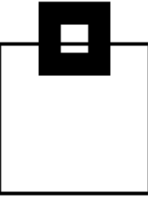
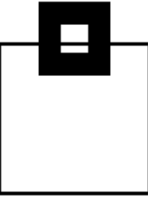

An Audit a day keeps the lawyers at bay!

Roy Boxwell, SEG



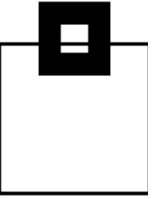
Agenda

1. Audit – do you need it, do you care?!
2. Audit - Voting
3. Audit needs and musts
4. Solution overview and their Pros/Cons
5. The viable way – let Db2 do the magic!



Agenda

1. Audit – do you need it, do you care?!
2. Audit - Voting
3. Audit needs and musts
4. Solution overview and their Pros/Cons
5. The viable way – let Db2 do the magic!



Audit – do you need it, do you care?!

- The new, Europe-wide, GDPR requires it!

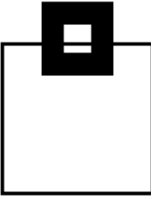
<https://www.eugdpr.org/>

Intro:

The EU General Data Protection Regulation (GDPR) replaced the Data Protection Directive 95/46/EC and is designed to harmonize data privacy laws across Europe, to protect and empower all EU citizens' data privacy and to reshape the way organizations across the region approach data privacy.

Enforcement date was nearly two years ago, on the 25th May 2018, from when those organizations in non-compliance will face heavy fines.

Audit – do you need it, do you care?!



Definitions:

Art. 4 GDPR Definitions

For the purposes of this Regulation:

‘personal data’ means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, *an identification number, location data, an online identifier* or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or *social identity* of that natural person;

This includes TCP/IP addresses and Email addresses...



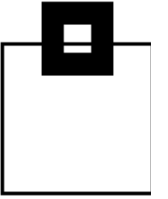
Audit – do you need it, do you care?!

Definitions:

Art. 25 GDPR Data protection by design and by default

1. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, **implement appropriate technical and organisational measures**, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

Audit – do you need it, do you care?!



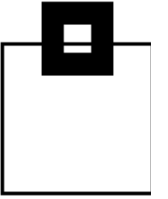
Definitions:

Art. 25 GDPR Data protection by design and by default

2. The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. **In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.**



Audit – do you need it, do you care?!



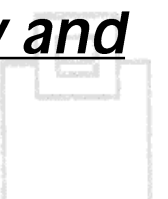
Definitions:

Art. 32 GDPR Security of processing

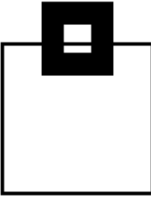
Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the pseudonymisation and encryption of personal data;

- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;*



Audit – do you need it, do you care?!



Definitions:

Art. 32 GDPR Security of processing

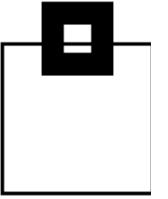
the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from *accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.*



Audit – do you need it, do you care?!



The fines are also amazingly high.

First, for the “minor” problem of being over 72 hours late when data leaks have occurred (a breach), is 2% of global turnover or €10,000,000 (Nearly \$12,000,000) – whichever is **higher**.

Then, if you are really naughty, like disregarding basic data laws, moving data abroad or ignoring an individual’s rights, then you get hit for 4% of global turnover or €20,000,000 (nearly \$24,000,000) – again whichever is **higher**.



Audit – do you need it, do you care?!

The fines are also amazingly high.

Here's a fun website you do ***not*** want your firm name to appear on:

<https://www.enforcementtracker.com/>

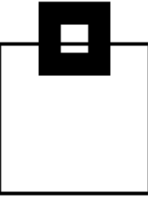
Current “winner” (as of 8th April 2020) is British Airways on the 8th July 2019:

204,600,000€

British Airways

Art. 32 GDPR

Insufficient technical and organisational measures to ensure information security



Audit – do you need it, do you care?!

Art. 83 GDPR General conditions for imposing administrative fines

Each SA shall ensure that the imposition of administrative fines (...) be **effective, proportionate and dissuasive**.

When deciding (...) due regard shall be given to the following:

the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;

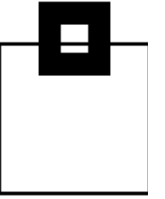
the intentional or negligent character of the infringement;

any action taken by the controller or processor to mitigate the damage suffered by data subjects;

the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;

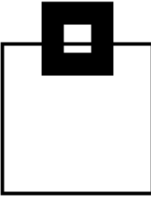
Agenda

1. Audit – do you need it, do you care?!
2. **Audit - Voting**
3. Audit needs and musts
4. Solution overview and their Pros/Cons
5. The viable way – let Db2 do the magic!



Audit – Voting

Please vote for one of the options below



Please vote for one of the options below

- Option 1:



Problem? What problem?

