Db2 for z/OS and pervasive encryption

Mark Rader
IBM Washington Systems Center
Db2 for z/OS

Midwest Db2 User Groups
St. Louis, Wisconsin, Chicago
10-12 March, 2020

Please note

- IBM’s statements regarding its plans, directions, and intent are subject to change or withdrawal without notice and at IBM’s sole discretion.
- Information regarding potential future products is intended to outline our general product direction and it should not be relied on in making a purchasing decision.
- The information mentioned regarding potential future products is not a commitment, promise, or legal obligation to deliver any material, code or functionality. Information about potential future products may not be incorporated into any contract.
- The development, release, and timing of any future features or functionality described for our products remains at our sole discretion.
- 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.

Agenda

- Setting the stage: current Db2 for z/OS security environment
  - Remote access protection
  - Data access protection

- Pervasive encryption overview
  - Data encryption hierarchy
  - Z pervasive encryption
    - DFSMS role in data set encryption

- Db2 for z/OS encryption
  - Db2 11 and 12 support for data set encryption
  - Db2 12 for z/OS V12R1M502 encryption enhancements
  - Database encryption options in Db2 for z/OS

- Summary

Today's security challenges

Payment Card Industry Data Security Standard

PCI DSS COMPLIANT

$ 3.62M

Average cost of a data breach in 2017 [1]

GDPR

European Union General Data Protection Regulation

27.7%

Likelihood of an organization having a data breach over the next two years [2]

Health Insurance Portability and Accountability Act

HIPAA

1,2 Source: 2017 Ponemon Cost of Data Breach Study: Global Analysis -- http://www.ibm.com/security/data-breach/

Remote access protection

Network Layer

- IP Filtering
- IPSec
- Intrusion Detection Services
- AT-TLS

RACF

- Certificate Authentication (AT-TLS)
- Multi-factor Authentication
- Passphrase
- Passticket
- Kerberos
- DSNR Authorization
- SERVAUTH

Db2

- Trusted Connections
- System Profiling
- DSNLEUSR Stored Procedure

Data access protection

Separation of Duties

- Granular Authorities
- * Install and Migrate without SYSADM
- Trusted Contexts and Roles
- * Transfer Ownership

Privacy controls

- Row Permission
- Column Mask
- Row level encryption
  - ENCRYPT_TDES
  - IBM Guardium Encryption Tool for IMS™ and Db2 for z/OS
  - * ENCRYPT_DATAKEY BIF (V12R1M505)
- ***Data set Encryption***

