

# DB2 z/OS Audit - Viable workload tracking.

**Craig Mullins and Ulf Heinrich**  
*SEGUS & SOFTWARE ENGINEERING*

Session Code: V02

On May 24, 2016 | at 1pm | Platform: DB2 for z/OS



# AGENDA

- 1. Audit needs and musts**
- 2. Solution overview and their Pros/Cons**
- 3. The viable way – let DB2 do the magic!**
- 4. Customer results from the banking industry**

# Security and data breach protection



Source: 2015 Gemalto Breach Level Index <http://bit.ly/1PUCspY>

## Security and data breach protection

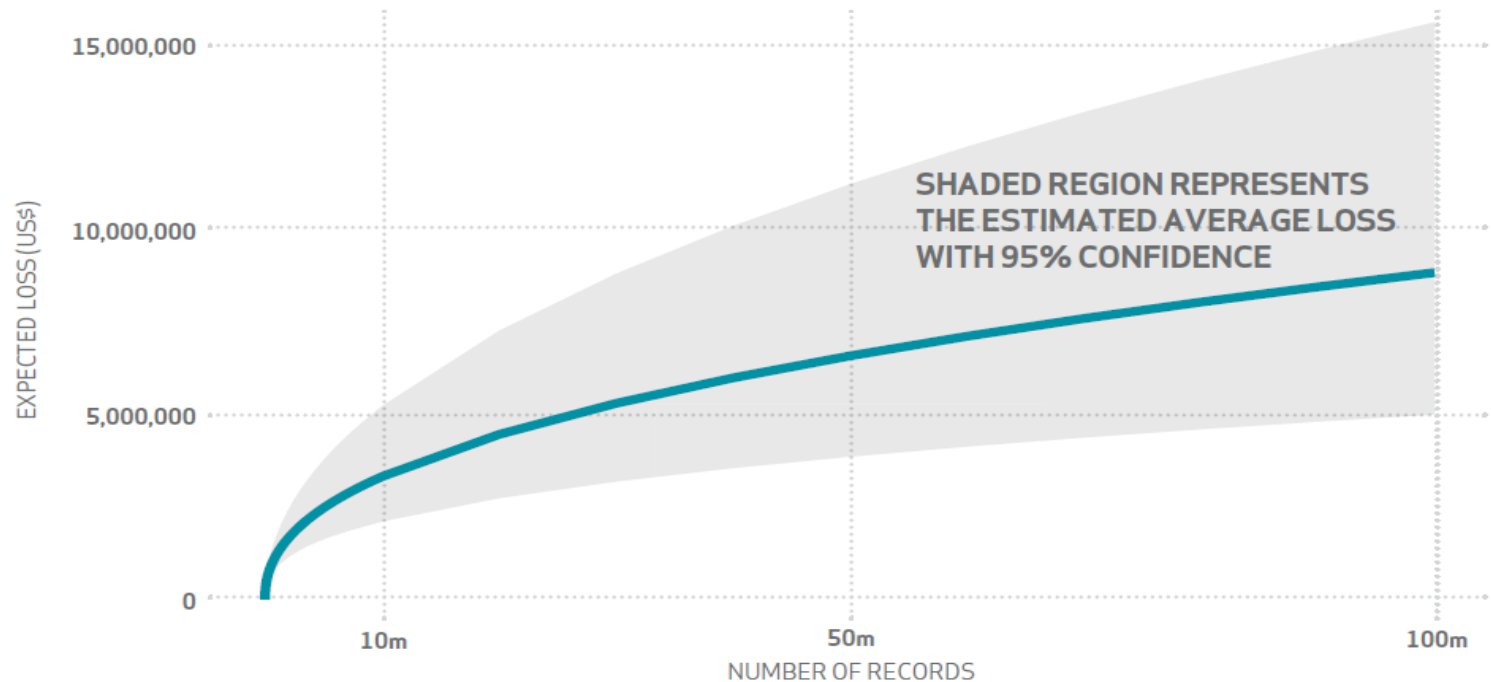
- According to the 2016 Cyberthreat Defense Report from CyberEdge Group
  - 85% are **spending more** than 5% of their IT budgets on security. Nearly a third are spending more.
  - 76% were **affected by a successful cyberattack** in 2015.
  - Only 30% are confident that their organization has made **adequate investments** to monitor the activities of privileged users.
  - **Low security awareness** among employees continues to be the greatest inhibitor to defending against cyber threats, followed closely by **too much data for IT security teams to analyze**
- Reputation can be negatively impacted by data breaches
- Financial loss can be significant... *details next slide*





## The cost of a data breach

- Average loss for a breach of 1,000 records between \$52,000 and \$87,000
- Average loss for a breach affecting 10 million records between \$2.1 million and \$5.2 million

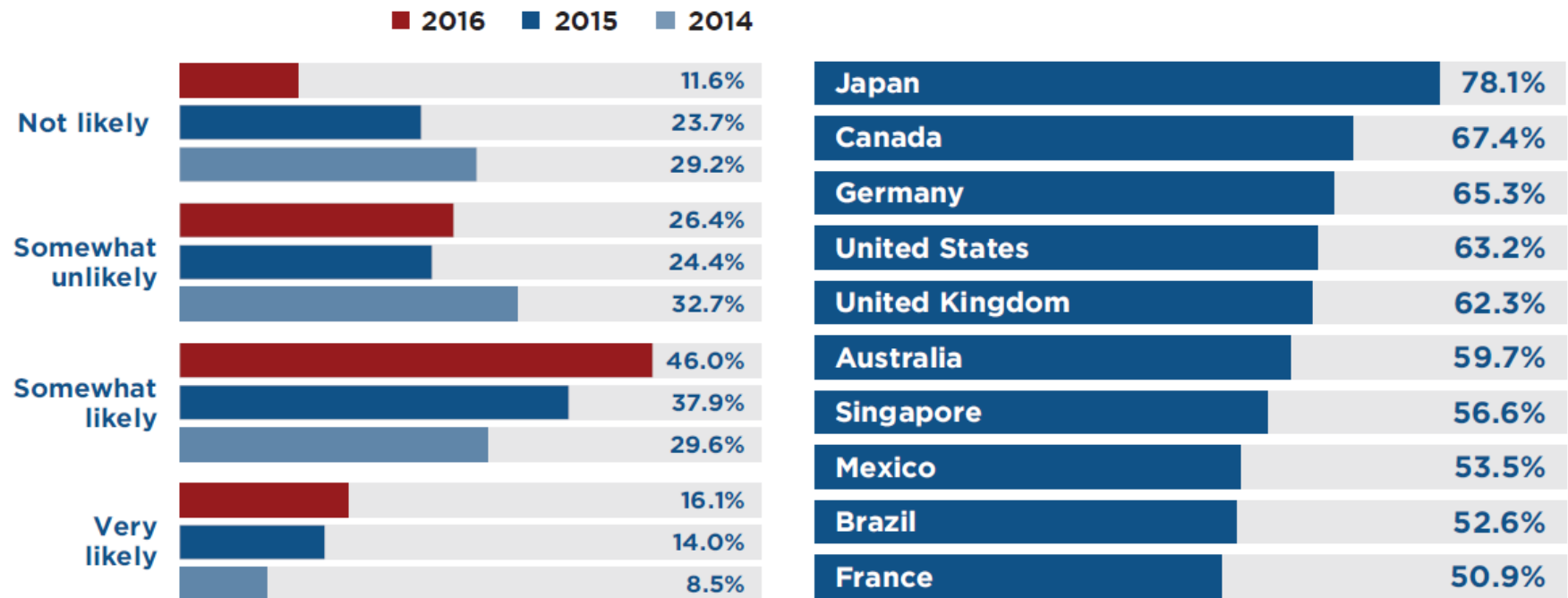


Source: 2015 Verizon Data Breach Investigation Report

# Number of cyber attacks likely to grow this year

## Future Likelihood of Successful Cyberattacks

What is the likelihood that your organization's network will become compromised by a successful cyberattack in 2016? (n=978)



Source: 2016 Cyberthreat Defense Report, CyberEdge Group

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

## Attackers use...

- SQL injection
- DDoS
- Third-party software
- XSS
- Malware
- Phishing
- Watering holes/Honey pots
- Physical access



... with the ultimate goal of gaining access to your crown jewels

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

Enterprise database servers are a primary target of many security breaches! Why?

