2015年5月8日

IBM DB2 Native Encryption
DB2 V10.5 FP5

2015 1Q QIT報告書

IBM アナリティクス事業部
TSDL. 統合システム技術センター
ISE. オープン・ミドルウェア

本資料掲載事項は、ある特定の環境・使用状況においての正確性がIBMによって確認されていますが、すべての環境において同様の結果が得られる保証はありません。これらの技術を自身の環境に適用する際には、自己の責任において十分な検証と確認を実施いただくことをお奨めいたします。

目次

第1部　DB2 Native Encryption概要

目次

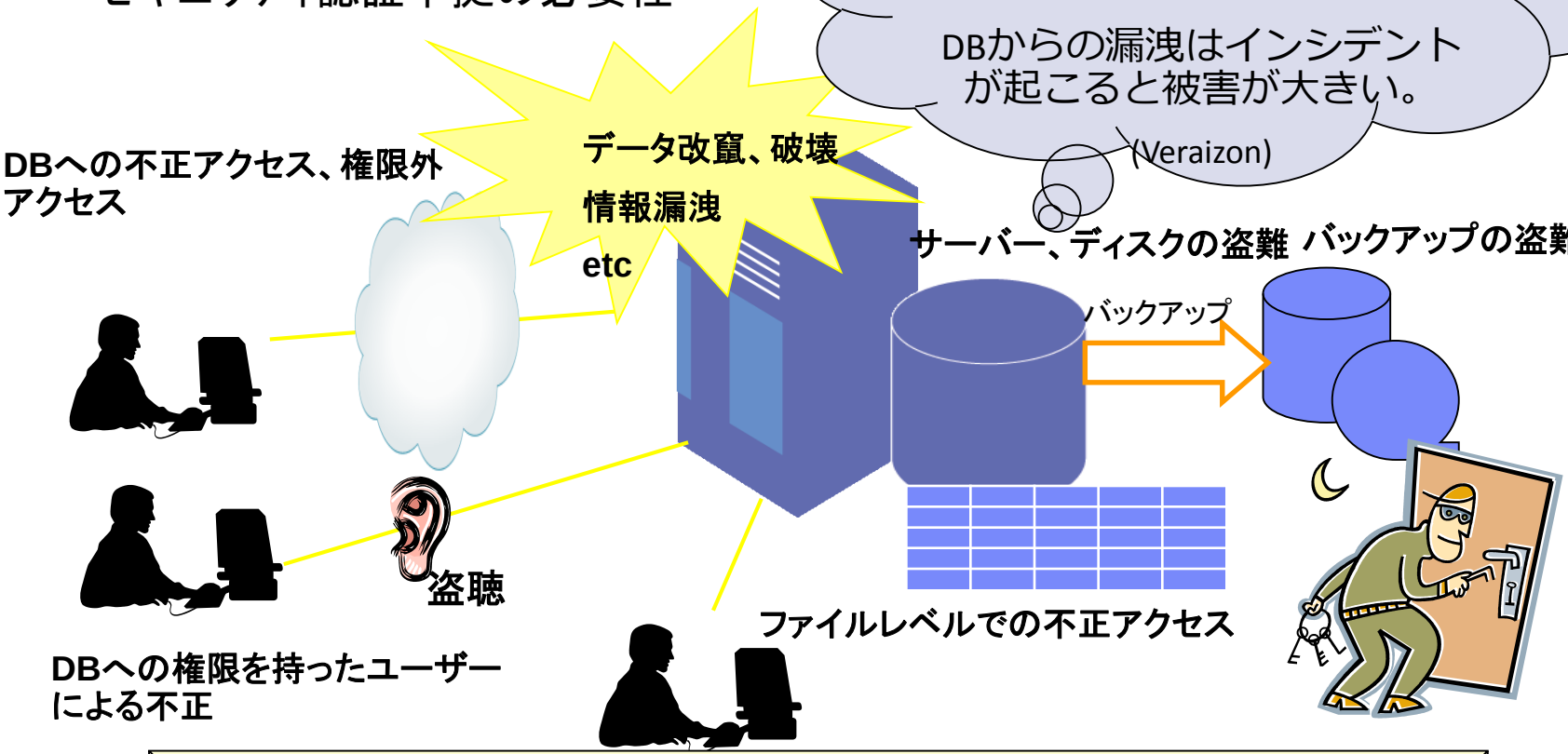
DBセキュリティ対策の必要性

- DBには価値の高い情報が集積
- 個人情報保護のための施策の義務付け
- セキュリティ認証準拠の必要性

データ漏洩セキュリティインシデントのうち、漏洩したレコード数では、全体の96%がDBから。

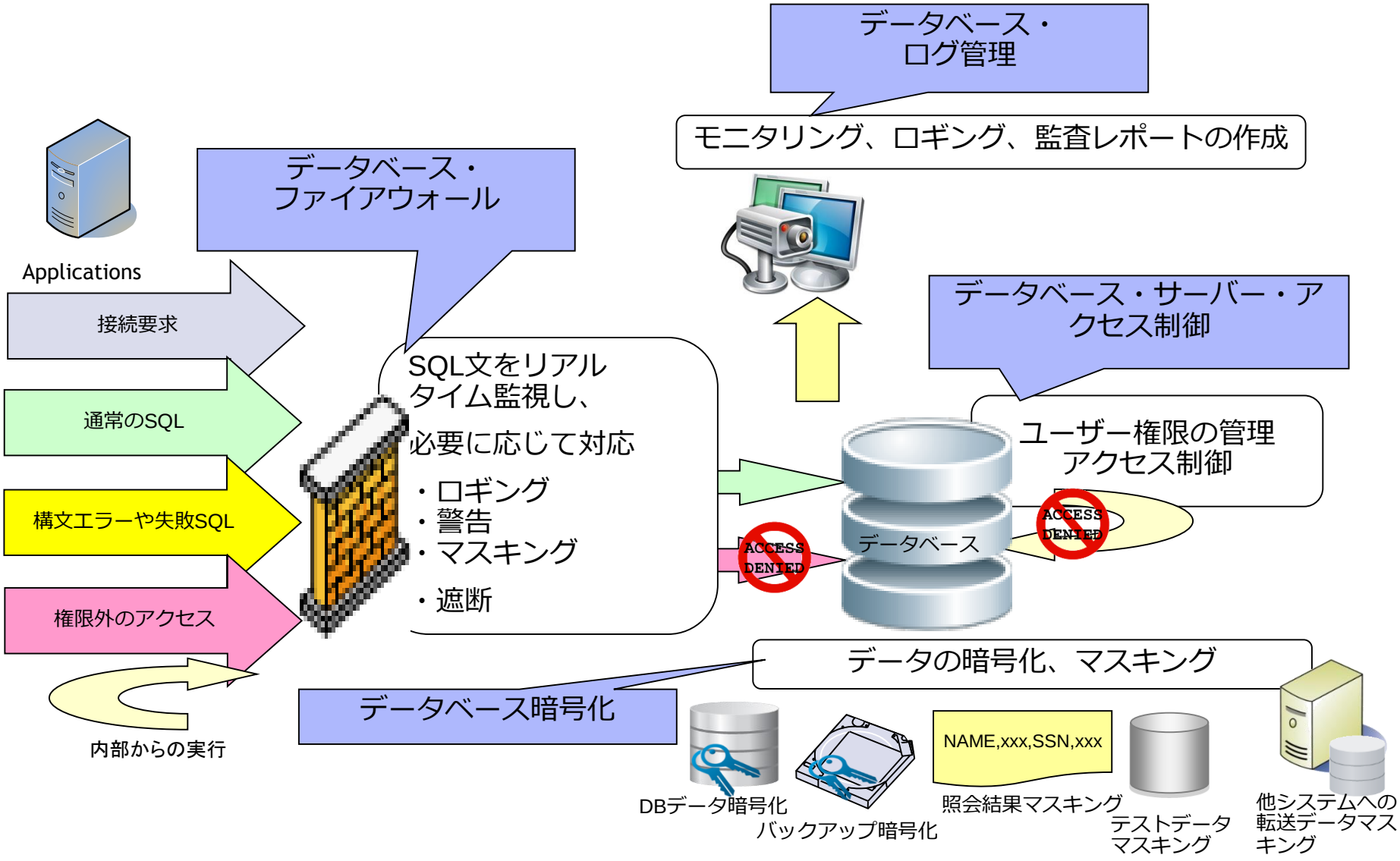
DBからの漏洩はインシデントが起こると被害が大きい。

(Veraizon)

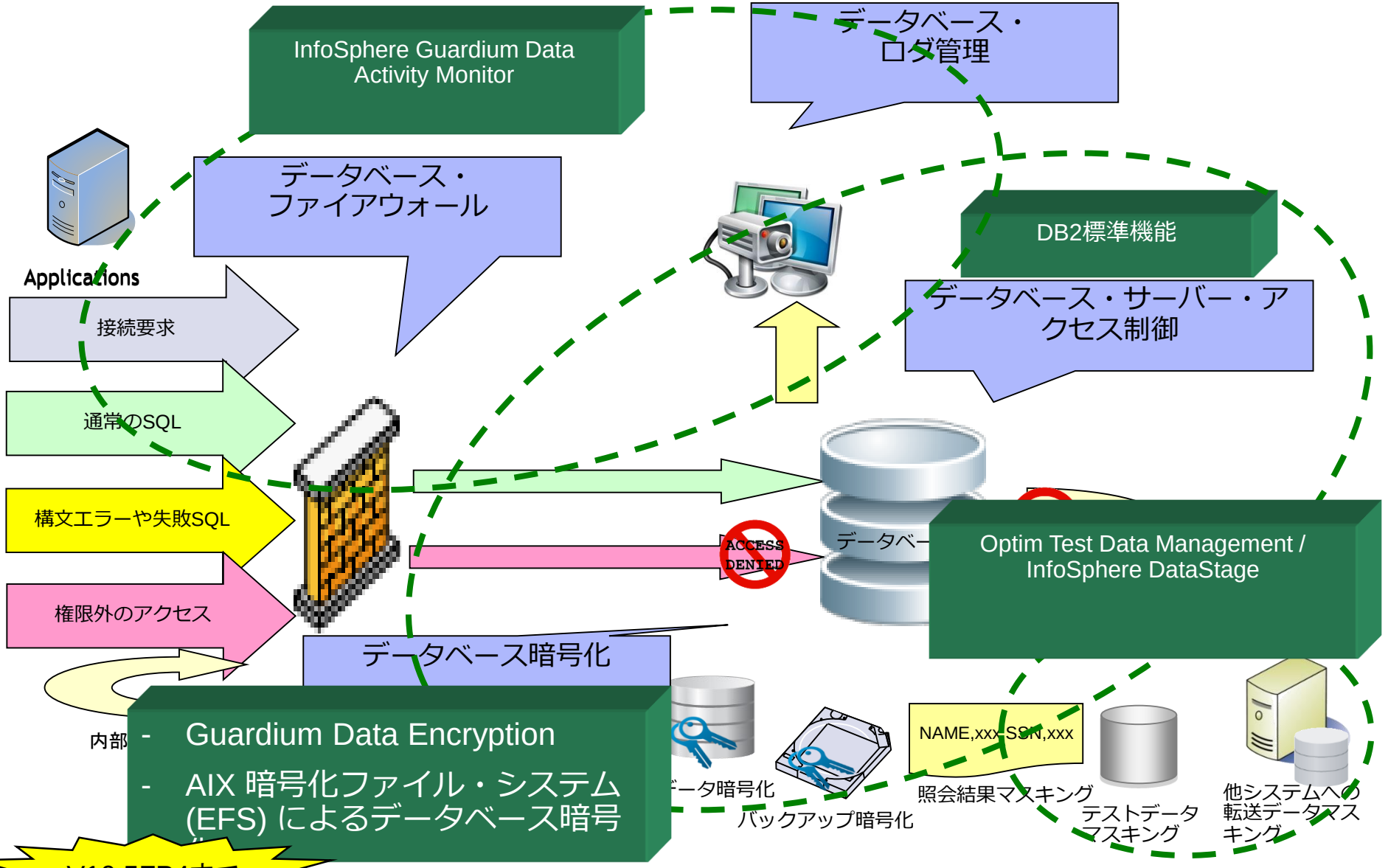


最終的に情報を保管しているデータベースの保護が重要

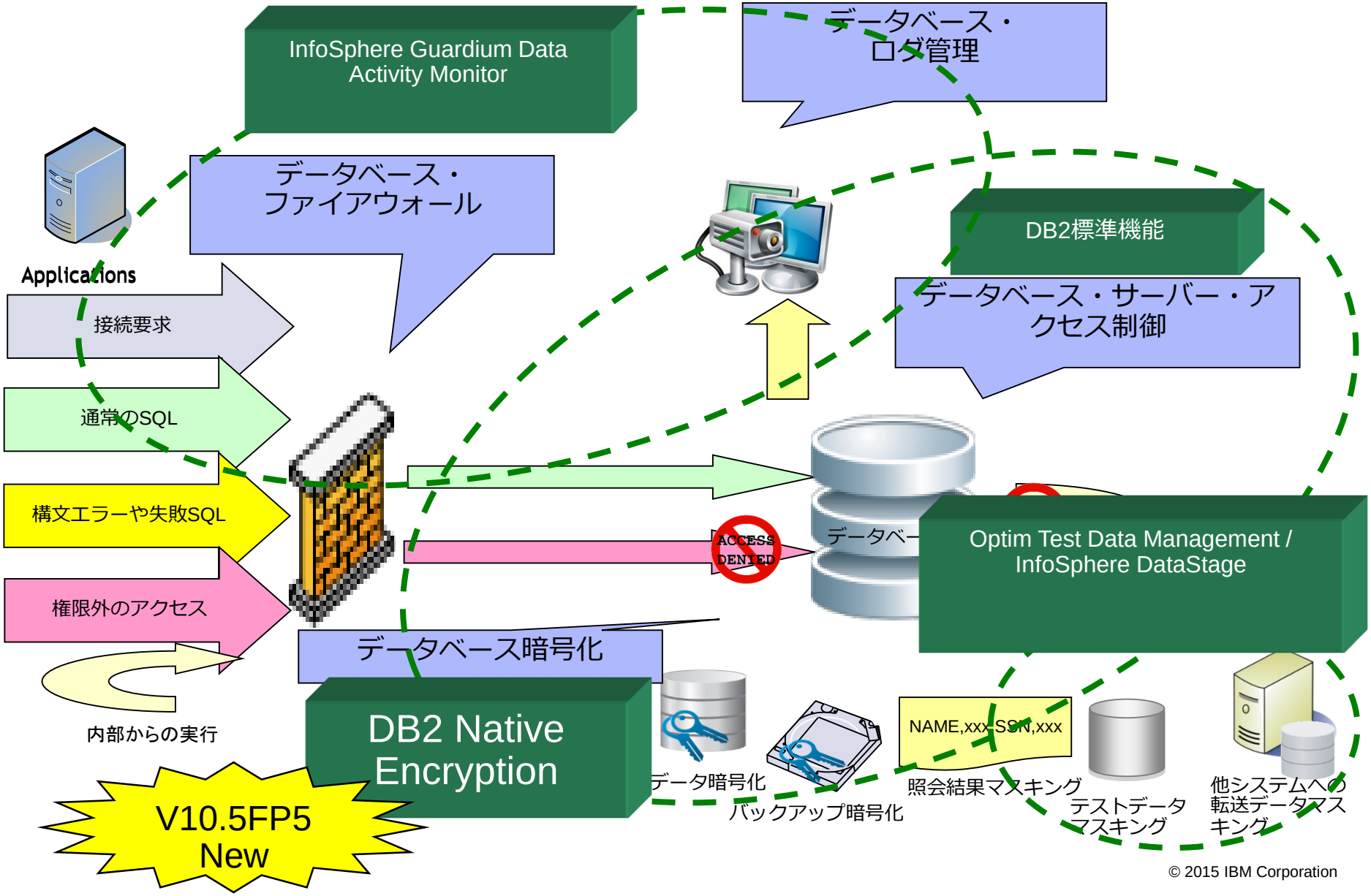
データベース・セキュリティー・ソリューション



IBMのデータベース・セキュリティー・ソリューション



IBMのデータベース・セキュリティー・ソリューション



DB2 Native Encryption

- ネイティブに IBM DB2 データベース・エンジン自体内で暗号化機能を提供
  - 実装が簡単

```
CREATE DATABASE mydb ENCRYPT;
```

  - アプリケーションに透過的

- Runs wherever DB2 runs!
  - 全DB2プラットフォームとトポロジーで利用可能
    - AIX, Linux, pLinux, zLinux, Windows, Solaris, HP-UX
    - pureScale, DPF, BLU
  - クラウドでも、アプライアンスでも
  - HWの暗号化アクセラレータを使用できる
    (Intel, Powerプラットフォームにおける AES暗号化の場合)

- 標準への準拠
  - NIST SP 800-131 compliant cryptographic algorithms
  - FIPS 140-2 certified encryption

- ※必要なライセンスは別途ご確認ください。
  http://w3.ibm.com/sales/support/ShowDoc.wss?docid=IMP14831JPJA)

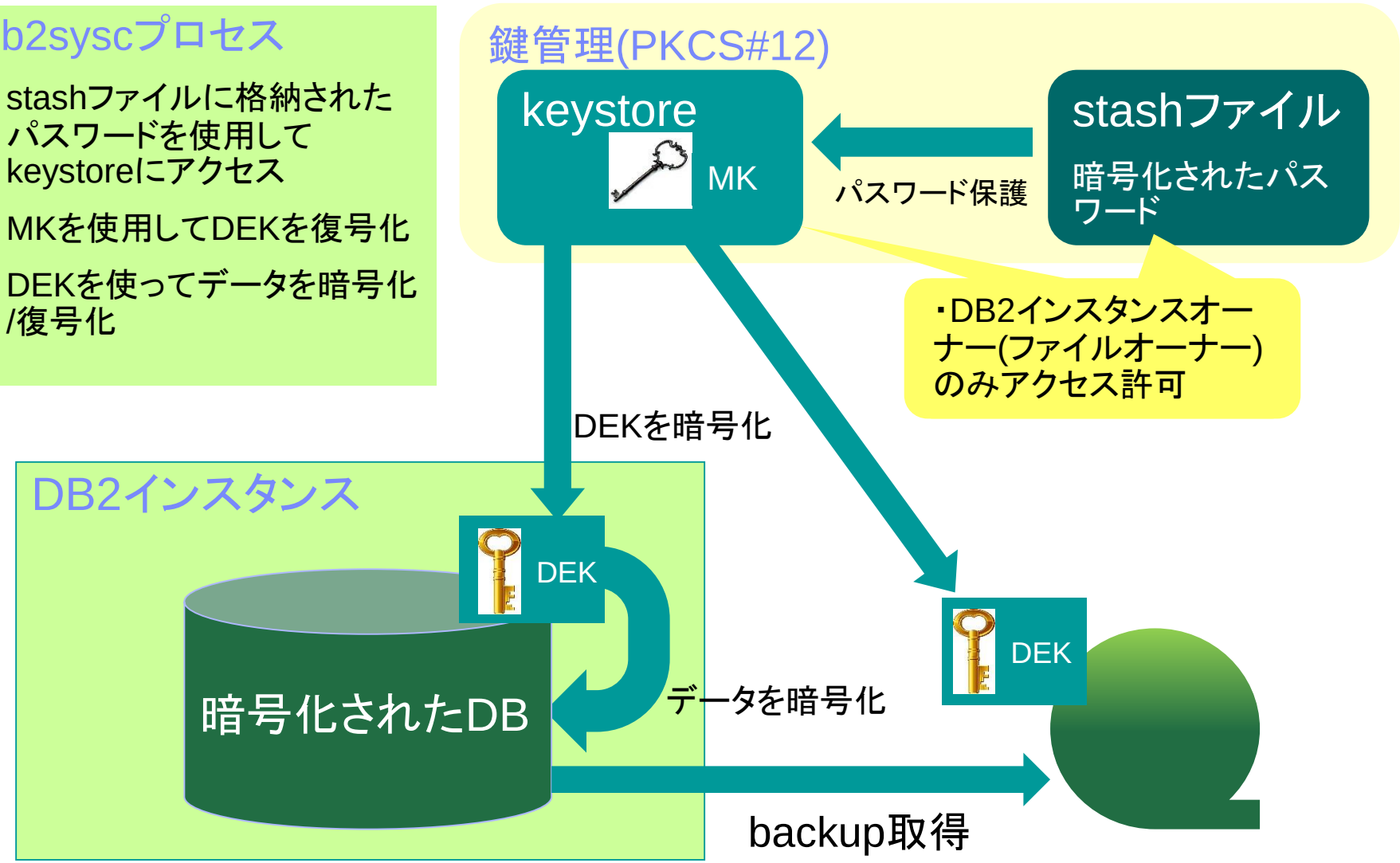
DB2 Native Encryption

- 暗号化されるオブジェクト
  - データベースのすべてのデータ
    - 表スペース
    - すべてのデータタイプ (LOB, XML, etc.)
    - トランザクションログ(アクティブ、アーカイブ)
    - LOAD COPY ファイル
    - ダンプファイル
  - バックアップ
- GSKitによる鍵管理および暗号化
  - 2層モデルによる鍵管理(PKCS#12準拠)
    - Data Encryption Key (DEK): 実際にデータの暗号化に使用される鍵
    - Master Key (MK) : DEKを暗号化する鍵
  - DEK は、MKによって暗号化されてデータベース内に保管される
  - MKは、暗号化されて外部のキーストアファイルに保管される
  - SYSPROC.ADMIN_ROTATE_MASTER_KEY プロシージャを使用してMKのローテーションを行う (PCI等で要求される)