Audit

- Audit policies
- Audit change data
  - Temporal
  - GENERATED ALWAYS AS clause

* Db2 12 for z/OS

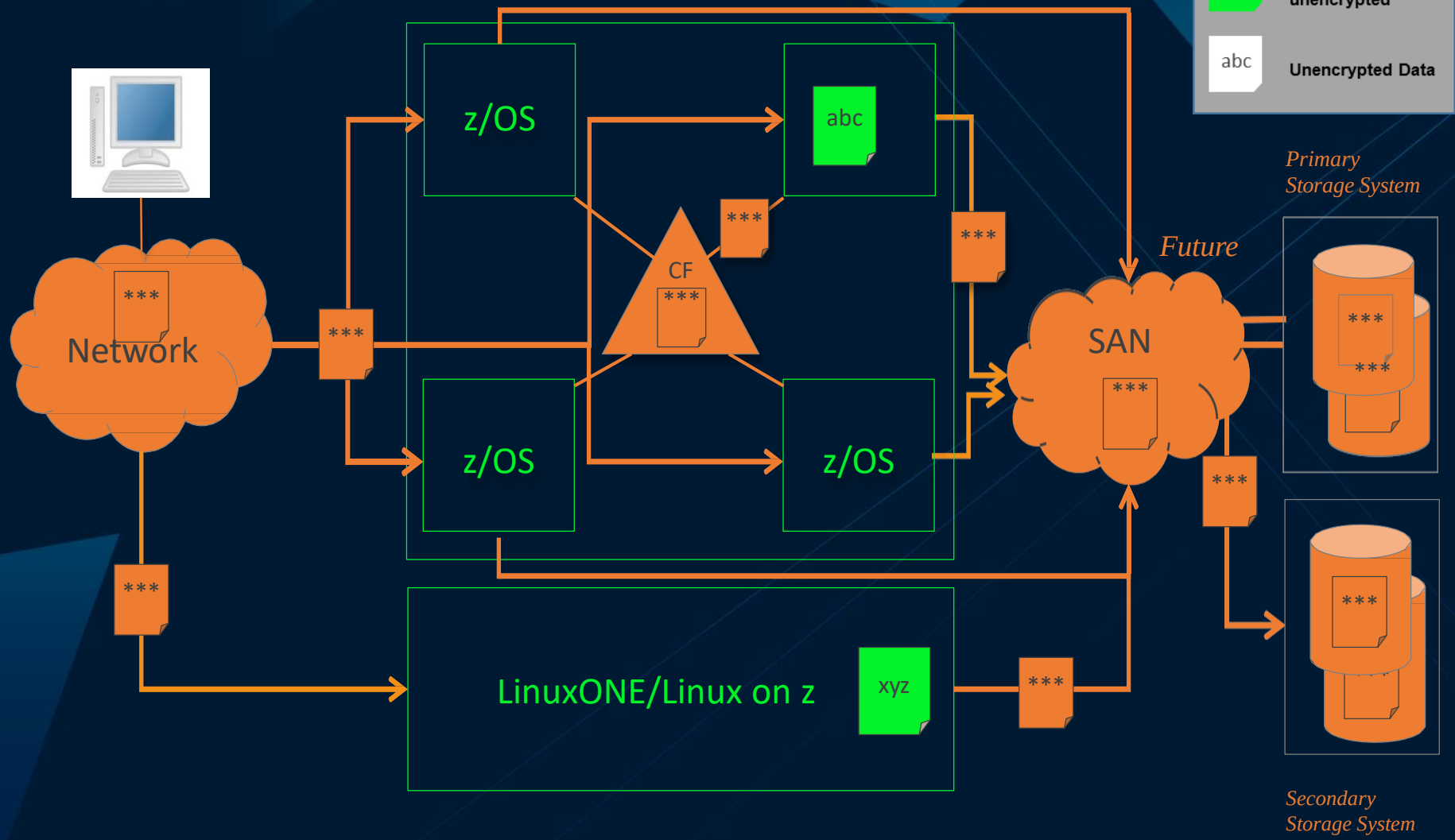
Pervasive encryption overview

Pervasive encryption with IBM Z – enabled through tight platform integration

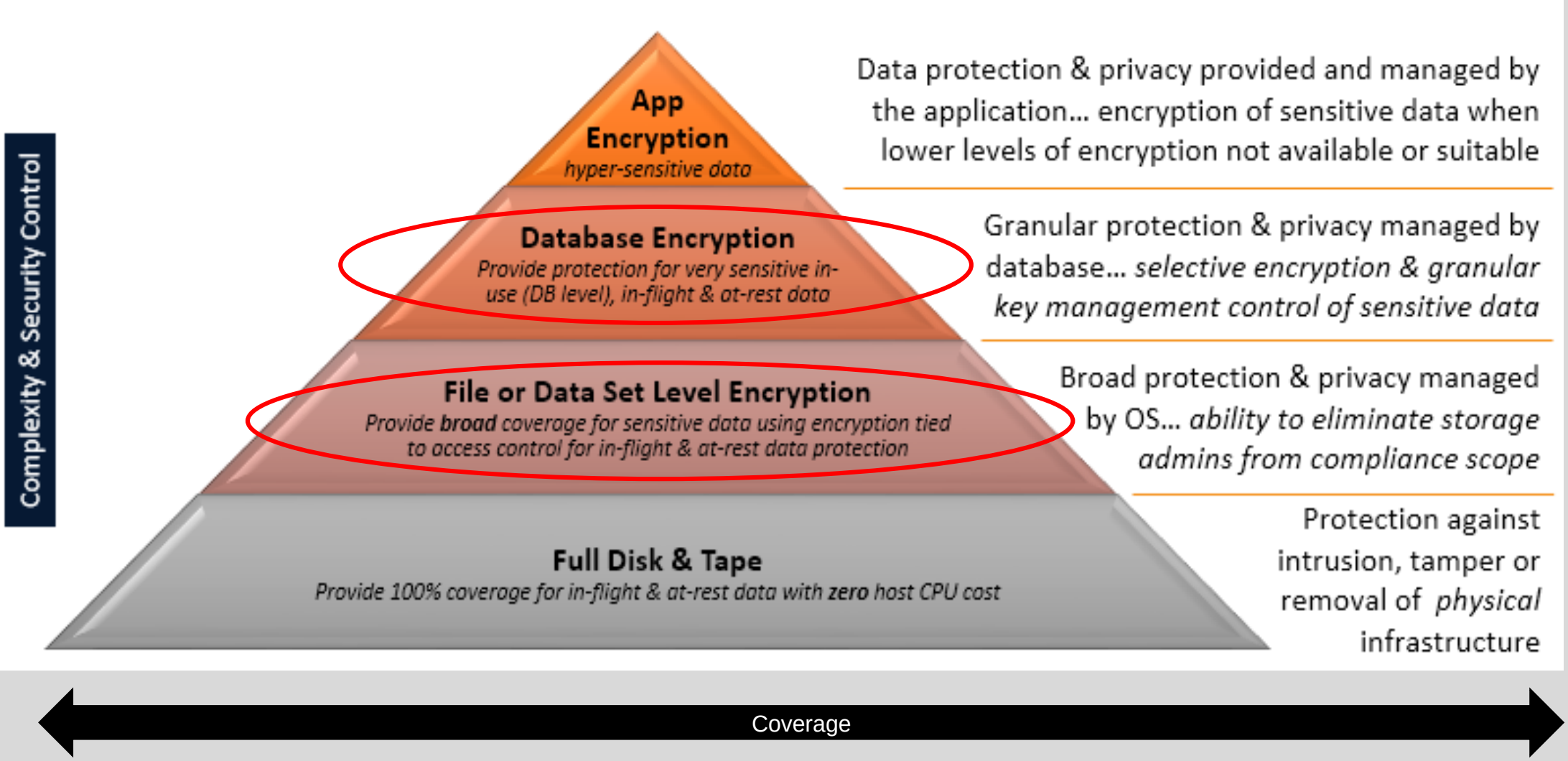
Integrated Crypto Hardware		Hardware accelerated encryption on every core, CPACF performance improvements of 7x Crypto Express6S – PCIe Hardware Security Module (HSM) & Cryptographic Coprocessor
Data at Rest		Broadly protect Linux file systems and z/OS data sets using policy controlled encryption that is transparent to applications and databases
Clustering		Protect z/OS Coupling Facility data end-to-end, using encryption that's transparent to applications
Network		Protect network traffic using standards based encryption from end to end, including encryption readiness technology to ensure that z/OS systems meet approved encryption criteria
Secure Service Container		Secure deployment of software appliances including tamper protection during installation and runtime, restricted administrator access, and encryption of data and code in-flight and at-rest
Key Management		The IBM Enterprise Key Management Foundation (EKMF) provides real-time, centralized secure management of keys and certificates with a variety of cryptographic devices and key stores

Data protection // encrypt everything

