Db2 Security Update

Karen Wilkins MBCS
IBM UK Ltd

November 2018
Session IM




Agenda

- Transfer Ownership
- Support install or migrate Db2 without requiring SYSADM authority
- New UNLOAD privilege
- RACF Exit updates
- Pervasive Encryption

Separation of Duties

- Db2 V10
  - Introduced the system database administrator and the security administrator authorities
  - Separated security administration from system administration
- Db2 V12
  - Transfer Ownership
  - Allows a system administrator to install or migrate a subsystem without requiring access to user data
  - New UNLOAD privilege to separate SQL and utility access

Transfer Ownership

- Object ownership privileges are implicit and cannot be revoked

- DROP and CREATE
  - Availability
- CATMAINT UPDATE FROM OWNER(…) TO ROLE
  - Includes all objects
- TRANSFER OWNERSHIP
  - Allows to transfer the ownership of system and database objects to an authorization-ID or a role

Transfer Ownership - Options

- New SQL statement TRANSFER OWNERSHIP applies to
  - Database objects
    - Database, Table space, Table, View, Index, Alias – Base table or view ownership is transferred
  - System object
    - Stogroup
  - No application objects (e.g. RE-BIND for plan/packages, others must be re-created)
  - No security objects (DROP, CREATE)
  - No change to the schema of the transferred object

Transfer Ownership - Syntax

```
>>-TRANSFER OWNERSHIP OF--| object |--TO--| new-owner |---------->
>------REVOKE PRIVILEGES-------------------------------------------><
object:
|--+-DATABASE-database-name-----------------------------------+--|
   +-INDEX--index-name-----------------------------------------+
   +-STOGROUP-stogroup-name-------------------------------------+
   +-TABLE--table-name-----------------------------------------+
   +-TABLESPACE-+-----------------+--tablespace-name----------+
   |            '-database-name.-'                             |
   '-VIEW--view-name-------------------------------------------'
new-owner:
|--+-ROLE--role-name----------+-------------------------------|
   +-USER--authorization-name-+
   '-SESSION_USER-------------'
```

