wert für MAXDATA mindestens 4125 betragen.

Wenn Sie den NCP-Parameter MAXBFRU angeben, müssen Sie einen Wert auswählen, der für Ihre RU-Größe plus 29 Byte ausreicht. Bei NCP definiert der Parameter MAXBFRU die Anzahl der VTAM-E/A-Puffer für die PIU. Wenn Sie für IOBUF eine Puffergröße von 441 angeben, verarbeitet MAXBFRU=10 die RU-Größe 4 KB korrekt, weil  $10 \cdot 441$  größer ist als  $4096 + 29$ .

- Im Handbuch *DRDA Connectivity Guide* wird beschrieben, wie Sie die Auswirkung der verteilten Datenbank auf den VTAM-IOBUF-Pool abschätzen können. Wenn ein zu großer Anteil der IOBUF-Poolressource belegt ist, hat dies nachteilige Auswirkungen auf die Leistung aller VTAM-Anwendungen.

### Zugehörige Konzepte:

- „DB2 für OS/390 und z/OS“ auf Seite 73

---

## DB2 UDB für iSeries

OS/400 umfasst DB2<sup>®</sup> UDB für iSeries, das IBM<sup>®</sup> Verwaltungssystem für relationale Datenbanken für iSeries<sup>™</sup>-Systeme. In DB2 Universal Database für AS/400 Version 4.2 wurde die Unterstützung für die DRDA<sup>®</sup>-Kommunikation über TCP/IP eingeführt.

Ab Version 2 Release 1 Modifikation 1 des Lizenzprogramms OS/400<sup>®</sup> werden ferne DRDA-Arbeitseinheiten unterstützt, und ab OS/400 Version 3 Release 1 werden verteilte DRDA-Arbeitseinheiten (DUOW) unterstützt. Diese Unterstützung ist Bestandteil des Betriebssystems OS/400. Die Lizenzprogramme Query Manager und SQL Development Kit von DB2 UDB für iSeries sind also für die Verwendung der DRDA-Unterstützung oder zum Ausführen von Programmen mit eingebetteten SQL-Anweisungen nicht erforderlich.

### Zugehörige Konzepte:

- „Datendarstellung (iSeries)“ auf Seite 129
- „Sicherheitsüberlegungen für Anwendungsserver (iSeries)“ auf Seite 105
- „Sicherheitsüberlegungen für Anwendungsrequester (iSeries)“ auf Seite 122

### Zugehörige Tasks:

- „Definieren von DB2 als Anwendungsserver – SNA (iSeries)“ auf Seite 51
- „Definieren von DB2 als Anwendungsrequester – SNA (iSeries)“ auf Seite 33

SQL/DS™ (DB2 für VM) Version 3 Release 5 unterstützt bei VM-Systemen DRDA®-Anwendungsserver für ferne Arbeitseinheiten und Anwendungsrequester.

Jeder Datenbankmanager von DB2® für VM kann mehrere Datenbanken (allerdings immer nur eine einzige Datenbank gleichzeitig) verwalten und wird normalerweise mit dem Namen der Datenbank bezeichnet, die momentan verwaltet wird. Der Name dieser relationalen Datenbank ist innerhalb einer Gruppe miteinander verbundener SNA-Netzwerke eindeutig.

SQL/DS (DB2 für VM) Version 3 Release 5 unterstützt bei VM-Systemen DRDA-Anwendungsserver für ferne Arbeitseinheiten und Anwendungsrequester. SQL/DS (DB2 für VSE) Version 3 Release 5 stellt bei VSE-Systemen DRDA-Anwendungsserver-Unterstützung für ferne Arbeitseinheiten bereit.

Zudem unterstützt DB2 für VSE & VM Version 5 Release 1 sowohl bei VM- als auch VSE-Systemen DRDA-Anwendungsserver für verteilte Arbeitseinheiten. Dieses Kapitel enthält hauptsächlich Informationen zur Verbindung von Systemen mit DB2 für VSE & VM mit andersartigen fernen DRDA-Systemen. Weitere Informationen zum Verbinden zweier Systeme mit DB2 für VSE & VM enthalten die folgenden Handbücher:

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

### **Verarbeitung verteilter Datenbanken - DRDA- und VM-Komponenten:**

Die verschiedenen DRDA- und VM-Komponenten für die Verarbeitung verteilter Datenbanken werden im Folgenden beschrieben. Über diese Komponenten können die Datenbankmanager von DB2 für VM auf lokale relationale Datenbanken zugreifen und mit fernen DRDA-Systemen im SNA-Netzwerk kommunizieren.

**AVS** APPC/VTAM-Unterstützung (AVS) ist eine VM-Komponente, über die VM-Anwendungen auf das SNA-Netzwerk zugreifen können. Sie stellt die Funktionalität für die logische Einheit (Logical Unit, LU) bereit, wie sie durch SNA definiert ist. Eine LU wird in der VM-Umgebung als *Gateway* bezeichnet. AVS wird in einem Gruppensteuerungssystem als eine VTAM®-Anwendung ausgeführt. AVS setzt APPC/VM-Makroaufrufe in APPC/VTAM-Makroaufrufe um und umgekehrt. APPC/VM verwendet AVS zum Weiterleiten und Umsetzen von Datenströmen. Mit AVS können Anforderungen von DB2 für VM zwischen dem lokalen VM-System und fernen SNA-Standorten übertragen werden. AVS muss verwendet werden, wenn Anwendungen oder Datenbanken unter DB2 für VM mit Datenbanken oder Anwendungen kommunizieren, die nicht unter DB2 für VM ausgeführt werden.

Auf der Seite des Anwendungsrequesters muss der Benutzer die Berechtigung zur Herstellung einer Verbindung über einen AVS-Gateway erhalten, bevor die Anforderungen gesendet werden können. Außerdem muss der empfangende AVS-Gateway auf der Seite des Anwendungsservers die entsprechende Berechtigung zum Herstellen einer Verbindung zur Servermaschine unter DB2 für VM erhalten, bevor AVS die Anforderungen des Benutzers weiterleiten kann. Die Berechtigung erfolgt durch Bereitstellen der entsprechenden Anweisung für die IUCV-Verzeichnissteuerung in der Benutzermaschine, der Datenbankmaschine sowie der sendenden und

empfangenden AVS-Maschinen. Ausführliche Informationen hierzu enthält das Handbuch *VM/ESA Connectivity Planning, Administration, and Operation*.

### **APPC/VM**

APPC/VM ist die VM-API auf Assemblerebene, die eine Untergruppe der LU 6.2-Funktionen bereitstellt, wie sie durch SNA definiert werden. Praktisch bedeutet dies, dass APPC/VM die LU 6.2-Verben bereitstellt, die Anwendungen unter DB2 für VM das Herstellen einer Verbindung zu lokalen und fernen Datenbankmanagern und die Verarbeitung in diesen Systemen ermöglichen. Die von APPC/VM unterstützten LU 6.2-Verben sind im Handbuch *VM/ESA CP Programming Services* aufgeführt.

### **Kommunikationsverzeichnis (Communications Directory)**

Das Kommunikationsverzeichnis ist eine CMS-Datei mit dem Dateityp NAMES, die beim Einrichten von APPC-Dialogen zwischen einem lokalen VM-Anwendungsrequester und einem Anwendungsserver eine bestimmte Aufgabe erfüllt. Dieses Verzeichnis stellt die erforderlichen Informationen zur Weiterleitung und Einrichtung eines APPC-Dialogs mit dem Zielserver bereit. Zu diesen Informationen gehören Angaben wie LU-Name, TPN, Sicherheit, Modusname, Benutzer-ID, Kennwort und Datenbankname.

DB2 für VM verwendet die COMDIR-Kennung :dbname, um RDB\_NAME in die entsprechenden Leitwegdaten aufzulösen.

Diese besondere Datei und ihre Funktion bei der Datenübertragung werden im Handbuch *VM/ESA Connectivity Planning, Administration, and Operation* beschrieben.

**CRR** CRR (Coordinated Resource Recovery) ist eine VM-Einrichtung, die das Festschreiben bzw. Zurücksetzen von Aktualisierungen geschützter Ressourcen koordiniert. Verteilte Anwendungsprogramme stellen in Zusammenarbeit mit CRR anhand geschützter Dialoge die Integrität der verteilten Transaktionsressourcen sicher.

### **CRR Recovery Server**

Der CRR Recovery Server ist eine Komponente von CRR und wird auf seiner eigenen virtuellen Maschine ausgeführt. Dieser Server ist für die Ausführung von Funktionen für Synchronisationspunktprotokollierung und Resynchronisation zuständig.

**GCS** Das Gruppensteuerungssystem (GCS, Group Control System) ist eine VM-Komponente mit folgenden Bestandteilen:

- Ein gemeinsam benutztes Segment, das auf einer virtuellen Maschine ausgeführt wird
- Ein Supervisor für virtuelle Maschinen, der mehrere virtuelle Maschinen in einer Gruppe zusammenfasst und ihre Operationen überwacht
- Eine Schnittstelle zwischen folgenden Programmprodukten:
  - Virtual Telecommunications Access Method (VTAM)
  - APPC/VTAM-Unterstützung (AVS)
  - Remote Spooling Communications Subsystem (RSCS)
  - Steuerprogramm (Control Program, CP)

GCS überwacht die Ausführung von VTAM-Anwendungen, wie z. B. AVS in einer VM-Umgebung. Virtuelle Maschinen, die unter der Überwachung von GCS ausgeführt werden, verwenden kein CMS.

### **Ressourcenadapter**

Der Ressourcenadapter ist der Teil der Logik von DB2 für VM, der sich in Ihrer virtuellen Maschine befindet und Ihrer Anwendung ermöglicht, Zugriff auf einen Server unter DB2 für VM anzufordern. Die Funktion für DRDA-Anwendungsrequester ist in den Ressourcenadapter integriert.

**TSAF** TSAF (Transparent Services Access Facility) ist eine VM-Komponente, die Kommunikationsunterstützung zwischen miteinander verbundenen VM-Systemen zur Verfügung stellt. Bis zu acht VM-Systeme können zu einem TSAF-Verbund zusammengeschlossen werden, der mit einem VM-LAN (oder einem Weitverkehrsnetzwerk) verglichen werden kann. Auf jedem teilnehmendem VM-System muss eine virtuelle TSAF-Maschine betrieben werden. Innerhalb eines TSAF-Verbunds sind alle Benutzer-IDs und Ressourcen-IDs eindeutig.

DB2 für VM verwendet TSAF, um Anforderungen für verteilte Datenbanken an andere Maschinen mit DB2 für VM innerhalb des TSAF-Verbunds weiterzuleiten. Wenn das lokale VM-System nicht über eine virtuelle AVS-Maschine verfügt, verwendet DB2 für VM TSAF, um DRDA-Anforderungen an ein VM-System weiterzuleiten, das über eine virtuelle AVS-Maschine verfügt. Über AVS kann die Anforderung an andere TSAF-Verbunde sowie an Systeme ohne DB2 für VM weitergeleitet werden.

Ein TSAF-Verbund wird im SNA-Netzwerk als eine oder mehrere logische Einheiten angesehen. Auf Ressourcen, die innerhalb eines TSAF-Verbunds als global definiert sind, können ferne APPC-Programme zugreifen, die sich an einer beliebigen Stelle im Verbund befinden können.

Normalerweise arbeitet ein TSAF-Verbund als eigenständige Komponente, unabhängig von VTAM und vom SNA-Netzwerk. Er kann jedoch mit AVS und VTAM zusammenarbeiten, um seine globalen Ressourcen für ferne APPC-Programme zugänglich zu machen, die sich an einer beliebigen Stelle im SNA-Netzwerk befinden. Dazu ist es erforderlich, dass eine AVS-Maschine und eine VTAM-Maschine auf mindestens einem Mitglied des TSAF-Verbunds ausgeführt werden. TSAF wird im VM/ESA®-Handbuch *VM/ESA Connectivity Planning, Administration, and Operation* beschrieben.

#### **VTAM**

VTAM (Virtual Telecommunications Access Method) stellt die Netzwerk-kommunikationsunterstützung für Konnektivität zur Verfügung. DB2 für VM verwendet die VTAM-Services über AVS, um Verbindungen und Anforderungen an ferne DRDA-Systeme weiterzuleiten. VTAM wird *ausschließlich* für ferne Anforderungen verwendet, die auf das SNA-Netzwerk zugreifen.

#### **\*IDENT**

AVS und TSAF verwenden den Transaktionsprogrammnamen (TPN) zum Weiterleiten von Anforderungen zwischen VM-Systemen, die über TSAF und AVS verbunden sind. Der TPN kann ein in SNA registrierter Transaktionsprogrammname oder ein gültiger alphanumerischer Name sein. In VM wird der TPN-Wert als Ressourcen-ID angesehen. Damit ferne DRDA-Systeme auf einen Server unter DB2 für VM zugreifen können, verwendet der Server unter DB2 für VM den VM-Systemservice IDENTIFY (\*IDENT), um sich selbst als Manager einer globalen Ressourcen-ID (TPN) zu definieren. Sobald der Server als globale Ressource identifiziert ist, können TSAF und AVS DRDA-Anforderungen an den Server unter DB2 für VM weiterleiten, sofern der empfangene TPN mit der Ressourcen-ID übereinstimmt.

Wie in Abb. 15 auf Seite 85 dargestellt, kann eine VM-Anwendung nur über den Anwendungsrequester (Ressourcenadapter) von DB2 für VM auf eine Datenbank eines Anwendungsservers von DB2 für VM oder eines DRDA-Anwendungsservers zugreifen. Eine Datenbank auf einem Anwendungsserver unter DB2 für VM kann

SQL-Anforderungen von jedem Anwendungsrequester unter DB2 für VM oder DRDA-Anwendungsrequester empfangen.

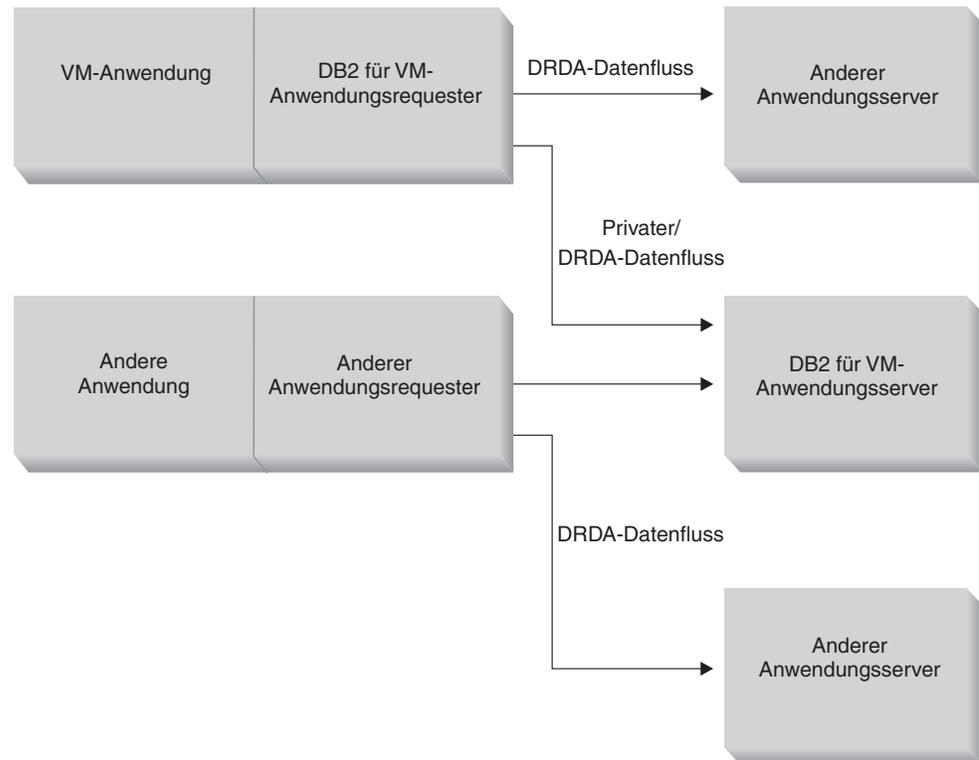


Abbildung 15. Anwendungsrequester und Anwendungsserver unter DB2 für VM

### Optionen für die Vorverarbeitung und Ausführung einer Anwendung:

DB2 für VM unterstützt im Befehl **sqlinit** drei Verarbeitungsoptionen, die dem Benutzer und dem Datenbankadministrator das Aktivieren der Unterstützung für verteilte Datenbanken ermöglichen. Vor Beginn der Vorverarbeitung bzw. der Ausführung der Anwendung kann der Benutzer eine der folgenden SQLINIT-Optionen angeben:

#### PROTOCOL(SQLDS)

Fordert die Verwendung des privaten SQLDS-Protokolls an. Dies ist die Standardoption. Sie kann zwischen einem Anwendungsrequester und -server unter DB2 für VM in einer lokalen oder fernen Umgebung verwendet werden. Der Anwendungsserver von DB2 für VM geht davon aus, dass der Requester die selben CCSIDs wie der Server verwendet. Die vom Requester über SQLINIT konfigurierten CCSID-Standardwerte<sup>2</sup> werden ignoriert, und dem Dialog wird keine LU 6.2-LUWID zugeordnet. Wenn Sie überall nur Systeme mit DB2 für VM und die selbe Standard-CCSID verwenden, ist diese Option am effektivsten.

#### PROTOCOL(AUTO)

Fordert den Anwendungsrequester von DB2 für VM auf festzustellen, ob der Anwendungsserver ein gleichartiges oder ein andersartiges System ist. Anschließend wird für ein gleichartiges System automatisch die Verwendung eines privaten SQLDS-Protokolls bzw. für ein andersartiges System

2. In DB2 für VM geben Anwendungsrequester und Anwendungsserver die Standard-CCSID mit Hilfe der Option CHARNAME für SQLINIT bzw. SQLSTART an. CHARNAME ist ein symbolischer Name, der intern den entsprechenden CCSIDs zugeordnet wird.

die Verwendung des DRDA-Protokolls ausgewählt. Die Option kann zwischen gleichartigen (lokalen und fernen) und andersartigen Systemen verwendet werden. Wenn für den Anwendungsserver nicht PROTOCOL=SQLDS festgelegt ist, können auf dem Anwendungsrequester und -Server unterschiedliche Standard-CCSIDs verwendet werden. Die Anforderungen und Antworten werden entsprechend umgesetzt. Die Option AUTO ist in folgenden Fällen zu empfehlen:

- Wenn Sie auf gleichartige und andersartige Systeme zugreifen müssen
- Wenn die Standard-CCSIDs auf Requester und Server unterschiedlich sind (und die Option PROTOCOL auf dem Anwendungsserver nicht SQLDS ist)
- Wenn jedem Dialog eine LU 6.2-LUWID zugeordnet sein muss, damit Sie einen Prozess problemlos zum Ursprungsstandort zurückverfolgen können (dies ist hilfreich, wenn Sie in Ihrem Netzwerk mit verteilten Datenbanken eine große Anzahl von fernen Systemen mit DB2 für VM zu verwalten haben)

### PROTOCOL(DRDA)

Zwingt den Anwendungsrequester unter DB2 für VM, bei der Kommunikation mit dem Anwendungsserver nur das DRDA-Protokoll zu verwenden. Diese Option kann zwischen gleichartigen (lokalen und fernen) und andersartigen Systemen verwendet werden. Wenn der Anwendungsserver ein gleichartiges System ist, wird zwischen den beiden Systemen mit DB2 für VM das DRDA-Protokoll verwendet. Der Anwendungsrequester und der Anwendungsserver können über unterschiedliche Standard-CCSIDs verfügen. Die Anforderungen und Antworten werden entsprechend umgesetzt. Sie können diese Option zwischen zwei Systemen mit DB2 für VM zu Testzwecken oder für bestimmte Anwendungen verwenden, bei denen durch die Verwendung des DRDA-Protokolls aufgrund größerer Puffer zum Senden und Empfangen von Daten ein höherer Durchsatz erzielt werden kann.

In Tabelle 3 werden die Funktionsbeschreibungen der SQLINIT-Verarbeitungsoptionen des Anwendungsrequesters unter DB2 für VM verglichen.

*Tabelle 3. Vergleich der SQLINIT-Verarbeitungsoptionen des Anwendungsrequesters unter DB2 für VM*

[SQLDS]	[ AUTO ]	[DRDA]
Beide Partner müssen Systeme mit DB2 für VM sein.	Verbindung zu jedem DRDA-System möglich.	Verbindung zu jedem DRDA-System möglich.
Lokale Kommunikation mit Partner über TSAF oder AVS/VTAM möglich.	Lokale Kommunikation mit einem System mit DB2 für VM oder mit einem fernen System mit DB2 für VM über TSAF bzw. AVS möglich. Bei andersartigen Systemen muss über AVS kommuniziert werden.	Lokale Kommunikation mit einem System mit DB2 für VM oder mit einem fernen System mit DB2 für VM über TSAF bzw. AVS möglich. Bei andersartigen Systemen muss über AVS kommuniziert werden.
Unterstützt statisches, dynamisches und erweitertes dynamisches SQL.	Unterstützt statisches, dynamisches und erweitertes dynamisches SQL.	Unterstützt statisches, dynamisches und erweitertes dynamisches SQL <sup>3</sup> .

3. Erweitertes dynamisches SQL wird für den DRDA-Datenfluss unterstützt, indem eine Umsetzung in statische oder dynamische Anweisungen ausgeführt wird. Dabei gelten eine Reihe von Einschränkungen.

Tabelle 3. Vergleich der SQLINIT-Verarbeitungsoptionen des Anwendungsrequesters unter DB2 für VM (Forts.)

[SQLDS]	[ AUTO ]	[DRDA]
Von SQLINIT für den Anwendungsrequester definierte CCSIDs werden vom Anwendungsserver unter DB2 für VM ignoriert.	Von SQLINIT für den Anwendungsrequester definierte CCSIDs werden vom Anwendungsserver unter DB2 für VM beachtet, und entsprechende Umsetzungen werden ausgeführt (sofern der Anwendungsserver ebenfalls auf AUTO gesetzt ist).	Von SQLINIT für den Anwendungsrequester definierte CCSIDs werden vom Anwendungsserver unter DB2 für VM beachtet, und entsprechende Umsetzungen werden ausgeführt.
Feste Blockgröße von 8 KB; Aufruf OPEN gibt keine Zeilen zurück; Anwendungsrequester muss den Cursor explizit schließen.	Verbindung von DB2 für VM mit DB2 für VM: SQLDS-Methode; alle anderen Verbindungen: DRDA-Methode.	Variable Blockgröße von 1 KB bis 32 KB; stärker komprimierte Datenpaketierung; Aufruf OPEN gibt einen Zeilenblock zurück; Anwendungsserver kann den Cursor implizit schließen, so dass der Anwendungsrequester keinen CLOSE-Aufruf senden muss.
Kann mit Cursoranweisungen INSERT und PUT jeweils einen Zeilenblock mit fester Blockgröße von 8 KB gleichzeitig einfügen.	Verbindung von DB2 für VM mit DB2 für VM: SQLDS-Methode; alle anderen Verbindungen: DRDA-Methode.	PUT-Anweisungen werden in reguläre Einfügungen einzelner Zeilen umgesetzt und zeilenweise abgesendet.
Alle für DB2 für VM spezifischen Befehle werden unterstützt.	Verbindung von DB2 für VM mit DB2 für VM: SQLDS-Methode; alle anderen Verbindungen: DRDA-Methode.	Bedienerbefehle von DB2 für VM, einige Anweisungen von DB2 für VM und einige ISQL- und DBSU-Befehle werden nicht unterstützt (weitere Informationen finden Sie Handbuch <i>DB2 Server for VSE &amp; VM SQL Reference</i> ).
LUWID wird nicht unterstützt.	LUWID wird unterstützt.	LUWID wird unterstützt.

### Optionen zum Starten der Datenbankservermaschine:

In diesem Abschnitt werden die verschiedenen Optionen zum Starten der Datenbankservermaschine beschrieben.

#### Parameter PROTOCOL:

Beim Starten der Datenbankservermaschine kann der Datenbankadministrator eine der folgenden Optionen für den Parameter PROTOCOL angeben.

#### SQLDS

Die empfohlene Standardoption, wenn der Anwendungsserver nur Unterstützung für Anwendungsrequester unter DB2 für VM oder für Anwendungsanfragen von DB2 für VSE bei gemeinsamer Benutzung der VSE-Gastmaschine bereitstellen muss. Der Anwendungsserver verwendet nur den privaten Datenfluss (SQLDS).

Der Anwendungsserver reagiert auf die vom Anwendungsrequester ausgewählte Verarbeitungsoption. Verwendet ein Requester unter DB2 für VM die Einstellung PROTOCOL(SQLDS), wird die Verarbeitung auf dem Server unter DB2 für VM regulär mit privatem Datenfluss fortgesetzt. Verwendet der Requester unter DB2 für VM die Einstellung PROTOCOL(AUTO), weist der Server unter DB2 für VM den Requester an, auf privaten Datenfluss umzuschalten. Zwischen dem Anwendungsrequester und dem Anwendungsserver werden keine CCSID-Informationen ausgetauscht.

Der Anwendungsserver geht davon aus, dass die CCSIDs des Anwendungsrequesters mit denen des Anwendungsservers übereinstimmen. Verwendet der Requester unter DB2 für VM die Einstellung PROTOCOL(DRDA), wird der Dialog beendet. Wenn ein Anwendungsrequester mit einer anderen DB2-Version als DB2 für VSE & VM versucht, auf den Server unter DB2 für VM zuzugreifen, wird der Dialog beendet.

### **AUTO**

Die empfohlene Option, wenn der Anwendungsserver die Unterstützung für das private Protokoll und das DRDA-Protokoll bereitstellen muss. Die Anwendungsrequester unter DB2 für VM, die die Einstellung PROTOCOL(SQLDS) oder PROTOCOL(AUTO) verwenden, kommunizieren über den privaten Datenfluss. Für einen Anwendungsrequester, der die Einstellung SQLDS verwendet, werden keine CCSID-Informationen ausgetauscht, und der Anwendungsserver geht davon aus, dass die CCSIDs des Anwendungsrequesters mit denen des Anwendungsservers übereinstimmen. Für einen Requester, der die Einstellung AUTO verwendet, werden CCSID-Informationen ausgetauscht, und die CCSID-Umsetzung von Anforderungen und Antworten wird entsprechend ausgeführt. Der DRDA-Datenfluss ist für alle Requester ohne DB2 für VM und für alle Requester unter DB2 für VM erforderlich, die die Einstellung PROTOCOL(DRDA) verwenden.

### **Parameter SYNCPNT:**

Dieser Parameter gibt an, ob ein Synchronisationspunktmanager (SPM) zum Koordinieren von verteilten DRDA-2-Arbeitseinheiten für das Lesen und Schreiben auf mehreren Systemen verwendet wird.

Wird Y angegeben, verwendet der Server einen Synchronisationspunktmanager (sofern möglich), um zweiphasige Festschreibungen und Resynchronisationsfunktionen zu koordinieren. Wird N angegeben, verwendet der Anwendungsserver keinen SPM, um zweiphasige Festschreibungen durchzuführen. Wenn N angegeben wird, ist der Anwendungsserver auf verteilte Arbeitseinheiten für Lesen auf mehreren Systemen und Schreiben auf einem einzigen System begrenzt, und der Server kann das System sein, auf das geschrieben wird. Wenn Y angegeben wird, für den Anwendungsserver jedoch kein Synchronisationspunktmanager zur Verfügung steht, wird der Server so betrieben, als ob N angegeben wurde.

Die Standardeinstellung ist SYNCPNT=Y, wenn die Einstellung PROTOCOL=AUTO verwendet wird. Bei Verwendung der Einstellung PROTOCOL=SQLDS wird der Parameter SYNCPNT auf N gesetzt.

### **Beispiel für den Kommunikationsfluss des Anwendungsrequesters:**

Das folgende Beispiel zeigt, welche Rolle die einzelnen Komponenten beim Einrichten der Verbindung zwischen einem VM-Anwandsrequester und einem fernen DRDA-Server spielen. In Abb. 16 auf Seite 89 wird dargestellt, wie der Anwendungsrequester die Verbindung zu AVS herstellt und über VTAM auf das SNA-Netzwerk zugreift. Der Zugriff auf ferne Ressourcen erfolgt nicht über den lokalen Anwendungsserver unter DB2 für VM.

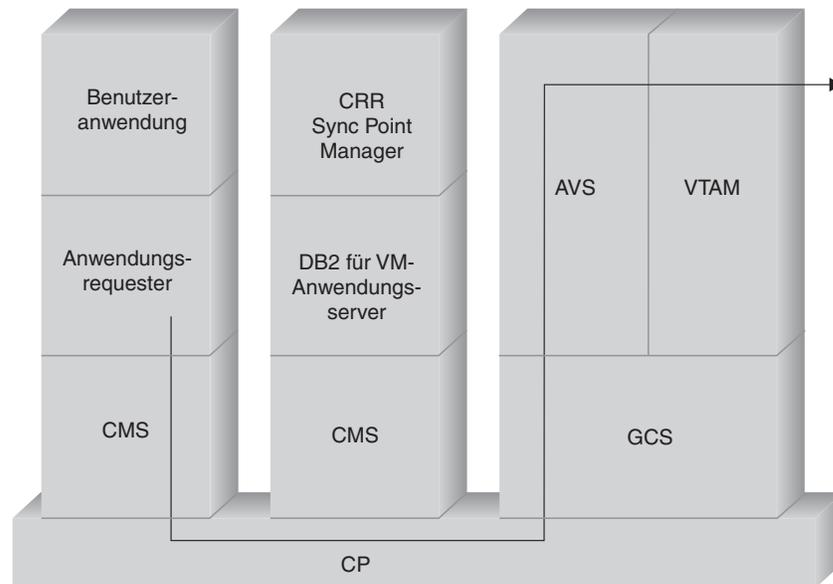


Abbildung 16. Anfordern des Zugriffs auf eine ferne Ressource

Angenommen, ein Anwendungsrequester unter DB2 für VM, der in einem TSAF-Verbund betrieben wird, soll auf ferne Daten zugreifen, die von einem DRDA-Anwendungsserver verwaltet werden. Per Definition heißt dies, dass auf dem lokalen VM-Host, auf dem sich der Anwendungsrequester befindet, eine TSAF-Maschine betrieben wird. Außerdem werden eine AVS-Komponente und eine VTAM-Maschine auf einem VM-System im TSAF-Verbund betrieben. AVS und VTAM könnten sich auch auf dem gleichen System wie der Anwendungsrequester und der Anwendungsserver befinden.

Nach dem Start definiert die VTAM-Maschine den lokalen AVS-Gateway gegenüber dem SNA-Netzwerk und definiert eine oder mehrere Sitzungen, die später zum Einrichten von Dialogen verwendet werden können.

Die AVS-Maschine vereinbart nach dem Starten Sitzungsbegrenzungen zwischen dem lokalen AVS-Gateway und den potenziellen Partner-LUs.

Der Anwendungsserver kann aktiv oder inaktiv sein. Der Bediener muss den Anwendungsserver starten, damit Anforderungen von gleichartigen oder andersartigen Anwendungsrequestern verarbeitet werden können.

Der Anwendungsrequester setzt eine APPC/VM-Anweisung CONNECT ab, um einen LU 6.2-Dialog mit dem Anwendungsserver einzurichten. Die Funktion CONNECT verwendet das CMS-Kommunikationsverzeichnis, um den Namen der relationalen Datenbank in den zugehörigen LU-Namen und den TPN aufzulösen, aus denen die Adresse des Anwendungsservers im SNA-Netzwerk besteht. Das CMS-Kommunikationsverzeichnis legt außerdem die Stufe der Dialogsicherheit und die Sicherheitstoken (z. B. Benutzer-ID und Kennwort) fest, die zum Zweck der Berechtigungsüberprüfung an den fernen Standort übermittelt werden. Wird SECURITY=PGM verwendet, muss der Anwendungsrequester eine Benutzer-ID und ein Kennwort an den Anwendungsserver übermitteln. Sie können die Benutzer-ID und das Kennwort im CMS-Kommunikationsverzeichnis oder im APPC-PASS-Datensatz angeben, der im Benutzerverzeichnis des Anwendungsrequesters

definiert ist. Bei der Verwendung von SECURITY=SAME wird nur die VM-Anmelde-ID des Benutzers des Anwendungsrequesters an den Anwendungsserver übermittelt, und es ist kein zusätzliches Kennwort erforderlich.

Beispiel: Wenn Sie SECURITY=SAME verwenden, überprüft der Host, ob eine AVS-Maschine lokal ausgeführt wird. Ist dies nicht der Fall, stellt der Host eine Verbindung zwischen dem Anwendungsrequester und der lokalen TSAF-Maschine her. Die lokale TSAF-Maschine fragt die AVS-Maschine unter den anderen TSAF-Maschinen im TSAF-Verbund ab und stellt eine Verbindung zur AVS-Maschine her.

Die AVS-Komponente im TSAF-Verbund setzt die APPC/VM-Verbindungsanforderung in den äquivalenten APPC/VTAM-Funktionsaufruf um. Anschließend verwendet AVS eine vorhandene Sitzung oder richtet eine neue Sitzung zwischen dem Gateway (LU) und der fernen LU ein. Danach richtet AVS einen Dialog mit der fernen LU ein und übermittelt den LU-Namen, den TPN, die Sicherheitsstufe und die Benutzer-ID. Ist die ferne LU ebenfalls ein VM-System, werden Sitzung und Dialog von der AVS-Komponente verwaltet, die auf diesem System ausgeführt wird.

#### Beispiel für den Kommunikationsfluss des Anwendungsservers:

Das folgende Beispiel zeigt, welche Rolle die einzelnen Komponenten beim Einrichten der Verbindung zwischen einem fernen Anwendungsrequester und einem lokalen DRDA-Server unter DB2 für VM spielen. In Abb. 17 wird dargestellt, dass VTAM die eingehende Verbindung an den spezifischen AVS-Gateway und anschließend an den Anwendungsserver weiterleitet.

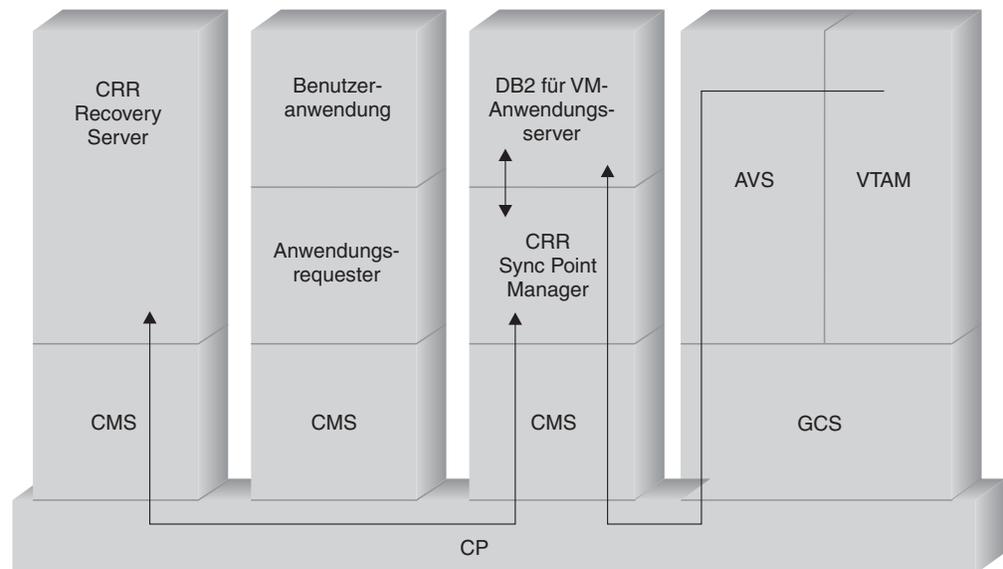


Abbildung 17. Einrichten des Zugriffs auf eine ferne Ressource

Angenommen, ein Anwendungsserver unter DB2 für VM wird in einem TSAF-Verbund betrieben. Per Definition heißt dies, dass auf dem lokalen VM-Host, auf dem sich der Anwendungsserver befindet, eine TSAF-Maschine betrieben wird. Außerdem werden eine AVS-Komponente und eine VTAM-Maschine auf einem VM-System im TSAF-Verbund betrieben. AVS und VTAM könnten sich auch auf dem gleichen System wie der Anwendungsrequester und der Anwendungsserver befinden.

Nach dem Start definiert die VTAM-Maschine den lokalen AVS-Gateway gegenüber dem SNA-Netzwerk und definiert eine oder mehrere Sitzungen, die später zum Einrichten von Dialogen verwendet werden können.

Die AVS-Maschine vereinbart nach dem Starten Sitzungsbeschränkungen zwischen dem lokalen AVS-Gateway und den potenziellen Partner-LUs.

Der Anwendungsserver kann aktiv oder inaktiv sein. Der Bediener muss den Anwendungsserver starten, damit Anforderungen von gleichartigen oder andersartigen Anwendungsrequestern verarbeitet werden können. Nach dem Starten verwendet der Anwendungsserver den Service \*IDENT, um die Ressourcen-ID, die er verwaltet, auf dem VM-Host-System zu registrieren. Durch jede Registrierung wird in einer internen Ressourcentabelle, die durch das VM-System verwaltet wird, ein Eintrag erstellt.

Nachdem die lokale AVS-Komponente die Sitzung mit ihrer Partner-LU eingerichtet hat, akzeptiert sie den Dialog und leitet den TPN, die Benutzer-ID und das Kennwort zur Gültigkeitsprüfung an den VM-Host weiter. Das VM-System sucht in der eigenen internen Ressourcentabelle nach dem TPN. Diese Tabelle enthält für jede Ressourcen-ID, die durch den Systemservice \*IDENT registriert wurde, einen Eintrag. Wenn der TPN gefunden wird, prüft das VM-System die Gültigkeit von Benutzer-ID und Kennwort anhand des eigenen Verzeichnisses oder mit Hilfe von RACF<sup>®</sup> bzw. einem äquivalenten Sicherheitsprodukt. Ist die Gültigkeitsprüfung erfolgreich, stellt AVS eine Verbindung zu dem Anwendungsserver her und übermittelt die Benutzer-ID zur Gültigkeitsprüfung für die Datenbank.

