



Scott Forstie – [forstie@us.ibm.com](mailto:forstie@us.ibm.com)  
@Forstie\_IBMi  
Db2 for i Business Architect

# Db2 for i – Row & Column Access Control



# Technology Options

## 1. Application-centric security

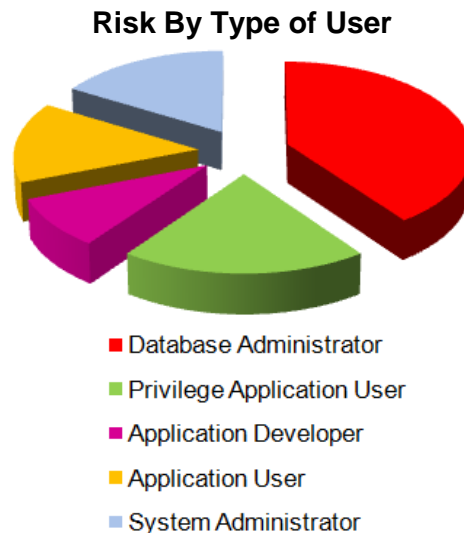
- Application layer provides custom data protection & tracking

## 2. Data-centric security

- Separation of duties
- Database enforced rules

## 3. Physical security

- Encryption hardware





# Contrasting Data Security

Technology	Field Procedures	Column Masks	Row Permissions	Views & Logical Files
<b>Use case</b>				
IBM i releases	7.1, 7.2, 7.3	7.2, 7.3	7.2, 7.3	All
Limit access to some/all data within a column	Yes	Yes	No	Yes
Limit access to rows	No	No	Yes	Yes
Security logic payload (customer experience)	External program (complex)	SQL rule (simple)	SQL rule (simple)	DDS or SQL (varies)
Software Vendor component	<ul style="list-style-type: none"> <li>• Townsend Security</li> <li>• Linoma</li> <li>• Enforcive</li> <li>• IBM i Lab Services</li> </ul>	<ul style="list-style-type: none"> <li>• SkyView Risk Assessor for IBM i</li> <li>• IBM i Lab Services</li> </ul>	<ul style="list-style-type: none"> <li>• SkyView Risk Assessor for IBM i</li> <li>• IBM i Lab Services</li> </ul>	N/A
Data encrypted at rest	Yes	No	No	No
Data encrypted in journal	Yes	No	No	No
Masked values apply to selection criteria	Yes	No	N/A	N/A
Data-Centric Solution	Yes	Yes	Yes	No



# Contrasting Db2 for i Governance

Technology	SQL Activity	Audit Journal	Data Journal
<b>Use case</b>			
<b>IBM i releases</b>	All	All	All
<b>Analysis &amp; Reporting</b>	<ul style="list-style-type: none"> <li>• IBM Security Guardium</li> <li>• PowerSC Tools for IBM i</li> <li>• Security ISVs</li> </ul>	<ul style="list-style-type: none"> <li>• IBM Security Guardium</li> <li>• PowerSC Tools for IBM i</li> <li>• Security ISVs</li> </ul>	<ul style="list-style-type: none"> <li>• InfoSphere Guardium DAM</li> <li>• PowerSC Tools for IBM i</li> <li>• Security ISVs</li> </ul>
<b>Solution infrastructure beyond IBM i</b>	Yes	No	No
<b>Capture SQL statements</b>	Yes	No	No
<b>Capture SQL host variable values and environment</b>	Yes	No	No
<b>Capture database specific Audit Journal details</b>	Yes	Yes	No
<b>Capture before and after images of data</b>	No	No	Yes
<b>Able to track which rows are seen by users</b>	No	No	No



# Separation of Duty

# Separation of duties

## Before IBM i 7.2

In order to grant or revoke privileges, a user must have one of the following:

1. Object ownership
2. Object management (\*OBJMGT) authority for the specified object
3. All object (\*ALLOBJ) user special authority

## Problem:

**To be able to grant the SELECT privilege, you must be allowed to see the data**

# Separation of duties

## With IBM i 7.2 and 7.3

**A user with security administration function usage (QIBM\_DB\_SECADM) will be able to grant or revoke privileges on any object to anyone, even if they do not have the SELECT privilege.**

### **Note that:**

- You should audit the QIBM\_DB\_SECADM users for \*SECURITY actions
- Only someone with \*SECADM authority can grant the QIBM\_DB\_SECADM function usage

# Separation of duty - example

**MARYSEC** – A Security Officer responsible for granting and revoking security



```
CRTUSRPRF USRPRF(MARYSEC)  
PASSWORD(xxxxxxxx)  
USRCLS(*SECADM) TEXT('Security Officer')
```

```
GRTOBJAUT OBJ(<data-libraries>) OBJTYPE(*LIB)  
USER(MARYSEC) AUT(*USE)
```

```
CHGFCNUSG FCNID(QIBM_DB_SECADM)  
USER(MARYSEC) USAGE(*ALLOWED)
```



# Separation of duty - example

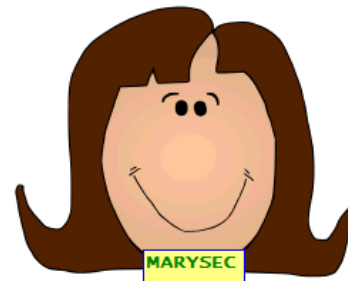
- **Use QIBM\_DB\_SECADM as a alternative authorization technique**

