Db2 for i – Row & Column Access Control

Scott Forstie – forstie@us.ibm.com
@Forstie_IBMi
Db2 for i Business Architect

© 2016, 2017 IBM Corporation
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

<table>
<thead>
<tr>
<th>Use case</th>
<th>Field Procedures</th>
<th>Column Masks</th>
<th>Row Permissions</th>
<th>Views &amp; Logical Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM i releases</td>
<td>7.1, 7.2, 7.3</td>
<td>7.2, 7.3</td>
<td>7.2, 7.3</td>
<td>All</td>
</tr>
<tr>
<td>Limit access to some/all data within a column</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Limit access to rows</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Security logic payload</td>
<td>External program (complex)</td>
<td>SQL rule (simple)</td>
<td>SQL rule (simple)</td>
<td>DDS or SQL (varies)</td>
</tr>
<tr>
<td>(customer experience)</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software Vendor component</td>
<td>Townsend Security • Linoma • Enforcive • IBM i Lab Services</td>
<td>SkyView Risk Assessor for IBM i • IBM i Lab Services</td>
<td>SkyView Risk Assessor for IBM i • IBM i Lab Services</td>
<td>N/A</td>
</tr>
<tr>
<td>Data encrypted at rest</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Data encrypted in journal</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Masked values apply to selection criteria</td>
<td>Yes</td>
<td>No</td>
<td>N/A</td>
<td>N/A</td>
</tr>
<tr>
<td>Data-Centric Solution</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>
## Contrasting Db2 for i Governance

<table>
<thead>
<tr>
<th>Use case</th>
<th>SQL Activity</th>
<th>Audit Journal</th>
<th>Data Journal</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM i releases</td>
<td>All</td>
<td>All</td>
<td>All</td>
</tr>
<tr>
<td>Analysis &amp; Reporting</td>
<td>• IBM Security Guardium</td>
<td>• IBM Security Guardium</td>
<td>• InfoSphere Guardium DAM</td>
</tr>
<tr>
<td></td>
<td>• PowerSC Tools for IBM i</td>
<td>• PowerSC Tools for IBM i</td>
<td>• PowerSC Tools for IBM i</td>
</tr>
<tr>
<td></td>
<td>• Security ISVs</td>
<td>• Security ISVs</td>
<td>• Security ISVs</td>
</tr>
<tr>
<td>Solution infrastructure beyond IBM i</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Capture SQL statements</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Capture SQL host variable values and environment</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Capture database specific Audit Journal details</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Capture before and after images of data</td>
<td>No</td>
<td>No</td>
<td>Yes</td>
</tr>
<tr>
<td>Able to track which rows are seen by users</td>
<td>No</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>
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 an 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
- qsrut - list authorized users
- qsysrui - 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?

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

<table>
<thead>
<tr>
<th><strong>Base Table</strong></th>
<th>The table (physical file) containing business critical data.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Dependent Object</strong></td>
<td>Any object (file, schema, function, or other object) the permission or mask references.</td>
</tr>
<tr>
<td><strong>Permission</strong></td>
<td>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. <strong>0 to many ➔ permissions allowed per table</strong></td>
</tr>
<tr>
<td><strong>Mask</strong></td>
<td>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. <strong>0 or 1 ➔ masks allowed per column</strong></td>
</tr>
<tr>
<td><strong>RULETEXT</strong></td>
<td>The expression to be used by the permission (WHERE clause predicates) or mask (selection CASE expression)</td>
</tr>
</tbody>
</table>
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;
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 USERPROFILE_NAME = USER));

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

ALTER TABLE EMPLOYEE ACTIVATE ROW ACCESS CONTROL;

SELECT LASTNAME, EMPNO, WORKDEPT, SSN
FROM EMPLOYEE
ORDER BY 1;
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
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 *LBL that is defined over EMPLOYEE in BURNXMP5.
  3 -- User-defined function RETURN_NAME_FUNCTION in *LBL, which is not secure.
Alter statement enhancements

**ALTER TRIGGER**

Only the QIBM_DB_SECADM user can mark a trigger or function as SECURED.

**ALTER FUNCTION**

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)

  ![DSPOBJAUT Command Example](image)

- **Use Access Client Solutions (ACS)**

  ![Access Client Solutions Example](image)
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

<table>
<thead>
<tr>
<th>SQLCODE</th>
<th>SQLSTATE</th>
<th>Operation</th>
<th>Row and Column Access Control</th>
<th>Statement Text</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>00000</td>
<td>OPEN</td>
<td>Row access control</td>
<td>select * from toystore.sales</td>
</tr>
</tbody>
</table>
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

Information About the Plan Perf...

<table>
<thead>
<tr>
<th>Information About the Plan Perf...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scrollable</td>
</tr>
<tr>
<td>Plan Name</td>
</tr>
<tr>
<td>Plan Step Type</td>
</tr>
<tr>
<td>Plan Step Name</td>
</tr>
<tr>
<td>Statement Text</td>
</tr>
</tbody>
</table>
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
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
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 mcain@us.ibm.com
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 BURNMPS. 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 BURNMPS. 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!
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?

```sql
-- 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:
  o Files containing RCAC will Restore
  o Permissions and masks cannot be created or altered, but can be disabled
  o 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:

<table>
<thead>
<tr>
<th>Blogs</th>
<th>Twitter</th>
<th>#Hashtags</th>
</tr>
</thead>
<tbody>
<tr>
<td>IBM Systems Magazine You and i (Steve Will)</td>
<td>@IBMSystems @COMMONug @IBMChampions @IBMSystemsISVs @LinuxIBMMag @OpenPOWERorg @AIXMag @IBMiMag @ITJungleNews @SAPonIBM @SiDforIBM @IBMAIXeSupp @IBMAIXdoc @Forstie_IBMi</td>
<td>#PowerSystems #IBMi #IBMAIX #POWER8 #LinuxonPower #OpenPOWER #HANAonPower #ITinfrastructure #OpenSource #HybridCloud #BigData</td>
</tr>
<tr>
<td>IBM Systems Magazine i-Can (Dawn May)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Systems Magazine: iDevelop (Jon Paris and Susan Gantner)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Systems Magazine: iTalk with Tuohy</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Systems Magazine: Open your i (Jesse Gorzinski)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM Db2 for i (Mike Cain)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IBM DB2 Web Query for i (Doug Mack)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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 inquiries, 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, Chipshopper, 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, 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, SPECapc, 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.