DB2 Native Encryptionアーキテクチャー

db2syscプロセス

- stashファイルに格納されたパスワードを使用してkeystoreにアクセス
- MKを使用してDEKを復号化
- DEKを使ってデータを暗号化/復号化



DEK：Data Encryption Key
MK ：Master Key

目次

参考：DB2暗号化ソリューション比較(1)

	DB2 Native Encryption	AIX Encrypted File System (EFS)	InfoSphere Guardium Data Encryption (GDE)	ENCRYPT 関数 encypt() / decrypt_bin(), decrypt_char()
機能を提供する製品	DB2	AIX	GDE	DB2
暗号化の範囲	DB全体 バックアップ	選択したファイルシステム	選択したファイルシステム バックアップ	指定した列 バックアップ中でも指定した列は暗号化されている
暗号化対象の前提	DB2 V10.5 FP5以上　AESE, AWSEでは標準機能、それ以外のエディションでは有償フィーチャー	AIXプラットフォームのみ JFS2のみ	製品サポート情報確認が必要	暗号化列のデータタイプはCHAR/VARCHARのみ
暗号化アルゴリズム	3DES, AES(128, 192, 256)	AES(128, 192, 256)	3DES, AES(128,256)	RC2 鍵は関数実行時に与えるパスワードからMD5で派生

参考：DB2暗号化ソリューション比較(2)

	DB2 Native Encryption	AIX Encrypted File System (EFS)	InfoSphere Guardium Data Encryption (GDE)	ENCRYPT 関数 encypt() / decrypt_bin(), decrypt_char()
システム構成への影響	なし	なし	GDEサーバー(鍵管理、運用)を別マシンとして構成する	なし
アプリケーションへの影響	透過的	透過的	透過的	SQLにより暗号化/復号化を実施
物理設計への影響	透過的	透過的	透過的	暗号化する列の列長を変更する
パフォーマンスへの影響	パフォーマンステストポート参照 AES暗号化アクセラレーション(CPU)が使用できる	仕組み的にDB2 Encryption Offernngと同等のはず Power7+, Power8であれば、AESアクセラレーションが使用可能となる	仕組み的にDB2 Encryption Offernngと同等のはず	暗号化列数、アクセスパス、実行されるSQLでの該当列の使用方法によって異なる 比較的重い
使用の容易性	非常に簡単	プロセス起動時のキーの読み込みなどに考慮が必要	セキュリティ設計が必要	物理設計の考慮、アプリケーションの変更、鍵管理方法の設計等が必要

参考：DB2暗号化ソリューション比較(3)

	DB2 Native Encryption	AIX Encrypted File System (EFS)	InfoSphere Guardium Data Encryption (GDE)	ENCRYPT 関数 encypt() / decrypt_bin(), decrypt_char()
鍵管理の仕組	あり	あり	あり	なし(作成要)
鍵のローテーション	可能	可能	可能	不可(データをすべて暗号化しなおす)
他システムとのデータ共有 (バックアップの他システムへのリストア、HADR(*2), ディスク共有、等)	可能 マスターキーをexport/importするか、キーストアファイルの共有	ファイルシステムのパスを指定した暗号化であるため、バックアップファイルが暗号化されるかどうかは、バックアップ取得先による ディスクを共有する場合は、キーの共有が必要	可能 外部の鍵管理サーバーを使用	可能

目次

システム構成

- 暗号化負荷はCPU負荷となる
  - CPUは、通常構成に比べ、20-30%程度大きめに見積もることを推奨する
  - 暗号化はディスクへの書き込み時、復号はディスクからの読み取り時に行われる
    - このため、暗号化データベースの負荷はディスクへのIOの量に依存する

鍵管理の運用上の注意点

- ✓ キーストアのバックアップを忘れない
- ✓ Master Key (MK)は削除しない
  - バックアップを取得した後で、MKを削除すると、バックアップはリストアできない
  - 過去に取得したバックアップをリストアして、ロールフォワードするためには、バックアップイメージおよび、すべてのアーカイブログのキーが必要

- ✓ Master Key (MK)ラベルの命名規則を決定しておく
  - DB名、日付が分かるものを作成する
    - 必要なMKを判別するため
  - DB2が自動的に作成するMKを使用してもよい
    - DB2によるMK自動生成での命名規則
      DB2_SYSGEN_<instance名>_<database名>_<timestamp>
    - HADRでキーをローテートする場合は、DB2による自動生成ではなく、ユーザーがMKを作成することが必要

キーの紛失　＝　データベース使用不可能

第2部　パフォーマンステストレポート

目次

- 第2部　パフォーマンステストレポート
  - プロジェクト概要
    - テスト項目
    - 結果サマリー
  - 構成　設定
  - OLTP パフォーマンステスト テスト結果
  - ユーティリティテストシナリオ　テスト結果
    - Load Import
    - Backup Restore
    - Key Rotation
  - PMR　/ APAR
  - (参考)暗号化データベースの作成手順
  - DB2 構成情報詳細　(db2level / db2set / DBM CFG / DB CFG)

プロジェクト概要：IBM DB2 Native Encryption パフォーマンス検証

- 目的
  - DB2 Native Encryptionのパフォーマンス検証

- 背景
  - 個人情報保護、セキュリティー認証の取得、コンプライアンス準拠の必要性から、DBセキュリティ強化が求められる状況が増え、DB2暗号化の提案のための問合せが急増している。

  - DB2における暗号化といえば、従来は、Guardium Data EncryptionやAIX暗号化ファイル・システム (EFS) によるデータベース暗号化などを組み合わせて検討する必要があったが、DB2　Native EncryptionによりDB2がデータベースを暗号化する機能を持つことにより、手軽に適用可能となった。

  - 暗号化機能の利用時/非利用時で、OLTPトランザクションおよびユーティリティー実行時のパフォーマンスを比較検証することにより、提案品質向上とデリバリー時トラブルの未然防止を図る。

テスト項目

- 次の2つの項目について、 従来の通常データベースと DB2 Native Encryption で暗号化されたデータベースのパフォーマンスを比較する。

1.ユーティリティーテスト
  - Load / reorgchk / reorg/ runstats / Import / Export
  - Backup / Restore
  - Key Rotation

2.OLTP パフォーマンステスト

IBM Knowledge Center での DB2 Native encryption についての記述はこちら

http://www-01.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.sec.doc/doc/c0061758.html?lang=en

物理構成

- 今回の計測の目的は暗号化によるパフォーマンスへの影響を確認すること。
  - テスト項目ごとに　使用するディスクと CPU数を調整している。　（使用したシステムのCPUが速いため、ディスク待ちとなってしまうことが多い状況だった。ディスク待ちによるパフォーマンスへの影響を最小限にするため　調整している）
  - 今回搭載のCPU Intel(R) Xeon(R) CPU E5-2680 v2は　Intel AES-NI付き

Intel AES-NI : Advanced Encryption Standard New Instructions (AES-NI) は、迅速で安全なデータ暗号化 / 復号化処理を可能にする命令セットです。AES-NI は幅広い暗号化への応用、例えばバルク暗号化、複合化、認証、乱数生成、および認証暗号化の実行における応用に有益です。(http://ark.intel.com/ja/products/75277)

DB Server : db2encs
X3550M4 V2　7914-L3J (S/N 06BYXCR)
CPU : Intel(R) Xeon(R) CPU E5-2680 v2 @ 2.80GHz (fam: 06, model: 3e, stepping: 04) (10Corex2slot = 20Core)
Memory : 64GB
Disk
- 内部ディスク1TB x 4

内部ディスク1 1TB /dev/sda
システム , テストログ・シェル

- SSD
(OLTP TPCCで使用)

SSD 480GB /sdddbdisk TPCC Database

SSD 31.4GB /sddlogdisk TPCC Active Log

- Fibre : Brocade BFA FC (2port) x 2
Brocade BFA FC/FCOE SCSI driver - version: 3.2.23.0

S/W 構成

Red Hat Enterprise Linux 7 (x86_64)

使用イメージ　RHEL-7.0 20140507.0-Server-x86_64-dvd1.iso

DB2 V10.5 FP5　(4/6 Special_33839 適用)
•DB2 Advanced Enterprise Server Edition
•License type: CPU オプション

client1 (9117-MMA)
CPU : 4.7GHz POWER6+ x 16
Memory : 32GB

AIX level 7100-02-01-1245
DB2 V10.5 FP3

Ethernet

SAN Switch
2498-B24

Fibre 8Gbps

DS8700 (Total 750GB)

/dbnoenc Database 200GB	/lognoenc Active log 50GB
/dbenc Database 200GB	/logenc Active log 50GB
UtilData 200GB	Backup image 50GB

目次

- 第2部　パフォーマンステストレポート
  - プロジェクト概要
    - テスト項目
    - 結果サマリー
  - 構成　設定
  - OLTP パフォーマンステスト テスト結果
  - ユーティリティテストシナリオ　テスト結果
    - Load Import
    - Backup Restore
    - Key Rotation
  - PMR / APAR
  - (参考)暗号化データベースの作成手順
  - DB2 構成情報詳細 (db2level / db2set / DBM CFG / DB CFG)

今回の環境と処理における　結果サマリー

- OLTPテスト結果

  スループット(Transaction / sec)には　暗号化の影響がほとんど見られなかった。

  暗号化/通常DB = 100-103%

  CPU 使用率　暗号化したほうが、わずかにCPU使用率が高くなる。

  暗号化/通常DB = 110%以下

  暗号化の影響は CPU 使用率のusに現れている。

- ユーティリティーテスト結果

  所要時間は　ディスク速度と物理I/O量に依存。
  （CPU速度に対して　遅いディスクを使用すると　所要時間が変化がないことがある)

  CPU 使用率　20-30%増加

目次

- 第2部　パフォーマンステストレポート
  - プロジェクト概要
    - テスト項目
    - 結果サマリー
  - 構成　設定
  - OLTP パフォーマンステスト テスト結果
  - ユーティリティテストシナリオ　テスト結果
    - Load Import
    - Backup Restore
    - Key Rotation
  - PMR / APAR
  - (参考)暗号化データベースの作成手順
  - DB2 構成情報詳細 (db2level / db2set / DBM CFG / DB CFG)

データベース構成

- DB2インスタンスは　通常DB用インスタンスと暗号化DB用インスタンスの2個を作成
  - 違いは 暗号化の設定のみ

- すべてのデータはデフォルトの表スペースUSERSPAC1へロード

- バッファープールはデフォルトIBMDEFAULTBP のみ使用　30GB 割り当て
  - OLTP パフォーマンステストで使用するTPCC SF400のデータがすべてバッファー・プールに読み込まれる。
  - OLTP パフォーマンステストでは 物理読み込みが発生しない状況とするのが目的

- PAGE_AGE_TRGT_MCR　の設定 (テストでのデータ更新を速やかにディスクに反映させる)
  - **page_age_trgt_mcr - ページ存続期間のターゲット・メンバー・クラッシュ・リカバリー構成パラメーター**
    - 表スペース・ストレージ で保存される前に、ローカル・バッファー・プールで保持する変更済みページのターゲット期間 (秒単位) を指定します。
  - 30秒へ変更　(デフォルト 240秒)
  - 暗号化は物理読み込み書き込み時に発生するため、テストで発生したバッファー・プールへの書き込みは　次のテスト実施前に完了させるのが目的

ファイルシステムについて

すべてのファイルシステムは xfs

sda以外は nobarrier でマウントされています。

```
[16:58:21 root@db2encs cronshell]# mount | grep ^/dev | grep -v -E "/sdb|/sdc|/sdd1"
/dev/mapper/rhel00-root on / type xfs (rw,relatime,attr2,inode64,noquota)
/dev/sde on /sdddbdisk type xfs (rw,relatime,attr2,nobarrier,inode64,noquota)
/dev/sdf on /sddlogdisk type xfs (rw,relatime,attr2,nobarrier,inode64,noquota)
/dev/sda2 on /boot type xfs (rw,relatime,attr2,inode64,noquota)
/dev/sda1 on /boot/efi type vfat
(rw,relatime,fmask=0077,dmask=0077,codepage=437,iocharset=ascii,shortname=winnt,errors=remount-ro)
/dev/mapper/rhel00-home on /home type xfs (rw,relatime,attr2,inode64,noquota)
/dev/mapper/mpathb on /dbenc type xfs (rw,relatime,attr2,nobarrier,inode64,noquota)
/dev/mapper/mpathf on /logalt type xfs (rw,relatime,attr2,nobarrier,inode64,noquota)
/dev/mapper/mpathe on /logenc type xfs (rw,relatime,attr2,nobarrier,inode64,noquota)
/dev/mapper/mpathc on /dbalt type xfs (rw,relatime,attr2,nobarrier,inode64,noquota)
/dev/mapper/mpatha on /dbnoenc type xfs (rw,relatime,attr2,nobarrier,inode64,noquota)
/dev/mapper/mpathd on /lognoenc type xfs (rw,relatime,attr2,nobarrier,inode64,noquota)
[16:59:01 root@db2encs cronshell]#
```

暗号化の設定について

テスト項目ごとに　ディスクのアクセススピードと物理ディスク数(iostatでの測定)の観点で使用するディスクを変更している。

OLTP パフォーマンステストでは　物理的に2つのディスク(データベースとアクティブログ)を使用する。 ランダムなディスクアクセスで可能な限り早いSSDを選択した。

Utilityテストでは　物理的に3つ(DB,LOG,データ)のディスクを使用する。DS8000の外部ディスクを使用。スピードではSSDにおとる。

水色の中のファイルは暗号化されません

ピンクの中のファイルはDB2 Native Encryptionにより暗号化されます。

	device	サイズ	目的	通常DB テスト	暗号化DBテスト
内部ディスク	sda	1TB	システム、テストログ・シェル		
	sdb-sdd	(各1TB)	（不使用)	(n/a)	(n/a)
SSD TPCC Test	sde	478GB	データベース /sdddbdisk/	DB : SDBNOENC /sdddbdisk/db2noenc	DB : SDBENC /sdddbdisk/db2enc
	sdf	20GB	アクティブログ /sddlogdisk/	/sddlogdisk/db2noenc	/sddlogdisk/db2enc
DS8000 Utility Test	mpatha	200GB	データベース　/dbnoenc/	DB: DBNOENC / NEWDB	(n/a)
	mpathb	200GB	データベース　/dbenc/	(n/a)	DB: DBENC / NEWDB
	mpathc	200GB	ユーティリティーテストで使用するファイル (/dbalt)	Load , Import ソースファイル / Export あて先ファイル	
				Backup	Backup
	mpathd	50GB	アクティブログ　/lognoenc	/lognoenc	(n/a)
	mpathe	50GB	アクティブログ　/logenc	(n/a)	/logenc
	mpathf	50GB	(/logalt)	基本バックアップイメージ	

テストに使用したファイル

	行数	サイズ(byte)
LOAD 用データ 87 GB (93,639,868,771 byte)		
lineitem.tbl.1	99,989,016	13,251,777,816
lineitem.tbl.10	99,986,806	13,362,549,100
lineitem.tbl.11	100,000,672	13,464,555,918
lineitem.tbl.12	99,995,809	13,463,828,349
lineitem.tbl.2	100,011,248	13,365,820,974
lineitem.tbl.3	100,005,547	13,365,129,958
lineitem.tbl.4	100,013,713	13,366,206,656
IMPORT 用データ 5GB		
lineitem.tbl.5GB	40,164,690	5,316,379,555

	行数	サイズ(byte)
OLTP TPCC SF400 (18GB)		
customer.tbl	12,000,000	6,846,092,131
district.tbl	4,000	415,247
item.tbl	100,000	7,963,332
stock.tbl	40,000,000	12,585,191,888
warehouse.tbl	400	38,744

Utility , OLTPテスト用データ ベースバックアップイメージ

通常DB環境 暗号化DB環境ともに 新規にDBを作成し TPCC SF400 をLoadした後 オフラインバックアップを取得して作成

- (通常DB環境) DBNOENC.0.db2noenc.DBPART000.20150305080701.001 (バックアップ・イメージ・サイズ:23,225,368,576 byte)
- (暗号化DB環境) DBENC.0.db2enc.DBPART000.20150305174516.001 (バックアップ・イメージ・サイズ: 23,225,368,576 byte)

Backup Restore用データ ベースバックアップイメージ

通常DB環境 暗号化DB環境ともに 新規にDBを作成し TPCC SF400 と Load用データ lineitem.tbl.1, 2,3 をLoadした後 オフラインバックアップを取得して作成

- (通常DB環境) DBNOENC.0.db2noenc.DBPART000.20150318165806.001(バックアップ・イメージ・サイズ: 68,518,129,664 byte)
- (暗号化DB環境) DBENC.0.db2enc.DBPART000.20150318173344.001(バックアップ・イメージ・サイズ: 68,518,129,664 byte)

目次

- 第2部　パフォーマンステストレポート
  - プロジェクト概要
    - テスト項目
    - 結果サマリー
  - 構成　設定
  - OLTP パフォーマンステスト テスト結果
  - ユーティリティテストシナリオ　テスト結果
    - Load Import
    - Backup Restore
    - Key Rotation
  - PMR / APAR
  - (参考)暗号化データベースの作成手順
  - DB2 構成情報詳細 (db2level / db2set / DBM CFG / DB CFG)

結果サマリー：OLTPテスト

以下は、暗号化DBのテストでは、DB2 V10.5 FP5にSpecial Build 33839を適用してテストを実施した結果である。

スループット(Transaction / sec)には　暗号化の影響が見られなかった。

暗号化/通常DB = 100-103%

CPU 使用率　暗号化したほうがわずかにCPUを使用する。

暗号化/通常DB = 110%以下

暗号化の影響は CPU 使用率のusに現れている。

MON_GET_DATABSE から

- LOG_DISK_WAIT_TIMEが暗号化による影響を多く受けていて　次がPOOL_WRITE_TIME(このケースではPOOL_ASYNC_WRITE_TIMEと同じ）
- LOG_DISK_WAIT_TIME では　DB2からみた物理I/O時間であるLOG_WRITE_TIMEが暗号化による影響を受けている

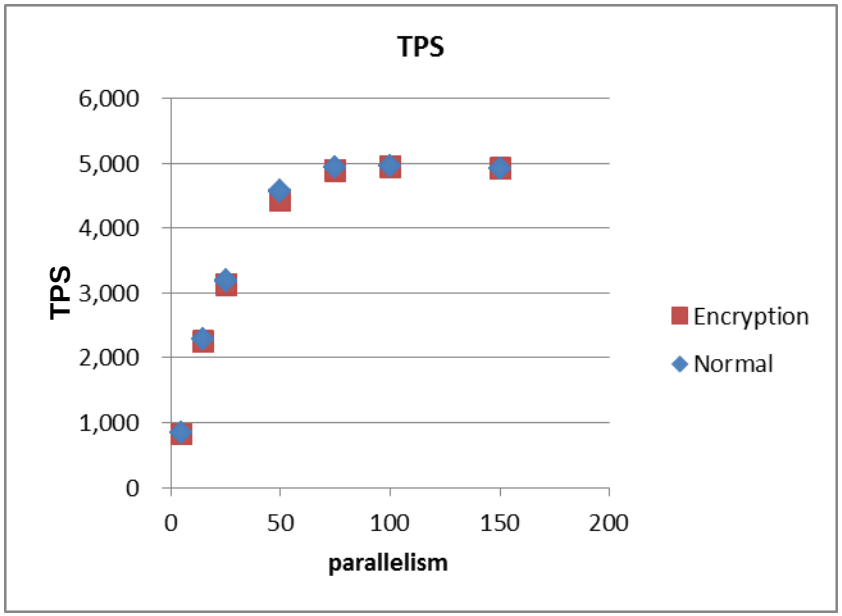
テストシナリオ　OLTPテスト

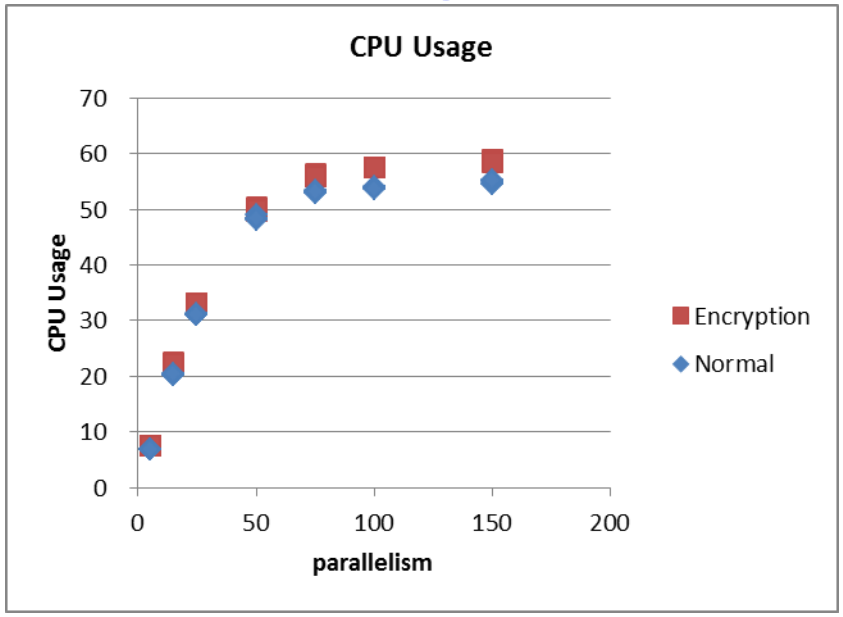
- Normal環境　Encryption環境で，並列数 5 15 25 50 75 100 150　各並列数 5回ずつテストを実行　1回のテストは5分実行