**Commands:**

CHGOBJOWN  
CHGOBJPGP  
GRTOBJAUT  
RVKOBJAUT  
EDTOBJAUT  
DSPOBJAUT  
WRKOBJ  
WRKLIB  
ADDAUTLE  
CHGAUTLE  
RMVAUTLE  
RTVAUTLE  
DSPAUTL  
DSPAUTLOBJ  
EDTAUTL  
WRKAUTL

**APIs: (also used by Navigator)**

qsyrtvua - retrieve users authorized to an object  
qsylusra - list users authorized to an object  
qsylatlo - list objects secured by an autl  
qsyrautu - retrieve users authorized to an object  
qsylautu - list authorized users  
qsyrusri - retrieve user information  
quslobj - list objects  
qgyolobj - open list of objects



**MARYSEC can  
manage security  
(and more) with just  
QIBM\_DB\_SECADM**

- **Other aspects of managing security don't have this alternative authorization method for security officers**

# CURRENT\_USER special register

- The CURRENT USER special register specifies the primary authorization ID that is being used for statement authorization.  
If a program adopts authority, it will return the adopted profile name.
- When multiple authorization IDs have been adopted the **most recently adopted authorization ID** within the thread.

# CURRENT\_USER special register

These **do NOT** adopt authority:

- SQL Routines built with SET OPTION Naming=\*SYS
- SQL Routines built with SET OPTION USRPRF=\*USER

These **do** adopt the authority of the \*PGM/\*SRVPGM owner:

- SQL Triggers
- SQL Routines built with SET OPTION Naming=\*SQL
- SQL Routines built with SET OPTION USRPRF=\*OWNER

External Routines adopt based upon this setting:

- User profile . . . . . : \*USER vs \*OWNER

# CURRENT\_USER special register

USER this, USER that... which one should I use?

Special Register	Definition
<b>USER</b> or <b>SESSION_USER</b>	The <u>effective user</u> of the thread is returned.
<b>SYSTEM_USER</b>	The authorization ID that <u>initiated the connection</u> is returned.
<b>CURRENT_USER</b> or <b>CURRENT_USER</b>	The most recently <u>adopted authorization ID</u> within the thread will be returned.  When no adopted authority has occurred, the effective user of the thread is returned.



# RCAC Basics

# RCAC Overview

## SQL Statements

- CREATE PERMISSION
- ALTER PERMISSION
- CREATE MASK
- ALTER MASK
- ALTER TRIGGER
- TRANSFER OWNERSHIP

## Built-in Function

- VERIFY\_GROUP\_FOR\_USER()

## Function Usage ID

- QIBM\_DB\_SECADM

## Catalogs

- QSYS2/SYSCONTROLS
- QSYS2/SYSCONTROLSDEP

## Operating System Option

IBM Advanced Data Security  
for i

**(5770SS1 - Option 47)**

No Charge



## Journal Entries

**For journal code D - Database file:**

- M1, M2, M3 for create/drop/alter mask
- P1, P2, P3 for create/drop/alter permission