- Because they contain your/your clients most valuable information...
  - Personally identifiable information (PII, such as SSN)
  - SPI, or sensitive personal information
  - Personal financial data (PFI, also credit reporting)
  - Bank account/credit card information
  - Health information

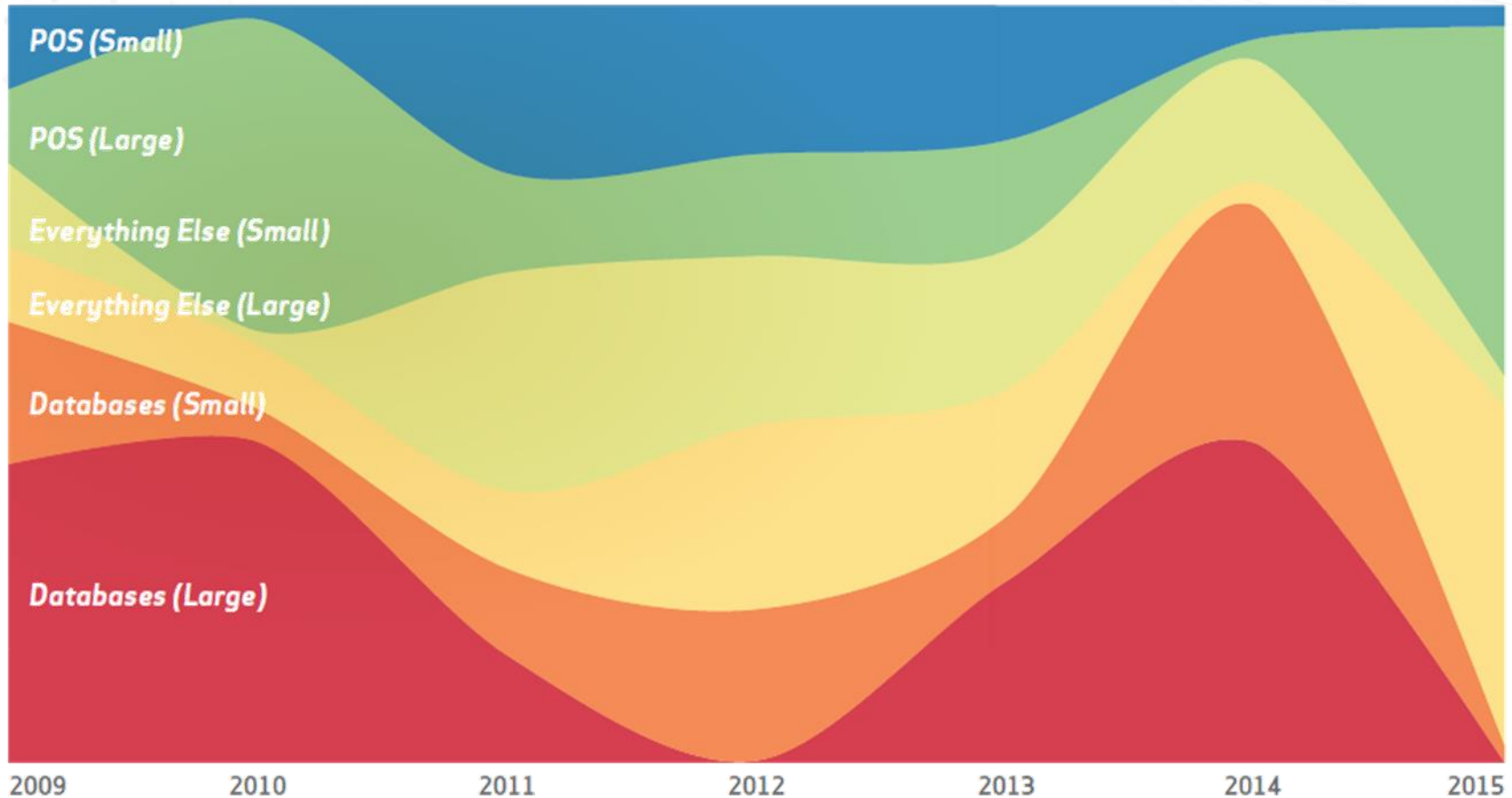
... and once they're in, there are high volumes of easy-to-access, structured data.

→ Companies (and governments) love Big Data – attackers love companies'/governments' databases!



# Databases are a significant target for attack

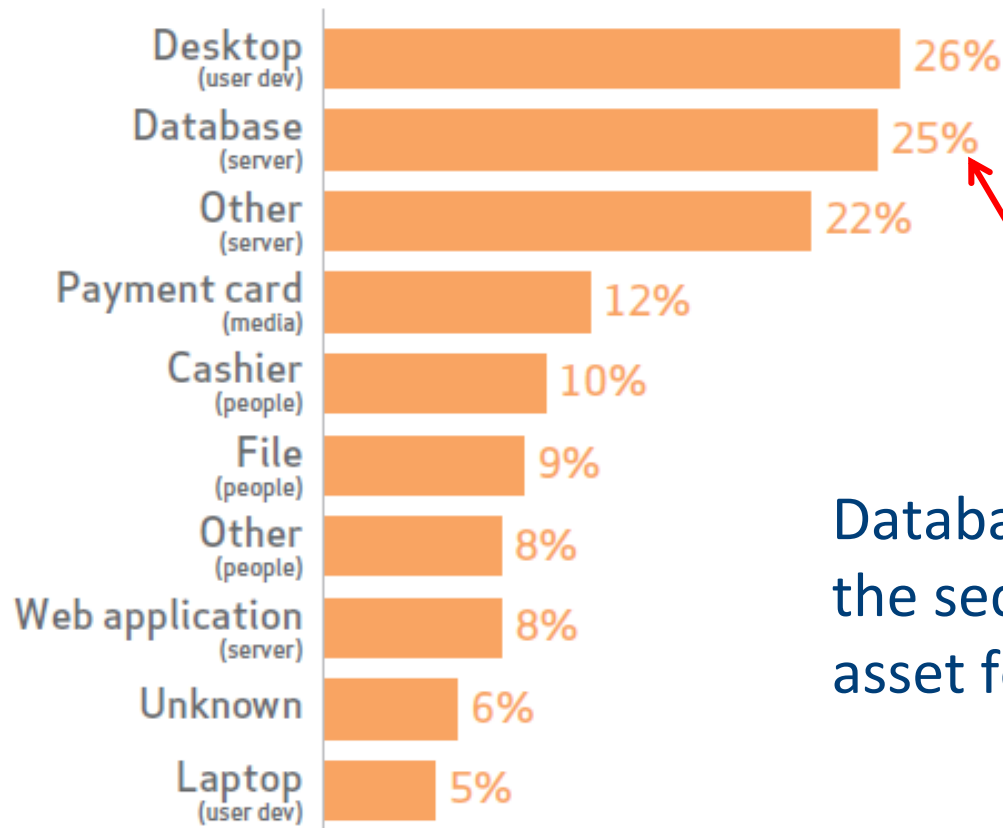
Small company = less than 1000 employee



Source: 2015 Verizon Data Breach Investigation Report

# Greatest inside misuse

## Top 10 assets affected within Insider Misuse (n=142)

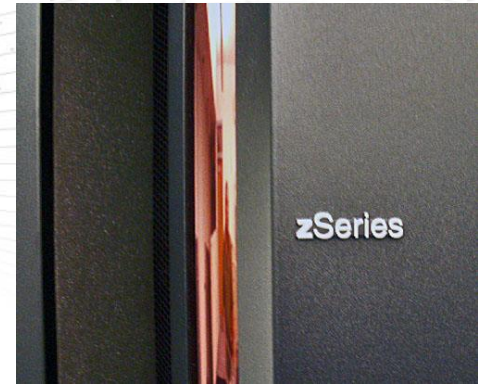


Database Servers constitute the second most affected asset for insider misuse.