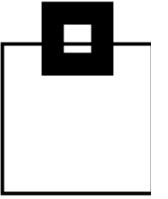
Please vote for one of the options below

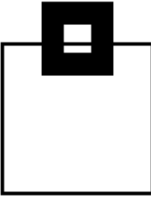
- Option 2:



© Can Stock Photo

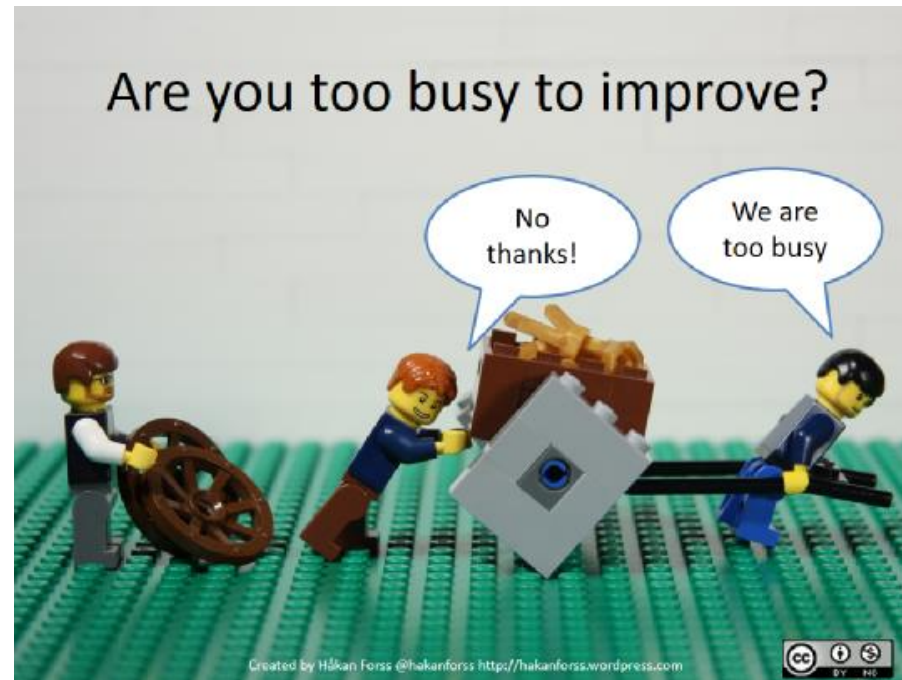
A shovel of sand hides many things...





Please vote for one of the options below

- Option 3:

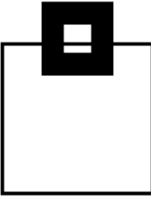


We already have a solution – we do not want to re-invent the wheel!



Agenda

1. Audit – do you need it, do you care?!
2. Audit - Voting
3. Audit needs and musts
4. Solution overview and their Pros/Cons
5. The viable way – let Db2 do the magic!



Audit needs and musts

Focusing on the major area of concern – the database server:

Audit Logging Requirements	Cobit (SOX) FIEL	PCI DSS	HIPAA	CMS ARS	GLBA	ISO 17799 27001	NERC	NIST 800-53 FISMA	GDPR
SELECTs against sensitive data		X	X	X	X	X		X	X
Insert, Update, Delete	X			X		X			X
Access violations	X	X	X	X	X	X	X	X	X
Schema Changes	X	X	X		X	X	X	X	
Grants/Revokes	X	X	X	X	X	X	X	X	X

Audit needs and musts

- Critical activities that enterprises should be auditing
 - Privileged Users
 - Access/changes/deletion to critical data
 - Access using inappropriate channels
 - Schema modifications
 - Unauthorized addition of user accounts

Who is the privileged user?

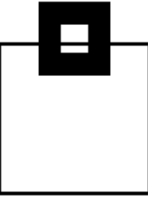


- Critical activities that enterprises should be auditing
 - End Users
 - Unusual access to excessive amounts of data
 - Access to data outside standard working hours
 - Access to data through inappropriate channels
 - Developers, Analysts and System Administrators
 - Access to live production systems
 - IT Operations
 - Inappropriate changes to DB/DB applications

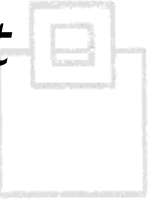


Danger

**Critical incidents might
be closer than you think**



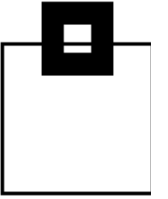
- ... or in other words:
Collect as much data as you can, because you probably don't know today what you'll need tomorrow
→ **breach patterns do change!!!**
- Make sure you include:
 - SELECTs (against sensitive data)
 - DDL
 - DML
 - DCL
 - Utilities (online + offline)
 - Commands
 - Assignment, or change of a user ID/authorization – especially privileged users



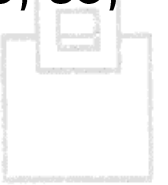
Audit needs and musts

- Be careful what happens outside of a table:
 - Consider clones
 - Consider backups
 - Consider extended statistics in catalog tables, like SYSCOLDIST + SYSKEYTGTDIST
 - Consider utility output (REORG, RUNSTATs)
 - Consider UNLOADs
 - Consider Replication
 - Consider access to the underlying VSAM cluster
- Also consider your INSTALL SYSADM/SYSOPR
 - Sorry DBAs, but Auditing requires a separation of duties

Audit needs and musts



- Most Home-Grown Solutions are based on the Db2 Audit Trace:
 - Class 1, 2, 7, 8 have very little overhead
 - Access violations (Class 1 IFCID 140)
 - GRANTS/REVOKEs (Class 2 IFCID 141)
 - Assignment, or modification of a user ID/authorization (Class 7 IFCIDs 55, 83, 87, 169, 319)
 - Db2 utility (Class 8 IFCIDs 23, 24, 25, 219, 220)
 - Class 3 (IFCID 142) has very little overhead
 - DDL (only for TB having the AUDIT ALL attribute)