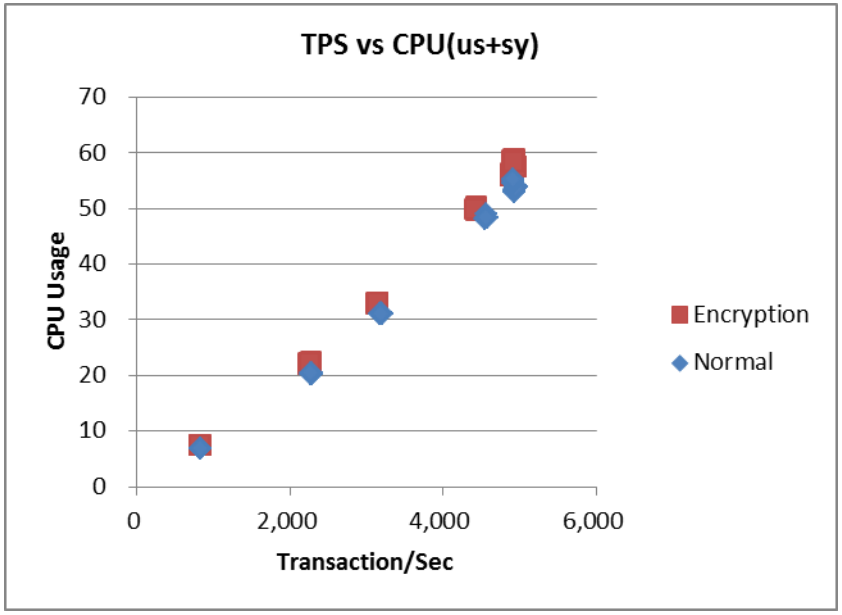
- Normal 環境　または　Encryption環境でのテスト開始時に　customer, district, item, stock, warehouse の次の2つを実行してすべてのデータを読み込む。
  - db2 +o select "* from $tabname“
  - db2 runstats on table ${DBUID}.$tabname with distribution and detailed indexes all

- 各回5分間のテスト開始前に データがInsertされるテーブル(orders new_order order_line)を次を使用して初期化(削除)。
  - db2 +o import from /dev/null of del replace into $deltbl

結果: TPCC SF400 Transaction/Sec CPU Usage 物理CPU12個







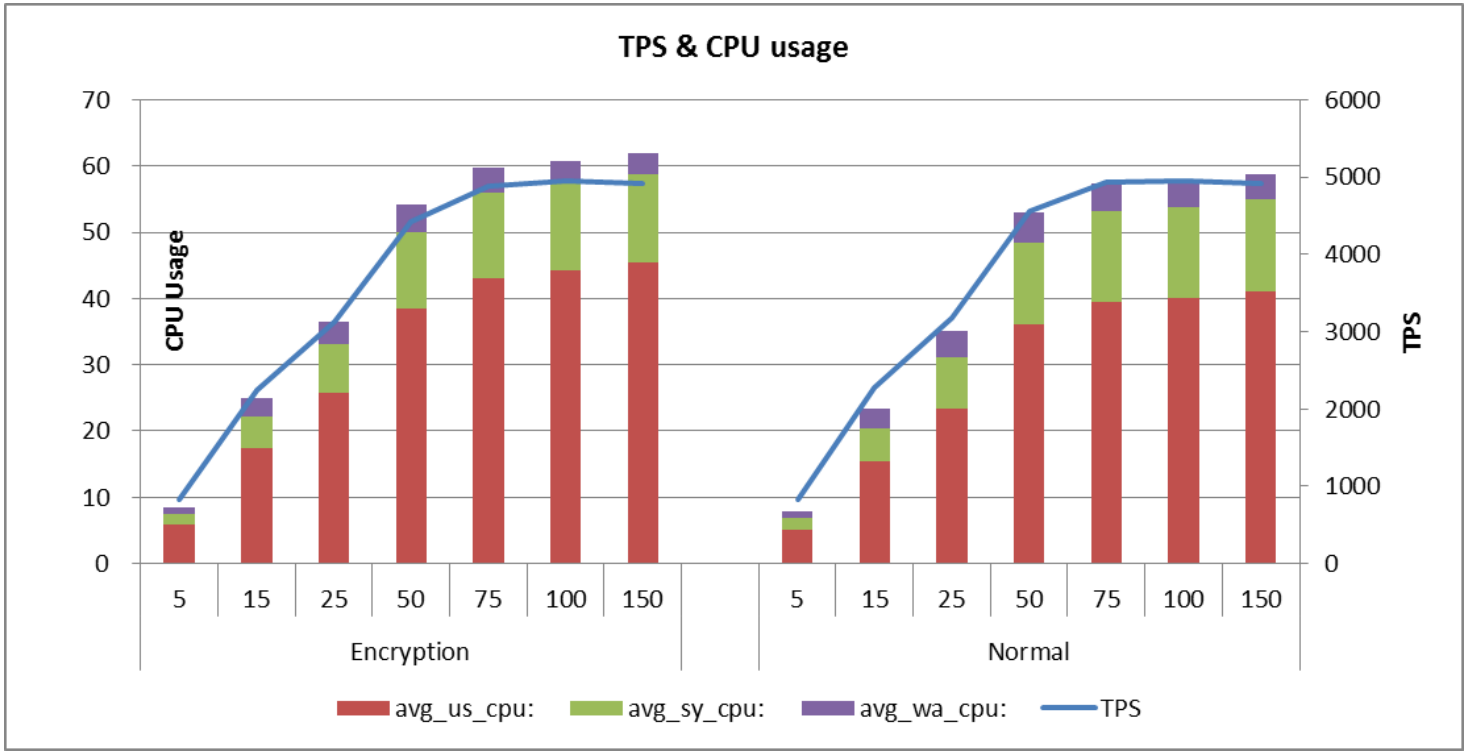
左上 **TPS**　暗号化していても通常とさほど変わりがない

上 **CPU Usage**　わずかに暗号化したほうがCPUを使用する。

左 : **TPS vs CPU(us+sy)**

おなじトランザクション量を処理するのに必要なCPUは 暗号化するほうが多いことがわかる。

結果: TPCC SF400 Transaction/Sec CPU Usage 物理CPU12個



para	TPS:			avg_cpu(us+sy)			avg_us_cpu			avg_sy_cpu			avg_wa_cpu	
	Encryption	Normal	Normal/Enc	Encryption	Normal	Enc/Normal	Encryption	Normal	Enc/Normal	Encryption	Normal	Enc/Normal	Encryption	Normal
5	821.74	834.48	102%	7.49	6.83	110%	5.91	5.09	116%	1.58	1.75	90%	1.01	1.03
15	2,246.93	2,279.19	101%	22.19	20.32	109%	17.31	15.35	113%	4.87	4.97	98%	2.69	3.06
25	3,131.76	3,185.13	102%	33.07	31.06	106%	25.81	23.30	111%	7.26	7.76	94%	3.48	4.11
50	4,427.58	4,564.28	103%	49.99	48.39	103%	38.45	36.03	107%	11.54	12.36	93%	4.14	4.64
75	4,885.11	4,934.58	101%	56.02	53.12	105%	43.06	39.50	109%	12.97	13.62	95%	3.66	4.32
100	4,946.82	4,947.06	100%	57.56	53.87	107%	44.33	40.14	110%	13.24	13.73	96%	3.24	4.04
150	4,913.15	4,908.97	100%	58.76	54.91	107%	45.42	41.12	110%	13.33	13.79	97%	3.09	3.83

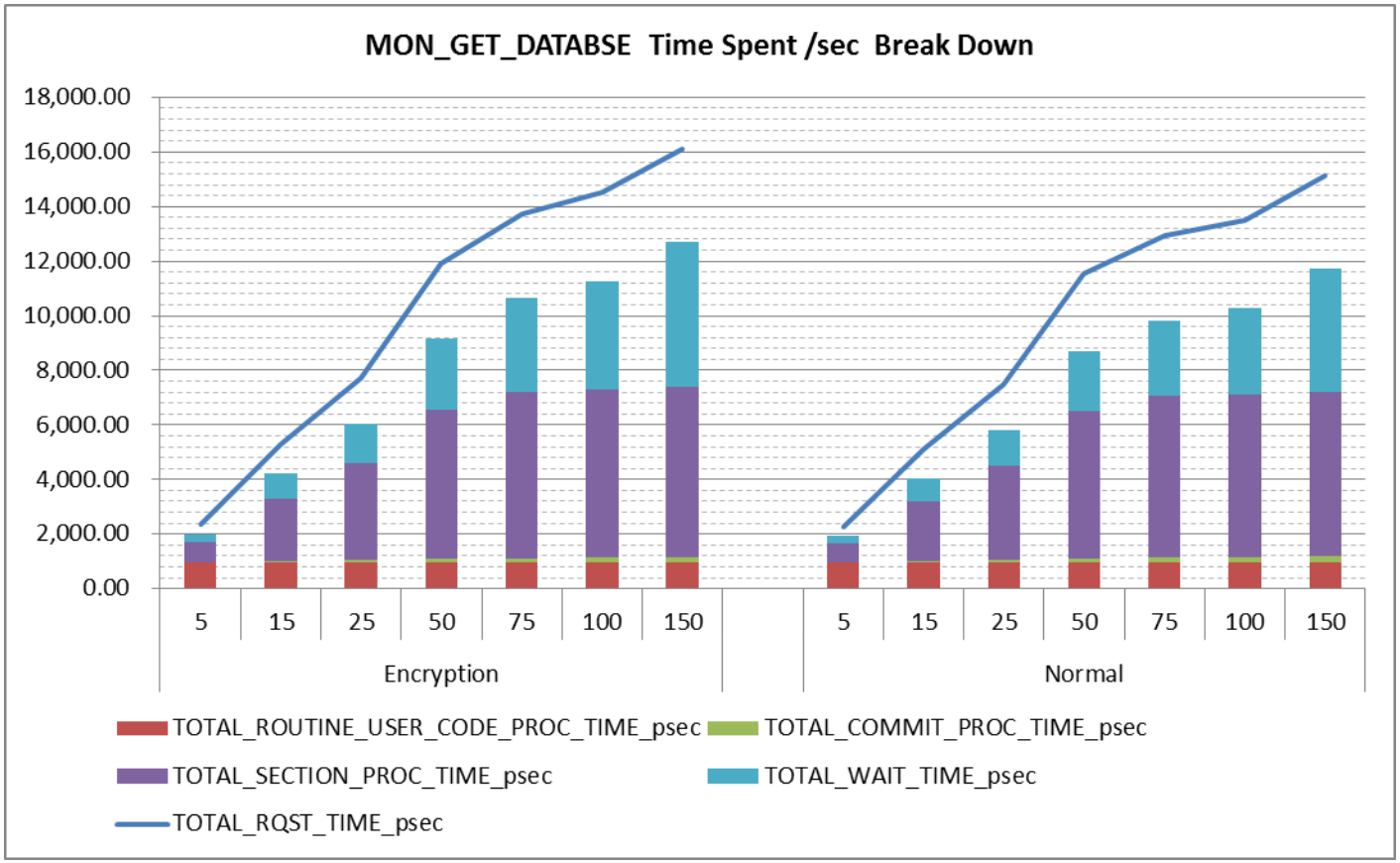
水色 104%以下 黄色 105%- 110% ピンク 111%以上

DB2 Native Encryptionでは (syではなく) usが使用される。

結果: TPCC SF400 iostat

		para	avg_rrqm/s	avg_wrqm/s	avg_r/s	avg_w/s	avg_rkB/s	avg_wkB/s	avgrq-sz	avgqu-sz	avg_await	avg_r_await	avg_w_await	avg_svctm	avg_%util
dbdisk	Encryption	5	0	192.96	0.71	4,257.31	4.43	17,879.60	8.40	9.22	2.16	0.03	2.16	0.02	7.85
		15	0	538.77	0.01	10,455.56	0.10	44,166.08	8.45	22.09	2.11	0.02	2.11	0.02	19.52
		25	0	761.67	0.01	14,264.50	0.12	60,366.10	8.46	30.25	2.12	0.03	2.12	0.02	26.90
		50	0	1,111.72	0.20	18,913.68	1.47	80,412.28	8.50	40.40	2.14	0.09	2.14	0.02	35.74
		75	0	1,262.83	0.02	19,544.92	0.18	83,534.56	8.55	41.75	2.14	0.04	2.14	0.02	37.55
		100	0	1,308.96	0.03	19,413.86	0.21	83,197.74	8.57	41.17	2.12	0.06	2.12	0.02	37.34
		150	0	1,322.85	0.01	19,140.30	0.08	82,153.90	8.58	40.35	2.11	0.03	2.11	0.02	36.81
	Normal	5	0	194.16	0.64	4,319.26	4.04	18,132.08	8.40	9.42	2.18	0.04	2.18	0.02	7.91
		15	0	544.07	0.01	10,845.84	0.08	45,757.16	8.44	23.54	2.17	0.01	2.17	0.02	20.19
		25	0	777.72	0.02	14,388.82	0.15	60,957.82	8.47	31.33	2.18	0.03	2.18	0.02	27.18
		50	0	1,142.27	0.21	18,892.18	1.47	80,456.36	8.52	40.89	2.17	0.09	2.17	0.02	35.30
		75	0	1,270.98	0.03	20,171.20	0.21	86,086.80	8.54	43.72	2.17	0.05	2.17	0.02	38.02
		100	0	1,305.10	0.02	19,079.02	0.11	81,857.40	8.58	41.00	2.15	0.05	2.15	0.02	36.10
		150	0	1,316.65	0.01	19,043.92	0.10	81,760.78	8.59	40.83	2.14	0.03	2.14	0.02	35.99
logdisk	Encryption	5	0	0.00	0.09	1,738.92	0.74	8,029.89	9.26	0.06	0.04	0.03	0.04	0.04	6.21
		15	0	0.00	0.25	5,243.40	2.02	22,573.68	8.61	0.20	0.04	0.05	0.04	0.04	20.11
		25	0	0.01	0.35	7,183.37	2.81	30,654.00	8.54	0.28	0.04	0.04	0.04	0.04	27.95
		50	0	0.01	0.50	9,118.52	3.98	39,605.32	8.69	0.37	0.04	0.06	0.04	0.04	37.08
		75	0	0.01	0.55	9,494.60	4.39	41,743.52	8.80	0.39	0.04	0.04	0.04	0.04	38.73
		100	0	0.01	0.56	9,445.33	4.45	41,720.58	8.84	0.39	0.04	0.04	0.04	0.04	38.75
		150	0	0.01	0.55	9,341.94	4.42	41,295.80	8.84	0.38	0.04	0.03	0.04	0.04	38.25
	Normal	5	0	0.00	0.09	1,819.09	0.75	8,186.53	9.01	0.06	0.03	0.02	0.03	0.03	6.07
		15	0	0.00	0.26	5,242.37	2.05	22,800.06	8.70	0.19	0.04	0.06	0.04	0.04	18.55
		25	0	0.01	0.36	7,271.90	2.87	31,438.20	8.65	0.26	0.04	0.06	0.04	0.04	26.42
		50	0	0.01	0.51	10,063.04	4.11	43,593.22	8.66	0.38	0.04	0.04	0.04	0.04	38.13
		75	0	0.01	0.56	10,609.90	4.44	46,157.16	8.70	0.41	0.04	0.05	0.04	0.04	40.92
		100	0	0.01	0.56	10,669.48	4.45	46,356.78	8.69	0.41	0.04	0.04	0.04	0.04	41.03
		150	0	0.01	0.55	10,474.80	4.41	45,635.50	8.71	0.41	0.04	0.04	0.04	0.04	40.57

MON_GET_DATABSE 1秒当たりの消費時間



TOTAL_ROUTINE_USER_CODE_PROC_TIMEは MON_GET_Database などモニター情報取得に費やされた時間と考えられる

TOTAL_SECTION_PROC_TIME　の違いは要因不明

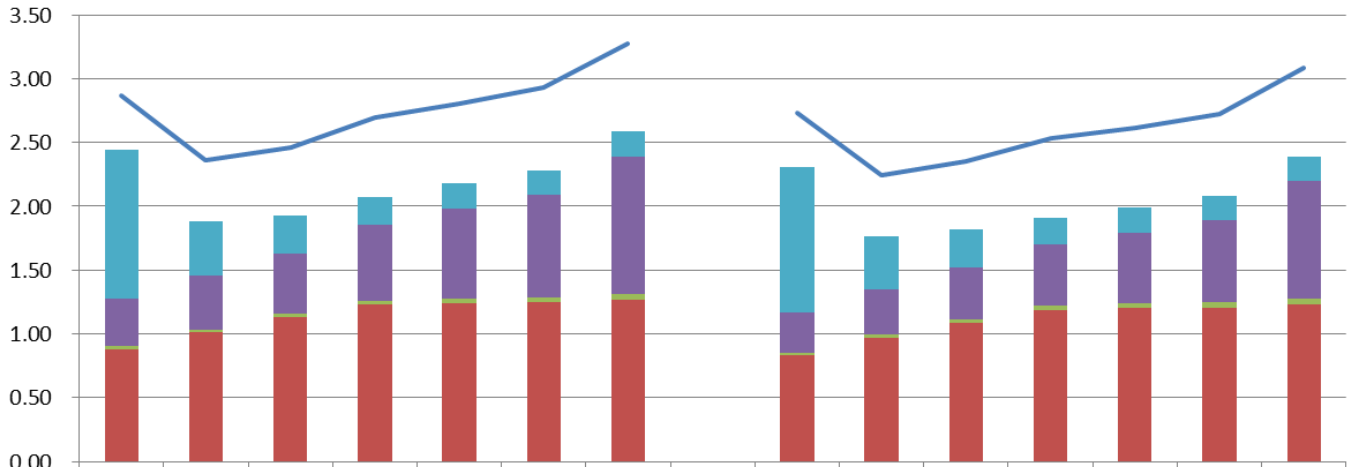
暗号化と通常の大きな違いは　TOTAL_WAIT_TIME

/sec	TOTAL_RQST_TIME			TOTAL_SECTION_PROC_TIME			TOTAL_WAIT_TIME		
	Encryption	Normal	Enc/Normal	Encryption	Normal	Enc/Normal	Encryption	Normal	Enc/Normal
5	2,360.23	2,282.96	103%	725.17	692.21	105%	307.35	263.65	117%
15	5,313.42	5,124.09	104%	2,273.46	2,206.35	103%	939.45	809.34	116%
25	7,706.88	7,492.87	103%	3,541.31	3,467.84	102%	1,466.72	1,280.94	115%
50	11,920.08	11,558.85	103%	5,440.70	5,407.61	101%	2,650.48	2,207.88	120%
75	13,720.56	12,921.56	106%	6,065.27	5,927.55	102%	3,443.35	2,749.29	125%
100	14,502.83	13,490.82	108%	6,173.14	5,969.58	103%	3,960.83	3,175.66	125%
150	16,099.65	15,128.30	106%	6,233.84	6,029.90	103%	5,297.65	4,528.61	117%

水色 104%以下　黄色 105%- 110%　ピンク　111%以上

MON_GET_DATABSE 1トランザクション当たりの消費時間

MON_GET_DATABSE
Time Spent / transaction
Break Down



	Encryption							Normal						
	5	15	25	50	75	100	150	5	15	25	50	75	100	150
TOTAL_ROUTINE_USER_CODE_PROC_TIME	1.16	0.42	0.30	0.22	0.20	0.19	0.19	1.14	0.42	0.30	0.21	0.19	0.19	0.19
TOTAL_WAIT_TIME	0.37	0.42	0.47	0.60	0.70	0.80	1.08	0.32	0.36	0.40	0.48	0.56	0.64	0.92
TOTAL_COMMIT_PROC_TIME	0.023	0.024	0.026	0.032	0.035	0.038	0.042	0.022	0.024	0.027	0.033	0.037	0.039	0.044
TOTAL_SECTION_PROC_TIME	0.88	1.01	1.13	1.23	1.24	1.25	1.27	0.83	0.97	1.09	1.18	1.20	1.21	1.23
TOTAL_RQST_TIME	2.87	2.36	2.46	2.69	2.81	2.93	3.28	2.74	2.25	2.35	2.53	2.62	2.73	3.08

