МОДЕЛЬ БЕЗОПАСНОСТИ СУБД IBM DB2

ИГОРЬ БУЛАТЕНКО, POSITIVE TECHNOLOGIES

POSITIVE / TECHNOLOGIES®

ОГЛАВЛЕНИЕ

1	Введение	3
2	Точка входа. Аутентификация	4
3	Авторизация. Привилегии	9
4	Пользователи, группы, роли. LBAC	11
5	Автоматические средства сканирования	12
6	Полезные запросы и команды	13
7	Исследовательский центр Positive Research	14

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

1 Введение

Система управления базами данных IBM DB2 начинает свое развитие в далеких 70-х годах и сейчас занимает прочное положение на рынке корпоративных СУБД, отвечая высоким требованиям к производительности, надежности, безопасности и масштабируемости. В частном секторе система DB2 не получила широкого распространения, несмотря на наличие бесплатной версии IBM DB2 Express. Возможно, именно из-за этого в Интернете не так много статей по поводу настройки и использования DB2.

Модель безопасности DB2 обладает широким функционалом и позволяет защитить данные как от внешнего воздействия, так и разграничить права доступа для внутренних пользователей средствами самой СУБД.

Однако неподготовленному пользователю сложно с нуля разобраться во всем этом многообразии, поэтому некоторые важные аспекты будут рассмотрены в данной статье.

.....

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

2 Точка входа. Аутентификация

Точка входа

Точка входа в DB2 выглядит следующим образом: СУБД -> экземпляр (instance), который может быть привязан к определенному порту -> имя конкретной базы данных. Настройки безопасности могут быть изменены как в конкретном экземпляре, так и в конкретной базе данных.

Аутентификация

Аутентификация – это первоочередной механизм безопасности, который применяется, когда вы пытаетесь соединиться с сервером DB2. При аутентификации проверяется корректность предоставляемых учетных данных. Главной особенностью в DB2 является то, что аутентификация пользователей производится только внешними плагинами. Внутренних пользователей, в отличие от Oracle или MS SQL Server, здесь не существует. Даже функция создания пользователя, которая есть в программе IBM Data Studio, на самом деле не создает пользователя, а назначает указанному пользователю привилегию на соединение с базой данных.

Существует несколько вариантов аутентификации, нужный вариант регулируется параметром AUTHENTICATION в менеджере базы данных. Значение данного параметра влияет на то, где будет производиться аутентификация клиентов (на стороне сервера или на стороне клиента) и будут ли данные передаваться в зашифрованном виде (значения с окончанием _ENCRYPT). Поддерживаемые значения данного параметра доступны по следующему адресу:

http://publib.boulder.ibm.com/infocenter/db2luw/v9/topic/com.ibm.db2.udb.doc/doc/c0005598.htm

Просмотреть конфигурацию менеджера базы данных можно с помощью запроса к таблице sysibmadm.dbmcfg, но для этого нужно иметь доступ к любой из баз данных, что не всегда возможно. Если у вас есть локальный доступ к серверу, то можно открыть процессор командной строки (db2 или db2.exe в Windows), соединиться с экземпляром и выполнить следующие команды:

```
db2 => attach to db2inst1
db2 => get database manager configuration
```

Значением по умолчанию для параметра AUTHENTICATION является SERVER. Проверка правильности предоставленных учетных данных пользователя производится на стороне сервера средствами операционной системы, но все данные при этом передаются в открытом виде и могут быть перехвачены злоумышленником.