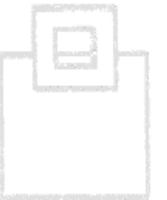
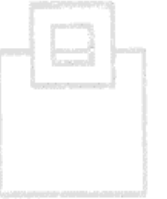
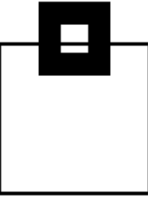
Audit needs and musts

- Most Home-Grown Solutions are based on the Db2 Audit Trace:
 - Class 4, 5 (IFCIDs 143, 144) has up to 5% overhead
 - 1st INSERT/UPDATE/DELETE, SELECT in a UOR
 - Class 10 (IFCIDs 270, 271) has low overhead
 - Trusted context Create/Alter and Column mask/Row permission Create/Drop/Alter
 - IFCIDs 90, 91 have very little overhead
 - Db2 Commands



Agenda

1. Audit – do you need it, do you care?!
2. Audit - Voting
3. Audit needs and musts
4. **Solution overview and their Pros/Cons**
5. The viable way – let Db2 do the magic!



Solution overview and their Pros/Cons

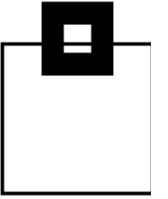
There are a variety of existing resources Db2 already provides/comes with:

- Db2 Log
- Db2 Trace
- Db2 Memory (DSC/EDM)
- Db2 Exits

The IBM Db2 logo is displayed within a blue rectangular box. The text "IBM Db2" is written in white, with "IBM" in a standard sans-serif font and "Db2" in a bold, sans-serif font.

IBM Db2

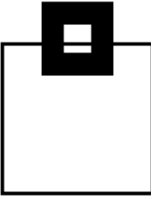
Solution overview and their Pros/Cons



Db2 Log:

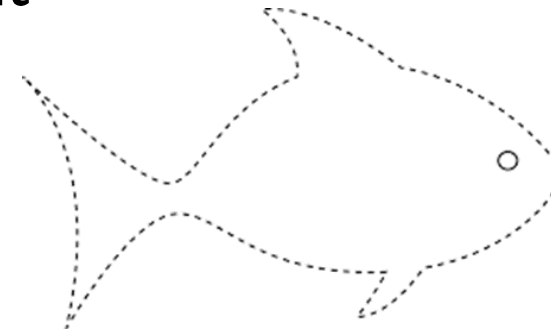
- Pros:
 - Comes with Db2 and supports all versions
 - No additional overhead
 - No additional costs (except you want to keep logs for a longer period of time than currently and, of course, your analysis)
 - Most companies have log analysis tools they're already familiar with
- Cons:
 - Not all required data is logged
 - SELECTs are especially lacking

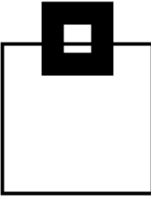




Db2 Trace:

- Pros:
 - Comes with Db2 and supports all versions
 - No additional costs (except for storing and processing the collected data)
 - Most companies have trace data analysis tools they're already familiar with
- Cons:
 - Depending on the scope (number of IFCIDs/classes), and the type (SMF, OPX, GTF, SRV), the overhead may be significant
 - You need to build your own repository
 - If not using OPX you lose time!

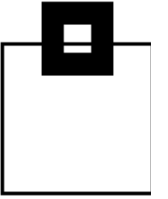




Db2 Trace:

- What are the differences:
 - There are different types of traces:
 - Statistics, Accounting, Audit, Monitor, Performance, Global
 - There are different classes
 - There are hundreds of individual IFCIDs
- Depending on your choice, the overhead is unmeasurable to significant
- A key difference in cost is the trace destination!
 - SMF, OPX, GTF, SRV





Db2 Trace:

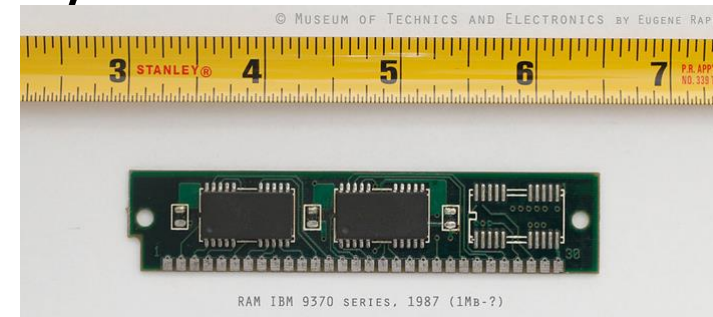
- What are the differences:
 - Processing the data requires simple to more sophisticated knowledge:
 - SMF: System Management Facility:
Most commonly used, easy to process (use DSN1SMFP) – Once a day “cuts” cost 24 hours
 - OPn/OPX: Buffer Destination Trace
very efficient, but Assembler needed to process (DSN1SDMP is pretty poor)
 - GTF: Generalized Trace Facility:
Used for detailed monitoring
 - SRV: Serviceability Routine:
I have never seen it used



Solution overview and their Pros/Cons

Db2 Memory (DSC/EDM):

- Pros:
 - Comes with Db2 and supports all versions
 - No additional overhead
 - No additional costs (except for storing and processing)
- Cons:
 - Not all required data is there
 - Usually you can't access it yourself, unless you hook into it
 - The information is volatile and can get lost quickly



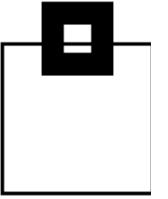
Solution overview and their Pros/Cons

Db2 Exits:

- Pros:
 - Partially comes with Db2 and supports all versions
 - No additional costs (except for storing and processing)
- Cons:
 - Not all required data is there
 - Lots of coding necessary to catch and process the data
 - The overhead may be significant



