Session RAA6
DB2 for z/OS Security Features and Audit

Gayathiri Chandran
IBM Silicon Valley Laboratory
gchandran@us.ibm.com

Acknowledgements and Disclaimers

Availability. References in this presentation to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates.

The workshops, sessions and materials have been prepared by IBM or the session speakers and reflect their own views. They are provided for informational purposes only, and are neither intended to, nor shall have the effect of being, legal or other guidance or advice to any participant. While efforts were made to verify the completeness and accuracy of the information contained in this presentation, it is provided !"I! without warranty of any kind, e#press or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this presentation or any other materials. $othing contained in this presentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

ll customer e#amples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. ctual environmental costs and performance characteristics may vary by customer. $othing contained in these materials is intended to, nor shall have the effect of, stating or implying that any activities undertaken by you will result in any specific sales, revenue growth or other results.

U.S. Government Users Restricted Rights - Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

IBM, the IBM logo, ibm.com, %B&, and R '(are trademarks or registered trademarks of International Business Machines 'orporation in the)nited !tates, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol *+ or ,-, these symbols indicate).!. registered or common law trademarks owned by IBM at the time this information was published. !uch trademarks may also be registered or common law trademarks in other countries. current list of IBM trademarks is available on the Web at .'opyright and trademark information/ at www.ibm.com0legal0copytrade.shtml

1ther company, product, or service names may be trademarks or service marks of others.

Agenda

- Trusted context and roles
- Row and column level access controls
- Access Control Authorization Exit enhancements
- Program Authorization
- Audit policies
- Temporal tables for audit
- Summary

Trusted Contexts and Roles

DB2 9: Trusted context and Role

- Better access control from application servers.
- llows connections to be established as today. pplication attributes are verified before associating it with a trusted conte#t such as the application id and where the re2uest originated
- !upports identity propagation allowing authenticated non 301! distributed I%s to flow to %B& to be included in audit logs
- llows a uni2ue set of privileges by use of a Role to be associated with an application preventing the misuse of privileges when not accessing through the application
- 4rovides fle#ibility by removing ob5ect dependency from users
- ddresses administrator challenges

Trusted Context

- **Trusted context** establishes trust between %B& and an e#ternal entity such as
  - RR! (*Resource Recovery !ervices ttachment (acility-
  - ' (*'all ttachment (acility-
  - %!$ 'ommand 4rocessor
  - pplication !erver
- 1nce established, a **trusted connection** provides the ability to
  - 6fficiently switch user with optional authentication
  - c2uire special set of privileges using a Role
  - c2uire special R '(!ecurity 7abel authority
- Manage trusted conte#t using !87 'R6 T60 7T6R0%R14 TR)!T6% '1$T69T

Database Role

- %atabase entity with one or more privileges
- 6stablished only through a trusted connection
-)ser assigned only one role in a trusted connection
- 'an optionally be the 1W$6R of %B& ob5ects
- Manage role using !87 'R6 T60%R14R176

```
CREATE ROLE ADMINROLE;

DB2 native authorization – new ROLE keyword  or !RANTEE"
!RANT #$#ADM TO ROLE ADMINROLE;

RAC% e&it authorization – new CRITERIA keyword"
'ERMIT D#NADM #(B#$#)#$#ADM ID*ADMINA+
       ,-EN*CRITERIA*#.LROLE*ADMINROLE+++
```

Trusted context - Local

- Trusted conte#t can be local or remote
- 7ocal trusted conte#t is based upon
  - !ystem uthid
    -) ser I% associated with the connection
  - :1B$ M6
    - :ob or started task name associated with the connection

```
E&a/01e" A22i3n a ro1e DBAROLE to any 4o5 na/ed ADMIN6OB that
7onne7t2 u2in3 auth ID #ALL$

CREATE ROLE DBAROLE;

CREATE TR(#TED CONTE8T DBACONTE8T
   BA#ED ('ON CONNECTION (#IN! #$#TEM A(T-ID #ALL$
   ATTRIB(TE# 6OBNAME*9ADMIN6OB:+
   DE%A(LT ROLE DBAROLE
   ENABLE;
```

