Securely auditing your mainframe Db2 for z/OS data usage

Roy Boxwell
Software Engineering GmbH

Agenda

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

Agenda

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

Audit – do you need it, do you care?!

YES!

Audit – do you need it, do you care?!

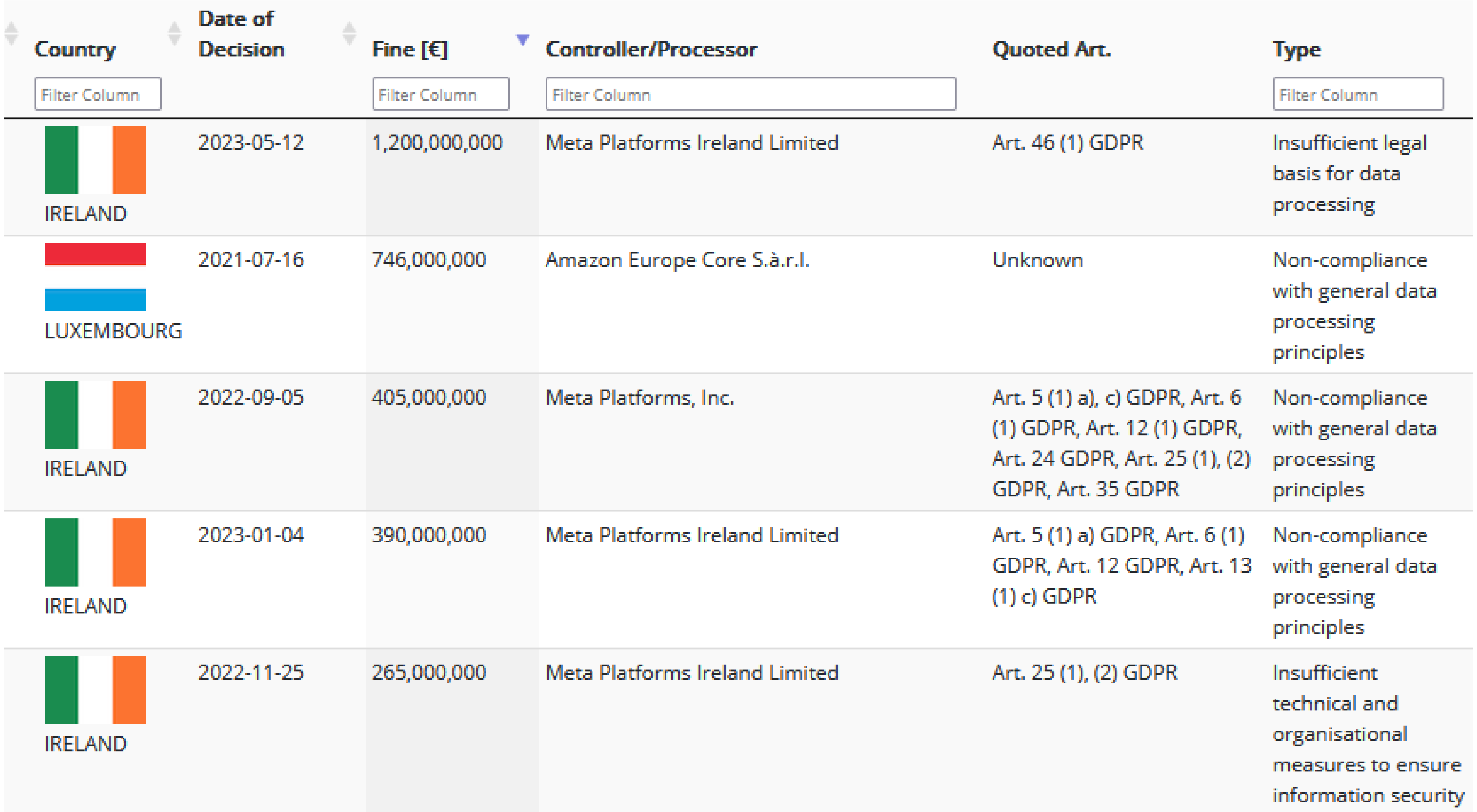
GDPR is in force and companies are paying mega-bucks!

Just go here:

