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?!

YES!

Audit – do you need it, do you care?!

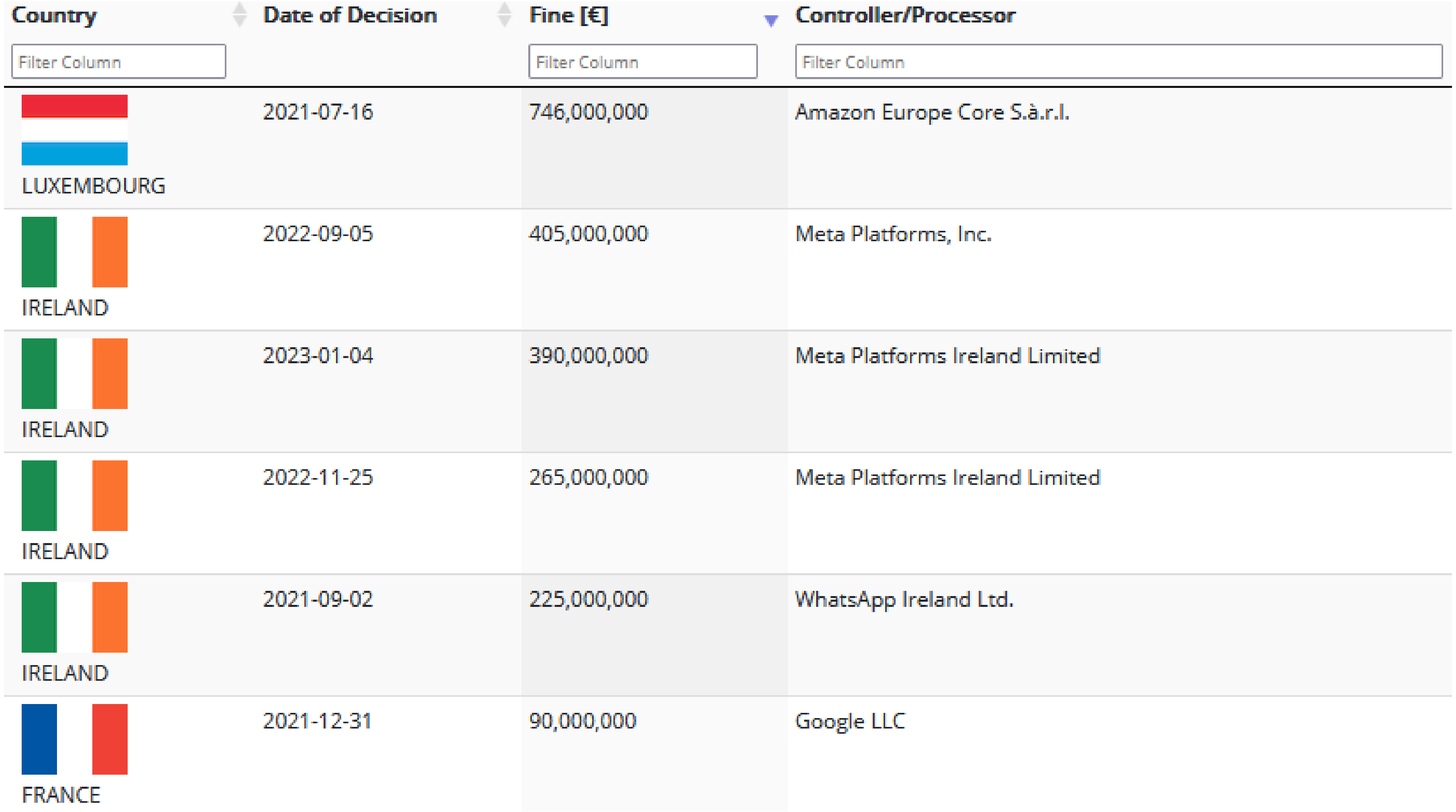
GDPR is in force and companies are paying mega-bucks!