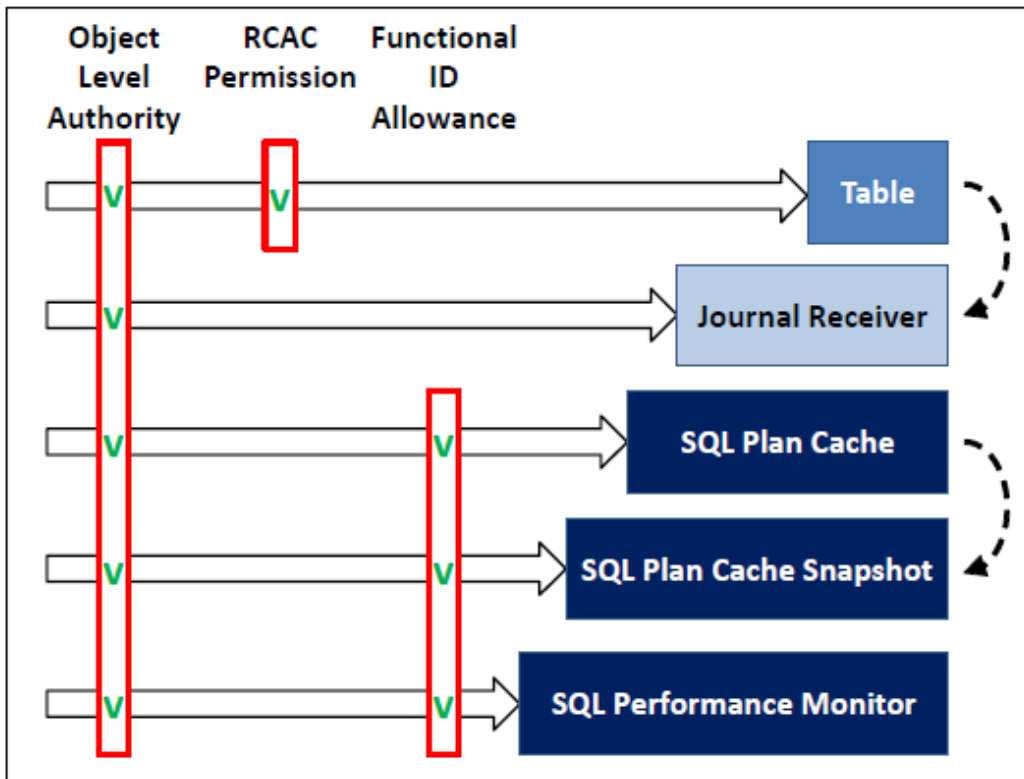
**For journal code T – Audit trail:**

- AX for Row and Column Access Control
- X2 for Query manager profile changes

# RCAC Terminology

<b>Base Table</b>	The table (physical file) containing business critical data.
<b>Dependent Object</b>	Any object (file, schema, function, or other object) the permission or mask references.
<b>Permission</b>	<p>A row permission defines a row access control rule for rows of a table by setting an SQL search condition that describes the set of rows a user can access.</p> <p><b>0 to many → permissions allowed per table</b></p>
<b>Mask</b>	<p>A column mask defines a column access control rule for a specific column in a table by using an SQL CASE expression that describes what column values a user is permitted to see and under what conditions.</p> <p><b>0 or 1 → masks allowed per column</b></p>
<b>RULETEXT</b>	The expression to be used by the permission (WHERE clause predicates) or mask (selection CASE expression)

# Data access authorization precedence rules





# Row Permissions

```
CREATE PERMISSION PATIENT_TABLE_HMO_PERMISSION
  ON PATIENT_TABLE FOR ROWS
WHERE((
  VERIFY_GROUP_FOR_USER(SESSION_USER, 'PCP') = 1 AND
  PATIENT_TABLE.PCP_ID = SESSION_USER)
OR
  VERIFY_GROUP_FOR_USER(SESSION_USER, 'ACCTGROUP') = 1
OR
  VERIFY_GROUP_FOR_USER(SESSION_USER, 'RESGROUP') = 1)
ENFORCED FOR ALL ACCESS ENABLE;

ALTER TABLE PATIENT_TABLE
  ACTIVATE ROW ACCESS CONTROL;
```

- **Logically, the table begins as an empty table, with permissions providing access to specific rows**
- 1 → n permissions are UNION'ed together
- No ordering considerations
- Isn't limited to User identity

# Column Masks

```
CREATE MASK SSN_MASK ON EMPLOYEE
FOR COLUMN SSN RETURN
CASE
WHEN (VERIFY_GROUP_FOR_USER(SESSION_USER, 'PAYROLL') = 1)
THEN SSN
WHEN (VERIFY_GROUP_FOR_USER(SESSION_USER, 'MGR') = 1)
THEN 'XXX-XX-' CONCAT RIGHT(SSN,4)
ELSE NULL
END ENABLE;

ALTER TABLE EMPLOYEE ACTIVATE COLUMN ACCESS CONTROL;
```


- **CASE** statement evaluated in order until WHEN expression evaluates to TRUE
- Applied when the column appears in the SELECT list
- Has no impact on selection (WHERE)
- Case logic is usually based upon identity, but can contain other rules

# Using Built-in Global Variables

```
CREATE OR REPLACE MASK SSN_MASK ON
EMPLOYEE
FOR COLUMN SSN
RETURN CASE
WHEN (QSYS2.JOB_NAME LIKE '%QZDAS%INIT')
THEN 'XXX-XX-' CONCAT
      RIGHT(SSN,4)
ELSE SSN END ENABLE;

ALTER TABLE EMPLOYEE
ACTIVATE COLUMN ACCESS CONTROL;

SELECT LASTNAME, EMPNO, SSN
FROM EMPLOYEE ORDER BY 1;
```



LASTNAME	EMPNO	SSN
ADAMSON	000150	XXX-XX-0015
ALONZO	200340	XXX-XX-0034
BROWN	000200	XXX-XX-0020
GEYER	000050	XXX-XX-0005
GOUNOT	000340	XXX-XX-0034
HAAS	000010	XXX-XX-0001
HEMMINGER	200010	XXX-XX-0001
HENDERSON	000090	XXX-XX-0009
JEFFERSON	000230	XXX-XX-0023
JOHN	200220	XXX-XX-0022
JOHNSON	000260	XXX-XX-0026
JONES	000210	XXX-XX-0021
KWAN	000030	XXX-XX-0003
LEE	000330	XXX-XX-0033
LUCCHESSI	000110	XXX-XX-0011
LUTZ	000220	XXX-XX-0022
MARINO	000240	XXX-XX-0024
MEHTA	000320	XXX-XX-0032
MONTEVERDE	200240	XXX-XX-0024
NATZ	200140	XXX-XX-0014
NICHOLLS	000140	XXX-XX-0014
O'CONNELL	000120	XXX-XX-0012
ORLANDO	200120	XXX-XX-0012