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

Рассмотрим, каким образом выглядит перехваченная информация в Wireshark.

```
  7 0.004828   10.111.          10.111.          DRDA     342 ACCSEC | SECCHK | ACCRDB
  8 0.006528   10.111.          10.111.          DRDA     359 ACCSECRD | SECCHKRM | ACCRDBRM | SQLCARD
  9 0.019271   10.111.          10.111.          DRDA     521 EXCSAT | EXCSQLSET | SQLSTT | PRPSQLSTT | SQLSTT | EXCSQLSTT | SQLD
 10 0.027482   10.111.          10.111.          DRDA     832 EXCSATRD | SQLCARD | SQLCARD | RSLSETRM | SQLDTARD | SQLRSLRD | OPN
 11 0.029554   10.111.          10.111.          DRDA     154 CLSQRY | RDBCMM
 12 0.029945   10.111.          10.111.          DRDA     119 SQLCARD | ENDUOWRM | SQLCARD
 13 0.229198   10.111.          10.111.          TCP       54 30799 > 50000 [ACK] Seq=1129 Ack=1273 Win=64264 Len=0
```

```
    Data (ASCII):
    Data (EBCDIC):
  ⊟ Parameter (Relational Database Name)
    Length: 22
    Code point: RDBNAM (0x2110)
    Data (ASCII): ⊠⊠⊠⊠⊠⊠@@@@@@@@@@@@
    Data (EBCDIC): DB2NEW
  ⊟ Parameter (Password)
    Length: 10
    Code point: PASSWORD (0x11a1)
    Data (ASCII): \230⊠\205\231⊠⊠
    Data (EBCDIC): qwerty
  ⊟ Parameter (User ID at the Target System)
    Length: 11
    Code point: USRID (0x11a0)
    Data (ASCII): \204\201⊠⊠⊠\231⊠
    Data (EBCDIC): dasusr1
⊞ DRDA (Access RDB)

0000  00 50 56 bb 00 de 70 71  bc 5f e5 0d 08 00 45 00   .PV...pq ._....E.
0010  01 48 5b fc 40 00 80 06  a6 dd 0a 6f 70 87 0a 6f   .H[.@... ...op..o
0020  71 71 78 4f c3 50 6f d2  e7 9b 26 92 f4 ed 50 18   qqxO.Po. ..&...P.
0030  7f c2 e3 3c 00 00 00 26  d0 41 00 01 00 20 10 6d   ...<...& .A... .m
0040  00 06 11 a2 00 03 00 16  21 10 c4 c2 f2 d5 c5 e6   ........ !.......
0050  40 40 40 40 40 40 40 40  40 40 40 40 00 3b d0 41   @@@@@@@@ @@@@.;.A
0060  00 02 00 35 10 6e 00 06  11 a2 00 03 00 16 21 10   ...5.n.. ......!.
0070  c4 c2 f2 d5 c5 e6 40 40  40 40 40 40 40 40 40 40   ......@@ @@@@@@@@
0080  40 40 00 0a 11 a1 98 a6  85 99 a3 a8 00 0b 11 a0   @@...... ........
0090  84 81 a2 a4 a2 99 11 00  bf d0 01 00 03 00 b9 20   ........ ....... 
00a0  01 00 06 21 0f 24 07 00  23 21 35 f1 f0 4b f1 f1   ...!.$.. #!5..K..
00b0  f1 4b f1 f1 f2 4b f1 f3  f5 4b f2 f0 f3 f4 f4 4b   .K...K.. .K.....K
```

Переданные от клиента логин и пароль видны в пакете при просмотре EBCDIC.

При изменении типа аутентификации на SERVER_ENCRYPT логин и пароль будут передаваться уже в зашифрованном виде и проверяться на стороне сервера.

Значение изменяется следующим образом:

db2 => attach to db2inst1
db2 => update database manager configuration using authentication server_encrypt
db2 => db2stop force
db2 => db2start