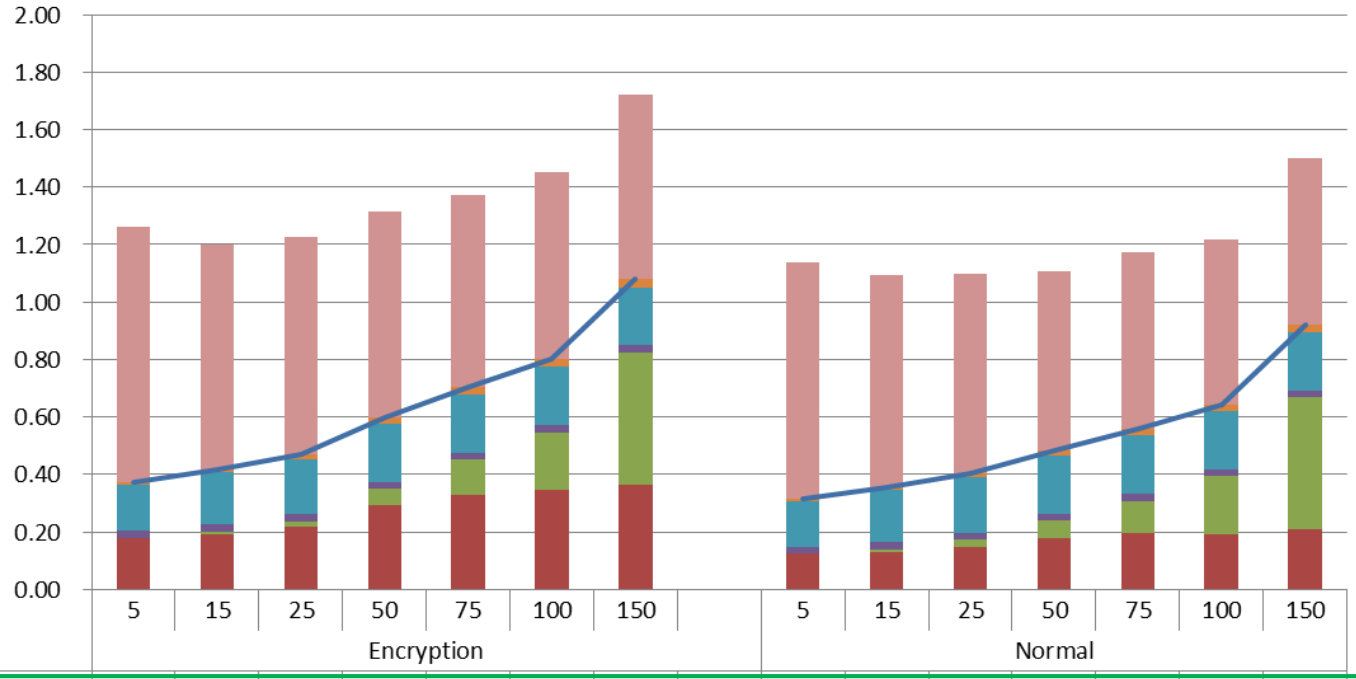
TOTAL_ROUTINE_USER_CODE_PROC_TIMEは MON_GET_Database などモニター情報取得に費やされた時間と考えられる

TOTAL_SECTION_PROC_TIME　の違いは要因不明

次に　TOTAL_WAIT_TIMEの違いを見る。

MON_GET_DATABSE 1トランザクション当たりの待機時間

MON_GET_DATABSE
WAIT_TIME / transaction
Break Down



データはあらかじめBPに読み込んでいるためPOOL_READ_TIMEが0となっている

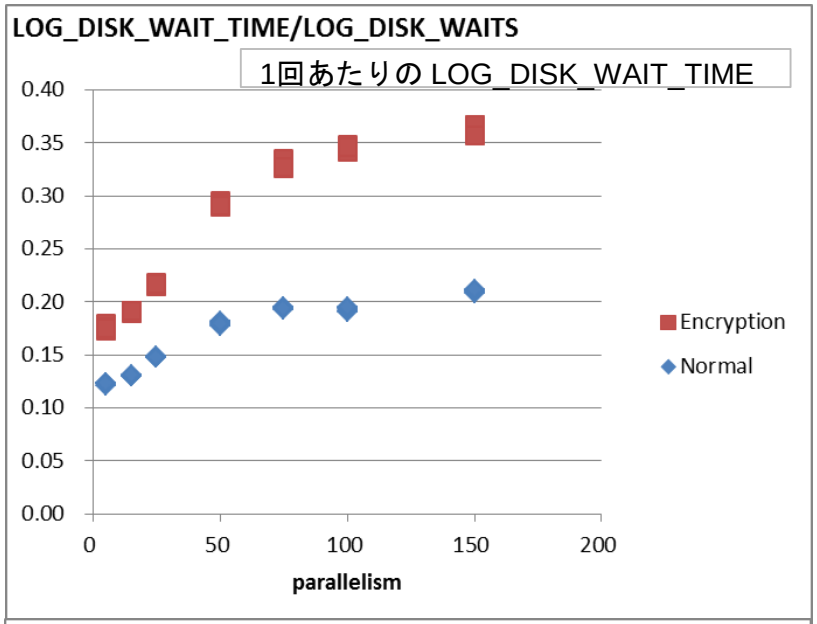
並列数が増えるにつれLOCK_WAIT_TIMEが増加している。 暗号化あるなしによる違いはない。

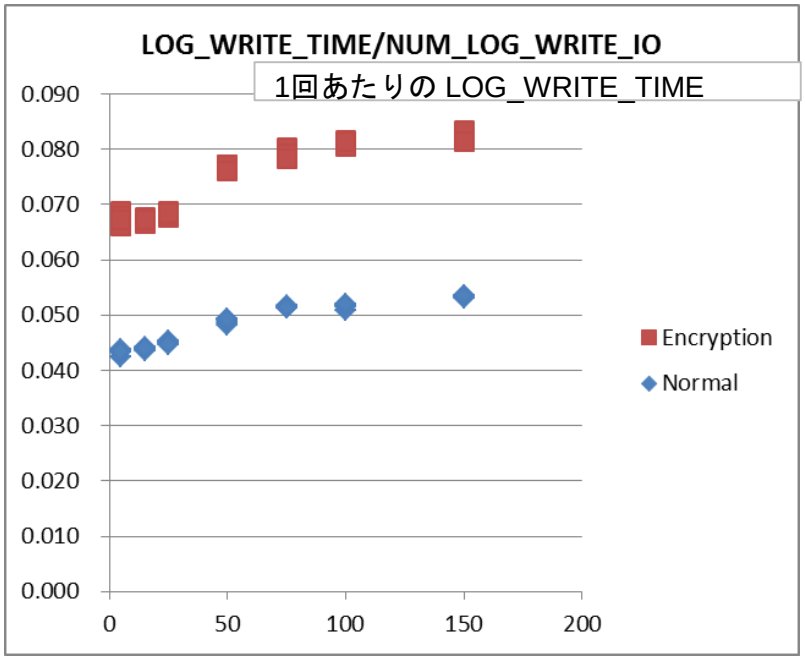
	Encryption							Normal						
	5	15	25	50	75	100	150	5	15	25	50	75	100	150
POOL_WRITE_TIME	0.89	0.78	0.76	0.72	0.67	0.65	0.64	0.82	0.74	0.70	0.63	0.62	0.57	0.58
POOL_READ_TIME	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00	0.00
TOTAL_EXTENDED_LATCH_WAIT_TIME	0.01	0.01	0.02	0.02	0.03	0.03	0.03	0.01	0.01	0.01	0.02	0.02	0.02	0.03
TCPIP_SEND_WAIT_TIME	0.16	0.18	0.19	0.20	0.20	0.20	0.20	0.16	0.18	0.19	0.20	0.20	0.20	0.20
TCPIP_RECV_WAIT_TIME	0.02	0.03	0.03	0.03	0.03	0.03	0.03	0.02	0.02	0.02	0.02	0.02	0.02	0.03
LOCK_WAIT_TIME	0.00	0.01	0.02	0.06	0.12	0.20	0.46	0.00	0.01	0.02	0.06	0.11	0.20	0.46
LOG_DISK_WAIT_TIME	0.18	0.19	0.22	0.29	0.33	0.35	0.36	0.12	0.13	0.15	0.18	0.19	0.19	0.21
TOTAL_WAIT_TIME	0.37	0.42	0.47	0.60	0.70	0.80	1.08	0.32	0.36	0.40	0.48	0.56	0.64	0.92

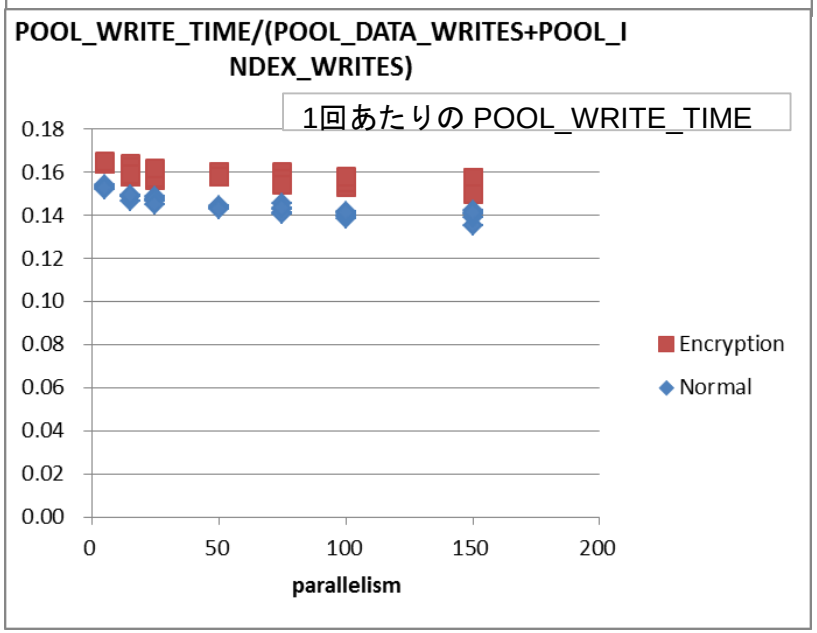
このケースでは　POOL_WRITE_TIMEは POOL_ASYNC_WRITE_TIMEと同じ
TOTAL_WAIT_TIMEで並列数が増え増加するのは　LOG_DISK_WAIT_TIME LOCK_WAIT_TIME

暗号化と通常の違いは POOL_WRITEと　LOG_WRITE時間に出ている。

1回あたりのLOG書き込み待ち時間 データ書き込み時間

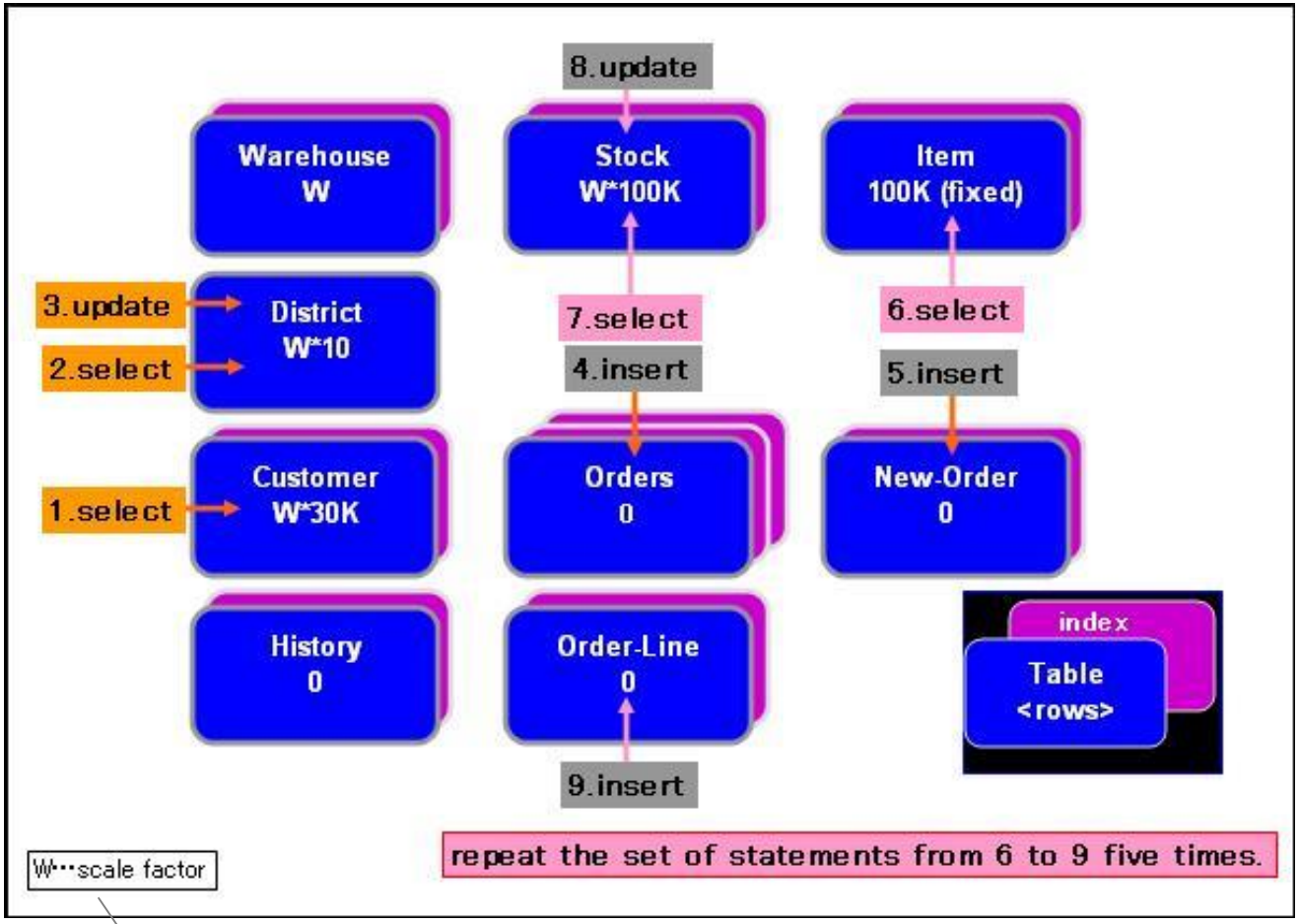






/sec	1回あたりのログ待ち時間 LOG_DISK_WAIT_TIME/LOG_DISK_WAITS			1回あたりの LOG_WRITE_TIME LOG_WRITE_TIME/NUM_LOG_WRITE_IO			1回あたりの POOL_WRITE_TIME POOL_WRITE_TIME/(POOL_DATA_WRITES+POOL_INDEX_WRITES)		
para	Encryption	Normal	Enc/Normal	Encryption	Normal	Enc/Normal	Encryption	Normal	Enc/Normal
5	0.18	0.12	144%	0.0677	0.0433	156%	0.1645	0.1531	107%
15	0.19	0.13	147%	0.0673	0.0440	153%	0.1604	0.1486	108%
25	0.22	0.15	147%	0.0683	0.0450	152%	0.1590	0.1471	108%
50	0.29	0.18	163%	0.0768	0.0489	157%	0.1591	0.1436	111%
75	0.33	0.19	169%	0.0792	0.0514	154%	0.1571	0.1426	110%
100	0.35	0.19	179%	0.0810	0.0516	157%	0.1557	0.1403	111%
150	0.36	0.21	173%	0.0825	0.0533	155%	0.1553	0.1397	111%

TPCC ワークロード



今回は
scale factor = 400

1.Select
2.Select
3.Update
4.Insert
5.Insert

6.Select
7.Select
8.Update
9.Insert

Repeat
5 times

目次

- 第2部　パフォーマンステストレポート
  - プロジェクト概要
    - テスト項目
    - 結果サマリー
  - 構成　設定
  - OLTP パフォーマンステスト テスト結果
  - ユーティリティテストシナリオ　テスト結果
    - Load Import
    - Backup Restore
    - Key Rotation
  - PMR / APAR
  - (参考)暗号化データベースの作成手順
  - DB2 構成情報詳細 (db2level / db2set / DBM CFG / DB CFG)

結果サマリー

- ユーティリティーテスト結果

所要時間は　ディスク速度と物理I/O量に依存。
（CPU速度に対して　遅いディスクを使用すると　所要時間が変化がないことがある)

CPU 使用率　20-30%増加

考察1：ユーティリティーテスト

DB2 Native Encryptionでは 物理書き出しの時暗号化され　物理読み込みの時復号化される。

暗号化負荷は計算処理であるため　暗号化の影響はCPU使用率にあらわれる。(暗号化したほうがCPU使用率が高くなる)

高速なCPUを使っている場合や多くのCPUを使用している場合は　物理I/Oの影響が処理時間に大きく現れる。 このためCPU負荷の違いが所要時間に反映されなくなる。

考察 2: ユーティリティーテスト

➢Load / reorgchk / reorg/ runstats / Import / Export

暗号化による所要時間の違いが目立たないケースが多い。

•物理CPU数が多いほど暗号化処理の影響は見えなくなる。(物理CPU4個と12個の結果参照)

•物理I/Oが多すぎるケース(例：Load Loadフェーズ)ではディスク待ちとなる

➢Backup / Restore

– Parallelismは指定していないためDB2による設定される。
– このため　物理CPU数による違いは見られない

Backup : Parallelism　3
暗号化/圧縮オプションによる影響が、所要時間CPU使用率に現れている。(物理I/Oの影響のため　所要時間の差が縮小している)

Restore : Parallelism　2
圧縮されているバックアップイメージのRestoreでは暗号化による影響が出ている
圧縮されていないバックアップイメージをRestoreするケースでは　物理I/Oが原因で　Disk Busyとなり所要時間に差は見られない

➢Key Rotation : 問題なし

目次

- 第2部　パフォーマンステストレポート
  - プロジェクト概要
    - テスト項目
    - 結果サマリー
  - 構成　設定
  - OLTP パフォーマンステスト テスト結果
  - ユーティリティテストシナリオ　テスト結果
    - Load Import
    - Backup Restore
    - Key Rotation
  - PMR / APAR
  - (参考)暗号化データベースの作成手順
  - DB2 構成情報詳細 (db2level / db2set / DBM CFG / DB CFG)

ユーティリティーテストシナリオ　Load Import について

太字部分のみ計測
(*1) 所要時間の計測は行うが短時間の作業のためモニター情報は取得しない
(*2) 元ファイルへのファイルキャッシュの影響を最小化するためのダミー実行

Load系テスト　データサイズ 87GB	Import系テスト　データサイズ 5GB
F00_crttbl1 (*1)	F00_crttbl1 (*1)
F01_Load3_insert_nonrecoverable (*2)	FI1_Import1_insert_COMMITAUTO (*2)
F00_crttbl1 (*1)	F00_crttbl1 (*1)
F01_Load3_insert_nonrecoverable	**FI1_Import1_insert**
F02_Delete not logged initiallyを設定し Active Logの出力を抑制した後　30%Delete	**FI2_Export1_del**
F03_reorgchk1_current (*1)	
F03_reorgchk2_update	
F04_reorg1_table	
F05_runstats1_table	

ユーティリティーテスト実行コマンド詳細-1

F00_crttbl1.ddl	DROP TABLE LD_AUTOSTORAGE ; CREATE TABLE LD_AUTOSTORAGE (COL1 INTEGER NOT NULL, L_ORDERKEY INTEGER NOT NULL, L_PARTKEY INTEGER NOT NULL, L_SUPPKEY INTEGER NOT NULL, L_QUANTITY FLOAT NOT NULL, L_EXTENDEDPRICE FLOAT NOT NULL, L_DISCOUNT FLOAT NOT NULL, L_TAX FLOAT NOT NULL, L_RETURNFLAG CHAR(1) NOT NULL, L_LINESTATUS CHAR(1) NOT NULL, L_SHIPDATE DATE NOT NULL, L_COMMITDATE DATE NOT NULL, L_RECEIPTDATE DATE NOT NULL, L_SHIPINSTRUCT CHAR(25) NOT NULL, L_SHIPMODE CHAR(10) NOT NULL, L_COMMENT VARCHAR(44) NOT NULL) in USERSPACE1 ; create index iLD_AUTOSTORAGE on LD_AUTOSTORAGE (col1) allow reverse scans;
F01_Load3_insert_nonrecoverable1.ddl	load from /testfiles/lineitem12GB/lineitem.tbl.10 , /testfiles/lineitem12GB/lineitem.tbl.11 , /testfiles/lineitem12GB/lineitem.tbl.12 of del MESSAGES /iselwork/Utillog/xxxx/loadmsg/xxxx insert into LD_AUTOSTORAGE nonrecoverable ;

特徴

- ✓ Load フェーズ　Loadデータの読み込みとDBへの書き出し量が多い
- ✓ Build フェーズ　物理I/Oは少ない

ユーティリティーテスト実行コマンド詳細-2

F02_Delete.sh	db2 -v +c "alter table LD_AUTOSTORAGE activate not logged initially" ; db2 -v "delete from (select col1 from LD_AUTOSTORAGE where mod (col1 , 10) in (1,3,9))" ; db2 -v commit ; 特徴 ✓ LOGを書き出さない設定 のためLOG書き出しは無しまたは少 ✓ 均等に削除させているため 表スキャンでDB Read 同量を DB Writeする ✓ 秒あたりの 物理 I/O 要求回数は最多
F03_reorgchk2_update.sh	db2 -v "reorgchk update statistics on table db2inst1.LD_AUTOSTORAGE“ 特徴 ほとんどDB Readのみ、LOG書き出しは少ない
F04_reorg1_table.sh	db2 -v "reorg table LD_AUTOSTORAGE" 特徴 Rebuild 前 全データ DB Read DB Write Rebuild では DBの読み込みが主 LOG書き出しは少ない
F05_runstats1_table.sh	db2 -v "runstats on table db2inst1.LD_AUTOSTORAGE" 特徴 DB Readのみ
FI1_Import1_insert1.ddl	import from /testfiles/lineitem0.5GB/lineitem.tbl.0.5GB of del COMMITCOUNT 10000 insert into LD_AUTOSTORAGE ; 特徴 (直前にダミーImportを行っているため Importデータの読み込みはなし) DB Writeと Log Write のOperation
FI2_Export1_del.ddl	export to /testfiles/exportdir/TEST_LD_AUTOSTORAGE.del of del select * from LD_AUTOSTORAGE with ur ; 特徴 直前にdb2stop/db2startを行っているため 全データ物理読み込みが行われる。