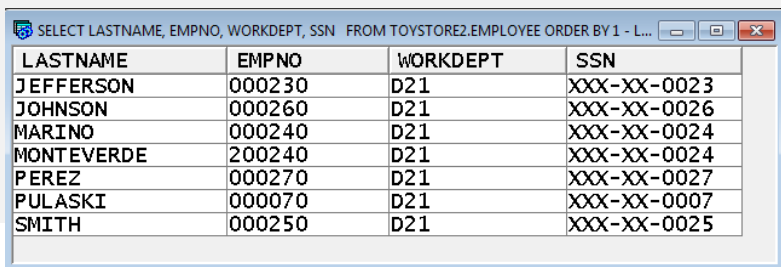
# Using Built-in Global Variables

```
CREATE OR REPLACE VARIABLE manager_of_department char(3)
DEFAULT
(SELECT DEPTNO FROM vdepmg1 WHERE MGRNO =
(SELECT EMPNO FROM vemp WHERE USER_PROFILE_NAME = USER));
```

```
CREATE OR REPLACE PERMISSION permission_on_employee on
employee FOR ROWS WHERE
(manager_of_department = WORKDEPT) OR
(USER_PROFILE_NAME = USER) ENFORCED FOR ALL ACCESS ENABLE;
```

```
ALTER TABLE EMPLOYEE ACTIVATE ROW ACCESS CONTROL;
```

```
SELECT LASTNAME, EMPNO,
WORKDEPT, SSN
FROM EMPLOYEE
ORDER BY 1;
```



SELECT LASTNAME, EMPNO, WORKDEPT, SSN FROM TOYSTORE2.EMPLOYEE ORDER BY 1 - L...

LASTNAME	EMPNO	WORKDEPT	SSN
JEFFERSON	000230	D21	XXX-XX-0023
JOHNSON	000260	D21	XXX-XX-0026
MARINO	000240	D21	XXX-XX-0024
MONTEVERDE	200240	D21	XXX-XX-0024
PEREZ	000270	D21	XXX-XX-0027
PULASKI	000070	D21	XXX-XX-0007
SMITH	000250	D21	XXX-XX-0025

# Constraints for Column Masks

**Question:** How do we protect against the masked value accidentally being added or updated in the table?

```
-- Numeric Column Mask Check Constraint  
ALTER TABLE toystore.employee ADD CHECK  
(SALARY <> 99999999.99)  
ON INSERT VIOLATION SET SALARY = DEFAULT  
ON UPDATE VIOLATION PRESERVE SALARY;
```



```
-- Character Column Mask Check Constraint  
ALTER TABLE toystore.employee ADD CHECK  
(SSN NOT LIKE '%XXX-XX%')  
ON INSERT VIOLATION SET SSN = DEFAULT  
ON UPDATE VIOLATION PRESERVE SSN;
```



# RCAC and Triggers

- Trigger programs have access to unmasked data
- Therefore, Triggers must be created or altered to have the **SECURED** attribute
- If a trigger is not secure, RCAC cannot be activated for the target table

```
Message ID . . . . . : SQ20469          Severity . . . . . : 30
Message type . . . . . : Diagnostic
Date sent . . . . . : 05/03/14          Time sent . . . . . : 13:10:55

Message . . . . . : Access control on table EMPLOYEE in BURNXMP5 is not valid.
Cause . . . . . : Row or column access control for table EMPLOYEE in
BURNXMP5 either cannot be activated or is not valid. The reason code is 37.
Reason codes are:
37 -- A trigger, INSERT_EMPLOYEE_TRIG1 in BURNXMP5, is defined for the
table and the trigger is not defined as secured or is a read trigger.
```

# RCAC and Functions

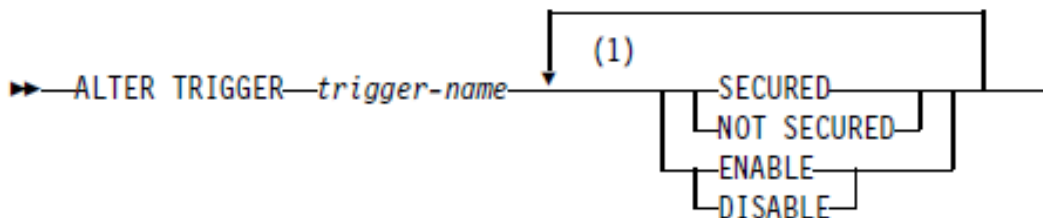
- Function invocations are allowed within RCAC rules and provide the ability to create more complex and modularized RCAC rule text logic
- **Therefore, Functions must be created or altered to have the SECURED attribute**
- If a function is not secure, the permission or mask cannot be enabled

```
Message ID . . . . . : SQ20474      Severity . . . . . : 30
Message type . . . . . : Diagnostic
Date sent . . . . . : 05/03/14      Time sent . . . . . : 13:53:44

Message . . . . . : Permission or mask EMPLOYEE_PERM1 in BURNXMP5 is not
valid.
Cause . . . . . :
The requested operation has failed because permission or mask
EMPLOYEE_PERM1 in BURNXMP5 directly or indirectly references one of the
following, as described by reason code 3.
  1 -- The table for which the row permission or the column mask is being
defined. The definition references EMPLOYEE in BURNXMP5, type *FILE, or
references view or alias RETURN_NAME_FUNCTION in *LIBL that is defined over
EMPLOYEE in BURNXMP5.
  3 -- User-defined function RETURN_NAME_FUNCTION in *LIBL, which is not
secure.
```