Solution overview and their Pros/Cons

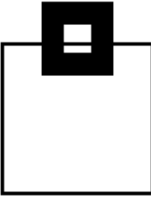


Additional Tools:

- Pros:
 - There are various solutions to choose from
 - Usually easy to use and more powerful than native Db2 options
- Cons:
 - Vendors charge for it
 - Implementation and processing overhead may be significant
 - Additional appliances lead to more vulnerability and administration overhead



Solution overview and their Pros/Cons



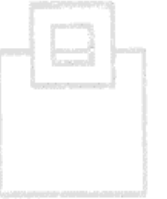
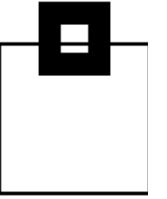
Additional Tools:

- What are the differences?
 - Good solutions have efficient data collectors and share repositories for Audit, Performance Management, Accounting, Analytics ...
 - Some solutions use hooks into the Db2 address space to capture SQL activity – errors can bring down Db2, or the entire LPAR, thus they try to protect Db2 by encapsulating the “foreign” code
 - Some solutions need additional appliances (easily up to 100+ virtual appliances)→ all SQL captured is sent (unencrypted!) through the network. If the connection gets lost they try to cache it. Keep in mind that attackers do DDoS attacks!



Agenda

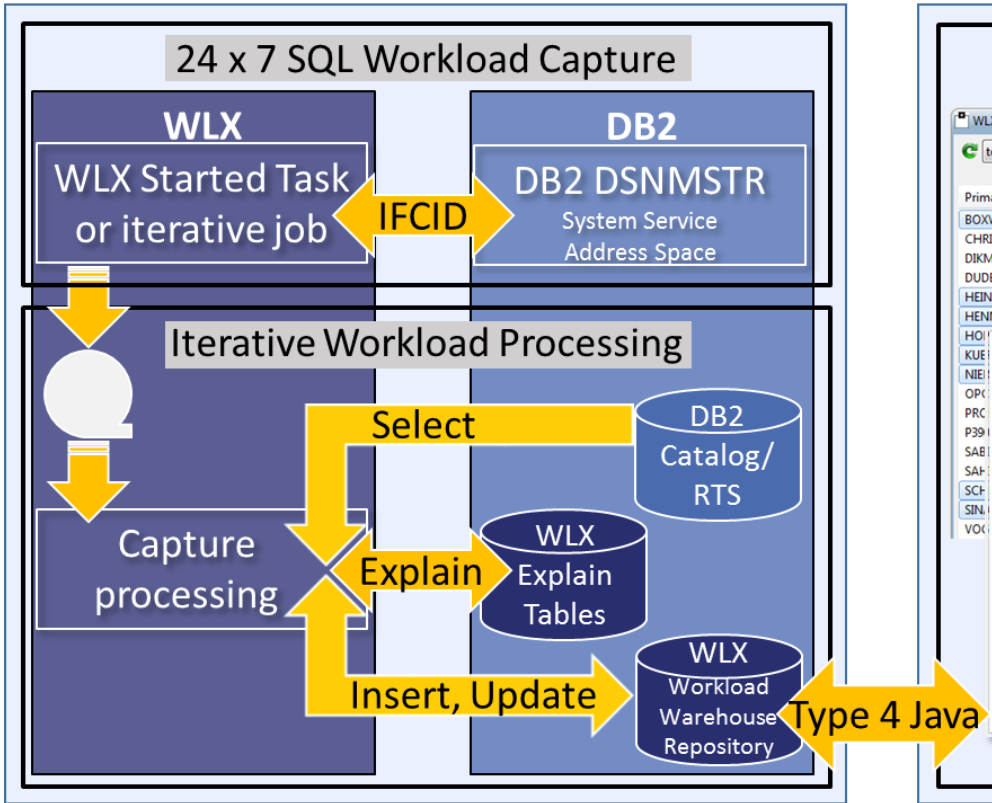
1. Audit – do you need it, do you care?!
2. Audit - Voting
3. Audit needs and musts
4. Solution overview and their Pros/Cons
5. The viable way – let Db2 do the magic!