ユーティリティーテスト結果　物理CPU 12個

testitem	Avg elapse(sec)			CPU Usage:　us+sy			Avg wa		
	Encryption	Normal	Enc/Normal	Encryption	Normal	Enc/Normal	Encryption	Normal	
F01_Load3_insert_non recoverable1	2,234	2,299	97%	15.16	13.31	114%	1.61	1.85	
LOAD	831	897	93%	33.51	27.69	121%	4.29	4.69	全ケース LOAD元データの読み込みで　Disk Busy発生
BUILD	1,400	1,400	100%	4.28	4.12	104%	0.02	0.03	iostatではDBへの書き込みが主　他に比べると　物理Read Write が少ない
F02_Delete	5,951	5,586	107%	1.88	1.32	143%	2.29	1.97	DB読み書きで 暗号化DBのほうが遅い
F03_reorgchk2_update	654	626	104%	4.86	4.10	118%	2.78	2.79	全ケースDB読み込みで　DISK Busy発生指定
F04_reorg1_table	3,544	3,390	105%	3.39	2.87	118%	1.77	1.93	
F05_runstats1_table	477	485	98%	5.41	4.65	116%	1.78	1.98	
FI1_Import1_insert1	1,317	1,303	101%	5.04	4.92	102%	0.15	0.00	
FI2_Export1_del	283	287	99%	4.13	4.05	102%	0.90	0.99	他に比べると　物理Read Write が少ない

水色 104%以下　黄色 105%- 110%　ピンク　111%以上

ユーティリティーテスト結果　物理CPU 4個

testitem	Avg elapse(sec)			CPU Usage us+sy			Avg wa		
	Encryption	Normal	Enc/Normal	Encryption	Normal	Enc/Normal	Encryption	Normal	
F01_Load3_insert_nonrecoverable1	2,461	2,445	101%	36.44	32.96	111%	2.87	4.15	
LOAD	1,062	1,051	101%	66.32	59.09	112%	6.52	9.52	Load元データの読み込みで DISK Busyが発生。読み込みスピードはほぼ同じ。 通常DBのほうがBusy率が高い （Enc:60% Normal:82%）
BUILD	1,396	1,391	100%	13.76	13.27	104%	0.10	0.09	
F02_Delete	5,125	4,806	107%	6.43	4.76	135%	7.72	8.18	暗号化の負荷が出ていると考えられる。
F03_reorgchk2_update	650	622	105%	15.69	12.53	125%	8.97	8.13	暗号化の負荷が出ていると考えられる。
F04_reorg1_table	5,056	3,935	128%	11.33	9.75	116%	4.55	5.88	
索引の再作成開始まで	1,664	1,283	130%	6.52	2.99	218%	11.54	13.93	暗号化の負荷が出ていると考えられる。
索引の再作成	3,392	2,652	128%	13.88	13.01	107%	0.99	2.00	暗号化DB 4回実行のうち2回でdbdiskに対する読み込み要求が非常に遅い。（まだ要因不明）
F05_runstats1_table	481	478	101%	17.44	15.01	116%	4.45	4.05	
FI1_Import1_insert1	1,325	1,307	101%	14.32	13.72	104%	1.01	0.96	**Log Disk（ここが所要時間に差が出なかった要因）** 書き込み要求数(avg_w/s)はEnc/Normal 160%と 暗号化DBのほうが多い(1回あたりの書き込み量が異なる。)
FI2_Export1_del	277	283	98%	13.50	12.70	106%	2.47	2.66	

水色 104%以下　黄色 105%- 110%　ピンク　111%以上

ユーティリティーテスト結果　物理CPU 12個 vmstat Summary

		avg_r:	max_r:	avg_b:	max_b:	avg_us+sy:	max_us+sy:	avg_us_cpu:	avg_sy_cpu:	avg_wa_cpu:
F01_Load3_insert_nonrecoverable1	Encryption	3.57	36	0.77	15	15.16	70	14.59	0.56	1.61
	Normal	3.22	36	0.78	16	13.31	64	12.74	0.57	1.85
LOAD	Encryption	7.68	36	2.02	15	33.51	70	32.06	1.44	4.29
	Normal	6.52	36	1.97	16	27.69	64	26.27	1.42	4.69
BUILD	Encryption	1.14	17	0.02	2	4.28	15	4.25	0.04	0.02
	Normal	1.11	22	0.02	2	4.12	21	4.09	0.03	0.03
F02_Delete	Encryption	0.62	23	0.68	2	1.88	27	1.62	0.27	2.29
	Normal	0.53	22	0.73	2	1.32	17	0.97	0.35	1.97
F03_reorgchk2_update	Encryption	1.33	6	0.78	2	4.86	9	4.74	0.12	2.78
	Normal	1.11	6	0.76	2	4.10	8	3.97	0.13	2.79
F04_reorg1_table	Encryption	0.92	24	0.61	3	3.39	17	3.27	0.12	1.77
	Normal	0.83	18	0.73	7	2.87	13	2.72	0.15	1.93
F05_runstats1_table	Encryption	1.48	5	0.41	2	5.41	9	5.32	0.09	1.78
	Normal	1.18	3	0.45	2	4.65	7	4.57	0.08	1.98
FI1_Import1_insert1	Encryption	1.26	12	0.16	2	5.04	8	4.07	0.97	0.15
	Normal	1.18	17	0.09	2	4.92	7	4.05	0.87	0.00
FI2_Export1_del	Encryption	1.11	5	0.25	3	4.13	21	4.01	0.12	0.90
	Normal	1.09	20	0.25	3	4.05	7	3.96	0.09	0.99

ユーティリティーテスト結果　物理CPU 12個 iostat Summary

		Disk	avg_%util	avg_wrqm/s	avg_r/s	avg_w/s	avg_rkB/s	avg_wkB/s	avgrq-sz	avgqu-sz	avg_await	avg_r_await	avg_w_await	avg_svctm
F01_Load3_insert_nonrecoverable1	Encryption	data	33.75	0.00	319.70	0.00	40,921.25	0.00	95.90	0.60	1.15	1.15	0.00	0.63
		encdb	16.20	805.93	0.69	491.58	3.58	53,350.63	104.98	2.13	2.22	0.11	2.17	0.20
		enclog	1.54	0.00	0.00	56.88	0.02	255.31	8.60	0.02	0.20	0.07	0.20	0.20
	Normal	data	36.59	0.00	311.16	0.00	39,828.43	0.00	100.46	0.66	1.14	1.14	0.00	0.63
		noencdb	16.12	775.14	0.61	469.25	3.23	51,913.55	110.79	2.23	2.67	0.12	2.60	0.23
		noenclog	0.91	0.00	0.00	37.28	0.02	176.66	8.93	0.01	0.22	0.06	0.22	0.23
LOAD	Encryption	data	**90.50**	0.00	856.92	0.00	109,684.00	0.00	256.00	1.62	3.06	3.06	0.00	1.67
		encdb	40.63	84.07	1.52	1,091.10	8.10	132,109.75	242.26	4.99	4.35	0.06	4.35	0.38
		enclog	3.92	0.00	0.00	112.70	0.04	525.69	9.71	0.04	0.44	0.12	0.44	0.44
	Normal	data	**93.58**	0.00	796.28	0.00	101,922.20	0.00	256.00	1.68	2.90	2.90	0.00	1.60
		noencdb	38.74	53.11	1.49	998.32	8.02	122,699.25	246.19	4.98	4.83	0.07	4.83	0.39
		noenclog	2.19	0.00	0.00	58.90	0.04	306.44	10.45	0.02	0.50	0.12	0.50	0.53
BUILD	Encryption	data	0.04	0.00	0.53	0.00	67.28	0.00	0.69	0.00	0.00	0.00	0.00	0.00
		encdb	1.53	1,239.53	0.06	125.68	0.24	6,575.14	23.41	0.44	0.96	0.14	0.89	0.09
		enclog	0.13	0.00	0.00	23.63	0.00	94.38	7.95	0.00	0.05	0.02	0.05	0.05
	Normal	data	0.13	0.00	1.03	0.00	132.42	0.00	0.91	0.00	0.01	0.01	0.00	0.00
		noencdb	1.65	1,237.20	0.04	131.03	0.17	6,667.60	24.13	0.48	1.28	0.16	1.17	0.13
		noenclog	0.10	0.00	0.00	23.46	0.00	93.72	7.96	0.00	0.05	0.01	0.05	0.05
F02_Delete (*1)	Encryption	encdb	**71.04**	2,933.06	4,031.83	1,384.20	17,330.25	17,308.43	12.25	1.25	0.23	0.10	0.27	0.13
	Normal	noencdb	**74.59**	3,127.97	4,296.67	1,474.21	18,468.63	18,452.53	12.46	1.35	0.25	0.11	0.31	0.13
F03_reorgchk2_update (*1)	Encryption	encdb	**68.12**	0.01	1,329.09	0.03	158,074.25	0.18	243.03	0.81	0.77	0.77	0.00	0.62
	Normal	noencdb	**67.41**	0.01	1,382.89	0.04	165,038.25	0.22	246.29	0.80	0.79	0.79	0.00	0.62
F04_reorg1_table	Encryption	encdb	47.54	349.43	373.21	379.66	45,929.43	39,611.70	183.09	2.31	2.25	1.29	2.68	0.57
		enclog	0.62	0.00	0.00	23.06	0.01	92.44	4.09	0.01	0.13	0.01	0.13	0.13
	Normal	noencdb	49.64	365.52	536.35	379.31	47,987.30	41,572.25	163.86	2.50	2.00	1.09	2.37	0.50
		noenclog	0.86	0.00	0.00	21.38	0.01	86.43	3.44	0.01	0.16	0.01	0.16	0.16
F05_runstats1_table (*1)	Encryption	encdb	40.99	0.02	1,096.58	0.05	139,861.00	0.24	255.04	0.42	0.38	0.38	0.00	0.37
	Normal	noencdb	41.35	0.02	1,078.80	0.06	137,580.00	0.35	255.01	0.43	0.40	0.40	0.00	0.38
FI1_Import1_insert1	Encryption	encdb	1.95	1,017.21	1.12	86.58	5.91	4,498.01	104.12	0.03	0.37	0.04	0.37	0.23
		enclog	14.87	0.00	0.21	701.86	1.69	9,910.15	30.18	0.15	0.21	0.18	0.21	0.21
	Normal	noencdb	2.73	1,073.64	1.14	131.87	5.98	5,084.52	75.64	0.04	0.29	0.02	0.29	0.20
		noenclog	7.56	0.00	0.21	319.84	1.71	9,356.02	59.85	0.08	0.24	0.19	0.24	0.24
FI2_Export1_del (*1)	Encryption	data	5.57	0.05	0.00	57.89	0.00	29,529.23	211.73	7.87	27.27	0.00	27.27	0.19
		encdb	15.65	0.03	155.57	0.06	19,421.57	0.29	251.72	0.19	1.48	1.48	0.01	1.16
	Normal	data	5.43	0.04	0.00	55.19	0.00	28,148.60	215.38	7.53	27.54	0.00	27.54	0.20
		noencdb	17.96	0.04	153.37	0.11	19,116.17	0.73	251.33	0.21	1.57	1.57	0.25	1.30

rrqmは全ケース0のため省略　(*1) LOG DISKの値があまりにも小さいため省略

目次

- 第2部　パフォーマンステストレポート
  - プロジェクト概要
    - テスト項目
    - 結果サマリー
  - 構成　設定
  - OLTP パフォーマンステスト テスト結果
  - ユーティリティテストシナリオ　テスト結果
    - Load Import
    - Backup Restore
    - Key Rotation
  - PMR / APAR
  - (参考)暗号化データベースの作成手順
  - DB2 構成情報詳細 (db2level / db2set / DBM CFG / DB CFG)

ユーティリティーテストシナリオ　Backup Restore

太字部分のみ所要時間計測

通常DB環境Backup Restore	暗号化DB環境Backup Restore
FR1_RESTORE_INIT_BACKUPIMAGE	FR1_RESTORE_INIT_BACKUPIMAGE
FB2_Backup_DB1	FB2_Backup_DB_ENC1.upd_db_cfg
FB2_Backup_DB1_db2ckbkp	**FB2_Backup_DB1**
FR2_RESTORE_New_crtedFB21	**FB2_Backup_DB1_db2ckbkp**
dropdbNEWDB	**FR2_RESTORE_New_crtedFB2_ENCDB1**
FB2_Backup_DB2COMPRESS	dropdbNEWDB
FR2_RESTORE_New_crtedFB22	FB2_Backup_DB_ENC_COMPRESS2.upd_db_cfg
dropdbNEWDB	**FB2_Backup_DB2COMPRESS**
	FB2_Backup_DB2_db2ckbkp
	FR2_RESTORE_New_crtedFB2_ENCDB2
	dropdbNEWDB
	FB2_Backup_DB_ENC_HIRA3.upd_db_cfg
	FB2_Backup_DB3
	FB2_Backup_DB3_db2ckbkp
	FR2_RESTORE_New_crtedFB2_ENCDB3
	dropdbNEWDB

ENCRLIB, ENCROPTS 更新 暗号化

ENCRLIB, ENCROPTS 更新 (暗号化+圧縮)

ENCRLIB, ENCROPTS 更新 (平文)

ユーティリティーテスト実行コマンド詳細-3 Backup Restore 通常DB環境

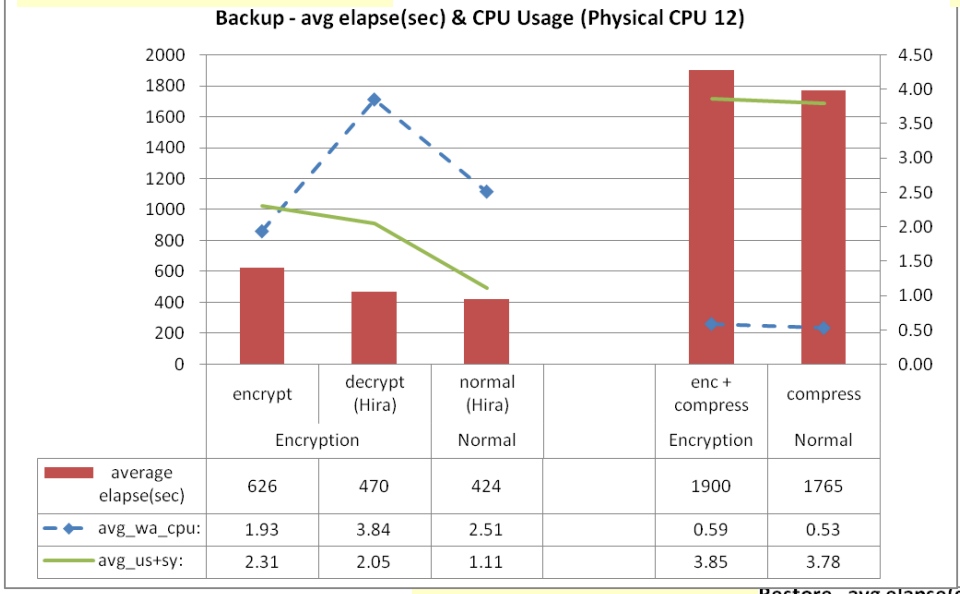
Backup	
FB2_Backup_DB1.sh	db2 –v backup DATABASE DBNOENC to /dbalt/testfiles/exportdir/FB2_Backup_DB
FB2_Backup_DB2COMPRESS.sh	db2 -v backup DATABASE DBNOENC to /dbalt/testfiles/exportdir/FB2_Backup_DB COMPRESS
db2ckbkp バックアップの検査コマンド	
FB2_Backup_DB*_db2ckbkp.sh	db2ckbkp -h /dbalt/testfiles/exportdir/FB2_Backup_DB/DBNOENC.0.db2noenc.DBPART000.xxxxxxxxxxxxxx.001
Restore	
FR2_RESTORE_New_crtedFB2*.sh	db2 -v RESTORE DATABASE DBNOENC from /dbalt/testfiles/exportdir/FB2_Backup_DB into NEWDB

ユーティリティーテスト実行コマンド詳細-3 Backup Restore 暗号化DB環境

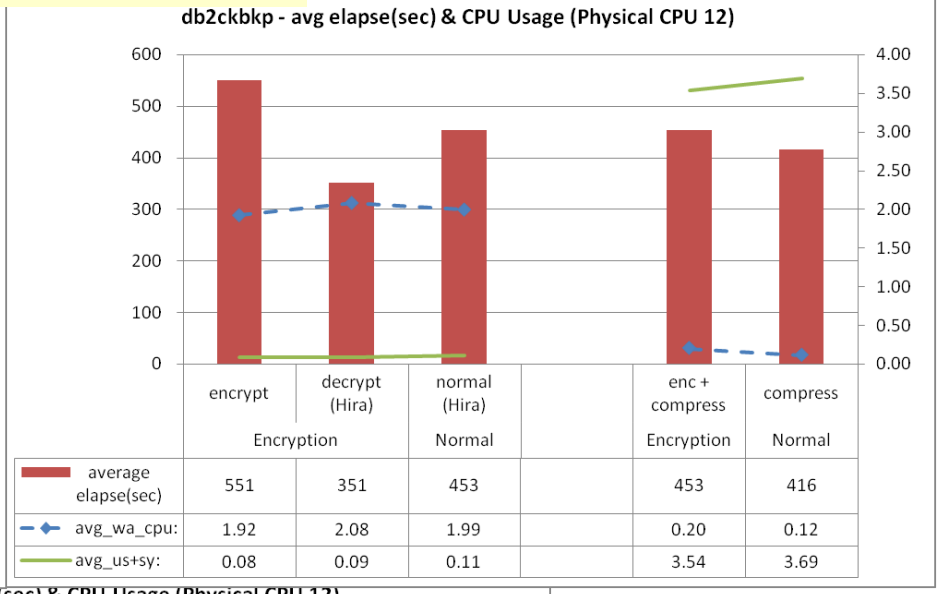
ENCRLIB, ENCROPTS 更新	
(暗号化) FB2_Backup_DB_ENC1.upd_db_cfg.sh	db2 +o connect to DBENC db2 -v "update db cfg for DBENC using ENCRLIB $HOME/sqllib/lib64/libdb2encr.so ENCROPTS 'CIPHER=AES:MODE=CBC:KEY LENGTH=256'" db2 connect reset
(暗号化+圧縮) FB2_Backup_DB_ENC_COMPRESS2.upd_db_cfg	db2 +o connect to DBENC db2 -v "update db cfg for DBENC using ENCRLIB /opt/ibm/db2/V10.5/lib64/libdb2compr_encr.so ENCROPTS 'CIPHER=AES:MODE=CBC:KEY LENGTH=256'" db2 connect reset
(平文) FB2_Backup_DB_ENC_HIRA3.upd_db_cfg	db2 +o connect to DBENC db2 update db cfg for DBENC using ENCRLIB NULL ENCROPTS NULL db2 connect reset
Backup	
FB2_Backup_DB*.sh	db2 -v backup DATABASE DBENC to /dbalt/testfiles/exportdir/FB2_Backup_DB
FB2_Backup_DB2COMPRESS.sh	db2 -v backup DATABASE DBENC to /dbalt/testfiles/exportdir/FB2_Backup_DB COMPRESS
db2ckbkp バックアップの検査コマンド	
FB2_Backup_DB*_db2ckbkp.sh	db2ckbkp -h /dbalt/testfiles/exportdir/FB2_Backup_DB/DBENC.0.db2enc.DBPART000.xxxxxxxxxxxxxx.001
Restore	
FR2_RESTORE_New_crtedFB2_ENCDB*.ddl	RESTORE DATABASE DBENC from /dbalt/testfiles/exportdir/FB2_Backup_DB into NEWDB ENCRYPT CIPHER AES KEY LENGTH 256 MASTER KEY LABEL DB2_SYSGEN_db2enc_DBENC_2015-03-05-16.56.20.;