https://www.enforcementtracker.com/

And sort by “Fine” descending…

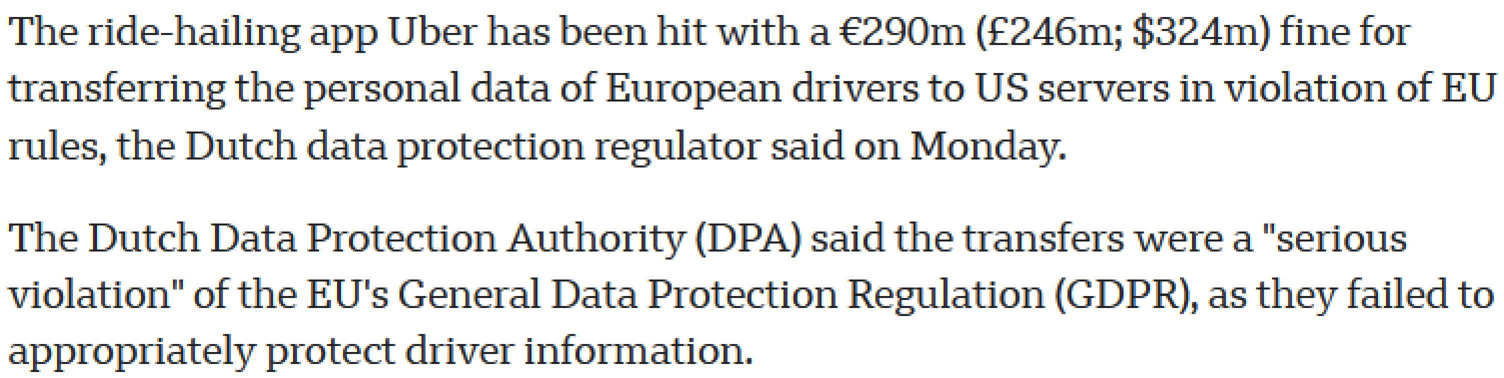
Audit – do you need it, do you care?!



Country	Date of Decision	Fine [€]	Controller/Processor	Quoted Art.	Type
Filter Column		Filter Column	Filter Column		Filter Column
IRELAND	2023-05-12	1,200,000,000	Meta Platforms Ireland Limited	Art. 46 (1) GDPR	Insufficient legal basis for data processing
LUXEMBOURG	2021-07-16	746,000,000	Amazon Europe Core S.à.r.l.	Unknown	Non-compliance with general data processing principles
IRELAND	2022-09-05	405,000,000	Meta Platforms, Inc.	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
IRELAND	2023-01-04	390,000,000	Meta Platforms Ireland Limited	Art. 5 (1) a) GDPR, Art. 6 (1) GDPR, Art. 12 GDPR, Art. 13 (1) c) GDPR	Non-compliance with general data processing principles
IRELAND	2022-11-25	265,000,000	Meta Platforms Ireland Limited	Art. 25 (1), (2) GDPR	Insufficient technical and organisational measures to ensure information security

Audit – do you need it, do you care?!

Fresh off the press on the 26th August 2024:



The ride-hailing app Uber has been hit with a €290m (£246m; $324m) fine for transferring the personal data of European drivers to US servers in violation of EU rules, the Dutch data protection regulator said on Monday.

The Dutch Data Protection Authority (DPA) said the transfers were a "serious violation" of the EU's General Data Protection Regulation (GDPR), as they failed to appropriately protect driver information.

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 needs and musts
3. Solution overview and their Pros/Cons
4. The viable way – let Db2 do the magic!
5. A special announcement!

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 269, 270) has low overhead
    - Trusted context DDL and Usage
  - IFCIDs 90, 91 have very little overhead
    - Db2 Commands

Agenda

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

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

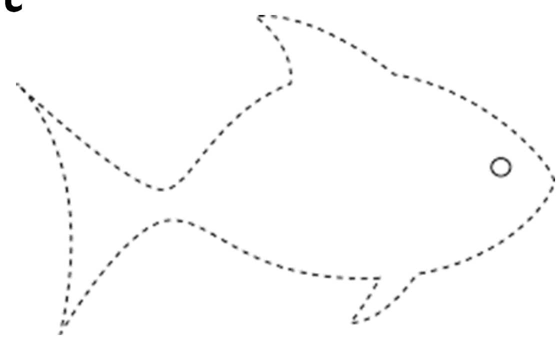
- Cons:
  - Not all required data is logged
    - SELECTs are especially lacking

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:

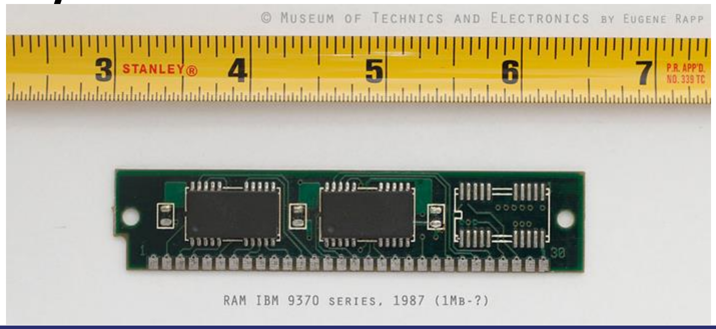
- What are the differences:
  - Processing the data requires simple to more sophisticated knowledge:
    - SMF: System Management Facility:
      Most commonly used, easy to process (use DSN1SMFP) – Once a day "cuts" cost 24 hours
    - OPn/OPX: Buffer Destination Trace
      very efficient, but Assembler 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. If the connection gets lost they try to cache it. Keep in mind that attackers do DDoS attacks!

