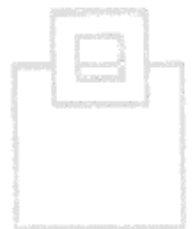


---

# DB2 for z/OS Security Audit: Protecting your Assets

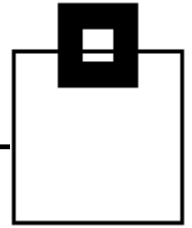
Webinar presented by Dave Beulke & Roy Boxwell

DB2 z/OS Audit using  
📄 **SQL Workload Expert for DB2 z/OS**



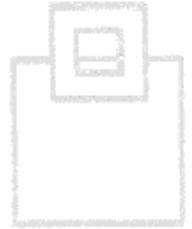
# Agenda

---



Part 1 with **Dave Beulke**:

**Proactive protective security framework**



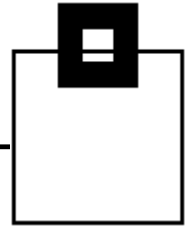
Part 2 with **Roy Boxwell**:

**WLX Audit & Real world Audit data examples**



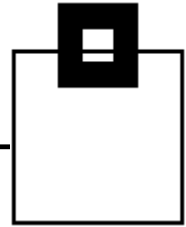
Q&A with **Dave Beulke & Roy Boxwell**





## Proactive protective security framework





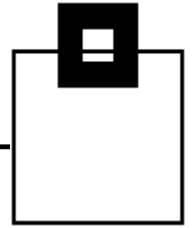
- Member of the inaugural IBM DB2 Information Champions
- One of 40 IBM DB2 Gold Consultant Worldwide
- President of DAMA-NCR, Past President of International DB2 Users Group - IDUG
- Best speaker at CMG conference & former TDWI instructor
  
- Former Co-Author of certification tests
  - DB2 DBA Certification tests
  - IBM Business Intelligence certification test
- Former Columnist for IBM Data Management Magazine
  - Consulting
    - CPU Demand Reduction Guaranteed!
    - DB2 Performance Review
    - DW & Database Design Review
    - Security Audit & Compliance
    - DB2 11 Migration Assistance
    - DB2 10 Performance IBM White Paper & Redbook
  - Teaching Educational Seminars
    - DB2 Version 11 Transition
    - DB2 Performance for Java Developers
    - Data Warehousing Designs for Performance
    - How to Do a Performance Review
    - Data Studio and pureQuery
  
- Extensive experience in security, Big Data systems, DW design and performance
  - Working with DB2 on z/OS since V1.2
  - Working with DB2 on LUW since OS/2 Extended Edition
  - Designed/implemented first data warehouse in 1988 for E.F. Hutton
  - Working with Java for Syspedia since 2001 –
  - Syspedia - Find, understand and integrate your data faster!

**Weekly Performance Tips:**  
[www.DaveBeulke.com](http://www.DaveBeulke.com)

# Security is the priority

---

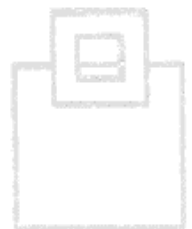
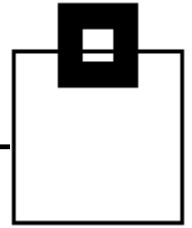
- Consulting Management Review
- Security Audits have become the top business priority
  - Performance Analytics
  - Big Data Designs
- Proactive Security
  - No more one time or static security reviews
  - Active security procedures
    - Constantly reviewing data access
    - Notification of unusual object access
      - Reviewing any type of special access
      - To any PII-HIPAA type of data objects