Source: 2014 Verizon Data Breach Investigation Report

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

But the mainframe is safe – isn't it?!



- 50% of the concerns are about privileged insiders
- 29% of the concerns are with web-enabled z/OS apps
- 21% of the concerns are with advanced persistent threats

*“As mainframes become a major component in SOA, they are increasingly exposed to malware. Web services on the mainframe have significantly impacted security”*

President, Mittal Technologies Inc.

Source: IBM Webinar 2/6/2014, Security Intelligence Solutions for System z and the Enterprise

## Audit needs and musts

However, protecting and auditing is a major cost factor these days, so the authorities had to force companies to pay attention:

- SOX – Sarbanes Oxley Act
- FIEL – Financial Instruments and Exchange Law
- PCI DSS – Payment Card Industry Data Security Standards
- HIPAA – Health Insurance Portability and Accountability Act
- CMS ARS – Center for Medicare/Medicaid Services Acceptable Risk Safeguards
- GLBA – Gramm-Leach-Bliley Act (Financial Services Modernization)
- ISO 17799 (Basel II), ISO 27001 (Basel III)
- NERC – North American Electric Reliability Corporation
- NIST 800-53 (FISMA) - National Institute of Standards and Technology (Federal Information Security Management Act)

## Audit needs and musts

Chose your *favorite(s)* and/or use reliable resources for guidance along the way:

- **COBIT**  
Control Objectives for Information and Related Technology
- **Center for Internet Security (CIS)**  
online community that identifies, validates, promotes and sustains the adoption of cybersecurity's best practices.
- **Department of Defense (DoD)**  
guidelines and procedures for information quality
- **Security Technical Implementation Guide (STIG)**  
methodology for standardized secure installation and maintenance of computer software and hardware.
- **Common Vulnerability Exposure (CVE)**  
a dictionary of publicly known information security vulnerabilities and exposure
- **Bundesamt für Sicherheit in der Informationstechnik (BSI)**  
German: Federal Office for Security



# Audit needs and musts

Focusing on the major areas 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
SELECTs against sensitive data		X	X	X	X	X		X
Insert, Update, Delete	X			X		X		
Access violations	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

## Audit needs and musts

- It is important to match your data collection requirements to the regulations that apply to your business
- You may need more to satisfy business requirements
- *Breach patterns do change, so you probably won't know today what you could need tomorrow*
- Make sure have a way to collect:
  - SELECTs (against sensitive data)
  - Modifications (INS/UPD/DEL)
  - DDL
  - DCL
  - Utilities (online + offline)
  - Commands
  - Assignment, or modification 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 data sets
- Also consider your INSTALL SYSADM/SYSOPR
  - 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
    - GRANTs/REVOKEs
    - Assignment, or modification of a user ID/authorization
    - Start of a DB2 online utility
  - Class 3 has very little overhead
    - DDL (only for TB having the AUDIT ALL attribute)
  - Class 4, 5 up to 15% - 20% overhead
    - 1<sup>st</sup> SELECT, INSERT/UPDATE/DELETE of a UOR
  - IFCID 90, 91 have very little overhead
    - DB2 Commands

## Solution overview and their Pros/Cons

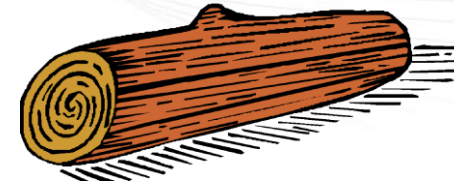
- There are a variety of existing resources DB2 already provides/comes with:
  - DB2 Log
  - DB2 Trace
  - DB2 Memory (DSC/EDM)
  - DB2 Exits
- And of course additional products





# 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)
  - Many 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

# 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
    - And it can be troubling to match your needs to the exact traces, classes, IFCIDs required
- 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)
    - 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:  
Not commonly 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
  - Lot's 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?
  - 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 use network sniffing, but that can be problematic for mainframe auditing
    - What if the request is DB2 batch or CICS and does not go over a network?
  - Some solutions need additional appliances (some may require 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!

# Solution overview and their Pros/Cons

## Additional Tools:

- What are the differences?
  - Some solutions exploit zIIP processors
    - Optional (scope)
    - Forced usage
  - Some solutions offer reporting in real-time
  - Some solutions offer alerting
    - This requires a rule, or profile setup  
→ keep in mind that they are based on known patterns
  - and of course solutions differ in
    - Setup (collector per DB2 system/LPAR)
    - Filtering
    - Dedicated support of compliance reports

# Solution overview and their Pros/Cons

## Additional Tools:

- What are the differences?
  - Some solutions have additional capabilities:
    - Covering a variety of databases (DB2 z/OS/LUW, IMS, Oracle, SQL Server, ...)
    - Covering applications (CICS, SAP, ...)
    - Covering dataset activity and Content Managers (VSAM, FTP, SharePoint, ...)
    - Covering Big Data (Hadoop, HANA, ...)
    - Covering vulnerability scanning of up to entire infrastructures (including network, firewall, workstations, ...)
    - Covering logons, connects

→ Depending on your choice it may become complex and expensive and you're locked to a specific vendor!



# Solution overview and their Pros/Cons

## Additional Tools:

- What are the differences?
- Guess What?!

→ Several tools exploit the IFI collector!

## 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 of SMF processing:

- 23/24/25 Utility start/phase/stop (+219=Listdef+220=DSs)
- 90/91 Commands and their completion status
- 140 Authorization failures
- 141 Authorization changes
- 62/142 DDL/DDI for tables with audit changes/all
- 316/318 Dynamic SQL (SELECT, INSERT, UPDATE, DELETE)  
(+317 for the full SQL statement)
- 400/401 Static SQL (SELECT, INSERT, UPDATE, DELETE)  
(+SYSPACKSTMT for the full SQL statement)

Add the correlation headers to get detailed authentication data

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 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 exploiting proven, integrated technology
- ➔ No new vulnerabilities:
  - 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)

If you don't want to improve your Home Grown solution, find a vendor who exploits this technology

# The viable way – let DB2 do the magic

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

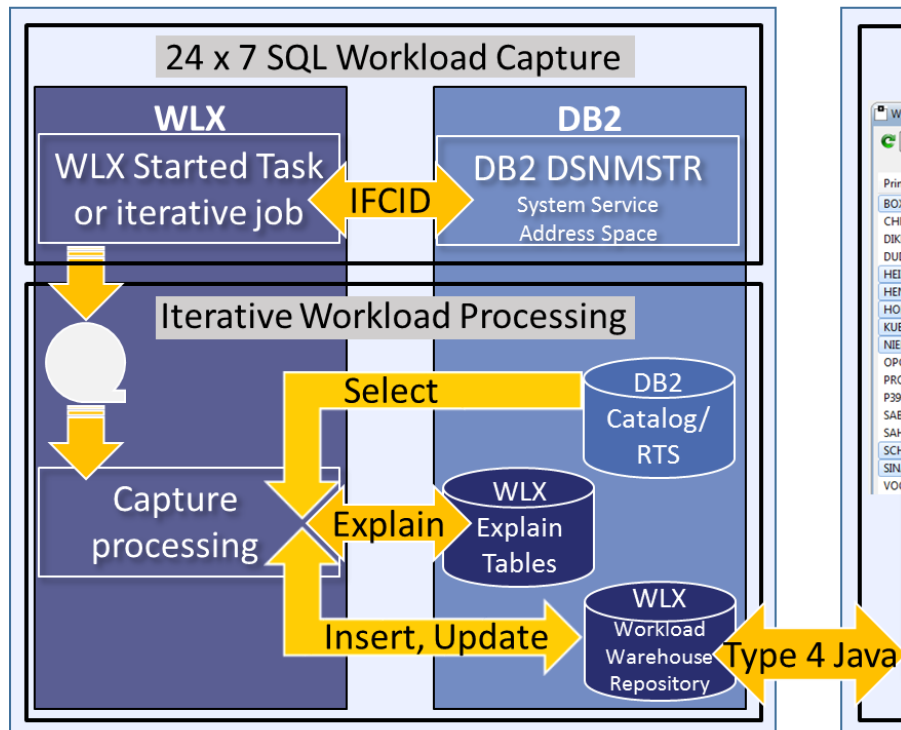
- SQL text
- Statement ID
- Date/time
- Current status
- Resource consumption
- Identification/environmental data