Ist die Suche in der Tabelle nicht erfolgreich, nimmt AVS an, dass sich der TPN möglicherweise in einem anderen VM-System im TSAF-Verbund befindet, stellt eine Verbindung zur lokalen TSAF-Maschine her und leitet die Benutzer-ID, das Kennwort und den TPN an diese Maschine weiter. Die TSAF-Maschine fragt die übrigen TSAF-Maschinen im TSAF-Verbund ab. Bestätigt eine dieser Maschinen das Vorhandensein des TPN in ihrer Ressourcentabelle, stellt die lokale TSAF-Maschine eine Verbindung zur fernen TSAF-Maschine her und übermittelt Benutzer-ID und Kennwort zur Überprüfung anhand des VM-Verzeichnisses dieser Maschine. Ist die Gültigkeitsprüfung erfolgreich, stellt die ferne TSAF-Maschine eine Verbindung zum Anwendungsserver her und übermittelt die Benutzer-ID zur Gültigkeitsprüfung für die Datenbank.

Wenn der Anwendungsrequester Unterstützung für verteilte DRDA-Arbeits-einheiten in Anspruch nehmen will, richtet er einen geschützten Dialog (d. h. SYNCLEVEL=SYNCPT) mit dem Anwendungsserver unter DB2 für VM ein. CMS erstellt vor der Verbindungsherstellung zu DB2 für VM eine CMS-Arbeitseinheit für den geschützten Dialog auf der Maschine unter DB2 für VM. DB2 für VM verwendet diese CMS-Arbeitseinheit anschließend bei jedem Arbeitsvorgang für den Requester. Nach dem Arbeitsbeginn für den Requester registriert DB2 für VM diese CMS-Arbeitseinheit beim CRR-Synchronisationspunktmanager (CRR Sync Point Manager). Wenn DB2 danach im geschützten Dialog eine SNA-Markierung für Festschreiben (COMMIT) bzw. Zurücksetzen (ROLLBACK) empfängt, weist DB2 den CRR-Synchronisationspunktmanager an, die Arbeitseinheit festzuschreiben bzw. zurückzusetzen. Der CRR-Synchronisationspunktmanager steuert die COMMIT- bzw. ROLLBACK-Operation und weist den CRR Recovery Server an, bei Bedarf eine Synchronisationspunktprotokollierung auszuführen.

Je nach Komplexität der Verbindungswege können an dem APPC-Dialog zwischen Anwendungsrequester und Anwendungsserver weitere Systeme beteiligt sein. Alle Zwischenverbindungen werden jedoch vom VM-System verwaltet, und sie sind für

den Anwendungsrequester oder die Benutzeranwendung transparent. Die APPC/VM-Schnittstelle ermöglicht Anwendungsservern unter DB2 für VM den Datenaustausch mit APPC-Anwendungsprogrammen an folgenden Standorten:

- Im selben VM-System
- In einem anderen VM-System
- In einem VM-System innerhalb eines SNA-Netzwerks, auf dem AVS und VTAM ausgeführt werden
- In einem VM-System innerhalb eines anderen TSAF-Verbunds, auf dem AVS und VTAM ausgeführt werden
- In einem Nicht-VM-System innerhalb eines SNA-Netzwerks, das das LU 6.2-Protokoll unterstützt
- In einem System eines anderen Herstellers als IBM innerhalb eines SNA-Netzwerks, das das LU 6.2-Protokoll unterstützt

**Zugehörige Konzepte:**

- „Sicherheitsüberlegungen für Anwendungsserver (VM)“ auf Seite 108
- „Datendarstellung (VM)“ auf Seite 132
- „Sicherheitsüberlegungen für Anwendungsrequester (VM)“ auf Seite 124
- „DB2 für VSE“ auf Seite 94

**Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsserver (VM)“ auf Seite 67
- „Definieren von DB2 als Anwendungsrequester (VM)“ auf Seite 39

**Zugehörige Referenzen:**

- „Prüfliste zum Aktivieren eines DB2-Anwendersrequesters (VM)“ auf Seite 141

---

## Weitere Konzepte

### Definieren der Kommunikation – Anwendungsrequester (VM)

In der VM-Umgebung wird die Kommunikationsverwaltung von einer Kombination mehrerer Komponenten ausgeführt. Die an der Kommunikation zwischen nicht gleichartigen DRDA-Systemen beteiligten Komponenten sind APPC/VM, das CMS-Kommunikationsverzeichnis, TSAF, AVS und VTAM.

APPC/VM ist die LU 6.2-API auf Assemblerebene, die vom Anwendungsrequester unter DB2 für VM zur Anforderung von Übertragungsdiensten verwendet wird. Das CMS Communications Directory stellt die Weiterleitungs- und Sicherheitsinformationen des verteilten Partnersystems zur Verfügung. AVS aktiviert den Gateway und wandelt den abgehenden APPC/VM-Datenfluss in einen APPC/VTAM-Datenfluss sowie den eingehenden APPC/VTAM-Datenfluss in einen APPC/VM-Datenfluss um.

APPC/VM, TSAF und AVS sind davon abhängig, dass die Anforderungen durch das CMS-Kommunikationsverzeichnis, VTAM und \*IDENT an den richtigen DRDA-Partner weitergeleitet werden.

Damit VTAM mit den im CMS-Kommunikationsverzeichnis angegebenen Partneranwendungen kommunizieren kann, müssen Sie folgende Informationen bereitstellen:

1. Definieren Sie die LU-Namen aller Anwendungsrequester und Anwendungsserver für VTAM. Platzierung und Syntax dieser Definitionen hängen davon ab, wie das ferne System logisch und physisch mit dem VTAM-System verbunden ist.
2. Erstellen Sie in der VTAM-Modustabelle für jeden Modusnamen, der im CMS-Kommunikationsverzeichnis angegeben ist, einen Eintrag. Diese Einträge beschreiben die Größe der Anforderungseinheit (Request Unit, RU), die Größe des Nachrichtendosierfensters und die Serviceklasse für einen bestimmten Modusnamen.
3. Wenn Sie die Partner-LU-Prüfung (Sicherheit auf Sitzungsebene) verwenden wollen, müssen Sie VTAM- und RACF-Profile (oder gleichwertige Angaben) für den Prüfalgorithmus bereitstellen.

### **Überlegungen zur AVS-Sitzungsbegrenzung:**

Wenn ein Anwendungsrequester AVS verwendet, um mit einem fernen Anwendungsserver zu kommunizieren, wird eine Verbindung eingeleitet. Wird durch diese Verbindung die geltende Sitzungsbegrenzung überschritten, versetzt AVS die Verbindung in den Wartestatus, bis wieder eine Sitzung verfügbar wird. Sobald eine Sitzung verfügbar wird, ordnet AVS die zurückgestellte Verbindung dieser Sitzung zu, und die Steuerung wird an die Benutzeranwendung zurückgegeben. Um diese Situation zu vermeiden, sollten Sie die maximale Auslastung im Voraus einplanen, indem Sie im Grenzwert für die Sitzungsbegrenzung einige zusätzliche Verbindungen zulassen. Stellen Sie sicher, dass der Wert für MAXCONN im Benutzerverzeichnis der AVS-Maschine groß genug ist, um die maximale Auslastung durch APPC/VM-Verbindungen zu unterstützen.

#### **Zugehörige Konzepte:**

- „DB2 für VM“ auf Seite 82

## **Festlegen der RU-Größen und der Nachrichtendosierung (VM)**

Die in der VTAM<sup>®</sup>-Modustabelle von Ihnen definierten Einträge geben die Größe der Anforderungseinheiten (RU-Größe) und die Zähler für die Nachrichtendosierung (Pacing Count) an. Fehlende oder fehlerhafte Definitionen für diese Werte können sich nachteilig auf alle VTAM-Anwendungen auswirken.

Bedenken Sie bei der Wahl der RU-Größen, Sitzungsbegrenzungen und Nachrichtendosierungszähler, welche Auswirkungen diese Werte auf das vorhandene SNA-Netzwerk haben können. Überprüfen Sie beim Installieren eines neuen verteilten Datenbanksystems die folgenden Punkte:

- Stellen Sie für VTAM-CTC-Verbindungen sicher, dass der Parameterwert für MAXBFRU groß genug ist, um Ihre RU-Größe plus der 29 Byte, die VTAM als SNA-Anforderungs- und Übertragungskopf hinzufügt, zu verarbeiten. MAXBFRU wird in Einheiten von 4 KB gemessen, d. h. der Wert für MAXBFRU muss mindestens 2 betragen, um eine RU-Größe von 4 KB zu unterstützen.
- Stellen Sie für NCP-Verbindungen sicher, dass der Wert für MAXDATA groß genug ist, um Ihre RU-Größe plus 29 Byte zu verarbeiten. Wenn Sie als RU-Größe 4 KB angegeben haben, muss der Wert für MAXDATA mindestens 4125 betragen.

Wenn Sie den NCP-Parameter MAXBFRU angeben, wählen Sie einen Wert aus, der für Ihre RU-Größe plus 29 Byte ausreicht. Bei NCP definiert der Parameter MAXBFRU die Anzahl der VTAM-E/A-Puffer für die PIU. Wenn Sie für IOBUF eine Puffergröße von 441 angeben, reicht die Einstellung MAXBFRU=10 für die RU-Größe 4 KB aus, da  $10 \cdot 441$  größer ist als  $4096 + 29$ .

- Im Handbuch *DRDA Connectivity Guide* wird beschrieben, wie Sie die Auswirkung der verteilten Datenbank auf den VTAM-IOBUF-Pool abschätzen können. Wenn ein zu großer Anteil der IOBUF-Poolressource belegt ist, hat dies nachteilige Auswirkungen auf die Leistung aller VTAM-Anwendungen.

#### **Zugehörige Konzepte:**

- „DB2 für VM“ auf Seite 82

---

## **DB2 für VSE**

SQL/DS™ (DB2 für VSE) Version 3 Release 5 stellt VSE-Systemen DRDA®-Anwendungsserver-Unterstützung für ferne Arbeitseinheiten zur Verfügung.

In der VSE/ESA™-Betriebsumgebung stellt DB2® für VSE die Anwendungsserver-Funktion für eine DRDA-Umgebung zur Verfügung. Die Anwendungsrequester-Funktion wird nicht zur Verfügung gestellt. In diesem Abschnitt werden die verschiedenen Komponenten von DB2 für VSE und von VSE beschrieben, die an der Verarbeitung für verteilte Datenbanken beteiligt sind. Über diese Komponenten kann das Datenbankverwaltungssystem unter DB2 für VSE mit fernen DRDA-Anwendungsrequestern in einem SNA-Netzwerk kommunizieren.

#### **CICS(ISC)**

Die CICS-Komponente (CICS - Customer Information Control System) für die Kommunikation zwischen Systemen (Intersystem Communication) stellt die SNA-LU 6.2-Funktionen (APPC-Funktionen) für den Anwendungsserver unter DB2 für VSE zur Verfügung.

#### **CICS(SPM)**

Die CICS®-Komponente zur Synchronisationspunktverwaltung (Sync Point Management) ist integraler Bestandteil der Unterstützung verteilter DRDA-Arbeitseinheiten unter DB2 für VSE. Sie fungiert als Synchronisationspunktteilnehmer und ist für die Koordination der zweiphasigen Festschreibung auf einem VSE/ESA-System zuständig.

#### **CICS(TRUE)**

Der taskbezogene CICS-Benutzerexit (Task-Related User Exit) ist eine von der Transaktion AXE (APPC-XPCC-Exchange) verwendete Schnittstelle mit dem CICS-Synchronisationspunktmanager.

#### **ACF/VTAM®**

CICS(ISC) verwendet VTAM® für VSE zum Einrichten bzw. Binden von LU-LU-Sitzungen für/an ferne Systeme. DB2 für VSE verwendet LU 6.2-Basisdialoge über diese Sitzungen, um mit fernen DRDA-Anwendungsrequestern zu kommunizieren.

#### **AXE**

Die Transaktion AXE (APPC-XPCC-Exchange) ist eine CICS-Transaktion, die von dem fernen DRDA-Anwendungsrequester aktiviert wird. Sie bestimmt den Leitweg für den DRDA-Datenstrom zwischen dem fernen Anwendungsrequester und dem Anwendungsserver unter DB2 für VSE mit Hilfe der CICS-LU 6.2-Unterstützung und der VSE-XPCC-Funktionen (Cross Partition Communication Protocol).

### Verzeichnis DBNAME

Das Verzeichnis DBNAME (Verzeichnis der Datenbanknamen) ordnet eine eingehende Anforderung zur Dialogzuordnung einem vorgegebenen Anwendungsserver zu, der vom eingehenden TPN definiert wird. Weitere Informationen finden Sie im Handbuch *SQL/DS System Administration Guide for VSE*.

**XPCC** Die partitionsübergreifende DFV-Steuerung (XPCC - Cross Partition Communication Control) ist die VSE-Makroschnittstelle, die die Datenübertragung zwischen VSE-Partitionen ermöglicht.

### Beispiel für den Kommunikationsfluss des Anwendungsservers:

In Abb. 18 wird dargestellt, welche Rolle die einzelnen Komponenten beim Einrichten der Kommunikation zwischen dem Anwendungsserver unter DB2 für VSE und dem fernen Anwendungsrequester spielen.

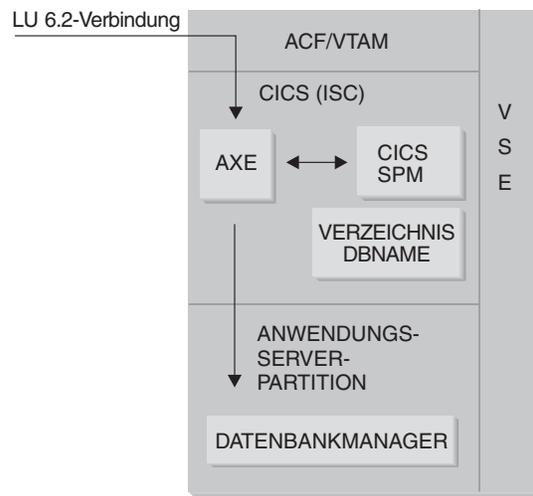


Abbildung 18. Einrichten des Zugriffs auf den Anwendungsserver

Der Anwendungsrequester setzt ein APPC-Verb ALLOCATE mit einem bestimmten LU- und Transaktionsprogrammnamen (TPN) ab, um einen LU 6.2-Dialog mit dem Anwendungsserver einzurichten. Mit dem LU-Namen wird die Anforderung ALLOCATE über VTAM an CICS weitergeleitet. Nach dem Empfang des Verbs ALLOCATE prüft CICS, ob eine Transaktion AXE mit diesem TPN definiert ist, und führt eine CICS-Anmeldung durch. Ist für die CICS-Verbindung die Dialogsicherheitsstufe VERIFY definiert, werden vom Anwendungsrequester sowohl eine Benutzer-ID als auch ein Kennwort erwartet und beim Anmelden verwendet.

Die CICS-Anmeldetabelle (DFHSNT) muss mit diesen Angaben (Benutzer-ID und Kennwort) aktualisiert werden, damit die Verbindung akzeptiert wird. Ist die Sicherheitsstufe IDENTIFY definiert, ist nur die Benutzer-ID erforderlich, und CICS überlässt die Sicherheitsprüfung dem fernen System. Ist die Sicherheitsprüfung erfolgreich, startet CICS die Transaktion AXE, um Anforderungen und Antworten zwischen dem Anwendungsrequester und einem Anwendungsserver zu übermitteln. Für den vom Anwendungsrequester verwendete TPN muss im Verzeichnis DBNAME von DB2 für VSE ein Eintrag definiert sein, der auf einen im Betrieb befindlichen Server unter DB2 für VSE innerhalb des VSE-Systems verweist.

Wenn der Anwendungsrequester Unterstützung für verteilte Arbeitseinheiten in Anspruch nehmen will, gibt er im APPC-Verb ALLOCATE für SYNCLEVEL den Wert SYNCPT an. Nach dem Starten der Transaktion AXE fragt der Anwendungsrequester CICS ab, um den Wert für SYNCLVL im Dialog festzustellen. Ist der Wert SYNCPT, geschieht Folgendes:

- Falls erforderlich, aktiviert die Transaktion AXE Unterstützung für TRUE, damit sie mit dem CICS-Synchronisationspunktmanager kommunizieren kann.
- Die Transaktion registriert die logische Arbeitseinheit für den CICS-Synchronisationspunktmanager.

#### **Einschränkungen des Anwendungsservers:**

Im Unterschied zu seinem VM-Gegenstück akzeptiert der Anwendungsserver unter DB2 für VSE DRDA-Daten von fernen Anwendungsrequestern. Private Protokolle werden nicht unterstützt. Daher können VM-Anwandsrequester nicht auf einen VSE-Server mit PROTOCOL=SQLDS zugreifen. Der DRDA-Server von DB2 für VSE kann nicht durch gemeinsame Benutzung von VSE-Gastmaschinen Anforderungen von fernen Anwendungsrequestern an einen Server unter DB2 für VM weiterleiten. Solche Anforderungen müssen direkt an den DRDA-Server unter DB2 für VM übermittelt werden.

#### **Startparameter des Anwendungsservers:**

##### **Parameter RMTUSERS**

Der Datenbankadministrator kann beim Starten des Anwendungsservers den Parameter RMTUSERS angeben, um die maximale Anzahl der fernen Anwendungsrequester festzulegen, die eine Verbindung zu dem Server herstellen dürfen. Dieser Wert ist vergleichbar mit dem Wert für MAXCONN im VM-Verzeichnis der Datenbankservermaschine unter DB2 für VM. Dieser Parameter ermöglicht eine gleichmäßige Aufteilung der Transaktionsfolge auf lokale und ferne Verarbeitung.

Ist der Wert für RMTUSERS größer als die Anzahl der verfügbaren Agenten von DB2 für VSE (definiert durch NCUSER), müssen einige ferne Benutzer warten, bis ein Agent von DB2 für VSE ihre Anforderungen bearbeiten kann. Normalerweise wird ein Agent von DB2 für VSE einem wartenden Benutzer erneut zugeordnet, sobald eine logische Arbeitseinheit (Logical Unit of Work, LUW) beendet ist. Der Anwendungsserver unter DB2 für VSE unterstützt privilegierten Zugriff, d. h. ein ferner Benutzer kann einen Agenten von DB2 für VSE für mehrere LUWs bis zum Ende des Dialogs reservieren.

##### **Parameter SYNCPT**

Dieser Parameter gibt an, ob ein Synchronisationspunktmanager (SPM) zum Koordinieren von verteilten DRDA-2-Arbeitseinheiten für das Lesen und Schreiben auf mehreren Systemen verwendet wird.

Wird Y angegeben, verwendet der Server einen Synchronisationspunktmanager (sofern möglich), um zweiphasige Festschreibungen und Resynchronisationsfunktionen zu koordinieren. Wird N angegeben, verwendet der Anwendungsserver keinen SPM, um zweiphasige Festschreibungen durchzuführen. Wenn N angegeben wird, ist der Anwendungsserver auf Arbeitseinheiten für Lesen auf mehreren Systemen und Schreiben auf einem einzigen System begrenzt, und der Server kann das System sein, auf das geschrieben wird. Wenn Y angegeben wird, für den Anwendungsserver jedoch kein Synchronisationspunktmanager zur Verfügung steht, wird der Server so betrieben, als ob N angegeben wurde.

Die Standardeinstellung ist SYNCNT=Y, wenn RMTUSERS größer als Null ist. Bei Verwendung der Einstellung RMTUSERS=0 wird der Parameter SYNCNT auf N gesetzt.

**Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsserver (VSE)“ auf Seite 59



---

## Kapitel 12. Sicherheitsüberlegungen für Anwendungsserver

---

### Sicherheitsüberlegungen für Anwendungsserver (OS/390 und z/OS)

Wenn ein Anwendungsrequester eine Anforderung für eine verteilte Datenbank an den Anwendungsserver unter DB2® für OS/390® und z/OS™ weiterleitet, können dabei die folgenden Sicherheitsaspekte eine Rolle spielen:

- Herkunftsüberprüfung
- Endbenutzernamen
- Netzwerksicherheit
- Sicherheit des Datenbankmanagers
- SicherheitssystemSicherheitssystem

#### Zugehörige Konzepte:

- „Sicherheitsüberlegungen für Anwendungsrequester (OS/390 und z/OS)“ auf Seite 115
- „DB2 für OS/390 und z/OS“ auf Seite 73

#### Zugehörige Tasks:

- „Definieren von DB2 als Anwendungsserver (OS/390 und z/OS)“ auf Seite 47

---

### Weitere Konzepte

#### Herkunftsüberprüfung (OS/390 und z/OS)

Wenn der Hostanwendungsserver Endbenutzernamen von einem Anwendungsrequester empfängt, kann der Anwendungsserver die von einem bestimmten Anwendungsrequester empfangenen Endbenutzernamen beschränken. Hierzu wird die *Herkunftsüberprüfung* verwendet. Durch die Herkunftsüberprüfung kann der Anwendungsserver angeben, dass eine bestimmte Benutzer-ID nur von bestimmten Partnern verwendet werden darf.

So kann der Anwendungsserver beispielsweise die „Herkunft“ des Endbenutzernamens JONES auf DALLAS beschränken. Wenn ein anderer Anwendungsrequester (nicht DALLAS) versucht, den Namen JONES an den Anwendungsserver zu senden, kann der Anwendungsserver die Anforderung zurückweisen, weil der Name nicht vom korrekten Netzwerkstandort kommt.

Das Hostsystem implementiert die Herkunftsüberprüfung als Teil der Umsetzung von Endbenutzernamen für eingehende Anforderungen, die im nächsten Abschnitt beschrieben wird.

**Anmerkung:** Für eingehende TCP/IP-Anforderungen werden keine Eingangs- und Herkunftsüberprüfungen ausgeführt.

#### Zugehörige Konzepte:

- „Sicherheitsüberlegungen für Anwendungsserver (OS/390 und z/OS)“ auf Seite 99

## Endbenutzernamen - Anwendungsserver (OS/390 und z/OS)

Die vom Anwendungsrequester übergebene Benutzer-ID ist möglicherweise nicht im gesamten SNA-Netzwerk eindeutig. Der DB2-Anwendungsserver muss unter Umständen die Namensumsetzung für eingehende Anforderungen ausführen, um im gesamten SNA-Netzwerk eindeutige Endbenutzernamen erstellen zu können. Gleichermaßen muss der DB2-Anwendungsserver unter Umständen die Namensumsetzung für abgehende Anforderungen ausführen, um den an der Anwendung beteiligten sekundären Servern einen eindeutigen Endbenutzernamen zur Verfügung zu stellen.

Die Namensumsetzung für eingehende Anforderungen wird aktiviert, indem die Spalte USERNAMES in der Tabelle SYSIBM.LUNAMES bzw. SYSIBM.IPNAMES auf 'I' (Namensumsetzung für eingehende Anforderungen) oder 'B' (Namensumsetzung für eingehende und abgehende Anforderungen) gesetzt wird. Ist die Namensumsetzung für eingehende Anforderungen aktiviert, setzt DB2 die vom Anwendungsrequester gesendete Benutzer-ID und den Eigernamen des DB2-Plans um (wenn der Anwendungsrequester ein weiteres DB2-System ist).

Wenn der Anwendungsrequester eine Benutzer-ID und ein Kennwort mit dem APPC-Verb ALLOCATE sendet, werden die Benutzer-ID und das Kennwort vor dem Umsetzen der Benutzer-ID auf Gültigkeit überprüft. Die Spalte PASSWORD in der Tabelle SYSIBM.USERNAMES wird nicht für die Gültigkeitsprüfung des Kennworts verwendet. Statt dessen werden die Benutzer-ID und das Kennwort zur Gültigkeitsprüfung an das externe Sicherheitssystem (RACF oder ein äquivalentes Produkt) übergeben.

Bei der Prüfung der eingehenden Benutzer-ID im Verb ALLOCATE stellt DB2 Benutzerexits für die Berechtigungsüberprüfung zur Verfügung, die verwendet werden können, um eine Liste der sekundären Berechtigungs-IDs (AUTHIDs) bereitzustellen und zusätzliche Sicherheitsprüfungen auszuführen. Weitere Informationen hierzu finden Sie im Handbuch *DB2 for OS/390 Administration Guide*.

Der Prozess zur Namensumsetzung für eingehende Anforderungen sucht in der Tabelle SYSIBM.USERNAMES nach einer Zeile, die einem der in der folgenden Liste dargestellten Muster entsprechen muss (TYPE.AUTHID.LINKNAME):

1. I.AUTHID.LINKNAME – Ein bestimmter Endbenutzer von einem bestimmten Anwendungsrequester
2. I.AUTHID.leer – Ein bestimmter Endbenutzer von einem beliebigen Anwendungsrequester
3. I.leer.LINKNAME – Ein beliebiger Endbenutzer von einem bestimmten Anwendungsrequester

Wenn keine Zeile gefunden wird, wird der Fernzugriff verweigert. Wenn eine Zeile gefunden wird, wird der Fernzugriff zugelassen, und der Name des Endbenutzers wird in den in der Spalte NEWAUTHID zur Verfügung gestellten Wert geändert. Dabei gibt ein leerer Wert für NEWAUTHID an, dass der Name nicht geändert wird. Alle von DB2 ausgeführten Ressourcenberechtigungsprüfungen (z. B. SQL-Tabellenzugriffsrechte) werden an den umgesetzten Endbenutzernamen und nicht an den Originalbenutzernamen vorgenommen.

Wenn der DB2-Anwendungsserver einen Endbenutzernamen vom Anwendungsrequester empfängt, können durch die Funktion zur Namensumsetzung für eingehende Anforderungen mehrere Ziele erreicht werden:

- Sie können einen Endbenutzernamen so ändern, dass er eindeutig ist. So setzen beispielsweise die folgenden SQL-Anweisungen den Endbenutzernamen JONES auf dem Anwendungsrequester NEWYORK (LUNAME LUNYC) in einen anderen Namen (NYJONES) um.

```

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

```

Abbildung 19. Ändern eines Endbenutzernamens, damit er eindeutig ist

- Sie können den Endbenutzernamen ändern, um eine Gruppe von Endbenutzern durch einen einzelnen Namen zu repräsentieren. Beispielsweise könnten Sie alle Benutzer vom Anwendungsrequester NEWYORK (LUNAME LUNYC) durch den Benutzernamen NYUSER repräsentieren. Dadurch können Sie dem Namen NYUSER SQL-Zugriffsrechte erteilen und den SQL-Zugriff steuern, der den Benutzern des Systems NEWYORK erteilt wird.

```

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

```

Abbildung 20. Ändern des Endbenutzernamens, damit eine Gruppe von Endbenutzern durch einen einzelnen Namen repräsentiert wird

- Sie können die durch einen bestimmten Anwendungsrequester übertragenen Endbenutzernamen einschränken. Durch diese Verwendung der Umsetzung für Endbenutzernamen wird die Herkunftsüberprüfung ausgeführt. . Beispielsweise lassen die folgenden SQL-Anweisungen nur SMITH und JONES als Endbenutzernamen vom Anwendungsrequester NEWYORK zu. Allen anderen Namen wird der Zugriff verweigert, da sie nicht in der Tabelle SYSIBM.USERNAMES aufgelistet sind.

```

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', ' ', ' ');

```

Abbildung 21. Einschränken der von einem Anwendungsrequester übermittelten Endbenutzernamen

- Sie können beschränken, welche Anwendungsrequester eine Verbindung zum DB2-Anwendungsserver herstellen können. Dies ist eine weitere Funktion der

Herkunftsüberprüfung. Im folgenden Beispiel werden alle vom Anwendungsrequester NEWYORK (LUNYC) und dem Anwendungsrequester CHICAGO (LUCHI) gesendeten Endbenutzernamen akzeptiert. Anderen Anwendungsrequestern wird der Zugriff verweigert, da in der Standardzeile der Tabelle SYSIBM.LUNAMES die Namensumsetzung für alle eingehenden Anforderungen angegeben ist.

```

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', ' ', ' ');

```

Abbildung 22. Beschränken der Anwendungsrequester, die eine Verbindung herstellen können

#### Zugehörige Konzepte:

- „Sicherheitsüberlegungen für Anwendungsserver (OS/390 und z/OS)“ auf Seite 99

## Netzwerksicherheit - Anwendungsserver (OS/390 und z/OS)

Bei SNA-Verbindungen stellt LU 6.2 die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene
- Sicherheit auf Dialogebene
- Verschlüsselung

Für die Netzwerksicherheit muss nun nur noch die SNA-Sicherheit auf Dialogebene behandelt werden. Einige Aspekte der Sicherheit auf Dialogebene gelten nur für DB2-Anwendungsserver. Weitere Informationen hierzu finden Sie im Handbuch *DB2 for OS/390 Administration Guide*. Der DB2-Anwendungsserver spielt in der Netzwerksicherheit die folgenden beiden unterschiedliche Rollen:

- Als Requester für sekundäre Server ist der DB2-Anwendungsserver für das Absetzen von APPC-Anforderungen zuständig, die die für sekundäre Server erforderlichen Parameter der SNA-Sicherheit auf Dialogebene enthalten. Der DB2-Anwendungsserver verwendet die Spalte USERNAMES in der Tabelle SYSIBM.LUNAMES und der Tabelle SYSIBM.USERNAMES, um die Anforderungen der SNA-Sicherheit auf Dialogebene für alle sekundären Server zu definieren.
- Als Server für den Anwendungsrequester legt der DB2-Anwendungsserver die Anforderungen der SNA-Sicherheit auf Dialogebene für den Anwendungsrequester fest. DB2 verwendet die Spalte USERSECURITY der Tabelle SYSIBM.LUNAMES, um die für jeden Anwendungsrequester im Netzwerk erforderliche Dialogsicherheit zu ermitteln. In der Spalte USERSECURITY werden die folgenden Werte verwendet:

- C Hiermit wird angegeben, dass DB2 vom Anwendungsrequester bei jeder Anforderung für verteilte Datenbanken das Senden einer Benutzer-ID und eines Kennworts (LU 6.2 SECURITY=PGM) erfordert. Ist in der Spalte ENCRYPTPSWDS der Tabelle SYSIBM.LUNAMES der Wert 'Y' enthalten, geht DB2 davon aus, dass das Kennwort bereits in verschlüs-

seltem RACF<sup>®</sup>-Format vorliegt (dies ist nur für einen DB2-Anwendungsrequester möglich). Enthält die Spalte ENCRYPTPSWDS nicht den Wert 'Y', erwartet DB2 das Kennwort im LU 6.2-Standardformat (EBCDIC-Zeichendarstellung). In beiden Fällen übergibt DB2 die Werte für Benutzer-ID und Kennwort zur Gültigkeitsprüfung an das Sicherheitssystem. Das Sicherheitssystem muss die Prüfung der APPC-Benutzer-ID und des APPC-Kennworts zur Verfügung stellen, wie z. B. RACF. Weist das Sicherheitssystem das Paar aus Benutzer-ID und Kennwort zurück, wird der Zugriff auf die verteilten Datenbanken verweigert.

#### **Jeder andere Wert**

Hiermit wird angegeben, dass der Anwendungsrequester eine bereits überprüfte Benutzer-ID (LU 6.2 SECURITY=SAME) oder eine Benutzer-ID und ein Kennwort (LU 6.2 SECURITY=PGM) senden kann. Werden eine Benutzer-ID und ein Kennwort gesendet, verarbeitet DB2 sie wie für den Wert 'C' oben beschrieben. Ist in der Anforderung nur eine Benutzer-ID enthalten, wird das Sicherheitssystem aufgerufen, um den Benutzer zu überprüfen, sofern nicht die Tabelle sysusernames verwendet wird, um die eingehenden Benutzer-IDs zu verwalten.

Wenn eine Sicherheitsverletzung festgestellt wird, fordert LU 6.2 den DB2-Anwendungsserver auf, den Prüfcode der SNA-Sicherheitsstörung ('080F6051'X) an den Anwendungsrequester zurückzugeben. Da dieser Prüfcode die Fehlerursache nicht beschreibt, stellt DB2 die folgenden beiden Methoden zur Verfügung, um die Ursachen von Sicherheitsverletzungen in einer verteilten Umgebung aufzuzeichnen:

- Eine Nachricht DSNL030I mit der LUWID des Requesters und einem DB2-Ursachencode, der den Fehler beschreibt, wird angezeigt. DSNL030I enthält auch (sofern bekannt) die zurückgewiesene AUTHID, die von der Anwendungsanforderung gesendet wurde.
- In der NetView-Datenbank für Hardwareüberwachung wird ein Alert eingetragen, der die gleichen Informationen wie die Nachricht DSNL030I enthält.

#### **Zugehörige Konzepte:**

- „Sicherheitsüberlegungen für Anwendungsserver (OS/390 und z/OS)“ auf Seite 99

## **Sicherheit des Datenbankmanagers - Anwendungsserver (OS/390 und z/OS)**

Als Eigner der Datenbankressourcen steuert der DB2<sup>®</sup>Anwendungsserver die Datenbanksicherheitsfunktionen für SQL-Objekte, die sich auf dem DB2-Anwendungsserver befinden. Der Zugriff auf von DB2 verwaltete Objekte wird durch Zugriffsrechte gesteuert, die Benutzern durch den DB2-Administrator oder die Eigner der einzelnen Objekte erteilt werden. Der DB2-Anwendungsserver steuert die folgenden beiden grundlegenden Objektklassen:

- **Pakete** – Einzelne Endbenutzer erhalten mit Hilfe der DB2-Anweisung GRANT die Berechtigung zum Erstellen, Ersetzen und Ausführen von Paketen. Ist ein Endbenutzer Eigner eines Pakets, kann er das Paket direkt ausführen und ersetzen. Anderen Endbenutzern muss mit der Anweisung GRANT ausdrücklich die Berechtigung zum Ausführen eines Pakets auf dem DB2-Anwendungsserver erteilt werden. Die Berechtigung USE kann für einzelne Endbenutzer oder für PUBLIC erteilt werden. Wird sie für PUBLIC erteilt, können alle Endbenutzer das Paket ausführen.

Nach dem Binden einer Anwendung an DB2 enthält das Paket die im Anwendungsprogramm enthaltenen SQL-Anweisungen. Diese SQL-Anweisungen werden wie folgt klassifiziert:

### **Statisches SQL**

Statisches SQL bedeutet, dass die SQL-Anweisung und die SQL-Objekte, auf die in der Anweisung verwiesen wird, zu dem Zeitpunkt, zu dem die Anwendung an DB2 gebunden wird, bekannt sind. Der Ersteller des Pakets muss über die Berechtigung zum Ausführen für jede der statischen SQL-Anweisungen in dem Paket verfügen.

Wenn Endbenutzer die Berechtigung zum Ausführen eines Pakets erhalten, verfügen sie damit automatisch über die Berechtigung zum Ausführen aller statischen SQL-Anweisungen in dem Paket. Daher benötigen Endbenutzer keine DB2-Tabellenzugriffsrechte, wenn das von ihnen ausgeführte Paket ausschließlich statische SQL-Anweisungen enthält.

### **Dynamisches SQL**

Dynamisches SQL bezeichnet eine SQL-Anweisung, die vor der Ausführung des Pakets nicht bekannt ist. Dies bedeutet, dass die SQL-Anweisung von dem betreffenden Programm erstellt und mit der SQL-Anweisung PREPARE dynamisch an DB2 gebunden wird. Wenn ein Endbenutzer eine dynamische SQL-Anweisung ausführt, muss er über die erforderlichen Tabellenzugriffsrechte zum Ausführen der SQL-Anweisung verfügen. Da die SQL-Anweisung bei der Erstellung des Plans bzw. Pakets noch nicht bekannt ist, wird dem Endbenutzer die erforderliche Berechtigung vom Paketdesigner nicht automatisch erteilt.

- **SQL-Objekte** – Hierbei handelt es sich um Tabellen, Sichten, Synonyme oder Aliasnamen. DB2-Benutzern können verschiedene Berechtigungsstufen zum Erstellen, Löschen, Ändern oder Lesen einzelner SQL-Objekte erteilt werden. Diese Berechtigung ist für das Binden statischer SQL-Anweisungen und zum Ausführen dynamischer SQL-Anweisungen erforderlich.

Beim Erstellen eines Pakets kann mit der Option DISABLE/ENABLE gesteuert werden, welche DB2-Verbindungstypen das Paket ausführen können. Mit RACF® und DB2-Sicherheitsexitroutrinen kann Endbenutzern selektiv die Verwendung von DDF erlaubt werden. RLF kann verwendet werden, um Begrenzungen der Verarbeitungszeit für ferne Bindevorgänge und für die Ausführung dynamischer SQL-Anweisungen anzugeben.

Beispiel: Der Eigner eines DB2-Pakets mit dem Namen MYPKG heißt JOE. JOE kann SAL die Berechtigung zum Ausführen des Pakets erteilen, indem er die DB2-Anweisung GRANT USE absetzt. Wenn SAL das Paket ausführt, geschieht folgendes:

- DB2 prüft, ob SAL die Berechtigung USE für das Paket erteilt wurde.
- SAL kann alle statischen SQL-Anweisungen im Paket absetzen, da JOE über die zum Erstellen des Pakets erforderlichen Zugriffsrechte auf SQL-Objekte verfügt.
- Enthält das Paket dynamische SQL-Anweisungen, muss SAL über eigene SQL-Tabellenzugriffsrechte verfügen. Beispielsweise kann SAL SELECT \* FROM JOE.TABLE5 erst absetzen, nachdem SAL der Lesezugriff auf JOE.TABLE5 erteilt wurde.

### **Zugehörige Konzepte:**

- „Sicherheitsüberlegungen für Anwendungsserver (OS/390 und z/OS)“ auf Seite 99

## Sicherheitssystem - Anwendungsserver (OS/390 und z/OS)

Die Verwendung des Sicherheitssystems (RACF oder ein äquivalentes Produkt) durch den DB2<sup>®</sup>-Anwendungsserver hängt davon ab, wie die Funktion zur Namensumsetzung für eingehende Anforderungen in der Tabelle SYSIBM.LUNAMES definiert wurde.