# Requirements for security are evolving

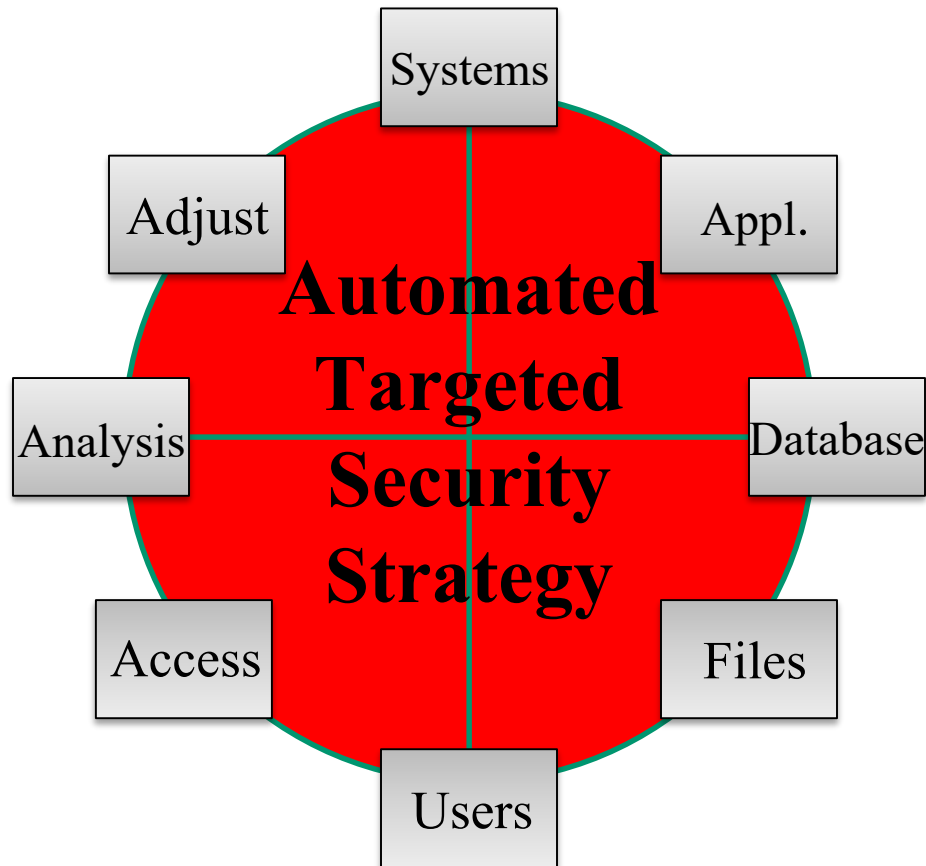
---

- Dynamic Hacking happening today!
  - 24x7x365 exposure
  - New hacking techniques discovered daily
  - Constant threat of hacking
- Comprehensive multi-dimensional solutions
  - Every company is a mixture of technology
  - Platforms, systems and variety of applications
  - Purchased, home grown security challenges
  - Customized company and industry procedures



# Plan Development

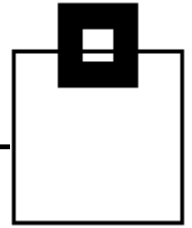
- Unique to your company



# Constant Vigilance

---

- Specialized Security Audit reporting requirements
  - Always think of compliance reporting
  - Company specific
  - Industry detailed
- All SQL Access – every moment – everyday
  - Every access from anywhere
  - All Applications - anything Ad Hoc
- Data object security profiles
  - Read/Write access
  - Associated data tables of files- all copies
  - User to Objects & Object to users

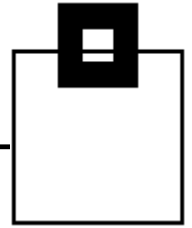




# Analytical Analysis

---

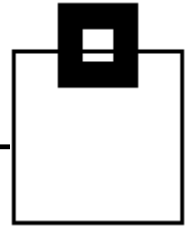
- History of Access
- Access activity changes over time
  - Security and User Ids change
  - New applications accessing PII data
- History of Id Profile
  - Authority to reference the PII data
  - Table objects change – new columns
  - Compliance report of authorized users
- Immediate, daily, weekly, monthly quarterly
  - Security and Audit Industry specific compliance report



# Establishment of baseline

---

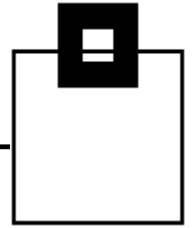
- The access and security normal activity
  - Mix of platforms, systems, databases and application
  - Regular, irregular and one time access
- Categories of access
  - Read – Write –
    - Within security expectations
    - Stretching security reach
    - One time – specials/unknowns
  - Application profile read write
  - Open system access
    - Tools, new application interfaces



# Monitoring and Measurement

---

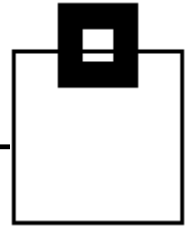
- Performance overhead considerations
  - System, database, application and user overhead
  - Extreme detail needed
    - Situational awareness
    - Security risk assessment/judgement
- Deviation to the baseline
  - Normal vs. Abnormal security behavior
  - What are your standard reports?
    - PII access
    - Aggregate access figures
    - Exception/summary reporting



# Internal Audits

---

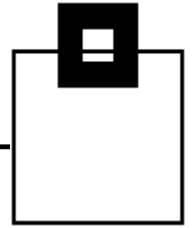
- Review applications, objects, users and tools
- Compliance Reporting
  - Point of view security reporting
    - Data Stewart owner
    - Security auditor review
    - Industry formats
- Control of non-conforming objects
  - One time access
  - Single user probe
  - Elevated authority access