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

Пакет аутентификации при этом будет выглядеть так:

```
⊟ Parameter (Relational Database Name)
    Length: 22
    Code point: RDBNAM (0x2110)
    Data (ASCII): ⊠⊠⊠⊠⊠⊠@@@@@@@@@@@@@@
    Data (EBCDIC): DB2NEW
⊟ Parameter (Security Token)
    Length: 36
    Code point: SECTKN (0x11dc)
    Data (ASCII): \204⊠⊠?⊠.\024⊠⊠⊠F\027\236⊠\225⊠r5\222p⊠s⊠⊠&5K\212\255⊠\202A
    Data (EBCDIC): d64?{.\024u...\027.2nB.5k.6...&5..[]b.

0000  00 50 56 bb 00 de 70 71  bc 5f e5 0d 08 00 45 00   .PV...pq ._....E.
0010  01 39 77 96 40 00 80 06  8b 52 0a 6f 70 87 0a 6f   .9w.@... .R.op..o
0020  71 71 79 00 c3 50 37 e1  16 93 70 fa 6f 19 50 18   qqy..P7. ..p.o.P.
0030  80 00 9e bc 00 00 00 c7  d0 41 00 01 00 c1 10 41   ........ .A.....A
0040  00 80 11 5e e6 89 95 a2  98 93 4b 85 a7 85 40 40   ...^.... ..K...@@
0050  40 40 40 40 40 40 40 40  f1 f7 c5 c3 f2 f1 c6 c3   @@@@@@@@ ........
0060  f0 f0 f0 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0070  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0080  00 00 00 60 f0 f0 f0 f1  c9 c2 e4 d3 c1 e3 c5 d5   ...`.... ........
0090  d2 d6 40 40 40 40 40 40  40 40 40 40 40 40 40 40   ..@@@@@@ @@@@@@@@
00a0  40 40 40 40 40 40 c4 c2  f2 d5 c5 e6 40 40 f0 c4   @@@@@@.. ....@@..
00b0  c2 f2 40 40 40 40 40 40  40 40 40 40 40 40 40 f0   ..@@@@@@ @@@@@@@.
00c0  00 18 14 04 14 03 00 0a  24 07 00 0a 14 74 00 05   ........ $....t..
00d0  24 0f 00 08 14 40 00 09  00 0b 11 47 d8 c4 c2 f2   $....@.. ...G....
00e0  61 d5 e3 00 0e 11 6d c9  c2 e4 d3 c1 e3 c5 d5 d2   a.....m. ........
00f0  d6 00 0c 11 5a e2 d8 d3  f0 f9 f0 f7 f0 00 4a d0   ....Z... ......J.
0100  01 00 02 00 44 10 6d 00  06 11 a2 00 09 00 16 21   ....D.m. .......!
0110  10 c4 c2 f2 d5 c5 e6 40  40 40 40 40 40 40 40 40   .......@ @@@@@@@@
0120  40 40 40 00 24 11 dc 84  f6 f4 3f c0 2e 14 a4 fd   @@@.$... ..?.....
0130  a0 46 17 9e f2 95 c2 72  35 92 70 f6 53 cf b7 26   .F.....r 5.p.S..&
0140  35 4b 8a ad bd 82 41                               5K....A
```

Однако текст запросов и результат будет все равно передаваться в открытом виде.

Пакет с запросом в Wireshark:

```
15 0.690297  10.111.        10.111.        TCP     54 7916 > 50000 [ACK] Seq=1094 Ack=1247 Win=64290 Len=0
16 58.196049 10.111.        10.111.        DRDA   321 PRPSQLSTT | SQLATTR | SQLSTT | OPNQRY
17 58.236555 10.111.        10.111.        TCP     60 50000 > 7916 [ACK] Seq=1247 Ack=1361 Win=10240 Len=0
18 58.492650 10.111.        10.111.        DRDA   405 SQLDARD | OPNQRYRM | QRYDSC | QRYDTA | ENDQRYRM | SQLCARD
19 58.521232 10.111.        10.111.        DRDA    64 RDBCMM
20 58.521951 10.111.        10.111.        TCP     60 50000 > 7916 [ACK] Seq=1598 Ack=1371 Win=10240 Len=0
21 58.521981 10.111.        10.111.        DRDA   108 50000 > 7916 [PSH, ACK] Seq=1598 Ack=1371 Win=10240 Len=54 | ENDUOWRM | SQLCARD
22 58.722973 10.111.        10.111.        TCP     54 7916 > 50000 [ACK] Seq=1371 Ack=1652 Win=65482 Len=0

    Length: 36
    Magic: 0xd0
  ⊞ Format: 0x43
    CorrelId: 1
    Length2: 50
    Code point: SQLSTT (0x2414)
⊟ Parameter (Data)
    Length: 0
    Code point: DATA (0x0000)
    Data (ASCII): (select 'some text' from sysibm.sysdummy1⊠
    Data (EBCDIC): (..%... '.?_. ....' ..?_ .....__.....__...
  SQL statement (ASCII): (select 'some text' from sysibm.sysdummy1
  SQL statement (EBCDIC): (..%... '.?_. ....' ..?_ .....__.....__...
⊟ DRDA (Open Query)
  ⊟ DDM (OPNQRY)
    Length: 102
    Magic: 0xd0
  ⊞ Format: 0x01
    CorrelId: 2
```


Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

Пакет с ответом в Wireshark:

```
18 58.492650  10.111.          10.111.          DRDA    405 SQLDARD | OPNQRYRM | QRYDSC | QRYDTA | ENDQRYRM | SQLCARD
19 58.521232  10.111.          10.111.          DRDA     64 RDBCMM
20 58.521951  10.111.          10.111.          TCP      60 50000 > 7916 [ACK] Seq=1598 Ack=1371 Win=10240 Len=0
21 58.521981  10.111.          10.111.          DRDA    108 50000 > 7916 [PSH, ACK] Seq=1598 Ack=1371 Win=10240 Len=54 | ENDUOWRM | SQL
22 58.722973  10.111.          10.111.          TCP      54 7916 > 50000 [ACK] Seq=1371 Ack=1652 Win=65482 Len=0

    CorrelId: 2
    Length2: 25
    Code point: QRYDSC (0x241a)
DRDA (Query Answer Set Data)
  DDM (QRYDTA)
    Length: 23
    Magic: 0xd0
    Format: 0x53
    CorrelId: 2
    Length2: 17
    Code point: QRYDTA (0x241b)
DRDA (End of Query)
  DDM (ENDQRYRM)
    Length: 38
    Magic: 0xd0
    Format: 0x52
    CorrelId: 2
    Length2: 32

0030  00 50 6e e7 00 00 00 7e  d0 43 00 01 00 78 24 11   .Pn....~ .C...x$.
0040  00 00 00 00 00 30 30 30  30 30 53 51 4c 30 39 30   .....000 00SQL090
0050  31 32 00 00 00 00 00 00  00 00 00 01 00 00 00 01   12...... ........
0060  00 00 00 21 ff ff ff 00  00 00 00 20 20 20 20 20   ...!.... ...
0070  20 20 20 20 20 20 00 12  44 42 32 4e 45 57 20 20         .. DB2NEW
0080  20 20 20 20 20 20 20 20  20 20 00 00 00 00 ff ff             ......
0090  01 00 00 00 00 00 09 00  00 00 00 00 00 00 c0 01   ........ ........
00a0  04 b8 00 01 00 00 01 31  00 00 00 00 00 00 00 00   .......1 ........
00b0  00 00 ff ff 00 2c d0 52  00 02 00 26 22 05 00 06   .....,.R ...&"...
00c0  11 49 00 00 00 06 21 02  24 17 00 05 21 1f f1 00   .I....!. $...!...
00d0  05 21 50 01 00 0c 21 5b  00 00 00 00 00 00 00 00   .!P...![ ........
00e0  00 1f d0 53 00 02 00 19  24 1a 06 76 d0 3e 00 09   ...S.... $..v.>..
00f0  09 71 e0 54 00 01 d0 00  01 06 71 f0 e0 00 00 00   .q.T.... ..q.....
0100  17 d0 53 00 02 00 11 24  1b ff 00 00 09 73 6f 6d   ..S....$ .....som
0110  65 20 74 65 78 74 00 26  d0 52 00 02 00 20 22 0b   e text.& .R... ..
```

В случае, если для параметра AUTHENTICATION настроено значение DATA_ENCRYPT, то шифруются учетные данные пользователя, а также информация, передаваемая между клиентом и сервером.