Agenda

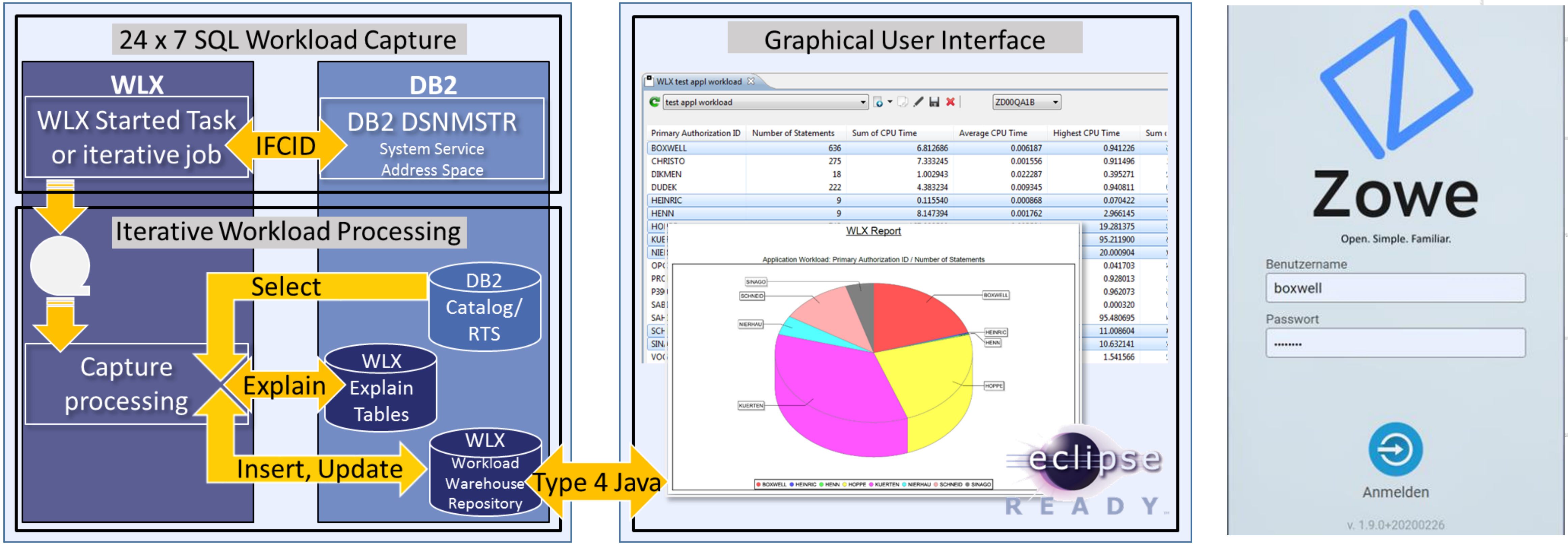
1. Audit – do you need it, do you care?!
2. Audit needs and musts
3. Solution overview and their Pros/Cons
4. The viable way – let Db2 do the magic!
5. A special announcement!

The viable way – let Db2 do the magic

Efficient data collector for your desired scope of Audit

Mainframe Engine

Workstation Engine


24 x 7 SQL Workload Capture
WLX
WLX Started Task or iterative job
IFCID
DB2
DB2 DSNMSTR
System Service Address Space
Iterative Workload Processing
Select
DB2 Catalog/ RTS
Capture processing
Explain
WLX Explain Tables
Insert, Update
WLX Workload Warehouse Repository
Type 4 Java
Graphical User Interface
WLX Report
Application Workload: Primary Authorization ID / Number of Statements
SINAGO
SCHNEID
NIERHAU
KUERTEN
BOXWELL
HEINRIC
HENN
HOPPE
BOXWELL HEINRIC HENN HOPPE KUERTEN NIERHAU SCHNEID SINAGO
eclipse
READY
Zowe
Open. Simple. Familiar.
Anmelden
v. 1.9.0+20200226

WLX test appl workload

test appl workload

ZD00QA1B

Primary Authorization ID	Number of Statements	Sum of CPU Time	Average CPU Time	Highest CPU Time	Sum
BOXWELL	636	6.812686	0.006187	0.941226	
CHRISTO	275	7.333245	0.001556	0.911496	
DIKMEN	18	1.002943	0.022287	0.395271	
DUDEK	222	4.383234	0.009345	0.940811	
HEINRIC	9	0.115540	0.000868	0.070422	
HENN	9	8.147394	0.001762	2.966145	
HO				19.281375	
KUE				95.211900	
NIE				20.000904	
OP				0.041703	
PR				0.928013	
P39				0.962073	
SAB				0.000320	
SAH				95.480695	
SCH				11.008604	
SIN				10.632141	
VO				1.541566	

Benutzername: boxwell

Passwort: ••••••••

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
55/83/87/169/319	SQLID setting
62/142	DDL and CREATE/ALTER/DROP for tables with AUDIT changes or all
90/91	Commands and their completion status

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 DDL/Usage and Column Masks/Row Permissions
361	Administrative Authority usage
404	LOAD Authority usage

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!