Trusted Context - Remote

- Remote trusted conte#t is based upon
  - !ystem uthid
    -) ser I% associated with the connection
  - %%R6 ! ! or ! 6R ;) T<
    - ' lient=s I4 address, domain name or ! 6R ;) T< security 3one name of the connection
  - 6 $ ' R>4TI 1 $
    - ' onnection encryption level * $ 1 $ 6 ? 7 1 W ? < I@<-

```
E&a/01e" A22i3n a ro1e TELLER to a 7onne7tion e2ta51i2hed  ro/
I' addre22 ;)<=)<=)<2= and the auth ID #R>RID=<)

CREATE ROLE TELLER;

CREATE TR(#TED CONTE8T TELLERCONTE8T
   BA#ED ('ON CONNECTION (#IN! #$#TEM A(T-ID #R>RID=<
   ATTRIB(TE# ADDRE##*9;)<=)<=)<2=:+
   DE%A(LT ROLE TELLER
   ENABLE;
```

Trusted Context Auth ID Switching

- llows trusted connection to be used by different users
- 1ptional authentication re2uirement
- !pecific R176 and R '(!ecurity 7abel can be assigned to the user

```
E&a/01e" A22i3n a ro1e TELLER to a 7onne7tion e2ta51i2hed  ro/
l'L‰e3R;)<=)<=)<2=' edi2h'2i2elD@#aÂta1@AA' ed
```

Trusted Context Auth ID Switching

- !witch user optionsA
  - B uthori3ation name
  - B 69T6R$ 7 !6')RIT> 4R1(I76 4rofile"name
    - C %B& primary authori3ation id or one of their groups has to be permitted to use the specified profile.
  - B 4)B7I'
- %istributed Identity
  - B R '(R 'M 4 command is used to map a distributed I% to a %B& R '(I%.

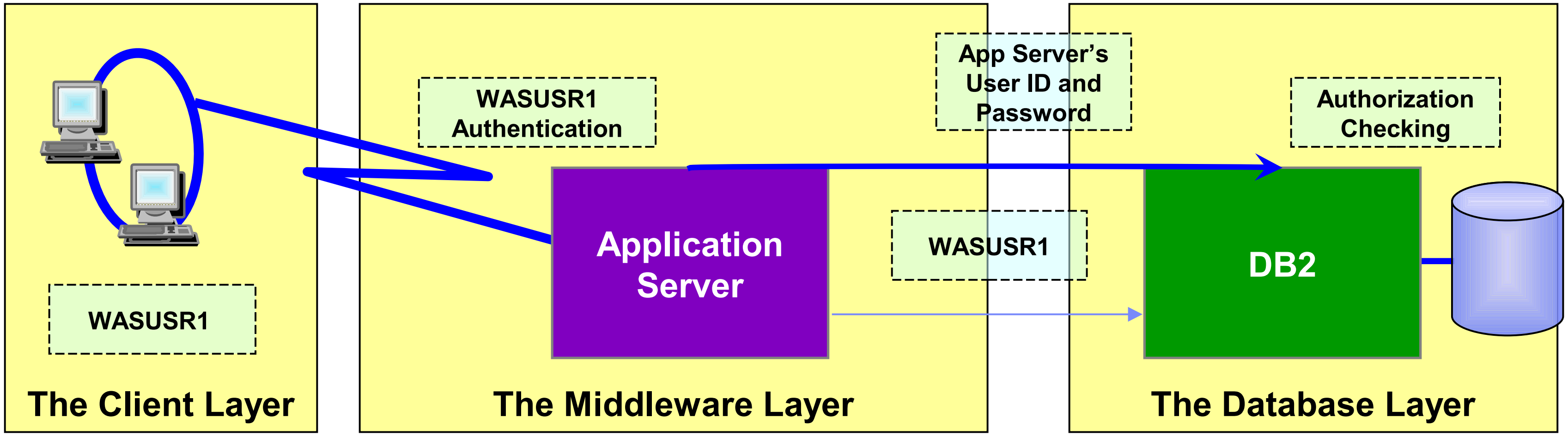
Use case: Separate owner privileges from DBA

- <elps address concerns with implicit owner privileges and %B access to sensitive data

- n auditable %B process can be done with trusted conte#t and roleA
  - @rant %B %M to role, %B R176
  - When a %B needs to perform a system changeA
    - C 6$ B76 trusted conte#t to allow access
    - C %I! B76 trusted conte#t after the change is done
  - n auditor can review the audit trace

```
CREATE ROLE DBAROLE;
!RANT DBADM ON DATABA#E 'RODDB TO ROLE
DBAROLE;
CREATE TR(#TED CONTE8T DBACT8<
BA#ED ('ON CONNECTION (#IN! #$#TEM A(T-ID ADMIN<
DE%A(LT ROLE DBAROLE ,IT- ROLE A# OB6ECT O,NER AND .(ALI%IER
ATTRIB(TE# *6OBNAME 96M@A+
ENABLE;
```

Trusted connections provide more effective controls and accurate audit trail for remote access



- The application serverDs user I% and password are used to establish the trusted connection
- The user is switched in the trusted connection and client user I% is propagated to the server and checked for database access
- %B& EF support for distributed identities introduced in 301 !   ; EREE allows to map client user I% to R   ' (user I%
  - distributed identity is a mapping between a R   ' (user I% and one or more distributed user identities, as they are known to application servers
  - %istributed identities are part of the %B& audit log.