- Wenn Sie für die Spalte USERNAMES 'T' oder 'B' angeben, ist die Namensumsetzung für eingehende Anforderungen aktiv, und DB2 nimmt an, dass der DB2-Administrator die Namensumsetzung für eingehende Anforderungen als Teil der Durchsetzung der Systemsicherheit ausführt. Das externe Sicherheitssystem wird nur aufgerufen, wenn der Anwendungsrequester eine Anforderung mit Benutzer-ID und Kennwort (SECURITY=PGM) sendet. Ihr Sicherheitssystem muss die Prüfung der APPC-Benutzer-ID und des APPC-Kennworts zur Verfügung stellen, wie z. B. RACF<sup>®</sup>.

Enthält die Anforderung vom Anwendungsrequester nur eine Benutzer-ID (SECURITY=SAME), wird das externe Sicherheitssystem nicht aufgerufen, da die Regeln für die Namensumsetzung für eingehende Anforderungen definieren, welche Benutzer eine Verbindung zum DB2-Anwendungsserver herstellen dürfen.

- Wenn Sie eine andere Angabe als 'T' oder 'B' für die Spalte USERNAMES vornehmen, werden die folgenden Überprüfungen des Sicherheitssystems ausgeführt:
  - Wird eine Anforderung für verteilte Datenbanken des Anwendungsrequesters empfangen, ruft DB2 das externe Sicherheitssystem auf, um die Gültigkeit der Benutzer-ID (und des Kennworts, sofern bereitgestellt) des Endbenutzers zu überprüfen.
  - Das externe Sicherheitssystem wird aufgerufen, um zu prüfen, ob der Endbenutzer über die Berechtigung zum Herstellen einer Verbindung zum DB2-Subsystem verfügt.
- In jedem Fall wird ein Benutzerexit für Berechtigungsüberprüfungen implementiert, um eine Liste der sekundären Berechtigungs-IDs bereitzustellen.

Weitere Informationen finden Sie im Handbuch *DB2 UDB for OS/390<sup>®</sup> and z/OS<sup>™</sup> Administration Guide*.

### Zugehörige Konzepte:

- „Sicherheitsüberlegungen für Anwendungsserver (OS/390 und z/OS)“ auf Seite 99

---

## Sicherheitsüberlegungen für Anwendungsserver (iSeries)

Wenn ein Anwendungsrequester eine Anforderung für verteilte Datenbanken an den iSeries<sup>™</sup>-Anwendungsserver weiterleitet, kann die Sicherheit in folgenden Bereichen eine Rolle spielen:

- Endbenutzernamen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Sicherheit von iSeries

### **Endbenutzernamen:**

Der Anwendungsrequester sendet eine Benutzer-ID zur Sicherheitsüberprüfung an den Anwendungsserver. Der auf dem iSeries-Anwendungsserver ausgeführte Job verwendet diese Benutzer-ID oder in einigen Fällen eine Standard-Benutzer-ID.

Der AS/400-Anwendungsserver stellt keine Umsetzung von Benutzer-IDs für eingehende Anforderungen zur Behebung von Konflikten zwischen Benutzer-IDs zur Verfügung, die nicht eindeutig sind, und gruppiert auch nicht mehrere Benutzer unter einer einzigen Benutzer-ID. Jede von einem Anwendungsrequester gesendete Benutzer-ID muss auf dem Anwendungsserver vorhanden sein. Ein Verfahren zur Gruppierung eingehender Anforderungen unter einer einzigen Benutzer-ID (mit gewissen Sicherheitseinbußen) ist das Angeben einer Standard-Benutzer-ID in einem Kommunikationseintrag des Subsystems, das die Startanforderungen für ferne Jobs verarbeitet. Informationen hierzu finden Sie in den Beschreibungen der Befehle ADDCMNE und CHGCMNE im Handbuch *AS/400 CL Reference*.

### **Sicherheit im SNA-Netzwerk:**

LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene
- Sicherheit auf Dialogebene
- Verschlüsselung (vom iSeries-System nicht unterstützt)

Der Anwendungsserver unter DB2<sup>®</sup> UDB für iSeries verwendet die Sicherheit auf Sitzungsebene in der selben Weise wie der Anwendungsrequester unter DB2 UDB für iSeries.

Der Anwendungsserver steuert die für den Datenaustausch verwendeten SNA-Dialogebenen. Der Parameter SECURELOC in der APPC-Einheitenbeschreibung und der Wert für den Standortschutz in der Liste der fernen APPN-Standorte legen fest, was vom Anwendungsrequester für den Datenaustausch akzeptiert wird.

Die folgenden Optionen für die SNA-Sicherheit auf Dialogebene sind verfügbar:

#### **SECURITY=SAME**

Wird auch als bereits geprüfte Sicherheit bezeichnet. Nur die Benutzer-ID des Anwendungsbenedutzers ist für den Anwendungsserver erforderlich. Es wird kein Kennwort übermittelt. Diese Stufe der Dialogsicherheit auf dem Anwendungsserver wird aktiviert, indem der Parameter SECURELOC in der APPC-Einheitenbeschreibung auf \*YES gesetzt wird oder indem der Wert für den Standortschutz in der Liste ferner APPN-Standorte auf \*YES eingestellt wird.

#### **SECURITY=PGM**

Bewirkt, dass sowohl Benutzer-ID als auch Kennwort für den Anwendungsserver für die Gültigkeitsprüfung erforderlich sind. Diese Stufe der Dialogsicherheit auf dem Anwendungsserver wird aktiviert, indem die standardmäßige Benutzer-ID im Kommunikationseintrag des iSeries-Subsystems auf \*NONE (keine standardmäßige Benutzer-ID) und der Parameter SECURELOC oder der Wert für den Standortschutz auf \*NO gesetzt werden.

#### **SECURITY=NONE**

Ein Anwendungsserver erwartet keine Benutzer-ID und kein Kennwort. Der Datenaustausch wird durch ein Standardbenutzerprofil auf dem Anwendungsserver zugelassen. Diese Option wird aktiviert, indem ein

Standardbenutzerprofil im Kommunikationsverzeichnis des Subsystems und der Wert \*NO für den Parameter SECURELOC oder den Wert für den Standortschutz angegeben werden.

Für SNA/DS (SNA Distribution Services) ist eine Standardbenutzer-ID erforderlich. Daher sollte SNA/DS im Normalfall (d. h. wenn keine Standardbenutzer-ID für DRDA<sup>®</sup>-Anwendungen erwünscht ist) über ein eigenes Subsystem verfügen.

Auf eine Methode zur Gruppierung eingehender Jobstartanforderungen unter einer einzigen Benutzer-ID wurde bereits im Abschnitt zu Endbenutzernamen hingewiesen. Bei dieser Methode wird die vom Anwendungsrequester gesendete Benutzer-ID nicht überprüft. Der Job auf dem Anwendungsserver wird mit einer Standardbenutzer-ID gestartet, und der Benutzer, der die Verbindung vom Anwendungsserver eingeleitet hat, erhält auch dann eine Zugriffsberechtigung für den Anwendungsserver, wenn die übermittelte Benutzer-ID nur über eingeschränkte Berechtigungen verfügt. Dies erfolgt, indem der Anwendungsserver als nicht geschützter Standort definiert, im Kommunikationseintrag des iSeries-Subsystems eine Standardbenutzer-ID angegeben und der Anwendungsrequester so konfiguriert wird, dass beim Herstellen der Verbindung nur eine Benutzer-ID gesendet wird. Wird ein Kennwort gesendet, wird die dazugehörige Benutzer-ID anstelle der Standardbenutzer-ID verwendet.

Die Kommunikationseinträge des iSeries-Subsystems unterscheiden sich durch die zum Starten des Datenaustauschs verwendeten Einheiten- und Modusnamen. Durch Zuordnen unterschiedlicher Standardbenutzer-IDs zu verschiedenen Paaren aus Einheit und Modus können Benutzer nach der Art ihrer Kommunikation mit dem Anwendungsserver gruppiert werden.

Das iSeries-System stellt außerdem eine Netzwerksicherheitseinrichtung zur Verfügung, die nur für die Verwaltung verteilter Datenbanken und verteilter Dateien verwendet wird. Ein Netzwerkattribut für diese Arten von Systemzugriff weist entweder alle Zugriffsversuche zurück oder bewirkt, dass die Sicherheit vom System auf der Grundlage einzelner Objekte gesteuert wird.

#### **Sicherheit im TCP/IP-Netzwerk:**

Mit dem Befehl **CRTDDMTCPA** kann angegeben werden, dass ein Server TCP/IP-Verbindungsanforderungen ohne Kennwort akzeptieren soll.

#### **Sicherheit des Datenbankmanagers:**

Alle Sicherheitseinrichtungen werden von der OS/400<sup>®</sup>-Sicherheitsfunktion gesteuert.

#### **Systemsicherheit:**

Das iSeries-System verfügt nicht über ein externes Sicherheitssystem. Alle Sicherheitseinrichtungen werden von der OS/400-Sicherheitsfunktion gesteuert, die integraler Bestandteil des Betriebssystems ist. Das Betriebssystem steuert die Vergabe von Berechtigungen für alle Objekte im System, wie beispielsweise Programmen, Paketen, Tabellen, Sichten und Objektgruppen.

Der Anwendungsserver steuert die Vergabe von Berechtigungen für die Objekte, die sich auf dem Anwendungsserver befinden. Die Sicherheitssteuerung für diese Objekte richtet sich danach, von welcher Benutzer-ID der Job auf dem

Anwendungsserver gestartet wird. Diese Benutzer-ID wird wie im Abschnitt zu den Endbenutzernamen beschrieben ermittelt.

Die Objektsicherheit kann mit Hilfe der CL-Befehle für Objektberechtigungen oder mit den SQL-Anweisungen GRANT und REVOKE verwaltet werden. Zu den CL-Befehlen für Objektberechtigungen gehören der Befehl zum Erteilen von Objektberechtigungen (GRTOBJAUT) und der Befehl zum Entziehen von Objektberechtigungen (RVKOBJAUT). Diese CL-Befehle gelten für jedes Objekt auf dem System. Die Anweisungen GRANT und REVOKE gelten nur für SQL-Objekte (Tabellen, Sichten und Pakete). Verwenden Sie zum Ändern der Berechtigungen für andere Objekte (z. B. Programme und Objektgruppen) die Befehle GRTOBJAUT und RVKOBJAUT.

Beim Erstellen von Objekten im System wird eine Standardberechtigung vergeben. Die Benutzer-ID, von der Tabellen, Sichten und Pakete erstellt werden, erhält sämtliche Berechtigungen. Alle anderen Benutzer-IDs (die Öffentlichkeit (PUBLIC)) erhalten die selben Berechtigungen, die sie auch für die Objektgruppe oder Bibliothek haben, in der das betreffende Objekt erstellt wird.

Die Berechtigungen für Objekte, auf die innerhalb des Pakets durch statische oder dynamische Anweisungen verwiesen wird, werden zur Laufzeit des Pakets überprüft. Wenn der Ersteller des Pakets keine Berechtigung für das Objekt hat, auf das verwiesen wird, werden beim Erstellen des Pakets entsprechende Warnungen zurückgegeben. Zur Ausführungszeit erhält der Benutzer, von dem das Paket ausgeführt wird, die Berechtigung des Paketerstellers. Wenn der Ersteller des Pakets Zugriffsberechtigung für eine Tabelle hat, der ausführende Benutzer jedoch nicht über diese Berechtigung verfügt, erhält dieser Benutzer automatisch die Berechtigungen des Paketerstellers, d. h. er kann nun ebenfalls auf die Tabelle zugreifen.

Weitere Informationen zur Systemsicherheit finden Sie im Handbuch *OS/400 Security - Reference*.

#### **Zugehörige Tasks:**

- „Erteilen und Entziehen von Berechtigungen:“ auf Seite 124

---

## **Sicherheitsüberlegungen für Anwendungsserver (VM)**

Wenn ein Anwendungsrequester eine Anforderung für eine verteilte Datenbank an den Anwendungsserver unter DB2<sup>®</sup> für VM weiterleitet, können dabei die folgenden Sicherheitsaspekte eine Rolle spielen:

- Endbenutzernamen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Von einem externen Sicherheitssystem implementierte Sicherheit

#### **Endbenutzernamen:**

In SQL und LU 6.2 wird jedem Endbenutzer eine Benutzer-ID mit einer Länge von 1 bis 8 Byte zugeordnet. Diese Benutzer-ID muss zwar innerhalb eines bestimmten Betriebssystems, jedoch nicht unbedingt im gesamten SNA-Netzwerk eindeutig sein. Zur Behebung von Namenskonflikten kann DB2 für VM optional die von AVS bereitgestellte Umsetzungsfunktion für Benutzer-IDs verwenden, allerdings nur unter folgenden Bedingungen:

- Der Anwendungsserver unter DB2 für VM muss in einer VM/ESA<sup>®</sup>-Umgebung ausgeführt werden
- Die eingehende Verbindungsanforderung muss über einen AVS-Gateway weitergeleitet werden
- Der Partner-Anwendungsrequester muss die Dialogsicherheit SECURITY=SAME verwenden (in der SNA-Terminologie auch als *bereits geprüft* bezeichnet)

Wenn eine Verbindung über AVS mit der Option SECURITY=SAME an einen Server weitergeleitet wird, ist die AVS-Umsetzung für Benutzer-IDs erforderlich. Der auf der AVS-Maschine abgesetzte Befehl AGW ADD USERID muss den Benutzern, die über eine bestimmte ferne LU oder einen bestimmten AVS-Gateway eine Verbindung anfordern, die Zugriffsberechtigung erteilen. Es muss eine Zuordnung für alle eingehenden LUs und Benutzer-IDs vorhanden sein, die mit SECURITY=SAME eine Verbindung herstellen. Der Befehl ist flexibel anwendbar, d. h. Sie können alle Benutzer-IDs von einer bestimmten LU bzw. allen fernen LUs generisch akzeptieren. Sie haben aber auch die Möglichkeit, nur eine bestimmte Gruppe von Benutzer-IDs von einer bestimmten LU zu akzeptieren.

Wenn Sie den Befehl AGW ADD USERID zum Berechtigen der eingehenden (bereits geprüften) Benutzer-IDs auf der lokalen AVS-Maschine verwenden, wird vom Host keine Gültigkeitsprüfung durchgeführt. Dies bedeutet, dass die Verbindung auch dann akzeptiert wird, wenn die berechtigte ID auf dem Host möglicherweise nicht vorhanden ist.

Die aktuelle Berechtigung der AVS-Benutzer-ID kann auf die folgenden beiden Arten geändert werden:

- Durch Stoppen von AVS mit dem Befehl AGW STOP; dadurch wird die Berechtigung der Benutzer-ID vollständig auf Leerwerte gesetzt.
- Durch Löschen der Benutzer-ID mit dem Befehl AGW DELETE USERID

Am Beispiel identischer Benutzer-IDs in verschiedenen Städten wird deutlich, wie die AVS-Umsetzungsfunktion einen Namenskonflikt beheben kann. Angenommen im System von Toronto gibt es eine Benutzer-ID JONES, und im System von Montreal existiert ein weiterer Benutzer mit der selben ID. Wenn JONES in Montreal auf Daten im System von Toronto zugreifen möchte, kann durch folgende Maßnahmen im System von Toronto der mögliche Namenskonflikt behoben und verhindert werden, dass JONES in Montreal die für JONES in Toronto erteilten Zugriffsberechtigungen verwenden kann:

1. Der AVS-Bediener muss mit dem Befehl AGW ADD USERID die ID des Benutzers in Montreal in eine lokale Benutzer-ID umsetzen. Beispiel: Wenn der Bediener den Befehl AGW ADD USERID MTLGATE JONES MONTJON absetzt, wird der Benutzer in Montreal im System von Toronto als MONTJON identifiziert. Wenn alle Benutzer in Montreal (über die ferne LU MTLGATE) die Verbindung herstellen können und lokal anhand ihrer fernen Benutzer-IDs identifiziert werden, muss der Bediener den Befehl AGW ADD USERID MTLGATE \* = absetzen. Diese AVS-Befehle können auch dem AVS-Profil hinzugefügt werden, damit sie beim Starten von AVS automatisch ausgeführt werden.
2. Der Datenbankadministrator muss mit dem Befehl GRANT von DB2 für VM eine Reihe von Berechtigungen speziell für die umgesetzte Benutzer-ID (in diesem Fall für MONTJON) erteilen.

Diese Aktionen können auch auf dem System von Montreal ausgeführt werden, um sicherzustellen, dass JONES in Toronto beim Zugriff auf ferne Daten im System von Montreal die für JONES in Montreal erteilten Berechtigungen nicht benutzen kann.

Die AVS-Befehle zur Unterstützung der Umsetzung für Benutzer-IDs werden im Handbuch *VM/ESA Connectivity Planning, Administration, and Operation* beschrieben.

### **Netzwerksicherheit:**

LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene
- Sicherheit auf Dialogebene
- Verschlüsselung

Der Anwendungsserver unter DB2 für VM verwendet die Sicherheit auf Sitzungsebene in der selben Weise wie der Anwendungsrequester unter DB2 für VM.

Der Anwendungsrequester kann entweder eine bereits geprüfte Benutzer-ID (SECURITY=SAME) oder eine Benutzer-ID mit Kennwort (SECURITY=PGM) senden. Wenn eine Benutzer-ID mit Kennwort gesendet wird, überprüft CP, RACF oder ein gleichwertiges Produkt diese Angaben anhand des VM-Verzeichnisses auf dem Anwendungsserver-Host. Schlägt die Gültigkeitsprüfung fehl, wird die Verbindungsanforderung zurückgewiesen; andernfalls wird sie akzeptiert. Enthält die Anforderung nur eine Benutzer-ID, akzeptiert DB2 für VM die Anforderung, ohne die Benutzer-ID auf ihre Gültigkeit zu prüfen.

**Anmerkung:** DB2 für VM stellt keine Verschlüsselungsfunktion bereit, weil VM/ESA Verschlüsselung nicht unterstützt.

### **Sicherheit des Datenbankmanagers:**

Der Anwendungsserver unter DB2 für VM überprüft, ob die von VM angegebene Benutzer-ID über die Berechtigung CONNECT zum Zugriff auf die Datenbank verfügt, und weist die Verbindung zurück, wenn diese Berechtigung nicht vorliegt.

Als Eigner der Datenbankressourcen steuert der Anwendungsserver unter DB2 für VM die Datenbanksicherheitsfunktionen für SQL-Objekte, die sich auf dem Anwendungsserver unter DB2 für VM befinden. Der Zugriff auf die von DB2 für VM verwalteten Objekte wird durch eine Reihe von Zugriffsrechten gesteuert, die der Administrator des Systems mit DB2 für VM oder der Eigner des jeweiligen Objekts den Benutzern erteilen kann. Der Anwendungsserver unter DB2 für VM steuert die folgenden beiden Objektklassen:

- **Pakete:** Einzelne Endbenutzer erhalten mit Hilfe der Anweisung GRANT von DB2 für VM die Berechtigung zum Erstellen, Ersetzen und Ausführen von Paketen. Wenn ein Endbenutzer ein Paket erstellt, erhält dieser Benutzer automatisch die Berechtigung zum Ausführen und Ersetzen eines Pakets. Anderen Endbenutzern muss mit der Anweisung GRANT EXECUTE ausdrücklich die Berechtigung zum Ausführen eines Pakets auf dem Anwendungsserver unter DB2 für VM erteilt werden. Das Zugriffsrecht RUN kann für einzelne Endbenutzer oder für PUBLIC erteilt werden, d. h. alle Benutzer dürfen das Paket ausführen.

Nach der Vorverarbeitung einer Anwendung in DB2 für VM enthält das Paket die im Anwendungsprogramm enthaltenen SQL-Anweisungen. Diese SQL-Anweisungen werden wie folgt klassifiziert:

- **Statisches SQL:** Dies bedeutet, dass die SQL-Anweisung und die SQL-Objekte, auf die in der Anweisung verwiesen wird, der Anwendung zum Zeitpunkt der Vorverarbeitung bekannt sind. Der Ersteller des Pakets muss über die Berechtigung zum Ausführen für jede der statischen SQL-Anweisungen in dem Paket verfügen.

Wenn ein Endbenutzer das Recht zum Ausführen eines Pakets erhält, verfügt er damit automatisch über die Berechtigung zum Ausführen aller statischen SQL-Anweisungen in dem Paket. Dies bedeutet, dass Endbenutzer keine Tabellenzugriffsrechte von DB2 für VM benötigen, wenn das Paket ausschließlich statische SQL-Anweisungen enthält.

- **Dynamisches SQL:** Bezeichnet eine SQL-Anweisung, die vor der Ausführung des Pakets nicht bekannt ist. Die SQL-Anweisung wird von dem betreffenden Programm erstellt und durch die SQL-Anweisung PREPARE oder die Anweisung EXECUTE IMMEDIATE für DB2 für VM dynamisch vorverarbeitet. Wenn ein Endbenutzer eine dynamische SQL-Anweisung ausführt, muss er über die erforderlichen Tabellenzugriffsrechte zum Ausführen der SQL-Anweisung verfügen. Da die SQL-Anweisung beim Erstellen des Pakets noch nicht bekannt ist, wird dem Endbenutzer die erforderliche Berechtigung vom Paketeigner nicht automatisch erteilt.
- **SQL-Objekte:** Dies können Tabellen, Sichten und Synonyme sein. Benutzern von DB2 für VM können verschiedene Berechtigungsstufen zum Erstellen, Löschen, Ändern oder Lesen einzelner SQL-Objekte erteilt werden. Diese Berechtigung ist für die Vorverarbeitung statischer SQL-Anweisungen und zum Ausführen dynamischer SQL-Anweisungen erforderlich.

#### Sicherheitssystem:

Die Verwendung dieses Subsystems durch den Anwendungsserver unter DB2 für VM ist optional. Wenn der Anwendungsserver die Identität des LU-Namens des Anwendungsrequesters überprüfen muss, ruft VTAM<sup>®</sup> das Sicherheitssystem auf, um den Datenaustausch für die Partner-LU-Prüfung auszuführen. Die Entscheidung über die Ausführung der Partner-LU-Prüfung wird unter Berücksichtigung des Werts getroffen, der im Parameter VERIFY der VTAM-Anweisung APPL für den Gateway angegeben ist, über den der Anwendungsserver unter DB2 für VM eingehende Anforderungen für verteilte Datenbanken empfängt.

Das Sicherheitssystem kann von CP auch aufgerufen werden, um die Benutzer-ID und das Kennwort zu überprüfen, die vom Anwendungsrequester gesendet wurden. Wenn RACF<sup>®</sup> als Sicherheitssystem verwendet wird und Sie nicht über ein RACF-Systemprofil verfügen, wird die Gültigkeitsprüfung von RACF ausgeführt. Wenn Sie über ein RACF-Systemprofil (z. B. RACFPROF) verfügen, führen Sie die folgenden Anweisungen aus, um diese Gültigkeitsprüfung von RACF anzufordern:

```
RALTER VMXEVT RACFPROF DELMEM (APPCPWL/NOCTL
```

```
RALTER VMXEVT RACFPROF ADDMEM (APPCPWL/CTL
```

```
SETEVT REFRESH RACFPROF
```

#### Zugehörige Konzepte:

- „DB2 für VM“ auf Seite 82
- „Sicherheitsüberlegungen für Anwendungsrequester (VM)“ auf Seite 124

#### Zugehörige Tasks:

- „Definieren von DB2 als Anwendungsserver (VM)“ auf Seite 67

---

## Sicherheitsüberlegungen für Anwendungsserver (VSE)

Der Anwendungsserver unter DB2<sup>®</sup> für VSE ist im Hinblick auf die systemübergreifende Kommunikationssicherheit von CICS<sup>®</sup> abhängig. CICS stellt die folgenden Sicherheitsstufen zur Verfügung:

- Bindezeitsicherheit

Dies ist die CICS-Implementierung der LU-LU-Prüfung auf SNA-LU 6.2-Sitzungsebene. Die Implementierung der Bindezeitsicherheit ist in der LU 6.2-Architektur optional. Auf der Seite des Anwendungsservers kann sie beim Definieren einer Verbindung zum Anwendungsrequester durch Angeben des Parameters BINDPASSWORD im Befehl CEDA DEFINE CONNECTION aktiviert werden. Auf der Seite des Anwendungsrequesters muss die Partner-LU, die den Anwendungsrequester bedient, ebenfalls Bindezeitsicherheit unterstützen und dasselbe Kennwort für die Partner-LU-Prüfung verwenden.

Die Bindezeitsicherheit kann dazu verwendet werden, ferne Systeme, die nicht über die entsprechende Berechtigung verfügen, daran zu hindern, Sitzungen mit CICS einzurichten (zu binden).

- Verbindungssicherheit

Durch die Verbindungssicherheit kann ein fernes System (und der darauf befindliche DRDA<sup>®</sup>-Anwenderrequester) auf die Zuordnung einer bestimmten Gruppe von AXE-Transaktionen begrenzt werden.

Beispielsweise könnten Sie zwei AXE-Transaktionen definieren: AXE2 mit Sicherheitsschlüssel 2 und AXE3 mit Sicherheitsschlüssel 3. Anwendungsrequestern eines fernen Systems könnte nun die Bedienersicherheit 3 (z. B. mit dem Parameter OPERSECURITY im Befehl CEDA DEFINE SESSION) zugeordnet werden, so dass sie nur eine Verbindung zu AXE3 herstellen können. Dabei könnte AXE3 keine Berechtigung für privilegierten Zugriff auf den Server haben, während AXE2 privilegierten Zugriff erhält.

- Benutzersicherheit

Dies ist die CICS-Implementierung der SNA LU 6.2-Sicherheit auf Dialogebene, die die Identifikationsprüfung für Endbenutzer zur Verfügung stellt.

Bei der Benutzersicherheit wird die Benutzer-ID anhand der CICS-Anmeldetabelle (DFHSNT) geprüft, bevor eine Anforderung zum Starten eines Dialogs akzeptiert wird. Beispielsweise dürfen DRDA-Anwenderrequester, die nicht in der CICS-Anmeldetabelle definiert sind, keine Verbindung zu einer AXE-Transaktion herstellen, um einen Dialog mit dem Server unter DB2 für VSE zu starten. Die Benutzersicherheitsstufe für ein fernes System kann mit dem Parameter ATTACHSEC im Befehl CEDA DEFINE CONNECTION aktiviert werden. Die folgenden drei Stufen der Verbindungssicherheit stehen zur Verfügung:

- LOCAL: Wird von DRDA nicht unterstützt.
- IDENTIFY: Entspricht SECURITY=SAME (oder: bereits definiert) in der LU 6.2-Terminologie. Bei dieser Sicherheitsstufe „vertraut“ CICS darauf, dass das ferne System eine Benutzerprüfung durchführt, bevor Dialoganforderungen für den Server unter DB2 für VSE akzeptiert werden. Bei der CICS-Anmeldung muss nur die Benutzer-ID angegeben werden. Wird jedoch zusätzlich ein Kennwort angegeben, führt CICS die Anmeldung mit dem Kennwort aus.
- VERIFY: Entspricht SECURITY=PGM in der LU 6.2-Terminologie. Bei dieser Sicherheitsstufe erwartet CICS, dass vom fernen System beim Zuordnen des Dialogs sowohl die Benutzer-ID als auch das Kennwort übermittelt werden. Die Verbindung wird zurückgewiesen, wenn kein Kennwort angegeben wird.

- Verbindliche SNA LU 6.2-Verschlüsselung auf Sitzungsebene. Diese Sicherheitsstufe wird nicht unterstützt.

Der Anwendungsserver ist für die Verwaltung der Datenbankressourcen zuständig und legt deshalb auch fest, welche Netzwerksicherheitseinrichtungen vom Anwendungsrequester bereitgestellt werden müssen. Beispielsweise müssen Sie bei Verwendung eines Anwendungsrequesters unter DB2 für VM die Anforderungen für Dialogsicherheit des Anwendungsservers im Kommunikationsverzeichnis des Anwendungsrequesters eintragen, indem Sie den entsprechenden Wert für die Kennung :security definieren. Dies wird in Abb. 23 dargestellt:

```

:nick.VSE1      :tpn.TOR3
                :luname.TORGATE VSEGATE
                :modename.IBMRDB
                :security.PGM
                :userid.SALESMGR
                :password.PROFIT
                :dbname.TORONTO3

Dabei gilt: TOR3   - Auf Datenbank TORONTO3 abgebildete Transaktions-ID
TORGATE  - VM/APPC-Gateway
VSEGATE  - APPLID der als Gateway zu TORONTO3 verwendeten
           CICS/VSE®-Partition
SALESMGR/PROFIT - USERID/PASSWORD definiert in DFHSNT von
                VSEGATE und berechtigt in TORONTO3
TORONTO3 - Der im Startparameter DBNAME angegebene Name
           für den Start des Anwendungsservers unter DB2
           für VSE (oder Name der Standarddatenbank aus dem
           Verzeichnis DBNAME bei Übergehen von DBNAME beim
           Start)

```

Abbildung 23. Beispieleintrag in CMS-Kommunikationsverzeichnis

### Sicherheit des Datenbankmanagers:

Die Benutzer-ID-Umsetzung wird vom VSE-Anwendungsserver nicht unterstützt. CICS verwendet die vom Requester übermittelte Benutzer-ID unverändert.

Sobald die Transaktion AXE von einem Anwendungsrequester gestartet wurde, fragt sie die Benutzer-ID von CICS ab und leitet sie an den Server unter DB2 für VSE weiter. Zum Einstellen der erforderlichen Benutzerberechtigungsstufe für Datenbankressourcen müssen Sie die Benutzer-ID im Katalog SYSTEM.SYSUS-ERAUTH von DB2 für VSE aktualisieren.

Der Anwendungsserver unter DB2 für VSE überprüft, ob die von CICS angegebene Benutzer-ID über die Berechtigung CONNECT zum Zugriff auf die Datenbank verfügt, und weist die Verbindung zurück, wenn diese Berechtigung nicht vorliegt.

Als Eigner der Datenbankressourcen steuert der Anwendungsserver unter DB2 für VSE die Datenbanksicherheitsfunktionen für SQL-Objekte, die sich auf dem Anwendungsserver unter DB2 für VSE befinden. Der Zugriff auf die von DB2 für VSE verwalteten Objekte wird durch eine Reihe von Zugriffsrechten gesteuert, die der Systemadministrator von DB2 für VSE oder der Eigner des jeweiligen Objekts den Benutzern erteilen kann. Der Anwendungsserver unter DB2 für VSE steuert die folgenden beiden Objektklassen:

- **Pakete:** Einzelne Endbenutzer erhalten mit Hilfe der Anweisung GRANT von DB2 für VSE die Berechtigung zum Erstellen, Ersetzen und Ausführen von Paketen. Wenn ein Endbenutzer ein Paket erstellt, erhält dieser Benutzer automatisch die Berechtigung zum Ausführen und Ersetzen eines Pakets.

Anderen Endbenutzern muss mit der Anweisung `GRANT EXECUTE` ausdrücklich die Berechtigung zum Ausführen eines Pakets auf dem Anwendungsserver unter DB2 für VSE erteilt werden. Das Zugriffsrecht `RUN` kann für einzelne Endbenutzer oder für `PUBLIC` erteilt werden, d. h. alle Benutzer dürfen das Paket ausführen.

Nach der Vorverarbeitung einer Anwendung in DB2 für VSE enthält das Paket die im Anwendungsprogramm enthaltenen SQL-Anweisungen. Diese SQL-Anweisungen werden wie folgt klassifiziert:

- **Statisches SQL:** Dies bedeutet, dass die SQL-Anweisung und die SQL-Objekte, auf die in der Anweisung verwiesen wird, der Anwendung zum Zeitpunkt der Vorverarbeitung bekannt sind. Der Ersteller des Pakets muss über die Berechtigung zum Ausführen für jede der statischen SQL-Anweisungen in dem Paket verfügen.

Wenn ein Endbenutzer das Recht zum Ausführen eines Pakets erhält, verfügt er damit automatisch über die Berechtigung zum Ausführen aller statischen SQL-Anweisungen in dem Paket. Dies bedeutet, dass Endbenutzer keine DB2-Tabellenzugriffsrechte auf dem VSE-System benötigen, wenn das Paket ausschließlich statische SQL-Anweisungen enthält.

- **Dynamisches SQL:** Bezeichnet eine SQL-Anweisung, die vor der Ausführung des Pakets nicht bekannt ist. Die SQL-Anweisung wird von dem betreffenden Programm erstellt und durch die Anweisung `SQL PREPARE` oder die Anweisung `EXECUTE IMMEDIATE` für DB2 für VSE dynamisch vorverarbeitet. Wenn ein Endbenutzer eine dynamische SQL-Anweisung ausführt, muss er über die erforderlichen Tabellenzugriffsrechte zum Ausführen der SQL-Anweisung verfügen. Da die SQL-Anweisung beim Erstellen des Pakets noch nicht bekannt ist, wird dem Endbenutzer die erforderliche Berechtigung vom Paketeigner nicht automatisch erteilt.
- **SQL-Objekte:** Dies können Tabellen, Sichten und Synonyme sein. Benutzern von DB2 für VSE können verschiedene Berechtigungsstufen zum Erstellen, Löschen, Ändern oder Lesen einzelner SQL-Objekte erteilt werden. Diese Berechtigung ist für die Vorverarbeitung statischer SQL-Anweisungen und zum Ausführen dynamischer SQL-Anweisungen erforderlich.

Eine Beschreibung des privilegierten Zugriffs von fernen Anwendungsrequestern auf den Anwendungsserver finden Sie im Handbuch *DB2 Server for VSE System Administration*.

Informationen zum Aktivieren der Verbindungssicherheit finden Sie im Handbuch *CICS on Open Systems: Intercommunication Guide*.

#### **Zugehörige Konzepte:**

- „DB2 für VSE“ auf Seite 94

#### **Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsserver (VSE)“ auf Seite 59

---

## Kapitel 13. Sicherheitsüberlegungen für Anwendungsrequester

---

### Sicherheitsüberlegungen für Anwendungsrequester (OS/390 und z/OS)

Wenn ein fernes System die Verarbeitung verteilter Datenbanken im Auftrag einer SQL-Anwendung ausführt, muss es in der Lage sein, die Sicherheitsanforderungen des Anwendungsrequesters, des Anwendungsservers und des verwendeten Netzwerks zu erfüllen. Diese Anforderungen betreffen einen oder mehrere der folgenden Bereiche:

- Endbenutzernamen
- Netzwerksicherheit
- Sicherheit des Datenbankmanagers
- Sicherheitssystem

#### Zugehörige Konzepte:

- „DB2 für OS/390 und z/OS“ auf Seite 73
- „Sicherheitsüberlegungen für Anwendungsserver (OS/390 und z/OS)“ auf Seite 99

#### Zugehörige Tasks:

- „Definieren von DB2 als Anwendungsrequester (OS/390 und z/OS)“ auf Seite 25

---

### Weitere Konzepte

#### Endbenutzernamen - Anwendungsrequester (OS/390 und z/OS)

Auf OS/390<sup>®</sup> und z/OS-Systemen wird jedem Endbenutzer eine *Benutzer-ID* aus 1 bis 8 Zeichen zugeordnet. Der Wert dieser Benutzer-ID muss zwar innerhalb eines bestimmten OS/390- und z/OS-Systems, jedoch nicht unbedingt im gesamten Netzwerk eindeutig sein.

Beispielsweise kann es im System NEWYORK einen Benutzer mit dem Namen JONES und im System DALLAS einen weiteren Benutzer dieses Namens geben. Wenn diese beiden Benutzer die selbe Person sind, entsteht dadurch kein Konflikt. Ist jedoch der Benutzer JONES in DALLAS nicht identisch mit dem Benutzer JONES in NEWYORK, kann das SNA-Netzwerk (und können folglich auch die verteilten Datenbanksysteme innerhalb dieses Netzwerks) den Benutzer JONES in NEWYORK nicht von dem Benutzer JONES in DALLAS unterscheiden. Wird diese Situation nicht durch geeignete Maßnahmen verhindert, können diese beiden Benutzer die Berechtigungen des jeweils anderen benutzen.

Zur Vermeidung solcher Namenskonflikte unterstützt DB2® die Umsetzung für Endbenutzernamen. Wenn eine Anwendung auf dem DB2-Anwendungsrequisiter eine Anforderung an eine verteilte Datenbank richtet, führt DB2 die Umsetzung für Namen aus, wenn in der Kommunikationsdatenbank die *Namensumsetzung für abgehende Anforderungen* als erforderlich angegeben ist. Ist die Namensumsetzung für abgehende Anforderungen ausgewählt, erzwingt DB2 stets, dass mit jeder abgehenden Anforderung für verteilte Datenbanken ein Kennwort gesendet wird.

Die Namensumsetzung für abgehende Anforderungen in DB2 wird aktiviert, indem die Spalte USERNAMES in der Tabelle SYSIBM.LUNAMES bzw. SYSIBM.IPNames auf 'O' oder 'B' gesetzt wird. Wenn USERNAMES auf 'O' gesetzt ist, wird die Umsetzung von Endbenutzernamen für abgehende Anforderungen ausgeführt. Wenn USERNAMES auf 'B' gesetzt ist, wird die Umsetzung von Endbenutzernamen für eingehende und abgehende Anforderungen ausgeführt.

Da Berechtigungen in DB2 sowohl von der Benutzer-ID des Endbenutzers als auch von der Benutzer-ID des Plan- bzw. Paketeigners von DB2 abhängen, wird der Umsetzungsprozess des Endbenutzernamens für die Benutzer-ID des Endbenutzers, die Benutzer-ID des Planeigners und die Benutzer-ID des Paketeigners ausgeführt.<sup>4</sup> Der Umsetzungsprozess für Namen durchsucht die Tabelle SYSIBM.USERNAMES in der folgenden Reihenfolge nach einer Zeile, die einem der folgenden Muster (TYPE.AUTHID.LINKNAME) entspricht:

1. O.AUTHID.LINKNAME – Eine Umsetzungsregel für einen bestimmten Endbenutzer eines bestimmten Partnersystems
2. O.AUTHID.leer – Eine Umsetzungsregel für einen bestimmten Endbenutzer eines beliebigen Partnersystems
3. O.leer.LINKNAME – Eine Umsetzungsregel für einen beliebigen Benutzer eines bestimmten Partnersystems

Wird keine übereinstimmende Zeile gefunden, wird die Anforderung für verteilte Datenbanken von DB2 zurückgewiesen. Wird eine Zeile gefunden, wird der Wert in der Spalte NEWAUTHID als Berechtigungs-ID verwendet. (Ein leerer Wert für NEWAUTHID gibt an, dass der Originalname ohne Umsetzung verwendet wird.)