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 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

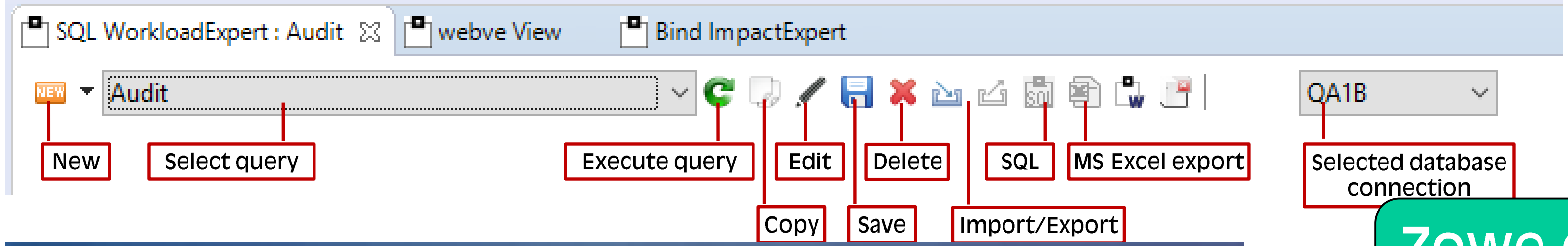
Use a GUI front end:

Exploit and integrate into Eclipse based GUI front ends

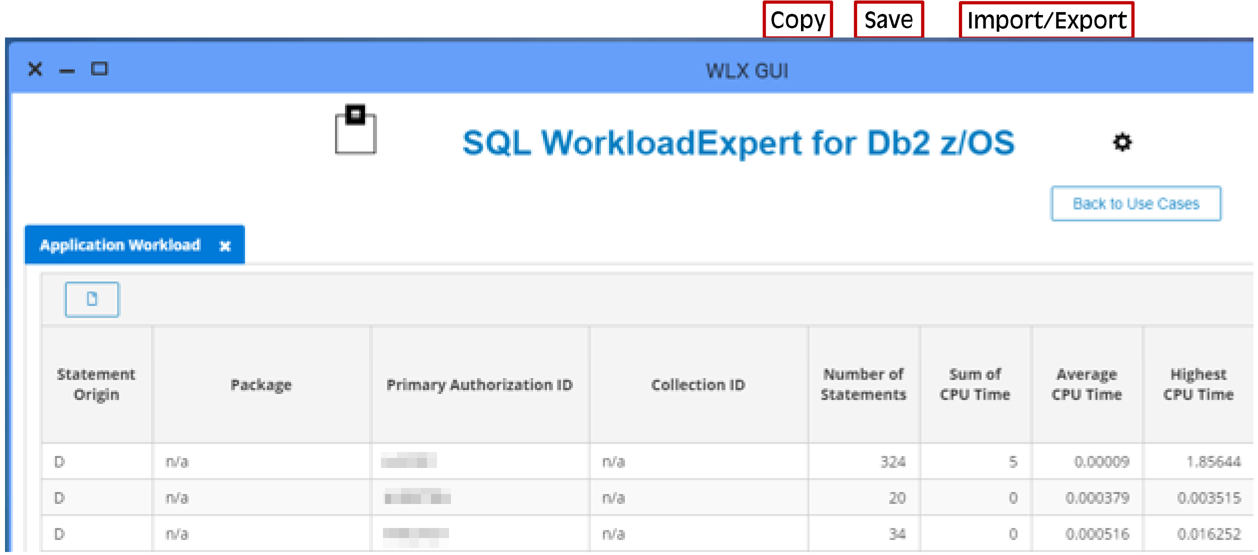
- GUIs can come as a Plug-in for
  - IBM Rational
  - IBM Data Studio
  - Eclipse native
- Use Zowe – It rocks!
- Existing Db2 connections are used to connect to the mainframe
- Interactive dialogs allow complex and powerful analysis
- Export features can create PDF reports and allow MS Excel handover