$ew improved security features provide more effective controls and accurate audit trail for remote access

- !upport client certificate authentication in 301 ! ;EREF
  - T"T7! secure handshake accomplishes identification and authentication for client certificates
  - %B& client driver presents its certificate as identification and its *proof-of-possession* as authentication
  - %B& server can retrieve the user I% associated with the client certificate in ! (for the T"T7! policy rule configurationA
    <andshakeRole G !erverWith ' lient uth, ' lient uthType G ! (' heck
  - R ' (certificate name filtering *R ' % ' 6RT M 4 command- can map many certificates with one R ' (userid
- !upport password phrases in 301 ! ;EREF
  - C R ' (password phrase is a character string made up of mi#ed"case letters, numbers, special characters, and is between H to EFF characters long
  - C ' an be used instead of a traditional I"character password

Row and Column Access Controls

!atisfy >our uditorA

$ew table controls to protect against unplanned !87 access

- J %efine additional data controls at the row and column level
  - !ecurity policies are defined using !87
  - !eparate security logic from application logic
- J !ecurity policies based on real time session attributes
  - 4rotects against !87 in5ection attacks
  - %etermines how column values are returned
  - %etermines which rows are returned
- J ll access via !87 including privileged users, adhoc 2uery tools, report generation tools is protected
- J 4olicies can be added, modified, or removed to meet current company rules without change to applications

Table controls to protect !87 access to individual row level

- 6stablish a row policy for a table
  - (ilter rows out of answer set
  - 4olicy can use session information, e.g. the !87 I% is in what group or user is using what role, to control which row is returned in result set
  - pplicable to !676'T, I$!6RT,)4% T6, %676T6, K M6R@6
  - %efined as a row permissionA

CREATE PERMISSION policy-name ON table-name
FOR ROWS WHERE search-condition
ENFORCED FOR ALL ACCESS ENABLE;

Table controls to protect ! 8 7 access to individual column level

- 6stablish a column policy for a table
  - Mask column values in answer set
  - 4olicy can use session information, e.g. the ! 8 7 I% is in what group or user is using what role, to control what masked value is returned in result set
  - pplicable to the output of outermost subselect
  - %efined as column masks A

```
CREATE MASK  mask-name ON table-name
   FOR  COLUMN  column-name RETURN CASE-expression
ENABLE;
```

%efine table policies based on who or how the table is being accessed

- !6!!I1$L)!6R " 4rimary authori3ation I% of the process
- ')RR6$T !87I% " !87 authori3ation I% of the process
- ;6RI(>L@R1)4L(1RL)!6R function
  - @et the authori3ation I%s for the value in !6!!I1$L)!6R
  - Returns E if any of those authori3ation I%s is in the argument list

```
W<6R6
   ;6RI(>L@R1)4L(1RL)!6R*!6!!I1$L)!6R,MM@R=,M4  >R177=-GE
```

- ;6RI(>LR176L(1RL)!6R function
  - @et the role for the value in !6!!I1$L)!6R
  - Return E if the role is in the argument list

```
W<6R6
    ;6RI(>LR176L(1RL)!6R*!6!!I1$L)!6R, =M@R=,M4  >R177=-GE
```

Managing row and column access controls

- When activated row and column access controlsA
  - ll row permissions and column masks become effective in all %M7
  - ll row permissions are connected with M1R= to filter out rows
  - ll column masks are applied to mask output
  - ll access to the table is prevented if no user"defined row permissions

```
7T6R T  B76  table"name
   'TI;  T6R1W        ''6!! '1$TR17
   'TI;  T6'17)M$    ''6!! '1$TR17N
```

Managing row and column access controls

- When deactivated row and column access controlsA
  - Make row permissions and column masks become ineffective in %M7
  - 1pens all access to the table

```
7T6R T B76 table"name
 %6 'TI; T6R1W       ''6!! '1$TR17
 %6 'TI; T6'17)M$  ''6!!'1$TR17N
```