Just go here:

https://www.enforcementtracker.com/

And sort by “Fine” descending…

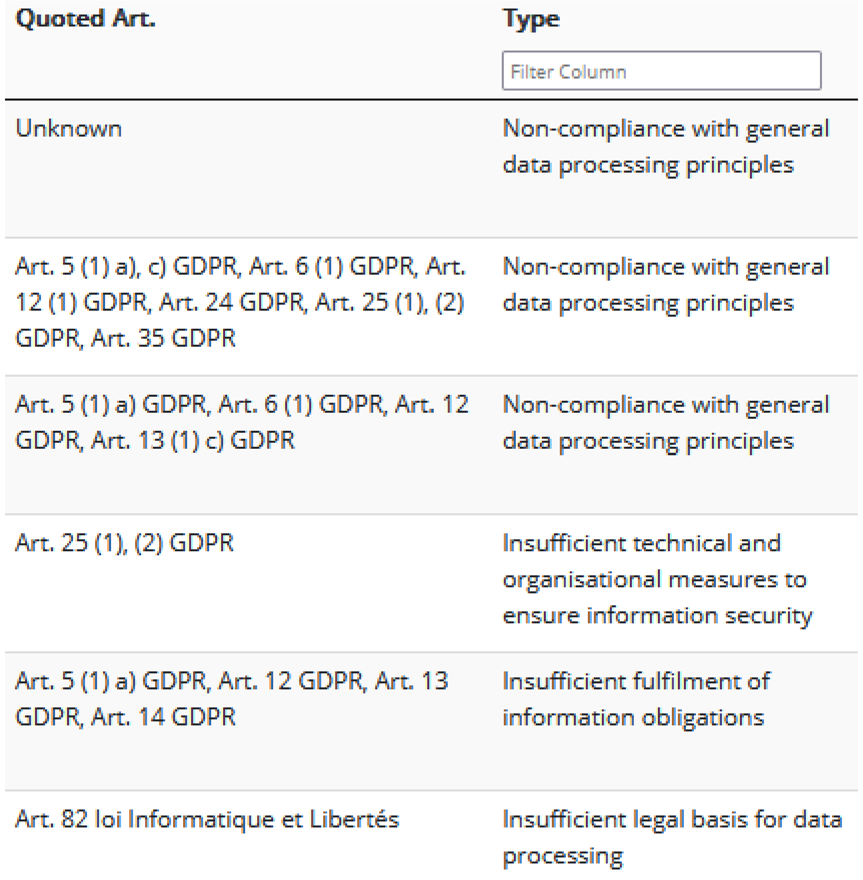
Audit – do you need it, do you care?!



Country	Date of Decision	Fine [€]	Controller/Processor
Filter Column		Filter Column	Filter Column
LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.
IRELAND	2022-09-05	405,000,000	Meta Platforms, Inc.
IRELAND	2023-01-04	390,000,000	Meta Platforms Ireland Limited
IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited
IRELAND	2021-09-02	225,000,000	WhatsApp Ireland Ltd.
FRANCE	2021-12-31	90,000,000	Google LLC

Audit – do you need it, do you care?!

What were they actually fined for?



Quoted Art.	Type Filter Column
Unknown	Non-compliance with general data processing principles
Art. 5 (1) a), c) GDPR, Art. 6 (1) GDPR, Art. 12 (1) GDPR, Art. 24 GDPR, Art. 25 (1), (2) GDPR, Art. 35 GDPR	Non-compliance with general data processing principles
Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR	Non-compliance with general data processing principles
Art. 25 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security
Art. 5 (1) a) GDPR, Art. 12 GDPR, Art. 13 GDPR, Art. 14 GDPR	Insufficient fulfilment of information obligations
Art. 82 loi Informatique et Libertés	Insufficient legal basis for data processing

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

Audit – Voting

Please vote for one of the options below

- Option 1:

Problem? What problem?