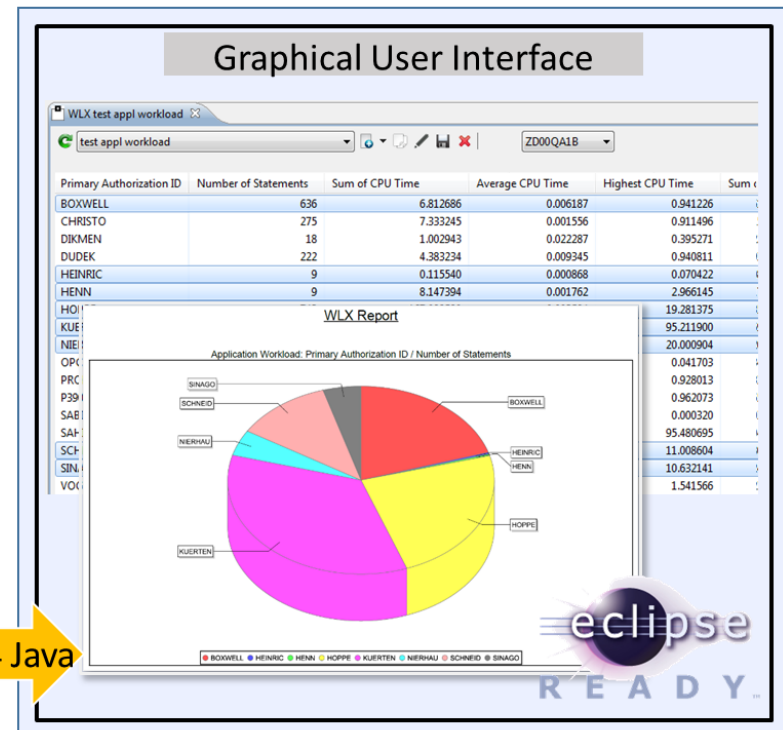
# The viable way – let DB2 do the magic

Efficient data collector for your  
desired scope of Audit

## Mainframe Engine



## Workstation Engine



# The viable way – let DB2 do the magic

## Capture the data e.g. using a STC:

Run a started task 24x7 to catch all the IFCIDs that DB2 will be throwing and store the data.

## Process the workload:

Externalize and process the data, such as every 60 min:

- customizable (e.g. 30 - 180 minutes)
- allow Ad hoc data refresh triggered via operator command for the started task (MODIFY)
- capture the SQL Text at trace time



# The viable way – let DB2 do the magic

## Use a GUI front end, preferably Eclipse:

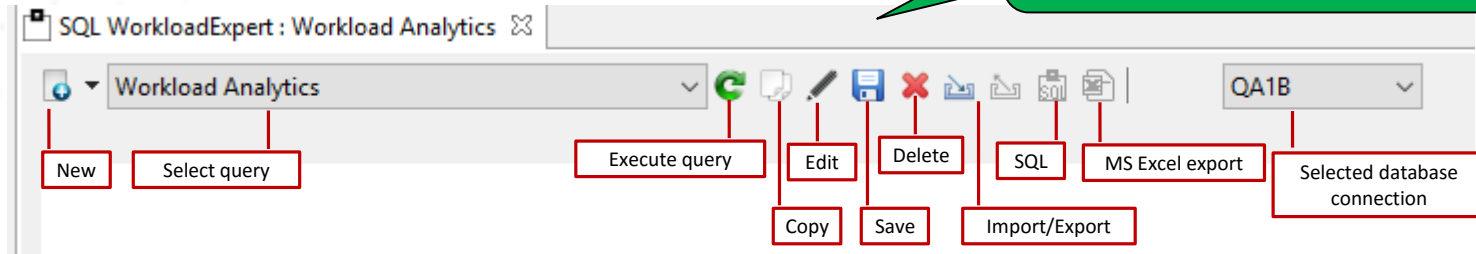
### Exploit and integrate into Eclipse based GUI front ends

- GUIs can come as a Plug-in for
  - IBM Rational
  - IBM Data Studio
  - Eclipse native
- 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 hand over



# The viable way – let DB2 do the magic

GUI features –  
button overview



# The viable way – let DB2 do the magic

SQL WorkloadExpert : Workload Analytics

Workload Analytics

QA1B

- ▶ Application Workload  
Detailed Application Workload Analysis
- ▶ Audit  
Audit - Who did What, When and Where
- ▶ BIF Usage - Standard  
Built-in Function Usage Analysis
- ▶ Cluster index detection  
This case lists all indexes which could be clustered
- ▶ Content Manager System  
Review KPIs per Primary Authorization
- ▶ CPU intensive SQLs  
CPU intensive SQL statements
- ▶ Delay detection  
Detect which SQLs have odd delay
- ▶ Disk I/O  
Disk I/O performance checking
- ▶ DSC/SSC flush rates  
DSC and SSC flush rate calculation
- ▶ Index maintenance costs  
Index maintenance cost determination by execution after an index change and comparison of the results
- ▶ Multi-row Fetch detect  
Multi-row Fetch candidate detection
- ▶ Never executed packages  
Never executed packages with static SQL statements
- ▶ Never executed SQL  
Never executed static SQL statements
- ▶ Never used objects  
Never used objects (tablespaces, tables and indexes)
- ▶ Object quiet times  
Object quiet times
- ▶ Object usage  
Object usage cross-referencing
- ▶ REORG suppr./detection  
Detect and verify REORGs and their effect on performance, I/O, etc
- ▶ Same SQL / mult. schemas  
Same SQL with multiple schemas
- ▶ SELECT only detection - Locksize tuning  
Detect which tables have only SELECT SQLs running against them
- ▶ SQL text analysis  
SQL text analysis
- ▶ Up and Down scaling  
Up and Down scaling of workloads
- ▶ Utility Review  
Utility Review, IFCIDs 23, 24, 25, 219, 220
- ▶ WLX KPIs and summaries  
WLX KPIs (Key performance indicators) and summaries

Exploit the repository for any workload analytics

# 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	
DSN9EP2L	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	
DSNTIUL	DSNTIB10	2	0.009314	0.000358	0.008642	0.009384	
FILLPROD	PTFCOLL008	2	0.058374	0.001496	0.034183	0.124546	
IMEMB	PTFCOLL008	1	2.383299	0.082182	2.383299	2.584011	

Result counter: 212

SQL Results Execution Plan Bookmarks \*Application Workload

Connection profile

Type: Name:

```

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 . INDXTYPE , IX . PIECESIZE , IX . PADDED , IX . AVGKEYLEN ,
6 IX . STATSTIME , 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 ( 'T' , '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