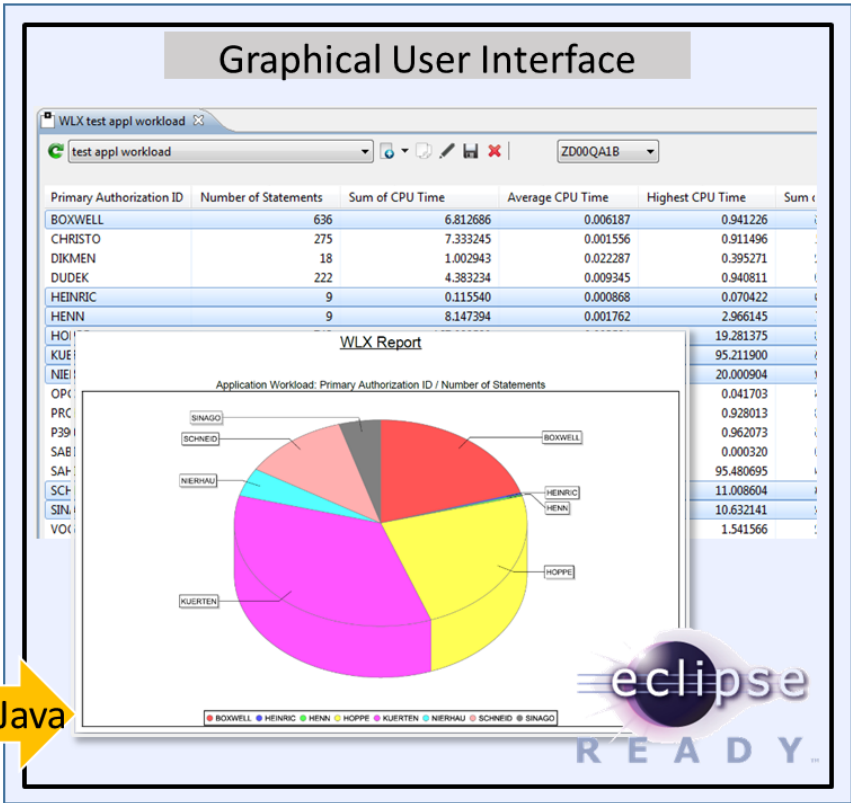
The viable way – let Db2 do the magic

Efficient data collector for
your desired scope of Audit

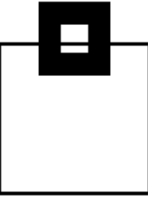
Mainframe Engine



Workstation Engine



The viable way – let Db2 do the magic



The most reliable/efficient solution is based on those reliable and robust Db2 key functions we've been using for ages.



Exploiting them results in the most powerful solution:

- You benefit from rock solid features, like:
 - Security
 - Compression
 - Native Db2 functions
 - Extended Client Identification Registers, `sqleseti()`



The only question is: What key Db2 functions are needed?



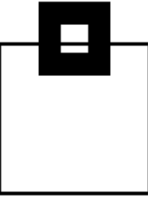
The viable way – let Db2 do the magic

Using IFCIDs along with OPX buffers delivers in-depth information without the overhead and delay of SMF processing.

The absolute minimum requirement is to get the SQL that is running in the enterprise so at least:

316/318 Dynamic SQL (SELECT, INSERT, etc.)
(+317 for the full SQL statement)

400/401 Static SQL (SELECT, INSERT, etc.)
(+SYSPACKSTMT for the full SQL statement)



The viable way – let Db2 do the magic

Using IFCIDs along with OPX buffers delivers in-depth information without the overhead and delay of SMF processing.

23/24/25 Utility start, phase change, and stop

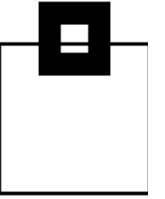
219/220 Utility Listdef and Template)

55/83/87/ SQLID setting

169/319

62/142 DDL and CREATE/ALTER/DROP for tables with AUDIT changes or all

90/91 Commands and their completion status

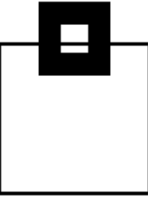


The viable way – let Db2 do the magic

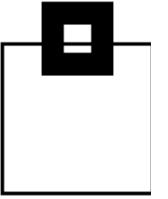
Using IFCIDs along with OPX buffers delivers in-depth information without the overhead and delay of SMF processing:

140	Authorization failures
141	Authorization changes
143/144	AUDIT Table access
197	Console messages
269/270/271	Trusted Context and Column Masks/Row Permissions

Add the correlation headers to get detailed authentication data.



The viable way – let Db2 do the magic



So now you have all that data for Audit. But also now think about what else you could do with all of it...



Just imagine the performance data contained within...or the usage analysis possible...



The possibilities are endless! This is a fantastic data source created for Audit but available for performance DBAs and even developers!



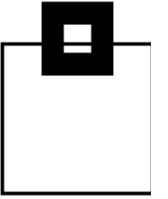
BUT:

Make sure it's secure!

- Set up and audit access to the repository
- Alert via WTO if someone messes with the IFCIDs you've chosen
- Consider automatically cancelling threads of users violating the rules



The viable way – let Db2 do the magic



All IFCIDs listed have a much smaller footprint than a blanket
AUDIT CHANGES/ALL

This is integrated, reliable Db2 technology, OPX is the right target for efficient capturing. Store it in a repository and protect it using proven technology (e.g. RACF, ACF2, Top Secret)



Using Db2 compression reduces storage requirements by exploiting proven, integrated technology



→ No new vulnerabilities like:

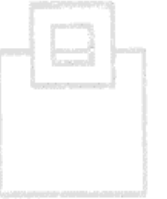
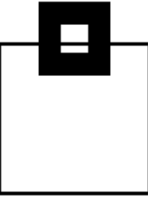
- Black Box appliance
- Massive sensitive data transmissions over the network



The viable way – let Db2 do the magic

Do your (automated) reporting/alerting/analytics as needed:

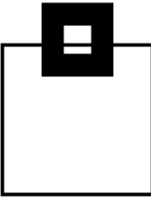
- SPUFI
- Batch Job
- Enterprise-wide reporting system
- GUI (DRDA based queries are fully zIIP eligible)
 - Eclipse based
 - ZOWE based



The viable way – let Db2 do the magic

DSC and EDM provide detailed workload insights, including flushed statements:

- SQL text
- Statement ID
- Date/time
- Current status
- Resource consumption
- Identification/environmental data

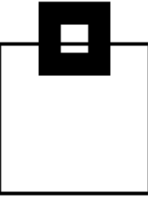


The viable way – let Db2 do the magic

Use a GUI front end:

Exploit and integrate into Eclipse based GUI front ends

- GUIs can come as a Plug-in for
 - IBM Rational
 - IBM Data Studio
 - Eclipse native
- Use ZOWE – It rocks!
- Existing Db2 connections are used to connect to the mainframe
- Interactive dialogs allow complex and powerful analysis
- Export features can create PDF reports and allow MS Excel handover



The viable way – let Db2 do the magic

GUI features –
button overview

SQL WorkloadExpert : Audit

webve View

Bind ImpactExpert

NEW

Audit

Execute query

Edit

Delete

SQL

MS Excel export

QA1B

New

Select query

Copy

Save

Import/Export

Selected database connection

WLX GUI

SQL WorkloadExpert for Db2 z/OS

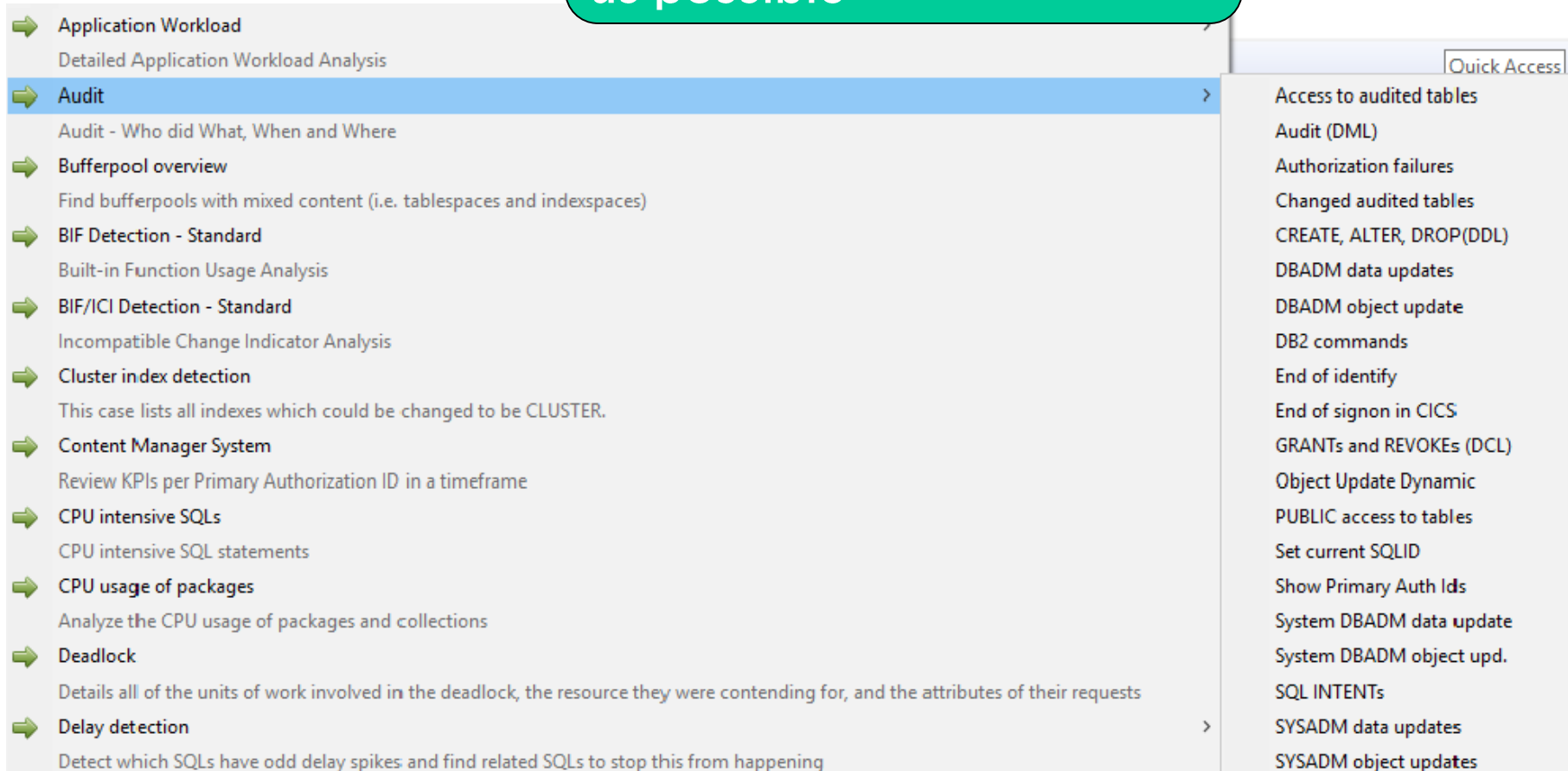
Back to Use Cases

Application Workload

Statement Origin	Package	Primary Authorization ID	Collection ID	Number of Statements	Sum of CPU Time	Average CPU Time	Highest CPU Time
D	n/a		n/a	324	5	0.00009	1.85644
D	n/a		n/a	20	0	0.000379	0.003515
D	n/a		n/a	34	0	0.000516	0.016252

The viable way – let Db2 do the magic

Delivered Use Cases make
using the product as easy
as possible



The viable way – let Db2 do the magic

Selection, Filtering and
Sorting makes the delivered
Use Cases easy to customize

Audit (DML)

Description: Audit

Projection Selection Sorting

Label	Description
Transaction name	A value provided by the RRS signon ...
WLX Key	The WorkloadExpert key for this wor...
End User ID	A value provided by the RRS signon ...
WLX DB2 SSID	The WorkloadExpert Group or Subsy...
Workstation name	A value provided by the RRS signon ...
Statement ID	The DB2 internal Statement ID
Primary Authorization ID	The Primary Authorization ID used t...
Statement Origin	D for Dynamic SQL or S for Static SQL
Statement Timestamp ...	The timestamp that this statement ...
Package	The package used by the statement
Statement Type	N for No SQL statement text availab..
Collection ID	The Collection ID used by the state...
Min. INSERT timestamp	Minimal INSERT timestamp
Number of Users	The total number of Users of this st...
Max. UPDATE timestamp	Maximum UPDATE timestamp
Number of Copies	The total number of copies of this s...
Status of the Statement	Zero is Normal, 16 is invalidated by ...