6#ample B simple banking scenario

- 1nly allow customer service representatives to see customer data but always with masked income
- TableA ') !T1M6R

Account	Name	Phone	Income	Branch
1111-2222-3333-4444	Alice	111-1111	22,000	A
2222-3333-4444-5555	Bob	222-2222	71,000	B
3333-4444-5555-6666	Louis	333-3333	123,000	B
4444-5555-6666-7777	David	444-4444	172,000	C

%efine row and column access control on customer table

- %efine row and column policies for customer service representatives
  - C llow access to all customer service representatives of the bank *a row permission-
  - C Mask all I$'1M6 values *a column mask-
    - – Return value F for incomes of &OFFF and below
    - – Return value E for incomes between &OFFF and POFFF
    - – Return value & for incomes between POFFF and EOFFFF
    - – Return value Q for incomes above EOFFFF
  - C 'ustomer service representatives are in the '!R group *who-

' reate Row 4ermission

- ' reate a row permission for customer service representatives

```
'R6  T6  46RMI!!I1$  '!RLR1WL   ''6!!  1$  ')!T1M6R
   (1R  R1W!  W<6R6
       ;6RI(>L@R1)4L(1RL)!6R*!6!!I1$L)!6R,='!R=-GE
6$(1R'6%(1R   77    ''6!!6$  B76N
```

' reate ' olumn Mask

- ' reate a column mask on I$ ' 1M6 column for customer service representatives

```
'R6  T6  M   !R  I$'1M6L'17)M$LM   !R  1$   ')!T1M6R

  (1R  '17)M$  I$'1M6  R6T)R$

      '   !6 W<6$ *; 6RI(>L@R1 )4L(1RL)!6R*!6!!I1$L)!6R,M'!R=-G E-

             T<6$  '   !6  W<6$ *I$'1M6 S EOFFFF- T<6$  Q
                           W<6$ *I$'1M6 S POFFF-   T<6$  &
                           W<6$ *I$'1M6 S &OFFF-   T<6$  E
                           67!6  F
                   6$%

          67!6 $)77
      6$%
6$  B76N
```

! tart enforcing row and column access contp rBf! P[illegible]

!electing from customer table
U after row and column access control activated

- !676'T ''1)$T,$ M6,I$'1M6,4<1$6 (R1M ')!T1M6RN

ACCOUNT	NAME	INCOME	PHONE
1111-2222-3333-4444	Alice	0	111-1111
2222-3333-4444-5555	Bob	1	222-2222
3333-4444-5555-6666	Louis	2	333-3333
4444-5555-6666-7777	David	3	444-4444

I$'1M6 automatically masked by %B&V

%B& effectively evaluates the following revised 2uery

```
!676'T   ''1)$T,
       $  M6,

       '  !6 W<6$ *;6RI(>L@R1)4L(1RL)!6R *!6!!I1$L)!6R,M'!R=-GE-
              T<6$ '  !6  W<6$ *I$'1M6 S EOFFFF- T<6$ Q
                         W<6$ *I$'1M6 S POFFF-   T<6$ &
                         W<6$ *I$'1M6 S &OFFF-   T<6$ E
                         67!6 F
                    6$%
          67!6 $)77
      6$% I$'1M6,

      4<1$6
(R1M  ')!T1M6R

W<6R6  ;6RI(>L@R1)4L(1RL)!6R *!6!!I1$L)!6R,M'!R=-GE  1R  EGFN
```