Transfer Ownership - Example

ADMF002:

```
          CREATE TABLE SZI10T
          ...
```

SYSIBM.SYSTABLES

CREATOR	NAME	CREATEDBY	OWNER
ADMF002	SZI10T	ADMF002	ADMF002

SYSIBM.SYSTABAUTH

GRANTOR	GRANTEE	TCREATOR	TTNAME
ADMF002	ADMF002	ADMF002	SZI10T

SECADM:

```
          TRANSFER OWNERSHIP OF TABLE ADMF002.SZI10T TO USER ADMF003
          REVOKE PRIVILEGES
```

SYSIBM.SYSTABLES

CREATOR	NAME	CREATEDBY	OWNER
ADMF002	SZI10T	ADMF002	ADMF003

SYSIBM.SYSTABAUTH

GRANTOR	GRANTEE	TCREATOR	TTNAME
ADMF003	ADMF003	ADMF002	SZI10T

Transfer Ownership - Example

ADMF002:

```
CREATE ALIAS PETER FOR TABLE SZI10T
...
```

SYSIBM.SYSTABLES

CREATOR	NAME	CREATEDBY	OWNER
ADMF002	PETER	ADMF002	ADMF002
ADMF002	SZI10T	ADMF002	ADMF002

SYSIBM.SYSTABAUTH

GRANTOR	GRANTEE	TCREATOR	TTNAME
ADMF002	ADMF002	ADMF002	SZI10T

SECADM:

```
TRANSFER OWNERSHIP OF TABLE ADMF002.PETER TO USER ADMF003
REVOKE PRIVILEGES
```

SYSIBM.SYSTABLES

CREATOR	NAME	CREATEDBY	OWNER
ADMF002	PETER	ADMF002	ADMF002
ADMF002	SZI10T	ADMF002	ADMF003

SYSIBM.SYSTABAUTH

GRANTOR	GRANTEE	TCREATOR	TTNAME
ADMF003	ADMF003	ADMF002	SZI10T

Transfer Ownership - Rules

- Authorization
  - Ownership or SECADM authority
  - Install SYSADM or SYSADM authority is not sufficient
    - SEPARATE_SECURITY ZPARM does not impact the SECADM authority
- Does not apply to catalog/directory objects
  - SQLCODE -618 or -607
- Ownership transfer of a table also includes dependent objects, like
  - Indexes (if the same owner)
  - Implicitly created table space for this base table
  - Implicitly and explicitly (same owner) created LOB objects (aux table, aux index, LOB table space)
  - XML objects (table, index, table space)
- Ownership of implicit created objects can not be explicitly transferred
- New owner needs privileges on dependent objects
  - Consider especially views

Transfer Ownership - Rules

- Ownership of implicit created objects cannot be explicitly transferred

```
 TRANSFER OWNERSHIP OF TABLE ADMF002.XSZI10T TO USER ADMF003
 REVOKE   PRIVILEGES ;


SQLERROR ON   TRANSFER  COMMAND, EXECUTE   FUNCTION
 RESULT OF SQL STATEMENT:
 DSNT408I SQLCODE = -20355, ERROR:  THE STATEMENT COULD NOT BE PROCESSED BECAUSE ONE OR
MORE   IMPLICITLY CREATED OBJECTS ARE INVOLVED. REASON: 6
```

reason code

- New owner needs privileges on dependent objects
  - Consider views especially

```
 CREATE VIEW ADMF002.SZI10V AS SELECT * FROM ADMF002.SZI10T
 TRANSFER OWNERSHIP OF VIEW  ADMF002.SZI10V     TO USER ADMF003
 REVOKE   PRIVILEGES ;

SQLERROR ON   TRANSFER  COMMAND, EXECUTE   FUNCTION
 RESULT OF SQL STATEMENT:
 DSNT408I SQLCODE = -20342, ERROR:  AUTHORIZATION ID ADMF003 DOES NOT HAVE THE
REQUIRED   PRIVILEGE SELECT ON OBJECT ADMF002.SZI10T OF TYPE TABLE FOR OWNERSHIP TRANSFER.
```

Transfer Ownership - Rules

- REVOKE PRIVILEGES clause (required) ensures that
  - the current owner will not have any implicit privileges after the transfer
  - the authorization cache entries for the current owner are purged
  - for dependent packages, current owner is required to have object privilege by other means or rebind the package to change the owner before ownership transfer
    - No package invalidation

- No change to the grants made by the previous owner
  - Could be revoked using REVOKE ... BY... clause

Transfer Ownership - Example

ADMF002:

```
CREATE TABLE SZI10T
...
```

SYSIBM.SYSTABLES

CREATOR	NAME	CREATEDBY	OWNER
ADMF002	SZI10T	ADMF002	ADMF002

SYSIBM.SYSTABAUTH

GRANTOR	GRANTEE	TCREATOR	TTNAME
ADMF002	ADMF002	ADMF002	SZI10T

ADMF002:

```
BIND PACKAGE MEMBER(#GTRF006)... (with reference to TABLE SZI10T)
```

SYSIBM.SYSTABAUTH

GRANTOR	GRANTEE	GRANTEETYPE	TCREATOR	TTNAME
ADMF002	ADMF002		ADMF002	SZI10T
ADMF002	#GTRF006	P	ADMF002	SZI10T

SECADM:

```
TRANSFER OWNERSHIP OF TABLE ADMF002.SZI10T TO USER ADMF003
REVOKE PRIVILEGES
...

SQLERROR ON   TRANSFER  COMMAND, EXECUTE   FUNCTION
 RESULT OF SQL STATEMENT:
 DSNT408I SQLCODE = -20342, ERROR:  AUTHORIZATION ID ADMF003 DOES NOT HAVE THE REQUIRED
          PRIVILEGE SELECT ON OBJECT ADMF002.SZI10T OF TYPE TABLE FOR OWNERSHIP TRANSFER.
```