Audit – Voting

Please vote for one of the options below

- Option 2:

© Can Stock Photo

A shovel of sand hides many things…

Audit – Voting

Please vote for one of the options below

- Option 3:

Are you too busy to improve?
No thanks!
We are too busy

Created by Håkan Forss @hakanforss http://hakanforss.wordpress.com

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

Audit needs and musts

- 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

Audit needs and musts

- … 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

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

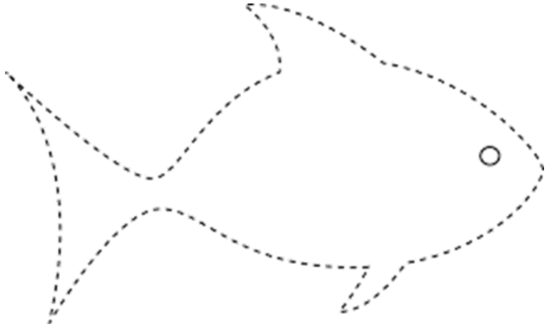
- Cons:
  - Not all required data is logged
    - SELECTs are especially lacking

Solution overview and their Pros/Cons

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!



Solution overview and their Pros/Cons

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

Solution overview and their Pros/Cons

Db2 Trace:

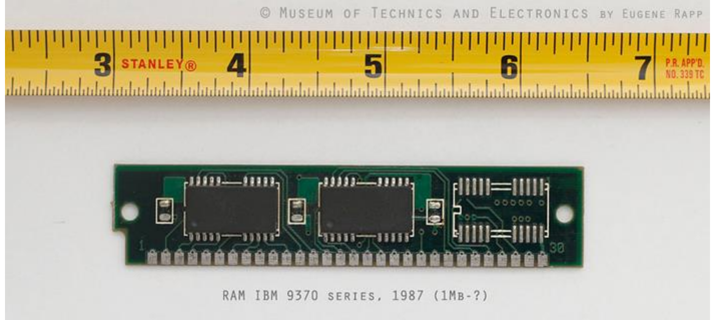
- What are the differences:
    - Processing the data requires simple to more sophisticated knowledge:
        - SMF: System Management Facility:
          Most commonly used, easy to process (use DSN1SMFP) – Once a day “cuts” cost 24 hours
        - OPn/OPX: Buffer Destination Trace
          very efficient, 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



© Museum of Technics and Electronics by Eugene Rapp

RAM IBM 9370 series, 1987 (1Mb-?)

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. I connection gets lost they try to cache it. Keep in mind that attackers do DDo 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

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)

Regular extracts are needed to catch the full SQL in case the statement is flushed!

400/401 Static SQL (SELECT, INSERT, etc.)

(+SYSPACKSTMT for the full SQL statement)

The viable way – let Db2 do the magic

What else do need? Well lets run through the required IFCIDs that deliver an Audit solution!

23/24/25	Utility start, phase change, and stop
219/220	Utility Listdef and Template
55/83/87/169/319	SQLID setting
62/142	DDL and CREATE/ALTER/DROP for tables with AUDIT changes or all
90/91	Commands and their completion status –Very important!

The viable way – let Db2 do the magic

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

The viable way – let Db2 do the magic

Add the Correlation Header processing and you are done!

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!

The viable way – let Db2 do the magic

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 the IFCIDs listed have a much smaller footprint than a blanket AUDIT CHANGES/ALL added to ever table that you have.