Protection of data at-rest and in-flight



Multiple layers of encryption of data



DFSMS dataset encryption - overview

- DFSMS encrypts/decrypts records when written to or read from disk
- DFSMS managed data sets 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 data set

Understanding DFSMS policy-based dataset encryption

- Data sets are defined as encrypted by specifying a key label during the creation of a new data set:
  - RACF data set profile
  - JCL, Dynamic Allocation, TSO Allocate, IDCAMS DEFINE
  - SMS DATACLAS
- During data set 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

DFSMS dataset encryption - overview

- Application transparency
  - Data remains encrypted during backup/recovery, migration/recall
  - In memory system or application data buffers remain in the clear
  - Access to the key label is controlled through SAF permissions, in addition to traditional data set permissions
- Segregation of duties
  - Storage administrators need access to the data set 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

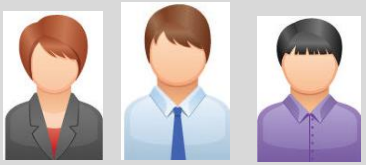
Allows secure key to be used as protected key via ICSF segment
- SYMCPACFWRAP
- SYMCPACFRET

– AND –

Permits Db2 use of the key label

In RACF, permit access to new resource in FACILITY class

3



Security / Database / Storage Admin

Associate the key label with the desired data set.