External Security (DSNX@XAC) Enhancements

%B& EEA 6#ternal !ecurity *%!$9W9 '- enhancements

Owner Authorization

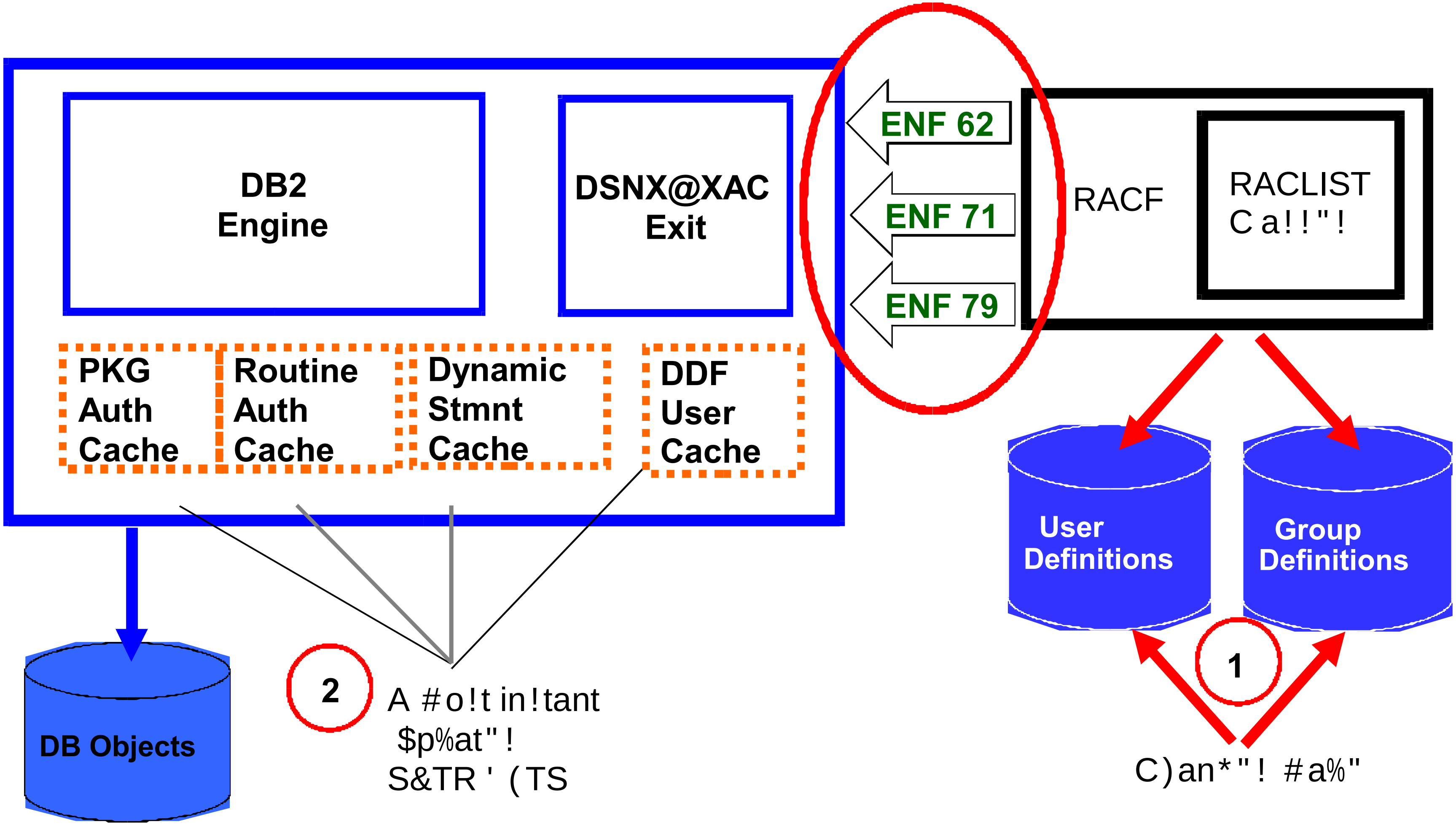
- !upport 1W$6R privileges for authori3ation
  - C llows owner to be checked for authori3ation on BI$% and R6BI$% commands
  - C !upports dynamic !87 authori3ation using %>$ MI'R)76! behavior
    - C 4ackage owner
    - C I% that e#ecutes the package
    - C I% that defined the routine
    - C I% that invokes the routine
  - C llows automatic rebind *)T1BI$%-
  - C 1wner can be a R '(I%, @R1)4 or R176. %B& provides owner '66 to R '(
  - C !imilar behavior between %B& native authori3ation and R '(e#it authori3ation

<ow to e#ploit owner authori3ation

- $ew installation parameter,)T<69ITL'<6'R to govern owner authori3ation
  - ; alueA %B&
    - 4rovides '66 of the owner for)T1BI$%0BI$%0R6BI$%
    - 4rovides '66 of the authori3ation I% as specified by the %>$ MI'R)76! value for dynamic !87 authori3ation
    - When owner is a group in R '(, 46RMIT the group access to the resource associated with the connection in R '(%!$R class
      - 6#A 46RMIT %!$ .B T'< '7 !!*%!$R- I%*%B @R1)4- ''6!!*R6 %-
  - ; alueA 4RIM R> *default B old behavior-
    - 4rovides '66 fo the primary authori3ation I% for all authori3ation checks
  - $o online update of this parameter