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

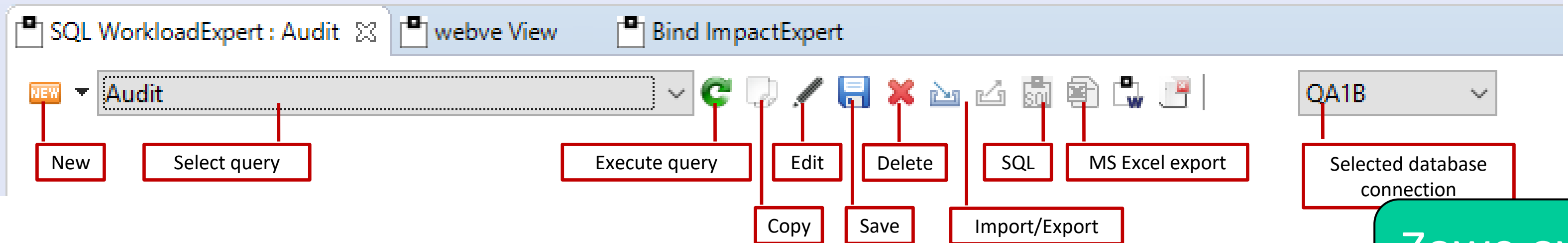
Use a GUI front end:

Exploit and integrate into Eclipse based GUI front ends

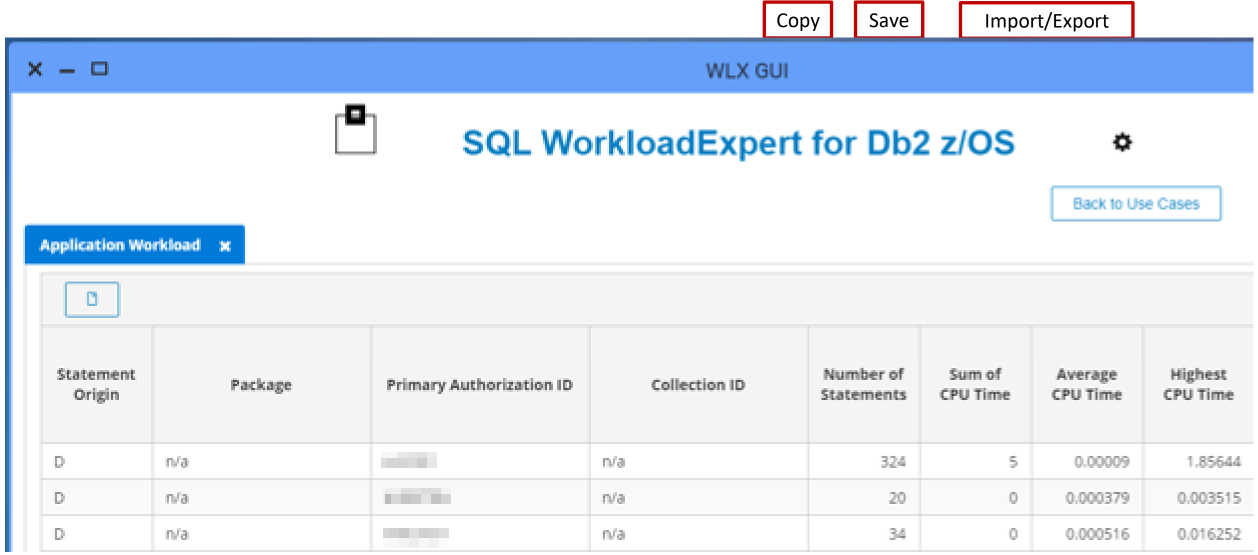
- GUIs can come as a Plug-in for
  - IBM Rational
  - IBM Data Studio
  - Eclipse native
- Use ZOWE – It rocks! HTML5 Graphics out-of-the-box
- Existing Db2 connections are used to connect to the mainframe
- Interactive dialogs allow complex and powerful analysis
- Export features can create PDF reports and allow MS Excel handover