Das weiter oben angeführte Beispiel soll erneut der Verdeutlichung dieser Sachverhalte dienen. Dem Benutzer JONES im System NEWYORK soll ein anderer Namen (NYJONES) gegeben werden, wenn JONES Anforderungen für verteilte Datenbanken an das System DALLAS absetzt. Angenommen, der Eigner der vom Benutzer JONES verwendeten Anwendung ist DSNPLAN (der Planeigner in DB2), und Sie müssen diese Benutzer-ID beim Senden an das System DALLAS nicht umzusetzen. Die SQL-Anweisungen, die zum Bereitstellen der Regeln für die Umsetzung für Namen in der Kommunikationsdatenbank erforderlich sind, werden in Abb. 24 auf Seite 117 dargestellt.

---

4. Wird die Anforderung an einen DB2-Server gesendet, wird die Namensumsetzung auch für den Planeigner und den Paketeigner ausgeführt. Den Namen der Paket- und Planeigner sind nie Kennwörter zugeordnet.

```

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

```

Abbildung 24. SQL für die Namensumsetzung für abgehende Anforderungen (SNA)

Die daraus resultierenden Kommunikationsdatenbanktabellen werden in Abb. 25 dargestellt:

NEWYORK.SYSIBM.LOCATIONS			
LOCATION	LINKNAME	PORT	TPN
DALLAS	LUDALLAS		

NEWYORK.SYSIBM.LUNAMES						
LUNAME	SYSMODENAME	SECURITY-IN	SECURITY-OUT	ENCRYPTPSWDS	MODESELECT	USERNAMES
LUDALLAS			A	N	N	O

NEWYORK.SYSIBM.USERNAMES				
TYPE	AUTHID	LINKNAME	NEWAUTHID	PASSWORD
0	JONES	LUDALLAS	NYJONES	JONESPWD
0	DSNPLAN	LUDALLAS		PLANPWD

Abbildung 25. Namensumsetzung für abgehende Anforderungen

In Abb. 26 auf Seite 118 wird ein einfacheres Beispiel für das Herstellen einer Verbindung zu einem DRDA<sup>®</sup>-Anwendungsserver unter DB2 für OS/390 und z/OS mit Hilfe einer SNA-Verbindung dargestellt.

```

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');

```

Abbildung 26. SQL für die Namensumsetzung für abgehende Anforderungen (einfaches Beispiel für SNA)

In Abb. 27 wird ein einfaches Beispiel für das Herstellen einer Verbindung zu einem DRDA-Anwendungsserver unter DB2 für OS/390 und z/OS mit Hilfe einer TCP/IP-Verbindung dargestellt.

```

-- DB2 für 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')
;

```

Abbildung 27. SQL für die Namensumsetzung für abgehende Anforderungen (einfaches Beispiel für TCP/IP)

#### Zugehörige Konzepte:

- „Sicherheitsüberlegungen für Anwendungsrequester (OS/390 und z/OS)“ auf Seite 115

## Netzwerksicherheit - Anwendungsrequester (OS/390 und z/OS)

Nachdem der Anwendungsrequester die Endbenutzernamen für die ferne Anwendung ausgewählt hat, muss er die erforderlichen Informationen für die LU 6.2-Netzwerksicherheit zur Verfügung stellen. LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene, die durch das Schlüsselwort VERIFY in der VTAM<sup>®</sup>-Anweisung APPL gesteuert wird
- Sicherheit auf Dialogebene, die durch den Inhalt der Tabelle SYSIBM.SYSLUNAMES gesteuert wird
- Datenverschlüsselung, die nur für VTAM 3.4 und spätere Releases von VTAM unterstützt wird

Der Anwendungsserver ist für die Verwaltung der Datenbankressourcen zuständig und legt deshalb auch fest, welche Netzwerksicherheitseinrichtungen seitens des Anwendungsrequesters erforderlich sind. Tragen Sie die Anforderungen der einzelnen Anwendungsserver an die Sicherheit auf Dialogebene in die Tabelle SYSIBM.SYSLUNAMES ein, indem Sie die jeweilige Sicherheitsanforderung des Anwendungsservers in die Spalte USERNAMES der Tabelle SYSIBM.SYSLUNAMES aufnehmen.

Die folgenden Optionen für die SNA-Sicherheit auf Dialogebene sind verfügbar:

### **SECURITY=SAME**

Diese Option wird auch als bereits geprüfte Sicherheit bezeichnet, weil nur die Benutzer-ID des Endbenutzers zum fernen System gesendet wird (es wird kein Kennwort übertragen). Verwenden Sie diese Stufe von Dialogsicherheit, wenn in der Spalte USERNAMES in der Tabelle SYSIBM.SYSLUNAMES kein Wert 'O' oder 'B' enthalten ist.

Da DB2 die Umsetzung für Endbenutzernamen mit der Sicherheit von abgehenden Dialogen koppelt, kann SECURITY=SAME nicht verwendet werden, wenn die Umsetzung von Endbenutzernamen für abgehende Anforderungen aktiviert ist.

### **SECURITY=PGM**

Benutzer-ID und Kennwort des Endbenutzers werden zur Gültigkeitsprüfung an das ferne System gesendet. Verwenden Sie diese Sicherheitsoption, wenn in der Spalte USERNAMES der Tabelle SYSIBM.SYSLUNAMES der Wert 'O' oder 'B' enthalten ist.

In Abhängigkeit von den in der Tabelle SYSIBM.SYSLUNAMES angegebenen Optionen ruft DB2 das Kennwort des Endbenutzers aus den folgenden beiden verschiedenen Quellen ab:

- Nicht verschlüsselte Kennwörter werden aus der Spalte PASSWORD in der Tabelle SYSIBM.SYSUSERNAMES abgerufen. DB2 extrahiert Kennwörter aus der Tabelle SYSIBM.SYSUSERNAMES, wenn die Spalte ENCRYPTPSWDS in der Tabelle SYSIBM.SYSLUNAMES nicht auf 'Y' gesetzt ist. Aus dieser Quelle abgerufene Kennwörter können an beliebige DRDA-Anwendungsserver übertragen werden.

In Abb. 28 auf Seite 120 werden die Kennwörter für die Beispielbenutzer SMITH und JONES definiert. In der Spalte LUNAME im Beispiel sind Leerzeichen enthalten, d. h. diese Kennwörter werden für alle fernen Systeme verwendet, auf die der Benutzer SMITH bzw. JONES zuzugreifen versucht.

```

INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('0', 'JONES', ' ', ' ', 'JONESPWD');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('0', 'SMITH', ' ', ' ', 'SMITHPWD');

```

Abbildung 28. Senden von Kennwörtern an ferne Standorte

- Verschlüsselte Kennwörter werden an den fernen Standort gesendet, wenn in der Spalte ENCRYPTPSWDS der Tabelle SYSIBM.SYSLUNAMES der Wert 'Y' enthalten ist. Verschlüsselte Kennwörter werden aus RACF® (oder einem äquivalenten Produkt) extrahiert und können nur von einem anderen DB2-System interpretiert werden. Für die Kommunikation mit einem Nicht-DB2-System darf ENCRYPTPSWDS nicht auf den Wert 'Y' gesetzt werden.

DB2 durchsucht die Tabelle SYSIBM.SYSUSERNAMES, um die Benutzer-ID (Wert für NEWAUTHID) zu ermitteln, die an das ferne System übertragen werden soll. Dieser umgesetzte Name wird für die RACF-Kennwortextraktion verwendet. Soll dieser Name nicht umgesetzt werden, müssen Sie Zeilen in der Tabelle SYSIBM.SYSUSERNAMES erstellen, durch die Namen ohne Umsetzung gesendet werden. Die Anweisungen in Abb. 29 ermöglichen das Senden von Anforderungen an LUDALLAS und LUNYC, ohne dass der Name (die Benutzer-ID) des Endbenutzers umgesetzt wird.

```

INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('0', ' ', 'LUNYC', ' ', ' ');
INSERT INTO SYSIBM.SYSUSERNAMES
  (TYPE, AUTHID, LUNAME, NEWAUTHID, PASSWORD)
VALUES ('0', ' ', 'LUDALLAS', ' ', ' ');

```

Abbildung 29. Senden von verschlüsselten Kennwörtern an ferne Standorte

#### SECURITY=NONE

Diese Option wird von DRDA nicht unterstützt; daher verfügt DB2 über keine Einrichtungen für diese Sicherheitsoption.

#### Zugehörige Konzepte:

- „Sicherheitsüberlegungen für Anwendungsrequester (OS/390 und z/OS)“ auf Seite 115

## Sicherheit des Datenbankmanagers - Anwendungsrequester (OS/390 und z/OS)

Der Anwendungsrequester kann durch die Namensumsetzung für abgehende Anforderungen an den Sicherheitsfunktionen für verteilte Datenbanken beteiligt sein. Mit der Namensumsetzung für abgehende Anforderungen können Sie den Zugriff auf einen bestimmten Anwendungsserver anhand der Identität des Endbenutzers und der Anwendung, von denen die Anforderung ausgeht, einschränken.

Der DB2-Anwendungsrequester kann auf folgende andere Arten an den System-sicherheitsfunktionen beteiligt sein:

#### **Binden ferner Anwendungen**

Endbenutzer binden ferne Anwendungen auf dem Anwendungsserver mit dem DB2-Befehl BIND PACKAGE. Die Verwendung des Befehls BIND PACKAGE auf dem Requester wird von DB2 nicht eingeschränkt. Ein Endbenutzer kann ein fernes Paket jedoch erst dann verwenden, nachdem es in einen DB2-Plan aufgenommen wurde. Die Verwendung des Befehls BIND PLAN wird hingegen von DB2 eingeschränkt. Ein Endbenutzer kann das ferne Paket nur dann zu einem Plan hinzufügen, wenn dem Endbenutzer mit der DB2-Anweisung GRANT das Zugriffsrecht BIND bzw. BINDADD erteilt wurde.

Verwenden Sie beim Binden eines Pakets die Option ENABLE/DISABLE, um anzugeben, ob das Paket von TSO, CICS/ESA, IMS/ESA oder einem fernen DB2-Subsystem verwendet werden soll.

#### **Ausführen ferner Anwendungen**

Damit ein DB2-Endbenutzer eine ferne Anwendung ausführen kann, muss er über die Berechtigung zum Ausführen des DB2-Plans verfügen, der dieser Anwendung zugeordnet ist. Der Eigner des DB2-Plans verfügt automatisch über die Berechtigung zum Ausführen des Plans. Anderen Endbenutzern kann die Berechtigung zum Ausführen des Plans durch die DB2-Anweisung GRANT EXECUTE erteilt werden. Auf diese Weise kann der Eigner einer Anwendung für verteilte Datenbanken individuell steuern, welche Benutzer die Anwendung verwenden dürfen.

#### **Zugehörige Konzepte:**

- „Sicherheitsüberlegungen für Anwendungsrequester (OS/390 und z/OS)“ auf Seite 115

---

## **Sicherheitssystem - Anwendungsrequester (OS/390 und z/OS)**

Das externe Sicherheitssystem auf MVS™-Systemen wird entweder durch RACF® oder durch gleichwertige Produkte bereitgestellt, die über eine mit RACF kompatible Schnittstelle verfügen. Der DB2®-Anwendungsrequester kann das externe Sicherheitssystem nicht direkt aufrufen (Ausnahme: Unterstützung für verschlüsselte Kennwörter). In den folgenden Situationen wird das externe Sicherheitssystem jedoch indirekt auf dem Anwendungsrequester verwendet:

- Das für die Verbindungsherstellung zwischen Endbenutzer und DB2 zuständige Produkt verwendet das externe Sicherheitssystem zur Überprüfung der Identität des Endbenutzers (Benutzer-ID und Kennwort). Dies geschieht vor der Verbindungsherstellung zwischen Endbenutzer und DB2. Wie bereits erwähnt, sind CICS/ESA, TSO und IMS/ESA® Beispiele für Produkte, die die Verbindung zwischen Endbenutzern und DB2 herstellen.
- Wenn Sie Sicherheit auf SNA-Sitzungsebene (über das Schlüsselwort VERIFY in der VTAM®-Anweisung APPL von DB2) verwenden, wird das externe Sicherheitssystem von VTAM aufgerufen, um die Identität des fernen Systems zu überprüfen.

#### **Zugehörige Konzepte:**

- „Sicherheitsüberlegungen für Anwendungsrequester (OS/390 und z/OS)“ auf Seite 115

---

## Sicherheitsüberlegungen für Anwendungsrequester (iSeries)

Wenn ein fernes System die Verarbeitung verteilter Datenbanken im Auftrag einer SQL-Anwendung ausführt, muss es in der Lage sein, die Sicherheitsanforderungen des Anwendungsrequesters, des Anwendungsservers und des verwendeten Netzwerks zu erfüllen. Diese Anforderungen betreffen einen oder mehrere der folgenden Bereiche:

- Endbenutzernamen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Vom iSeries™-Sicherheitssystem implementierte Sicherheit

### Endbenutzernamen:

Auf iSeries-Systemen wird Endbenutzern eine Benutzer-ID mit 1 bis 10 Zeichen zugeordnet, die zwar im betreffenden System, jedoch nicht unbedingt im gesamten Netzwerk eindeutig ist. Diese Benutzer-ID wird an das ferne System übermittelt, wenn die Verbindung zwischen zwei Datenbanken hergestellt wird. Zur Vermeidung von Konflikten zwischen Benutzer-IDs auf Systemen im Netzwerk wird häufig eine Namensumsetzung für abgehende Anforderungen durchgeführt, um die Benutzer-IDs zu ändern. Dadurch werden Konflikte gelöst, bevor die Benutzer-IDs über das Netzwerk gesendet werden.

Das iSeries-System stellt jedoch keine Namensumsetzung für abgehende Anforderungen zur Behebung potenzieller Konflikte auf dem Server zur Verfügung. Diese Konflikte müssen auf dem Anwendungsserver behoben werden, sofern Sie in der SQL-Anweisung CONNECT für iSeries nicht die zusätzlichen Klauseln USER und USING verwenden. USER gibt eine gültige ID auf dem Anwendungsserver und USING das entsprechende Kennwort für den Benutzer an.

### Netzwerksicherheit:

Nachdem der Anwendungsrequester die Endbenutzernamen für die ferne Anwendung ausgewählt hat, muss er die erforderlichen LU 6.2-Sicherheitsinformationen für das Netzwerk bereitstellen. LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene, gesteuert durch das Schlüsselwort LOCPWD im Befehl CRTDEVAPPC
- Sicherheit auf Dialogebene, gesteuert durch das Betriebssystem OS/400®
- Verschlüsselung (vom Betriebssystem OS/400 nicht unterstützt)

Die Sicherheit auf Sitzungsebene wird durch die LU-LU-Prüfung bereitgestellt. Jede LU verfügt über einen Schlüssel, der mit dem Schlüssel der fernen LU übereinstimmen muss. Dieser Schlüssel wird mit dem Schlüsselwort LOCPWD im Befehl CRTDEVAPPC festgelegt.

Der Anwendungsserver ist für die Verwaltung der Datenbankressourcen zuständig und legt deshalb auch fest, welche Netzwerksicherheitseinrichtungen seitens des Anwendungsrequesters erforderlich sind. Der iSeries-Sicherheitsadministrator muss sicherstellen, dass kein Anwendungsserver höhere Sicherheitsanforderungen stellt als vom iSeries-Anwenderrequester unterstützt werden.

Für die SNA-Dialogsicherheit sind die folgenden Optionen möglich:

**SECURITY=SAME**

Wird auch als bereits geprüfte Sicherheit bezeichnet. Nur die Benutzer-ID eines Anwendungsbenutzers wird zum fernen System gesendet. Es wird kein Kennwort übermittelt. Vor AS/400® Version 2 Release 2 Modifikationsstufe 0 wurde nur diese Stufe der Dialogsicherheit von iSeries-Anwendungsrequestern unterstützt.

**SECURITY=PGM**

Benutzer-ID und Kennwort des Anwendungsbenutzers werden zur Gültigkeitsprüfung an das ferne System gesendet. Vor AS/400 Version 2 Release 2 Modifikationsstufe 0 wurde diese Sicherheitsoption von iSeries-Anwendungsrequestern nicht unterstützt.

**SECURITY=NONE**

Wird nicht unterstützt, wenn das iSeries-System als Anwendungsrequester fungiert.

**Sicherheit des Datenbankmanagers:**

Das iSeries-System verfügt nicht über ein externes Sicherheitssystem. Alle Sicherheitsfunktionen werden über das Betriebssystem OS/400 gesteuert.

**Systemsicherheit:**

Das Betriebssystem OS/400 steuert die Vergabe von Berechtigungen für alle Objekte im System, einschließlich Programmen, Paketen, Tabellen, Sichten und Objektgruppen.

Der Anwendungsrequester steuert die Vergabe von Berechtigungen für Objekte, die sich auf dem Anwendungsrequester befinden. Die Sicherheit für Objekte auf dem Anwendungsserver wird vom Anwendungsserver auf der Basis der vom Anwendungsrequester übermittelten Benutzer-ID gesteuert. Die an den Anwendungsserver übermittelte Benutzer-ID ist dem Benutzer des iSeries-Anwendungsrequesters oder der in der Klausel USER der iSeries-SQL-Anweisung CONNECT angegebenen Benutzer-ID zugeordnet. Beispiel: `CONNECT TO rdbname USER benutzer-id USING kennwort.`

Die Objektsicherheit kann mit Hilfe der CL-Befehle für Objektberechtigungen oder mit den SQL-Anweisungen GRANT und REVOKE verwaltet werden. Zu den CL-Befehlen für Objektberechtigungen gehören der Befehl zum Erteilen von Objektberechtigungen (GRTOBJAUT) und der Befehl zum Entziehen von Objektberechtigungen (RVKOBJAUT). Diese Befehle gelten für jedes Objekt auf dem System. Die Anweisungen GRANT und REVOKE gelten nur für SQL-Objekte (Tabellen, Sichten und Pakete). Verwenden Sie zum Ändern der Berechtigungen für andere Objekte (z. B. Programme und Objektgruppen) die Befehle GRTOBJAUT und RVKOBJAUT.

Beim Erstellen von Objekten wird eine Standardberechtigung vergeben. Der Ersteller einer Tabelle, einer Sicht oder eines Programms erhält standardmäßig sämtliche Berechtigungen für die von ihm erstellten Objekte. Außerdem erhält PUBLIC für diese Objekte die selbe Berechtigung, die PUBLIC für die Bibliothek oder Objektgruppe dieser Objekte hat.

Weitere Informationen zur Systemsicherheit finden Sie im Handbuch *OS/400 Security - Reference*.

**Zugehörige Konzepte:**

- „Sicherheitsüberlegungen für Anwendungsserver (iSeries)“ auf Seite 105
- „DB2 UDB für iSeries“ auf Seite 81

**Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsrequester – SNA (iSeries)“ auf Seite 33
- „Erteilen und Entziehen von Berechtigungen:“ auf Seite 124

---

## Erteilen und Entziehen von Berechtigungen:

**Vorgehensweise:**

Verwenden Sie den folgenden Befehl, um dem Benutzer USER1 die Berechtigung \*USE für das Programm PGMA auf einem iSeries-System zu erteilen:

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

Verwenden Sie den folgenden Befehl, um diese Berechtigung zu entziehen:

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

\*PGM gibt in diesem Beispiel den Objekttyp Programm an. \*SQLPKG steht für ein Paket, \*LIB für eine Objektgruppe und \*FILE für eine Tabelle.

Darüber hinaus können die Befehle GRTOBJAUT und RVKOBJAUT verwendet werden, um zu verhindern, dass Benutzer Programme und Pakete erstellen. Wenn die Berechtigung für einen der Befehle CRTSQLxxx (mit xxx = RPG, C, CBL, FTN oder PLI) entzogen wird, kann der Benutzer keine Programme erstellen. Wird die Berechtigung für den Befehl CRTSQLPKG entzogen, kann der Benutzer weder vom Anwendungsrequester aus noch auf dem Anwendungsserver Pakete erstellen.

Geben Sie beispielsweise den folgenden Befehl ein, um dem Benutzer USER1 die Berechtigung \*USE für den Befehl CRTSQLPKG auf einem iSeries-System zu erteilen: `GRTOBJAUT OBJ(CRTSQLPKG) OBJTYPE(*CMD) USER(USER1) AUT(*USE)`

Dies betrifft die Ausführung des Befehls CRTSQLPKG auf dem Anwendungsrequester. Auf dem Anwendungsserver ermöglicht dieser Befehl das Erstellen von Paketen.

Verwenden Sie den folgenden Befehl, um diese Berechtigung zu entziehen:

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

**Zugehörige Konzepte:**

- „Sicherheitsüberlegungen für Anwendungsserver (iSeries)“ auf Seite 105
- „Sicherheitsüberlegungen für Anwendungsrequester (iSeries)“ auf Seite 122
- „DB2 UDB für iSeries“ auf Seite 81

---

## Sicherheitsüberlegungen für Anwendungsrequester (VM)

Wenn ein fernes System die Verarbeitung verteilter Datenbanken im Auftrag einer SQL-Anwendung ausführt, muss es in der Lage sein, die Sicherheitsanforderungen des Anwendungsrequesters, des Anwendungsrequesters und des verwendeten Netzwerks zu erfüllen.

Diese Anforderungen betreffen einen oder mehrere der folgenden Bereiche:

- Endbenutzernamen
- Sicherheitsparameter des Netzwerks
- Sicherheit des Datenbankmanagers
- Von einem externen Sicherheitssystem implementierte Sicherheit

#### Endbenutzernamen:

In SQL und LU 6.2 wird jedem Endbenutzer eine Benutzer-ID aus 1 bis 8 Zeichen zugeordnet. Der Wert dieser Benutzer-ID muss zwar innerhalb eines bestimmten Betriebssystems, jedoch nicht unbedingt im gesamten SNA-Netzwerk eindeutig sein.

Beispielsweise kann es im System TORONTO einen Benutzer mit dem Namen JONES und im System MONTREAL einen weiteren Benutzer dieses Namens geben. Wenn diese beiden Benutzer die selbe Person sind, entsteht dadurch kein Konflikt. Ist jedoch der Benutzer JONES in TORONTO nicht identisch mit dem Benutzer JONES in MONTREAL, kann das SNA-Netzwerk (und können folglich auch die verteilten Datenbanksysteme innerhalb dieses Netzwerks) den Benutzer JONES in TORONTO nicht vom Benutzer JONES in MONTREAL unterscheiden. Wird diese Situation nicht durch geeignete Maßnahmen verhindert, können diese beiden Benutzer die Berechtigungen des jeweils anderen benutzen.

Zur Vermeidung solcher Namenskonflikte unterstützt DB2<sup>®</sup> für VM die Umsetzung für Endbenutzernamen. Das System erzwingt jedoch keine Umsetzung von Benutzer-IDs. Ist eine solche, vom System erzwungene Umsetzung erforderlich, müssen Sie sicherstellen, dass auf dem Anwendungsserver die richtige Namensumsetzung für eingehende Anforderungen ausgeführt wird.

Die *Namensumsetzung für abgehende Anforderungen* wird mit Hilfe des CMS Communications Directory durchgeführt. Ein Eintrag im CMS Communications Directory muss die Angabe `:security.PGM` enthalten. In diesem Fall werden die entsprechenden Werte der Kennungen `:userid` und `:password` in der Verbindungsanforderung an den fernen Standort (Anwendungsserver) übermittelt.

Durch Erstellen des in Abb. 30 dargestellten Eintrags wird der Benutzer mit der ID JONES auf dem lokalen System (TORONTO) auf die Benutzer-ID JONEST abgebildet, wenn sich dieser Benutzer am Anwendungsserver MONTREAL\_SALES\_DB im System MONTREAL anmeldet. Auf diese Weise wird die Mehrdeutigkeit der Benutzer-ID behoben.

```
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
```

Abbildung 30. Namensumsetzung für abgehende Anforderungen

## Netzwerksicherheit:

Nach dem Auswählen des Endbenutzernamens, der den Anwendungsrequester am fernen Standort (Anwendungsserver) repräsentiert, muss der Anwendungsrequester die erforderlichen Informationen für die LU 6.2-Netzwerksicherheit zur Verfügung stellen. LU 6.2 stellt die folgenden drei Hauptsicherheitseinrichtungen für das Netzwerk zur Verfügung:

- Sicherheit auf Sitzungsebene, angegeben durch den Parameter VERIFY in der VTAM<sup>®</sup>-Anweisung APPL
- Sicherheit auf Dialogebene, angegeben im CMS Communications Directory
- Verschlüsselung

Der Anwendungsserver ist für die Verwaltung der Datenbankressourcen zuständig und legt deshalb auch fest, welche Netzwerksicherheitseinrichtungen vom Anwendungsrequester bereitgestellt werden müssen. Sie müssen die Sicherheitsanforderungen des Anwendungsservers im Kommunikationsverzeichnis des Anwendungsrequesters aufzeichnen, indem Sie den entsprechenden Wert für die Kennung :security einstellen.

Die folgenden Optionen für die SNA-Sicherheit auf Dialogebene werden von DRDA<sup>®</sup> unterstützt:

### SECURITY=SAME

Diese Option wird auch als bereits geprüfte Sicherheit bezeichnet, weil nur die ID des Endbenutzers (Anmelde-ID) zum fernen System gesendet wird. Das Kennwort wird nicht gesendet. Diese Stufe der Dialogsicherheit wird verwendet, wenn im Kommunikationsverzeichnis des Anwendungsrequesters für den betreffenden Anwendungsserver :security.SAME angegeben ist. Bei Verwendung dieser Option wird keine Umsetzung von Endbenutzernamen für abgehende Anforderungen ausgeführt. Die Anmelde-ID des CMS-Benutzers wird als Benutzer-ID zum fernen DRDA-Standort übermittelt. Die Kennung :userid im CMS Communications Directory wird für :security.SAME ignoriert.

### SECURITY=PGM

Diese Option bewirkt, dass ID und Kennwort des Endbenutzers zur Gültigkeitsprüfung an das ferne System (Anwendungsserver) gesendet werden. Diese Sicherheitsoption wird verwendet, wenn im Eintrag des CMS Communications Directory des Anwendungsrequesters :security.PGM angegeben ist. Bei Verwendung dieser Option wird die Umsetzung von Endbenutzernamen für abgehende Anforderungen ausgeführt.

DB2 für VM bietet keine Unterstützung für Kennwortverschlüsselung. Das Kennwort kann in der Kennung :password angegeben oder mit Hilfe einer Verzeichnisanweisung APPCPASS im Benutzerverzeichniseintrag des Endbenutzers gespeichert werden. Das Angeben in der Anweisung APPCPASS bietet die größtmögliche Kennwortsicherheit. Wenn das Kennwort nicht als Eintrag im CMS Communications Directory angegeben ist, wird der Eintrag im Systemverzeichnis (VM-Verzeichnis) des Benutzers nach einer Anweisung APPCPASS durchsucht.

### Anweisung APPCPASS:

Die Anweisung APPCPASS des VM-Systems bietet die größtmögliche Sicherheit für die Kombination aus Benutzer-ID und Kennwort, die vom Anwendungsrequester zum Herstellen einer Verbindung zu einem Anwendungsserver verwendet wird.

Die Flexibilität der Anweisung APPCPASS ermöglicht das Speichern von Sicherheitsinformationen auf folgende Arten:

- **Benutzer-ID und Kennwort:** In diesem Fall müssen die Kennungen :userid und :password im CMS Communications Directory leer sein.
- **Nur Benutzer-ID:** In diesem Fall muss die Kennung :userid im CMS Communications Directory leer sein, und die Kennung :password muss auf das Kennwort des Benutzers gesetzt sein.
- **Nur Kennwort:** In diesem Fall muss die Kennung :password im CMS Communications Directory leer sein, und die Kennung :userid muss auf die ID des Benutzers gesetzt sein.

In Abb. 31 wird der Fall dargestellt, in dem die Benutzer-ID im Kommunikationsverzeichnis des Benutzers und das Kennwort im VM-Verzeichniseintrag des Benutzers gespeichert ist. Die Benutzer-ID im Kommunikationsverzeichniseintrag ist auf MTLSSOU gesetzt, aber das Kennwort ist nicht definiert. Das Kennwort ist im VM-Verzeichniseintrag des Benutzers gespeichert.

```
UCOMDIR NAMES A1 V 132 Trunc=132 Size=8 Line=1 Col=1 Alt=8
====>
00001 :nick.MTLSSALES
00002 :tpn.SALES
00003 :luname.TORGATE MTLGATE
00004 :modename.BATCH
00005 :security.PGM
00006 :userid.MTLSSOU
00007 :password.
00008 :dbname.MONTREAL_SALES_DB
00009
```

Abbildung 31. Beispieleintrag im Kommunikationsverzeichnis ohne definiertes Kennwort

Wenn APPC/VM die Verbindung zwischen dem Anwendungsrequester und dem Anwendungsserver mit der Dialogsicherheit SECURITY=PGM einleitet, liest APPC/VM die Werte der Kennungen :userid und :password und leitet sie an den Anwendungsserver weiter. Wenn eine oder beide Kennungen leer sind, wird der VM-Verzeichniseintrag des Benutzers nach den fehlenden Informationen durchsucht. In diesem Fall muss der VM-Verzeichniseintrag die folgende Anweisung APPCPASS enthalten:

```
APPCPASS TORGATE MTLGATE MTLSSOU Q6VBN8XP
```

Diese Anweisung teilt APPC/VM mit, dass der Benutzer (Anwendungsrequester), der die Verbindung über den (lokalen) AVS-Gateway TORGATE, die Partner-LU namens MTLGATE und die Benutzer-ID MTLSSOU anfordert, das Kennwort Q6VBN8XP an den Anwendungsserver senden soll. Der Benutzer ist durch diese beiden Identifikationsangaben auf dem Anwendungsserver bekannt.

Das Einfügen der Anweisung APPCPASS im VM-Verzeichnis ist nicht Aufgabe des Endbenutzers. Der Endbenutzer muss vielmehr eine entsprechende Anfrage an den VM-Systemprogrammierer richten.

Weitere Informationen zur Sicherheit auf Dialogebene und zur Anweisung APPCPASS finden Sie im Handbuch *VM/ESA Connectivity Planning, Administration, and Operation*.

### Sicherheit des Datenbankmanagers:

Im Rahmen der umfassenden DRDA-Sicherheitseinrichtungen für verteilte Datenbanken kann der Anwendungsrequester mit darüber entscheiden, welche Benutzer

Anforderungen an verteilte Datenbanken absetzen dürfen. In DB2 für VM kann der Anwendungsrequester in folgenden drei Bereichen an den Sicherheitsfunktionen für verteilte Datenbanken beteiligt sein:

#### **Umsetzung von Benutzernamen für abgehende Anforderungen**

Mit der Umsetzung von Benutzernamen für abgehende Anforderungen können Sie den Zugriff auf einen bestimmten Anwendungsserver anhand der Identität des Endbenutzers einschränken, von dem die Anforderung ausgeht. DB2 für VM versucht zunächst, den Namen des Endbenutzers umzusetzen, bevor die Anforderung an den fernen Standort übermittelt wird. Die sicherste Methode bietet jedoch eine Herkunftsüberprüfung und Namensumsetzung für eingehende Anforderungen durch den Anwendungsserver, weil Benutzer von VM-Anwendungsrequestern die Möglichkeit haben, die Namensumsetzung für abgehende Anforderungen über ihr CMS-Kommunikationsverzeichnis außer Kraft zu setzen.

#### **Vorverarbeiten von Anwendungen**

Endbenutzer können eine Vorverarbeitung von Anwendungen für einen bestimmten Anwendungsserver mit Hilfe der Prozedur SQLPREP EXEC von DB2 für VM oder über den Befehl RELOAD PACKAGE des Dienstprogramms DBSU (Database Service Utility) veranlassen. DB2 für VM schränkt die Verwendung dieser Services nicht ein. Führt ein Endbenutzer die Vorverarbeitung einer Anwendung durch, so wird er dadurch zum Eigner des resultierenden Pakets.

#### **Ausführen von Anwendungen**

Damit ein Endbenutzer von DB2 für VM eine ferne Anwendung ausführen kann, muss er am fernen Standort (Anwendungsserver) über die Berechtigung zum Ausführen des fernen Pakets verfügen, das dieser Anwendung zugeordnet ist. Der Ersteller (Eigner) des Pakets ist automatisch berechtigt, das Paket auszuführen. Anderen Endbenutzern kann die Berechtigung zum Ausführen des Pakets durch die Anweisung GRANT execute von DB2 für VM erteilt werden. Auf diese Weise kann der Eigner einer Anwendung für verteilte Datenbanken individuell steuern, welche Benutzer die Anwendung verwenden dürfen.

#### **Sicherheitssystem:**

Das externe Sicherheitssystem auf VM-Systemen wird entweder durch RACF<sup>®</sup> oder durch gleichwertige Produkte bereitgestellt, die eine mit RACF kompatible Schnittstelle zur Verfügung stellen. Der Anwendungsrequester unter DB2 für VM hat keine direkte Schnittstelle zum externen Sicherheitssystem. Das externe Sicherheitssystem wird nicht zum Bereitstellen von Kennwörtern für die Dialogsicherheit verwendet. Wenn Sie Sicherheit auf Sitzungsebene verwenden, wird das externe Sicherheitssystem von VTAM aufgerufen, um die Gültigkeit des Namens der fernen LU im Rahmen der Partner-LU-Gültigkeitsprüfung zu überprüfen.

#### **Zugehörige Konzepte:**

- „Sicherheitsüberlegungen für Anwendungsserver (VM)“ auf Seite 108
- „DB2 für VM“ auf Seite 82

#### **Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsrequester (VM)“ auf Seite 39

---

## Kapitel 14. Datendarstellung

---

### Datendarstellung (OS/390 und z/OS)

DB2® wird mit einer Standardinstallations-CCSID (Coded Character Set Identifier = ID für codierten Zeichensatz) von 500 ausgeliefert. Diese Standardeinstellung ist für Ihre Installation wahrscheinlich nicht korrekt.

Bei der Installation von DB2 müssen Sie die Installations-CCSID auf die CCSID der Zeichen setzen, die von den Eingabeeinheiten an Ihrem Standort generiert und an DB2 gesendet werden. Diese CCSID wird in der Regel durch die verwendete Landessprache festgelegt. Ist die Installations-CCSID inkorrekt, führt die Zeichenumsetzung zu fehlerhaften Ergebnissen.

Stellen Sie sicher, dass das DB2-Subsystem die CCSIDs der einzelnen Anwendungsserver in die Installations-CCSID des DB2-Subsystems umsetzen kann. DB2 stellt Umsetzungstabellen für die gängigsten Kombinationen aus Quellen- und Ziel-CCSIDs, jedoch nicht für jede mögliche Kombination zur Verfügung. Falls erforderlich, können Sie der Gruppe verfügbarer Umsetzungstabellen und Umsetzungsroutrinen weitere Tabellen und Routinen hinzufügen.

Weitere Informationen zur Zeichenumsetzung in DB2 UDB für OS/390 und z/OS finden Sie im Handbuch *DB2 Universal Database™ for OS/390® and z/OS™ Administration Guide*.

#### Zugehörige Konzepte:

- „DB2 für OS/390 und z/OS“ auf Seite 73
- „Umsetzung von Zeichendaten“ in *DB2 Connect Enterprise Edition Einstieg*

#### Zugehörige Tasks:

- „Definieren von DB2 als Anwendungsserver (OS/390 und z/OS)“ auf Seite 47
- „Definieren von DB2 als Anwendungsrequester (OS/390 und z/OS)“ auf Seite 25

---

### Datendarstellung (iSeries)

Produkte mit DRDA®-Unterstützung führen alle erforderlichen Umsetzungen auf dem Anwendungsserver automatisch aus. Damit dies möglich wird, muss der CCSID-Wert (Coded Character Set ID - ID für codierten Zeichensatz) des Anwendungsservers ein Wert sein, der vom Anwendungsrequester für die Umsetzung unterstützt wird.

Der bei Auslieferung für das OS/400®-System gültige Standardwert für die CCSID ist 65535 (auch als X'FFFF' bezeichnet). Dieser Standardwert ist mit den anderen IBM® Produkten nicht kompatibel. Die CCSID des Systems kann mit dem CL-Befehl DSPSYSVAL QCCSID angezeigt werden. Zum Ändern dieser CCSID kann der Befehl CHGSYSVAL verwendet werden. Beispiel: CHGSYSVAL QCCSID VALUE(37). Außerdem kann die CCSID des Systems durch die dem DRDA-Serverjob zugeordnete CCSID außer Kraft gesetzt werden. Diese CCSID kann mit dem CL-Befehl CHGUSRPRF festgelegt werden. Beispiel: CHGUSRPRF BENUTZERID CCSID(37).

## **Anwendungsserver:**

Auf einem Anwendungsserver sollten Sie besonders auf die CCSID achten, die folgenden Bereichen zugeordnet ist:

### **Servicejob im Kommunikationssystem**

Die CCSID Ihres Servicejobs muss mit dem Anwendungsrequester kompatibel sein. Diese CCSID wird durch das Benutzerprofil der Benutzer-ID festgelegt, von der die Verbindung angefordert wird. Die OS/400-Arbeitsverwaltungsunterstützung (Work Management Support) initialisiert die CCSID des Jobs mit dem Wert der CCSID im Benutzerprofil. Ist im Benutzerprofil keine CCSID vorhanden, fragt die Arbeitsverwaltungsunterstützung die CCSID (QCCSID) aus dem Systemwert ab. Der Systemwert QCCSID ist anfangs auf die CCSID 65535 eingestellt.

Bevor Sie eine Anforderung an DB2<sup>®</sup> UDB für iSeries<sup>™</sup> einleiten, sollten Sie sich anmelden und den dem Befehl zum Ändern des Benutzerprofils (CHGUSRPRF) verwenden, um dem Benutzerprofil des Jobs, der die DRDA-Anforderungen verwaltet, einen zulässigen CCSID-Wert zuzuordnen.