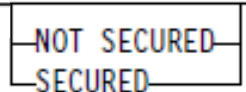
# Alter statement enhancements

## ALTER TRIGGER



## ALTER FUNCTION

- ALTER FUNCTION (external scalar)
- ALTER FUNCTION (external table)
- ALTER FUNCTION (SQL scalar)
- ALTER FUNCTION (SQL table)



**Only the QIBM\_DB\_SECADM user can mark a trigger or function as SECURED**





# RCAC – FAQ

# FAQ

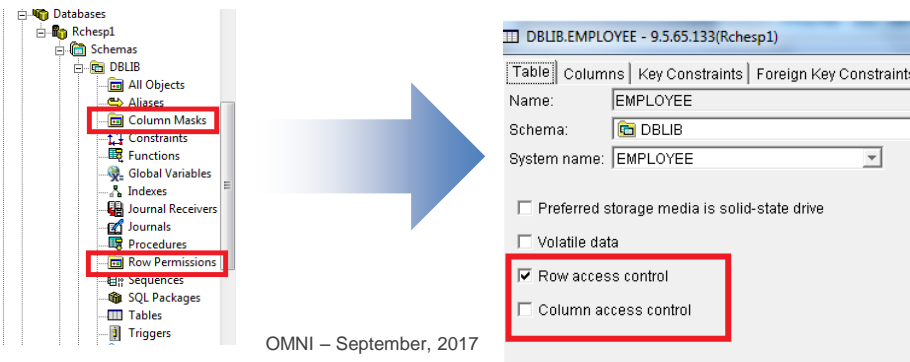
## How do I determine if RCAC is enabled for a file?

- DSPOBJAUT command  
(only appears if you have QIBM\_DB\_SECADM)

```

Object . . . . . : EMPLOYEE      Owner . . . . . : MITCHHOL
Library . . . . . : DBLIB        Primary group . . . . . : *NONE
Object type . . . . . : *FILE      ASP device . . . . . : *SYSBAS
Row or column access control . . . . . : Active
Object secured by authorization list . . . . . : *NONE
    
```

- Use Access Client Solutions (ACS)



The screenshot shows the IBM Access Client Solutions (ACS) interface. On the left, a tree view displays the database structure: Databases > Rchesp1 > Schemas > DBLIB > All Objects > Column Masks (highlighted with a red box) and Row Permissions (highlighted with a red box). A large blue arrow points from this tree to the right-hand pane. The right-hand pane shows the properties for the table 'DBLIB.EMPLOYEE - 9.5.65.133(Rchesp1)'. The 'Table' tab is selected, showing the table name 'EMPLOYEE' and schema 'DBLIB'. Under the 'Permissions' section, the 'Row access control' checkbox is checked and highlighted with a red box, while the 'Column access control' checkbox is unchecked.

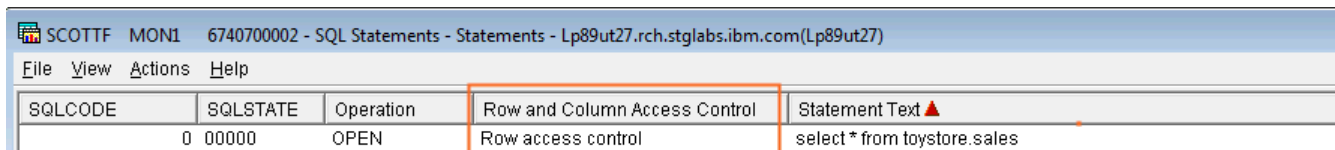
# Queries

To understand whether RCAC is applied on SQL statements

1. SQL Performance Monitor (Database Monitor)
2. Visual Explain

## SQL Performance Monitor analysis via Navigator

- Add the 'Row and Column Access' column to your dialog



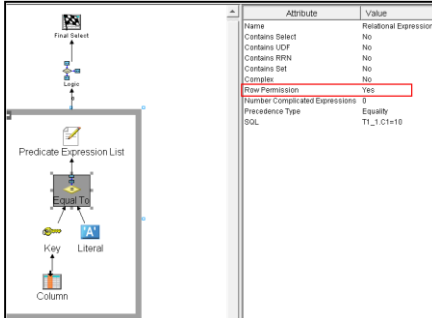
SQLCODE	SQLSTATE	Operation	Row and Column Access Control	Statement Text ▲
0	00000	OPEN	Row access control	select * from toystore.sales

# Visual Explain

- "Access Control" is in the **"Additional Information about SQL"** section. [Row, Column, Row and Column, or None]
- Row permissions are also noted in the **attribute section of predicates**
- Column masks show up by name only (not the whole mask definition) in the **statement text for a node**

Additional information about SQL...	
CLOSECURSOR Value	
ALWCPYDTA Value	Any Time
Pseudo Open	No
Pseudo Close	No
Hard Close Reason Code	Not Available
ODP Implementation	Reusable
Dynamic Replan Reason Code	Unknown
Timestamp When Plan Was Cre...	2014-04-01-08.30
Data Conversion Reason Code	Not applicable
Blocking Enabled	ALWBLK("ALLRE/
Delay Prep	Yes
Statement is Explainable	Yes
Naming Convention	SQL
Type of Dynamic Processing	System Wide Cacl
SQL Path	"QSYS","QSYS2","
Concurrent Access Resolution ...	Not applicable
IP Port Number	8,471
Client IP Address	9.10.111.53
IP Address Type	1
XML data CCSID	1,208
AQP Used in Access Plan	No
AQP Access Plan Iteration	1
Access Control	Row

Information About the Plan Perf...	
Scrollable	Yes
Plan Name	Logic
Plan Step Type	Logic
Plan Step Name	Node_2
Statement Text	SELECT T1_1.C1 T1_1.C2 FROM Node_7



The diagram shows a 'Final Select' node connected to a 'Predicate Expression List' node. The 'Predicate Expression List' node contains an 'Equal To' operator. Below the operator are 'Key' and 'Literal' nodes, which are connected to a 'Column' node. To the right of the diagram is a table showing the attributes and values for the 'Equal To' operator.