# Preventative and Corrective Actions

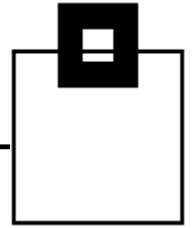
---

- Standardized regular reporting requirements
  - System, application, database and user
    - Broken down for accurate appropriate security
- How is your audit reporting setup to document events?
  - Frequency
  - Immediacy
  - Management notification(s)
- Level of Actions
  - Simple to the extreme

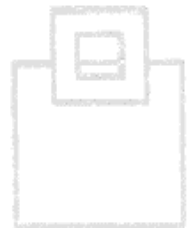


# Automated repeatable security strategy

---

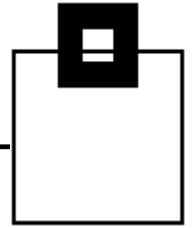


- Understand your company
  - Realize where targeted PII data exists
  - Leverage existing security infrastructure
- Follow or create standard security procedures
  - Establish history of access events
  - Understand exposure, access and remediation
- Tools are key to security success
  - Speed to action
  - Establish automatic security best next steps
  - Procedures developed with business users
  - Automation guarantees and improves response

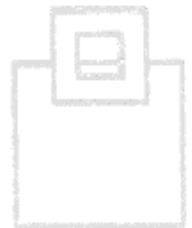


## Part 2 with Roy Boxwell:

---



### WLX Audit & Real world Audit data examples



## Hidden public problem?

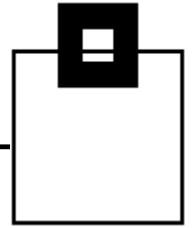
---

Lots of shops have some serious audit problems without even realizing it.

For example, SELECT on the DB2 Catalog is sometimes GRANTED to PUBLIC. This is generally OK, but what about the statistical data in some of these tables?

There are actually 12 tables containing 34 columns of data that is then available. These are the VARCHAR(2000) columns that contain COLVALUE, HIGHVALUE, KEYVALUE, LOWVALUE, HIGH2KEY, HIGHKEY, LOW2KEY, and LOWKEY columns.

Are these protected at your site?





## EMEA too slow?

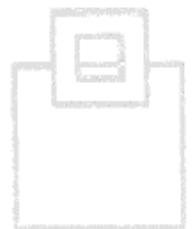
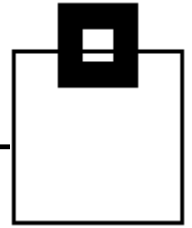
---

According to the M-Trends 2016 reports, in the USA the average time it took to detect a data breach was 146 days whereas in EMEA it was 469 days!

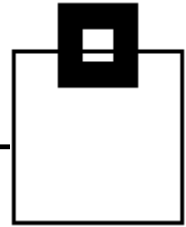
Here are the links to the two very interesting reports:

[\*https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf\*](https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016.pdf)

[\*https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016EMEA\\_LR.pdf\*](https://www2.fireeye.com/rs/848-DID-242/images/Mtrends2016EMEA_LR.pdf)