The viable way – let Db2 do the magic

GUI features – button overview



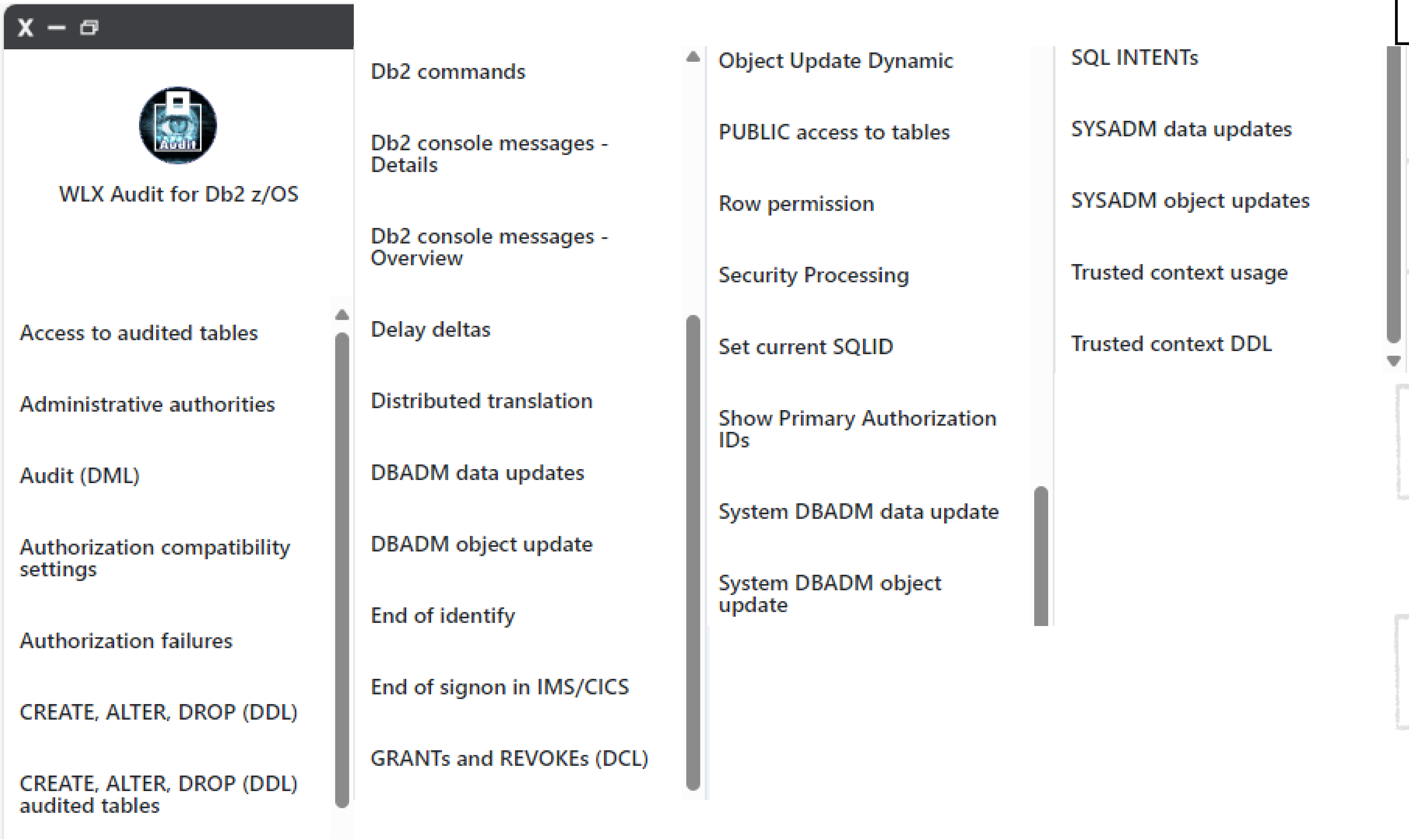
Zowe overview



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

Choose how you’d like to find out who did what and when…

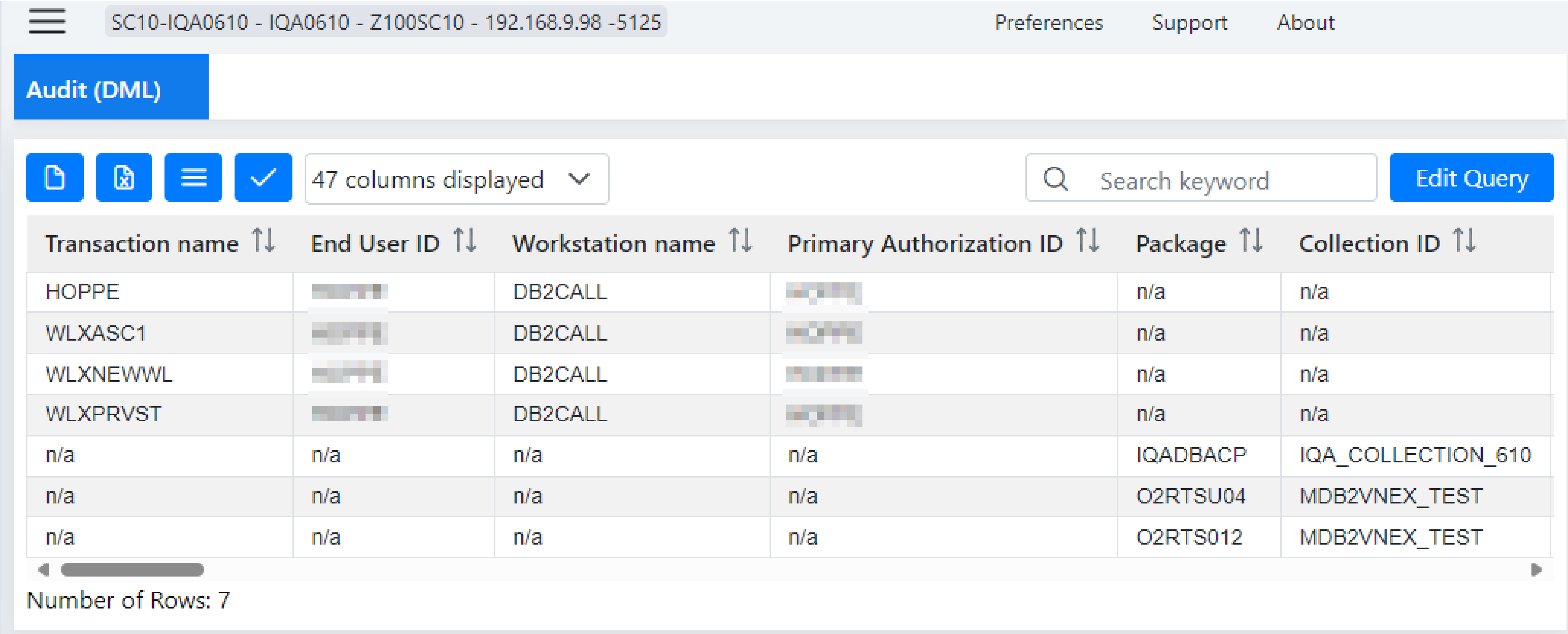


WLX Audit for Db2 z/OS

- 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 console messages - Details
- Db2 console messages - Overview
- Delay deltas