The viable way – let Db2 do the magic

GUI features – button overview



Zowe overview



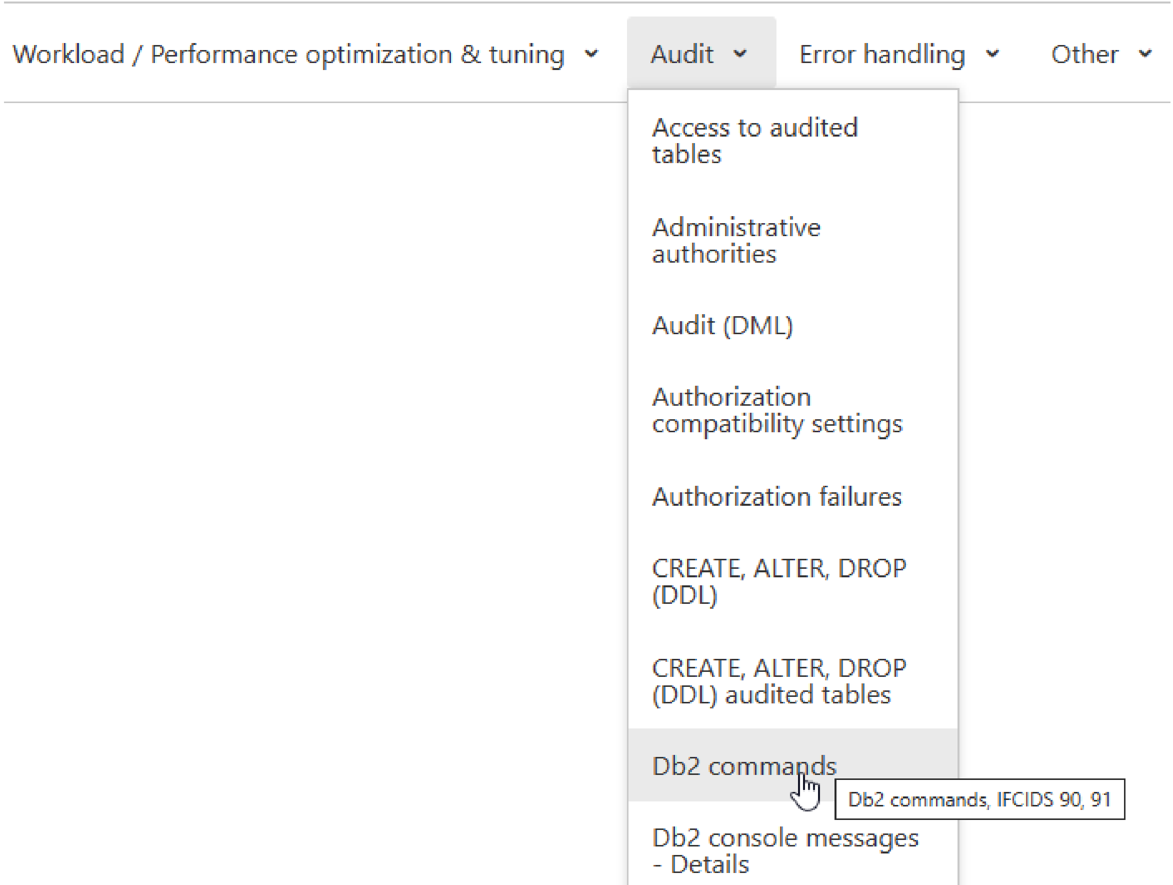
SQL WorkloadExpert for Db2 z/OS

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

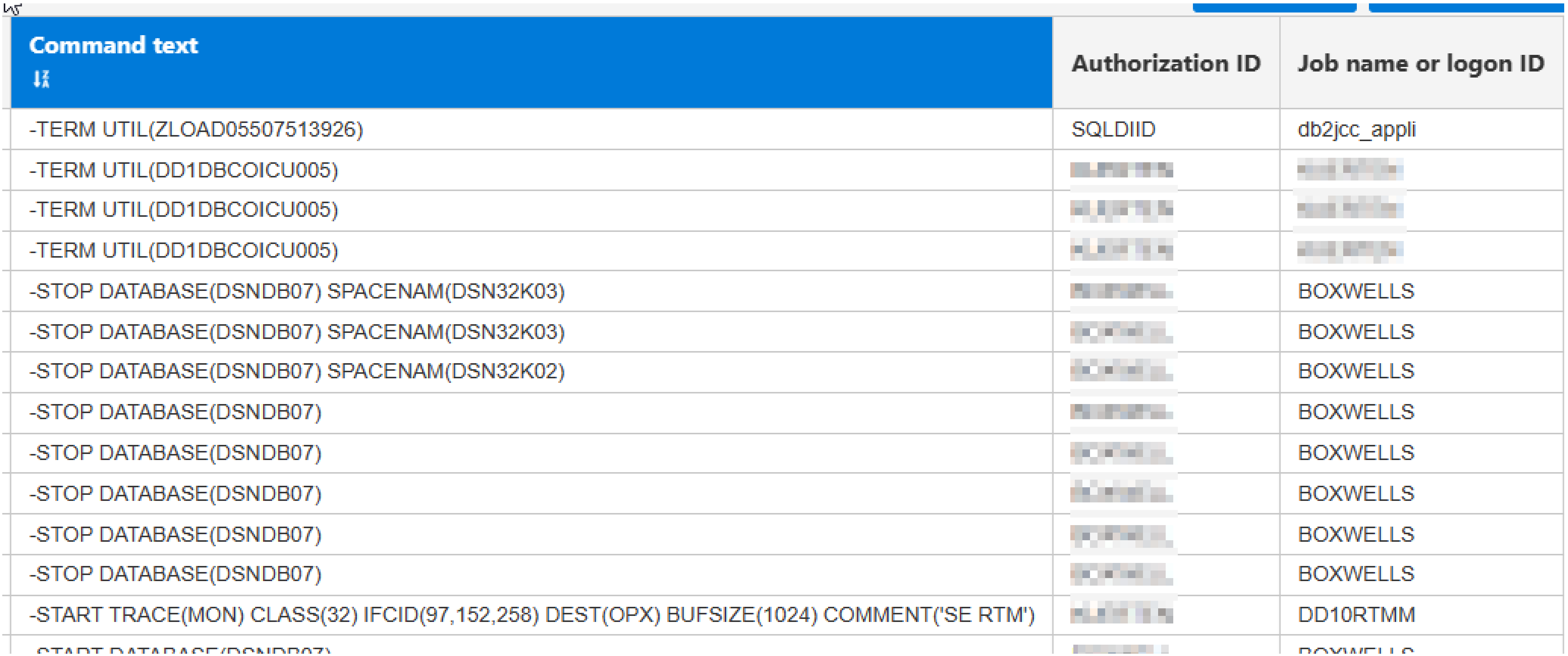
The viable way – let Db2 do the magic

SQL WorkloadExpert for Db2 z/OS

Delivered Use Cases make using the product as easy as possible


Workload / Performance optimization & tuning
Audit
Error handling
Other
Access to audited tables
Administrative authorities
Audit (DML)
Authorization compatibility settings
Authorization failures
CREATE, ALTER, DROP (DDL)
CREATE, ALTER, DROP (DDL) audited tables
Db2 commands
Db2 commands, IFCIDS 90, 91
Db2 console messages - Details