In RACF, alter DFP segment in data set profile - DATAKEY()

– OR –

IDCAMS DEFINE, TSO Allocate, etc.
(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

Online REORG

Non-disruptive

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 data sets

1

ICSF Admin

- 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

2

Security Admin

- Enable system to create encrypted data sets when specifying key label outside of the RACF data set 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

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

Db2 for z/OS encryption

Db2 support of z/OS data set encryption

- Db2 can 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
- Utilizes new z/OS DFSMS data set encryption support delivered in z/OS 2.3 and z/OS 2.2 (with OA50569 and OA53951)
  - Extended format only
- Db2 12 V12R1M502 adds additional controls to set up encryption policies using Db2 interfaces

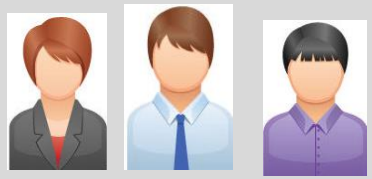
Encrypting Db2 system objects

3

- Options to define a key label used by Db2 (precedence order):
  - 1. Security Admin can set a key label in the DFP segment of RACF data set profile using the new DATAKEY keyword
  - 2. Database System Admin can set a 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

  OR

  - 2. Storage Admin can set a key label using IDCAMS DEFINE
    - Only option to encrypt active logs; ENCRYPTION_KEYLABEL will not apply
  - 3. Storage Admin can set a key label in the DFSMS data class



Security / Database System Admin / Storage Admin

In RACF, alter DFP segment in data set profile - DATAKEY()

– OR –

In Db2, set key label using system parameter
OR
IDCAMS DEFINE, etc.

– OR –

In DFSMS, assign to data class

Encrypting Db2 system objects

4

- Active logs
  - Encrypt new active logs
    - Define active log data set as encrypted and issue the SET LOG command NEWLOG option to add the newly defined active log data set to the active log inventory without stopping Db2
  - Encrypt all active logs
    - Stop Db2. Copy the contents of the active log data set to an encrypted data set. Restart Db2.
- Archive logs on disk
  - New archive logs 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 RECOVER utility followed by REBUILD INDEX ALL.

Database Admin

Online REORG

Can use ENCRYPTION_KEYLABEL system parameter

Encrypting Db2 system objects

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

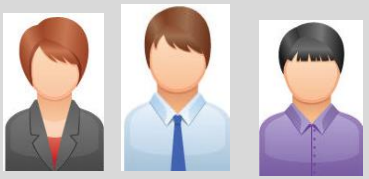
Encrypting user objects

- Options to define a key label for user objects encryption (precedence order):
  - 1. Security Admin can set a key label in the RACF data set profile DFP segment using the new DATAKEY keyword
  - 2. Storage Admin (or Database Admin) can set a key label via IDCAMS, TSO, etc...

OR

  - 2. Application Database Admin can set a key label using SQL interfaces: CREATE / ALTER with STOGROUP / TABLE (V12R1M502 only)
    - Enabled with APPLCOMPAT V12R1M502
  - 3. Storage Admin can set a key label in the DFSMS data class

3



Security / Database / Storage Admin

In RACF, alter DFP segment in data set profile - DATAKEY()

– OR –

IDCAMS DEFINE, etc.
OR
In Db2, set key label using SQL interfaces

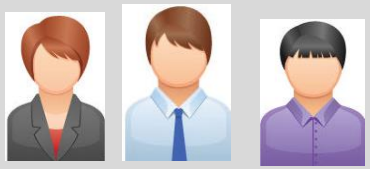
– OR –

In DFSMS, assign to data class

Encrypting user objects using 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
    - Only option for multi-table table spaces
- 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

In RACF, alter DFP segment in data set profile - DATAKEY()

– OR –

In Db2, set key label using SQL interfaces
OR
IDCAMS DEFINE, etc.