### **SQL-Objektgruppen**

Eine SQL-Objektgruppe besteht aus einem OS/400-Bibliotheksojekt, einem Journal, einem Journalempfänger und (optional) einem IDDU-Datenverzeichnis (IDDU Data Dictionary), wenn in der Anweisung CREATE COLLECTION die Klausel WITH DATA DICTIONARY angegeben wurde. Den physischen und logischen Dateien, die für einige dieser Objekte verwendet werden, wird standardmäßig die zur Zeit der Erstellung gültige CCSID des Jobs zugeordnet. Beim Abfragen des Datenverzeichnisses oder des Katalogs über einen Anwendungsrequester, der den CCSID-Wert dieser Dateien nicht unterstützt, werden möglicherweise nicht darstellbare oder verzerrte Daten angezeigt. Es ist auch möglich, dass der Anwendungsrequester in einer Nachricht darauf hinweist, dass der CCSID-Wert nicht unterstützt wird. Zur Behebung dieses Fehlers müssen Sie eine neue SQL-Objektgruppe mit einem CCSID-Wert erstellen, der für das andere System akzeptabel ist.

Die CCSID des Jobs kann mit dem Befehl zum Ändern des Jobs (CHGJOB) geändert werden. Alternativ hierzu können Sie für nachfolgende Jobs den Befehl zum Ändern des Benutzerprofils (CHGUSRPRF) verwenden, um den CCSID-Wert des Benutzerprofils zu ändern. Verwenden Sie in einem CL-Programm den Befehl zum Abrufen der Jobattribute (RTVJOBA), um die CCSID des aktuellen Jobs abzurufen. Verwenden Sie bei der interaktiven Verarbeitung den Befehl zum Arbeiten mit einem Job (WRKJOB) und wählen Sie in der zugehörigen Anzeige MIT JOB ARBEITEN die Option 2 (Jobdefinitionsattribute anzeigen) aus.

### **SQL-Tabellen und andere Dateien von DB2 UDB für iSeries, auf die über DRDA zugegriffen wird**

Eine SQL-Tabelle entspricht einer physischen Datei von DB2 UDB für iSeries innerhalb einer Bibliothek mit dem selben Namen wie Ihre Objektgruppe. Darüber hinaus entsprechen die Spalten einer Tabelle den Felddefinitionen einer physischen Datei. Die CCSID-Werte für die Tabelle oder die Spalten der Tabelle sind möglicherweise nicht mit dem Anwendungsrequester kompatibel.

Eine Hauptursache für CCSID-Inkompatibilitäten in älteren OS/400-Versionen als Version 3 Release 1 lag darin, dass viele Dateien oder SQL-Tabellen standardmäßig mit der CCSID 65535 gekennzeichnet wurden. In Version 3 Release 1 und nachfolgenden Releases werden die CCSIDs dieser Dateien automatisch auf einen anderen, besser geeigneten Wert gesetzt.

### **Anwendungsrequester:**

Auf einem Anwendungsrequester sollten Sie besonders auf die CCSID (Coded Character Set ID - ID für codierten Zeichensatz) achten, die folgenden Objekten zugeordnet ist:

#### **Anfordernder Job**

Die OS/400-Arbeitsverwaltungsunterstützung (Work Management Support) initialisiert die CCSID des Jobs mit dem Wert der CCSID im Benutzerprofil. Ist der CCSID-Wert im Benutzerprofil \*SYSVAL, fragt die Arbeitsverwaltungsunterstützung die CCSID aus dem Systemwert QCCSID ab. Der Systemwert QCCSID ist anfangs auf die CCSID 65535 eingestellt. Wenn 65535 für die CCSID von Jobs verwendet wird, über die von DB2 Universal Database™ Verbindungen hergestellt werden sollen, scheitern diese Verbindungsversuche. Da die Änderung des Systemwerts QCCSID Auswirkungen auf das gesamte System hat, wird empfohlen, die CCSID des Benutzerprofils für den Job zu ändern, mit dem der Serverjob ausgeführt wird. Legen Sie die CCSID des Benutzerprofils für den Job auf einen geeigneten Wert fest. Verwenden Sie beispielsweise CCSID 37 für amerikanisches Englisch. In der Regel sollte die Standard-CCSID für das iSeries-System gewählt werden, zu dem eine Verbindung hergestellt werden soll.

Die CCSID des Jobs kann mit dem Befehl zum Ändern des Jobs (CHGJOB) geändert werden. Alternativ hierzu können Sie für nachfolgende Jobs den Befehl zum Ändern des Benutzerprofils (CHGUSRPRF) verwenden, um den CCSID-Wert des Benutzerprofils zu ändern. Mit dem Befehl zum Abrufen der Jobattribute (RTVJOBA) können Sie feststellen, welche CCSID für einen Job in einem CL-Programm gilt. Verwenden Sie bei der interaktiven Verarbeitung den Befehl zum Arbeiten mit einem Job (WRKJOB) und wählen Sie in der zugehörigen Anzeige MIT JOB ARBEITEN die Option 2 (Jobdefinitionsattribute anzeigen) aus.

#### **Physische Datenbankdateien**

Wird im Befehl zum Erstellen einer physischen Datei (CRTPF) oder im Befehl zum Erstellen einer physischen Quellendatei (CRTSRCPF) keine CCSID explizit angegeben, wird für die Erstellung von physischen Datenbankdateien standardmäßig die Standard-CCSID des Jobs (die von der CCSID des Jobs abweichen kann) verwendet. Vor DB2 für AS/400® Version 3 Release 1 war der Standardwert die CCSID des Jobs, die häufig 65535 und für DRDA-Verwendung ungeeignet war. Die Standard-CCSID des Jobs ist nie 65535 und eignet sich daher besser für die CCSID physischer Dateien, auf die über DRDA zugegriffen wird.

Mit dem Befehl zum Anzeigen der Dateibeschreibung (DSPFD) können Sie die CCSID einer Datei und mit dem Befehl zum Anzeigen der Dateifeldbeschreibung (DSPFFD) die CCSID der Felder einer Datei abrufen.

Ändern Sie die CCSID einer physischen Datei mit dem Befehl zum Ändern der physischen Datei (CHGPF). Eine physische Datei kann nicht in jedem Fall geändert werden, wenn mindestens eine der folgenden Bedingungen zutrifft:

- Logische Dateien wurden über die physische Datei definiert. In diesem Fall müssen Sie eventuell folgende Schritte ausführen:
  1. Sichern Sie die logischen und die physischen Dateien zusammen mit ihren Zugriffspfaden.
  2. Drucken Sie eine Liste der Berechtigungen für logische Dateien (DSPOBJAUT).
  3. Löschen Sie die logischen Dateien.
  4. Ändern Sie die physischen Dateien.
  5. Stellen Sie die physischen und die logischen Dateien mit ihren Zugriffspfaden über die geänderten physischen Dateien wieder her.
  6. Erteilen Sie die persönliche Berechtigung für die logischen Dateien. Verwenden Sie hierzu die gedruckte Liste.
- Dateien oder Feldern wurde explizit ein CCSID-Wert zugeordnet. Erstellen Sie zum Ändern einer physischen Datei mit auf Feldebene zugeordneter CCSID die physische Datei erneut und kopieren Sie die Daten in die neue Datei. Verwenden Sie hierzu den Parameter FMTOPT(\*MAP) des Befehls zum Kopieren einer Datei (CPYF).
- Satzformate werden in einer älteren Version von OS/400 als Version 3 Release 1 gemeinsam benutzt.

#### **Zugehörige Konzepte:**

- „DB2 UDB für iSeries“ auf Seite 81
- „Umsetzung von Zeichendaten“ in *DB2 Connect Enterprise Edition Einstieg*

#### **Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsserver – SNA (iSeries)“ auf Seite 51
- „Definieren von DB2 als Anwendungsrequester – SNA (iSeries)“ auf Seite 33

---

## **Datendarstellung (VM)**

Für CHARNAME und CCSID müssen die für Ihre Installation am besten geeigneten Standardwerte ausgewählt werden. Durch die Auswahl der optimalen Werte wird die Integrität der Darstellung von Zeichendaten sichergestellt und zugleich der mit der CCSID-Umsetzung verbundene Systemaufwand reduziert.

#### **Anwendungsserver:**

Beispiel: Wenn auf die Anwendungsserver unter DB2<sup>®</sup> für VM nur lokale Benutzer von Workstations aus zugreifen, deren Controller mit Codepage 37 und Zeichensatz 697 (CP/CS 37/697) für amerikanisches Englisch generiert werden, sollten Sie für den Anwendungsrequester ENGLISH als Standardwert für CHARNAME definieren. Der Grund hierfür ist, dass CP/CS (Codepage/Codeset) 37/697 der CCSID 37 entspricht, die ihrerseits dem Wert ENGLISH für CHARNAME entspricht.

Zur Vermeidung unnötiger CCSID-Umsetzungen sollten Sie für den Anwendungsserver die selbe Standard-CCSID auswählen wie für die Anwendungsrequester, die am häufigsten auf Ihren Anwendungsserver zugreifen.

Das folgende Beispiel zeigt, welche Konflikte zwischen diesen beiden Zielsetzungen auftreten können:

- Ein Anwendungsserver hat weniger als fünf lokale Anwendungsrequester (für VM-Anwendungsrequester würde der Protokollparameter auf SQL/DS gesetzt) und zahlreiche (etwa 100) Anwendungsrequester, die über das DRDA<sup>®</sup>-Protokoll auf den Anwendungsserver zugreifen. Die Controller der lokalen Anwendungsrequester sind mit CP/CS 37/697 definiert. Die fernen Anwendungsrequester verwenden CCSID 285.

Wenn der Standardwert des Anwendungsservers für CHARNAME auf ENGLISH gesetzt ist, bleibt damit die Datenintegrität für die lokalen Anwendungsrequester gewahrt, aber für alle fernen Anwendungsrequester ist zusätzlicher Systemaufwand für die CCSID-Umsetzung erforderlich.

Wenn der Standardwert des Anwendungsservers für CHARNAME auf UK-ENGLISH gesetzt ist, wird zusätzlicher Systemaufwand bei der CCSID-Umsetzung für alle fernen Anwendungsrequester vermieden, aber es entstehen Probleme bei der Datenintegrität der lokalen Anwendungsrequester (bestimmte Daten werden auf den lokalen Anwendungsrequestern nicht korrekt angezeigt, beispielsweise wird anstelle des Zeichens für britisches Pfund (£) das Dollarzeichen (\$) angezeigt).

Fragen Sie die Tabelle SYSTEM.SYSOPTIONS ab, um die aktuelle CCSID des Systems anzuzeigen. Die Standard-CCSID des Anwendungsservers ist normalerweise der Wert für CCSIDMIXED. Ist dieser Wert Null, hat die Standard-CCSID des Systems den Wert für CCSIDSBCS. Die Werte für CHARNAME, CCSIDSBCS, CCSIDMIXED und CCSIDGRAPHIC in dieser Tabelle werden bei jedem Starten der Datenbank mit den verwendeten Systemstandardwerten aktualisiert. Die Werte in dieser Tabelle entsprechen möglicherweise nicht immer den Systemstandardwerten. Ein Benutzer mit der Berechtigung DBA könnte diese Werte geändert haben, obwohl diese Vorgehensweise nicht zu empfehlen ist. Zum Ändern der Standard-CCSID des Anwendungsservers müssen Sie den Parameter CHARNAME der Prozedur SQLSTART EXEC beim nächsten Starten des Anwendungsservers angeben. Weitere Informationen hierzu finden Sie im Handbuch *DB2 Server for VM System Administration*.

Für eine neu installierte Datenbank ist INTERNATIONAL der Standardwert für den Parameter CHARNAME des Anwendungsservers, und die Standard-CCSID des Anwendungsservers ist 500. Dies ist für Ihr System wahrscheinlich *nicht* korrekt. In einem durch Migration umgestellten System ist ENGLISH der Standardwert für CHARNAME, und die Standard-CCSID ist 37.

### **Anwendungsrequester:**

Der Anwendungsrequester muss über die korrekten Standardwerte für CHARNAME und CCSID verfügen. Durch die Auswahl der korrekten Werte wird die Integrität der Darstellung von Zeichendaten sichergestellt und zugleich der mit der CCSID-Umsetzung verbundene Systemaufwand reduziert.

Beispiel: Wenn Ihr Anwendungsrequester unter DB2 für VM mit Codepage 37 und Zeichensatz 697(CP/CS 37/697) für amerikanisches Englisch generiert wird, sollte der Anwendungsrequester ENGLISH als Standardwert für CHARNAME definieren. Der Grund hierfür ist, dass CP/CS 37/697 der CCSID 37 entspricht, die ihrerseits dem Wert ENGLISH für CHARNAME entspricht.

Der Standardwert für CHARNAME eines neu installierten oder durch Migration umgestellten Systems ist INTERNATIONAL mit CCSID 500. Dies ist für Ihre Installation wahrscheinlich *nicht* korrekt. Verwenden Sie den folgenden Befehl, um die Werte für die aktuellen Standard-CCSIDs anzuzeigen:

```
SQLINIT QUERY
```

Der korrekte CCSID-Wert für den Anwendungsrequester wird von den Umsetzungstabellen auf dem Anwendungsserver möglicherweise nicht unterstützt. Ist dies der Fall, können Sie die Verbindung auf eine der folgenden Arten herstellen:

- Veranlassen Sie, dass die CCSID-Umsetzungstabelle des Anwendungsservers aktualisiert wird, so dass die Umsetzung zwischen der Standard-CCSID des Anwendungsrequesters und der Standard-CCSID des Anwendungsservers unterstützt wird (Informationen zum Hinzufügen der Unterstützung für die CCSID-Umsetzung finden Sie in den Produkthandbüchern des Anwendungsservers).
- Definieren Sie für den Anwendungsrequester eine andere Standard-CCSID, die vom Anwendungsserver unterstützt wird. Dies kann zu Problemen bei der Datenintegrität führen. Deshalb sollten Sie sich vorher unbedingt über die möglichen Auswirkungen im Klaren sein. Ein Beispiel für eine solche Auswirkung könnte wie folgt aussehen:
  - Ein Anwendungsrequester verwendet einen mit CP/CS 37/697 definierten Controller. Der Anwendungsserver unterstützt keine Umsetzung von CCSID 37; er unterstützt jedoch eine Umsetzung von CCSID 285 (die Einstellung CHARNAME UK-ENGLISH (britisches Englisch) für SQL/DS).

Wenn der Standardwert des Anwendungsrequesters inritisches Englisch für CHARNAME (mit der CCSID 285) geändert wird, kann die Datenintegrität nicht aufrecht erhalten werden. Wenn der Anwendungsserver beispielsweise ein Zeichen fürritisches Pfund (£) übermittelt, zeigt der Anwendungsrequester stattdessen ein Dollarzeichen (\$) an. Bei anderen Zeichen können sich ebenfalls Veränderungen ergeben.

Zum Ändern des CCSID-Werts eines Anwendungsrequesters unter DB2 für VM müssen Sie den Parameter CHARNAME der Prozedur SQLINIT EXEC angeben.

Der korrekte CCSID-Wert für den Anwendungsserver wird von den Umsetzungstabellen auf dem Anwendungsrequester möglicherweise nicht unterstützt. Ist dies der Fall, können Sie die Verbindung auf eine der folgenden Arten herstellen:

- Aktualisieren Sie die vom Anwendungsrequester verwendete Umsetzungstabelle, so dass die Umsetzung zwischen der Standard-CCSID des Anwendungsservers und der Standard-CCSID des Anwendungsrequesters unterstützt wird. Diese Tabelle wird zum Erstellen der CMS-Datei ARISSTR MACRO verwendet, die vom Anwendungsrequester zur Unterstützung der CCSID-Umsetzung verwendet wird.
- Veranlassen Sie, dass die Standard-CCSID des Anwendungsservers geändert wird. Dies sollte nur durchgeführt werden, wenn es wirklich erforderlich ist. Beachten Sie dabei unbedingt die angestrebte Zielsetzung bei der Auswahl der Standard-CCSID des Anwendungsservers. Die Standard-CCSID des Anwendungsservers wirkt sich auf alle Anwendungsrequester aus, die eine Verbindung zu diesem Server herstellen, sowie auf die für den Anwendungsserver verwendete Bediener-Workstation und auf die in Tabellen auf dem Anwendungsserver gespeicherten Daten.

Weitere Informationen hierzu finden Sie im Handbuch *DB2 Server for VM System Administration*.

**Zugehörige Konzepte:**

- „DB2 für VM“ auf Seite 82
- „DB2 für VSE“ auf Seite 94
- „Umsetzung von Zeichendaten“ in *DB2 Connect Enterprise Edition Einstieg*

**Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsserver (VM)“ auf Seite 67
- „Definieren von DB2 als Anwendungsserver (VSE)“ auf Seite 59
- „Definieren von DB2 als Anwendungsrequester (VM)“ auf Seite 39



---

## Teil 5. Referenz für Host und iSeries



---

## Kapitel 15. Referenz

---

### Mit dem Konfigurationsassistenten konfigurierbare Produkte für die APPC-Kommunikation

Mit dem Konfigurationsassistenten (CA) kann APPC häufig automatisch konfiguriert werden. In der folgenden Tabelle sind die Produkte aufgelistet, die mit dem Konfigurationsassistenten konfiguriert werden können:

*Tabelle 4. Mit dem Konfigurationsassistenten konfigurierbare Produkte*

Produkt	Plattform	Mit dem CA konfiguriert?
IBM Personal Communications V4.2 und höher	Windows 98, Windows NT und Windows 2000	Ja
IBM Communications Server (Server)	Windows NT und Windows 2000	Ja
IBM Communications Server (Client)	Windows 98, Windows NT und Windows 2000	Nein
RUMBA	Windows 98, Windows NT und Windows 2000	Ja
Microsoft SNA (Server)	Windows NT und Windows 2000	Nein
Microsoft SNA (Client)	Windows 98, Windows NT und Windows 2000	Nein

#### Zugehörige Tasks:

- „Manuelles Konfigurieren der APPC-Kommunikation zwischen DB2 Connect und einem Host- und iSeries-Datenbankserver“ auf Seite 13
- „Aktualisieren von APPC-Profilen auf dem DB2 Connect-Server“ auf Seite 14

---

### Prüfliste zum Aktivieren eines DB2-Anwendungsservers (VSE)

Die folgende Prüfliste fasst die zum Aktivieren eines DRDA-Anwendungsservers erforderlichen Schritte zusammen, ausgehend von der Annahme, dass Ihr VSE-System mit der Zugriffsmethode ACF/VTAM für die Fernverarbeitung installiert ist und dass die zur Kommunikation mit den fernen Systemen erforderlichen VTAM-Definitionen (z. B. NCP-Definitionen) vollständig vorhanden sind.

1. Installieren Sie die Unterstützung für CICS-ISC und für die CICS-Funktion zur Neustartresynchronisation.
2. Definieren Sie CICS für VTAM für VSE.
3. Assemblieren Sie die Tabelle VTAM LOGMODE mit dem Eintrag IBMRDB.
4. Assemblieren Sie die CICS-Anmeldetabelle mit allen definierten fernen Benutzer-IDs und Kennwörtern.

5. Starten Sie CICS mit den richtigen SIT-Informationen:
  - ISC=YES
  - TST=YES, ARIAXELG definiert als RECOVERABLE in DFHTST und assembliert
  - APPLID=LU-Name (wie in der VTAM-Anweisung APPL definiert)
6. Definieren Sie die fernen Systeme für CICS (RDO darf verwendet werden):
  - CEDA DEF CONNECTION
  - CEDA DEF SESSION
  - CEDA DEF PROGRAM
  - CEDA DEF TRANSACTION

Diese Anweisungen müssen alle Definitionen in einer einzigen Gruppe (z. B. mit dem Namen IBMG) enthalten. Installieren Sie die Gruppe mit dem folgenden Befehl: CEDA INSTALL GROUP(IBM).
7. Aktualisieren Sie das Verzeichnis DBNAME (ARISDIRD.A):
  - Definieren Sie alle im Verzeichnis aufgeführten TPN für CICS. Nicht für CICS definierte TPN können nicht verwendet werden.
  - Definieren Sie jeden DRDA-Anwendungsserver unter DB2 für VSE in dem Verzeichnis mit einem gültigen TPN.
8. Führen Sie die Prozedur ARISBDID aus, um das aktualisierte Verzeichnis DBNAME zu assemblieren.
9. Bereiten Sie den Server unter DB2 für VSE wie folgt vor:
  - Führen Sie die Prozedur ARIS342D aus, um die DRDA-Unterstützung zu installieren.
  - Wenn Onlineanwendungen für DB2 für VSE (z. B. ISQL) in der CICS-Partition ausgeführt werden, erteilen Sie Planungsberechtigung (Schedule Authority) für die in der CICS-SIT-Tabelle angegebene CICS-APPLID.
  - Erteilen Sie Berechtigungen für alle fernen Benutzer.
10. Führen Sie (falls erforderlich) die CICS-Transaktion DAXP aus.
11. Starten Sie DB2 für VSE mit dem richtigen Parameter RMTUSERS und (optional) mit den Parametern DBNAME und SYNCNT.
12. Bereiten Sie Anwendungen auf dem VSE-DRDA-Anwendungsserver vor.

**Zugehörige Konzepte:**

- „DB2 für VSE“ auf Seite 94

**Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsserver (VSE)“ auf Seite 59

---

## Prüfliste zum Aktivieren eines DB2-Anwendungsrequesters (VM)

Die folgende Prüfliste fasst die erforderlichen Schritte zum Aktivieren eines DRDA-Anwendungsrequesters für DRDA-Kommunikation zusammen, ausgehend von der Annahme, dass Ihr VM-System mit der Zugriffsmethode ACF/VTAM für die Fernverarbeitung installiert ist und dass die zur Kommunikation mit den fernen Systemen erforderlichen VTAM-Definitionen (z. B. NCP-Definitionen) vollständig vorhanden sind.

1. Definieren Sie den lokalen AVS-Gateway für VTAM.
2. Installieren Sie DRDA-Unterstützung auf dem Anwendungsrequester unter DB2 für VM mit Hilfe der ausführbaren Datei ARISDBMA.
3. Definieren Sie ein CMS-Kommunikationsverzeichnis und fügen Sie dem VM-Verzeichnis auf der VM-Anwendungsmaschine andere erforderliche APPC-PASS-Anweisungen hinzu. Aktivieren Sie das Kommunikationsverzeichnis mit dem CMS-Befehl SET COMDIR.
4. Starten Sie VTAM und AVS, damit VM-Anwendungen über das SNA-Netzwerk kommunizieren können.
5. Setzen Sie die ausführbare Datei SQLINIT ab und geben Sie die Standarddatenbank, das zu verwendende Protokoll und die zu verwendenden CCSIDs mit Hilfe der Parameter DBNAME, PROTOCOL und CHARNAME an.
6. Bereiten Sie Anwendungen auf dem fernen Server vor.

### Zugehörige Konzepte:

- „DB2 für VM“ auf Seite 82

### Zugehörige Tasks:

- „Definieren von DB2 als Anwendungsrequester (VM)“ auf Seite 39

---

## Arbeitsblatt für TCP/IP-Parameterwerte

Verwenden Sie beim Ausführen der einzelnen Konfigurationsschritte die Spalte *Ihr Wert* in der folgenden Tabelle, um die erforderlichen Werte zu dokumentieren.

*Tabelle 5. Auf dem DB2 Connect-Server erforderliche TCP/IP-Werte*

Parameter	Beschreibung	Beispielwert	Ihr Wert
Hostname • Hostname ( <i>hostname</i> ) oder • IP-Adresse ( <i>ip-adresse</i> )	Verwenden Sie <i>hostname</i> oder <i>ip-adresse</i> des fernen Hosts.  Lösen Sie diesen Parameter wie folgt auf: <ul style="list-style-type: none"><li>• Erkundigen Sie sich bei Ihrem Netzwerkadministrator nach dem Host-Namen.</li><li>• Erkundigen Sie sich bei Ihrem Netzwerkadministrator nach der IP-Adresse, oder geben Sie den Befehl <b>ping</b> <i>hostname</i> ein.</li></ul>	nyx oder 9.21.15.235	

Tabelle 5. Auf dem DB2 Connect-Server erforderliche TCP/IP-Werte (Forts.)

Parameter	Beschreibung	Beispielwert	Ihr Wert
Servicename • Name des Verbindungsservices ( <i>svcname</i> ) oder • Portnummer/Protokoll ( <i>portnummer/tcp</i> )	<p>In der Datei <i>services</i> erforderliche Werte.</p> <p>Der Name des Verbindungsservices (Connection Service) ist ein beliebiger Name, der für die Portnummer (<i>portnummer</i>) der Verbindung auf dem Client steht.</p> <p>Die Portnummer für den DB2 Connect-Server muss mit der Portnummer identisch sein, die dem Parameter <i>svcname</i> in der Datei <i>services</i> auf dem Hostdatenbankserver zugeordnet ist. (Der Parameter <i>svcname</i> befindet sich in der Konfigurationsdatei des Datenbankmanagers auf dem Host.) Dieser Wert darf von keiner anderen Anwendung verwendet werden und muss innerhalb der Datei <i>services</i> eindeutig sein.</p> <p>Auf UNIX-Plattformen muss dieser Wert in der Regel mindestens 1024 betragen.</p> <p>Wenden Sie sich an Ihren Datenbankadministrator, um die zum Konfigurieren des Hostsystems verwendeten Werte zu erfahren.</p>	host1 oder 3700/tcp	
Zieldatenbankname ( <i>zieldatenbankname</i> )	<p>Der Datenbankname, wie er auf dem Host- oder iSeries-System bekannt ist.</p> <ul style="list-style-type: none"> <li>• Wenn Sie eine Verbindung zu einem DB2 UDB für OS/390- und z/OS-System herstellen, müssen Sie den Standortnamen verwenden.</li> <li>• Wenn Sie eine Verbindung zu einem DB2 UDB für iSeries-System herstellen, müssen Sie den Namen der lokalen RDB verwenden.</li> <li>• Wenn Sie eine Verbindung zu einem DB2 für VM- oder DB2 für VSE-System herstellen, müssen Sie den Datenbanknamen verwenden.</li> </ul>	newyork	
Name der lokalen Datenbank ( <i>lokaler-dcs-name</i> )	Ein beliebiger lokaler Kurzname für die Verwendung durch den DB2 Connect-Server, der die ferne Host- oder iSeries-Datenbank bezeichnet.	ny	

Tabelle 5. Auf dem DB2 Connect-Server erforderliche TCP/IP-Werte (Forts.)

Parameter	Beschreibung	Beispielwert	Ihr Wert
Knotenname ( <i>knotenname</i> )	Ein lokaler Aliasname oder Kurzname, der den Knoten beschreibt, zu dem eine Verbindung hergestellt werden soll. Sie können einen beliebigen Namen auswählen. Alle Werte für Knotennamen im lokalen Knotenverzeichnis müssen jedoch eindeutig sein.	db2node	

**Zugehörige Tasks:**

- „Manuelles Konfigurieren der TCP/IP-Kommunikation zwischen DB2 Connect und einem Host- bzw. iSeries-Datenbankserver“ auf Seite 3

---

## TCP/IP-Parameterwerte zum Katalogisieren von Datenbanken

Füllen Sie im folgenden Arbeitsblatt die Spalte *Ihr Wert* aus.

Tabelle 6. Arbeitsblatt: Parameterwerte für das Katalogisieren von Datenbanken

Parameter	Beschreibung	Beispielwert	Ihr Wert
Datenbankname ( <i>datenbankname</i> )	Lokaler DCS-Datenbankname ( <i>lokal-der-dcs-name</i> ) der fernen Datenbank. Diesen haben Sie beim Katalogisieren des DCS-Datenbankverzeichnisses angegeben. Beispiel: ny.	ny	
Aliasname der Datenbank ( <i>aliasname-der-datenbank</i> )	Ein beliebiger lokaler Kurzname für die ferne Datenbank. Wenn Sie keinen Aliasnamen angeben, wird der Datenbankname ( <i>datenbankname</i> ) standardmäßig auch als Aliasname verwendet. Verwenden Sie diesen Namen, wenn Sie eine Verbindung zu der Datenbank von einem Client aus herstellen.	localny	
Knotenname ( <i>knotenname</i> )	Verwenden Sie für den Knotennamen ( <i>knoten</i> ) den Wert, den Sie zum Katalogisieren des Knotens verwendet haben.	db2node	

**Zugehörige Tasks:**

- „Manuelles Konfigurieren der TCP/IP-Kommunikation zwischen DB2 Connect und einem Host- bzw. iSeries-Datenbankserver“ auf Seite 3
- „Katalogisieren der Datenbank“ auf Seite 8

## Arbeitsblatt für APPC-Parameterwerte

Bevor Sie den DB2 Connect-Server konfigurieren, sollten Sie dieses Arbeitsblatt für *jede* Host- bzw. iSeries-Datenbank, zu der eine Verbindung hergestellt werden soll, vom Host- oder iSeries-Administrator und dem LAN-Administrator ausfüllen lassen.

Nachdem Sie die Spalte *Ihr Wert* ausgefüllt haben, können Sie anhand des Arbeitsblatts die APPC-Kommunikation für DB2 Connect konfigurieren. Ersetzen Sie während des Konfigurationsvorgangs die in den Konfigurationsanweisungen enthaltenen Beispielwerte durch Ihre eigenen Werte aus dem Arbeitsblatt. Die in den Kästchen angegebenen Zahlen (wie zum Beispiel **1**) erleichtern die Zuordnung der Konfigurationsanweisungen zu den entsprechenden Werten des Arbeitsblatts.

Im Arbeitsblatt und in den Konfigurationsanweisungen finden Sie empfohlene Angaben oder Beispielwerte für erforderliche Konfigurationsparameter. Verwenden Sie für andere Parameter die Standardwerte des Kommunikationsprogramms. Wenn Ihre Netzwerkkonfiguration von der in diesen Anweisungen verwendeten Konfiguration abweicht, erkundigen Sie sich bei Ihrem Netzwerkadministrator nach den geeigneten Werten für Ihr Netzwerk.

In den Konfigurationsanweisungen wird das Symbol **\*** zur Bezeichnung solcher Einträge verwendet, die zwar geändert werden müssen, jedoch nicht im Arbeitsblatt enthalten sind.

Tabelle 7. Arbeitsblatt zur Planung von Host- und iSeries-Serververbindungen

Ref.-Nr.	Name auf dem DB2 Connect-Server	Netzwerk- oder VTAM-Name	Beispielwert	Ihr Wert
<b>Netzwerkelemente auf dem Host- oder iSeries-Datenbankserver</b>				
<b>1</b>	Hostname	Name des lokalen Netzwerks	SPIFNET	
<b>2</b>	Name der Partner-LU	Anwendungsname	NYM2DB2	
<b>3</b>	Netzwerk-ID		SPIFNET	
<b>4</b>	Partnerknotenname	Lokaler CP- oder SSCP-Name	NYX	
<b>5</b>	Zieldatenbankname ( <i>zieldatenbankname</i> )	<b>OS/390 oder z/OS:</b> LOCATION NAME (Standortname)  <b>VM/VSE:</b> DBNAME (Datenbankname)  <b>iSeries:</b> RDB-Name	NEWYORK	
<b>6</b>	Verbindungsname oder Modusname		IBMRDB	
<b>7</b>	Verbindungsname (Link Name)		LINKHOST	
<b>8</b>	Adresse des fernen Netzwerks oder LAN-Adresse	Adresse des lokalen Adapters oder Zieladresse	400009451902	
<b>Netzwerkelemente auf dem DB2 Connect-Server</b>				
<b>9</b>	Netzwerk- oder LAN-ID		SPIFNET	
<b>10</b>	Name des lokalen Steuerpunkts		NYX1GW	
<b>11</b>	Name der lokalen LU		NYX1GW0A	
<b>12</b>	Aliasname der lokalen LU		NYX1GW0A	

Tabelle 7. Arbeitsblatt zur Planung von Host- und iSeries-Serververbindungen (Forts.)

Ref.-Nr.	Name auf dem DB2 Connect-Server	Netzwerk- oder VTAM-Name	Beispielwert	Ihr Wert
<b>13</b>	Lokaler Knoten oder Knoten-ID	ID BLK	071	
<b>14</b>		ID NUM	27509	
<b>15</b>	Modusname		IBMRDB	
<b>16</b>	Symbolischer Bestimmungsname		DB2CPIC	
<b>17</b>	Name des fernen Transaktionsprogramms (TP)		<b>OS/390 oder z/OS:</b> X'07'6DB ('07F6C4C2') oder DB2DRDA  <b>VM/VSE:</b> AXE für VSE. Der Name der DB2 für VM-Datenbank oder X'07'6DB ('07F6C4C2') für VM  <b>iSeries:</b> X'07'6DB ('07F6C4C2') oder QCNTEDDM	
<b>DB2 Verzeichniseinträge auf dem DB2 Connect-Server</b>				
<b>19</b>	Knotenname		db2node	
<b>19</b>	Sicherheit		program	
<b>20</b>	Name der lokalen Datenbank ( <i>lokaler-dcs-name</i> )		ny	

Füllen Sie für jeden Server, zu dem eine Verbindung hergestellt werden soll, eine Kopie des Arbeitsblatts wie folgt aus:

1. Ermitteln Sie für *Netzwerk-ID* den Netzwerknamen des Hosts oder der iSeries sowie der DB2 Connect-Server (**1**, **3** und **9**). In der Regel sind diese Werte identisch. (Zum Beispiel SPIFNET.)
2. Ermitteln Sie für *Name der Partner-LU* (**2**) den Namen der VTAM-Anwendung (APPL) für OS/390, z/OS, VSE oder VM. Ermitteln Sie den lokalen Steuerpunktnamen für iSeries.
3. Ermitteln Sie für *Partnerknotenname* (**4**) den SSCP-Namen für OS/390, z/OS, VM oder VSE. Ermitteln Sie den lokalen Steuerpunktnamen für iSeries.
4. Ermitteln Sie für *Datenbankname* (**5**) den Namen der Host- und iSeries-Datenbank. Für OS/390 oder z/OS ist dies der Wert *LOCATION NAME*, für VM oder VSE *DBNAME* und für iSeries der Name einer relationalen Datenbank (RDB).
5. Für *Modusname* (**6** und **15**) genügt normalerweise die Standardangabe IBMRDB.
6. Ermitteln Sie für *Adresse des fernen Netzwerks* (**8**) die Controller-Adresse oder die lokale Adapteradresse des Ziel-Host- oder iSeries-Systems.
7. Ermitteln Sie den *lokalen Steuerpunktnamen* (**10**) des DB2 Connect-Servers. Dieser Name entspricht normalerweise dem PU-Namen für das System.

8. Ermitteln Sie den *Namen der lokalen LU* ( **11** ), der von DB2 Connect verwendet werden soll. Wenn Sie einen Synchronisationspunktmanager (SPM) zur Verwaltung von Aktualisierungen auf mehreren Systemen verwenden (zwei-phasige Festschreibung), sollte die lokale LU mit der LU für den SPM identisch sein. In diesem Fall darf diese LU nicht zugleich die Steuerpunkt-LU sein.
9. Der *Aliasname der lokalen LU* ( **12** ) ist in der Regel mit dem Namen der lokalen LU ( **11** ) identisch.
10. Legen Sie als *lokalen Knoten* oder *Knoten-ID* ( **13** und **14** ) die Werte fest, die für IDBLK und IDNUM für den DB2 Connect-Server eingetragen sind. Der Standardwert dürfte korrekt sein.
11. Wählen Sie für *Symbolischer Bestimmungsname* ( **16** ) einen geeigneten Wert aus.
12. Verwenden Sie als *Namen des (fernen) Transaktionsprogramms* ( **17** ) die Standardeinstellungen, die im Arbeitsblatt angeführt sind.
13. Lassen Sie die anderen Felder ( **18** bis **21** ) vorerst frei.

#### Zugehörige Tasks:

- „Manuelles Konfigurieren der APPC-Kommunikation zwischen DB2 Connect und einem Host- und iSeries-Datenbankserver“ auf Seite 13

---

## Schlüsselwörter der VTAM-Anweisung APPL von DB2 Connect

Für die VTAM-Anweisung APPL sind viele Schlüsselwörter verfügbar. Hier werden lediglich die Schlüsselwörter erläutert, die für dieses Handbuch relevant sind.

### LUDBD1

VTAM verwendet den Kennsatz der Anweisung APPL als LU-Namen. In diesem Fall ist der LU-Name LUDBD1. Die APPL-Syntax lässt keinen vollständigen NETID.LUNAME-Wert zu. Der NETID-Wert wird in der VTAM-Anweisung APPL nicht angegeben, da allen VTAM-Anwendungen automatisch die NETID für das VTAM-System zugeordnet wird.

### AUTOSES=1

Die Anzahl der SNA-Konfliktgewinnersitzungen, die automatisch gestartet werden, wenn eine APPC-Anforderung zum Ändern der Sitzungsanzahl (Change Number of Sessions - CNOS) abgesetzt wird.

Sie müssen nicht alle APPC-Sitzungen zwischen zwei beliebigen Partnerpaaren der verteilten Datenbankumgebung automatisch starten. Liegt der Wert für AUTOSES unter der Konfliktgewinnerbegrenzung (DMINWNL), verzögert VTAM das Starten der übrigen SNA-Sitzungen, bis sie von einer Anwendung für verteilte Datenbanken benötigt werden.

### DMINWNL=10

Die Anzahl der Sitzungen, in denen dieses System der Konfliktgewinner ist. Die CNOS-Verarbeitung verwendet den Parameter DMINWNL als Standardwert. Er kann jedoch für jeden Partner durch Hinzufügen einer Zeile zur Tabelle SYSIBM.SYSLUMODES in der Kommunikationsdatenbank außer Kraft gesetzt werden.

**DMINWNR=10**

Die Anzahl der Sitzungen, in denen das Partnersystem der Konfliktgewinner ist. Die CNOS-Verarbeitung verwendet den Parameter DMINWNR als Standardwert. Er kann jedoch für jeden Partner durch Hinzufügen einer Zeile zur Tabelle SYSIBM.SYSLUMODES in der Kommunikationsdatenbank außer Kraft gesetzt werden.

**DSESLIM=20**

Die Gesamtzahl der Sitzungen (Konfliktgewinner und Konfliktverlierer), die zwischen DB2 und einem anderen verteilten System für einen bestimmten Modusgruppennamen hergestellt werden können. Die CNOS-Verarbeitung verwendet den Parameter DSESLIM als Standardwert. Er kann jedoch für jeden Partner durch Hinzufügen einer Zeile zur Tabelle SYSIBM.SYSLUMODES in der Kommunikationsdatenbank außer Kraft gesetzt werden.