```

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

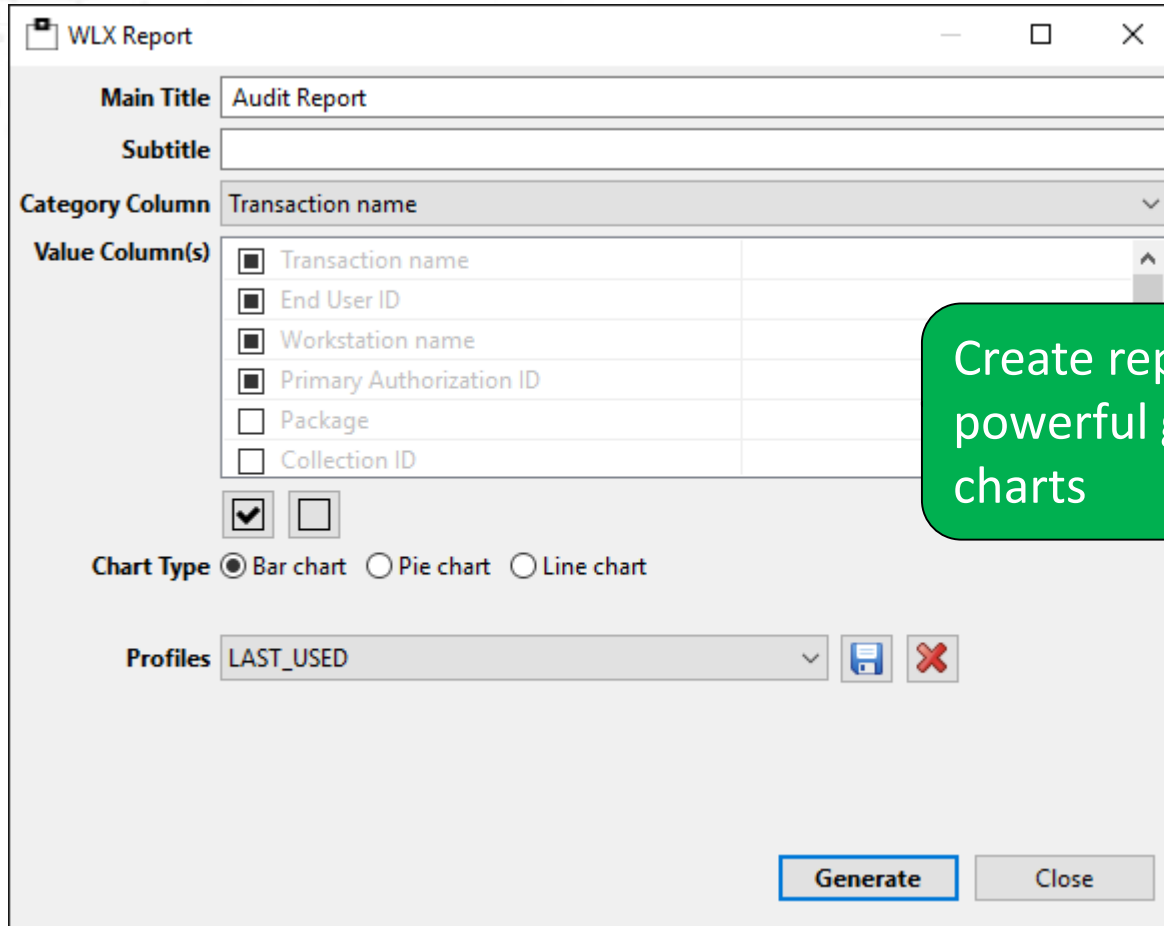
Writable Insert 10:26

## The viable way – let DB2 do the magic

## Compare workload and SQL to find anomalies

[illegible]

# The viable way – let DB2 do the magic



The screenshot shows a window titled "WLX Report" with the following fields and options:

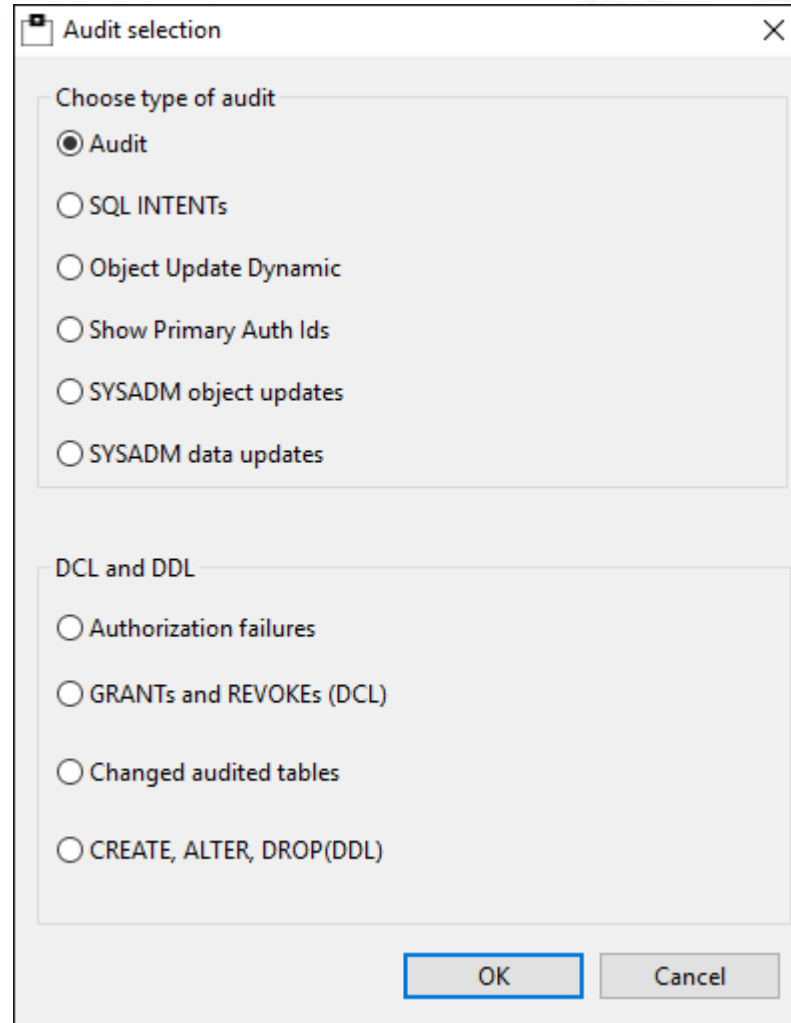
- Main Title:** Audit Report
- Subtitle:** (empty)
- Category Column:** Transaction name
- Value Column(s):** A list of columns with checkboxes:
  - ☒ Transaction name
  - ☒ End User ID
  - ☒ Workstation name
  - ☒ Primary Authorization ID
  - ☐ Package
  - ☐ Collection ID
- Chart Type:** ☒ Bar chart, ☐ Pie chart, ☐ Line chart
- Profiles:** LAST\_USED
- Buttons:** Generate, Close

Create reports using  
powerful graphical  
charts



# The viable way – let DB2 do the magic

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



A screenshot of a Windows-style dialog box titled "Audit selection". The dialog has a close button (X) in the top right corner. It contains two main sections. The first section, "Choose type of audit", has a list of radio buttons: "Audit" (selected), "SQL INTENTs", "Object Update Dynamic", "Show Primary Auth Ids", "SYSADM object updates", and "SYSADM data updates". The second section, "DCL and DDL", has a list of radio buttons: "Authorization failures", "GRANTs and REVOKEs (DCL)", "Changed audited tables", and "CREATE, ALTER, DROP(DDL)". At the bottom right, there are "OK" and "Cancel" buttons.

**Audit selection**

Choose type of audit

- ☒ Audit
- ☐ SQL INTENTs
- ☐ Object Update Dynamic
- ☐ Show Primary Auth Ids
- ☐ SYSADM object updates
- ☐ SYSADM data updates

DCL and DDL

- ☐ Authorization failures
- ☐ GRANTs and REVOKEs (DCL)
- ☐ Changed audited tables
- ☐ CREATE, ALTER, DROP(DDL)

OK Cancel

# The viable way – let DB2 do the magic

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

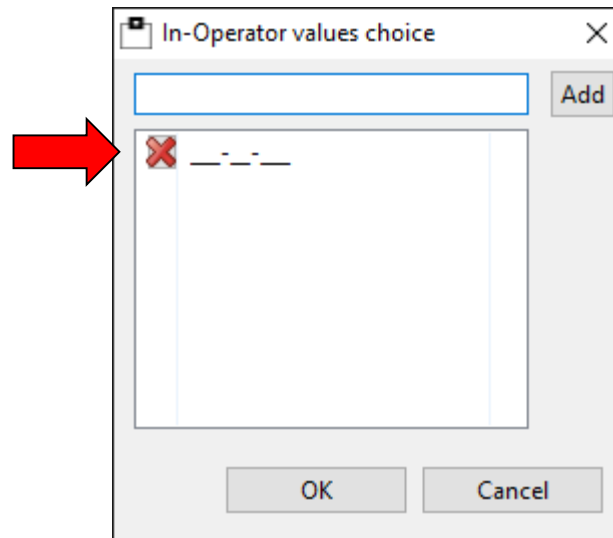
SQL WorkloadExpert : DML Audit

DML Audit QA1B

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	IQAO610	IQAXI0041	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQAO610	IQATI004	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQAO610	IQAXI0041	
BOXWELL	BOXWELL	TSO	BOXWELL	BOXWELL	BOXWELL	DSNISM68	SELECT	READ	SYSIBM	SYSIDUM...	
BOXWELL	BOXWELL	TSO	BOXWELL	BOXWELL	BOXWELL	DSNISM68	SELECT	READ	MVNXTEST	MVNX861	
BOXWELL	BOXWELL	TSO	BOXWELL	BOXWELL	BOXWELL	DSNISM68	SELECT	READ	MVNXTEST	MVNX86	
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	IQAO610	IQATI006	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQAO610	IQAXI0061	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQAO610	IQATI007	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQAO610	IQAXI0071	

## The viable way – let DB2 do the magic

Use free text search capabilities to scan your entire workload for sensitive data = in-depth audit candidates (e.g. credit card numbers, social security numbers, ...)