- 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…

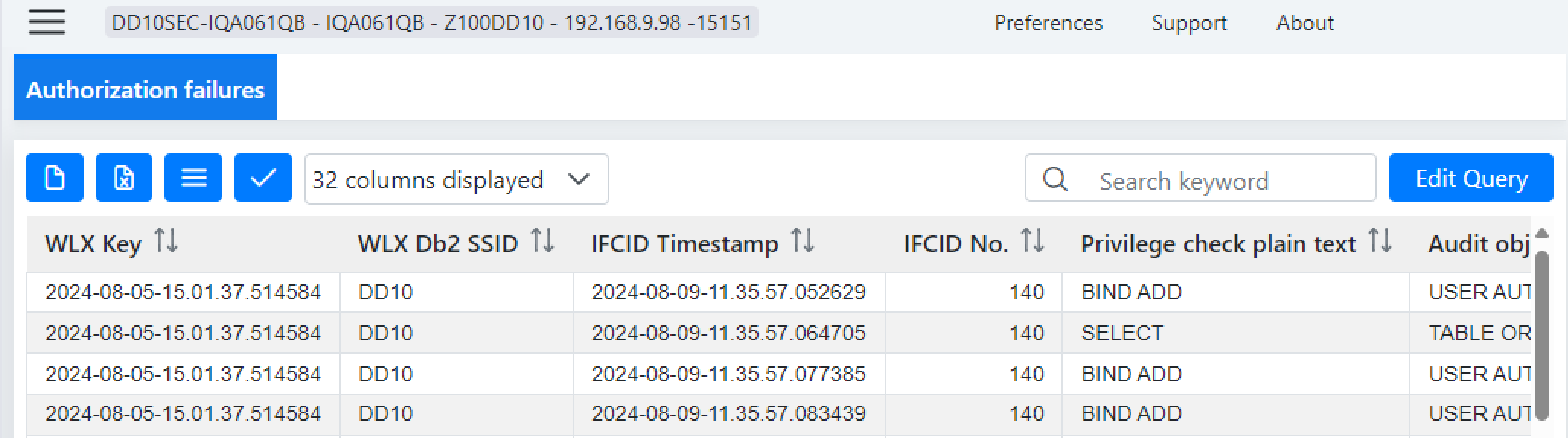


Transaction name	End User ID	Workstation name	Primary Authorization ID	Package	Collection ID
HOPPE	[redacted]	DB2CALL	[redacted]	n/a	n/a
WLXASC1	[redacted]	DB2CALL	[redacted]	n/a	n/a
WLXNEWWL	[redacted]	DB2CALL	[redacted]	n/a	n/a
WLXPRVST	[redacted]	DB2CALL	[redacted]	n/a	n/a
n/a	n/a	n/a	n/a	IQADBACP	IQA_COLLECTION_610
n/a	n/a	n/a	n/a	O2RTSU04	MDB2VNEX_TEST
n/a	n/a	n/a	n/a	O2RTS012	MDB2VNEX_TEST