Wenn der Partner die im Parameter DSESLIM, DMINWNL oder DMINWNR angeforderte Anzahl der Sitzungen nicht unterstützen kann, vereinbart der CNOS-Prozess für diese Parameter neue Werte, die für den Partner akzeptabel sind.

**EAS=9999**

Ein Schätzwert für die Gesamtzahl der Sitzungen, die von dieser VTAM-LU benötigt werden.

**MODETAB=RDBMODES**

Gibt die VTAM-MODE-Tabelle an, in der sich die einzelnen Modusnamen von DB2 befinden.

**PRCT=PSWDBD1**

Gibt das VTAM-Kennwort an, das benutzt werden muss, wenn DB2 versucht, eine Verbindung zu VTAM herzustellen. Wird das Schlüsselwort PRCT übergangen, ist kein Kennwort erforderlich, und Sie sollten das Schlüsselwort PASSWORD= im Dienstprogramm zum Ändern des Protokollinventars von DB2 übergehen.

**SECACPT=ALREADYV**

Gibt den höchsten Wert für die SNA-Sicherheit auf Dialogebene an, der von diesem DB2-System akzeptiert wird, wenn es eine Anforderung für verteilte Datenbanken von einem fernen System empfängt. Durch das Schlüsselwort ALREADYV wird angegeben, dass dieses DB2-System die folgenden drei Sicherheitsoptionen für SNA-Sitzungen von anderen DRDA-Systemen akzeptieren kann, die Daten von diesem DB2-System anfordern:

- SECURITY=SAME (eine bereits überprüfte Anforderung, die nur die Benutzer-ID des Requesters enthält)
- SECURITY=PGM (eine Anforderung, in der die Benutzer-ID und das Kennwort des Requesters enthalten sind)
- SECURITY=NONE (eine Anforderung, die keine Sicherheitsinformationen enthält). DB2 weist DRDA-Anforderungen mit SECURITY=NONE zurück

Es wird empfohlen, stets SECACPT=ALREADYV anzugeben, weil die Stufe der SNA-Dialogsicherheit für jeden Partner von DB2 aus der DB2-Kommunikationsdatenbank (Spalte USERSECURITY der Tabelle SYSIBM.SYSLUNAMES) stammt. SECACPT=ALREADYV gibt Ihnen die größte Flexibilität bei der Auswahl der Werte für USERSECURITY.

**VERIFY=NONE**

Gibt die Sicherheitsstufe für SNA-Sitzungen (Partner-LU-Prüfung) an, die für dieses DB2-System erforderlich ist. Der Wert NONE gibt an, dass keine Partner-LU-Prüfung erforderlich ist.

DB2 schränkt Ihre Auswahl für das Schlüsselwort VERIFY nicht ein. In einem nicht gesicherten Netzwerk wird die Einstellung VERIFY=REQUIRED empfohlen. Durch VERIFY=REQUIRED wird bewirkt, dass VTAM solche Partner zurückweist, die keine Partner-LU-Prüfung ausführen können. Wird VERIFY=OPTIONAL angegeben, führt VTAM die Partner-LU-Prüfung nur für solche Partner durch, die diese Unterstützung bereitstellen.

**VPACING=2**

Stellt den VTAM-Nachrichtendosierungszähler auf 2 ein.

**SYNCLVL=SYNCPT**

Gibt an, dass DB2 in der Lage ist, zweiphasige Festschreibung zu unterstützen. VTAM verwendet diese Informationen, um den Partner zu informieren, dass die zweiphasige Festschreibung verfügbar ist. Ist dieses Schlüsselwort vorhanden, verwendet DB2 automatisch die zweiphasige Festschreibung, sofern der Partner sie unterstützen kann.

**ATNLOSS=ALL**

Gibt an, dass DB2 bei jeder Beendigung einer VTAM-Sitzung informiert werden muss. Hierdurch wird sichergestellt, dass DB2 eine SNA-Resynchronisation ausführt, wenn sie erforderlich ist.

Mit DSESLIM, DMINWNL und DMINWNR können Sie standardmäßige VTAM-Sitzungsbegrenzungen für alle Partner festlegen. Für Partner mit speziellen Anforderungen an die Sitzungsbegrenzung können Sie die standardmäßigen Sitzungsbegrenzungen mit Hilfe der Tabelle SYSIBM.SYSLUMODES überschreiben. So ist es möglicherweise günstig, standardmäßige VTAM-Sitzungsbegrenzungen anzugeben, die für Ihre Windows-Systeme geeignet sind. Für andere Partner können Sie dann Zeilen in der Tabelle SYSIBM.SYSLUMODES erstellen, um die gewünschten Sitzungsbegrenzungen zu definieren. Beispielwerte:

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

**Zugehörige Konzepte:**

- „Sicherheitssystem - Anwendungsserver (OS/390 und z/OS)“ auf Seite 105
- „Netzwerksicherheit - Anwendungsserver (OS/390 und z/OS)“ auf Seite 102
- „Netzwerksicherheit - Anwendungsrequester (OS/390 und z/OS)“ auf Seite 119
- „Sicherheitssystem - Anwendungsrequester (OS/390 und z/OS)“ auf Seite 121

**Zugehörige Tasks:**

- „Definieren von DB2 als Anwendungsserver (OS/390 und z/OS)“ auf Seite 47
- „Definieren von DB2 als Anwendungsrequester (OS/390 und z/OS)“ auf Seite 25

---

## **Teil 6. Anhänge und Schlussteil**



---

# Anhang A. Technische Informationen zu DB2 Universal Database

---

## DB2-Dokumentation und Hilfe

Die technischen Informationen zu DB2<sup>®</sup> stehen über die folgenden Tools und Methoden zur Verfügung:

- DB2 Information - Unterstützung
  - Themen
  - Hilfe für DB2-Tools
  - Beispielprogramme
  - Lernprogramme
- Für den Download verfügbare PDF-Dateien, PDF-Dateien auf CD und gedruckte Bücher
  - Handbücher
  - Referenzhandbücher
- Befehlszeilenhilfe
  - Hilfe für Befehle
  - Hilfe für Nachrichten
  - Hilfe für SQL-Anweisungen
- Installierter Quellcode
  - Beispielprogramme

Darüber hinaus können Sie auf zusätzliche technische Informationen zu DB2 Universal Database<sup>™</sup>, wie beispielsweise technische Hinweise (Technotes), White Papers und Redbooks<sup>™</sup>, online über [ibm.com](http://ibm.com)<sup>®</sup> zugreifen. Rufen Sie die Website 'DB2 Information Management - Library' unter [www.ibm.com/software/data/pubs/](http://www.ibm.com/software/data/pubs/) auf.

## Aktualisierungen der DB2-Dokumentation

In bestimmten Fällen stellt IBM<sup>®</sup> in regelmäßigen Abständen Dokumentations-Fix-Paks und andere Dokumentationsaktualisierungen für 'DB2 Information - Unterstützung' zur Verfügung.

Wenn Sie über <http://publib.boulder.ibm.com/infocenter/db2help/> auf 'DB2 Information - Unterstützung' zugreifen, erhalten Sie stets die neuesten Informationen. Falls Sie 'DB2 Information - Unterstützung' lokal installiert haben, müssen Sie alle Aktualisierungen manuell installieren, bevor Sie sie anzeigen können. Diese Dokumentationsaktualisierungen ermöglichen Ihnen, die Informationen, die Sie von der CD mit *DB2 Information - Unterstützung* installiert haben, auf den neuesten Stand zu bringen, sobald neue Informationen verfügbar sind.

'DB2 Information - Unterstützung' wird häufiger aktualisiert als die PDF- und Hardcopy-Bücher. Um stets die jeweils neuesten technischen Informationen zu DB2 zur Verfügung zu haben, sollten Sie die Dokumentationsaktualisierungen installieren, sobald sie verfügbar sind, oder 'DB2 Information - Unterstützung' über die Website [www.ibm.com](http://www.ibm.com) aufrufen.

---

## DB2 Information - Unterstützung

Die DB2®-Komponente 'DB2 Information - Unterstützung' bietet Ihnen die Möglichkeit, auf alle Informationen zuzugreifen, die Sie zur optimalen Nutzung der Produkte innerhalb der DB2-Produktfamilie, wie z. B. DB2 Universal Database™, DB2 Connect™, DB2 Information Integrator und DB2 Query Patroller™, benötigen. 'DB2 Information - Unterstützung' dokumentiert auch die wichtigsten DB2-Funktionen und -Komponenten, einschließlich der Funktionen für die Replikation, das Data Warehousing und die DB2 Extender.

Wenn Sie für die Anzeige von 'DB2 Information - Unterstützung' Mozilla ab Version 1.0 oder Microsoft® Internet Explorer ab Version 5.5 verwenden, stehen Ihnen die folgenden Funktionen zur Verfügung. Für bestimmte Funktionen muss die JavaScript™-Unterstützung aktiviert werden :

### Flexible Installationsoptionen

Wählen Sie für die Anzeige der DB2-Dokumentation die Option, die Ihren Anforderungen am besten entspricht:

- Stellen Sie ohne großen Aufwand sicher, dass Ihre Dokumentation stets auf dem neuesten Stand ist, indem Sie auf die gesamte Dokumentation direkt über 'DB2 Information - Unterstützung' auf der IBM® Website unter <http://publib.boulder.ibm.com/infocenter/db2help/> zugreifen.
- Reduzieren Sie den Aktualisierungsaufwand auf ein Minimum und begrenzen Sie den Datenaustausch auf Ihr Intranet, indem Sie die DB2-Dokumentation auf einem einzigen Server innerhalb Ihres Intranets installieren.
- Erzielen Sie maximale Flexibilität und reduzieren Sie die Abhängigkeit von Netzwerkverbindungen, indem Sie die DB2-Dokumentation auf dem eigenen Computer installieren.

### Suchen

Sie können alle Themen in 'DB2 Information - Unterstützung' durchsuchen, indem Sie einen Suchbegriff im Textfeld **Suchen** eingeben. Schließen Sie Begriffe in Anführungszeichen ein, wenn Sie nach exakten Übereinstimmungen suchen möchten. Mit Hilfe von Platzhalterzeichen (\*, ?) und Booleschen Operatoren (AND, NOT, OR) können Sie die Suche eingrenzen.

### Aufgabenorientiertes Inhaltsverzeichnis

Die Themen in der DB2-Dokumentation können über ein zentrales Inhaltsverzeichnis lokalisiert werden. Das Inhaltsverzeichnis ist primär auf der Basis übergeordneter Aufgabenbereiche aufgebaut, enthält jedoch auch Einträge für Produktübersichten, Ziele, Referenzinformationen sowie einen Index und ein Glossar.

- Produktübersichten beschreiben die Beziehung zwischen den in der DB2-Produktfamilie verfügbaren Produkten sowie die von den einzelnen Produkten bereitgestellten Funktionen und enthalten darüber hinaus die neuesten Release-Informationen für diese Produkte.
- Aufgabenkategorien, wie z. B. Installation, Verwaltung und Entwicklung, umfassen Themen, mit deren Hilfe Sie die einzelnen Aufgaben schnell ausführen und sich außerdem genauere Kenntnisse über die Hintergrundinformationen zu diesen Aufgaben verschaffen können.
- In den Referenzthemen finden Sie detaillierte Informationen zu einem Thema, einschließlich der Anweisungs- und Befehlssyntax, der Hilfetexte zu Nachrichten und der Konfigurationsparameter.

### **Anzeigen des aktuellen Themas im Inhaltsverzeichnis**

Wenn Sie sehen möchten, welchem Bereich des Inhaltsverzeichnisses das aktuelle Thema zugeordnet ist, klicken Sie den Knopf **Aktualisieren / aktuelles Thema anzeigen** im Teilfenster des Inhaltsverzeichnisses oder den Knopf **Im Inhaltsverzeichnis anzeigen** im Inhaltsteilfenster an. Diese Funktion ist zum Beispiel dann von Nutzen, wenn Sie mehreren Links zu zugehörigen Themen in verschiedenen Dateien gefolgt sind oder ein Thema über das Ergebnis einer Suche aufgerufen haben.

**Index** Über den Index können Sie auf die gesamte Dokumentation zugreifen. Der Index ist alphabetisch nach Indexeinträgen sortiert.

### **Glossar**

Im Glossar finden Sie Definitionen zu Termini, die in der DB2-Dokumentation verwendet werden. Das Glossar ist alphabetisch nach Glossareinträgen sortiert.

### **Integrierte übersetzte Informationen**

Die Informationen in 'DB2 Information - Unterstützung' werden in der Sprache angezeigt, die Sie in den Benutzervorgaben des verwendeten Browsers festgelegt haben. Ist ein Thema nicht in der bevorzugten Sprache verfügbar, wird die englische Version des Themas angezeigt.

Technische Informationen zu iSeries™ finden Sie im Informationszentrum von IBM eServer™ iSeries unter [www.ibm.com/eserver/iseres/infocenter/](http://www.ibm.com/eserver/iseres/infocenter/).

### **Zugehörige Tasks:**

- „Aktualisieren der auf Ihrem Computer oder Intranet-Server installierten Komponente 'DB2 Information - Unterstützung'“ auf Seite 161

---

## **DB2 Information - Unterstützung: Installationsszenarios**

Je nach Arbeitsumgebung kann es unterschiedliche Anforderungen hinsichtlich des Zugriffs auf DB2®-Informationen geben. Sie können auf 'DB2 Information - Unterstützung' entweder auf der IBM® Website zugreifen oder auf einem Server im unternehmensinternen Netzwerk oder auf eine auf dem lokalen Computer installierte Version. In allen drei Fällen befindet sich die Dokumentation in 'DB2 Information - Unterstützung', einem strukturierten System themenbasierter Informationen, die über einen Browser angezeigt werden können. Standardmäßig greifen DB2-Produkte auf 'DB2 Information - Unterstützung' auf der IBM Website zu. Wenn Sie jedoch auf 'DB2 Information - Unterstützung' auf einem Intranet-Server oder auf dem eigenen Computer zugreifen möchten, müssen Sie 'DB2 Information - Unterstützung' mit Hilfe der entsprechenden CD installieren, die sich im Programmpaket des Produkts befindet. Anhand der nachfolgenden Übersicht über die verfügbaren Optionen für den Zugriff auf die DB2-Dokumentation und mit Hilfe der drei Installationsszenarios können Sie ermitteln, welche Methode für den Zugriff auf 'DB2 Information - Unterstützung' für Ihre Anforderungen und Arbeitsumgebung am besten geeignet ist und welche Aspekte Sie bei der Installation berücksichtigen müssen.

### **Übersicht über die verfügbaren Optionen für den Zugriff auf die DB2-Dokumentation:**

Die folgende Tabelle enthält Empfehlungen hinsichtlich der für Ihre Arbeitsumgebung geeigneten Optionen für den Zugriff auf die DB2-Produktdokumentation in 'DB2 Information - Unterstützung'.

Internetzugriff	Intranetzugriff	Empfehlung
Ja	Ja	Greifen Sie entweder über die IBM Website auf 'DB2 Information - Unterstützung' zu oder auf die auf einem Intranet-Server installierte Version von 'DB2 Information - Unterstützung'.
Ja	Nein	Greifen Sie über die IBM Website auf 'DB2 Information - Unterstützung' zu.
Nein	Ja	Greifen Sie auf die auf einem Intranet-Server installierte Version von 'DB2 Information - Unterstützung' zu.
Nein	Nein	Greifen Sie auf die auf einem lokalen Computer installierte Version von 'DB2 Information - Unterstützung' zu.

### Szenario: Zugriff auf 'DB2 Information - Unterstützung' auf Ihrem Computer:

Tsu-Chen besitzt eine Fabrik in einer Kleinstadt, in der es vor Ort keinen Anbieter für einen Internetzugang gibt. Für die Verwaltung des Lagerbestands, der Produktbestellungen, der Betriebsausgaben und seines Bankkontos hat Tsu-Chen DB2 Universal Database™ gekauft. Da er zuvor noch nie ein DB2-Produkt verwendet hat, muss er anhand der DB2-Produktdokumentation lernen, wie die Verwaltung funktioniert.

Nachdem er DB2 Universal Database mit der Option für die Standardinstallation auf seinem Computer installiert hat, versucht Tsu-Chen, auf die DB2-Dokumentation zuzugreifen. Sein Browser zeigt jedoch eine Fehlermeldung mit der Information an, dass die Seite, die geöffnet werden sollte, nicht gefunden werden kann. Tsu-Chen überprüft das Installationshandbuch für sein DB2-Produkt und findet heraus, dass er 'DB2 Information - Unterstützung' zunächst installieren muss, um auf seinem Computer auf die DB2-Dokumentation zugreifen zu können. Im Programmpaket findet er die *CD für DB2 Information - Unterstützung* und installiert sie.

Über das Programm zum Aufrufen von Anwendungen für sein Betriebssystem hat Tsu-Chen nun Zugriff auf 'DB2 Information - Unterstützung', um sich mit der Verwendung seines DB2-Produkts vertraut zu machen und so einen wertvollen Beitrag zum Erfolg seines Unternehmens leisten.

### Szenario: Zugriff auf 'DB2 Information - Unterstützung' über die IBM Website:

Colin ist IT-Berater bei einer Schulungsfirma. Er ist auf Datenbanktechnologie und SQL spezialisiert und hält Seminare zu diesen Themen für Unternehmen aus ganz Nordamerika ab. Hierfür verwendet er DB2 Universal Database. Im Rahmen seiner Seminare verwendet Colin die DB2-Dokumentation als Unterrichtsmaterial. Für SQL-Kurse beispielsweise verwendet Colin die DB2-Dokumentation zu SQL, um die grundlegende und erweiterte Syntax für Datenbankabfragen zu unterrichten.

Die meisten Unternehmen, bei denen Colin unterrichtet, verfügen über einen Internetzugang. Aus diesem Grund entschied sich Colin, seinen tragbaren Computer für den Zugriff auf 'DB2 Information - Unterstützung' über die Website von IBM zu konfigurieren, als er die letzte Version von DB2 Universal Database installiert hat. Diese Konfiguration ermöglicht es Colin, während seiner Seminare online auf die neueste DB2-Dokumentation zuzugreifen.

Wenn er auf Reisen ist, hat Colin bisweilen allerdings keinen Internetzugang. Dieser Umstand war für ihn recht problematisch, insbesondere dann, wenn er Zugriff auf die DB2-Dokumentation benötigte, um sich auf seine Seminare vorzubereiten. Um Situationen wie diese zu vermeiden, installierte Colin eine Kopie von 'DB2 Information - Unterstützung' auf seinem tragbaren Computer.

Auf diese Weise hat Colin nun jederzeit eine Kopie der DB2-Dokumentation zur Verfügung und ist dadurch wesentlich flexibler. Mit dem Befehl **db2set** kann Colin ohne Schwierigkeiten die Registrierdatenbankvariablen auf seinem tragbaren Computer so konfigurieren, dass er den jeweiligen Umständen entsprechend entweder über die Website von IBM oder über seinen tragbaren Computer auf 'DB2 Information - Unterstützung' zugreifen kann.

#### **Szenario: Zugriff auf 'DB2 Information - Unterstützung' über einen Intranet-Server:**

Eva arbeitet als leitende Datenbankadministratorin für eine Lebensversicherung. In ihre Zuständigkeit fallen auch das Installieren und Konfigurieren der neuesten Version von DB2 Universal Database auf den UNIX<sup>®</sup>-basierten Datenbankservern des Unternehmens. Vor Kurzem hat das Unternehmen seine Mitarbeiter darüber informiert, dass sie aus Sicherheitsgründen während der Arbeitszeit keinen Internetzugang erhalten würden. Da ihr Unternehmen in einer Netzwerkumgebung arbeitet, beschließt Eva, eine Kopie von 'DB2 Information - Unterstützung' auf einem Intranet-Server zu installieren, damit alle Mitarbeiter, die das Data Warehouse des Unternehmens regelmäßig verwenden (Vertriebsbeauftragte, Vertriebsleiter und Geschäftsanalysten), Zugriff auf die DB2-Dokumentation haben.

Eva weist ihr Datenbankteam an, die neueste Version von DB2 Universal Database auf allen Computern der Mitarbeiter mit Hilfe einer Antwortdatei zu installieren, um sicherzustellen, dass die Konfiguration des Zugriffs auf 'DB2 Information - Unterstützung' auf allen Computern mit dem Hostnamen und der Portnummer des Intranet-Servers erfolgt.

Durch ein Missverständnis installiert jedoch Migual, ein Datenbankadministrator in Evas Team, eine Kopie von 'DB2 Information - Unterstützung' auf mehreren Mitarbeitercomputern, anstatt DB2 Universal Database für den Zugriff auf 'DB2 Information - Unterstützung' über den Intranet-Server zu konfigurieren. Um diesen Fehler zu korrigieren, weist Eva Migual an, mit dem Befehl **db2set** die Registrierdatenbankvariablen von 'DB2 Information - Unterstützung' (DB2\_DOCHOST für den Hostnamen und DB2\_DOCPORT für die Portnummer) auf allen entsprechenden Computern zu ändern. Anschließend haben nun alle erforderlichen Computer im Netzwerk Zugriff auf 'DB2 Information - Unterstützung', und die Mitarbeiter können mit Hilfe der DB2-Dokumentation Antworten auf ihre Fragen zu DB2 finden.

---

## **Installation von 'DB2 Information - Unterstützung' mit dem DB2-Installationsassistenten (UNIX)**

Es gibt drei Möglichkeiten, auf die DB2-Produktdokumentation zuzugreifen: auf der IBM Website, auf einem Intranet-Server oder auf eine auf dem lokalen Computer installierte Version. Standardmäßig greifen DB2-Produkte auf die DB2-Dokumentation auf der IBM Website zu. Wenn Sie jedoch auf die DB2-Dokumentation auf einem Intranet-Server oder auf dem eigenen Computer zugreifen möchten, müssen Sie die Dokumentation von der CD 'DB2 Information - Unterstützung' aus installieren. Mit dem DB2-Installationsassistenten können Sie Ihre Installationsein-

stellungen definieren und 'DB2 Information - Unterstützung' auf einem Computer installieren, der das Betriebssystem UNIX verwendet.

### Voraussetzungen:

Dieser Abschnitt erläutert die Voraussetzungen für Hardware, Betriebssystem, Software und Kommunikation zum Installieren von 'DB2 Information - Unterstützung' auf UNIX-Computern.

- **Hardwarevoraussetzungen**

Sie benötigen einen der folgenden Prozessoren:

- PowerPC (AIX)
- HP 9000 (HP-UX)
- Intel 32-Bit (Linux)
- Solaris UltraSPARC-Computer (Solaris-Betriebsumgebung)

- **Betriebssystemvoraussetzungen**

Sie benötigen eines der folgenden Betriebssysteme:

- IBM AIX 5.1 (auf PowerPC)
- HP-UX 11i (auf HP 9000)
- Red Hat Linux 8.0 (auf Intel 32-Bit)
- SuSE Linux 8.1 (auf Intel 32-Bit)
- Sun Solaris Version 8 (auf UltraSPARC-Computern in der Solaris-Betriebsumgebung)

**Anmerkung:** 'DB2 Information - Unterstützung' kann unter einem Teil der UNIX-Betriebssysteme ausgeführt werden, unter denen DB2-Clients unterstützt werden. Daher wird empfohlen, entweder über die IBM Website auf 'DB2 Information - Unterstützung' zuzugreifen oder 'DB2 Information - Unterstützung' auf einem Intranet-Server zu installieren und dort auf die Dokumentation zuzugreifen.

- **Softwarevoraussetzungen**

- Unterstützte Browser:
  - Mozilla Version 1.0 oder höher

- Beim DB2-Installationsassistenten handelt es sich um ein grafisches Installationsprogramm. Um den DB2-Installationsassistenten auf Ihrem Computer ausführen zu können, benötigen Sie eine Implementierung der X Window System-Software zur Wiedergabe einer grafischen Benutzerschnittstelle (GUI). Bevor Sie den DB2-Installationsassistenten ausführen können, müssen Sie die entsprechende Anzeigefunktion (DISPLAY) unbedingt ordnungsgemäß exportieren. Geben Sie hierzu beispielsweise den folgenden Befehl an der Eingabeaufforderung ein:  
`export DISPLAY=9.26.163.144:0.`

- **Kommunikationsvoraussetzungen**

- TCP/IP

### Vorgehensweise:

Um 'DB2 Information - Unterstützung' mit Hilfe des DB2-Installationsassistenten zu installieren, gehen Sie wie folgt vor:

1. Melden Sie sich am System an.
2. Legen Sie die Produkt-CD von 'DB2 Information - Unterstützung' in das CD-Laufwerk ein, und hängen Sie die CD an Ihr System an.

3. Wechseln Sie in das Verzeichnis, in dem die CD angehängt ist. Geben Sie hierzu den folgenden Befehl ein:

```
cd /cd
```

Hierbei steht */cd* für den Mountpunkt der CD.

4. Geben Sie den Befehl **./db2setup** ein, um den DB2-Installationsassistenten zu starten.
5. Die IBM DB2-Klickstartleiste wird geöffnet. Um direkt mit der Installation von 'DB2 Information - Unterstützung' fortzufahren, klicken Sie **Produkt installieren** an. Die Onlinehilfe enthält Informationen, die Sie durch die verbleibenden Schritte der Installation führen. Um die Onlinehilfe aufzurufen, klicken Sie **Hilfe** an. Sie können jederzeit **Abbrechen** anklicken, um die Installation zu beenden.
6. Klicken Sie im Fenster **Wählen Sie das zu installierende Produkt** aus den Knopf **Weiter** an.
7. Klicken Sie **Weiter** im Fenster **Willkommen beim DB2-Installationsassistenten** an. Der DB2-Installationsassistent leitet Sie durch die erforderlichen Schritte zum Installieren des Programms.
8. Um mit der Installation fortfahren zu können, müssen Sie die Lizenzvereinbarung akzeptieren. Wählen Sie auf der Seite **Lizenzvereinbarung** die Option **Bedingungen in der Lizenzvereinbarung anerkennen** aus, und klicken Sie **Weiter** an.
9. Wählen Sie **DB2 Information - Unterstützung auf diesem Computer installieren** auf der Seite **Installationsaktion auswählen** aus. Wenn Sie 'DB2 Information - Unterstützung' zu einem späteren Zeitpunkt auf diesem Computer oder anderen Computern mit Hilfe einer Antwortdatei installieren möchten, wählen Sie **Ihre Einstellungen in einer Antwortdatei speichern** aus. Klicken Sie **Weiter** an.
10. Wählen Sie auf der Seite **Zu installierende Sprachen auswählen** die Sprachen aus, in denen 'DB2 Information - Unterstützung' installiert werden soll. Klicken Sie den Knopf **Weiter** an.
11. Konfigurieren Sie 'DB2 Information - Unterstützung' auf der Seite **Port von DB2 Information - Unterstützung angeben** für eingehende Kommunikation. Klicken Sie **Weiter** an, um mit der Installation fortzufahren.
12. Überprüfen Sie auf der Seite **Kopieren der Dateien starten** noch einmal die von Ihnen ausgewählten Installationseinstellungen. Wenn Sie die Einstellungen ändern möchten, klicken Sie **Zurück** an. Klicken Sie **Installieren** an, um die Dateien von 'DB2 Information - Unterstützung' auf Ihren Computer zu kopieren.

Sie können 'DB2 Information - Unterstützung' auch mit Hilfe einer Antwortdatei installieren.

Die Installationsprotokolldateien `db2setup.his`, `db2setup.log` und `db2setup.err` befinden sich standardmäßig im Verzeichnis `/tmp`.

Die Datei `db2setup.log` erfasst alle Installationsinformationen zu DB2-Produkten, einschließlich Fehlern. Die Datei `db2setup.his` zeichnet alle DB2-Produktinstallationen auf Ihrem Computer auf. DB2 hängt die Datei `db2setup.log` an die Datei `db2setup.his` an. Die Datei `db2setup.err` erfasst die gesamte Fehlerausgabe, die von Java zurückgegeben wird, wie beispielsweise Informationen zu Ausnahmere Bedingungen und Traps.

Nach Abschluss der Installation ist 'DB2 Information - Unterstützung' je nach UNIX-Betriebssystem in einem der folgenden Verzeichnisse installiert:

- AIX: /usr/opt/db2\_08\_01
- HP-UX: /opt/IBM/db2/V8.1
- Linux: /opt/IBM/db2/V8.1
- Solaris-Betriebsumgebung: /opt/IBM/db2/V8.1

**Zugehörige Tasks:**

- „Installation von 'DB2 Information - Unterstützung' mit dem DB2-Installationsassistenten (Windows)“ auf Seite 158

---

## Installation von 'DB2 Information - Unterstützung' mit dem DB2-Installationsassistenten (Windows)

Es gibt drei Möglichkeiten, auf die DB2-Produktdokumentation zuzugreifen: auf der IBM Website, auf einem Intranet-Server oder auf eine auf dem lokalen Computer installierte Version. Standardmäßig greifen DB2-Produkte auf die DB2-Dokumentation auf der IBM Website zu. Wenn Sie jedoch auf die DB2-Dokumentation auf einem Intranet-Server oder auf dem eigenen Computer zugreifen möchten, müssen Sie die DB2-Dokumentation von der CD 'DB2 Information - Unterstützung' aus installieren. Mit dem DB2-Installationsassistenten können Sie Ihre Installationseinstellungen definieren und 'DB2 Information - Unterstützung' auf einem Computer installieren, der ein Windows-Betriebssystem verwendet.

**Voraussetzungen:**

Dieser Abschnitt erläutert die Voraussetzungen für Hardware, Betriebssystem, Software und Kommunikation zum Installieren von 'DB2 Information - Unterstützung' unter Windows.

• **Hardwarevoraussetzungen**

Sie benötigen einen der folgenden Prozessoren:

- 32-Bit-Computer: eine Pentium- oder mit Pentium kompatible CPU

• **Betriebssystemvoraussetzungen**

Sie benötigen eines der folgenden Betriebssysteme:

- Windows 2000
- Windows XP

**Anmerkung:** 'DB2 Information - Unterstützung' kann unter einem Teil der Windows-Betriebssysteme ausgeführt werden, unter denen DB2-Clients unterstützt werden. Daher wird empfohlen, entweder über die IBM Website auf 'DB2 Information - Unterstützung' zuzugreifen oder 'DB2 Information - Unterstützung' auf einem Intranet-Server zu installieren und dort auf die Dokumentation zuzugreifen.

• **Softwarevoraussetzungen**

- Unterstützte Browser:
  - Mozilla 1.0 oder höher
  - Internet Explorer Version 5.5 oder 6.0 (Version 6.0 für Windows XP)

• **Kommunikationsvoraussetzungen**

- TCP/IP

### Einschränkungen:

- Sie benötigen einen Benutzereintrag mit Administratorberechtigung, um 'DB2 Information - Unterstützung' zu installieren.

### Vorgehensweise:

Um 'DB2 Information - Unterstützung' mit Hilfe des DB2-Installationsassistenten zu installieren, gehen Sie wie folgt vor:

1. Melden Sie sich mit dem für die Installation von 'DB2 Information - Unterstützung' definierten Benutzereintrag am System an.
2. Legen Sie die CD in das Laufwerk ein. Die IBM DB2 Setup-Klickstartleiste wird von der Funktion für automatische Ausführung gestartet, sofern diese Funktion aktiviert ist.
3. Der DB2-Installationsassistent ermittelt die Systemsprache und startet das Installationsprogramm für diese Sprache. Wenn Sie das Installationsprogramm nicht in Englisch ausführen möchten oder wenn beim automatischen Starten des Programms ein Fehler aufgetreten ist, können Sie den DB2-Installationsassistenten auch manuell starten.

Um den DB2-Installationsassistenten manuell zu starten, gehen Sie wie folgt vor:

- a. Klicken Sie **Start** an, und wählen Sie die Option **Ausführen** aus.
- b. Geben Sie im Feld **Öffnen** den folgenden Befehl ein:

```
x:\setup.exe /i zweistellige sprachenkennung
```

Hierbei steht *x*: für das CD-Laufwerk und *zweistellige sprachenkennung* für die Sprache, in der das Installationsprogramm ausgeführt werden soll.

- c. Klicken Sie **OK** an.
4. Die IBM DB2-Klickstartleiste wird geöffnet. Um direkt mit der Installation von 'DB2 Information - Unterstützung' fortzufahren, klicken Sie **Produkt installieren** an. Die Onlinehilfe enthält Informationen, die Sie durch die verbleibenden Schritte der Installation führen. Um die Onlinehilfe aufzurufen, klicken Sie **Hilfe** an. Sie können jederzeit **Abbrechen** anklicken, um die Installation zu beenden.
  5. Klicken Sie im Fenster **Wählen Sie das zu installierende Produkt** aus den Knopf **Weiter** an.
  6. Klicken Sie **Weiter** im Fenster **Willkommen beim DB2-Installationsassistenten** an. Der DB2-Installationsassistent leitet Sie durch die erforderlichen Schritte zum Installieren des Programms.
  7. Um mit der Installation fortfahren zu können, müssen Sie die Lizenzvereinbarung akzeptieren. Wählen Sie auf der Seite **Lizenzvereinbarung** die Option **Bedingungen in der Lizenzvereinbarung anerkennen** aus, und klicken Sie **Weiter** an.
  8. Wählen Sie **DB2 Information - Unterstützung auf diesem Computer installieren** auf der Seite **Installationsaktion auswählen** aus. Wenn Sie 'DB2 Information - Unterstützung' zu einem späteren Zeitpunkt auf diesem Computer oder anderen Computern mit Hilfe einer Antwortdatei installieren möchten, wählen Sie **Ihre Einstellungen in einer Antwortdatei speichern** aus. Klicken Sie **Weiter** an.
  9. Wählen Sie auf der Seite **Zu installierende Sprachen auswählen** die Sprachen aus, in denen 'DB2 Information - Unterstützung' installiert werden soll. Klicken Sie den Knopf **Weiter** an.

10. Konfigurieren Sie 'DB2 Information - Unterstützung' auf der Seite **Port von DB2 Information - Unterstützung angeben** für eingehende Kommunikation. Klicken Sie **Weiter** an, um mit der Installation fortzufahren.
11. Überprüfen Sie auf der Seite **Kopieren der Dateien starten** noch einmal die von Ihnen ausgewählten Installationseinstellungen. Wenn Sie die Einstellungen ändern möchten, klicken Sie **Zurück** an. Klicken Sie **Installieren** an, um die Dateien von 'DB2 Information - Unterstützung' auf Ihren Computer zu kopieren.

Sie haben die Möglichkeit, 'DB2 Information - Unterstützung' mit Hilfe einer Antwortdatei zu installieren. Sie können auch den Befehl **db2rspgn** verwenden, um eine Antwortdatei auf der Grundlage einer vorhandenen Installation zu generieren.

Die Dateien db2.log und db2wi.log im Verzeichnis 'Eigene Dateien'\DB2LOG\ enthalten Informationen zu Fehlern, die während der Installation aufgetreten sind. Die Position des Verzeichnisses 'Eigene Dateien' hängt von den Einstellungen Ihres Computers ab.

Die Datei db2wi.log erfasst die neuesten DB2-Installationsinformationen. Die Datei db2.log erfasst die Protokollinformationen von DB2-Produktinstallationen.

#### Zugehörige Tasks:

- „Installation von 'DB2 Information - Unterstützung' mit dem DB2-Installationsassistenten (UNIX)“ auf Seite 155

---

## Aufrufen von 'DB2 Information - Unterstützung'

'DB2 Information - Unterstützung' bietet Ihnen die Möglichkeit, auf alle Informationen zuzugreifen, die Sie zur Verwendung der DB2-Produkte für die Betriebssysteme Linux, UNIX und Windows, wie z. B. DB2 Universal Database, DB2 Connect, DB2 Information Integrator und DB2 Query Patroller, benötigen.

Rufen Sie 'DB2 Information - Unterstützung' auf eine der folgenden Arten auf:

- Von einem Computer aus, auf dem ein DB2 UDB-Client oder -Server installiert ist
- Von einem Intranet-Server oder einem lokalen Computer aus, auf dem 'DB2 Information - Unterstützung' installiert ist
- Über die IBM Website

#### Voraussetzungen:

Führen Sie vor dem Aufrufen von 'DB2 Information - Unterstützung' folgende Schritte aus:

- *Optional*: Konfigurieren des Browsers für die Anzeige der Themen in der gewünschten Landessprache
- *Optional*: Konfigurieren des DB2-Clients für die Verwendung der auf Ihrem Computer oder Intranet-Server installierten Komponente 'DB2 Information - Unterstützung'

### Vorgehensweise:

Gehen Sie wie folgt vor, um 'DB2 Information - Unterstützung' auf einem Computer aufzurufen, auf dem ein DB2 UDB-Client oder -Server installiert ist:

- Wählen Sie (unter Windows) **Start** → **Programme** → **IBM DB2** → **Information** → **DB2 Information - Unterstützung** aus.
- Geben Sie in der Befehlszeile Folgendes ein:
  - Unter Linux und UNIX: Geben Sie den Befehl **db2icdocs** ein.
  - Unter Windows: Geben Sie den Befehl **db2icdocs.exe** ein.

Gehen Sie wie folgt vor, um die auf einem Intranet-Server oder lokalen Computer installierte Komponente 'DB2 Information - Unterstützung' in einem Webbrowser zu öffnen:

- Öffnen Sie die Webseite unter <http://<hostname>:<portnummer>/>. Dabei stellt <hostname> den Namen des Hosts dar und <portnummer> die Nummer des Ports, an dem 'DB2 Information - Unterstützung' verfügbar ist.

Gehen Sie wie folgt vor, um 'DB2 Information - Unterstützung' auf der IBM Website in einem Webbrowser zu öffnen:

- Öffnen Sie die Webseite unter [publib.boulder.ibm.com/infocenter/db2help/](http://publib.boulder.ibm.com/infocenter/db2help/).