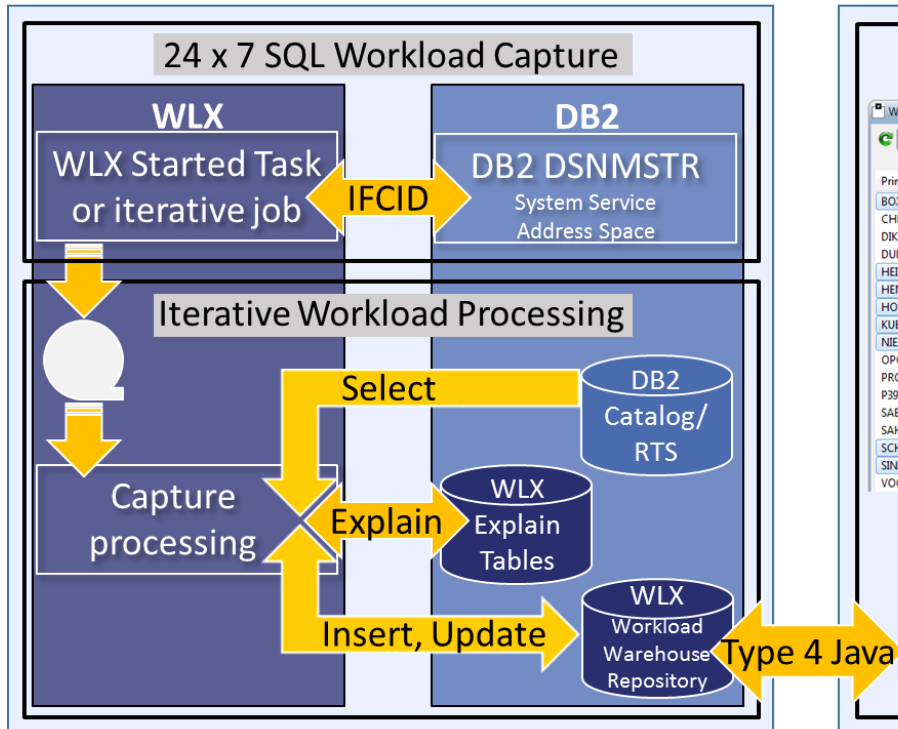


# WLX Architecture

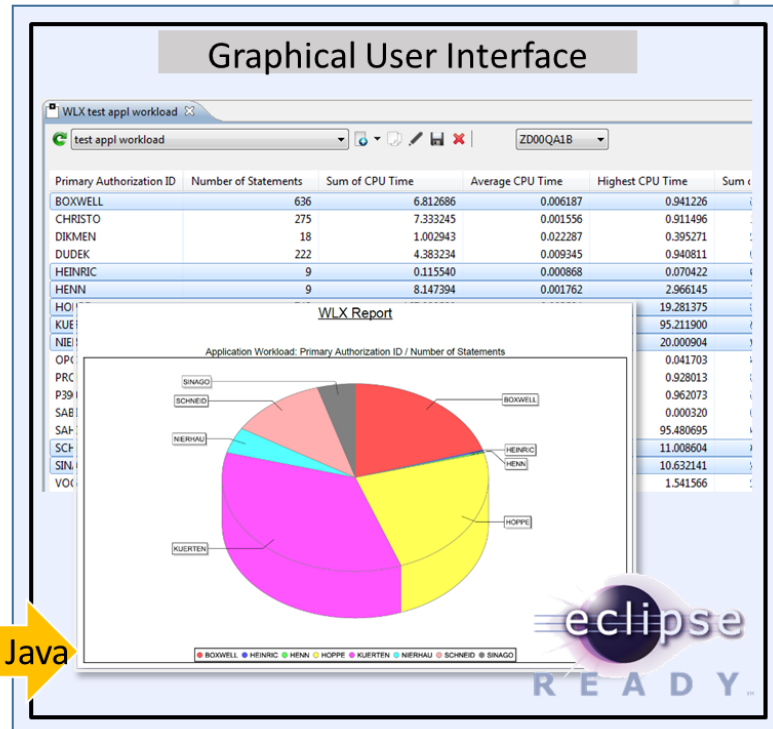


Captures the hard to get SQLs, even the ones that disappear ...

Mainframe Engine



Workstation Engine



# WLX Audit

---

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

23/24/25 Utility start/phase/stop (219/220 Listdef/Template)

90/91 Commands and their completion status

140 Authorization failures

141 Authorization changes

62/142 DDL/DDI for tables with audit changes/all

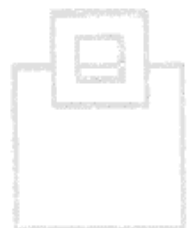
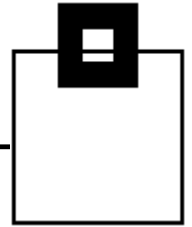
143 1<sup>st</sup> Change of audited object in UOR

144 1<sup>st</sup> Select of audited object in UOR

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

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

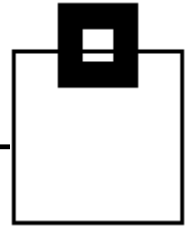
Adding the correlation headers provides detailed authentication data



# WLX Audit

---

- 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
  - Stores it in a repository
  - Using DB2 compression reduces storage requirements exploiting proven, integrated technology
- No new vulnerabilities:
- Black Box appliance
  - Massive sensitive data transmissions over the network