ユーティリティーテスト結果 Backup Restore　物理CPU 12個

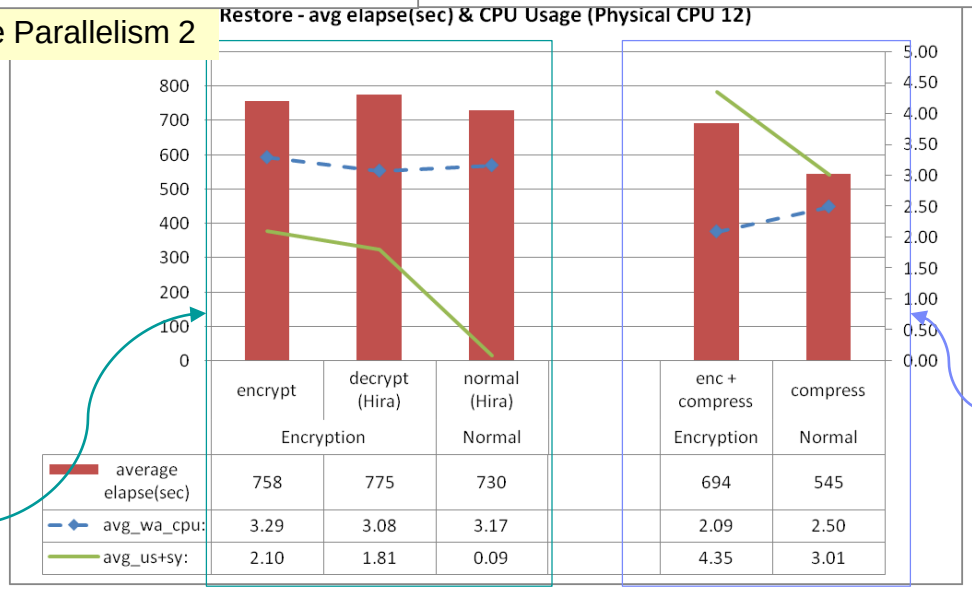
Backup : Parallelism 3　暗号化による影響が出ている



(参考)db2ckbkp



Restore Parallelism 2



Restore : Disk Busyのため　所要時間の差があまり見られない

圧縮されているバックアップイメージのRestore

暗号化による影響が出ている

ユーティリティーテスト結果 Backup Restore　物理CPU 12個

testitem	Env	Option	average elapse		average speed		avg_us+sy:		avg wa	backup image(byte)	
			(sec)	/Normal	(GB/min)	/Normal	%	/Normal			
Backup	Encryption	encrypt	626	147%	6.13	68%	2.31	208%	1.93	68,518,129,664	
		decrypt(plain)	470	111%	8.14	90%	2.05	185%	3.84	68,518,129,664	
	Normal	normal(plain)	424	(n/a)	9.03	(n/a)	1.11	(n/a)	2.51	68,518,129,664	normal(plain) は DISK Busy のため。 Diskがもっと早ければ早くなるだろう
	Encryption	enc + compress	1900	108%	1.07	93%	3.85	102%	0.59	36,264,448,000	PMR 73496,999,760 db2diag.logに不要なメッセージが出ています。
	Normal	compress	1765	(n/a)	1.15	(n/a)	3.78	(n/a)	0.53	36,214,104,064	
db2ckbkp	Encryption	encrypt	551	121%	7.16	82%	0.08	75%	1.92	68,518,129,664	Disk Busyのため。 Diskがもっと早ければ早くなるだろう
		decrypt(plain)	351	77%	10.98	125%	0.09	77%	2.08	68,518,129,664	
	Normal	normal(plain)	453	(n/a)	8.78	(n/a)	0.11	(n/a)	1.99	68,518,129,664	
	Encryption	enc + compress	453	109%	4.48	92%	3.54	96%	0.20	36,264,448,000	
	Normal	compress	416	(n/a)	4.89	(n/a)	3.69	(n/a)	0.12	36,214,104,064	
Restore	Encryption	encrypt	758	104%	5.07	97%	2.10	2298%	3.29	68,518,129,664	Disk Busyのため。Diskがもっと早ければ早くなるだろう
		decrypt(plain)	775	106%	4.95	94%	1.81	1976%	3.08	68,518,129,664	
	Normal	normal(plain)	730	(n/a)	5.24	(n/a)	0.09	(n/a)	3.17	68,518,129,664	
	Encryption	enc + compress	694	127%	2.92	79%	4.35	145%	2.09	36,264,448,000	
	Normal	compress	545	(n/a)	3.72	(n/a)	3.01	(n/a)	2.50	36,214,104,064	

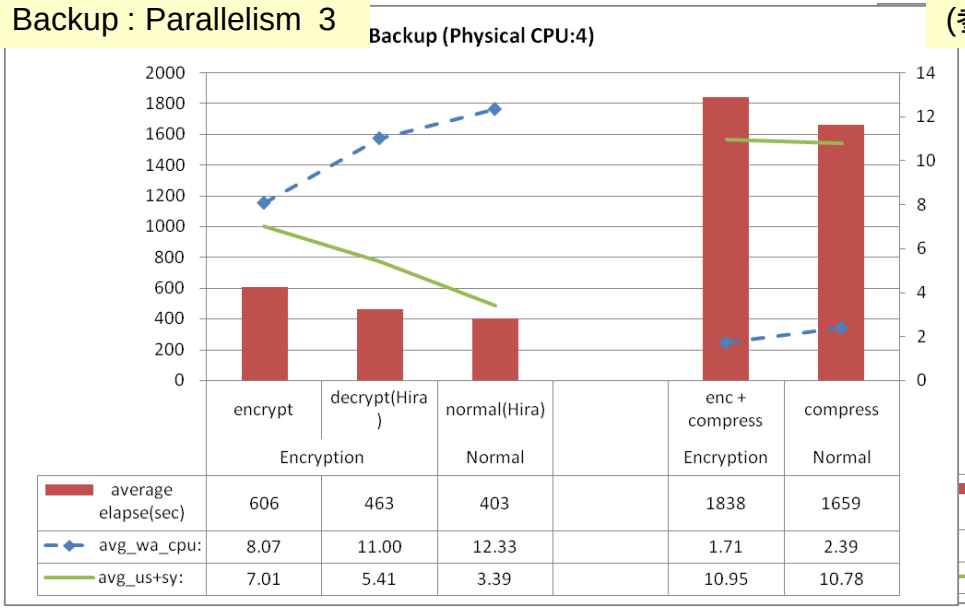
ユーティリティーテスト結果 Backup Restore iostat 物理CPU 12個

					avg_%util	avg_wrqm/s	avg_r/s	avg_w/s	avg_rkB/s	avg_wkB/s	avgrq-sz	avgqu-sz	avg_await	avg_r_await	avg_w_await	avg_svctm
Backup	Encryption	encrypt (*1)	data	dm-5	19.45	0.04	0.00	202.21	0.00	103,268.67	988.05	27.41	127.81	0.00	127.81	0.91
			encdb	dm-4	53.00	0.03	827.28	0.05	104,565.00	0.31	243.00	0.53	0.66	0.66	0.48	0.65
		decrypt(plain) (*1)	data	dm-5	25.21	0.91	0.00	263.81	0.00	134,235.00	954.80	35.50	125.65	0.00	125.65	0.89
			encdb	dm-4	**66.42**	0.05	1,077.27	0.07	136,146.67	0.43	236.87	0.67	0.63	0.64	1.54	0.63
	Normal	normal(plain)	data	dm-5	29.16	0.03	0.00	291.20	0.00	148,733.33	903.65	41.18	124.26	0.00	124.26	1.26
			noencdb	dm-8	**85.81**	0.20	1,187.57	120.14	150,126.67	15,330.70	244.44	0.88	0.69	1.29	3.13	0.67
			noenclog	dm-6	2.57	0.02	1.21	26.87	19.37	12,405.17	105.41	1.54	8.04	0.35	8.23	1.33
	Encryption	enc + compress (*1)	data	dm-5	3.04	0.30	0.00	36.36	0.00	18,468.33	988.29	4.21	109.76	0.00	109.76	0.79
			encdb	dm-4	13.08	0.01	277.21	0.02	35,051.67	0.10	252.09	0.13	0.48	0.48	0.09	0.48
	Normal	compress (*1)	data	dm-5	3.32	0.16	0.00	38.76	0.00	19,767.47	977.85	4.64	110.13	0.00	110.13	0.79
			noencdb	dm-8	14.32	0.03	298.04	0.06	37,686.20	1.55	251.21	0.14	0.49	0.49	0.07	0.49
db2ckbkp	Encryption	encrypt	data	dm-5	**91.22**	0.00	862.83	6.13	110,513.63	3,126.26	265.04	2.55	3.72	2.04	4.90	1.12
		decrypt(plain)	data	dm-5	**95.41**	0.00	955.54	13.75	122,317.00	7,012.51	271.31	3.52	4.48	1.96	10.67	1.04
	Normal	normal(plain)	data	dm-5	**96.43**	0.00	1,041.56	12.82	133,366.00	6,538.91	272.42	3.54	4.86	1.90	9.42	1.03
	Encryption	enc + compress	data	dm-5	12.84	0.05	131.19	1.54	16,812.13	752.66	186.71	0.38	2.58	2.04	6.84	1.44
	Normal	compress	data	dm-5	8.96	0.00	143.59	1.91	18,376.80	966.58	144.38	0.36	0.99	0.64	5.72	0.37
Restore (*1)	Encryption	encrypt	data	dm-5	**71.88**	0.00	492.30	0.00	63,090.27	0.00	211.39	1.33	2.40	2.40	0.00	1.30
			encdb	dm-4	52.02	0.02	0.45	892.30	1.96	179,115.67	411.34	26.55	31.44	0.10	31.91	0.60
		decrypt(plain)	data	dm-5	**60.60**	0.00	455.43	0.00	58,305.70	0.00	216.75	1.14	2.70	2.70	0.00	1.49
			encdb	dm-4	50.19	0.02	0.29	872.65	1.35	173,795.67	404.95	25.61	30.26	0.13	30.36	0.59
	Normal	normal(plain)	data	dm-5	**69.94**	0.00	489.74	0.00	62,707.40	0.00	206.31	1.31	2.19	2.19	0.00	1.18
			noencdb	dm-8	52.51	0.03	0.16	928.51	0.81	186,018.67	415.87	27.59	32.53	0.15	32.60	0.60
	Encryption	enc + compress	data	dm-5	11.38	0.00	83.64	0.00	10,683.13	0.00	82.29	0.21	1.00	1.00	0.00	0.61
			encdb	dm-4	52.71	0.03	0.49	984.33	2.13	193,887.00	422.54	28.45	34.08	0.14	34.27	0.56
	Normal	compress	data	dm-5	15.10	0.00	102.89	0.00	13,178.67	0.00	93.60	0.28	1.64	1.64	0.00	1.13
			noencdb	dm-8	**64.34**	0.05	0.66	1,282.82	3.58	243,447.67	459.71	35.89	42.93	0.07	43.18	0.58

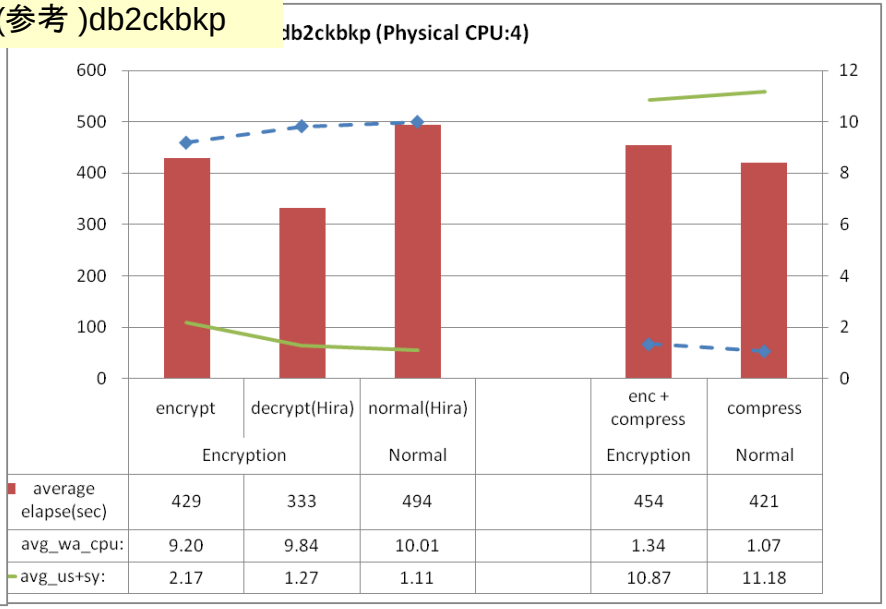
rrqmは全ケースOのため省略 (*1) LOG DISKの値があまりにも小さいため省略

ユーティリティーテスト結果 Backup Restore 物理CPU 4個

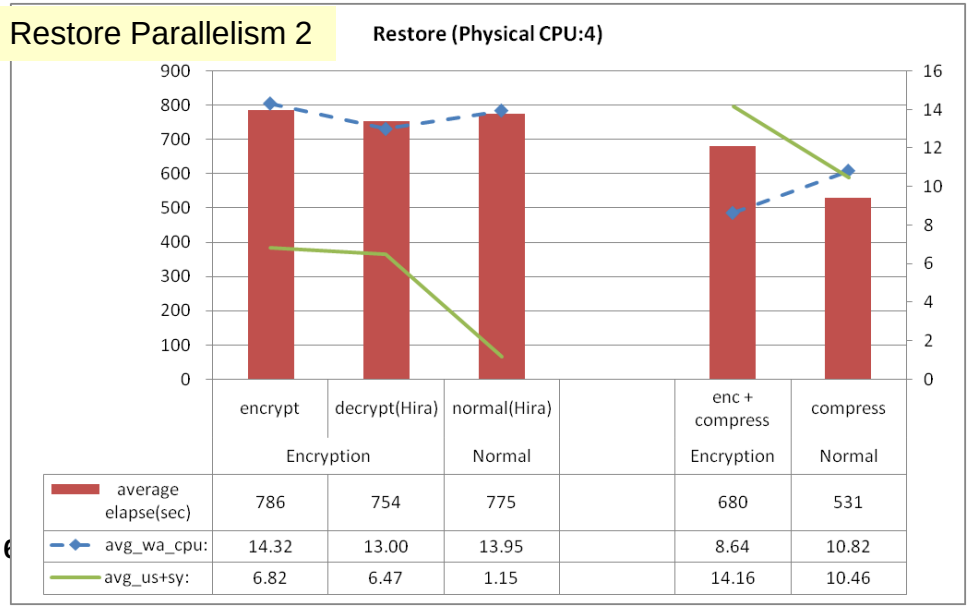
Backup : Parallelism 3



(参考)db2ckbkp



Restore Parallelism 2



Parallelismの指定なし。

このため 物理CPUの個数にかかわらず

Backup : Parallelism = 3

Restore : Parallelism = 2

結果は 物理CPU12個のケースと同じ

ユーティリティーテスト結果 Backup Restore 物理CPU 4個

testitem	Env	Option	average elapse		average speed		avg_us+sy:		avg wa	backup image(byte)	
			(sec)	/Normal	(GB/min)	/Normal	%	/Normal			
Backup	Encryption	encrypt	606	150%	6.32	67%	7.01	207%	8.07	68,518,129,664	
		decrypt(plain)	463	115%	8.27	87%	5.41	160%	11.00	68,518,129,664	dbdisk Utilization 66.83%
	Normal	normal(plain)	403	(n/a)	9.51	(n/a)	3.39	(n/a)	12.33	68,518,129,664	1秒当たりのdbdiskへの読み出し要求が一番多い。 dbdisk utilization 85.41%
	Encryption	enc + compress	1838	111%	1.10	90%	10.95	102%	1.71	36,264,448,000	PMR 73496,999,760 db2diag.logに不要なメッセージが出ています。
	Normal	compress	1659	(n/a)	1.22	(n/a)	10.78	(n/a)	2.39	36,214,104,064	
db2ckbkp	Encryption	encrypt	429	87%	9.12	116%	2.17	196%	9.20	68,518,129,664	バックアップデータ読みによるDisk Busy
		decrypt(plain)	333	67%	11.54	147%	1.27	115%	9.84	68,518,129,664	バックアップデータ読みによるDisk Busy
	Normal	normal(plain)	494	(n/a)	7.84	(n/a)	1.11	(n/a)	10.01	68,518,129,664	バックアップデータ読みによるDisk Busy
	Encryption	enc + compress	454	108%	4.47	93%	10.87	97%	1.34	36,264,448,000	
	Normal	compress	421	(n/a)	4.81		11.18	(n/a)	1.07	36,214,104,064	
Restore	Encryption	encrypt	786	101%	4.88	98%	6.82	591%	14.32	68,518,129,664	
		decrypt(plain)	754	97%	5.08	102%	6.47	561%	13.00	68,518,129,664	
	Normal	normal(plain)	775	(n/a)	4.96	(n/a)	1.15	(n/a)	13.95	68,518,129,664	
	Encryption	enc + compress	680	128%	2.98	78%	14.16	135%	8.64	36,264,448,000	
	Normal	compress	531	(n/a)	3.81	(n/a)	10.46	(n/a)	10.82	36,214,104,064	

目次

- 第2部　パフォーマンステストレポート
  - プロジェクト概要
    - テスト項目
    - 結果サマリー
  - 構成　設定
  - OLTP パフォーマンステスト テスト結果
  - ユーティリティテストシナリオ　テスト結果
    - Load Import
    - Backup Restore
    - Key Rotation
  - PMR / APAR
  - (参考)暗号化データベースの作成手順
  - DB2 構成情報詳細 (db2level / db2set / DBM CFG / DB CFG)

Key Rotation 1

1. 状況確認

"SELECT * FROM TABLE (SYSPROC.ADMIN_GET_ENCRYPTION_INFO())“

OBJECT_NAME	NEWDB
OBJECT_TYPE	DATABASE
ALGORITHM	AES
ALGORITHM_MODE	CBC
KEY_LENGTH	256
MASTER_KEY_LABEL	DB2_SYSGEN_db2enc_DBENC_2015-03-05-16.56.20
KEYSTORE_NAME	/home/db2enc/sqllib/NativeEncryption.p12
KEYSTORE_TYPE	PKCS12
KEYSTORE_HOST	db2encs
KEYSTORE_IP	192.168.10.6
KEYSTORE_IP_TYPE	IPV4
PREVIOUS_MASTER_KEY_LABEL	DB2_SYSGEN_db2enc_DBENC_2015-03-05-16.56.20
AUTH_ID	DB2ENC
APPL_ID	*LOCAL.db2enc.150325042037
ROTATION_TIME	2015-03-25-13.20.37.000000

Key Rotation 2

2 . AES キーファイル作成　(256bit AES key 32byte)

head –c 32 /dev/random > $HOME/sqllib/DB2_qit_db2enc_DBENC_2015-03-25-13.30

[13:30:37 db2enc@db2encs ~]$ head -c 32 /dev/random > $HOME/sqllib/DB2_qit_db2enc_DBENC_2015-03-25-13.30

[13:35:57 db2enc@db2encs ~]$ od -x $HOME/sqllib/DB2_qit_db2enc_DBENC_2015-03-25-13.30

0000000 df9a 19ab 55dc ef87 b99f c017 ecde b060

0000020 4eb4 a1fe 7120 12d3 6677 0e0a 534e 1d17

0000040

[13:36:16 db2enc@db2encs ~]$

AIX環境　Linuxでは head -c 32 .. で32バイトのファイルが作成できる
AIXでは33バイトになる。AIXでは
dd count=1 bs=32 if=/dev/random > random.key
といったコマンドで　32バイトのランダムファイルが作成可能

3 .マスターキーをキーストアに作成する

$HOME/sqllib/gskit/bin/**gsk8capicmd_64 –secretkey –add -db $HOME/sqllib/NativeEncryption.p12 -label DB2_qit_db2enc_DBENC_2015-03-25-13.30 -stashed -file $HOME/sqllib/DB2_qit_db2enc_DBENC_2015-03-25-13.30**

[13:36:16 db2enc@db2encs ~]$ $HOME/sqllib/gskit/bin/gsk8capicmd_64 -secretkey -add -db

$HOME/sqllib/NativeEncryption.p12 -label DB2_qit_db2enc_DBENC_2015-03-25-13.30 -stashed -file $HOME/sqllib/DB2_qit_db2enc_DBENC_2015-03-25-13.30

[13:37:03 db2enc@db2encs ~]$

#確認

$HOME/sqllib/gskit/bin/**gsk8capicmd_64 –cert –list -db $HOME/sqllib/NativeEncryption.p12 -stashed**

[13:37:03 db2enc@db2encs ~]$ $HOME/sqllib/gskit/bin/gsk8capicmd_64 -cert -list -db $HOME

/sqllib/NativeEncryption.p12 -stashed

証明書が見つかりました

* デフォルト, - 個人, ! トラステッド, # secret key

#　　DB2_SYSGEN_db2enc_DBENC_2015-02-25-10.18.10

#　　**DB2_qit_db2enc_DBENC_2015-03-25-13.30**

[13:37:23 db2enc@db2encs ~]$

Key Rotation 3

4 . Key Rotation Procedure の実行

DBへ接続した状態で開始

[13:37:23 db2enc@db2encs ~]$ db2 connect

データベース接続情報

データベース・サーバー = DB2/LINUXX8664 10.5.5
SQL 許可 ID = DB2ENC
ローカル・データベース別名 = NEWDB

[13:39:09 db2enc@db2encs ~]$ date
2015年 3月 25日 水曜日 13:39:09 JST
[13:39:09 db2enc@db2encs ~]$ db2 "**CALL SYSPROC.ADMIN_ROTATE_MASTER_KEY('DB2_qit_db2enc_DBENC_2015-03-25-13.30')**"