The viable way – let Db2 do the magic

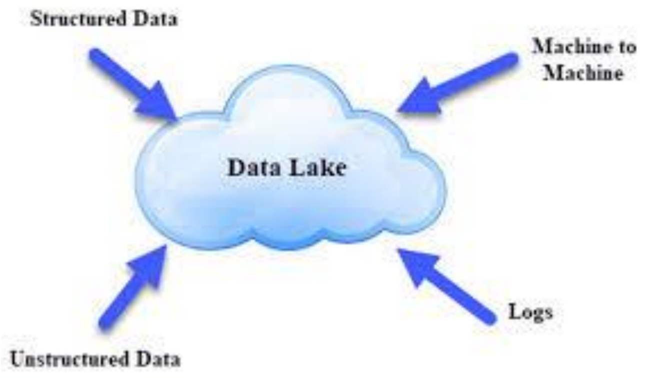


Command text	Authorization ID	Job name or logon ID
-TERM UTIL(ZLOAD05507513926)	SQLDIID	db2jcc_appli
-TERM UTIL(DD1DBCOICU005)	[redacted]	[redacted]
-TERM UTIL(DD1DBCOICU005)	[redacted]	[redacted]
-TERM UTIL(DD1DBCOICU005)	[redacted]	[redacted]
-STOP DATABASE(DSNDB07) SPACENAM(DSN32K03)	[redacted]	BOXWELLS
-STOP DATABASE(DSNDB07) SPACENAM(DSN32K03)	[redacted]	BOXWELLS
-STOP DATABASE(DSNDB07) SPACENAM(DSN32K02)	[redacted]	BOXWELLS
-STOP DATABASE(DSNDB07)	[redacted]	BOXWELLS
-STOP DATABASE(DSNDB07)	[redacted]	BOXWELLS
-STOP DATABASE(DSNDB07)	[redacted]	BOXWELLS
-STOP DATABASE(DSNDB07)	[redacted]	BOXWELLS
-STOP DATABASE(DSNDB07)	[redacted]	BOXWELLS
-START TRACE(MON) CLASS(32) IFCID(97,152,258) DEST(OPX) BUFSIZE(1024) COMMENT('SE RTM')	[redacted]	DD10RTMM
-START DATABASE(DSNDB07)	[redacted]	BOXWELLS

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 one or two 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

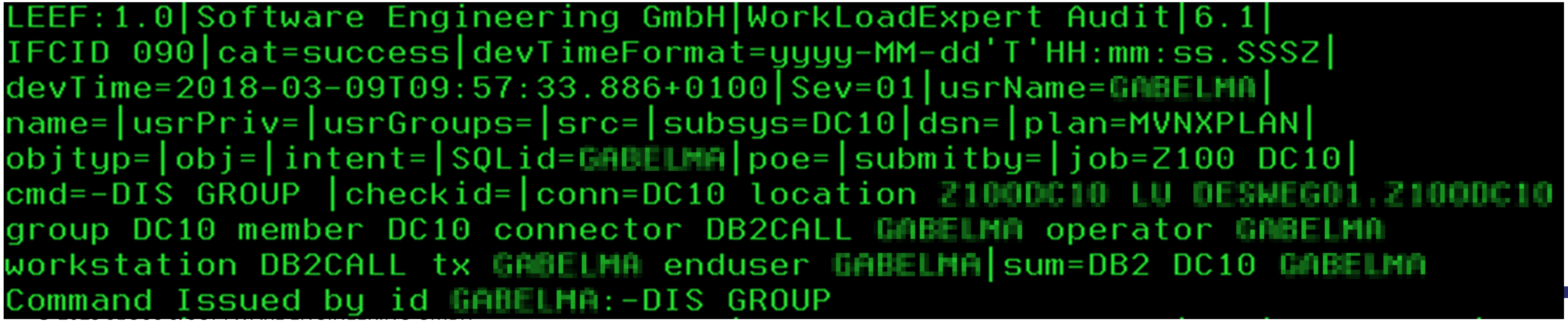


The viable way – let Db2 do the magic

So you can optionally export the data in LEEF (Log Event Extended Format) or syslogger format for the SIEM system of your choice!

Syslog

Radar



```
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=[redacted]|
name=|usrPriv=|usrGroups=|src=|subsys=DC10|dsn=|plan=MVNXPLAN|
objtyp=|obj=|intent=|SQLid=[redacted]|poe=|submitby=|job=Z100 DC10|
cmd=-DIS GROUP |checkid=|conn=DC10 location [redacted]
group DC10 member DC10 connector DB2CALL [redacted] operator [redacted]
workstation DB2CALL tx [redacted] enduser [redacted]|sum=DB2 DC10 [redacted]
Command Issued by id [redacted]:-DIS GROUP
```

Questions???

Many thanks for your attention and now….