Support Installation or Migration

Without requiring SYSADM

- Install or migrate Db2 subsystem using installation SYSOPR authority
  - Requires current SQLID to be set to SYSINSTL
    - Objects created will be owned by SYSINSTL
  - Requires BIND owner with privilege to bind and execute SQL in the package
  - SYSINSTL may need to be defined in RACF (or other system security product) to execute stored procedures defined with SECURITY USER

- Does not have access to non-system objects

Support Installation or Migration

Without requiring SYSADM

- Installation SYSOPR enhancements
  - Execute the CATMAINT utility to install or migrate to a new release
  - Issue the –ACTIVATE NEW FUNCTION command
  - Set current SQLID to SYSINSTL regardless of SEPARATE SECURITY zparm setting
  - Access to all catalog tables and all tables in the system databases
  - BINDAGENT privilege to specify any owner

- System defined routines
  - CREATE / ALTER PROCEDURE / FUNCTION issued by installation SYSADM or installation SYSOPR user when current SQLID = ‘SYSINSTL’
  - System DBADM, SQLADM, install SYSOPR authorities
  - Implicit execute privilege on the routines and the routine packages

Support Installation or Migration

Without requiring SYSADM

- Installation SYSOPR enhancements when current SQLID is set to ‘SYSINSTL’
  - Issue SQL CREATE, ALTER, DROP statements to manage most objects in the Db2 subsystem
    - Exception: Security objects
    - Additional privileges required to create object such as views, functions, triggers
    - Can create procedure and function in schema, SYSTOOLS and SYSFUN
  - Issue SQL GRANT statement to grant privileges on system objects and resources
    - All database, table space, table privileges on objects in system databases
    - USE privilege on Bufferpool and Stogroup
    - All privileges on plans that begin with ‘DSN’
    - All privileges on packages where the collection-ID and package-name begin with ‘DSN’
    - Execute privilege on system-defined routines

New UNLOAD Privilege

- New UNLOAD privilege checked, by default, with new function activation for UNLOAD utility access
- AUTH_COMPATIBILITY ZPARM can be set to SELECT_FOR_UNLOAD to retain SELECT privilege check
- IFCID 404 can be activated to audit SELECT privilege users for UNLOAD
  - V11 IFCID 404 retrofit APAR is PI55706
- SQL GRANT (table or view privileges) statement
  - New UNLOAD keyword added
  - Available before activate new function
- SQL REVOKE (table or view privileges) statement
  - New UNLOAD keyword added
- SYSIBM.SYSTABAUTH
  - New UNLOADAUTH column added

```
GRANT UNLOAD ON DSN8C10.EMP TO SALLY;
REVOKE UNLOAD ON DSN8C10.EMP FROM SALLY;
```

RACF Exit Updates

- RACF Access control Module (DSNXRXAC) has been enhanced to
  - Support new UNLOAD privilege

Db2 Privilege	Resource	Class
UNLOAD	<subsystem>.table-qualifier.table-name.UNLOAD	MDSNTB

  - For UPDATE and REFERENCES on tables
    - Table-qualifiers and table-names each truncated at 100 characters
    - Column-name truncated at 30 characters

Db2 Support of z/OS Dataset Encryption

- Db2 can now transparently encrypt data at rest without database downtime or requiring the administrator to redefine objects which could cause disruption to operations. No application changes required.
  - Encrypt active and archive log datasets
  - Encrypt catalog and directory table spaces
  - Encrypt user table spaces
- Utilises new z/OS DFSMS data set encryption support delivered in z/OS 2.3 and z/OS 2.2
- Db2 12 adds additional controls to set up encryption policies using Db2 interfaces

DFHSM Dataset Encryption - Overview

- DFSMS encrypts/decrypts records when written to or read from disk

- DFSMS managed datasets that support encryption of data at rest:
  - BSAM/QSAM
    - Sequential – Extended format only
  - VSAM and VSAM/RLS
    - KSDS, LDS, ESDS, RRDS, VRRDS – Extended format only