Значение изменяется аналогично рассмотренному выше примеру:

db2 => attach to db2inst1
db2 => update database manager configuration using authentication data_encrypt
db2 => db2stop force
db2 => db2start

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

После этого передаваемые данные также будут шифроваться:

```
DRDA (Unknown (0xd297))
  DDM (Unknown (0xd297))
    Length: 62
    Magic: 0xd0
    Format: 0x44
    CorrelId: 1
    Length2: 56111

0000  00 50 56 bb 00 de 70 71  bc 5f e5 0d 08 00 45 00   .PV...pq ._....E.
0010  01 38 65 e5 40 00 80 06  9d 04 0a 6f 70 87 0a 6f   .8e.@... ...op..o
0020  71 71 1f 15 c3 50 26 2b  d5 d8 2f c5 d8 61 50 18   qq...P&+ ../..aP.
0030  7f 13 0c 00 00 00 00 53  d0 51 00 01 00 4d 20 0d   .......S .Q...M .
0040  00 44 21 13 44 42 32 4e  45 57 20 20 20 20 20 20   .D!.DB2N EW
0050  20 20 20 20 20 20 4e 55  4c 4c 49 44 20 20 20 20         NU LLID
0060  20 20 20 20 20 20 20 20  53 59 53 53 48 32 30 30            SYSSH200
0070  20 20 20 20 20 20 20 20  20 20 53 59 53 4c 56 4c              SYSLVL
0080  30 31 00 04 00 05 21 16  f1 00 1e d0 54 00 01 7a   01....!. ....T..z
0090  b1 a1 79 b4 6d fa 87 f6  2e 7d 78 b8 88 ea 06 b5   ..y.m... .}x.....
00a0  3a 6f 9e f6 07 b4 a7 00  3e d0 44 00 01 db 2f d2   :o....... >.D.../.
00b0  97 29 7d cd 70 f0 e0 97  46 5e 7a 9d 53 8e 37 e8   .)}.p... F^z.S.7.
00c0  c7 31 30 aa be 7f ae 89  00 f9 80 c5 18 44 75 cc   .10..... .....Du.
00d0  29 dc 71 a1 41 5a 03 e5  6a d6 c8 7e e4 40 63 05   ).q.AZ.. j..~.@c.
00e0  9c 00 61 a5 7c 00 61 d0  01 00 02 00 5b 20 0c 00   ..a.|.a. ....[ ..
00f0  44 21 13 44 42 32 4e 45  57 20 20 20 20 20 20 20   D!.DB2NE W
0100  20 20 20 20 20 4e 55 4c  4c 49 44 20 20 20 20 20        NUL LID
0110  20 20 20 20 20 20 20 53  59 53 53 48 32 30 30 20          S YSSH200
0120  20 20 20 20 20 20 20 20  20 53 59 53 4c 56 4c 30            SYSLVL0
0130  31 00 04 00 08 21 14 00  00 7f ff 00 06 21 41 ff   1....!.. .....!A.
0140  ff 00 05 21 5d 01                                  ...!].
```

Также, нужно обратить внимание на тип аутентификации CLIENT. При данном типе аутентификации считается, что между клиентом и сервером существует защищенный канал связи, и в случае, если пользователь получил доступ к клиенту, он может получить доступ к серверу без проверки правильности учетных данных. То есть аутентификация как таковая происходит на стороне клиента, проверки на стороне сервера не производится. Даже если у пользователя, который соединяется с сервером, нет прав на доступ, он все равно получает все привилегии, которые назначены группе PUBLIC. Поэтому не стоит использовать такой тип аутентификации, это предоставит злоумышленникам возможность без особых усилий получить доступ к серверу.