Number of Rows: 7

The viable way – let Db2 do the magic

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

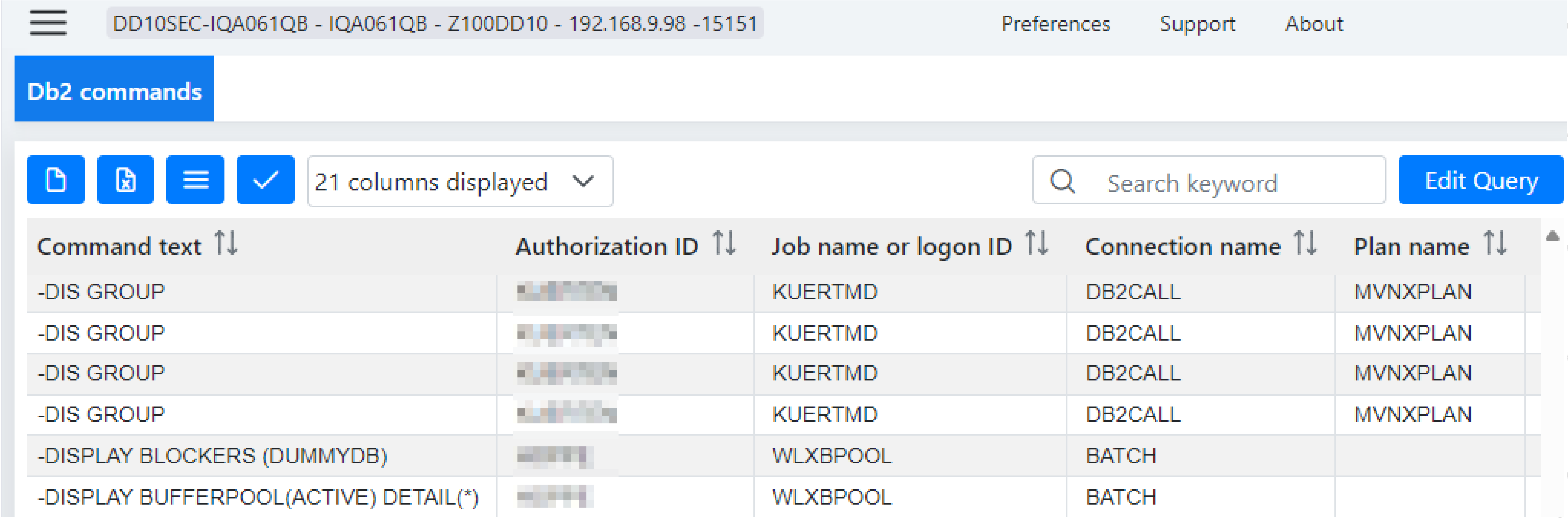


DD10SEC-IQA061QB - IQA061QB - Z100DD10 - 192.168.9.98 -15151

WLX Key	WLX Db2 SSID	IFCID Timestamp	IFCID No.	Privilege check plain text	Audit obj
2024-08-05-15.01.37.514584	DD10	2024-08-09-11.35.57.052629	140	BIND ADD	USER AUT
2024-08-05-15.01.37.514584	DD10	2024-08-09-11.35.57.064705	140	SELECT	TABLE OR
2024-08-05-15.01.37.514584	DD10	2024-08-09-11.35.57.077385	140	BIND ADD	USER AUT
2024-08-05-15.01.37.514584	DD10	2024-08-09-11.35.57.083439	140	BIND ADD	USER AUT

The viable way – let Db2 do the magic

Choose how you’d like to find out who did what and when…



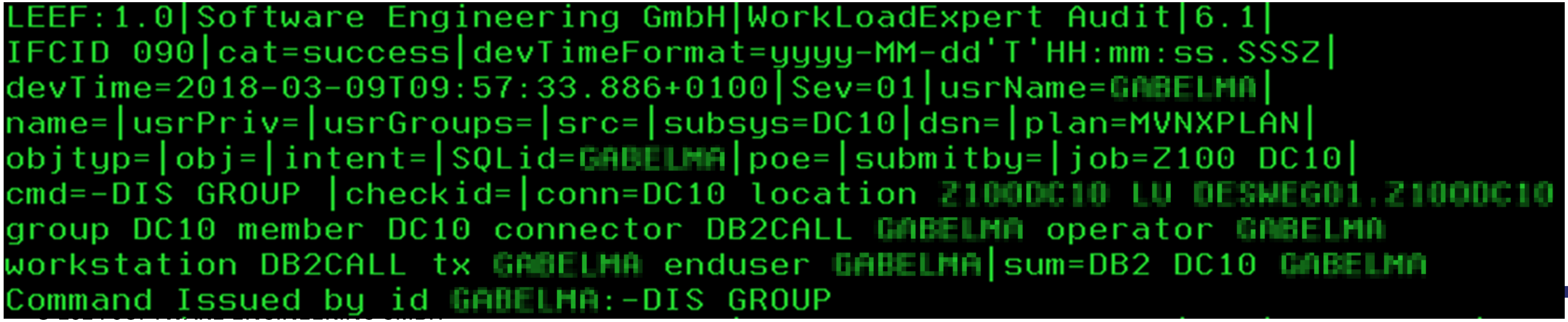
Command text	Authorization ID	Job name or logon ID	Connection name	Plan name
-DIS GROUP	[redacted]	KUERTMD	DB2CALL	MVNXPLAN
-DIS GROUP	[redacted]	KUERTMD	DB2CALL	MVNXPLAN
-DIS GROUP	[redacted]	KUERTMD	DB2CALL	MVNXPLAN
-DIS GROUP	[redacted]	KUERTMD	DB2CALL	MVNXPLAN
-DISPLAY BLOCKERS (DUMMYDB)	[redacted]	WLXBPOOL	BATCH	
-DISPLAY BUFFERPOOL(ACTIVE) DETAIL(*)	[redacted]	WLXBPOOL	BATCH	