- Encryption type – AES 256 bit key (XTS, protected key)

- Key Label – a 64-byte label of the key in the ICSF CKDS that is used for the encryption/decryption of the dataset

Understanding DFSMS Policy-Based Dataset Encryption

- Datasets are defined as encrypted by specifying a key label during the creation of a new dataset:
  - SAF dataset profile
  - JCL, Dynamic Allocation, TSO Allocate, IDCAMS DEFINE
  - SMS DATACLAS

- During dataset open, DFSMS:
  - Checks the user access to the key label
  - Specifies the key label to ICSF to retrieve the secure / protected key from the CKDS

- ICSF:
  - Locates the secure key in the CKDS using the key label specified by DFSMS
  - Calls the adapter to unwrap the key value from the Master key
  - Rewraps the key value under a CPACF wrapping key to make it a protected key
  - Protected key stored in ICSF cache

DFHSM Dataset Encryption - Overview

- Application Transparency
  - Data remains encrypted during backup/recovery , migration/recall
  - In memory system or application buffers remain in the clear
  - Access to the key label is controlled through SAF permissions, in addition to traditional dataset permissions
- Segregation of Duties
  - Storage Administrators need access to the dataset but not access to the key label

Steps to Enable Encryption

1

ICSF Admin

Generates an encryption key and key label. Stores it in the ICSF CKDS

2

Security Admin

Sets up RACF for use of key label

Allows secure key to be used as protected key via ICSF segment
- SYMCPACFWRAP
- SYMCPACFRET

- AND -

Permits Db2 use of key label

In RACF, permit access to new resource in FACILITY class

3

Security / Database / Storage Admin

Associate the key label with the desired dataset

In RACF, alter DFP segment in dataset profile – DATAKEY()

- OR -

(V12 only) In Db2, set key label for system objects and user objects

- OR -

In DFSMS, assign to data class

4

Database Admin

Migrate to encrypted data

Non-disruptive ONLINE REORG

Steps to Enable Encryption

System Set Up - ICSF

- Key Labels defined in CKDS associated with secure AES256 keys
  - CKDS (key material) must be accessible across systems in the sysplex and replicated to sites that will access the encrypted datasets

ICSF Admin

Generates an encryption key and key label. Stores it in the ICSF CKDS

- Create the key labels and data keys
  - ICSF services
    - CSNBKGN – generate an AES 256-bit data key
    - CSNBKRC2 – create a key label in the CKDS with associated data key
  - ICSF key generator utility program (KGUP)

REXX example to create keys:
https://www.ibm.com/developerworks/community/blogs/79c1eec4-00c4-48ef-ae2b-01bd8448dd6c/entry/Rexx_Sample_Secure_Key_Generate_256_Bit_AES_DATA_Key?lang=en

Steps to Enable Encryption

System Set Up - RACF

- Enable system to create encrypted datasets when specifying key label outside of the RACF dataset profile
  - User must have at least READ authority to a new resource in the FACILITY class: STGADMIN.SMS.ALLOW.DATASET.ENCRYPT

- Set up CSFKEYS to enable the use of ICSF keys:
  - CSFKEYS general resource class
  - Example

```
RDEFINE CSFKEYS key-label UACC(NONE) –
   ICSF(SYMCPACFWRAP(YES) SYMCPACFRET(YES))
PERMIT key-label CLASS(CSFKEYS) ID(SYSDSP) ACCESS(READ)
PERMIT key-label CLASS(CSFKEYS) ID(JOHN)
WHEN(CRITERIA(SMS(DSENCRYPTION)))
```

Db2 Address Space ID

Security Admin

- Protect the resource CSFSERV class that ICSF uses to control access to the cryptographic services
  - Profile CSFKRR2 for protecting key labels