Если же вдруг по какой-то причине необходим такой тип аутентификации, то нужно учесть, что существует еще два дополнительных параметра, которые в конечном итоге влияют на то, как будет проходить проверка учетных данных пользователя. Это параметр trust_allclnts (http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/topic/com.ibm.db2.luw.admin.config.doc/doc/r0000380.html), с помощью которого можно указать, каких клиентов считать доверенными, и параметр trust_clntauth (http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/topic/com.ibm.db2.luw.admin.config.doc/doc/r0000381.html), определяющий, где проверять логин и пароль, если они были переданы при соединении. Оба этих параметра влияют на аутентификацию, только если параметр AUTHENTICATION имеет значение CLIENT.

В случае успешной аутентификации ID пользователя соотносится с идентификатором DB2. Обычно идентификатор совпадает с именем пользователя, но в нем используются символы верхнего регистра.

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

3 Авторизация. Привилегии

Авторизация

В процессе авторизации проверяется, есть ли у пользователя необходимые права для запрошенных им действий. Существуют полномочия (authorities) экземпляра СУБД и базы данных.

Полномочия уровня конкретного экземпляра прописываются в конфигурации менеджера БД. Речь идет о следующих полномочиях:

- SYSADM (полномочия администратора системы);
- SYSCTRL (полномочия на управление системой);
- SYSMAINT (полномочия на обслуживание системы);
- SYSMON (полномочия на мониторинг системы).

Задаются данные привилегии с помощью указания той группы, в которую будет входить пользователь. Для этого используются следующие параметры файла dbmcfg (соответственно указанным выше полномочиям):

- SYSADM_GROUP;

- SYSCTRL_GROUP;

- SYSMAINT_GROUP;

- SYSMON_GROUP.

Легко получить список пользователей, которые входят в группу, средствами DB2 нельзя, нужно делать это в самой операционной системе или анализировать, в какие группы входит конкретный пользователь (запрос см. на вкладке "полезные запросы").

При настройке DB2 обязательно необходимо проверить список пользователей, которым назначено полномочие SYSADM. Это полномочие позволяет управлять всеми объектами базы данных.

Полномочия конкретной базы можно посмотреть в представлении SYSCAT.DBAUTH (http://publib.boulder.ibm.com/infocenter/db2luw/v9r5/topic/com.ibm.db2.luw.sql.ref.doc/doc/r000

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

1041.html). Обратите внимание на привилегию CONNECTAUTH, которая определяет, будет у пользователя доступ к БД или нет, и привилегию NOFENCEAUTH, которая отвечает за создание неизолированных (not fenced) процедур и функций. Такие процедуры выполняются

в адресном пространстве базы данных и, в случае ошибки, могут нарушить целостность базы данных и таблиц в ней.

Привилегии

Привилегии в DB2 могут быть выданы на различные объекты. Привилегии доступа к таблицам можно просмотреть в представлении SYSCAT.TABAUTH. Данные о типе выданной привилегии хранятся в отдельных колонках, в зависимости от самой привилегии (SELECTAUTH, DELETEAUTH и т. д.). При выдаче привилегии с помощью команды GRANT для привилегий REFERENCES и UPDATE можно также указать имена колонок, на которые будут распространяться данные привилегии. Информацию об этом можно посмотреть в представлении SYSCAT.COLAUTH

Привилегии подпрограмм (функций, процедур и методов) можно посмотреть в представлении SYSCAT.ROUTINEAUTH. Здесь все не совсем тривиально, в зависимости от полей SPECIFICNAME и TYPENAME привилегии могут быть выданы на все подпрограммы заданной схемы.

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

4 Пользователи, группы, роли. LBAC

Пользователи, группы, роли

Все полномочия базы данных и различные привилегии могут быть выданы пользователям, группам или ролям. Существование пользователей, групп и членство пользователей в группах регулируется вне самой базы данных. В связи с этим желательно учитывать определенные рекомендации и знать некоторые тонкости при выдаче полномочий и привилегий. Не рекомендуется выдавать привилегии и полномочия базы данных, в особенности возможность соединения с базой данных (CONNECTAUTH), группам. Следует выдавать привилегии конкретным пользователям или ролям, которым это необходимо. Поддержка ролей появилась в DB2 начиная с версии 9.5. Управление членством в ролях производится внутри самой базы данных.