– OR –

In DFSMS, assign to data class

Encrypting user objects

- Execute the REORG utility to encrypt existing table spaces

4

- New table spaces or partitions defined are encrypted using the key label based on the hierarchy

Database Admin

- Run REPORT TABLESPACESET utility to display key label for the table spaces used by each table using the new SHOWKEYLABEL option (V12R1M502 only)

Online REORG to encrypt existing user objects

Utilities considerations

- All online utilities support table spaces and indexes whose underlying VSAM data sets are encrypted
- Input / Output data sets
  - Key label can also be specified using
    - JCL DSKEYLBL option
  - Authorization ID of the job requires access to the key label for any encrypted input or output data sets
- Stand alone utilities
  - Authorization ID of the job requires access to the key label for any encrypted data sets

Utilities considerations

- Db2 managed table spaces and index spaces
  - Utilities used to convert to encrypted data sets (except when REUSE option is specified)
    - REORG TABLESPACE or REORG INDEX
    - LOAD REPLACE
    - REBUILD INDEX
    - RECOVER from image copies – PIT or full recovery
  - PART or DSNUM option to encrypt / decrypt at the partition level
- User managed table spaces and index spaces
  - IDCAMS DELETE / DEFINE with the KEYLABEL option
  - Execute RECOVER and/or REBUILD INDEX utilities to restore the data
- FlashCopy image copies (FCIC), DFSMSdss concurrent image copies, shadow data sets
  - Allocated with the same key label as the table space or index

Db2 data set encryption considerations

— Compression

- Db2 compression works seamlessly with data set encryption
- Compression is performed first

— Performance

- There will be some CPU cost for encryption
- Internal benchmarks show significant savings on z14 vs. z13

Db2 V11 APAR **PI81900 (UI51358)**
Db2 V12 base APAR **PI81907 (UI51499)**

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

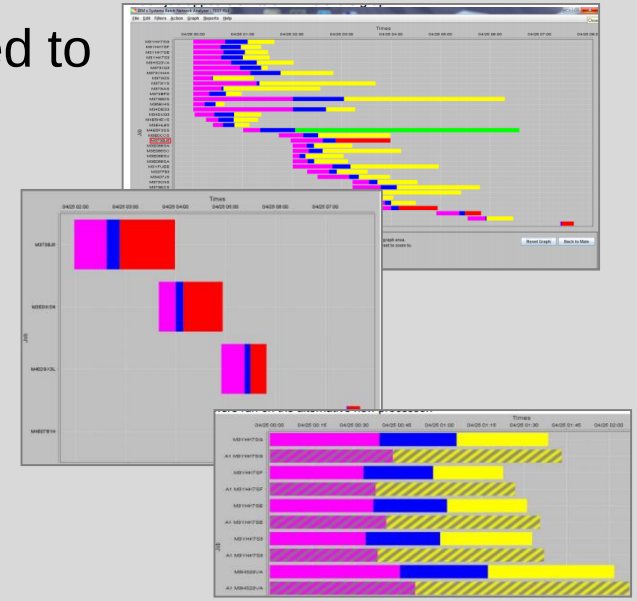
Db2 V12 V12R1M502 APAR **PI95511 (UI55093)**

https://www.ibm.com/support/knowledgecenter/en/SSEPEK_12.0.0/wnew/src/tpc/db2z_fl_v12r1m502.html#db2z_fl_v12r1m502__48635

z Systems Batch Network Analyzer (zBNA) Tool

Estimating Resources and Technology Options using z Batch Network Analyzer (zBNA)

- zBNA is a no charge, as-is PC-based analysis tool originally designed to analyze batch windows
- Uses SMF workload data and generates graphical and text based reports
- Previously enhanced for zEDC to identify & evaluate BSAM / QSAM compression candidates
- **Enhanced for Encryption**
  - To help clients estimate the CPU impact of enabling encryption
  - zBNA V1.8.1



Available on techdocs for customers, business partners, and IBMers
http://www.ibm.com/support/techdocs/atsmastr.nsf/WebIndex/PRS5132

Data set encryption summary

- For Db2 11 and Db2 12, a key label can be defined by the security administrator or storage administrator, a data base administrator can use Db2 REORG utility to seamlessly migrate Db2 data sets to encrypted data sets with no application outages
- For Db2 12, function level V12R1M502 provides new Db2 interfaces to configure and manage Db2 key labels
- Make sure all disaster recover user ids and sites have access to any key labels used to protect Db2 data sets and the key management system is fully deployed across the enterprise
- Recommendation: plan and implement enterprise security and encryption strategy