Encrypting Db2 System Objects

- The options to define a key label used by Db2 (Precedence Order)
  - Security Admin can set a key label in the DFP segment of RACF dataset profile using the new DATAKEY keyword
  - Database System Admin can set a new key label using ENCRYPTION_KEYLABEL system parameter (V12R1M502 only)
    - -SET SYSPARM command is required for the ZPARM value to take effect
    - Group Scope: Takes effect on all the members of a data sharing group immediately
    - Security related parameter: Requires installation SYSADM or SECADM authority to set the ZPARM
    - Db2 DBM1 and MSTR address space IDs must be permitted access to the key label
  - Storage Admin can set a key label using IDCAMS DEFINE for active logs
  - Storage Admin can set a key label in the DFSMS data class

3

Security / Database / Storage Admin

Associate the key label with the desired dataset

In RACF, alter DFP segment in dataset profile – DATAKEY()

- OR -

(V12 only) In Db2, set key label for system objects and user objects

- OR -

In DFSMS, assign to data class

Encrypting Db2 System Objects

- Active Logs
  - Encrypt new logs
    - Define active log dataset as encrypted and issue the SET LOG command NEWLOG option to add the newly defined active log dataset to the active log inventory without stopping Db2
  - Encrypt all active logs
    - Stop Db2. Copy the contents of the active log dataset to an encrypted dataset. Restart Db2.

- Archive Logs
  - New archive logs are automatically encrypted based on the key label setting

- Catalog and Directory table spaces
  - Execute REORG TABLESPACE utility to encrypt table spaces and index spaces in DSNDB06 and DSNDB01
  - Encrypt DSNDB01.SYSUTILX – execute REORG utility followed by REBUILD INDEXALL

Encrypting Db2 System Objects

- Display encryption key label using DFSMS interfaces, SMF records
- Once at V12R1M502
  - Run REPORT TABLESPACESET utility to display key label associated for each catalog and directory table spaces using the new SHOWKEYLABEL option
  - Issue –DISPLAY LOG command to obtain current key label information for current active log datasets
  - Issue –DISPLAY ARCHIVE command to obtain current key label information for archive log datasets that are in use

Encrypting User Objects

- The options to define a key label for user objects encryption (Precedence Order)
  - Security Admin can set a key label in the RACF dataset profile DFP segment using the new DATAKEY keyword
  - Application Database Admin can set a key label using SQL interfaces, CREATE / ALTER TABLE / STOGROUP (V12R1M502 only)
    - Enabled with APPLCOMPAT V12R1M502
  - Storage Admin can set a key label in the DFSMS data class

Security / Database / Storage Admin

Associate the key label with the desired dataset

In RACF, alter DFP segment in dataset profile – DATAKEY()

- OR -

(V12 only) In Db2, set key label for system objects and user objects

- OR -

In DFSMS, assign to data class

Encrypting User Objects with Db2 Controls

at V12R1M502

- SQL CREATE / ALTER STOGROUP – New KEY LABEL option
  - Adds a key label at the storage group level to encrypt all the table spaces using the storage group

- SQL CREATE / ALTER TABLE – New KEY LABEL option
  - Adds a key label at the table level to encrypt all the table spaces associated with the table
  - Includes explicitly or implicitly created base table space, auxiliary table spaces, XML table spaces, index spaces
  - Supported only for tables that reside in a universal table space or a partitioned table space

3

Security / Database / Storage Admin

Associate the key label with the desired dataset

In RACF, alter DFP segment in dataset profile – DATAKEY()

- OR -

(V12 only) In Db2, set key label for system objects and user objects

- OR -

In DFSMS, assign to data class

Encrypting User Objects

- Execute the REORG utility to encrypt existing table spaces
- New table spaces or partitions defined are encrypted using the key label based on the hierarchy
- Run REPORT TABLESPACESET utility to display key label for the table spaces used by each table using the new SHOWKEYLABEL option (V12R1M502 only)