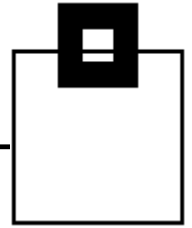


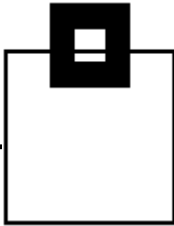
# WLX Audit

---

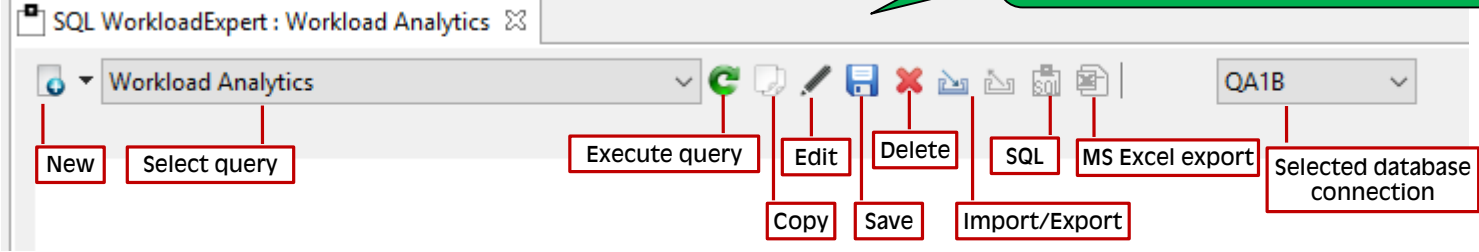
Do your (automated) reporting/alerting/analytics as needed:

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

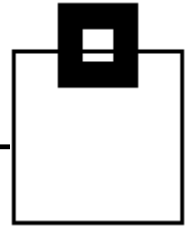




GUI features –  
button overview



# WLX Audit



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

# WLX Audit

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

Audit selection

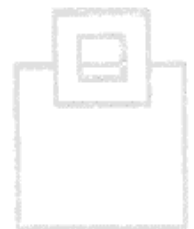
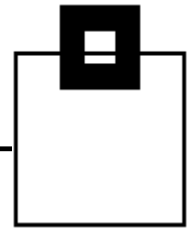
Choose type of audit

- 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)