>> > < <<

Label	Operator	Value	Description
WLX Key	=	newest	The WorkloadExpert key for this wor...
End User ID	=	SUSPECT	A value provided by the RRS signon ...

↑ ↓

OK Cancel

The viable way – let Db2 do the magic

SQL WorkloadExpert : Workload Analytics

Workload Analytics QA1B

Package	Collection ID	Number of Statements	Sum of CPU Time	Average CPU Time	Highest CPU Time	Sum of Elapsed Time	Average Elap
COISEAR	PTFCOLL008	3	1.548881	0.059572	0.896205	2.139390	
COQAPTF	PTFCOLL008	1	0.119930	0.029982	0.119930	0.299563	
DSMDB2X	SDB2VNEX_TEST	1	0.006221	0.006221	0.006221	0.028612	
DSMDSL	SDB2VNEX_TEST	3	0.081807	0.013634	0.042393	0.094554	
DSMHISDB	SDB2VNEX_TEST	1	0.004614	0.002307	0.004614	0.005366	
DSN\$EP2L	DSNTEP2	1	0.000712	0.000356	0.000712	0.000712	
DSNREXX	DSNREXX	2	0.038444	0.000573	0.024368	0.040348	
DSNTIAP	DSNTIAP	2	0.191846	0.000067	0.111507	0.219824	
DSNTIAUL	DSNTIB10	2				0.009384	
FILLPROD	PTFCOLL008	2				0.124546	
IMEMB	PTFCOLL008	1				2.584011	
ICARRACB	ICARRACB	1				0.510001	

Result counter : 212

Drill down to the statement text to see what the suspect did

SQL Results Execution Plan Bookmarks

Connection profile

Type: Name: Database: Status: Disconnected, Auto Commit

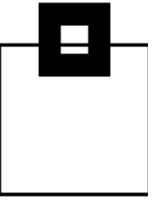
```
1 DECLARE SYSINDEXES_01 CURSOR FOR SELECT RTRIM ( IX . DBNAME ) , RTRIM ( IX . TBCreator ) , RTRIM ( IX . TBNAME ) ,
2 RTRIM ( IX . CREATOR ) , RTRIM ( IX . NAME ) , IX . CLUSTERING , IX . CLUSTERED , CASE WHEN IX . CLUSTERRATIOF > 0
3 THEN IX . CLUSTERRATIOF WHEN IX . CLUSTERRATIO <= 0 THEN FLOAT ( IX . CLUSTERRATIO )
4 ELSE FLOAT ( IX . CLUSTERRATIO ) / 100 END AS CLUSTERRATIOF , IX . FIRSTKEYCARD , IX . FULLKEYCARD , IX . NLEAF ,
5 IX . NLEVELS , IX . UNIQUERULE , IX . COLCOUNT , IX . INDEXTYPE , IX . PIECESIZE , IX . PADDED , IX . AVGKEYLEN ,
6 IX . STATTIME , IX . DATAREPEATFACTOR , TB . TYPE , RTRIM ( TB . TSNAME ) FROM SYSIBM . SYSINDEXES IX ,
7 SYSIBM . SYSTABLES TB WHERE TB . CREATOR = IX . TBCreator AND TB . NAME = IX . TBNAME
8 AND TB . TYPE IN ( 'I' , 'X' , 'M' , 'P' , 'H' , 'R' ) ORDER BY CAST ( IX . CREATOR AS VARCHAR ( 128 ) CCSID EBCDIC )
9 , CAST ( IX . NAME AS VARCHAR ( 128 ) CCSID EBCDIC )
10 FOR FETCH ONLY WITH UR
```