4

Database Admin

Migrate to encrypted data

Non-disruptive ONLINE REORG

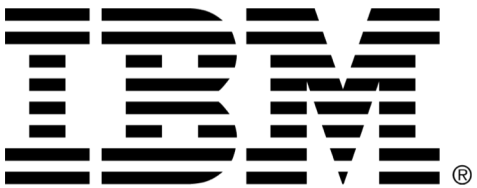
Db2 Dataset Encryption Considerations

- Compression
  - Db2 compression works seamlessly with dataset encryption
  - Compression is performed first

- Performance
  - Encryption cost for IBM Brokerage Online Transaction Workload in a 2-way data sharing environment
    - 2.3% ITR loss on z13
    - 0.4% ITR loss on z14
  - The elapsed time and Db2 CPU time are minimal for an upper bound random SELECT workload
    - Not noticeable in 4K, about 2% with 32K
    - CPU difference observed in DBM1 IIT time is not captured by Db2

Db2 v11 APAR **PI81900** PTF **UI51358**
Db2 v12 base APAR **PI81907** PTF **UI51499**

https://www.ibm.com/support/knowledgecenter/SSEPEK_11.0.0/seca/src/tpc/db2z_dfsmsencryptionsupport.html


IBM

Legal Disclaimer

- © IBM Corporation 2015. All Rights Reserved.
- The information contained in this publication is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this publication, it is provided AS IS without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this publication or any other materials. Nothing contained in this publication 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.
- 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. Product release dates and/or capabilities referenced in this presentation may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. Nothing 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.
- If the text contains performance statistics or references to benchmarks, insert the following language; otherwise delete:
  Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. The actual throughput or performance that any user will experience will vary depending upon many factors, including considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve results similar to those stated here.
- If the text includes any customer examples, please confirm we have prior written approval from such customer and insert the following language; otherwise delete:
  All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. Actual environmental costs and performance characteristics may vary by customer.
- Please review text for proper trademark attribution of IBM products. At first use, each product name must be the full name and include appropriate trademark symbols (e.g., IBM Lotus® Sametime® Unyte™). Subsequent references can drop "IBM" but should include the proper branding (e.g., Lotus Sametime Gateway, or WebSphere Application Server). Please refer to http://www.ibm.com/legal/copytrade.shtml for guidance on which trademarks require the ® or ™ symbol. Do not use abbreviations for IBM product names in your presentation. All product names must be used as adjectives rather than nouns. Please list all of the trademarks that you use in your presentation as follows; delete any not included in your presentation. IBM, the IBM logo, Lotus, Lotus Notes, Notes, Domino, Quickr, Sametime, WebSphere, UC2, PartnerWorld and Lotusphere are trademarks of International Business Machines Corporation in the United States, other countries, or both. Unyte is a trademark of WebDialogs, Inc., in the United States, other countries, or both.
- If you reference Adobe® in the text, please mark the first use and include the following; otherwise delete:
  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.
- If you reference Java™ in the text, please mark the first use and include the following; otherwise delete:
  Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.
- If you reference Microsoft® and/or Windows® in the text, please mark the first use and include the following, as applicable; otherwise delete:
  Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.
- If you reference Intel® and/or any of the following Intel products in the text, please mark the first use and include those that you use as follows; otherwise delete:
  Intel, Intel Centrino, 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.
- If you reference UNIX® in the text, please mark the first use and include the following; otherwise delete:
  UNIX is a registered trademark of The Open Group in the United States and other countries.
- If you reference Linux® in your presentation, please mark the first use and include the following; otherwise delete:
  Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both. Other company, product, or service names may be trademarks or service marks of others.
- If the text/graphics include screenshots, no actual IBM employee names may be used (even your own), if your screenshots include fictitious company names (e.g., Renovations, Zeta Bank, Acme) please update and insert the following; otherwise delete: All references to [insert fictitious company name] refer to a fictitious company and are used for illustration purposes only.

We want your feedback!

- Please submit your feedback online at ….
  - http://conferences.gse.org.uk/2018/feedback/IM
- Paper feedback forms are also available from the Chair person
- This session is IM