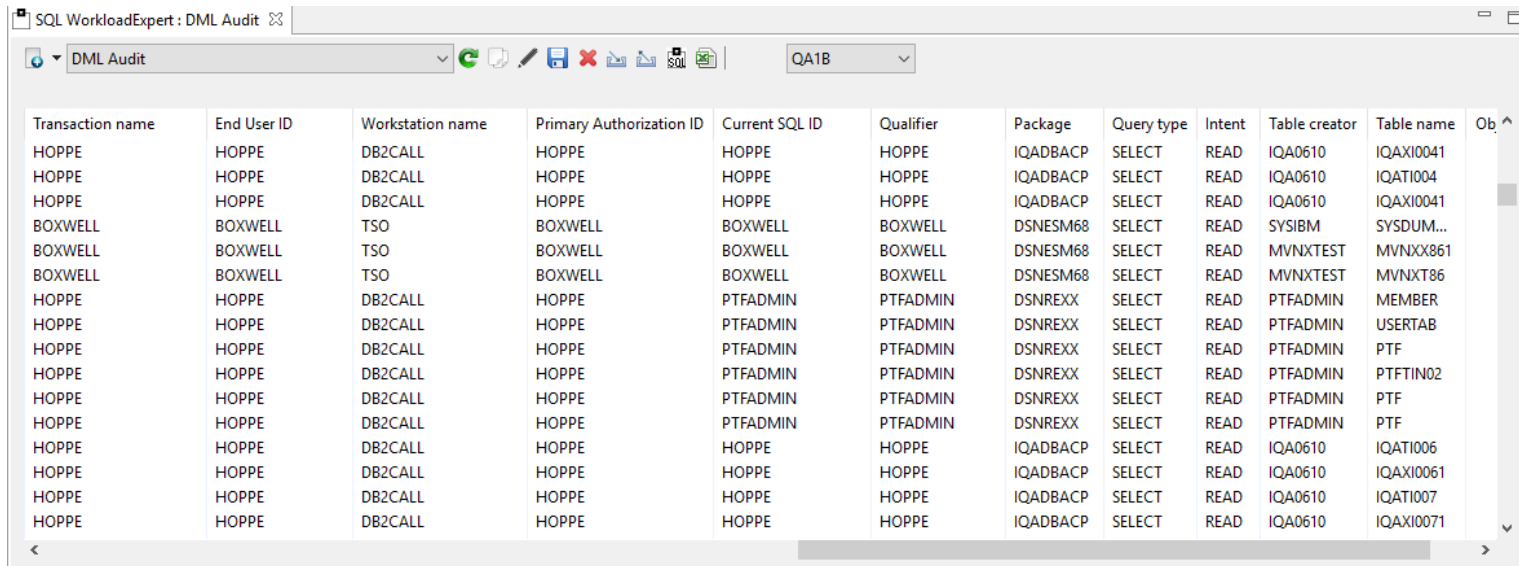
OK Cancel





# WLX Audit

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

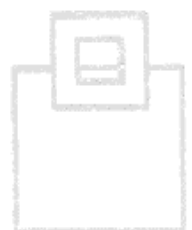
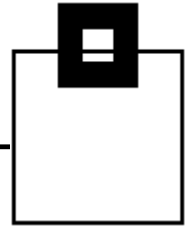
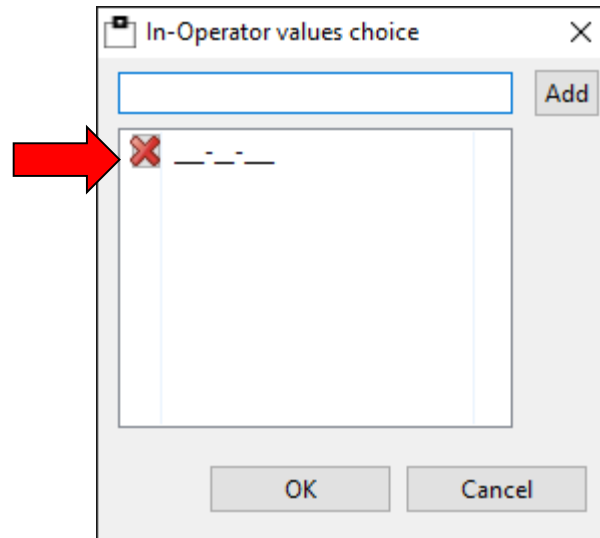


The screenshot shows the SQL WorkloadExpert: DML Audit window. The window title is "SQL WorkloadExpert : DML Audit". The main area displays a table with the following columns: Transaction name, End User ID, Workstation name, Primary Authorization ID, Current SQL ID, Qualifier, Package, Query type, Intent, Table creator, Table name, and Ob. The table contains 20 rows of data.

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	MVNXTEST	MVNX861	
BOXWELL	BOXWELL	TSO	BOXWELL	BOXWELL	BOXWELL	DSNESM68	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	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	

# WLX Audit

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, ...)

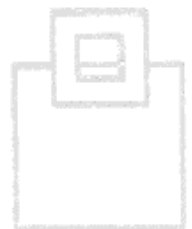
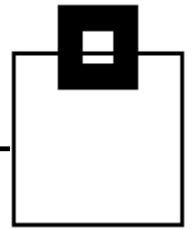


# Customer results from the banking industry

---

## 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

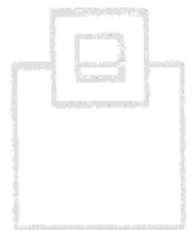
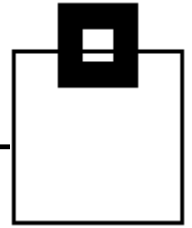


# Customer results from the banking industry

---

## Setup:

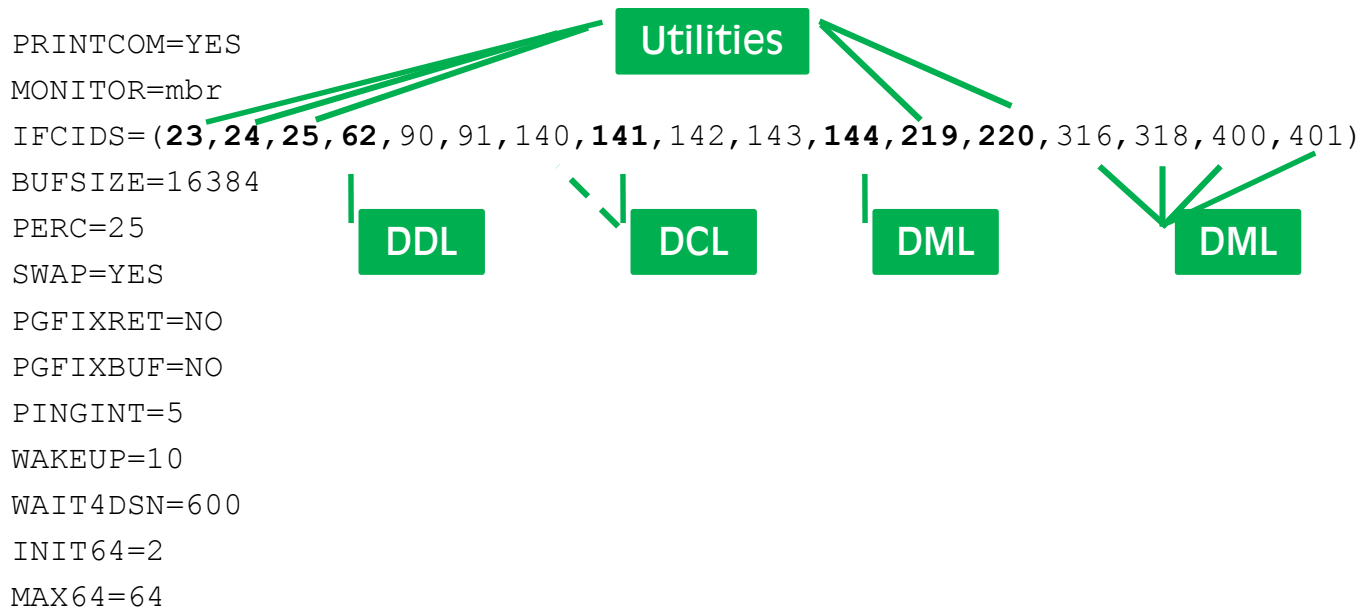
- **WLX STC HA implementation**
  - STC at the LPAR/DB2 DS member level to assure continuous capturing even during LPAR restart
- **Workload processing once a day to generate daily audit reports**
  - Automated via job scheduler
  - All DB2 systems merged into a common report
  - Objects and activity (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