出力パラメーターの値

パラメーター名: LABEL
パラメーター値: DB2_qit_db2enc_DBENC_2015-03-25-13.30

リターン状況 = 0
[13:39:09 db2enc@db2encs ~]$ date
2015年 3月 25日 水曜日 13:39:09 JST
[13:39:09 db2enc@db2encs ~]$

db2diag.log に次のようなLOGが記録される

2015-03-25-13.39.09.459766+540 I827186882E551 LEVEL: Event
PID : 3135 TID : 140736930506496 PROC : db2sysc 0
INSTANCE: db2enc NODE : 000 DB : NEWDB
APPHDL : 0-11 APPID: *LOCAL.db2enc.150325042943
AUTHID : DB2ENC HOSTNAME: db2encs
EDUID : 25 EDUNAME: db2agent (NEWDB) 0
FUNCTION: DB2 UDB, bsu security, sqlexRotateMasterKey, probe:1052
DATA #1 : String, 36 bytes
Key Rotation successful using label:
DATA #2 : String, 18 bytes
DB2_qit_db2enc_DBENC_2015-03-25-13.30

Key Rotation 4

5. 変更後確認

"SELECT * FROM TABLE (SYSPROC.ADMIN_GET_ENCRYPTION_INFO())“

	変更前	変更後
OBJECT_NAME	NEWDB	NEWDB
OBJECT_TYPE	DATABASE	DATABASE
ALGORITHM	AES	AES
ALGORITHM_MODE	CBC	CBC
KEY_LENGTH	256	256
MASTER_KEY_LABEL	DB2_SYSGEN_db2enc_DBENC_2015-03-05-16.56.20	**DB2_qit_db2enc_DBENC_2015-03-25-13.30**
KEYSTORE_NAME	/home/db2enc/sqllib/NativeEncryption.p12	/home/db2enc/sqllib/NativeEncryption.p12
KEYSTORE_TYPE	PKCS12	PKCS12
KEYSTORE_HOST	db2encs	db2encs
KEYSTORE_IP	192.168.10.6	192.168.10.6
KEYSTORE_IP_TYPE	IPV4	IPV4
PREVIOUS_MASTER_KEY_LABEL	DB2_SYSGEN_db2enc_DBENC_2015-03-05-16.56.20	DB2_SYSGEN_db2enc_DBENC_2015-03-05-16.56.20
AUTH_ID	DB2ENC	DB2ENC
APPL_ID	*LOCAL.db2enc.150325042037	*LOCAL.db2enc.150325042943
ROTATION_TIME	2015-03-25-13.20.37.000000	**2015-03-25-13.39.09.000000**

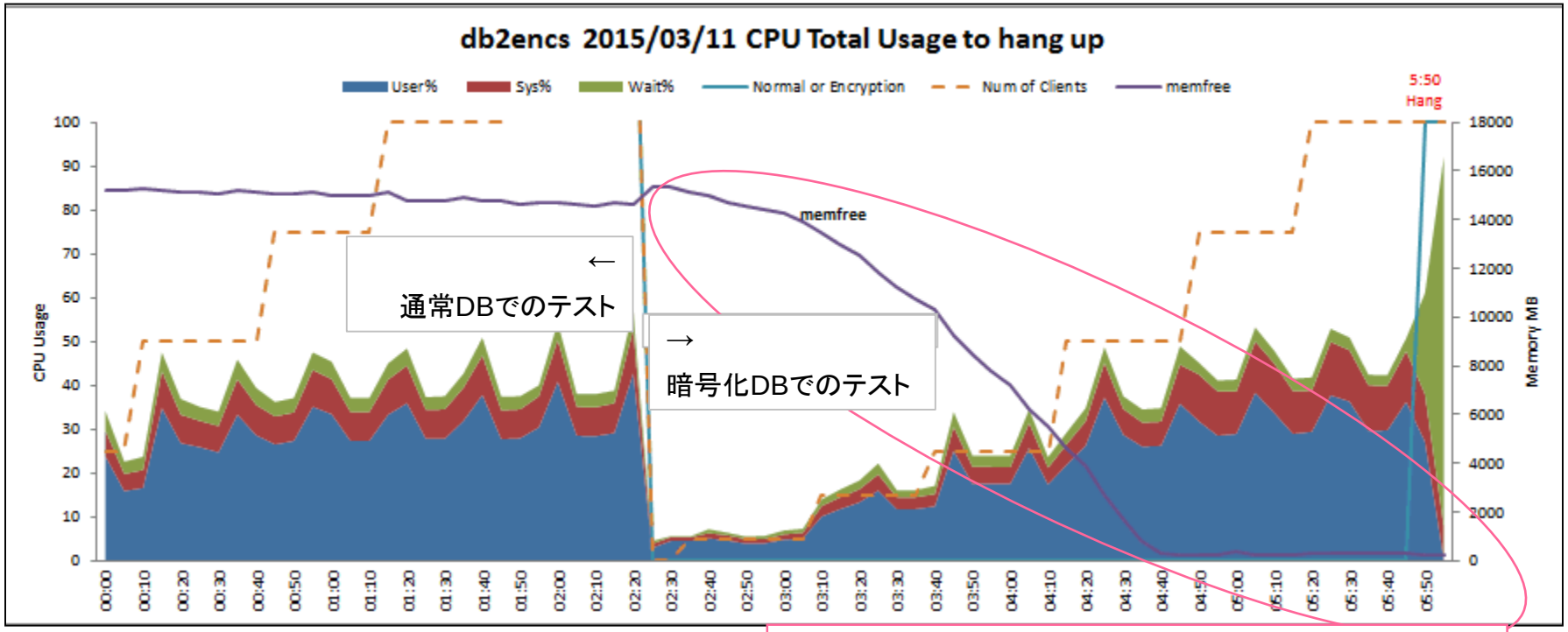
目次

- 第2部　パフォーマンステストレポート
  - プロジェクト概要
    - テスト項目
    - 結果サマリー
  - 構成　設定
  - OLTP パフォーマンステスト テスト結果
  - ユーティリティテストシナリオ　テスト結果
    - Load Import
    - Backup Restore
    - Key Rotation
  - PMR / APAR
  - (参考)暗号化データベースの作成手順
  - DB2 構成情報詳細　(db2level / db2set / DBM CFG / DB CFG)

PMR1 70704,999,760

DB2 V10.5 FP5では 暗号化DBの時のみ 大きなメモリーリークが発生し システムハングとなってしまった。

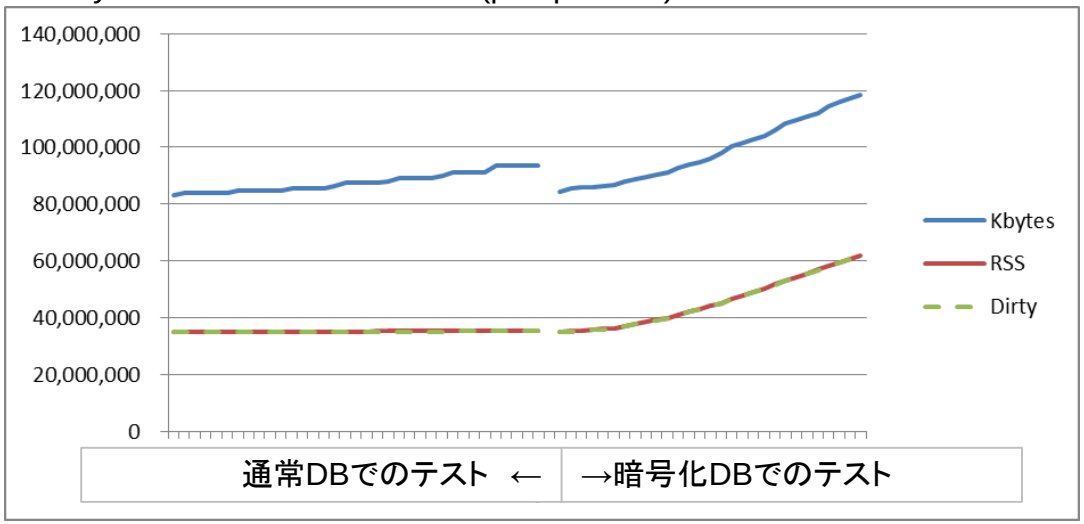
db2pd memsetsで取得されている値はあまり違いは見られない



DB2暗号化機能を使用したDBでのトランザクションを実行していると メモリーのfreeが どんどん減少してしい 最終的にシステムハングにいたってしまった。

PMR1 70704,999,760

db2syscのメモリー使用量の推移 (pmapで確認)



Kbytes: キロバイト単位のマップサイズ

RSS: キロバイト単位の常駐メモリサイズ

Dirty: キロバイト単位のダーティーページ(共有とプライベート両方)

pmapの出力から [anon]で 131072 (kB)が複数個 新規にアロケーションされている。

おおよその計算で

DBDISK 80MB/sec LOGDISK 40MB/sec の書き込みを5分実行して 131072(kB) x 9 のメモリーリークが発生

(80+40)*60*5/9=4000 MBの物理書き込みで 131072(kB) 一つの メモリーリークが発生することになる

PMR1 APAR IT08289: PRIVATE MEMORY LEAK DUE TO NATIVE ENCRYPTION.

Abstract
IT08289: PRIVATE MEMORY LEAK DUE TO NATIVE ENCRYPTION.

Error description:
The memory consumption on db2sysc process keeps growing only when native encryption is enabled.
For example, the private segments (Esid 10,11,12.. in svmon) keep growing in AIX systems, and [anon] blocks in pmap keep increasing in Linux systems.

However, the DB2 memory statistics shows no leak sign in the PRIVATE set, db2pd -dbptnmem and db2pd -memblock shows stable memory stats on private memory usage.

The malloc debug in AIX shows one of major leak is observed in the following code path.

0x090000000004a428 malloc_common_debugging
0x090000001a0d6d0c default_malloc_ex
0x090000001a0d7e9c C101_CRYPTO_malloc@AF28_12
0x090000001a07bf94 efCRYPTO_malloc
0x090000001a083b7c efCRYPTO_calloc
0x0900000019f99098 ICCC_EVP_CIPHER_CTX_new@AF299_235
0x0900000019f96e08 ICCC_EVP_CIPHER_CTX_new
0x0900000019f8d2b4 ICC_EVP_CIPHER_CTX_new
0x0900000002b62300 cryptSetupEncryptCipherCtx
0x090000000204fcc8
sqlexRedeemCipherTicket__FP17sqlexCipherTicketPUcUlP5sqlca
0x0900000002339720
sqlpEncrypt__FCPCvCUlPvT2P17sqlexCipherTicketPUcPib
0x0900000003b64bb8
sqlpgEncryptUserDataInNLogPages__FCPvPvCUsP17sqlexCipherTicketC
0x0900000005ab5b80
sqlpgWriteNLogPagesInternal__FR12SQLO_FHANDLECPvPvClCUlCPUlCUsP
0x0900000005a6c388
sqlpgWriteNLogPagesInternal__FR12SQLO_FHANDLECPvPvClCUlCPUlCUsP
0x0900000005a6c184
sqlpgWriteNLogPages__FR12SQLO_FHANDLECPvPvCUlClT4CPUlCUsP17sqle
0x0900000005a6bb24
sqlpgWriteToDisk__FP9SQLP_DBCBP9SQLP_LFPBUlbT4T3
0x0900000005a6b6d8
sqlpgPingPong__FP9SQLP_DBCBP9SQLP_LFPBUlbT3
0x0900000005a6b148
sqlpgwlp__FP9SQLP_DBCBUlT2PC9SQLP_LSN8T2
0x0900000005a63534 sqlpLoggwMain__11sqpLoggwEduFv

Local Fix:
Please turn off native encryption.

DB2 V10.5 FP6 で修正提供予定

PMR1 テクニカルフラッシュ
[DB2 LUW] V10.5 FP5 のみ: Native encryption を有効にすると、db2sysc プロセスのプライベート・メモリーでリークが発生する
http://www.ibm.com/support/docview.wss?uid=swg21883617

障害概要
Native encryption が有効なデータベースでトランザクションを実行するとプライベート・メモリーがリークする

対象ソフトウェア
DB2 V10.5 FP5 のみ

症状
DB2 V10.5 FP5 から、特殊なハードウェアやソフトウェアなしでデータベース全体を暗号化可能な Native encryption 機能がサポートされます。

DB2 native encryption
http://www.ibm.com/support/knowledgecenter/SSEPGG_10.5.0/com.ibm.db2.luw.admin.sec.doc/doc/c0061758.html?lang=ja

Native encryption が有効なデータベースでトランザクションを実行すると、DB2 エンジン・プロセス (db2sysc) のプライベート・メモリーでリークが観察されることがあります。
このとき、db2pd の -dbptnmem や -memblock pid=<db2sysc_pid> ではメモリー・リークの症状は観察できません。
svmon (AIX) の Esid 11, 12 などや、pmap (Linux) の anon ブロックなど、db2sysc プロセスのプライベート・セグメントの数および消費量の単調増加が観察されます。

原因
Native encryption は IBM Crypt for C (ICC) 関数を利用して暗号化を行います。ここで関数の呼び出し方に問題があり、暗号化で使用するメモリーを解放しないケースがありました。
この問題は APAR IT08289 として報告され、2015 年秋に出荷予定の V10.5 FP6 で修正されます。

発生条件
以下のすべての条件を満たす場合に、メモリー・リークが発生します。

DB2 V10,5 FP5 を使用している
ENCRYPT オプションを指定してデータベースを作成している
ENCRYPT オプションを利用したデータベースでトランザクションを実行している

確認方法
db2pd や表関数などの DB2 機能では当メモリー・リークは確認できません。
ENCRYPT オプションを指定して作成したデータベースを利用中に、db2sysc のプライベート・セグメントが増加した場合は、この問題に遭遇している可能性があります。

AIX で malloc debug を有効にした場合、以下のようなコード・パスによる数十から百数バイト程度のメモリー割り当てが多数観察されます。

```
malloc_common_debugging
default_malloc_ex
C101_CRYPTO_malloc@AF28_12
efCRYPTO_malloc
efCRYPTO_calloc
ICCC_EVP_CIPHER_CTX_new@AF299_235
ICCC_EVP_CIPHER_CTX_new
ICC_EVP_CIPHER_CTX_new
cryptSetupEncryptCipherCtx
sqlexRedeemCipherTicket__FP17sqlexCipherTicketPUcUlP5sqlca
sqlpEncrypt__FCPCvCUlPvT2P17sqlexCipherTicketPUcPib
sqlpgEncryptUserDataInNLogPages__FCPvPvCUsP17sqlexCipherTicketC
sqlpgWriteNLogPagesInternal__FR12SQLO_FHANDLECPvPvClCUlCPUlCUsP
sqlpgWriteNLogPagesInternal__FR12SQLO_FHANDLECPvPvClCUlCPUlCUsP
sqlpgWriteNLogPages__FR12SQLO_FHANDLECPvPvCUlCIT4CPUlCUsP17sqle
sqlpgWriteToDisk__FP9SQLP_DBCBP9SQLP_LFPBUlbT4T3
sqlpgPingPong__FP9SQLP_DBCBP9SQLP_LFPBUlbT3
sqlpgwlp__FP9SQLP_DBCBUlT2PC9SQLP_LSN8T2
sqlpLoggwMain__11sqpLoggwEduFv
```

解決策
この問題は V10.5 FP6 で修正されます。FP6 の公開後に FP6 を適用してください。
この問題に遭遇し、FP6 の公開が待てない場合は、テクニカル・サポートに連絡して個別修正を要求してください。

回避策
データベース作成時に ENCRYPT オプションを指定しないでください。

関連情報
パスポート・アドバンテージによく寄せられる質問

お問合せ先
技術的な内容に関して、サービス契約のもと IBM サービス・ラインにお問い合わせください。
IBM サービス・ライン

PMR2 73496,999,760

バックアップ　暗号化+圧縮　**/opt/ibm/db2/V10.5/lib64/libdb2compr_encr.so**　を使用して　Backupを実行するとdb2diag.log にCompress_Internal failedが出続けている

Description

暗号化+圧縮　/opt/ibm/db2/V10.5/lib64/libdb2compr_encr.so　を使用して　Backupを実行　36GB(36,264,448,000 byte)のバックアップイメージが作成されると　db2diag.log には　1620回　次のような　Compress_Internal faile が出力されていました。

```
2015-03-17-18.17.25.296119+540 I815853882E533       LEVEL: Error
PID     : 11119              TID : 140734158071552 PROC : db2sysc 0
INSTANCE: db2enc             NODE : 000           DB   : DBENC
APPHDL  : 0-111              APPID: *LOCAL.db2enc.150317090848
AUTHID  : DB2ENC             HOSTNAME: db2encs
EDUID   : 1154               EDUNAME: db2bm.1031.0 (DBENC) 0
FUNCTION: DB2 UDB, database utilities, Compress, probe:168
DATA #1 : String, 27 bytes
Compress_Internal failed:rc
DATA #2 : unsigned integer, 4 bytes
100
```

このエラーメッセージによる実害はありません。FP6で出力されないよう修正される予定です。

APAR発行予定です。

PMR2 APAR IT08289: PRIVATE MEMORY LEAK DUE TO NATIVE ENCRYPTION.

Abstract
IT08320: NATIVE ENCRYPTION: COMPRESS BACKUP PRODUCES COMPRESS_INTERNAL FAILED:RC 100 IN DB2DIAG.LOG.

Error description:
Large number of errors like as below might be printed in the db2diag.log if users backup a database with native encryption and compress options.

2015-03-17-18.17.25.296119+540 I815853882E533 LEVEL: Error
PID : 11119 TID : 140734158071552 PROC :db2sysc 0
INSTANCE: db2inst1 NODE : 000 DB :ENCDB
APPHDL : 0-111 APPID:*LOCAL.db2inst1.150317090848
AUTHID : db2inst1 HOSTNAME: host01
EDUID : 1154 EDUNAME: db2bm.1031.0 (ENCDB) 0
FUNCTION: DB2 UDB, database utilities, Compress, probe:168
DATA #1 : String, 27 bytes
Compress_Internal failed:rc
DATA #2 : unsigned integer, 4 bytes
100 (= SQLUV_BUFFER_TOO_SMALL)

The following steps illustrate how to hit this condition.

db2 "update db cfg for ENCDB using ENCRLIB <path_to_lib>/libdb2compr_encr.so ENCROPTS '<encryption_options>'"
db2 "backup db ENCDB to <target_path> compress"

This error messages should not be printed in the db2diag.log because the error has been recovered automatically and no user intervention is required.
The backup image is healthy, and it can be used for restore without problems.

Local Fix:
Please ignore the error messages in the db2diag.log.