### Zugehörige Konzepte:

- „DB2 Information - Unterstützung“ auf Seite 152

### Zugehörige Tasks:

- „Anzeigen von Themen in der gewünschten Sprache in 'DB2 Information - Unterstützung'“ auf Seite 162
- „Aufrufen der Kontexthilfe über ein DB2-Tool“ auf Seite 170
- „Aktualisieren der auf Ihrem Computer oder Intranet-Server installierten Komponente 'DB2 Information - Unterstützung'“ auf Seite 161
- „Aufrufen der Hilfe für Nachrichten über den Befehlszeilenprozessor“ auf Seite 171
- „Aufrufen der Hilfe für Befehle über den Befehlszeilenprozessor“ auf Seite 171
- „Aufrufen der Hilfe für den SQL-Status über den Befehlszeilenprozessor“ auf Seite 172

---

## Aktualisieren der auf Ihrem Computer oder Intranet-Server installierten Komponente 'DB2 Information - Unterstützung'

Die Komponente 'DB2 Information - Unterstützung', auf die Sie über <http://publib.boulder.ibm.com/infocenter/db2help/> zugreifen können, wird in regelmäßigen Abständen durch neue oder geänderte Dokumentationen aktualisiert. IBM stellt in bestimmten Fällen auch Aktualisierungen von 'DB2 Information - Unterstützung' zum Download bereit, die Sie auf Ihrem Computer oder Intranet-Server installieren können. Durch die Aktualisierung von 'DB2 Information - Unterstützung' werden keine DB2-Client- oder -Serverprodukte aktualisiert.

### Voraussetzungen:

Sie benötigen Zugriff auf einen Computer, der über eine Verbindung zum Internet verfügt.

### Vorgehensweise:

Gehen Sie wie folgt vor, um die auf Ihrem Computer bzw. Intranet-Server installierte Komponente 'DB2 Information - Unterstützung' zu aktualisieren:

1. Öffnen Sie 'DB2 Information - Unterstützung' auf der IBM Website unter <http://publib.boulder.ibm.com/infocenter/db2help/>.
2. Klicken Sie im Downloadbereich der Eingangsseite den Link **DB2 Universal Database-Dokumentation** unter der Überschrift für Service und Unterstützung an.
3. Stellen Sie fest, ob die Version der installierten Komponente 'DB2 Information - Unterstützung' veraltet ist, indem Sie die Stufe des neuesten aktualisierten Dokumentationsimage mit der installierten Dokumentationsstufe vergleichen. Die installierte Dokumentationsstufe ist auf der Eingangsseite von 'DB2 Information - Unterstützung' aufgeführt.
4. Wenn eine neuere Version von 'DB2 Information - Unterstützung' verfügbar ist, laden Sie das neueste aktualisierte Image für *DB2 Information - Unterstützung* für das von Ihnen verwendete Betriebssystem herunter.
5. Befolgen Sie zur Installation des aktualisierten Image für *DB2 Information - Unterstützung* die Anweisungen auf der Webseite.

### Zugehörige Tasks:

- „Kopieren von Dateien von der CD mit der DB2-HTML-Dokumentation auf einen Webserver“ in *DB2 Universal Database Personal Edition Einstieg*

### Zugehörige Referenzen:

- „DB2-Dokumentation in PDF-Format und gedrucktem Format“ auf Seite 163

---

## Anzeigen von Themen in der gewünschten Sprache in 'DB2 Information - Unterstützung'

In 'DB2 Information - Unterstützung' werden Themen, wenn möglich, in der Sprache angezeigt, die in den Vorgaben Ihres Browsers angegeben ist. Falls ein Thema nicht in die gewünschte Sprache übersetzt wurde, wird es in 'DB2 Information - Unterstützung' in Englisch angezeigt.

### Vorgehensweise:

Um Themen in der gewünschten Sprache im Browser 'Internet Explorer' anzuzeigen, gehen Sie wie folgt vor:

1. Klicken Sie im Internet Explorer **Extras** —> **Internetoptionen...** —> **Sprachen...** an. Das Fenster **Spracheinstellung** wird geöffnet.
2. Stellen Sie sicher, dass die gewünschte Sprache als erster Eintrag in der Liste angegeben ist.
  - Klicken Sie den Knopf **Hinzufügen...** an, um eine neue Sprache zur Liste hinzuzufügen.

**Anmerkung:** Das Hinzufügen einer Sprache bedeutet nicht zwangsläufig, dass der Computer über die erforderlichen Schriftarten verfügt, um die Themen in der gewünschten Sprache anzuzeigen.

- Um eine Sprache an den Anfang der Liste zu verschieben, wählen Sie zunächst die gewünschte Sprache und anschließend den Knopf **Nach oben** aus, bis die Sprache an erster Stelle in der Liste steht.

3. Aktualisieren Sie die Seite, um 'DB2 Information - Unterstützung' in der gewünschten Sprache anzuzeigen.

Um Themen in der gewünschten Sprache im Browser 'Mozilla' anzuzeigen, gehen Sie wie folgt vor:

1. Wählen Sie in Mozilla **Bearbeiten** —> **Einstellungen** —> **Sprachen** aus. Die Anzeige für die Auswahl der Sprache wird im Fenster mit den Einstellungen aufgerufen.
2. Stellen Sie sicher, dass die gewünschte Sprache als erster Eintrag in der Liste angegeben ist.
  - Wenn Sie eine neue Sprache hinzufügen möchten, klicken Sie den Knopf **Hinzufügen...** an, um eine Sprache im entsprechenden Fenster auszuwählen.
  - Um eine Sprache an den Anfang der Liste zu verschieben, wählen Sie zunächst die gewünschte Sprache und anschließend den Knopf **Nach oben** aus, bis die Sprache an erster Stelle in der Liste steht.
3. Aktualisieren Sie die Seite, um 'DB2 Information - Unterstützung' in der gewünschten Sprache anzuzeigen.

---

## DB2-Dokumentation in PDF-Format und gedrucktem Format

In den folgenden Tabellen sind die offiziellen Buchtitel, Formularnummern und PDF-Dateinamen aufgeführt. Zum Bestellen von Hardcopybüchern benötigen Sie den offiziellen Buchtitel. Zum Drucken der PDF-Version benötigen Sie den PDF-Dateinamen.

Die DB2-Dokumentation ist in die folgenden Kategorien unterteilt:

- DB2-Kerninformationen
- Verwaltungsinformationen
- Informationen zur Anwendungsentwicklung
- Informationsmanagement
- Informationen zu DB2 Connect
- Einführungsinformationen
- Lernprogramminformationen
- Informationen zu Zusatzkomponenten
- Release-Informationen

In den folgenden Tabellen wird für die einzelnen Bücher der DB2-Bibliothek beschrieben, welche Informationen zum Bestellen von Hardcopies bzw. zum Drucken oder Anzeigen der PDF-Versionen erforderlich sind. Eine vollständige Beschreibung der in der DB2-Bibliothek verfügbaren Bücher finden Sie im IBM Publications Center unter folgender Adresse:  
[www.ibm.com/shop/publications/order](http://www.ibm.com/shop/publications/order).

### DB2-Kerninformationen

Diese Bücher enthalten grundlegende Informationen für alle DB2-Benutzer. Diese Informationen sind sowohl für Programmierer als auch für Datenbankadministratoren geeignet und unterstützen Sie bei der Arbeit mit DB2 Connect, DB2 Warehouse Manager und anderen DB2-Produkten.

Tabelle 8. DB2-Kerninformationen

Name	IBM Form	PDF-Dateiname
IBM DB2 Universal Database Command Reference	SC09-4828	db2n0e81
IBM DB2 Universal Database Glossar	Keine Formnummer	db2t0g81
IBM DB2 Universal Database Fehlernachrichten, Band 1	GC12-3043, nicht als Hardcopy verfügbar	db2m1g81
IBM DB2 Universal Database Fehlernachrichten, Band 2	GC12-3042, nicht als Hardcopy verfügbar	db2m2g81
IBM DB2 Universal Database Neue Funktionen	SC12-3044	db2q0g81

## Verwaltungsinformationen

Die Informationen in diesen Büchern umfassen die Themen, die zum effektiven Entwerfen, Implementieren und Verwalten von DB2-Datenbanken, Data Warehouses und Systemen zusammenschlossener Datenbanken erforderlich sind.

Tabelle 9. Verwaltungsinformationen

Name	IBM Form	PDF-Dateiname
IBM DB2 Universal Database Systemverwaltung: Konzept	SC12-3057	db2d1g81
IBM DB2 Universal Database Systemverwaltung: Implementierung	SC12-3059	db2d2g81
IBM DB2 Universal Database Systemverwaltung: Optimierung	SC12-3058	db2d3g81
IBM DB2 Universal Database Administrative API Reference	SC09-4824	db2b0e81
IBM DB2 Universal Database Dienstprogramme für das Versetzen von Daten Handbuch und Referenz	SC12-3055	db2dmg81
IBM DB2 Universal Database Datenwiederherstellung und hohe Verfügbarkeit Handbuch und Referenz	SC12-3054	db2hag81
IBM DB2 Universal Database Data Warehouse-Zentrale Verwaltung	SC12-3068	db2ddg81
IBM DB2 Universal Database SQL Reference, Volume 1	SC09-4844	db2s1e81
IBM DB2 Universal Database SQL Reference, Volume 2	SC09-4845	db2s2e81
IBM DB2 Universal Database System Monitor Guide and Reference	SC09-4847	db2f0e81

## Informationen zur Anwendungsentwicklung

Die Informationen in diesen Büchern sind besonders für Anwendungsentwickler und Programmierer von Interesse, die mit DB2 Universal Database (DB2 UDB) arbeiten. Sie finden hier Informationen zu den unterstützten Programmiersprachen und Compilern sowie die Dokumentation, die für den Zugriff auf DB2 UDB über die verschiedenen unterstützten Programmierschnittstellen, z. B. eingebettetes SQL, ODBC, JDBC, SQLJ und CLI, erforderlich ist. Wenn Sie die Komponente 'DB2 Information - Unterstützung' verwenden, können Sie auch auf HTML-Versionen des Quellcodes für die Beispielprogramme zugreifen.

*Tabelle 10. Informationen zur Anwendungsentwicklung*

<b>Name</b>	<b>IBM Form</b>	<b>PDF-Dateiname</b>
<i>IBM DB2 Universal Database Application Development Guide: Building and Running Applications</i>	SC09-4825	db2axe81
<i>IBM DB2 Universal Database Application Development Guide: Programming Client Applications</i>	SC09-4826	db2a1e81
<i>IBM DB2 Universal Database Application Development Guide: Programming Server Applications</i>	SC09-4827	db2a2e81
<i>IBM DB2 Universal Database Call Level Interface Guide and Reference, Volume 1</i>	SC09-4849	db2l1e81
<i>IBM DB2 Universal Database Call Level Interface Guide and Reference, Volume 2</i>	SC09-4850	db2l2e81
<i>IBM DB2 Universal Database Data Warehouse Center Application Integration Guide</i>	SC27-1124	db2ade81
<i>IBM DB2 XML Extender Verwaltung und Programmierung</i>	SC12-3062	db2sxx81

## Informationsmanagement

Die Informationen in diesen Büchern beschreiben den Einsatz von Komponenten, mit denen Sie die Data Warehousing- und Analysefunktionen von DB2 Universal Database erweitern können.

*Tabelle 11. Informationsmanagement*

<b>Name</b>	<b>IBM Form</b>	<b>PDF-Dateiname</b>
<i>IBM DB2 Warehouse Manager Standard Edition Informationskatalogzentrale Verwaltung</i>	SC12-3070	db2dig81
<i>IBM DB2 Warehouse Manager Standard Edition Installation</i>	GC12-3069	db2idg81
<i>IBM DB2 Warehouse Manager Standard Edition Managing ETI Solution Conversion Programs with DB2 Warehouse Manager</i>	SC18-7727	iwhe1mste80

## Informationen zu DB2 Connect

Die Informationen in dieser Kategorie beschreiben den Zugriff auf Daten auf großen und mittleren Serversystemen mit Hilfe von DB2 Connect Enterprise Edition oder DB2 Connect Personal Edition.

*Tabelle 12. Informationen zu DB2 Connect*

Name	IBM Form	PDF-Dateiname
<i>IBM Konnektivität Ergänzung</i>	Keine Formnummer	db2h1g81
<i>IBM DB2 Connect Enterprise Edition Einstieg</i>	GC12-3051	db2c6g81
<i>IBM DB2 Connect Personal Edition Einstieg</i>	GC12-3049	db2c1g81
<i>IBM DB2 Connect Benutzerhandbuch</i>	SC12-3048	db2c0g81

## Einführungsinformationen

Die Informationen in dieser Kategorie unterstützen Sie beim Installieren und Konfigurieren von Servern, Clients und anderen DB2-Produkten.

*Tabelle 13. Einführungsinformationen*

Name	IBM Form	PDF-Dateiname
<i>IBM DB2 Universal Database für DB2-Clients Einstieg</i>	GC12-3052, nicht als Hardcopy verfügbar	db2itg81
<i>IBM DB2 Universal Database für DB2-Server Einstieg</i>	GC12-3047	db2isg81
<i>IBM DB2 Universal Database Personal Edition Einstieg</i>	GC12-3045	db2i1g81
<i>IBM DB2 Universal Database Installation und Konfiguration Ergänzung</i>	GC12-3046, nicht als Hardcopy verfügbar	db2iyg81
<i>IBM DB2 Universal Database Data Links Manager Einstieg</i>	GC12-3056	db2z6g81

## Lernprogramminformationen

In den Lernprogramminformationen werden DB2-Funktionen vorgestellt. Darüber hinaus wird die Ausführung verschiedener Tasks beschrieben.

*Tabelle 14. Lernprogramminformationen*

Name	IBM Form	PDF-Dateiname
<i>Lernprogramm für das Informationsmanagement: Data Warehouse - Einführung</i>	Keine Formnummer	db2tug81
<i>Lernprogramm für das Informationsmanagement: Data Warehouse - Weiterführende Informationen</i>	Keine Formnummer	db2tag81
<i>Lernprogramm für die Informationskatalogzentrale</i>	Keine Formnummer	db2aig81
<i>Video Central für e-business Lernprogramm</i>	Keine Formnummer	db2twg81

Tabelle 14. Lernprogramminformationen (Forts.)

Name	IBM Form	PDF-Dateiname
Lernprogramm für Visual Explain	Keine Formnummer	db2tv81

## Informationen zu Zusatzkomponenten

Die Informationen in dieser Kategorie beschreiben das Arbeiten mit den DB2-Zusatzkomponenten.

Tabelle 15. Informationen zu Zusatzkomponenten

Name	IBM Form	PDF-Dateiname
IBM DB2 Cube Views Handbuch und Referenz	n/v	db2aag81
IBM DB2 Query Patroller-Handbuch: Installation, Verwaltung und Verwendung	GC12-3225	db2dwg81
IBM DB2 Spatial Extender und Geodetic Extender Benutzer- und Referenzhandbuch	SC12-3063	db2sbg81
IBM DB2 Universal Database Data Links Manager Administration Guide and Reference	SC27-1221	db2z0e82
DB2 Net Search Extender Verwaltung und Benutzerhandbuch	SH12-3021	n/v

**Anmerkung:** Die HTML-Version dieses Dokuments wird nicht von der HTML-Dokumentations-CD installiert.

## Release-Informationen

Die Release-Informationen enthalten zusätzliche Informationen für das verwendete Produktrelease und die verwendete FixPak-Stufe. Die Release-Informationen enthalten außerdem Zusammenfassungen der Dokumentationsaktualisierungen in den verschiedenen Releases, Aktualisierungen und FixPaks.

Tabelle 16. Release-Informationen

Name	IBM Form	PDF-Dateiname
DB2 Release-Informationen	Siehe Anmerkung.	Siehe Anmerkung.
DB2 Installationsinformationen	Nur auf der Produkt-CD-ROM verfügbar.	n/v

**Anmerkung:** Die Release-Informationen stehen in den folgenden Formaten zur Verfügung:

- XHTML und Textformat auf den Produkt-CDs
- PDF-Format auf der CD mit der PDF-Dokumentation

Darüber hinaus sind die Abschnitte zu *bekanntem Problemen und Fehlerumgehungen* sowie zur *Inkompatibilität zwischen einzelnen Releases*, die Teil der Release-Informationen sind, auch über 'DB2 Information - Unterstützung' verfügbar.

Informationen zum Anzeigen der Release-Informationen in Textformat auf UNIX-Plattformen finden Sie in der Datei `Release.Notes`. Diese Datei befindet sich im Verzeichnis `DB2DIR/Readme/%L`. Hierbei steht `%L` für die länderspezifische Angabe und `DB2DIR` für eine der folgenden Angaben:

- Für AIX-Betriebssysteme: `/usr/opt/db2_08_01`
- Für alle anderen UNIX-Betriebssysteme: `/opt/IBM/db2/V8.1`

**Zugehörige Tasks:**

- „Drucken von DB2-Büchern mit PDF-Dateien“ auf Seite 168
- „Bestellen gedruckter DB2-Bücher“ auf Seite 169
- „Aufrufen der Kontexthilfe über ein DB2-Tool“ auf Seite 170

---

## Drucken von DB2-Büchern mit PDF-Dateien

DB2-Bücher können mit Hilfe der PDF-Dateien auf der CD mit der *DB2-PDF-Dokumentation* gedruckt werden. Mit Adobe Acrobat Reader können Sie entweder das gesamte Handbuch oder bestimmte Seitenbereiche des Handbuchs ausdrucken.

**Voraussetzungen:**

Stellen Sie sicher, dass Adobe Acrobat Reader installiert ist. Falls Sie Adobe Acrobat Reader noch nicht installiert haben, finden Sie das Produkt auf der Adobe-Website unter folgender Adresse: [www.adobe.com](http://www.adobe.com)

**Vorgehensweise:**

Gehen Sie wie folgt vor, um ein DB2-Buch mit einer PDF-Datei auszudrucken:

1. Legen Sie die CD mit der *DB2-PDF-Dokumentation* in das CD-ROM-Laufwerk ein. Hängen Sie unter UNIX-Betriebssystemen die CD mit der *DB2-PDF-Dokumentation* an. Informationen zum Anhängen einer CD unter UNIX-Betriebssystemen finden Sie im Handbuch *Einstieg* für das jeweilige Betriebssystem.
2. Öffnen Sie `index.htm`. Die Datei wird in einem Browserfenster geöffnet.
3. Klicken Sie den Titel der PDF an, die Sie aufrufen möchten. Die PDF wird in Acrobat Reader geöffnet.
4. Wählen Sie **Datei** → **Drucken** aus, um einen beliebigen Teil des gewünschten Buches zu drucken.

**Zugehörige Konzepte:**

- „DB2 Information - Unterstützung“ auf Seite 152

**Zugehörige Tasks:**

- „Bestellen gedruckter DB2-Bücher“ auf Seite 169

**Zugehörige Referenzen:**

- „DB2-Dokumentation in PDF-Format und gedrucktem Format“ auf Seite 163

---

## Bestellen gedruckter DB2-Bücher

Wenn Sie die Hardcopyversion der Bücher bevorzugen, können Sie sie auf eine der nachfolgend aufgeführten Arten bestellen.

### Vorgehensweise:

In bestimmten Ländern oder Regionen können gedruckte Bücher bestellt werden. Auf der Website mit IBM Veröffentlichungen für das jeweilige Land bzw. die jeweilige Region finden Sie Informationen darüber, ob dieser Service im betreffenden Land bzw. in der betreffenden Region angeboten wird. Wenn die Veröffentlichungen bestellt werden können, haben Sie folgende Möglichkeiten:

- Wenden Sie sich an den zuständigen IBM Vertragshändler oder Vertriebsbeauftragten. Informationen zum lokalen IBM Ansprechpartner finden Sie im globalen IBM Verzeichnis für Kontakte unter folgender Adresse:  
[www.ibm.com/planetwide](http://www.ibm.com/planetwide).
- Weitere Informationen enthält das IBM Publications Center unter <http://www.ibm.com/shop/publications/order>. Die Möglichkeit, Bücher über das IBM Publications Center zu bestellen, besteht möglicherweise nicht in allen Ländern.

Die gedruckten Bücher sind zu dem Zeitpunkt, an dem das DB2-Produkt verfügbar gemacht wird, identisch mit den PDF-Versionen auf der CD mit der *DB2-PDF-Dokumentation*. Darüber hinaus stimmt der Inhalt der gedruckten Bücher mit den entsprechenden Informationen auf der CD für *DB2 Information - Unterstützung* überein. Diese CD enthält jedoch zusätzliche Informationen, die in den PDF-Büchern nicht enthalten sind (wie beispielsweise SQL-Verwaltungsroutinen und HTML-Beispiele). Nicht alle Bücher, die auf der CD mit der DB2-PDF-Dokumentation verfügbar sind, können als Hardcopy bestellt werden.

**Anmerkung:** 'DB2 Information - Unterstützung' wird häufiger aktualisiert als die PDF- oder die Hardcopyversion der Bücher. Installieren Sie die Dokumentationsupdates, sobald diese verfügbar sind, oder greifen Sie über 'DB2 Information - Unterstützung' unter <http://publib.boulder.ibm.com/infocenter/db2help/> auf die neuesten Informationen zu.

### Zugehörige Tasks:

- „Drucken von DB2-Büchern mit PDF-Dateien“ auf Seite 168

### Zugehörige Referenzen:

- „DB2-Dokumentation in PDF-Format und gedrucktem Format“ auf Seite 163

---

## Aufrufen der Kontexthilfe über ein DB2-Tool

Die Kontexthilfe bietet Informationen zu den Tasks bzw. Steuerelementen, die einem bestimmten Fenster, Notizbuch, Assistenten oder Advisor zugeordnet sind. Die Kontexthilfe steht in allen DB2-Verwaltungs- und -entwicklungstools zur Verfügung, die über eine grafische Benutzerschnittstelle verfügen. Zwei Arten der Kontexthilfe stehen zur Verfügung:

- Die über den Knopf **Hilfe** aufgerufenen Hilfetexte, der in jedem Fenster bzw. Notizbuch zur Verfügung steht.
- Die Kurzhilfe. Hierbei handelt es sich um Informationsfenster, die angezeigt werden, wenn sich der Mauszeiger auf einem Feld oder Steuerelement befindet oder wenn bei der Auswahl eines Feldes oder Steuerelements in einem Fenster, Notizbuch, Assistenten oder Advisor die Taste F1 gedrückt wird.

Über den Knopf **Hilfe** können Sie auf Übersichtsinformationen, Informationen zu Voraussetzungen sowie Informationen zu Tasks zugreifen. In der Kurzhilfe werden die einzelnen Felder und Steuerelemente beschrieben.

### Vorgehensweise:

Gehen Sie wie folgt vor, um Kontexthilfe aufzurufen:

- Hilfe zu Fenstern und Notizbüchern können Sie anzeigen, indem Sie eines der DB2-Tools aufrufen und anschließend ein beliebiges Fenster oder Notizbuch öffnen. Klicken Sie den Knopf **Hilfe** in der rechten unteren Ecke des Fensters bzw. Notizbuchs an, um die Kontexthilfe aufzurufen.

Zugriff auf die Kontexthilfe besteht darüber hinaus über den Menüpunkt **Hilfe** am oberen Rand jeder Zentrale der DB2-Tools.

Innerhalb von Assistenten und Advisorfunktionen klicken Sie den Link für die Taskübersicht auf der ersten Seite an, um die Kontexthilfe aufzurufen.

- Kurzhilfe zu einzelnen Steuerelementen eines Fensters oder Notizbuchs können Sie aufrufen, indem Sie das gewünschte Steuerelement anklicken und anschließend **F1** drücken. Die Kurzhilfeinformationen mit Details zum jeweiligen Steuerelement werden in einem gelben Fenster angezeigt.

**Anmerkung:** Wenn die Kurzhilfe angezeigt werden soll, sobald sich der Mauszeiger auf einem Feld oder Steuerelement befindet, wählen Sie das Markierungsfeld **Kurzhilfe automatisch anzeigen** auf der Seite **Dokumentation** des Notizbuchs 'Tools - Einstellungen' aus.

Ähnlich wie die Kurzhilfe sind auch Dialogfenster mit Diagnoseinformationen eine Form der kontextbezogenen Hilfe; sie enthalten Regeln für die Dateneingabe. Diese Diagnoseinformationen werden in einem violetten Fenster angezeigt, das aufgerufen wird, wenn die eingegebenen Daten nicht gültig oder nicht ausreichend sind. Die Kontexthilfe mit Diagnoseinformationen kann für folgende Felder angezeigt werden:

- Musseingabefelder
- Felder, in denen die Daten einem bestimmten Format entsprechen müssen, wie z. B. Datumsfelder

### Zugehörige Tasks:

- „Aufrufen von 'DB2 Information - Unterstützung'“ auf Seite 160
- „Aufrufen der Hilfe für Nachrichten über den Befehlszeilenprozessor“ auf Seite 171
- „Aufrufen der Hilfe für Befehle über den Befehlszeilenprozessor“ auf Seite 171

- „Aufrufen der Hilfe für den SQL-Status über den Befehlszeilenprozessor“ auf Seite 172

---

## Aufrufen der Hilfe für Nachrichten über den Befehlszeilenprozessor

Die Hilfe für Nachrichten beschreibt die Ursache von Nachrichten und die Aktionen, die der Benutzer zur Behebung des aufgetretenen Fehlers ausführen sollte.

### Vorgehensweise:

Zum Aufrufen der Hilfe für Nachrichten müssen Sie den Befehlszeilenprozessor öffnen und Folgendes eingeben:

? *XXXnnnnn*

Dabei ist *XXXnnnnn* eine gültige Nachrichtenennung.

So kann beispielsweise durch die Eingabe von ? SQL30081 die Hilfe zur Nachricht SQL30081 angezeigt werden.

### Zugehörige Tasks:

- „Aufrufen der Kontexthilfe über ein DB2-Tool“ auf Seite 170
- „Aufrufen von 'DB2 Information - Unterstützung'“ auf Seite 160
- „Aufrufen der Hilfe für Befehle über den Befehlszeilenprozessor“ auf Seite 171
- „Aufrufen der Hilfe für den SQL-Status über den Befehlszeilenprozessor“ auf Seite 172

---

## Aufrufen der Hilfe für Befehle über den Befehlszeilenprozessor

Die Hilfe für Befehle erläutert die Syntax von Befehlen im Befehlszeilenprozessor.

### Vorgehensweise:

Zum Aufrufen der Hilfe für Befehle müssen Sie den Befehlszeilenprozessor öffnen und Folgendes eingeben:

? *command*

Dabei stellt *command* ein Schlüsselwort bzw. den vollständigen Befehl dar.

So kann beispielsweise durch die Eingabe von ? catalog Hilfe für alle CATALOG-Befehle angezeigt werden, während mit ? catalog database nur Hilfe für den Befehl CATALOG DATABASE angezeigt wird.

### Zugehörige Tasks:

- „Aufrufen der Kontexthilfe über ein DB2-Tool“ auf Seite 170
- „Aufrufen von 'DB2 Information - Unterstützung'“ auf Seite 160
- „Aufrufen der Hilfe für Nachrichten über den Befehlszeilenprozessor“ auf Seite 171
- „Aufrufen der Hilfe für den SQL-Status über den Befehlszeilenprozessor“ auf Seite 172

---

## Aufrufen der Hilfe für den SQL-Status über den Befehlszeilenprozessor

DB2 Universal Database gibt für Bedingungen, die auf Grund einer SQL-Anweisung generiert werden können, einen SQLSTATE-Wert zurück. Die SQLSTATE-Hilfe erläutert die Bedeutung der SQL-Statuswerte und der SQL-Statusklassencodes.

### Vorgehensweise:

Zum Aufrufen der Hilfe für SQL-Statuswerte müssen Sie den Befehlszeilenprozessor öffnen und Folgendes eingeben:

*? sqlstate* oder *? klassencode*

Hierbei steht *sqlstate* für einen gültigen fünfstelligen SQL-Statuswert und *klassencode* für die ersten beiden Ziffern dieses Statuswertes.

So kann beispielsweise durch die Eingabe von *? 08003* Hilfe für den SQL-Statuswert 08003 angezeigt werden, durch die Eingabe von *? 08* Hilfe für den Klassencode 08.

### Zugehörige Tasks:

- „Aufrufen von 'DB2 Information - Unterstützung'“ auf Seite 160
- „Aufrufen der Hilfe für Nachrichten über den Befehlszeilenprozessor“ auf Seite 171
- „Aufrufen der Hilfe für Befehle über den Befehlszeilenprozessor“ auf Seite 171

---

## DB2-Lernprogramme

Die Lernprogramme von DB2<sup>®</sup> unterstützen Sie bei der Einarbeitung in die verschiedenen Themenbereiche von DB2 Universal Database. Sie umfassen Übungen mit in einzelne Arbeitsschritte untergliederten Anweisungen zum Entwickeln von Anwendungen, Optimieren der SQL-Abfrageleistung, Arbeiten mit Data Warehouses, Verwalten von Metadaten und Entwickeln von Webservices mit Hilfe von DB2.

### Vorbereitungen:

Die XHTML-Version der Lernprogramme kann über 'DB2 Information - Unterstützung' unter <http://publib.boulder.ibm.com/infocenter/db2help/> angezeigt werden.

In einigen der Lernprogrammübungen werden Beispieldaten und Codebeispiele verwendet. Informationen zu den spezifischen Voraussetzungen zur Ausführung der Tasks finden Sie in der Beschreibung des jeweiligen Lernprogramms.

### Lernprogramme von DB2 Universal Database:

Klicken Sie einen der Lernprogrammtitel in der folgenden Liste an, um das entsprechende Lernprogramm aufzurufen.

*Lernprogramm für das Informationsmanagement: Data Warehouse - Einführung*  
Ausführung grundlegender Data Warehousing-Tasks mit Hilfe der Data Warehouse-Zentrale.

*Lernprogramm für das Informationsmanagement: Data Warehouse - Weiterführende Informationen*

Ausführung weiterführender Data Warehousing-Tasks mit Hilfe der Data Warehouse-Zentrale.

*Lernprogramm für die Informationskatalogzentrale*

Erstellen und Verwalten eines Informationskatalogs zum Lokalisieren und Verwenden von Metadaten mit Hilfe der Informationskatalogzentrale.

*Lernprogramm für Visual Explain*

Analysieren, Optimieren und Anpassen von SQL-Anweisungen zur Leistungsverbesserung mit Hilfe von Visual Explain.

---

## Informationen zur Fehlerbehebung in DB2

Eine breite Palette verschiedener Informationen zur Fehlerbestimmung und Fehlerbehebung steht zur Verfügung, um Sie bei der Verwendung von DB2®-Produkten zu unterstützen.

### **DB2-Dokumentation**

Informationen zur Fehlerbehebung stehen in der gesamten Komponente 'DB2 Information - Unterstützung' sowie in den PDF-Büchern der DB2-Bibliothek zur Verfügung. Folgen Sie der Verzweigung 'Unterstützung und Fehlerbehebung' in der Navigationsbaumstruktur von 'DB2 Information - Unterstützung' (im linken Teilfenster des Browserfensters), um eine umfassende Liste der DB2-Dokumentationen zur Fehlerbehebung aufzurufen.

### **DB2-Website mit technischer Unterstützung**

Auf der DB2-Website mit technischer Unterstützung finden Sie Informationen zu Problemen und den möglichen Ursachen und Fehlerbehebungsmaßnahmen. Die DB2-Website mit technischer Unterstützung stellt Links zu den neuesten DB2-Veröffentlichungen, technischen Hinweisen (TechNotes), APARs (Authorized Program Analysis Reports), FixPaks, den neuesten Listen mit internen DB2-Fehlercodes sowie weiteren Ressourcen zur Verfügung. Sie können diese Wissensbasis nach möglichen Lösungen für aufgetretene Probleme durchsuchen.

Rufen Sie die DB2-Website mit technischer Unterstützung unter <http://www.ibm.com/software/data/db2/udb/winos2unix/support> auf.

### **DB2-Lernprogramme zur Fehlerbestimmung**

Auf der Website mit den DB2-Lernprogrammen zur Fehlerbestimmung finden Sie Informationen dazu, wie Sie Fehler, die bei der Verwendung von DB2-Produkten möglicherweise auftreten, rasch identifizieren und beheben können. Eines der Lernprogramme bietet eine Einführung in die verfügbaren DB2-Einrichtungen und -Tools zur Fehlerbestimmung sowie Entscheidungshilfen für deren Verwendung. Andere Lernprogramme befassen sich mit zugehörigen Themen, wie beispielsweise der Fehlerbestimmung für die Datenbanksteuerkomponente, der Fehlerbestimmung für die Leistung und der Fehlerbestimmung für Anwendungen.

Die vollständige Liste der DB2-Lernprogramme zur Fehlerbestimmung finden Sie auf der DB2-Website mit technischer Unterstützung unter <http://www.ibm.com/software/data/support/pdm/db2tutorials.html>.

### **Zugehörige Konzepte:**

- „DB2 Information - Unterstützung“ auf Seite 152

---

## Eingabehilfen

Eingabehilfen unterstützen Benutzer mit körperlichen Behinderungen, wie z. B. eingeschränkter Bewegungsfähigkeit oder Sehkraft, beim erfolgreichen Einsatz von Softwareprodukten. Im Folgenden sind die wichtigsten Eingabehilfen aufgeführt, die in den Produkten von DB2<sup>®</sup> Version 8 zur Verfügung stehen:

- Die gesamte DB2-Funktionalität kann sowohl über die Maus als auch über die Tastatur gesteuert werden. Weitere Informationen hierzu finden Sie unter „Tastatureingabe und Navigation“.
- Sie können die Größe und Farbe der verwendeten Schriftarten in den DB2-Schnittstellen anpassen. Weitere Informationen hierzu finden Sie unter „Eingabehilfen für Bildschirme“.
- DB2-Produkte unterstützen Anwendungen mit Eingabehilfen, die mit der Java<sup>™</sup> Accessibility API arbeiten. Weitere Informationen hierzu finden Sie unter „Kompatibilität mit Unterstützungseinrichtungen“ auf Seite 175.
- Die DB2-Dokumentation steht in behindertengerechtem Format zur Verfügung. Weitere Informationen hierzu finden Sie unter „Dokumentation im behindertengerechten Format“ auf Seite 175.

## Tastatureingabe und Navigation

### Tastatureingabe

Die verfügbaren DB2-Tools können unter ausschließlicher Benutzung der Tastatur verwendet werden. Mit entsprechenden Tasten oder Tastenkombinationen können Operationen ausgeführt werden, die auch über die Maus verfügbar sind. Die Standardtastenkombinationen des Betriebssystems werden für die entsprechenden Standardoperationen des Betriebssystems verwendet.

Weitere Informationen zur Verwendung von Tasten oder Tastenkombinationen für die Ausführung von Operationen finden Sie unter " 'Direktaufrufe über die Tastatur: Gemeinsame GUI - Hilfe'.

### Navigation über die Tastatureingabe

Sie können in den Benutzerschnittstellen der DB2-Tools mit Hilfe von Tasten oder Tastenkombinationen navigieren.

Weitere Informationen zur Navigation in den DB2-Tools mit Hilfe der Tastatureingabe finden Sie unter " 'Direktaufrufe über die Tastatur: Gemeinsame GUI - Hilfe'.

### Tastatureingabebereich

Unter UNIX<sup>®</sup>-Betriebssystemen ist der Bereich des aktiven Fensters, in dem die Tastatureingabe wirksam ist, hervorgehoben.

## Eingabehilfen für Bildschirme

Die DB2-Tools stellen Funktionen bereit, mit denen sehbehinderten Benutzern verbesserten Eingabehilfen zur Verfügung stehen. Diese Eingabehilfen umfassen die Unterstützung individuell anpassbarer Schriftarteneigenschaften.

### Schriftarteneinstellungen

Über das Notizbuch 'Tools - Einstellungen' können Sie die Farbe, Größe und Schriftart des Textes in Menüs und Dialogfenstern auswählen.

Weitere Informationen zur Angabe von Schriftarteneinstellungen finden Sie unter " 'Ändern der Schriftarten für Menüs und Text: Gemeinsame GUI - Hilfe'.

## Unabhängigkeit von Farben

Zur Verwendung der Funktionen des vorliegenden Produkts ist es nicht erforderlich, zwischen unterschiedlichen Farben differenzieren zu können.

## Kompatibilität mit Unterstützungseinrichtungen

Die Schnittstellen der DB2-Tools unterstützen die Java Accessibility API. Hierdurch wird der Einsatz von Sprachausgabeprogrammen und anderen Unterstützungseinrichtungen für Personen mit Behinderungen mit den DB2-Produkten ermöglicht.

## Dokumentation im behindertengerechten Format

Die Dokumentation für DB2 steht im Format XHTML 1.0 zur Verfügung, das mit den meisten Webbrowsern geöffnet werden kann. XHTML ermöglicht das Aufrufen der Dokumentation mit den Anzeigeeinstellungen, die Sie in Ihrem Browser definiert haben. Darüber hinaus ist der Einsatz von Sprachausgabeprogrammen und anderen Unterstützungseinrichtungen möglich.

Syntaxdiagramme stehen in der Schreibweise mit Trennzeichen zur Verfügung. Dieses Format ist nur dann verfügbar, wenn Sie mit Hilfe eines Sprachausgabeprogramms auf die Onlinedokumentation zugreifen.

### Zugehörige Konzepte:

- „Syntaxdiagramme in der Schreibweise mit Trennzeichen“ auf Seite 175

---

## Syntaxdiagramme in der Schreibweise mit Trennzeichen

Syntaxdiagramme stehen für Benutzer, die mit Hilfe eines Sprachausgabeprogramms auf 'DB2 Information - Unterstützung' zugreifen, in der Schreibweise mit Trennzeichen zur Verfügung.

In der Schreibweise mit Trennzeichen steht jedes Syntaxelement in einer separaten Zeile. Wenn zwei oder mehr Syntaxelemente stets gemeinsam angegeben (oder nicht angegeben) werden müssen, können sie in derselben Zeile stehen, da sie als ein zusammengesetztes Syntaxelement betrachtet werden können.

Jede Zeile beginnt mit einer Zahl in der Schreibweise mit Trennzeichen, zum Beispiel 3 oder 3.1 oder 3.1.1. Um diese Zahlen korrekt zu hören, müssen Sie sicherstellen, dass das Sprachausgabeprogramm so konfiguriert ist, dass die Interpunktion angesagt wird. Alle Syntaxelemente mit derselben Zahl in der Schreibweise mit Trennzeichen (z. B. alle Syntaxelemente mit der Zahl 3.1) stellen Alternativen dar, die sich gegenseitig ausschließen. Wenn Sie die Zeilen '3.1 USERID' und '3.1 SYSTEMID' hören, wissen Sie, dass die Syntax entweder USERID oder SYSTEMID enthalten kann, nicht jedoch beides.