# Customer results from the banking industry

## Requirements:

- Capture DDL, DCL, DML from 'inside' as well as DDF
- Capture any activity in a UoR
- Capture static and dynamic SQL statements
- Show logon id as well as functional id
- Generate daily audit reports matching give filters
- Generate specific reports matching specific SQL statement classification
- Generate reports based on RACF id/group
- Generate unified reports for a data sharing group, as well as individual subsystem
- Email reports to DB2 Auditor group
- Capture DB2 online utilities
- Merge multiple systems reports

# Customer results from the banking industry

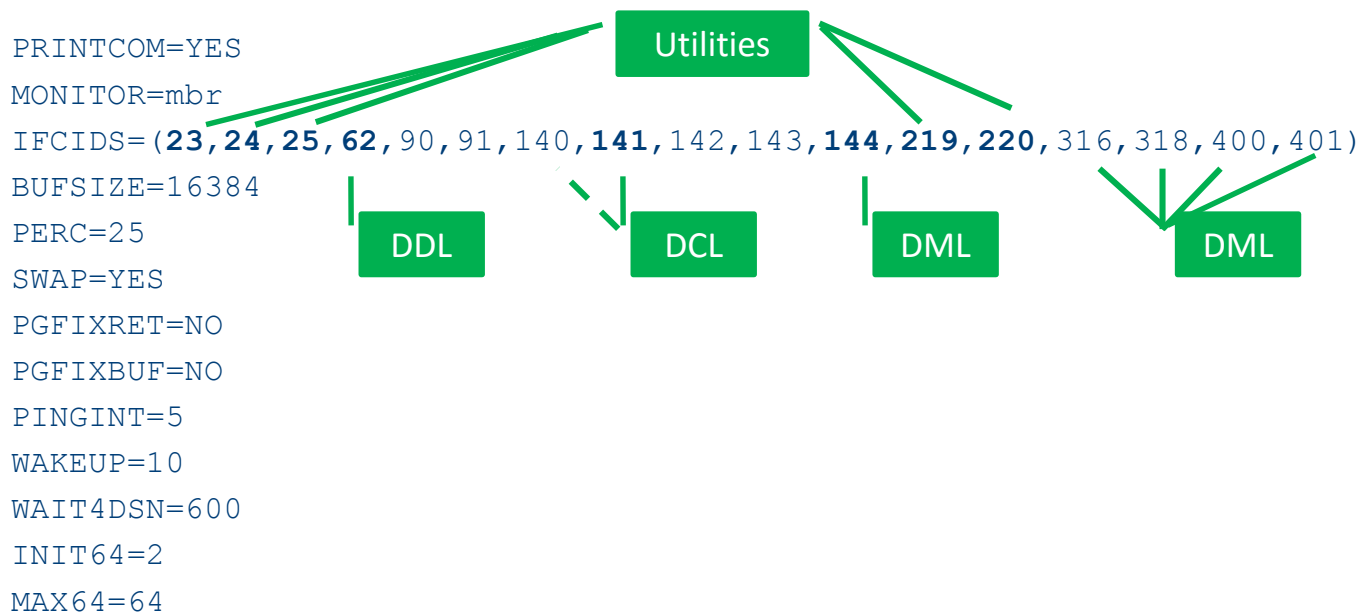
## Setup:

- WLX STC HA implementation
  - STC at the LPAR/DB2 DS member level to assure continuous capturing even during LPAR restart
- Workload processing once a day to generate daily audit reports
  - Automated via job scheduler
  - All DB2 systems merged into a common report
  - Objects and activity (DML, DDL, DCL) filtered
  - Reports sent via Email
- Specific reporting as needed via GUI
  - In-depth suspect analysis
  - Banking authority quarterly/annual reports

# Customer results from the banking industry

## Customization:

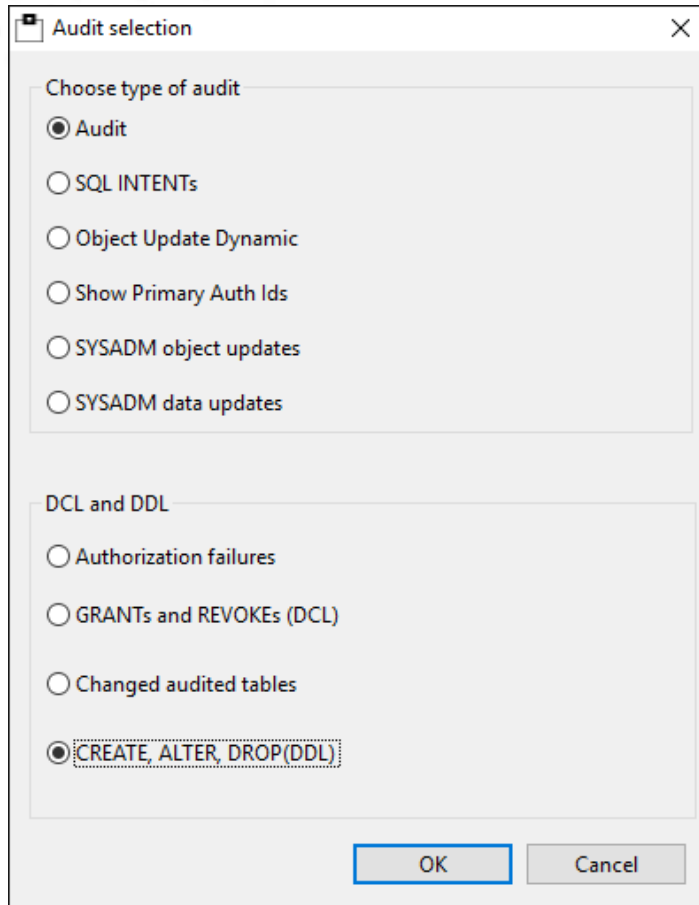
- *Capture DDL, DCL, DML from 'inside' as well as DDF*
- *Capture any activity in a UoR*
- *Capture static and dynamic SQL statement*
- *Capture DB2 online utilities*





# Customer results from the banking industry

Show DDL activities:



**Audit selection**

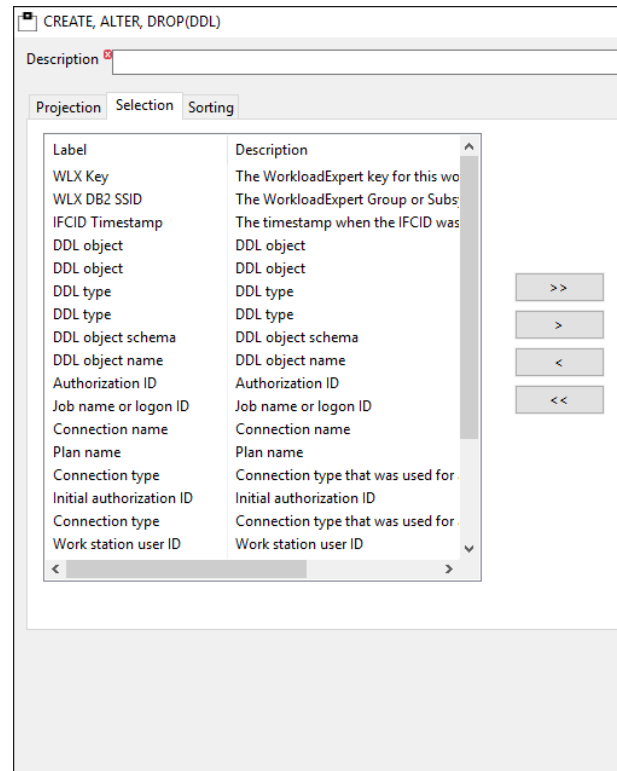
Choose type of audit

- ☒ Audit
- ☐ SQL INTENTS
- ☐ Object Update Dynamic
- ☐ Show Primary Auth Ids
- ☐ SYSADM object updates
- ☐ SYSADM data updates