%B& EEA 6#ternal !ecurity *%!$9W9 '- 6nhancements

Sync RACF Permission Changes to DB2 Cache



RACF ENF Signals Heard by DB2 11

- R ' (6vent $otifications *6$(-
  - $otifications generated by R ' (when a profile is changed
- %B& EE listens forA
  - 6$(X&A R ' (options refreshed
    - !6TR14T! R '7I!T R6(R6!<
  - 6$(PEA) ser permissions changed
    - 7T)!6R R6; 1R6, '1$$6'T R6; 1R6, %67)!6R, %67@R1)4, R6M1; 6
  - 6$(PHA) ser permissions to access resource changed
    - 46RMIT..%676T6, ''6!!*$1$6-, R6!6T, W<6$*'RIT6RI *!87R176...--
    - R 7T6R..) ''*$1$6-, %67M6MN R%676T6
    - 1n receipt of 6$(PH, %B& stores the changes and refreshes cache entries only when 6$(X& is heard
    - Re2uirementA R ' (class descriptor table must have !I@$ 7 G >6!
      - 6nabled for IBM supplied R ' (resource classes for %B&

How to exploit cache refresh enhancement

- $ew installation parameter,)T<69ITL' '<6R6(R6!< to govern cache refresh
  - ; alueA 77
    - %B& listens for 6$(X&, 6$(PE and 6$(PH signals
    - 4ackage authori3ation cache, Routine authori3ation cache and dynamic statement cache entries are refreshed and dependent packages are invalidated
  - ; alueA $1$6 *default B old behavior-
    - The cache entries are not refreshed and dependent packages are not invalidated.
  - $o online update of this parameter

Cache Refresh Considerations

- The cache entries may not be refreshed or packages invalidated if user inherited authori3ation from a group and privilege is revoked from the group
- 6$(notification ignored for some generic resource names or more entries cleared from the cache
- !tatic package invalidation
  - %B& listens for 6$(X& and 6$(PH signals for static package invalidation
  - 1nly profile names with discrete characters are supported
  - 6$(notification ignored for profiles in %!$ %M class
  - %B& has to be started
- 'ache refresh considerations linkA

httpA00publib.boulder.ibm.com0infocenter0d3ichelp0v&r&0topic0com.ibm.db&3EE.doc.seca0src0tpc0db&3Lengsignalprocessing.htm

Program Authorization

DB2 11: Program Authorization

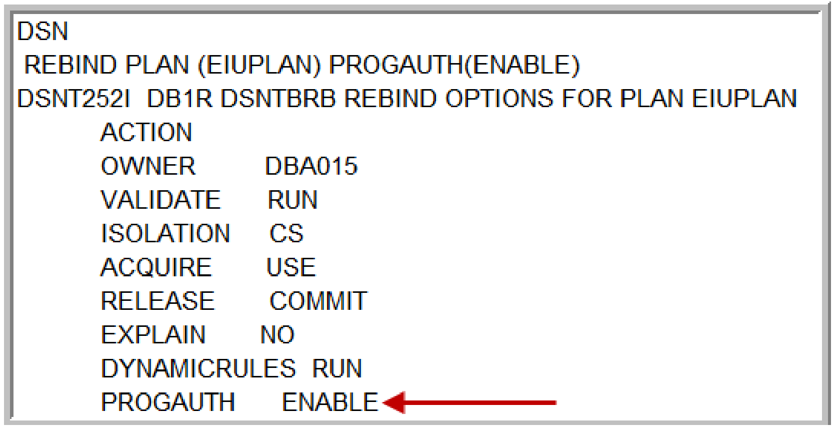
- llows a plan owner to authori3e a %B& production application program
  - 1wner controls the packages an application can use by defining a package list
  - 4ackage lists are difficult to manage causing the use of wild cards
- 4erformed in addition to package authori3ation
-)seful when all of the programs and packages that might use a plan are unknown

How to exploit Program Authorization

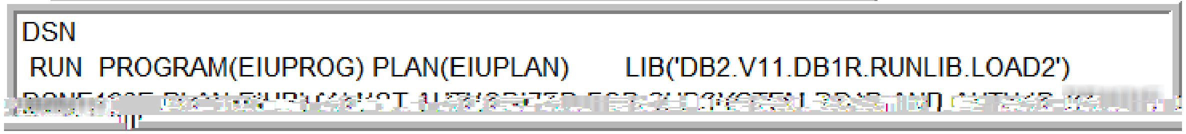
- Re2uires table, !>!IBM.%!$4R1@)T< and inde#, !>!IBM.%!$4R1@)T<LI%9E to e#ist
  - ' reated by installation 5ob, %!$TI:!@
- BI$% or R6BI$% 47 $ with 4R1@)T<*6$ B76- option
- dd a row in the !>!IBM.%!$4R1@)T< table for each program and plan combination for the 4R1@)T< enabled plan
- %B& ensures the program is authori3ed for the plan
- $ot supported forA
  - RR! (applications that use the default plan name, TRR! (
  - Multi"conte#t 1%B' applications with the plan name, %!$ '7I.
  - 4rograms that run in stored procedure address spaces