The viable way – let Db2 do the magic

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

Syslog

Radar

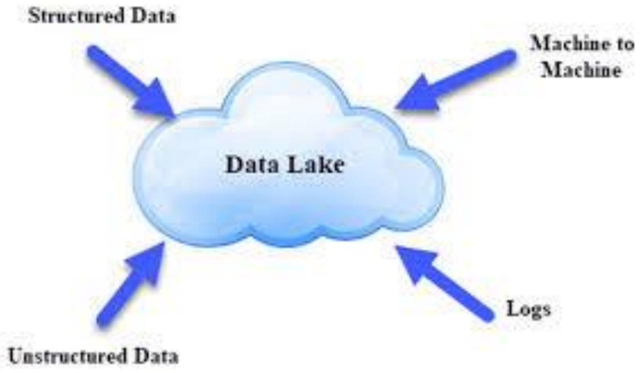


```
LEEF:1.0|Software Engineering GmbH|WorkLoadExpert Audit|6.1|
IFCID 090|cat=success|devTimeFormat=yyyy-MM-dd'T'HH:mm:ss.SSSZ|
devTime=2018-03-09T09:57:33.886+0100|Sev=01|usrName=[redacted]|
name=|usrPriv=|usrGroups=|src=|subsys=DC10|dsn=|plan=MVNXPLAN|
objtyp=|obj=|intent=|SQLid=[redacted]|poe=|submitby=|job=Z100 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
```

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



Agenda

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

Agenda

1. Audit – do you need it, do you care?!
2. Audit needs and musts
3. Solution overview and their Pros/Cons
4. The viable way – let Db2 do the magic!
5. A free Security Audit Check for Db2 z/OS

Security Audit Check for Db2 z/OS

This year's SEG Christmas give-away will be a free Security Audit Check for Db2 z/OS – Short form: SAC2.

It audits six "classes" of things:

1) All security relevant ZPARMs including defaults that should not be left at their default value! As well as DDF settings for TLS.
2) The Communication Database (CDB).
3) All grants to objects in the Db2 Catalog, Directory, XML , AI.
4) All grants to PUBLIC or grants "with grant" option.
5) Trusted Contexts, Row Permissions, Column Masks, Audit Policies and Roles.
6) Privileged user Ids (SYSADM, SYSOPR, SQLADM etc.)

Security Audit Check for Db2 z/OS

All security relevant ZPARMs:

AUDITST
AUTH
AUTH_COMPATIBILITY
AUTHEXIT_CACHEREFRESH
AUTHEXIT_CHECK
BINDNV
DBACRVW
DISALLOW_SSARAUTH
ENCRYPTION_KEYLABEL
EXTSEC
REVOKE_DEP_PRIVILEGES
SECADM1
SECADM2
SEPARATE_SECURITY
SYSADM
SYSADM2
SYSOPR1
SYSOPR2
TCPALVER

Security Audit Check for Db2 z/OS

Defaults that should **not** be left at their default value:

Catalog Alias
Member Name
Command prefix
Db2 Location Name
DRDA Port

Group Name
SSID
Unknown User Id
Db2 LU Name
SECURE Port

Any of these still being at its default value is leaving your system a little bit more open than it should be!

For Ports it also checks that SSL is active and all ALIAS usage is also correct.

Security Audit Check for Db2 z/OS

The Communication Database (CDB). Reporting any problems found and recommendations:

- Use of SNA (VTAM is deprecated!)
- Use of SYSIBM.IPLIST (Not recommended any more)
- Any rows in SYSIBM.IPNAMES with a SECURITY_OUT value not = ‘R’
- Any rows in SYSIBM.LOCATIONS with SECURE = ‘N’
- Any rows in SYSIBM.LUNAMES with a SECURITY_OUT value not = ‘R’ or a SECURITY_IN value not = ‘V’
- USERNAMES listing out those with spaces in AUTHID, LINKNAME or NEWAUTHID

Security Audit Check for Db2 z/OS

Use of grants to PUBLIC:

All SYSIBM.SYSxxxxxAUTH tables will be checked for any GRANTs to PUBLIC.

With, possibly, the exception of SYSIBM.SYSDUMMY1 there should be no grants to PUBLIC found.

Even the SYSIBM.SYSDUMMY1 should not really be done anymore!

All usage of WITH GRANT OPTION will be listed as this does not conform to modern security practices.

Security Audit Check for Db2 z/OS

Trusted Contexts, Row Permissions, Column Masks, Audit Policies and Roles:

All Trusted Contexts will be listed with Auth Ids and Attributes.

All Row Permissions will be listed.

All Column Masks will be listed.

All Audit Policy Usage will be decoded, listed and verified as being started and/or Tamper proof.

All Roles will be listed.

All of these must be individually validated that they are all 100% correct!

Security Audit Check for Db2 z/OS

All Privileged Ids will be listed with their respective Privilege(s):

SYSADM SYSOPR SQLADM
MONITOR1 MONITOR2 System DBADM
SYSCTRL DATAACCESS ACCESSCTRL
CREATE SECURE

All of these must be individually validated that they are all 100% correct!

Questions???

Many thanks for your attention and now….