Writable Insert 10:26

The viable way – let Db2 do the magic

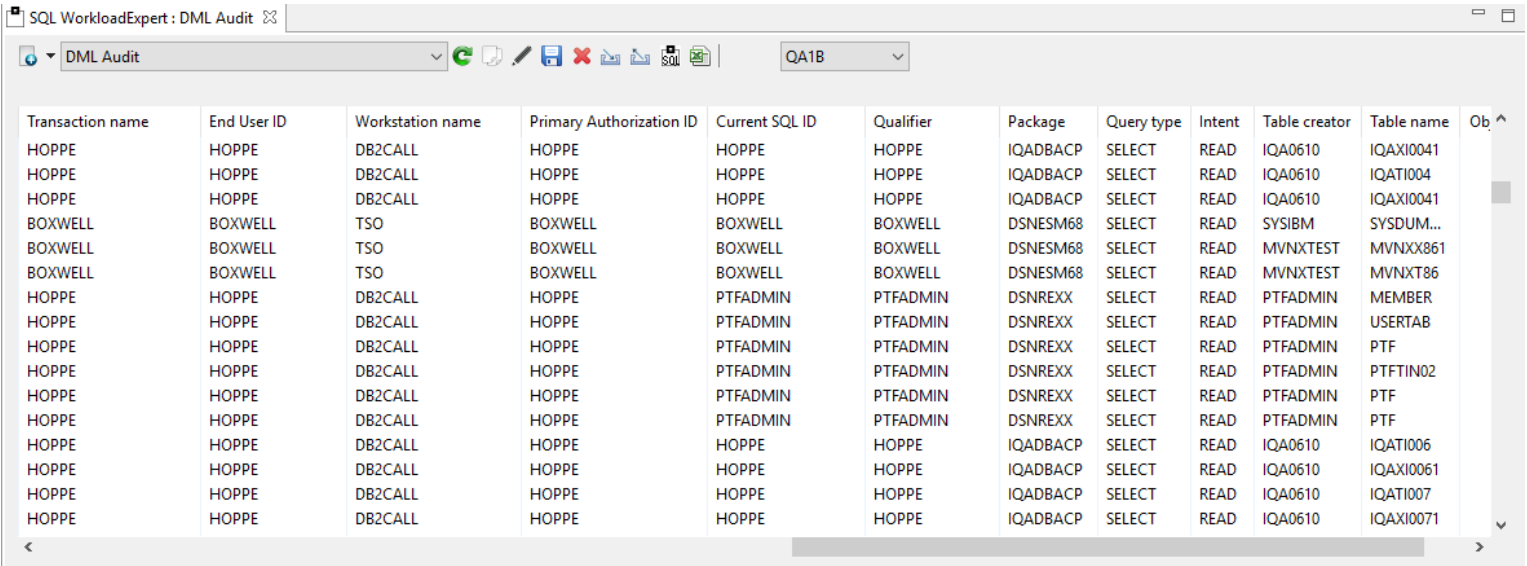
Choose how you'd like
to find out who did
what and when...

- Access to audited tables
- Audit (DML)
- Authorization failures
- CREATE, ALTER, DROP (DDL)
- CREATE, ALTER, DROP (DDL) audited tables
- Db2 commands
- Db2 console messages - Details
- Db2 console messages - Overview
- Distributed translation
- DBADM data updates
- DBADM object update
- End of identify
- End of signon in IMS/CICS
- GRANTs and REVOKEs (DCL)
- Object Update Dynamic
- PUBLIC access to tables
- Row permission
- Security Processing
- Set current SQLID
- Show Primary Authorization IDs
- System DBADM data update
- System DBADM object update
- SQL INTENTs
- SYSADM data updates
- SYSADM object updates
- Trusted context usage
- Trusted context DDL



The viable way – let Db2 do the magic

Choose how you'd like to find out who did what and when...



The screenshot shows the 'SQL WorkloadExpert : DML Audit' window. It features a toolbar with icons for refresh, save, print, and other functions. A dropdown menu is set to 'DML Audit' and a filter is set to 'QA1B'. The main area displays a table with 12 columns: Transaction name, End User ID, Workstation name, Primary Authorization ID, Current SQL ID, Qualifier, Package, Query type, Intent, Table creator, Table name, and Ob. The table contains 18 rows of data, showing various transactions performed by users like HOPPE and BOXWELL on different workstations (DB2CALL, TSO) using various packages (IQADBACP, DSNESM68, DSNREXX).

Transaction name	End User ID	Workstation name	Primary Authorization ID	Current SQL ID	Qualifier	Package	Query type	Intent	Table creator	Table name	Ob
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQAXI0041	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQATI004	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQAXI0041	
BOXWELL	BOXWELL	TSO	BOXWELL	BOXWELL	BOXWELL	DSNESM68	SELECT	READ	SYSIBM	SYSDUM...	
BOXWELL	BOXWELL	TSO	BOXWELL	BOXWELL	BOXWELL	DSNESM68	SELECT	READ	MVNXTTEST	MVNXX861	
BOXWELL	BOXWELL	TSO	BOXWELL	BOXWELL	BOXWELL	DSNESM68	SELECT	READ	MVNXTTEST	MVNXT86	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	MEMBER	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	USERTAB	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	PTF	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	PTFTIN02	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	PTF	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	PTF	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQATI006	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQAXI0061	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQATI007	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQAXI0071	

The viable way – let Db2 do the magic

Optionally use our LEEF (Log Event Extended Format) or sysloger support for the SIEM system of your choice!



```
LEEF:1.0|Software Engineering GmbH|WorkLoadExpert Audit|6.1|
IFCID 090|cat=success|devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSZ|
devTime=2018-03-09T09:57:33.886+0100|Sev=01|usrName=GABELHA|
name=|usrPriv=|usrGroups=|src=|subsys=DC10|dsn=|plan=MVNXPLAN|
objtyp=|obj=|intent=|SQLid=GABELHA|poe=|submitby=|job=Z100 DC10|
cmd=-DIS GROUP |checkid=|conn=DC10 location Z100DC10 LU DESWEG01.Z100DC10
group DC10 member DC10 connector DB2CALL GABELHA operator GABELHA
workstation DB2CALL tx GABELHA enduser GABELHA|sum=DB2 DC10 GABELHA
Command Issued by id GABELHA:-DIS GROUP
```

The viable way – let Db2 do the magic

These days most z/OS Audit systems collect data and transfer to a Data Lake of your choice for post processing every two to three hours e.g. WorkLoadExpert, zSecure etc.

This data is typically RACF, SMF and Master Log data on its way to e.g. QRadar, Splunk, AlienVault et al



Questions???

Many thanks for your attention and now....