Die Nummerierung bei der Schreibweise mit Trennzeichen gibt den Grad der Ausgliederung an. Beispiel: Wenn auf das Syntaxelement mit der Zahl 3 in der Schreibweise mit Trennzeichen eine Reihe von Syntaxelementen mit der Zahl 3.1 folgt, sind alle Syntaxelemente mit der Zahl 3.1 dem Syntaxelement mit der Zahl 3 untergeordnet.

Bestimmte Wörter und Symbole werden zusätzlich zu den Zahlen in der Schreibweise mit Trennzeichen verwendet, um weitere Informationen zu den Syntaxelementen anzugeben. In manchen Fällen können diese Wörter und Symbole am Anfang des Elements selbst stehen. Zur einfacheren Identifizierung wird dem Wort oder Symbol ein umgekehrter Schrägstrich (\) vorangestellt, wenn es Teil des

Syntaxelement ist. Das Symbol \* (Stern) kann zusätzlich zu einer Zahl in der Schreibweise mit Trennzeichen verwendet werden, um anzugeben, dass das Syntaxelement wiederholt wird. Beispiel: Das Syntaxelement \*FILE mit der Zahl 3 in der Schreibweise mit Trennzeichen erhält das Format 3 \\* FILE. Format 3\* FILE gibt an, dass das Syntaxelement FILE wiederholt wird. Format 3\* \\* FILE gibt an, dass das Syntaxelement \* FILE wiederholt wird.

Zeichen wie beispielsweise Kommas, die bei einer Folge von Syntaxelementen als Trennzeichen verwendet werden, werden in der Syntax unmittelbar vor den Elementen dargestellt, die sie trennen. Diese Zeichen können in derselben Zeile stehen wie das jeweilige Element oder in einer separaten Zeile mit derselben Zahl in der Schreibweise mit Trennzeichen, die auch dem betreffenden Element zugeordnet ist. Die Zeile kann auch ein weiteres Symbol enthalten, das Informationen zu den Syntaxelementen angibt. So bedeuten z. B. die Zeilen 5.1\*, 5.1 LASTRUN und 5.1 DELETE, dass, wenn Sie mehr als eines der Elemente LASTRUN und DELETE verwenden, diese Elemente durch Kommas voneinander getrennt werden müssen. Wenn kein Trennzeichen angegeben wird, verwendet das System zum Trennen der einzelnen Syntaxelemente ein Leerzeichen.

Wenn einem Syntaxelement das Symbol % vorangestellt ist, gibt dies einen Verweis an, der an anderer Stelle definiert ist. Die Zeichenfolge, die auf das Symbol % folgt, ist der Name eines Syntaxfragments und kein Literal. So gibt die Zeile 2.1 %OP1 beispielsweise einen Verweis auf das separate Syntaxfragment OP1 an.

Die nachfolgend aufgeführten Wörter und Symbole werden zusätzlich zu den Zahlen in der Schreibweise mit Trennzeichen verwendet:

- ? stellt ein optionales Syntaxelement dar. Eine Zahl in der Schreibweise mit Trennzeichen, auf die das Symbol ? (Fragezeichen) folgt, gibt an, dass alle Syntaxelemente mit einer entsprechenden Zahl in der Schreibweise mit Trennzeichen sowie alle untergeordneten Syntaxelemente optional sind. Ist nur ein Syntaxelement mit einer Zahl in der Schreibweise mit Trennzeichen vorhanden, wird das Symbol ? in derselben Zeile angezeigt wie das Syntaxelement (zum Beispiel 5? NOTIFY). Sind mehrere Syntaxelemente mit einer Zahl in der Schreibweise mit Trennzeichen vorhanden, wird das Symbol ? in einer separaten Zeile angezeigt, gefolgt von den optionalen Syntaxelementen. Wenn Sie beispielsweise die Zeilen 5 ?, 5 NOTIFY und 5 UPDATE hören, wissen Sie, dass die Syntaxelemente NOTIFY und UPDATE optional sind; das bedeutet, Sie können eines oder keines dieser Elemente auswählen. Das Symbol ? entspricht einer Umgehungslinie in einem Pfeildiagramm.
- ! stellt ein Standardsyntaxelement dar. Eine Zahl in der Schreibweise mit Trennzeichen, auf die das Symbol ! (Ausrufezeichen) und ein Syntaxelement folgen, gibt an, dass es sich bei diesem Syntaxelement um die Standardoption für alle Syntaxelemente handelt, denen dieselbe Zahl in der Schreibweise mit Trennzeichen zugeordnet ist. Nur für eines der Syntaxelemente, denen dieselbe Zahl in der Schreibweise mit Trennzeichen zugeordnet ist, darf das Symbol ! angegeben werden. Wenn Sie beispielsweise die Zeilen 2? FILE, 2.1! (KEEP) und 2.1 (DELETE) hören, wissen Sie, dass (KEEP) die Standardoption für das Schlüsselwort FILE ist. Wenn Sie in diesem Beispiel das Schlüsselwort FILE verwenden, jedoch keine Option angeben, wird die Standardoption KEEP verwendet. Eine Standardoption ist auch für die nächsthöhere Zahl in der Schreibweise mit Trennzeichen gültig. In diesem Beispiel bedeutet das: Wenn das Schlüsselwort FILE weggelassen wird, wird der Standardwert FILE(KEEP) verwendet. Wenn Sie jedoch die Zeilen 2? FILE, 2.1, 2.1.1! (KEEP) und 2.1.1 (DELETE) hören, gilt die Standardoption KEEP nur für die nächsthöhere Zahl in der Schreibweise mit

Trennzeichen, 2.1 (der kein Schlüsselwort zugeordnet ist), nicht jedoch für 2? FILE. Wird das Schlüsselwort FILE weggelassen, wird kein Wert verwendet.

- \* stellt ein Syntaxelement dar, das keinmal, einmal oder mehrmals wiederholt werden kann. Eine Zahl in der Schreibweise mit Trennzeichen, auf die das Symbol \* (Stern) folgt, gibt an, dass dieses Syntaxelement keinmal, einmal oder mehrmals verwendet werden kann, d. h., es ist optional und kann wiederholt werden. Wenn Sie beispielsweise die Zeile 5.1\* Datenbereich hören, wissen Sie, dass Sie einen, mehrere oder keinen Datenbereich angeben können. Hören Sie die Zeilen 3\*, 3 HOST und 3 STATE, wissen Sie, dass Sie HOST, STATE, beide oder keines der Elemente angeben können.

#### **Anmerkungen:**

1. Wenn neben einer Zahl in der Schreibweise mit Trennzeichen ein Stern (\*) angezeigt wird und nur ein Element mit dieser Zahl vorhanden ist, können Sie dieses Element mehrmals wiederholen.
  2. Wenn neben einer Zahl in der Schreibweise mit Trennzeichen ein Stern angezeigt wird und diese Zahl mehreren Elementen zugeordnet ist, können Sie mehrere Elemente aus der Liste verwenden, jedes davon jedoch nur einmal. Im vorhergehenden Beispiel könnten Sie HOST STATE angeben, nicht jedoch HOST HOST.
  3. Das Symbol \* entspricht einer zum Ausgangspunkt zurück führenden Linie in einem Pfeildiagramm.
- + stellt ein Syntaxelement dar, das mindestens einmal angegeben werden muss. Eine Zahl in der Schreibweise mit Trennzeichen, auf die das Symbol + (Pluszeichen) folgt, gibt an, dass dieses Syntaxelement mindestens einmal angegeben werden muss und wiederholt werden kann. Wenn Sie beispielsweise die Zeile 6.1+ Datenbereich hören, müssen sie mindestens einen Datenbereich angeben. Wenn Sie die Zeilen 2+, 2 HOST und 2 STATE hören, wissen Sie, dass Sie HOST, STATE oder beides angeben müssen. Wie auch für das Symbol \* gilt hier, dass mit dem Pluszeichen ein bestimmtes Element nur dann wiederholt werden kann, wenn es sich um das einzige Element mit dieser Zahl in der Schreibweise mit Trennzeichen handelt. Das Symbol + entspricht wie das Symbol \* einer zum Ausgangspunkt zurück führenden Linie in einem Pfeildiagramm.

#### **Zugehörige Referenzen:**

- „How to read the syntax diagrams“ in *SQL Reference, Volume 2*

---

## **Common Criteria-Zertifizierung von DB2 Universal Database-Produkten**

Für DB2 Universal Database läuft momentan der Bewertungsprozess für die Zertifizierung entsprechend der Richtlinien von Common Criteria Evaluation Assurance Level 4 (EAL4). Weitere Informationen zu Common Criteria finden Sie auf der Common Criteria-Website unter: <http://niap.nist.gov/cc-scheme/>.



---

## Anhang B. Bemerkungen

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Dienstleistungen von IBM verwendet werden können. An Stelle der IBM Produkte, Programme oder Dienstleistungen können auch andere ihnen äquivalente Produkte, Programme oder Dienstleistungen verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte der IBM verletzen. Die Verantwortung für den Betrieb der Produkte, Programme oder Dienstleistungen in Verbindung mit Fremdprodukten und Fremddienstleistungen liegt beim Kunden, soweit nicht ausdrücklich solche Verbindungen erwähnt sind.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Europe, Director of Licensing, 92066 Paris La Defense Cedex, France.

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die Angaben in diesem Handbuch werden in regelmäßigen Zeitabständen aktualisiert. Die Änderungen werden in Überarbeitungen bekanntgegeben. IBM kann jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter dienen lediglich als Benutzerinformationen und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängigen, erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Canada Limited  
Office of the Lab Director  
8200 Warden Avenue  
Markham, Ontario  
L6G 1C7  
CANADA

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des im Handbuch aufgeführten Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt im Rahmen der Allgemeinen Geschäftsbedingungen der IBM, der Internationalen Nutzungsbedingungen der IBM für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer gesteuerten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Garantie, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Informationen über Produkte anderer Hersteller als IBM wurden von den Herstellern dieser Produkte zur Verfügung gestellt, bzw. aus von ihnen veröffentlichten Ankündigungen oder anderen öffentlich zugänglichen Quellen entnommen. IBM hat diese Produkte nicht getestet und übernimmt im Hinblick auf Produkte anderer Hersteller keine Verantwortung für einwandfreie Funktion, Kompatibilität oder andere Ansprüche. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten der IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele der IBM.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufes. Sie sollen nur die Funktionen des Lizenzprogrammes illustrieren; sie können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden, Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

#### COPYRIGHTLIZENZ:

Diese Veröffentlichung enthält Beispielanwendungsprogramme, die in Quellsprache geschrieben sind. Sie dürfen diese Beispielprogramme kostenlos kopieren, ändern und verteilen, wenn dies zu dem Zweck geschieht, Anwendungsprogramme zu entwickeln, verwenden, vermarkten oder zu verteilen, die mit der Anwendungsprogrammierschnittstelle konform sind, für die diese Beispielprogramme geschrieben werden. Diese Beispiele wurden nicht unter allen denkbaren Bedingungen getestet. Daher kann IBM die Zuverlässigkeit, Wartungsfreundlichkeit oder Funktion dieser Programme weder zusagen noch gewährleisten.

Kopien oder Teile der Beispielprogramme bzw. daraus abgeleiteter Code müssen folgenden Copyrightvermerk beinhalten:

© (Name Ihrer Firma) (Jahr). Teile des vorliegenden Codes wurden aus Beispielprogrammen der IBM Corp. abgeleitet. © Copyright IBM Corp. *Jahr/Jahre angeben*. Alle Rechte vorbehalten.

---

## Marken

Folgende Namen sind in gewissen Ländern Marken der International Business Machines Corporation und wurden in mindestens einem der Dokumente in der DB2 UDB-Dokumentationsbibliothek verwendet:

ACF/VTAM	iSeries
AISPO	LAN Distance
AIX	MVS
AIXwindows	MVS/ESA
AnyNet	MVS/XA
APPN	Net.Data
IBM System AS/400	NetView
BookManager	OS/390
C Set++	OS/400
C/370	PowerPC
CICS	pSeries
Database 2	QBIC
DataHub	QMF
DataJoiner	RACF
DataPropagator	RS/6000
DataRefresher	S/370
DB2	SP
DB2 Connect	SQL/400
DB2 Extenders	SQL/DS
DB2 OLAP Server	System/370
DB2 Information Integrator	IBM System /390
DB2 Query Patroller	SystemView
DB2 Universal Database	Tivoli
Distributed Relational Database Architecture	VisualAge
DRDA	VM/ESA
eServer	VSE/ESA
Extended Services	VTAM
FFST	WebExplorer
First Failure Support Technology	WebSphere
IBM	WIN-OS/2
IMS	z/OS
IMS/ESA	zSeries

Folgende Namen sind in gewissen Ländern Marken oder eingetragene Marken anderer Unternehmen und wurden in mindestens einem der Dokumente in der DB2 UDB-Dokumentationsbibliothek verwendet.

Microsoft, Windows, Windows NT und das Windows-Logo sind in gewissen Ländern Marken der Microsoft Corporation.

Intel und Pentium sind in gewissen Ländern Marken der Intel Corporation.

Java und alle auf Java basierenden Marken sind in gewissen Ländern Marken von Sun Microsystems, Inc.

UNIX ist in gewissen Ländern eine eingetragene Marke von The Open Group.

Andere Namen von Unternehmen, Produkten oder Dienstleistungen können Marken anderer Unternehmen sein.



# Index

## A

- ACF/VTAM 94
  - ADDRDBDIRE, Befehl 51
  - ADDRDBDIRE, Befehl zum Hinzufügen eines Eintrags im Verzeichnis relationaler Datenbanken 34
  - ADDSVRAUTE, Befehl 53
  - AIX
    - konfigurieren
    - Bull SNA 16
  - Aktualisieren
    - HMTL-Dokumentation 161
  - Ändern der Sitzungsanzahl (CNOS) 146
  - Ändern von Netzwerkattributen, Befehl 35
  - Anwendungsrequester 25, 121
    - Datendarstellung 129
    - fernes System, Definition 30
    - Kommunikationssystem 80
    - lokales System, Definition (VTAM) 26
    - Nachrichtendosierung 80
    - OS/400
      - Kommunikationsdefinitionen 35
      - konfigurieren 33
      - Nachrichtendosierung 35
      - Netzwerkinformationen 33
      - RU-Größe einstellen 35
      - Sicherheit 122
    - RU-Größe einstellen 80
    - Sicherheit
      - Datenbankmanager 120
      - Endbenutzernamen 115
      - Netzwerk 119
      - Subsystem 121
  - SQL/DS VM
    - aktivieren 141
    - AVS-Sitzungsbegrenzung, Überlegungen 92
    - Datendarstellung 124
    - fernes System, Definition 41
    - Kommunikationssystem 92
    - konfigurieren 39
    - lokales System, Definition 40
    - Nachrichtendosierung 93
    - Netzwerkinformationen 39
    - RU-Größe einstellen 93
    - Sicherheit 124
    - SQL/DS VSE aktivieren 139
    - Verbindungen (SNA) 47
  - Anwendungsserver
    - Datendarstellung 105, 129
    - Herkunftsüberprüfung 99
    - konfigurieren 47
    - Namensumsetzung für eingehende Anforderungen 100
    - OS/390 und z/OS 47
    - OS/400
      - Datendarstellung 129
      - Definition 51
      - Endbenutzernamen 105
  - Anwendungsserver (*Forts.*)
    - OS/400 (*Forts.*)
      - ferne Datenbank benennen 51
      - konfigurieren 51
      - RU-Größe einstellen 51
      - Sicherheit 105
    - Sicherheit
      - Datenbankmanager 103
      - Endbenutzernamen 100
      - Netzwerk 102
      - Subsystem 105
  - Sicherheit des Datenbankmanagers 103
  - SNA 47
  - SQL/DS VM
    - Datendarstellung 132
    - Definition 68
    - Endbenutzernamen 108
    - konfigurieren 67
    - Namensumsetzung für eingehende Anforderungen 108
    - Netzwerkinformationen 67
    - Sicherheit 108
  - SQL/DS VSE
    - Definition 63
    - konfigurieren 59
    - Netzwerkinformationen 59
    - Sicherheit 112
    - starten 64
  - VSE
    - Einschränkungen 94
    - RMTUSERS, Startparameter 94
    - SYNCPNT, Startparameter 94
- APPC (Advanced Program-to-Program Communication)
  - Bull SNA 16
  - Communications Server für Windows NT SNA Client 15
  - konfigurieren mit dem Konfigurationsassistenten 139
  - manuell konfigurieren 13
  - SNAPLUSLink 16
- APPC/VM-Unterstützung 82
- APPC/VTAM-Unterstützung 82
- APPCPASS, Anweisung 124
- APPL-Anweisungen 26
- APPN (Advanced Peer-to-Peer Networking), Positionslisten erstellen 35
- Arbeitsblätter
  - Parameterwert APPC 144
- Aufrufen
  - Hilfe für Befehle 171
  - Hilfe für Nachricht 171
  - Hilfe zu SQL-Anweisungen 172
- Authentifizierung
  - Typen
    - CLIENT 73
- AVS
  - Gatewaydefinition, Beispiel 40
  - Komponente von VM 82

- AVS (*Forts.*)
  - Sitzungsbegrenzung, Überlegungen 92
- AXE 94

## B

- Befehlszeilenprozessor (CLP)
  - Knoten katalogisieren 6, 17
- Behinderungen 174
- Beispiele
  - ADDRDBDIRE, Befehl 34
  - Anwendungsrequester und Anwendungsrequester unter DB2 für VM 82
  - AVS-Gatewaydefinition 40
  - Berechtigungen erteilen, OS/400 124
  - DSNTIIPR, Installationsanzeige 26
  - Eintrag im CMS-Kommunikationsverzeichnis 112
  - Kommunikationsfluss, SQL/DS VSE 94
  - Kommunikationsfluss des Anwendungsservers 82
  - Namensumsetzung für abgehende Anforderungen
    - SNA 115
    - TCP/IP 115
  - RESID-Namensdatei, SQL/DS auf VM 68
  - VM-Datenfluss 82
  - VM-Verzeichnis comdir, Einträge 124
  - VTAM-Anweisung APPL 26
- Bestellen von DB2-Büchern 169
- BSDS-Parameter (Bootstrap Data Set) aktualisieren 26, 49

## C

- CCSID (Coded Character Set Identifier)
  - DB2, Standardeinstellung 129
  - VM
    - aktuelle anzeigen 132
    - Standardwert 132
- CDB (Kommunikationsdatenbank) 30
- CHARNAME, Parameter 82, 124, 132
- CHGNETA, Befehl 35
- CICS (Customer Information Control System)
  - CICS-LU 6.2-Sitzungen für VSE einrichten 59
  - Installation 59
- CICS(ISC) 94
- CICS(SPM) 94
- CICS(TRUE) 94
- CLI (Call Level Interface)
  - Anwendungen
    - CURRENTPACKAGESET 73
- CMS-Kommunikationsverzeichnis
  - Beispiel für Eintrag 112

CMS-Kommunikationsverzeichnis (*Forts.*)  
 Katalogisieren von RDB\_NAMES 41  
 Sicherheit 124  
 comdir (Kommunikationsverzeichnis)  
 Beispieleintrag 41, 124  
 CMS 41  
 SET COMDIR, Befehl 41  
 VM 82  
 Communications Server für Windows NT  
 SNA Client  
 erforderliche Version 15  
 manuell konfigurieren 15  
 Controllerbeschreibungen erstellen 35  
 Coordinated Resource Recovery  
 (CRR) 82  
 CRR-Server (CRR = Coordinated  
 Resource Recovery) 82  
 CRTCFGL, Befehl 35  
 CRTCOSD, Befehl 35  
 CRTCTLAPPC, Befehl 35  
 CRTCTLHOST, Befehl 35  
 CRTDDMTCPA, Befehl 105  
 CRTDEVAPPC, Befehl 35  
 CRTLINETH, Befehl 35  
 CRTLNSDL, Befehl 35  
 CRTLINTRN, Befehl 35  
 CRTLINX25, Befehl 35  
 CRTMODD, Befehl 35  
 CURRENTPACKAGESET, CLI/ODBC-  
 Schlüsselwort 73

## D

Datenbanken  
 katalogisieren 8, 19  
 Datenbanknamen, Verzeichnis 94  
 Datendarstellung  
 DB2-Anwendungsrequester 129  
 DB2-Anwendungsserver 105, 129  
 OS/400-Anwendungsserver 129  
 SQL/DS-Anwendungsrequester 124  
 SQL/DS auf VM, Anwendungs-  
 server 132  
 DB2-Bücher  
 PDF-Dateien drucken 168  
 DB2 Connect  
 aktualisieren, APPC-Profil 14  
 server  
 TCP/IP konfigurieren 4  
 DB2 für VM  
 DRDA, Übersicht 82  
 DB2 Information - Unterstützung 152  
 aufrufen 160  
 installieren 155, 158  
 DB2-Lernprogramme 172  
 DB2-Tabelle, LINKNAME 30  
 DB2 Universal Database für iSeries 81  
 Distributed Database Programming,  
 Handbuch 53  
 DRDA-TCP/IP-Client  
 konfigurieren 53  
 Überlegungen 53  
 DRDA-TCP/IP-Server  
 konfigurieren 53  
 Überlegungen 53  
 TCP/IP-Verbindungen konfigurieren 34

DB2 Universal Database für OS/390 und  
 z/OS 25  
 Definieren des lokalen Systems  
 TCP/IP 29  
 DYNAMICRULES(BIND) 73  
 Portnummern 29  
 Sicherheitsverbesserungen 73  
 Desktop, Sicherheit für ODBC- und  
 Java-Anwendungen 73  
 erweiterte Sicherheitscodes 73  
 TCP/IP-Sicherheit bereits  
 überprüft 73  
 Unterstützung für Kennwort-  
 änderung 73  
 Verbindungen verteilter Datenbanken  
 Vergleiche 73  
 Verbindungseinrichtungen  
 CAF 73  
 CICS/ESA 73  
 DDF 73  
 IMS/ESA 73  
 TSO 73  
 DB2 Universal Database für VM  
 Übersicht 82  
 DB2 Universal Database für VSE  
 Komponenten für verteilte Verarbei-  
 tung  
 ACF/VTAM 94  
 AXE 94  
 CICS(ISC) 94  
 CICS(SPM) 94  
 CICS(TRUE) 94  
 Verzeichnis DBNAME 94  
 XPCC 94  
 Übersicht 94  
 DB2 Universal Database für VSE und VM  
 Hostverbindungen 82  
 DBNAME, Netzwerkelement (VSE oder  
 VM) 144  
 DBNAME, Verzeichnis 94  
 DDF (Distributed Data Facility) 25  
 DDF-Datensatz 26  
 Direktaufrufe über die Tastatur  
 Unterstützung bei 174  
 Dokumentation  
 anzeigen 160  
 Drucken  
 PDF-Dateien 168  
 DSNTIPR, Installationsanzeige  
 Beispiel 26  
 Dynamisches SQL  
 CURRENTPACKAGESET 73  
 Pakete 103, 108, 112

## E

Eingabehilfen  
 Funktionen 174  
 Syntaxdiagramme in der Schreibweise  
 mit Trennzeichen 175  
 Einheitenbeschreibung erstellen 35  
 Endbenutzernamen  
 Anwendungsrequester  
 DB2 115  
 OS/400 122  
 SQL/DS auf VM 124

Endbenutzernamen (*Forts.*)  
 Anwendungsserver  
 OS/400 105  
 SQL/DS auf VM 108  
 Sicherheit 100

## F

Fehlerbehebung  
 Onlineinformationen 173  
 Fern  
 Datenbanknamen, CMS-  
 Kommunikationsverzeichnis 41  
 Standorte 119  
 Transaktionsprogramm 144  
 Verbindungsadresse 144  
 Ferne Arbeitseinheit  
 Verbindungen 73

## G

GCS (Group Control System) 82  
 Gedruckte Bücher bestellen 169  
 GRTOBJAUT, Befehl 105, 124  
 Gruppensteuerungssystem (GCS) 82

## H

Herkunftsüberprüfung 99  
 Hilfe  
 anzeigen 160, 162  
 für Befehle  
 aufrufen 171  
 für Nachrichten  
 aufrufen 171  
 für SQL-Anweisungen  
 aufrufen 172  
 Hilfe für Befehle  
 aufrufen 171  
 Hilfe für Nachricht  
 aufrufen 171  
 Hilfe zu SQL-Anweisungen  
 aufrufen 172  
 Host-Datenbankserver  
 binden, Anwendungen und Dienst-  
 programme 9, 20  
 Hostdatenbank  
 Verbindung testen 10, 21  
 HP-UX  
 SNAPLUS2 konfigurieren 17  
 HTML-Dokumentation  
 aktualisieren 161

## I

IDENT 82  
 Installieren  
 DB2 Information - Unterstüt-  
 zung 155, 158  
 IP-Adresse  
 auflösen 4  
 IRLM 73  
 iSeries  
 DB2 UDB 81  
 Verbindung testen 10, 21

iSeries-Datenbankserver  
binden, Anwendungen und Dienst-  
programme 9, 20

## K

Katalogisieren  
APPC-Knoten 17  
Datenbanken 8, 19  
ferne DCS-Datenbank 7, 18  
TCP/IP-Parameterwerte 143  
TCP/IP-Knoten 6  
Kennwörter  
ändern, Unterstützung für (OS/390  
und z/OS) 73  
Kommunikation  
APPC 139  
Datenbanktabellen, DB2  
SYSIBM.LOCATIONS 30  
Datenflussbeispiel, SQL/DS VSE 94  
Subsystem  
DB2-Anwendungsrequester 80  
OS/400-Anwendungsrequester 35  
Verbindungen testen 10, 21  
Verzeichnis, VM-Umgebung 41, 82  
VM-Datenfluss, Beispiele 82  
Kommunikationsprotokolle  
APPC 13  
Konfigurieren  
Anwendungsserver 144  
Bull SNA 16  
DRDA-Server 144  
IBM eNetwork Communications Ser-  
ver für AIX 16  
IBM eNetwork Communications Ser-  
ver für Windows NT SNA API Cli-  
ent 15  
iSeries 144  
Listen erstellen 35  
Microsoft SNA Client 16  
Microsoft SNA Server 15  
SNAPLus 16  
SQLDS 144  
Überlegungen, Kennwort-  
änderung 73  
VM 144  
VSE 144

## L

Lernprogramme 172  
LINKNAME, Tabelle 30  
LOCATION NAME (z/OS, OS/390) 144  
Lokal  
Adapteradresse 144  
LU-Name 144  
Steuerpunktname 144  
Lokales System  
definieren, DB2 (VTAM) 26  
SQL/DS-Anwendungsrequester 40  
LU-Arbeitsblätter 144

## M

Microsoft SNA Client  
erforderliche Version 16

Microsoft SNA Client (*Forts.*)  
konfigurieren 16  
Microsoft SNA Server  
konfigurieren 15  
MODEENT 144  
Modusbeschreibung erstellen 35  
Modusname 144  
MVS (Multiple Virtual Storage)  
DB2-Adressräume 73

## N

Nachrichten  
austauschen, DB2 25  
Nachrichten austauschen, DB2 25  
Nachrichtendosierungszähler  
DB2-Anwendungsrequester 80  
OS/400-Anwendungsrequester 35  
OS/400-Anwendungsserver 51  
SQL/DS-Anwendungsrequester 93  
Namenskonventionen  
ferne Datenbank, OS/400 51  
lokale Datenbank, OS/400 34  
Namensumsetzung für abgehende Anfor-  
derungen  
Beispiel 115  
DB2-Anwendungsrequester 115  
SNA 115  
SQL/DS-Anwendungsrequester 124  
TCP/IP 115  
Namensumsetzung für eingehende  
Anforderungen  
DB2-Anwendungsserver 100  
SQL/DS auf VM, Anwendungs-  
server 108  
NetView 73  
Netzwerk  
Austauschen von Nachrichten 25  
ID 144  
Name 144  
Netzwerkinformationen  
OS/400-Anwendungsrequester 33  
SQL/DS-Anwendungsrequester 39  
SQL/DS auf VM, Anwendungs-  
server 67  
SQL/DS VSE-Anwendungsserver  
Einrichten 59  
SON (Benachrichtigung bei  
Sitzungsausfall) 59  
Netzwerksicherheit  
DB2-Anwendungsrequester 119  
DB2-Anwendungsserver 102  
DB2 UDB für iSeries, Anwendungs-  
server 105  
SQL/DS-Anwendungsrequester 124  
SQL/DS auf VM, Anwendungs-  
server 108

## O

ODBC (Open Database Connectivity)  
Anwendungen  
CURRENTPACKAGESET 73  
Online  
Hilfe, zugreifen auf 170

OS/390  
Sicherheitsüberlegungen 99  
OS/400  
Kommunikation aktivieren 35  
Netzwerkattribute 35

## P

Pakete  
DB2, Sicherheit des Anwendungs-  
servers 103  
SQL/DS-Datenbankmanager, Sicher-  
heit 112  
dynamisches SQL 108  
statisches SQL 108  
Parameterwerte, Arbeitsblatt für  
TCP/IP konfigurieren 141  
Partner  
Knotenname 144  
LU-Name 144  
Portnummern  
DB2 UDB für OS/390 und z/OS 29  
Privates Protokoll, OS/390 und z/OS 73  
PROTOCOL, Parameter  
Optionen  
AUTO 82  
SQLDS 82  
PU 144

## R

RDB-Name (iSeries) 144  
Relationale Datenbank  
Name 144  
Verzeichnis  
Beschreibung, OS/400 34  
Eintragsinformationen, iSeries 34  
RELOAD PACKAGE, Befehl 124  
RESID (Ressourcen-ID)  
Namensdatei, SQL/DS auf VM, Bei-  
spiel 68  
Transaktionsprogrammname  
(TPN) 68  
Ressourcenadapter, VM 82  
RMTUSERS, Parameter 94  
RU-Größe einstellen  
Anwendungsrequester 80  
OS/400-Anwendungsrequester 35  
OS/400-Anwendungsserver 51  
SQL/DS-Anwendungsrequester 93  
VM 93  
RVKOBJAUT, Befehl  
\*USE, Berechtigung 105  
Sicherheit 124

## S

Sekundäre Server  
Verbindung herstellen 73  
Senden von Kennwörtern  
unverschlüsselt 119  
verschlüsselt 119  
Serviceklasse  
erstellen 35  
OS/400, Beschreibung 35

- services, Datei
  - aktualisieren 5
- SET COMDIR, Befehl 41
- SET CURRENT PACKAGESET, Anweisung 73
- Sicherheit
  - Anwendungsrequester
    - DB2, Netzwerk 119
    - DB2, Subsystem 121
    - DB2-Datenbankmanager 120
    - OS/390 115
    - OS/400 122
    - OS/400-Datenbankmanager 122
    - SQL/DS-Datenbankmanager 124
    - z/OS 115
  - Anwendungsserver
    - DB2, Subsystem 105
    - DB2-Datenbankmanager 103
    - OS/390 99
    - SQL/DS auf VM, Subsystem 108
    - z/OS 99
  - Berechtigungen erteilen
    - Beispiel, iSeries 124
  - Datenbankmanager
    - ferne Anwendungen ausführen 120
    - ferne Anwendungen binden 120
    - iSeries 105
    - VM-Anwendungsserver 108
  - Endbenutzernamen
    - DB2-Anwendungsrequester 115
    - DB2-Anwendungsserver 100
    - OS/400-Anwendungsrequester 122
    - OS/400-Anwendungsserver 105
    - SQL/DS-Anwendungsrequester 124
    - VM-Anwendungsserver 108
  - erweiterte Codes
    - OS/390 und z/OS 73
  - fernes System 115
  - Herkunftsüberprüfung in DB2 99
  - iSeries-System 105
  - Netzwerk
    - DB2-Anwendungsserver 102
    - iSeries-Anwendungsserver 105
    - OS/400-Anwendungsrequester 122
    - SQL/DS-Anwendungsrequester 124
    - VM-Anwendungsserver 108
  - Prozess
    - DB2-Anwendungsserver 99
    - SQL/DS auf VM, Anwendungsserver 108
    - SQL/DS-Subsystem 124
  - Standardberechtigung
    - iSeries 122
  - Sicherheit des Datenbankmanagers
    - DB2-Anwendungsrequester 120
    - DB2-Anwendungsserver 103
    - OS/400-Anwendungsrequester 122
    - SQL/DS-Anwendungsrequester
      - Anwendungen ausführen 124
      - Anwendungen vorverarbeiten 124
    - Benutzernamen umsetzen, für abgehende Anforderungen 124

- Sicherheit des Datenbankmanagers
  - (Forts.)
    - SQL/DS auf VM, Anwendungsserver 108
- Sitzungsbegrenzungen
  - SQL/DS auf VM 92
- SNA (Systems Network Architecture)
  - konfigurieren
    - SNAPLus 16
  - manuell konfigurieren
    - Communications Server für Windows NT SNA Client 15
    - Microsoft SNA Client 16
- SNAPLus2 für HP-UX konfigurieren 17
- SON (Benachrichtigung bei Sitzungsausfall) 59
- SQL (Structured Query Language)
  - dynamisch 103
  - Objekte
    - DB2-Sicherheit 103
    - SQL/DS-Datenbankmanager, Sicherheit 108, 112
  - statisch 103
- SQL/DS
  - Sicherheit des Datenbankmanagers
    - dynamisches SQL 112
    - statisches SQL 112
  - VM 82
  - VSE 59
- SQLINIT 82
- SSCP 144
- Standardberechtigung, iSeries 122
- Statisches SQL
  - Pakete 103, 108, 112
- Steuerpunktname 144
- STRTCPSVR, Befehl 53
- Subsystem
  - Name 25
- Symbolischer Bestimmungsname 144
- Synchronisationspunktmanager (SPM)
  - SYNCPNT, Parameter 82
- SYNCPNT, Parameter 82, 94
- Syntaxdiagramme in der Schreibweise mit Trennzeichen 175
- SYSIBM.LOCATIONS, Tabelle 30
- Systemsicherheit, OS/400 122

## T

- TCP/IP
  - aktualisieren
    - Datei 'services' 5
  - herkömmlicher Port 446 für
    - DRDA 51
  - iSeries, Einrichtung
    - DRDA-Anwendungsrequester 53
    - DRDA-Anwendungsserver 53
  - Konfiguration
    - Arbeitsblatt 4
    - DB2 Connect-Server 141
  - manuell konfigurieren
    - Host-Datenbankservers 3
    - iSeries-Datenbankservers 3
  - Parameterwerte, Arbeitsblatt für 141
  - Parameterwerte zum Katalogisieren von Datenbanken 143

- TCP/IP (Forts.)
  - Sicherheit
    - DRDA, Überlegungen 53
    - iSeries 105
    - überprüft 73
- TPN (Transaktionsprogrammname)
  - DB2-Tabelle, SYSIBM.LOCATIONS 30
  - DRDA-Standardwert, OS/400 34
  - OS/400-Anwendungsserver 51
  - SQL/DS auf VM, RESID (Ressourcen-ID) 68
- Transaktionsmanager
  - Planung, Arbeitsblatt 144
- Transparent Services Access Facility (TSAF) 82
- TSAF (Transparent Services Access Facility) 82

## V

- Verbindung
  - Beschreibungen erstellen 35
- Verbindungen
  - Verbindungstypen
    - DB2, verteilte Datenbank 73
    - SQL/DS auf verteilter VM-Datenbank 82
- Verbindungseinrichtungen 73
- Verbindungssicherheit, Stufen 112
- Verteilte Arbeitseinheit
  - Zugriff, anwendungsgesteuert 73
  - Zugriff, systemgesteuert 73
- Verteilte relationale Datenbanken
  - DB2, Verbindungen 73
- VM
  - DRDA
    - Anwendungsrequester vorbereiten 43
    - Anwendungsserver vorbereiten 43
    - Komponenten 82
  - Kommunikationsverzeichnis (comdir) 82
  - Ressourcenadapter 82
  - Verzeichniseinträge 124
- VRYCFG, Befehl 35
- VTAM
  - Anwendungsname ist Name der Partner-LU 144
  - APPL-Anweisungen
    - DB2, Beispiel 26
    - Standardsitzungsbegrenzungen 146
  - BSDS, Beispiel 26
  - Definition 73
  - DRDA, Aufgabe in 82

## W

- WRKCFGSTS, Befehl 35

## X

- XPCC 94

## Z

z/OS

Sicherheitsüberlegungen 99

Zieldatenbank

Name 144

Zugriff

Host-Server

^IBM eNetwork Communication

Server V5 für AIX 16

für 32-Bit-Windows-Betriebssysteme 15

SNA-API-Client 15



---

## Kontaktaufnahme mit IBM

Telefonische Unterstützung erhalten Sie über folgende Nummern:

- Unter 0180 3 313233 erreichen Sie Hallo IBM, wo Sie Antworten zu allgemeinen Fragen erhalten.
- Unter 0190 7 72243 erreichen Sie die DB2 Helpline, wo Sie Antworten zu DB2-spezifischen Problemen erhalten.

Informationen zur nächsten IBM Niederlassung in Ihrem Land oder Ihrer Region finden Sie im IBM Verzeichnis für weltweite Kontakte, das Sie im Web unter <http://www.ibm.com/planetwide> abrufen können.

---

## Produktinformationen

Informationen zu DB2 Universal Database-Produkten erhalten Sie telefonisch oder im World Wide Web unter <http://www.ibm.com/software/data/db2/udb>.

Diese Site enthält die neuesten Informationen zur technischen Bibliothek, zum Bestellen von Büchern, zu Produktdownloads, Newsgroups, FixPaks, Neuerungen und Links auf verfügbare Webressourcen.

Telefonische Unterstützung erhalten Sie über folgende Nummern:

- Unter 0180 3 313233 erreichen Sie Hallo IBM, wo Sie Antworten zu allgemeinen Fragen erhalten.
- Unter 0180 5 5090 können Sie Handbücher telefonisch bestellen.

Informationen dazu, wie Sie sich mit IBM in Verbindung setzen können, finden Sie auf der globalen IBM Internet-Seite unter folgender Adresse:  
[www.ibm.com/planetwide](http://www.ibm.com/planetwide)





**IBM**