DB2 V10.5 FP6 で修正提供予定

目次

(参考)暗号化データベースの作成手順

1. キーストアの作成

[db2enc@db2encs bin]$ /home/db2enc/sqllib/gskit/bin/gsk8capicmd_64 -keydb -create -db /home/db2enc/sqllib/NativeEncryption.p12 -pw Db2_105_EncryptionPwd –strong -type pkcs12 -stash

2. インスタンスにキーストアを構成

[db2enc@db2encs bin]$ db2 update dbm cfg using keystore_type pkcs12 keystore_location /home/db2enc/sqllib/NativeEncryption.p12

DB20000I UPDATE DATABASE MANAGER CONFIGURATION

コマンドが正常に完了しました。

SQL1362W 即時変更のためにサブミットされた 1つ以上のパラメーターが動的に変更されませんでした。

クライアントの変更は、次回のアプリケーション始動時、または TERMINATEコマンドが発行されるまで有効になりません。次の DB2START コマンドまで、サーバーの変更は有効になりません。

[db2enc@db2encs bin]$ db2 terminate

DB20000I TERMINATE コマンドが正常に完了しました。

[db2enc@db2encs ~]$ db2start

02/25/2015 10:18:05   0   0   SQL1063N DB2START の処理が正常に終了しました。

SQL1063N DB2START の処理が正常に終了しました。

3. 暗号化DBの作成

[db2enc@db2encs ~]$ db2 create db dbenc encrypt

DB20000I CREATE DATABASE コマンドが正常に完了しました。

目次

- 第2部　パフォーマンステストレポート
  - プロジェクト概要
    - テスト項目
    - 結果サマリー
  - 構成　設定
  - OLTP パフォーマンステスト テスト結果
  - ユーティリティテストシナリオ　テスト結果
    - Load Import
    - Backup Restore
    - Key Rotation
  - PMR / APAR
  - (参考)暗号化データベースの作成手順
  - DB2 構成情報詳細　(db2level / db2set / DBM CFG / DB CFG)

db2level (2015/02 – 4/6 V10.5 FP5 4/6 Special_33839 適用)

```
DB21085I  This instance or install (instance name, where applicable: "db2enc")
uses "64" bits and DB2 code release "SQL10055" with level identifier
"0606010E".
Informational tokens are "DB2 v10.5.0.5", "special_33839", "IP23633_33839", and
Fix Pack "5".
Product is installed at "/opt/ibm/db2/V10.5_Special_33839".
```

db2set

```
[i] DB2COMM=TCPIP
[g] DB2SYSTEM=db2encs
[g] DB2INSTDEF=db2enc
```

Database Manager Configuration - 1

```
     Node type = Enterprise Server Edition with local and remote clients

 Description                                   Parameter   Current Value              Delayed Value
 ---------------------------------------------------------------------------------------------------------
 Database manager configuration release level            = 0x1000

 CPU speed (millisec/instruction)             (CPUSPEED) = 1.141499e-07             1.141499e-07
 Communications bandwidth (MB/sec)      (COMM_BANDWIDTH) = 1.000000e+02             1.000000e+02

 Max number of concurrently active databases     (NUMDB) = 32                       32
 Federated Database System Support           (FEDERATED) = NO                       NO
 Transaction processor monitor name        (TP_MON_NAME) =

 Default charge-back account           (DFT_ACCOUNT_STR) =

 Java Development Kit installation path       (JDK_PATH) = /home/db2enc/sqllib/java/jdk64 /home/db2enc/sqllib/java/jdk64

 Diagnostic error capture level              (DIAGLEVEL) = 3                        3
 Notify Level                                (NOTIFYLEVEL) = 3                      3
 Diagnostic data directory path                 (DIAGPATH) = /home/db2enc/sqllib/db2dump/ /home/db2enc/sqllib/db2dump/
 Current member resolved DIAGPATH                          = /home/db2enc/sqllib/db2dump/ /home/db2enc/sqllib/db2dump/
 Alternate diagnostic data directory path (ALT_DIAGPATH) =
```

```
Database Manager Configuration - 2
Current member resolved ALT_DIAGPATH                    =
 Size of rotating db2diag & notify logs (MB)  (DIAGSIZE) = 0                    0

 Default database monitor switches
   Buffer pool                          (DFT_MON_BUFPOOL) = OFF                OFF
   Lock                                    (DFT_MON_LOCK) = OFF                OFF
   Sort                                    (DFT_MON_SORT) = OFF                OFF
   Statement                               (DFT_MON_STMT) = OFF                OFF
   Table                                  (DFT_MON_TABLE) = OFF                OFF
   Timestamp                            (DFT_MON_TIMESTAMP) = ON               ON
   Unit of work                              (DFT_MON_UOW) = OFF                OFF
 Monitor health of instance and databases   (HEALTH_MON) = OFF                OFF

 SYSADM group name                         (SYSADM_GROUP) = DB2ENC              DB2ENC
 SYSCTRL group name                       (SYSCTRL_GROUP) =
 SYSMAINT group name                     (SYSMAINT_GROUP) =
 SYSMON group name                         (SYSMON_GROUP) =

 Client Userid-Password Plugin            (CLNT_PW_PLUGIN) =

 Client Kerberos Plugin                  (CLNT_KRB_PLUGIN) =

 Group Plugin                               (GROUP_PLUGIN) =

 GSS Plugin for Local Authorization      (LOCAL_GSSPLUGIN) =

 Server Plugin Mode                      (SRV_PLUGIN_MODE) = UNFENCED           UNFENCED

 Server List of GSS Plugins        (SRVCON_GSSPLUGIN_LIST) =

 Server Userid-Password Plugin          (SRVCON_PW_PLUGIN) =

 Server Connection Authentication            (SRVCON_AUTH) = NOT_SPECIFIED      NOT_SPECIFIED
 Cluster manager                                           =
```

Database Manager Configuration - 3

```
Database manager authentication        (AUTHENTICATION) = SERVER                    SERVER
 Alternate authentication          (ALTERNATE_AUTH_ENC) = NOT_SPECIFIED              NOT_SPECIFIED
 Cataloging allowed without authority   (CATALOG_NOAUTH) = NO                        NO
 Trust all clients                      (TRUST_ALLCLNTS) = YES                       YES
 Trusted client authentication          (TRUST_CLNTAUTH) = CLIENT                    CLIENT
 Bypass federated authentication            (FED_NOAUTH) = NO                        NO

 Default database path                       (DFTDBPATH) = /sdddbdisk/db2enc         /sdddbdisk/db2enc

 Database monitor heap size (4KB)          (MON_HEAP_SZ) = AUTOMATIC(90)             AUTOMATIC(90)
 Java Virtual Machine heap size (4KB)     (JAVA_HEAP_SZ) = 2048                      2048
 Audit buffer size (4KB)                  (AUDIT_BUF_SZ) = 0                         0
 Global instance memory (4KB)          (INSTANCE_MEMORY) = AUTOMATIC(14790084)       AUTOMATIC(14790084)
 Member instance memory (4KB)                            = GLOBAL                    GLOBAL
 Agent stack size                       (AGENT_STACK_SZ) = 1024                      1024
 Sort heap threshold (4KB)                  (SHEAPTHRES) = 0                         0

 Directory cache support                     (DIR_CACHE) = YES                       YES

 Application support layer heap size (4KB)   (ASLHEAPSZ) = 15                        15
 Max requester I/O block size (bytes)         (RQRIOBLK) = 65535                     65535
 Workload impact by throttled utilities(UTIL_IMPACT_LIM) = 10                        10

 Priority of agents                           (AGENTPRI) = SYSTEM                    SYSTEM
 Agent pool size                       (NUM_POOLAGENTS) = AUTOMATIC(100)           AUTOMATIC(100)
 Initial number of agents in pool      (NUM_INITAGENTS) = 0                        0
 Max number of coordinating agents     (MAX_COORDAGENTS) = AUTOMATIC(200)          AUTOMATIC(200)
 Max number of client connections      (MAX_CONNECTIONS) = AUTOMATIC(MAX_COORDAGENTS) AUTOMATIC(MAX_COORDAGENTS)

 Keep fenced process                        (KEEPFENCED) = YES                     YES
 Number of pooled fenced processes         (FENCED_POOL) = AUTOMATIC(MAX_COORDAGENTS) AUTOMATIC(MAX_COORDAGENTS)
 Initial number of fenced processes    (NUM_INITFENCED) = 0                        0

 Index re-creation time and redo index build  (INDEXREC) = RESTART                  RESTART
```

```
Database Manager Configuration - 4
 Transaction manager database name          (TM_DATABASE) = 1ST_CONN                 1ST_CONN
 Transaction resync interval (sec)      (RESYNC_INTERVAL) = 180                      180

 SPM name                                      (SPM_NAME) = db2encs1                 db2encs1
 SPM log size                              (SPM_LOG_FILE_SZ) = 256                   256
 SPM resync agent limit                     (SPM_MAX_RESYNC) = 20                    20
 SPM log path                                 (SPM_LOG_PATH) =

 TCP/IP Service name                           (SVCENAME) = 51000                   51000
 Discovery mode                                (DISCOVER) = SEARCH                  SEARCH
 Discover server instance                 (DISCOVER_INST) = ENABLE                  ENABLE

 SSL server keydb file                     (SSL_SVR_KEYDB) =
 SSL server stash file                     (SSL_SVR_STASH) =
 SSL server certificate label              (SSL_SVR_LABEL) =
 SSL service name                           (SSL_SVCENAME) =
 SSL cipher specs                         (SSL_CIPHERSPECS) =
 SSL versions                                (SSL_VERSIONS) =
 SSL client keydb file                     (SSL_CLNT_KEYDB) =
 SSL client stash file                     (SSL_CLNT_STASH) =

 Maximum query degree of parallelism    (MAX_QUERYDEGREE) = ANY                     ANY
 Enable intra-partition parallelism      (INTRA_PARALLEL) = NO                      NO

 Maximum Asynchronous TQs per query     (FEDERATED_ASYNC) = 0                       0

 No. of int. communication buffers(4KB)(FCM_NUM_BUFFERS) = AUTOMATIC(4096)          AUTOMATIC(4096)
 No. of int. communication channels    (FCM_NUM_CHANNELS) = AUTOMATIC(2048)         AUTOMATIC(2048)
 Inter-node comm. parallelism           (FCM_PARALLELISM) = 1                       1
 Node connection elapse time (sec)          (CONN_ELAPSE) = 10                      10
 Max number of node connection retries (MAX_CONNRETRIES) = 5                       5
 Max time difference between nodes (min) (MAX_TIME_DIFF) = 60                      60

 db2start/db2stop timeout (min)         (START_STOP_TIME) = 10                      10
```

```
Database Manager Configuration - 5
 WLM dispatcher enabled                 (WLM_DISPATCHER) = NO                        NO
 WLM dispatcher concurrency             (WLM_DISP_CONCUR) = COMPUTED(96)             COMPUTED
 WLM dispatcher CPU shares enabled (WLM_DISP_CPU_SHARES) = NO                        NO
 WLM dispatcher min. utilization (%) (WLM_DISP_MIN_UTIL) = 5                         5

 Communication buffer exit library list (COMM_EXIT_LIST) =

 Current effective arch level          (CUR_EFF_ARCH_LVL) = V:10 R:5 M:0 F:5 I:0 SB:0  V:10 R:5 M:0 F:5 I:0 SB:0
 Current effective code level          (CUR_EFF_CODE_LVL) = V:10 R:5 M:0 F:5 I:0 SB:33 V:10 R:5 M:0 F:5 I:0 SB:33

 Keystore type                            (KEYSTORE_TYPE) = PKCS12                    PKCS12
 Keystore location                      (KEYSTORE_LOCATION) = /home/db2enc/sqllib/Native /home/db2enc/sqllib/Native


Database Connection Information -1

 Database server        = DB2/LINUXX8664 10.5.5
 SQL authorization ID   = DB2ENC
 Local database alias   = SDBENC

-----------------------------------
2015/04/07 17:03:57

       Database Configuration for Database SDBenc

 Description                                  Parameter   Current Value              Delayed Value
 ---------------------------------------------------------------------------------------------------
 Database configuration release level                  = 0x1000
 Database release level                                = 0x1000

 Database territory                                    = JP
 Database code page                                    = 1208
 Database code set                                     = UTF-8
 Database country/region code                          = 81
 Database collating sequence                           = IDENTITY                 IDENTITY
 Alternate collating sequence              (ALT_COLLATE) =
```

```
Database Connection Information -2
 Number compatibility                                = OFF
 Varchar2 compatibility                              = OFF
 Date compatibility                                  = OFF
 Database page size                                  = 4096                    4096

 Statement concentrator                 (STMT_CONC) = OFF                     OFF

 Discovery support for this database    (DISCOVER_DB) = ENABLE                ENABLE

 Restrict access                                     = NO
 Default query optimization class       (DFT_QUERYOPT) = 5                    5
 Degree of parallelism                  (DFT_DEGREE) = 1                      1
 Continue upon arithmetic exceptions    (DFT_SQLMATHWARN) = NO                NO
 Default refresh age                    (DFT_REFRESH_AGE) = 0                 0
 Default maintained table types for opt (DFT_MTTB_TYPES) = SYSTEM              SYSTEM
 Number of frequent values retained     (NUM_FREQVALUES) = 10                 10
 Number of quantiles retained           (NUM_QUANTILES) = 20                  20

 Decimal floating point rounding mode   (DECFLT_ROUNDING) = ROUND_HALF_EVEN   ROUND_HALF_EVEN

 Backup pending                                      = NO

 All committed transactions have been written to disk    = NO
 Rollforward pending                                 = NO
 Restore pending                                     = NO

 Multi-page file allocation enabled                  = YES

 Log retain for recovery status                      = NO
 User exit for logging status                        = NO

 Self tuning memory                     (SELF_TUNING_MEM) = ON (Active)        ON
 Size of database shared memory (4KB)   (DATABASE_MEMORY) = AUTOMATIC(9658328) AUTOMATIC(9658328)
 Database memory threshold              (DB_MEM_THRESH) = 100                 100
 Max storage for lock list (4KB)              (LOCKLIST) = AUTOMATIC(16992)   AUTOMATIC(16992)
 Percent. of lock lists per application       (MAXLOCKS) = AUTOMATIC(98)      AUTOMATIC(98)
```

Database Connection Information -3

Package cache size (4KB)	(PCKCACHESZ)	=	AUTOMATIC(8192)	AUTOMATIC(8192)
Sort heap thres for shared sorts (4KB)	(SHEAPTHRES_SHR)	=	AUTOMATIC(5000)	AUTOMATIC(5000)
Sort list heap (4KB)	(SORTHEAP)	=	AUTOMATIC(256)	AUTOMATIC(256)
Database heap (4KB)	(DBHEAP)	=	AUTOMATIC(5210)	AUTOMATIC(5210)
Catalog cache size (4KB)	(CATALOGCACHE_SZ)	=	300	300
Log buffer size (4KB)	(LOGBUFSZ)	=	2150	2150
Utilities heap size (4KB)	(UTIL_HEAP_SZ)	=	AUTOMATIC(83966)	AUTOMATIC(83966)
SQL statement heap (4KB)	(STMTHEAP)	=	AUTOMATIC(8192)	AUTOMATIC(8192)
Default application heap (4KB)	(APPLHEAPSZ)	=	AUTOMATIC(256)	AUTOMATIC(256)
Application Memory Size (4KB)	(APPL_MEMORY)	=	AUTOMATIC(40000)	AUTOMATIC(40000)
Statistics heap size (4KB)	(STAT_HEAP_SZ)	=	AUTOMATIC(4384)	AUTOMATIC(4384)
Interval for checking deadlock (ms)	(DLCHKTIME)	=	10000	10000
Lock timeout (sec)	(LOCKTIMEOUT)	=	-1	-1
Changed pages threshold	(CHNGPGS_THRESH)	=	80	80
Number of asynchronous page cleaners	(NUM_IOCLEANERS)	=	AUTOMATIC(12)	AUTOMATIC(12)
Number of I/O servers	(NUM_IOSERVERS)	=	AUTOMATIC(28)	AUTOMATIC(28)
Sequential detect flag	(SEQDETECT)	=	YES	YES
Default prefetch size (pages)	(DFT_PREFETCH_SZ)	=	AUTOMATIC	AUTOMATIC
Track modified pages	(TRACKMOD)	=	NO	NO
Default number of containers		=	1	1
Default tablespace extentsize (pages)	(DFT_EXTENT_SZ)	=	32	32
Max number of active applications	(MAXAPPLS)	=	AUTOMATIC(282)	AUTOMATIC(282)
Average number of active applications	(AVG_APPLS)	=	AUTOMATIC(1)	AUTOMATIC(1)
Max DB files open per application	(MAXFILOP)	=	61440	61440
Log file size (4KB)	(LOGFILSIZ)	=	10240	10240
Number of primary log files	(LOGPRIMARY)	=	130	130
Number of secondary log files	(LOGSECOND)	=	90	90
Changed path to log files	(NEWLOGPATH)	=		

```
Database Connection Information -4
 Path to log files                                  = /sddlogdisk/db2enc/NODE0000/LOGSTREAM0000/
/sddlogdisk/db2enc/NODE0000/LOGSTREAM0000/
 Overflow log path                    (OVERFLOWLOGPATH) =
 Mirror log path                        (MIRRORLOGPATH) =
 First active log file                                  =
 Block log on disk full               (BLK_LOG_DSK_FUL) = NO                    NO
 Block non logged operations           (BLOCKNONLOGGED) = NO                    NO
 Percent max primary log space by transaction  (MAX_LOG) = 0                     0
 Num. of active log files for 1 active UOW(NUM_LOG_SPAN) = 0                     0

 Percent log file reclaimed before soft chckpt (SOFTMAX) = 0                     0
 Target for oldest page in LBP       (PAGE_AGE_TRGT_MCR) = 30                    30

 HADR database role                                     = STANDARD              STANDARD
 HADR local host name                 (HADR_LOCAL_HOST) =
 HADR local service name               (HADR_LOCAL_SVC) =
 HADR remote host name               (HADR_REMOTE_HOST) =
 HADR remote service name             (HADR_REMOTE_SVC) =
 HADR instance name of remote server (HADR_REMOTE_INST) =
 HADR timeout value                      (HADR_TIMEOUT) = 120                   120
 HADR target list                    (HADR_TARGET_LIST) =
 HADR log write synchronization mode     (HADR_SYNCMODE) = NEARSYNC             NEARSYNC
 HADR peer window duration (seconds)  (HADR_PEER_WINDOW) = 0                     0

 First log archive method               (LOGARCHMETH1) = OFF                   OFF
 Archive compression for logarchmeth1    (LOGARCHCOMPR1) = OFF                  OFF
 Options for logarchmeth1                 (LOGARCHOPT1) =
 Second log archive method              (LOGARCHMETH2) = OFF                   OFF
 Archive compression for logarchmeth2    (LOGARCHCOMPR2) = OFF                  OFF
 Options for logarchmeth2                 (LOGARCHOPT2) =
 Failover log archive path               (FAILARCHPATH) =
 Number of log archive retries on error   (NUMARCHRETRY) = 5                     5
 Log archive retry Delay (secs)         (ARCHRETRYDELAY) = 20                    20
 Vendor options                              (VENDOROPT) =

 Auto restart enabled                     (AUTORESTART) = ON                    ON
```

Database Connection Information -5

```
Index re-creation time and redo index build  (INDEXREC) = SYSTEM                SYSTEM (RESTART)
 Log pages during index build             (LOGINDEXBUILD) = OFF                 OFF
 Default number of loadrec sessions     (DFT_LOADREC_SES) = 1                   1
 Number of database backups to retain    (NUM_DB_BACKUPS) = 12                  12
 Recovery history retention (days)      (REC_HIS_RETENTN) = 366                 366
 Auto deletion of recovery objects     (AUTO_DEL_REC_OBJ) = OFF                 OFF

 TSM management class                    (TSM_MGMTCLASS) =
 TSM node name                           (TSM_NODENAME) =
 TSM owner                                  (TSM_OWNER) =
 TSM password                            (TSM_PASSWORD) =

 Automatic maintenance                      (AUTO_MAINT) = ON                    ON
   Automatic database backup             (AUTO_DB_BACKUP) = OFF                 OFF
   Automatic table maintenance           (AUTO_TBL_MAINT) = ON                  ON
     Automatic runstats                   (AUTO_RUNSTATS) = ON                  ON
       Real-time statistics              (AUTO_STMT_STATS) = ON                 ON
       Statistical views                (AUTO_STATS_VIEWS) = OFF                OFF
       Automatic sampling                  (AUTO_SAMPLING) = OFF                OFF
     Automatic reorganization                 (AUTO_REORG) = OFF                 OFF

 Auto-Revalidation                          (AUTO_REVAL) = DEFERRED              DEFERRED

 Currently Committed                        (CUR_COMMIT) = ON                    ON
 CHAR output with DECIMAL input          (DEC_TO_CHAR_FMT) = NEW                 NEW
 Enable XML Character operations          (ENABLE_XMLCHAR) = YES                 YES
 WLM Collection Interval (minutes)       (WLM_COLLECT_INT) = 0                   0

 Monitor Collect Settings
 Request metrics                         (MON_REQ_METRICS) = BASE                BASE
 Activity metrics                        (MON_ACT_METRICS) = BASE                BASE
 Object metrics                          (MON_OBJ_METRICS) = EXTENDED            EXTENDED
 Routine data                               (MON_RTN_DATA) = NONE                NONE
   Routine executable list              (MON_RTN_EXECLIST) = OFF                 OFF
 Unit of work events                        (MON_UOW_DATA) = NONE                NONE
   UOW events with package list          (MON_UOW_PKGLIST) = OFF                 OFF
   UOW events with executable list      (MON_UOW_EXECLIST) = OFF                 OFF
```

```
Database Connection Information -6
Lock timeout events                   (MON_LOCKTIMEOUT) = NONE                      NONE
 Deadlock events                          (MON_DEADLOCK) = WITHOUT_HIST              WITHOUT_HIST
 Lock wait events                         (MON_LOCKWAIT) = NONE                      NONE
 Lock wait event threshold                (MON_LW_THRESH) = 5000000                  5000000

 Number of package list entries           (MON_PKGLIST_SZ) = 32                      32
 Lock event notification level            (MON_LCK_MSG_LVL) = 1                      1

 SMTP Server                                (SMTP_SERVER) =
 SQL conditional compilation flags          (SQL_CCFLAGS) =
 Section actuals setting                 (SECTION_ACTUALS) = NONE                   NONE
 Connect procedure                          (CONNECT_PROC) =
 Adjust temporal SYSTEM_TIME period (SYSTIME_PERIOD_ADJ) = NO                       NO
 Log DDL Statements                       (LOG_DDL_STMTS) = NO                      NO
 Log Application Information              (LOG_APPL_INFO) = NO                      NO
 Default data capture on new Schemas     (DFT_SCHEMAS_DCC) = NO                     NO
 HADR spool log data limit (4KB)        (HADR_SPOOL_LIMIT) = AUTOMATIC(0)          AUTOMATIC(0)
 HADR log replay delay (seconds)       (HADR_REPLAY_DELAY) = 0                     0
 Default table organization               (DFT_TABLE_ORG) = ROW                     ROW
 Default string units                      (STRING_UNITS) = SYSTEM                  SYSTEM
 National character string mapping        (NCHAR_MAPPING) = GRAPHIC_CU16            GRAPHIC_CU16
 Database is in write suspend state                       = NO
 Extended row size support              (EXTENDED_ROW_SZ) = ENABLE                  ENABLE
 Encryption Library for Backup                  (ENCRLIB) = libdb2encr.so           libdb2encr.so
 Encryption Options for Backup                 (ENCROPTS) = CIPHER=AES:MODE=CBC:KEY LENGTH=256 CIPHER=AES:MODE=CBC:KEY
LENGTH=256
 Encrypted database                                       = YES                     YES
```