Также, в DB2 существует встроенная роль PUBLIC. Пользователю базы данных нет необходимости предоставлять роль PUBLIC: отозвать у пользователя роль PUBLIC невозможно. Когда привилегия предоставляется роли PUBLIC, фактически происходит предоставление привилегии всем пользователям базы данных. Не следует выдавать какие-либо полномочия базы данных роли PUBLIC. Привилегии на таблицы и представления стоит выдавать с крайней осторожностью, только на просмотр и без возможности переназначения (WITH GRANT OPTION).

Из-за особенности аутентификации при выдаче привилегий существование пользователя или группы в системе не проверяется. В результате в системе могут появиться аутентификационные пользователи без привязки к реальным пользователям системы. Найти таких пользователей можно с помощью следующего SQL-запроса:

SELECT authid FROM sysibmadm.authorizationids WHERE authidtype = 'U' AND authid NOT IN (SELECT username FROM TABLE(sysfun.USERS()) AS W)

Для поиска подобных групп используется аналогичный запрос, но при этом в запросе указывается, что данные о PUBLIC выводить не нужно:

SELECT authid FROM sysibmadm.authorizationids WHERE authidtype = 'G' AND authid NOT IN (SELECT groupname FROM TABLE(sysfun.groups()) AS W) AND authid != 'PUBLIC'

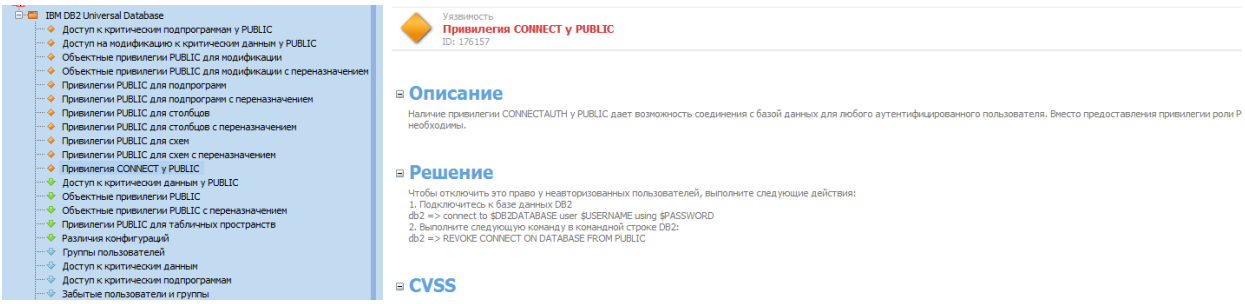
LBAC

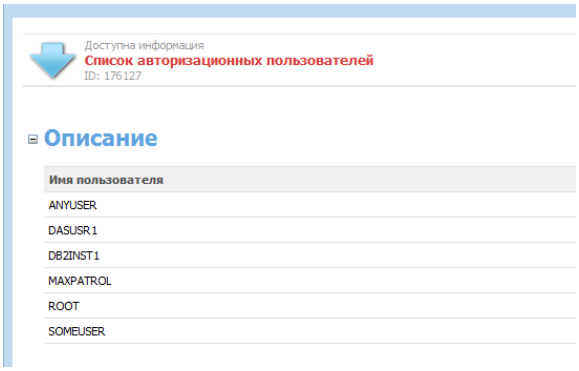
В DB2 есть мощный механизм разграничения доступа к данным в таблицах на основе меток (Label-based access control). Механизм позволяет установить метки защиты на конкретные строки или столбцы таким образом, что пользователь, у которого нет доступа к защищенным данным, не будет даже знать об их существовании. Нет смысла подробно рассказывать о методах реализации LBAC, так как у производителя есть учебное руководство по этой теме: http://www.ibm.com/developerworks/ru/edu/dm0605wong/index.html