DCL and DDL

- ☐ Authorization failures
- ☐ GRANTS and REVOKEs (DCL)
- ☐ Changed audited tables
- ☒ CREATE, ALTER, DROP(DDL)

OK Cancel



**CREATE, ALTER, DROP(DDL)**

Description

Projection Selection Sorting

Label	Description
WLX Key	The WorkloadExpert key for this wo
WLX DB2 SSID	The WorkloadExpert Group or Subs
IFCID Timestamp	The timestamp when the IFCID was
DDL object	DDL object
DDL object	DDL object
DDL type	DDL type
DDL type	DDL type
DDL object schema	DDL object schema
DDL object name	DDL object name
Authorization ID	Authorization ID
Job name or logon ID	Job name or logon ID
Connection name	Connection name
Plan name	Plan name
Connection type	Connection type that was used for
Initial authorization ID	Initial authorization ID
Connection type	Connection type that was used for
Work station user ID	Work station user ID

>> > < <<

# Customer results from the banking industry

## Show DCL activities:

☒ Audit selection
 

Choose type of audit

☒ Audit

☐ SQL INTENTS

☐ Object Update Dynamic

☐ Show Primary Auth Ids

☐ SYSADM object updates

☐ SYSADM data updates

DCL and DDL

☐ Authorization failures

☒ GRANTS and REVOKEs (DCL)

☐ Changed audited tables

☐ CREATE, ALTER, DROP(DDL)

OK

Cancel

GRANTS and REVOKEs (DCL)

Description

Projection

Selection

Sorting

Label	Description
WLX Key	The WorkloadExpert key for the
WLX DB2 SSID	T Label
IFCID Timestamp	T Function
IFCID No.	T Authorization type
Audit object type	A Statement text
Privilege check	T Reason access
DBID	Ir Authorization ID
Access type	A Job name or logon ID
OBID	Ir Return code access control
Authorization type	A Connection name
Multi-Level Security	M Reason code access control
Reason access	R Plan name
SQL Code	S Initial authorization ID
Row control	R Connection type
Audit object type	A MLS RID
Grant creator	A Seclabel
SQL text length	T Work station user ID
	Transaction or application na...
	Source table owner

# Customer results from the banking industry

## Access violations due to insufficient authorities:

Access violations

QA1B

WLX Key	WLX DB2 SSID	IFCID Timestamp	IFCID No.	Privilege check	Audit object type	Authorization type	Connection type	Return cc
2015-10-23-09.33.24.333858	QA1B	2015-10-28-11.50.07.247943	140	SELECT	TABLE OR VIEW	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2015-10-23-09.33.24.333858	QA1B	2015-10-28-11.50.07.289261	140	SELECT	TABLE OR VIEW	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2015-10-23-09.33.24.333858	QA1B	2015-10-28-11.50.07.325412	140	SELECT	TABLE OR VIEW	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2016-02-15-18.38.31.829844	QA1B	2016-02-16-12.58.21.269156	140	SELECT	TABLE OR VIEW	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2016-02-15-18.38.31.829844	QA1B	2016-02-16-12.58.21.339446	140	SELECT	TABLE OR VIEW	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2016-02-15-18.38.31.829844	QA1B	2016-02-16-12.58.21.406366	140	SELECT	TABLE OR VIEW	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2015-08-12-16.20.11.186065	QA1B	2015-08-14-13.28.37.600644	140	SELECT	TABLE OR VIEW	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2015-08-12-16.20.11.186065	QA1B	2015-08-14-13.28.37.603033	140	EXPLAIN	USER AUTH	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2015-08-12-16.20.11.186065	QA1B	2015-08-14-13.30.53.782964	140	INSERT	TABLE OR VIEW	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2015-08-12-16.20.11.186065	QA1B	2015-08-14-13.30.53.785690	140	EXPLAIN	USER AUTH	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2015-08-12-16.20.11.186065	QA1B	2015-08-14-13.31.55.923128	140	UPDATE	TABLE OR VIEW	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2015-08-12-16.20.11.186065	QA1B	2015-08-14-13.31.55.930239	140	EXPLAIN	USER AUTH	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2015-08-12-16.20.11.186065	QA1B	2015-08-14-15.22.39.339049	140	UPDATE	TABLE OR VIEW	PRIM/SEC	DB2 CALL ATTACH	
2015-08-12-16.20.11.186065	QA1B	2015-08-14-15.22.39.341406	140	EXPLAIN	USER AUTH	PRIM/SEC	DB2 CALL ATTACH	
2015-08-12-16.20.11.186065	QA1B	2015-08-14-15.22.43.521867	140	INSERT	TABLE OR VIEW	PRIM/SEC	DB2 CALL ATTACH	
2015-08-12-16.20.11.186065	QA1B	2015-08-14-15.22.43.524196	140	EXPLAIN	USER AUTH	PRIM/SEC	DB2 CALL ATTACH	

Result counter : 18

# Customer results from the banking industry

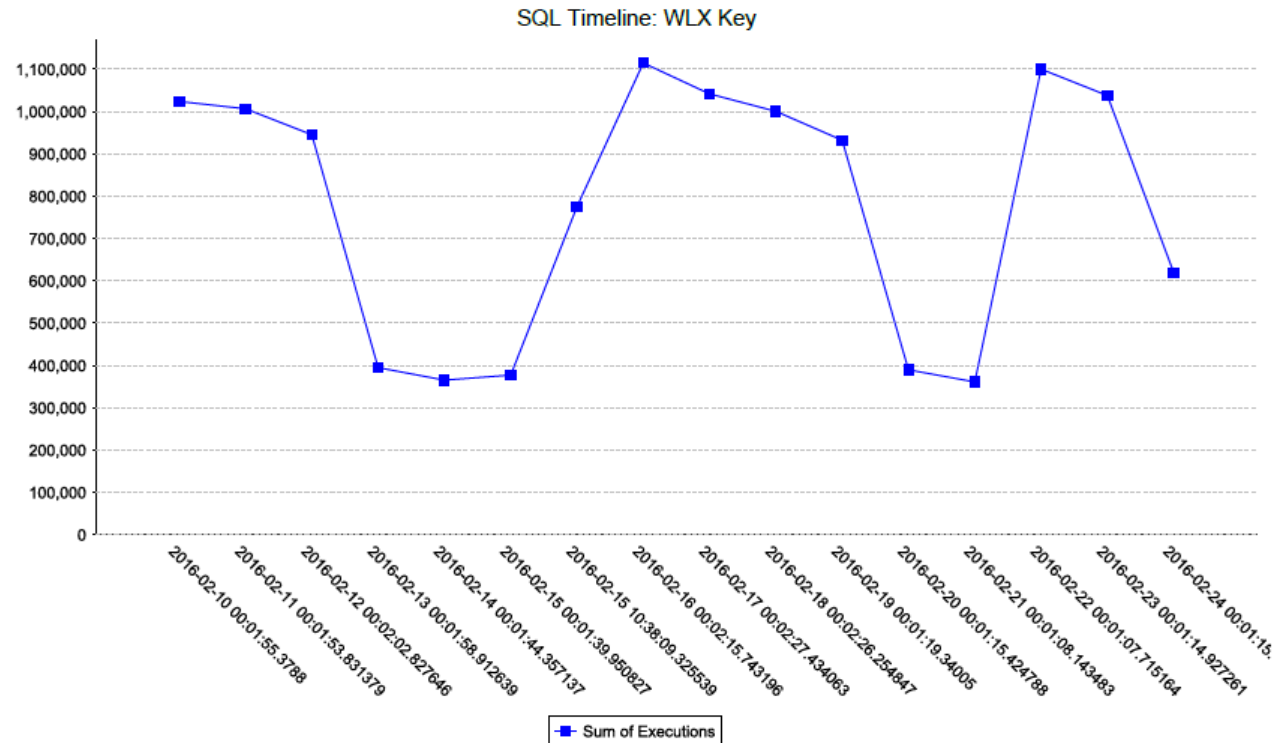
## DML Reporting:

Label	Description	
Statement Timestamp	The timestamp that this statement was written into the SSC c	
WLX DB2 SSID	The WorkloadExpert Group or Subsystem DB2 name for this v	
Primary Authorization ID	The Primary Authorization ID used to identify the application	
Package	The package used by the statement	
Collection ID	The Collection ID used by the statement	
Primary Authorization ID	The Primary Authorization ID used to identify the application	
Sum of Executions	The total number of Executions	
Transaction name	A value provided by the RRS signon or resignon	
End User ID	A value provided by the RRS signon or resignon	
Workstation name	A value provided by the RRS	User provided id string
Package CONTOKEN	For Static SQL the CONTOKE	Authorization ID
Current SQL ID	The Current SQL ID that is r	Job name or logon ID
Qualifier	The Qualifier used at Bind ti	Connection name
First referred Table Qualifier	The first table Qualifier in th	Plan name
First referred Table Name	The first table name in the s	Initial authorization ID
Statement text	The complete text for the SC	Connection type that was used for an access
Query no.	Query number	Accounting token
		Work station user ID
		Transaction or application na...
		Workstation name
		Trusted context name

# Customer results from the banking industry

Detected anomalies: suspicious increase in SQL executions:

## WLX Report





# Customer results from the banking industry

*Show logon id as well as functional id:*

SQL WorkloadExpert : Database activity

Database activity QA1B

Transaction name	End User ID	Workstation name	Primary Authorization ID	Current SQL ID	Qualifier	Package	Query type	Table creator	Table name	Object type
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	UPDCUR	IQA0610	IQATXX00	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	UPDCUR	IQA0610	IQATXX00	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04	KUERTEN	IQADBACP	UPDATE	IQA0610	IQAXXX001	I
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04	KUERTEN	IQADBACP	UPDATE	IQA0610	IQATXX00	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04	KUERTEN	IQADBACP	DELETE	IQAXXX04	PLAN_TA...	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04	KUERTEN	IQADBACP	DELETE	IQAXXX04	DSN_STA...	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04	KUERTEN	IQADBACP	DELETE	IQAXXX04	DSN_PRE...	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04	KUERTEN	IQADBACP	DELETE	IQAXXX04	DSN_FILT...	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04	KUERTEN	IQADBACP	DELETE	IQAXXX04	DSN_DET...	T
WLXNEWWL	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	INSERT	IQA0610	IQATW009	T
WLXNEWWL	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	UPDATE	IQA0610	IQATW042	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	UPDATE	IQA0610	IQATW042	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	DELETE	IQA0610	IQATW007	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	INSERT	IQA0610	IQATW007	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	UPDATE	IQA0610	IQAXW0421	I
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	UPDATE	IQA0610	IQATW042	T

Result counter : 94



# Customer results from the banking industry

*Generate daily audit reports matching give filters*

Object Update Dynamic

Description: Database activity

Projection Selection Sorting

Label	Description
Rate of IO cost	The IO cost in ...
Seconds in Cache	Seconds in Ca...
Query no.	Query number
User provided id string	User provided ...
Authorization ID	Authorization ID
Job name or logon ID	Job name or l...
Connection name	Connection n...
Plan name	Plan name
Initial authorization ID	Initial authoriz...
Connection type	Connection ty...
Accounting	Accounting to...
Work station user ID	Work station u...
Transaction or application name	Transaction or...
Workstation name	The endusers ...
Context name	Trusted contex...
Role name	Role name ass...
Original user id	Original applic...
Correlation token	Correlation to...

>> > < <<

Label	Operator	Value	Description
WLX Key	=	newest	The WorkloadExpert k...
Statement Times...	=	2016-03-07-13.57.24.772000	The timestamp that th...
WLX DB2 SSID ...	=	DB2P	The WorkloadExpert G...
Primary Authoriz...	NOT LIKE	SA%	The Primary Authoriza...
Table name	IN	%CUST%, %PAYMNT%, %TRSACT%	Table name
Transaction nam...	=	CICT99	A value provided by th...
End User ID	=		A value provided by th...
Workstation nam...	=		A value provided by th...
Current SQL ID ...	=		The Current SQL ID th...
Query type	=		Query type
Statement text ...	=		The complete text for t...
Query no.	=		Query number
User provided id ...	=		User provided id string
Authorization ID	=		Authorization ID
Job name or log...	=		Job name or logon ID
Connection name	=		Connection name
Plan name	=		Plan name

↑ ↓

OK Cancel



# Customer results from the banking industry

## Runtime & Costs:

- Capture STC < 15sec. CPU/month (3-way DS)
- 150k stmt. < 3min processing

## Results:


- Fully automated report generation for authorities and internal/external auditors, provided via Email
- Exceptional workload detected and stopped within minutes
- Power User-IDs found, being used for daily work
- Access from VPN/WAN networks found
- Access violations detected
- 3<sup>rd</sup> party applications with update intent, but should actually be read

## Appendix

- DB2 APARs to check for:
  - PI30040 DB2 11 UI26407 – Forward fit SQLCODE 420
  - PI33409 DB2 10 UI26352 – REVOKE MQT
  - PI35766 DB2 11 UI31693 – Elapsed time incorrect for parallel queries
  - PI46967 DB2 10 UI31646 DB2 11 UI31647 – Invalid IFCID 401 after IDAA APAR PI23083/PI30005
  - PI48100 DB2 10 UI32273 – Abend SOC4 in Pre V8 packages


## Advertisement ;-)

So now you know...

- Of course it is easier with the Audit component of  **SQL WorkLoadExpert for DB2 z/OS**
  - Data Warehouse
  - Extensible and Extendable
  - Low CPU cost
  - Fully based on official DB2 features and functions
  - Exploits DB2 security and compression
  - Is inside your protected environment
    - No new vulnerability
    - No time consuming implementation
  - Utilizes your existing investments

## WLX typical use cases

### Application Development:

- Application Workload Analysis: E.g. which machine load is produced by a certain Application?
- Explain Tool link (e.g.  **SQL PerformanceExpert**, IBM DataStudio)
- Show same SQL on Multiple Schemas to detect “heavy-hitters”
- SQL Text Analysis for free text search (e.g.: BIF [Built-in Function] and UDF [User-Defined Functions] -usage, Java-formatted timestamps, etc.)
- View to detect “heavy-hitters” resulting from identical statements using different predicates First Topic
- Find unused (orphaned) SQL



## WLX typical use cases

### Workload/Performance management:

- Workload-Change, Problem-Detection and Trending, Comparison of CPU consumption, I/O, execution rates, current KPIs and deltas – calculated and summarized to the costs of multiple apps
- Disc Problem Detection – I/O Rates
- SQL KPIs – Background Noise and Exceptions
- SELECT Only Table Detection (READ only activity)
- Delay Detection (All queries which are delayed)
- Up and Down Scaling of SQL Workloads
- DSC Flush Analysis
- CPU Intensive Statements
- Index Maintenance Costs

# WLX functional packages of use cases

## Database Administration:

- Find never used Objects (Tables, Indexes, and Tablespaces)
- Find never executed Packages

## Audit and Security:

- AUDIT tables being accessed
- AUDIT DB2 data being accessed
- AUDIT data manipulation (insert/update/delete)
- See where updates came from (inside or outside the local network)
- See where data is being accessed from (IP address, intra-/extranet, etc.)
- SQL Text Analysis for free text search (BIF [Built-in Function] and UDF [User-Defined Functions] -usage, Java-formatted timestamps, etc.)

# Craig Mullins and Ulf Heinrich

SEGUS & SOFTWARE ENGINEERING

[u.heinrich@segus.com](mailto:u.heinrich@segus.com)

Session V02

DB2 z/OS Audit - Viable workload tracking

*Please fill out your session  
evaluation before leaving!*