Attribute	Value
Name	Relational Expression
Contains Select	No
Contains CCF	No
Contains RRN	No
Contains Set	No
Complete	No
Row Permission	Yes
Number Complicated Expressions	0
Precedence Type	Equality
SOL	T1_1.C1=10

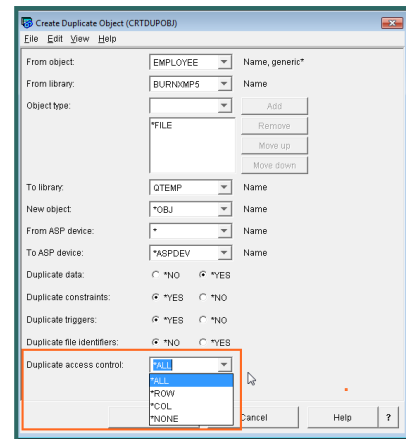
# Copying Files

- Create Duplicate Object (**CRTDUPOBJ**) & Copy Library (**CPYLIB**) command

**Duplicate access control (ACCCTL)** - new parameter for RCAC which defaults to include all RCAC controls

Command will fail if directed to copy data and to remove enabled RCAC

When access control is duplicated, must abide by RCAC restrictions



# Copying Files

- Copy File (**CPYF**) & Copy To Import File (**CPYTOIMPF**) commands

No duplicate access control parameter

**RCAC is applied prior to copying the file**

No warning or failure is indicated when RCAC is applied on the copy

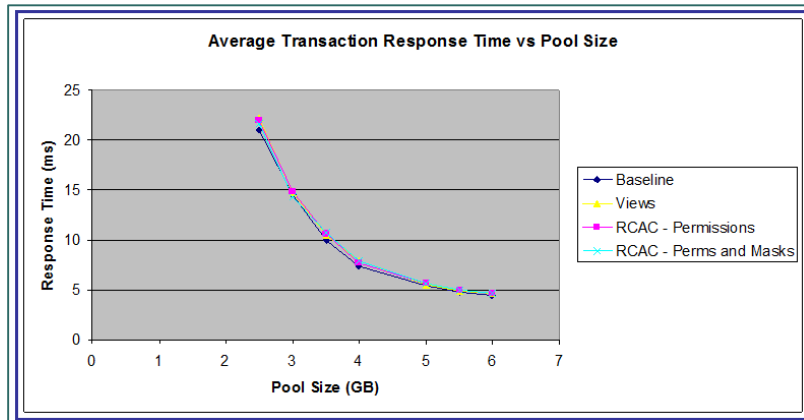
Beware, you could end up with fewer rows and/or masked columns values



# RCAC - Resources

# Performance

Read this article to understand how Row Permissions & Column Masks will impact performance of SQL and Native DB workloads.

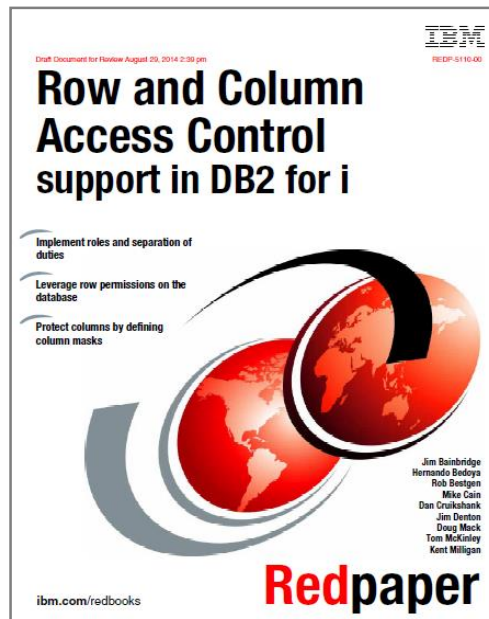


<https://ibm.biz/DB2foriRCACperf>



# RCAC Redpaper

Many of your questions will be answered by reading this Redpaper



[www.redbooks.ibm.com/redpieces/abstracts/redp5110.html](http://www.redbooks.ibm.com/redpieces/abstracts/redp5110.html)

# RCAC Workshop

**Offered by the STG Lab Services team**

**Four day facilitated workshop led by the Db2 for i Center of Excellence including the following:**

- Review of the current state, current requirements, and future requirements for managing data access
- Education on possible solutions and related best practices for their implementation
- Discussion and formulation of a strategic roadmap for implementation