Program Authorization

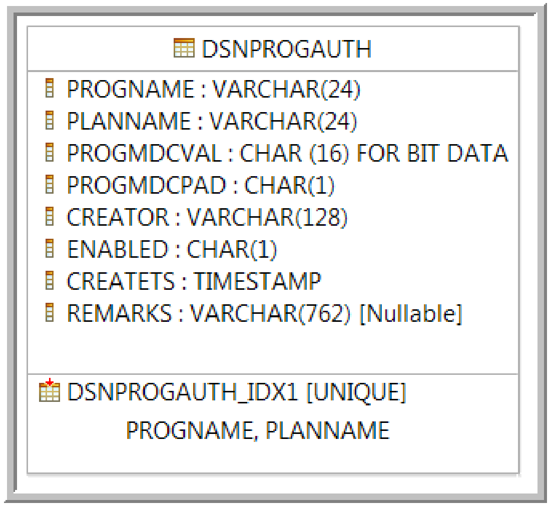
- R6BI$% and run with no %!$4R1@)T< entry



```
DSN
 REBIND PLAN (EIUPLAN) PROGAUTH(ENABLE)
DSNT252I  DB1R DSNTBRB REBIND OPTIONS FOR PLAN EIUPLAN
        ACTION
        OWNER        DBA015
        VALIDATE     RUN
        ISOLATION    CS
        ACQUIRE      USE
        RELEASE      COMMIT
        EXPLAIN      NO
        DYNAMICRULES  RUN
        PROGAUTH     ENABLE
```



```
DSN
 RUN  PROGRAM(EIUPROG) PLAN(EIUPLAN)      LIB('DB2.V11.DB1R.RUNLIB.LOAD2')
[illegible]
```



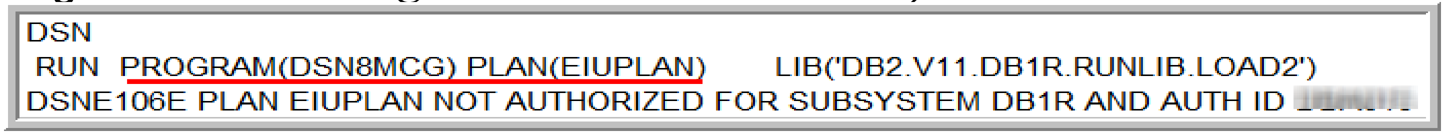
DSNPROGAUTH

- PROGNAME : VARCHAR(24)
- PLANNAME : VARCHAR(24)
- PROGMDCVAL : CHAR (16) FOR BIT DATA
- PROGMDCPAD : CHAR(1)
- CREATOR : VARCHAR(128)
- ENABLED : CHAR(1)
- CREATETS : TIMESTAMP
- REMARKS : VARCHAR(762) [Nullable]

DSNPROGAUTH_IDX1 [UNIQUE]

PROGNAME, PLANNAME

- I$!6RT %!$4R1@)T< entry for 6I)4R1@
  - $oteA %efaults to 6$ B76%G$
- 4rogram 6I)4R1@ now e#ecutes the plan
- 4rogram %!$IM'@ not allowed to use 6I)47 $



```
DSN
 RUN  PROGRAM(DSN8MCG) PLAN(EIUPLAN)      LIB('DB2.V11.DB1R.RUNLIB.LOAD2')
DSNE106E PLAN EIUPLAN NOT AUTHORIZED FOR SUBSYSTEM DB1R AND AUTH ID [redacted]
```

Audit

%B& EFA udit 4olicies

- $ew udit policy allows you to comply without the need of e#ternal collectors. Managed in the %B& catalog.
- uditor can define an audit policy to audit any access to specific tables for specific programs during day
  - udit policy does not re2uire)%IT clause to be specified using %%7
  - udit policy generate records for all !87 read and update access
  - udit policy includes additional records identifying the specific !87 statements
  - udit policy provides wildcarding of based on table names
- uditor can define an audit policy to identify any unusual use of a privileged authority
  - Records each use of an administrative authority
  - udit records written only when authority is used for access
  - 6#ternal collectors only report users with a system authority