Database level

encryption options in Db2 for z/OS

Database encryption options

- Encryption at the column level
- Data remains encrypted in the Db2 buffer pool

	Old BIF since V8	UDFs	New BIF - FL505
Encrypt function	ENCRYPT_TDES	User-defined	ENCRYPT_DATAKEY
Integration	✓	Guardium (above)	✓
ICSF key infrastructure	appl. key-mgmt	✓	✓
Authorization on keylabel	No	✓	✓
Encryption algorithm	TDES	AES-256	AES-256
Encrypted data in BPool	✓	✓	✓

V12R1M505 – new encrypt/decrypt BIF

- ENCRYPT_DATAKEY (data string, keylabel, algorithm) allows
  - Column-based encryption of security-sensitive data
  - String and numeric datatypes are supported
    - Resulting datatype is VARBINARY for any non-LOB and BLOB for any LOB input value
    - Schema change required for cipher text column
  - Use of ICSF protected keys and RACF keylabel protection
    - Primary authid requires permit for keylabel defined in CSFKEYS class
  - AES256D|R – 256-bit AES CBC mode encryption algorithm
    - ‘D’ – fixed initialization vector to generate a cipher text
    - ‘R’ – random initialization vector to generate a cipher text

- DECRYPT_DATAKEY_BIGINT … _CHAR … _INTEGER …
  - Datatype dependent BIFs: DECRYPT_DATAKEY_xxxx (encrypted data)

Questions ?

Db2 for z/OS pervasive encryption summary

- Db2 encryption is part of IBM Z pervasive encryption
  - Tight platform integration
- Db2 11 for z/OS and Db2 12 for z/OS take advantage of DFSMS data set encryption
- Db2 12 for z/OS offers additional support for encryption
  - V12R1M502
    - System objects via system parameter (DSNZPARM) setting for key label
    - User objects via SQL (CREATE/ALTER) for TABLE or Db2 STOGROUP
    - Various display options
  - V12R1M505
    - Encrypt / decrypt built-in function

Thank you!

Notices and disclaimers

- © 2020 International Business Machines Corporation. No part of this document may be reproduced or transmitted in any form without written permission from IBM.
- **U.S. Government Users Restricted Rights — use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM.**
- Information in these presentations (including information relating to products that have not yet been announced by IBM) has been reviewed for accuracy as of the date of initial publication and could include unintentional technical or typographical errors. IBM shall have no responsibility to update this information. **This document is distributed "as is" without any warranty, either express or implied. In no event, shall IBM be liable for any damage arising from the use of this information, including but not limited to, loss of data, business interruption, loss of profit or loss of opportunity.** IBM products and services are warranted per the terms and conditions of the agreements under which they are provided.
- IBM products are manufactured from new parts or new and used parts.
  In some cases, a product may not be new and may have been previously installed. Regardless, our warranty terms apply."
- **Any statements regarding IBM's future direction, intent or product plans are subject to change or withdrawal without notice.**
- Performance data contained herein was generally obtained in a controlled, isolated environments. Customer examples are presented as illustrations of how those
- customers have used IBM products and the results they may have achieved. Actual performance, cost, savings or other results in other operating environments may vary.
- References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business.
- Workshops, sessions and associated materials may have been prepared by independent session speakers, and do not necessarily reflect the views of IBM. All materials and discussions are provided for informational purposes only, and are neither intended to, nor shall constitute legal or other guidance or advice to any individual participant or their specific situation.
- It is the customer's responsibility to insure its own compliance with legal requirements and to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the customer follows any law.

Notices and disclaimers continued

- Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products about this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. IBM does not warrant the quality of any third-party products, or the ability of any such third-party products to interoperate with IBM's products. **IBM expressly disclaims all warranties, expressed or implied, including but not limited to, the implied warranties of merchantability and fitness for a purpose.**
- The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents, copyrights, trademarks or other intellectual property right.
- IBM, the IBM logo, ibm.com and [names of other referenced IBM products and services used in the presentation] are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at: www.ibm.com/legal/copytrade.shtml