**For more information, contact [mcaïn@us.ibm.com](mailto:mcaïn@us.ibm.com)**



**i**thankyou

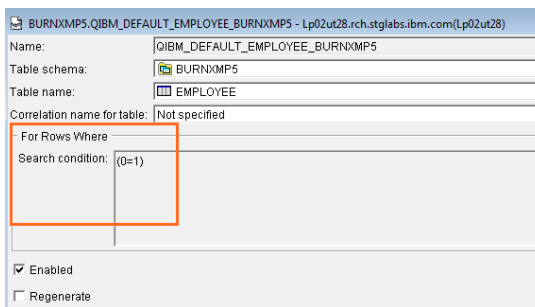
[www.ibm.com/developerworks/ibmi/techupdates/db2](http://www.ibm.com/developerworks/ibmi/techupdates/db2)

# More FAQ

- You aren't allowed to INSERT rows that you would be unable to query

```
SQL State: 22542
Vendor Code: -20471
Message: [SQ20471] INSERT or UPDATE does not satisfy row permissions. Cause . . .
. . . : Row access control is enforced for EMPLOYEE in BURNXMP5. Consequently,
all attempts to insert or update rows in that table are checked to ensure that
the resulting rows conform to the row permissions defined for the table. The
INSERT or UPDATE could not be done because a resulting row did not satisfy one or
more row permissions for EMPLOYEE in BURNXMP5. Recovery . . . : Change the
data being inserted or updated so that it conforms to the rules defined for the
row permissions.
```

- If you activate ROW ACCESS CONTROL for a table that has NO row permissions defined and ENABLED, all rows become inaccessible for all users. Ouch!



BURNXMP5.QIBM\_DEFAULT\_EMPLOYEE\_BURNXMP5 - Lp02ut28.rch.stglabs.ibm.com(Lp02ut28)

Name:	QIBM_DEFAULT_EMPLOYEE_BURNXMP5
Table schema:	BURNXMP5
Table name:	EMPLOYEE
Correlation name for table:	[Not specified]
For Rows Where	
Search condition:	(0=1)
<input checked="" type="checkbox"/> Enabled	
<input type="checkbox"/> Regenerate	

# More FAQ

- You can't save a \*FILE to previous releases when column masks or row permissions exist over that file

```
SAVOBJ OBJ(QCSRC) LIB(SCOTTF) DEV(*SAVF) OBJTYPE(*FILE) SAVF(QGPL/SAV1) T
GTRLS(V7R1M0)
File not valid for save.
FILE QCSRC in SCOTTF not saved.
```

```
Message ID . . . . . : CPI3215      Severity . . . . . : 10
Message type . . . . . : Information
Date sent . . . . . : 05/05/14      Time sent . . . . . : 14:01:33
```

```
Message . . . . . : File not valid for save.
Cause . . . . . : File QCSRC in library SCOTTF could not be saved for the
specified target release for reason code 1. The reason codes are:
1 - The file has fields in its record format whose attributes are not
supported on the target release or the file is an SQL table or view that
specifies new function that is not supported on the target release.
```

# More FAQ

- **How do you count rows?**

```
-- Count(*) returns 4
select count(*) from TOYSTORE51.project ;

-- NUMBER_ROWS returns 20
select NUMBER_ROWS from QSYS2.SYSPARTITIONSTAT where
    TABLE_SCHEMA = 'TOYSTORE51' and TABLE_NAME = 'PROJECT';

-- DSPFD returns Current number of records . . . . . : 20
c1: dspfd toystore51/project ;
```

- **If Option 47 is not installed:**

- **Files containing RCAC will Restore**
- **Permissions and masks cannot be created or altered, but can be disabled**
- **Tables, views, or indexes cannot be accessed which contain active permissions or masks**



# Power Systems Social Media

## IBM Power Systems Official Channels:



<https://facebook.com/IBMPowerSystems>



<https://twitter.com/IBMPowerSystems>



<https://www.linkedin.com/company/ibm-power-systems>




<http://www.youtube.com/c/ibmpowersystems>



<https://www.ibm.com/blogs/systems/topics/servers/power-systems/>



# More to Follow:

Blogs	 Twitter	#Hashtags
<ul style="list-style-type: none"> <li>• <a href="#">IBM Systems Magazine You and i (Steve Will)</a></li> <li>• <a href="#">IBM Systems Magazine i-Can (Dawn May)</a></li> <li>• <a href="#">IBM Systems Magazine: iDevelop (Jon Paris and Susan Gantner)</a></li> <li>• <a href="#">IBM Systems Magazine: iTalk with Tuohy</a></li> <li>• <a href="#">IBM Systems Magazine: Open your i (Jesse Gorzinski)</a></li> <li>• <a href="#">IBM Db2 for i (Mike Cain)</a></li> <li>• <a href="#">IBM DB2 Web Query for i (Doug Mack)</a></li> </ul>	<p> <a href="#">@IBMSystems</a>  <a href="#">@COMMONug</a>  <a href="#">@IBMChampions</a>  <a href="#">@IBMSystemsISVs</a>  <a href="#">@LinuxIBMMag</a>  <a href="#">@OpenPOWERorg</a>  <a href="#">@AIXMag</a>  <a href="#">@IBMiMag</a>  <a href="#">@ITJungleNews</a>  <a href="#">@SAPonIBMi</a>  <a href="#">@SiDforIBMi</a>  <a href="#">@IBMAIXeSupp</a>  <a href="#">@IBMAIXdoc</a>    <a href="#">@Forstie IBMi</a> </p>	<p> <a href="#">#PowerSystems</a>  <a href="#">#IBMi</a>  <a href="#">#IBMAIX</a>  <a href="#">#POWER8</a>  <a href="#">#LinuxonPower</a>  <a href="#">#OpenPOWER</a>  <a href="#">#HANAonPower</a>  <a href="#">#ITinfrastructure</a>  <a href="#">#OpenSource</a>  <a href="#">#HybridCloud</a>  <a href="#">#BigData</a> </p>





# Special notices

This document was developed for IBM offerings in the United States as of the date of publication. IBM may not make these offerings available in other countries, and the information is subject to change without notice. Consult your local IBM business contact for information on the IBM offerings available in your area.