<ow to e#ploit udit policies

- !ecurity administrator using the new !6' %M authority maintains %B& audit policies in a new catalog table
  - !>!IBM.!>!)%IT417I'I6!
- udit policies enabled using B!T TR '6 command
- udit policies disabled using B!T1 TR '6 command
-)p to I audit policies can be specified to auto start or auto start as secure during %B& start up
- 1nly user with !6' %M authority can stop a secure audit policy trace

udit policy categories

' ategories	Mapping I(' I%s
' <6 ' RI$@	I(' I% IQ *only authentication failures-, I(' I% EYF
; 7I% T6	I(' I%s OO, IQ, IP, EXH, &XH, QEH
1B:M I$T	I(' I% EY&
696 ')T6	I(' I%s EYQ, EYY, EYO
' 1$T69T	I(' I%s &Q, &Y, &O
!6 ' M I$T	I(' I%s EYE, &PF, &PE
!>! %MI$	I(' I% QXE * udits installation !>! %M, installation !>!14R, !>!14R, !>! ' TR7, !>! %M-
%B %MI$	I(' I% QXE * udits %BM I$T, %B ' TR7, %B %M, 4 ' R %M, !87 %M, system %B %M, % T ' ' 6!!, ' ' 6!! ' TR7, !6 ' %M-

6#ampleA %ynamic auditing of tables

- udit all the tables that start with M4 >= in 6M471>66 schema
  - %oes not re2uire)%IT clause to be specified during table definition

```
I$!6RT I$T1 !>!IBM.!>!  )%IT417I'I6!*  )%IT417I'>$  M6,
1B:6'T!'<6M  , 1B:6'T$  M6, 1B:6'TT>46, 696')T6-
  ;  7)6!*DT  B  %TED,M6M471>66D,D==4  >Z==D,DTD,D  D-N

"!T  TR  '6*  )%IT-%6!T*@T(-  )%T47'>*T  B  %TE-N
```

6#ample B udit privileged authority

- udit successful e#ecution of all actions using installation ! > ! %M authority and system %B %M authority

```
I$!6RT I$T1 !>!IBM.!>!  )%IT417I'I6!
  *  )%IT417I'>$  M6, !>!  %MI$, %B  %MI$-
  ;  7)6! *M  )%IT  %MI$D,MID,MBD-N

"!T  TR  '6*  )%IT- %6!T *@T(-  )%T47'>*  )%IT  %MI$-N
```

%B& EFA Temporal table

%B& can now manage different versions of your data

- Temporal table allows %B& to automatically maintain different versions of your data
- Two types of time se2uences of table rows are supported through the introduction of database defined time periods
  - !>!T6MLTIM6 is used to support data .versioning/ which archives old rows into a history table
  - B)!I$6!!LTIM6 is a period that represents when a row is valid to the user or application
  - BIT6M41R 7 table combines !>!T6MLTIM6 period and B)!I$6!!LTIM6 period

%efining system period on an e#isting table

- !ystem versioning is implemented by altering an e#isting or creating a table with two timestamps, a history table, and defining the versioning relationship between tables
- fter the base and history tables are appropriately definedA
  - 7T6R T B76 table"name %% ; 6R!I1 I@ is specified on the base table that is to be versioned
- uditor can 2uery historical data through ! 8 7
  - %B& rewrites the user=s 2uery to include data from the history table

Summary

- ✓ Trusted connections provide better user accountability and improved compliance.
- ✓ Row and column access table controls to safe guard your data
- ✓ 4rogram uthori3ation provides additional control on plan management
- ✓ ccess ' ontrol uthori3ation 6#it enhancements provide consistent security model and improved R ' (integration
- ✓ uditing features using audit policies provide better auditing capabilities
- ✓ Temporal data to comply with regulations to maintain historical data

R"+"r"n,"!

- S",$rit- F$n,tion! o+ IBM .B2 10 +or /0'S 1S224379593004
  - **http://www.redbooks.ibm.com**
- .B2 10 +or /0'S T",)ni,a '5"r5i"6 1S224378923004
  - **http://www.redbooks.ibm.com**
- .B2 10 +or /0'S Mana*in* S",$rit- 1SC19334963014
  - **http://pic.dhe.ibm.com/infocenter/dfom/iOp9f2e2ettmicp9com.io2tde.oc.s4p9:**

[illegible]

[illegible]

Thank
You