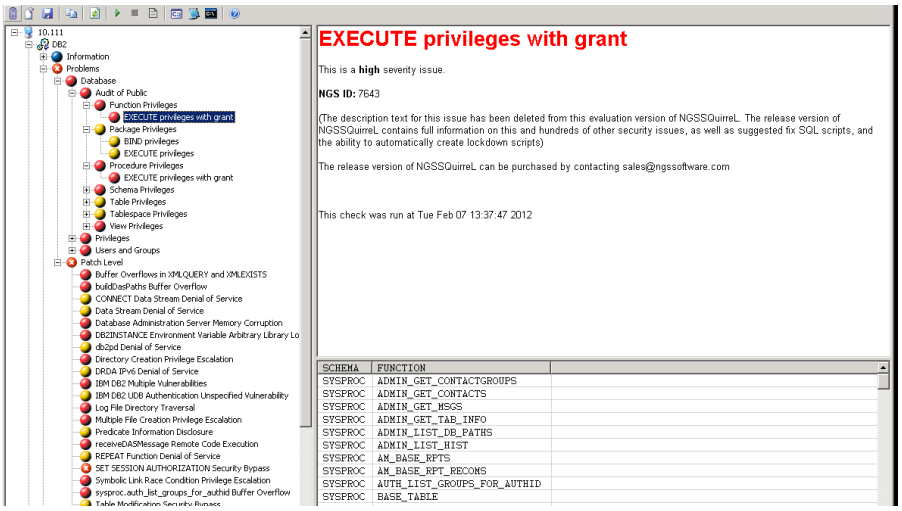
Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

5 Автоматические средства сканирования

При настройке безопасности сервера IBM DB2 важным моментом является использование каких-либо сканеров безопасности (например, NGS SQuirreL for DB2, MaxPatrol и т. п.). Сканеры явно укажут на уязвимости настроек, которые вы могли пропустить, или выведут информацию в удобном для анализа виде:







Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

6 Полезные запросы и команды

Получить настройки менеджера базы данных:
select name, value from sysibmadm.dbmcfg *либо* *db2 => get dbm cfg*

Изменить параметр менеджера базы данных:
db2 => update database manager configuration using <parameter> <value>

После этого необходим перезапуск экземпляра:
db2 => db2stop force
db2 => db2start

Получить настройки базы данных:
select name, value from sysibmadm.dbcfg
либо
db2 => get db cfg for <DBName>

Список пользователей операционной системы:
select username from table(sysfun.USERS()) AS t

Список групп операционной системы:
select groupname from table(sysfun.GROUPS()) AS t

Вывести авторизационные идентификаторы (пользователей, групп или ролей, которым назначались привилегии):
select AUTHID, AUTHIDTYPE from sysibmadm.AUTHORIZATIONIDS

Вывести текущее имя базы данных:
select current server from sysibm.sysdummy1

Ввести текущее имя пользователя:
select user from sysibm.sysdummy1

Получить список групп, в которые входит пользователь:
select GROUPNAME from table(sysfun.groups_for_user('<username>')) as t

Список всех установленных СУБД:
$ db2ls

Список всех экземпляров в СУБД:
$ db2ilist

Ограничить количество выводимых строк:
*select * from tabname fetch first 5 rows only*

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.

7 Исследовательский центр Positive Research

Positive Research – один из крупнейших в Европе исследовательских центров в области информационной безопасности. Он является инновационным подразделением компании Positive Technologies, ключевого эксперта в сегменте практических аспектов защиты информации.

С 2004 года при содействии Positive Research лидеры ИТ-отрасли, среди которых Microsoft, Cisco, Google, Avaya, Citrix, VmWare, Trend Micro, устранили несколько сотен уязвимостей и недочетов систем безопасности.

Copyright. © ЗАО «Позитив Текнолоджиз» 2012.
Использование данных материалов допускается с обязательной ссылкой на правообладателя и источник заимствования. ЗАО «Позитив Текнолоджиз» не несет ответственности за любые убытки или возможный ущерб, возникший при использовании материалов данных документов.