Information in this document concerning non-IBM products was obtained from the suppliers of these products or other public sources. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.

All statements regarding IBM future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.

The information contained in this document has not been submitted to any formal IBM test and is provided "AS IS" with no warranties or guarantees either expressed or implied.

All examples cited or described in this document are presented as illustrations of the manner in which some IBM products can be used and the results that may be achieved. Actual environmental costs and performance characteristics will vary depending on individual client configurations and conditions.

IBM Global Financing offerings are provided through IBM Credit Corporation in the United States and other IBM subsidiaries and divisions worldwide to qualified commercial and government clients. Rates are based on a client's credit rating, financing terms, offering type, equipment type and options, and may vary by country. Other restrictions may apply. Rates and offerings are subject to change, extension or withdrawal without notice.

IBM is not responsible for printing errors in this document that result in pricing or information inaccuracies.

All prices shown are IBM's United States suggested list prices and are subject to change without notice; reseller prices may vary.

IBM hardware products are manufactured from new parts, or new and serviceable used parts. Regardless, our warranty terms apply.

Any performance data contained in this document was determined in a controlled environment. Actual results may vary significantly and are dependent on many factors including system hardware configuration and software design and configuration. Some measurements quoted in this document may have been made on development-level systems. There is no guarantee these measurements will be the same on generally-available systems. Some measurements quoted in this document may have been estimated through extrapolation. Users of this document should verify the applicable data for their specific environment.



# Special notices (cont.)

IBM, the IBM logo, ibm.com AIX, AIX (logo), AIX 5L, AIX 6 (logo), AS/400, BladeCenter, Blue Gene, ClusterProven, DB2, ESCON, i5/OS, i5/OS (logo), IBM Business Partner (logo), IntelliStation, LoadLeveler, Lotus, Lotus Notes, Notes, Operating System/400, OS/400, PartnerLink, PartnerWorld, PowerPC, pSeries, Rational, RISC System/6000, RS/6000, THINK, Tivoli, Tivoli (logo), Tivoli Management Environment, WebSphere, xSeries, z/OS, zSeries, Active Memory, Balanced Warehouse, CacheFlow, Cool Blue, IBM Systems Director VMControl, pureScale, TurboCore, Chiphopper, Cloudscape, DB2 Universal Database, DS4000, DS6000, DS8000, EnergyScale, Enterprise Workload Manager, General Parallel File System, , GPFS, HACMP, HACMP/6000, HASM, IBM Systems Director Active Energy Manager, iSeries, Micro-Partitioning, POWER, PowerExecutive, PowerVM, PowerVM (logo), PowerHA, Power Architecture, Power Everywhere, Power Family, POWER Hypervisor, Power Systems, Power Systems (logo), Power Systems Software, Power Systems Software (logo), POWER2, POWER3, POWER4, POWER4+, POWER5+, POWER6, POWER6+, POWER7, System i, System p, System p5, System Storage, System z, TME 10, Workload Partitions Manager and X-Architecture are trademarks or registered trademarks of International Business Machines Corporation in the United States, 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 U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries.

A full list of U.S. trademarks owned by IBM may be found at: <http://www.ibm.com/legal/copytrade.shtml>.

Adobe, the Adobe logo, PostScript, and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Altivec is a trademark of Freescale Semiconductor, Inc.

AMD Opteron is a trademark of Advanced Micro Devices, Inc.

InfiniBand, InfiniBand Trade Association and the InfiniBand design marks are trademarks and/or service marks of the InfiniBand Trade Association.

Intel, Intel logo, Intel Inside, Intel Inside logo, Intel Centrino, Intel Centrino logo, Celeron, Intel Xeon, Intel SpeedStep, Itanium, and Pentium are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

Java and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

Linux is a registered trademark of Linus Torvalds in the United States, other countries or both.

Microsoft, Windows and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries or both.

NetBench is a registered trademark of Ziff Davis Media in the United States, other countries or both.

SPECint, SPECfp, SPECjbb, SPECweb, SPECjAppServer, SPEC OMP, SPECviewperf, SPECcapc, SPECchpc, SPECjvm, SPECmail, SPECimap and SPECsfs are trademarks of the Standard Performance Evaluation Corp (SPEC).

The Power Architecture and Power.org wordmarks and the Power and Power.org logos and related marks are trademarks and service marks licensed by Power.org.

TPC-C and TPC-H are trademarks of the Transaction Performance Processing Council (TPPC).

UNIX is a registered trademark of The Open Group in the United States, other countries or both.

Other company, product and service names may be trademarks or service marks of others.