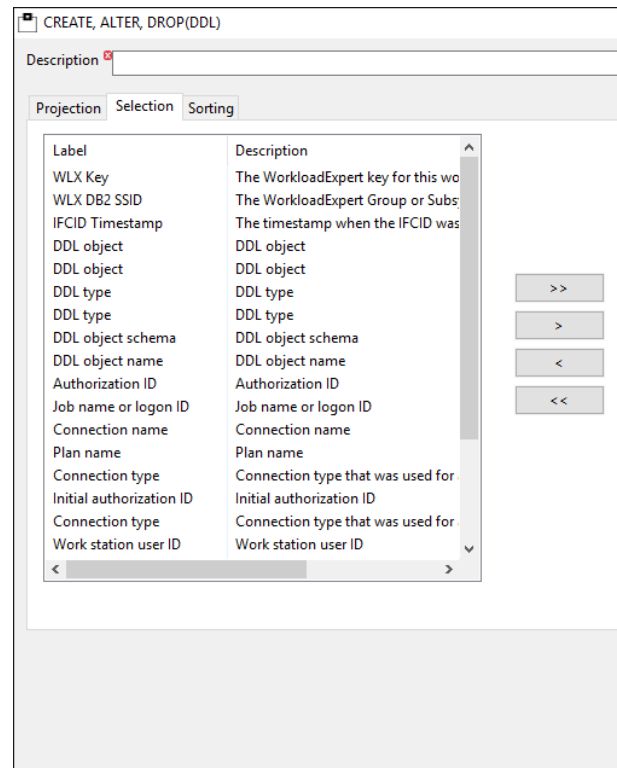
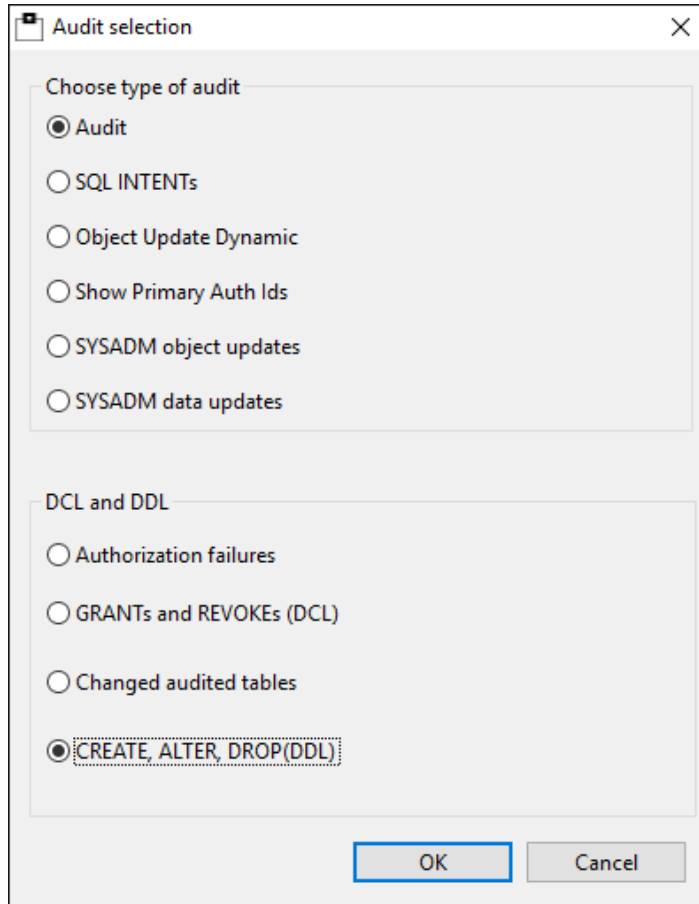
## Customization:

- *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*

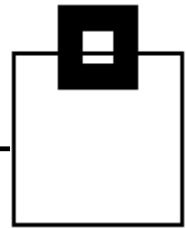


# Customer results from the banking industry

## Show DDL activities:



# Customer results from the banking industry



Show DCL activities:

GRANTs and REVOKEs (DCL)

Description

Projection Selection Sorting

Label	Description
WLX Key	The WorkloadEvent key for th
WLX DB2 SSID	T
IFCID Timestamp	T
IFCID No.	T
Audit object type	A
Privilege check	T
DBID	Ir
Access type	A
OBID	Ir
Authorization type	A
Multi-Level Security	M
Reason access	R
SQL Code	S
Row control	R
Audit object type	A
Grant creator	A
SQL text length	T

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)

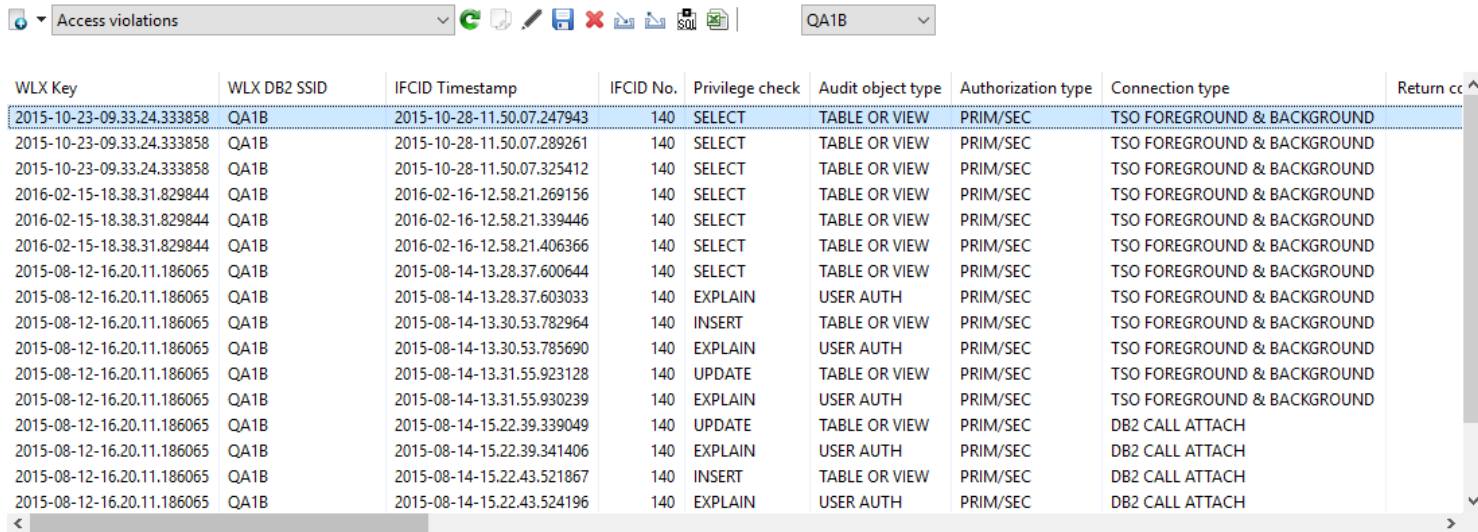
OK Cancel

Description

- Function
- Authorization type
- The complete text for the SQL
- Reason access granted (only f
- Authorization ID
- Job name or logon ID
- Return code from access cont
- Connection name
- User defined reason code from
- Plan name
- Initial authorization ID
- Connection type that was use
- RID of a row being updated/d
- Seclabel for/of MLS table row
- Work station user ID
- Transaction or application nar
- Source table owner

# Customer results from the banking industry

## Access violations due to insufficient authorities:

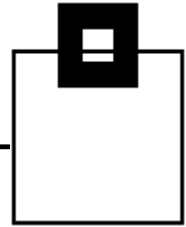


WlX Key	WlX DB2 SSID	IFCID Timestamp	IFCID No.	Privilege check	Audit object type	Authorization type	Connection type	Return cc
2015-10-23-09.33.24.333858	QA1B	2015-10-28-11.50.07.247943	140	SELECT	TABLE OR VIEW	PRIM/SEC	TSO FOREGROUND & BACKGROUND	
2015-10-23-09.33.24.333858	QA1B	2015-10-28-11.50.07.289261	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:

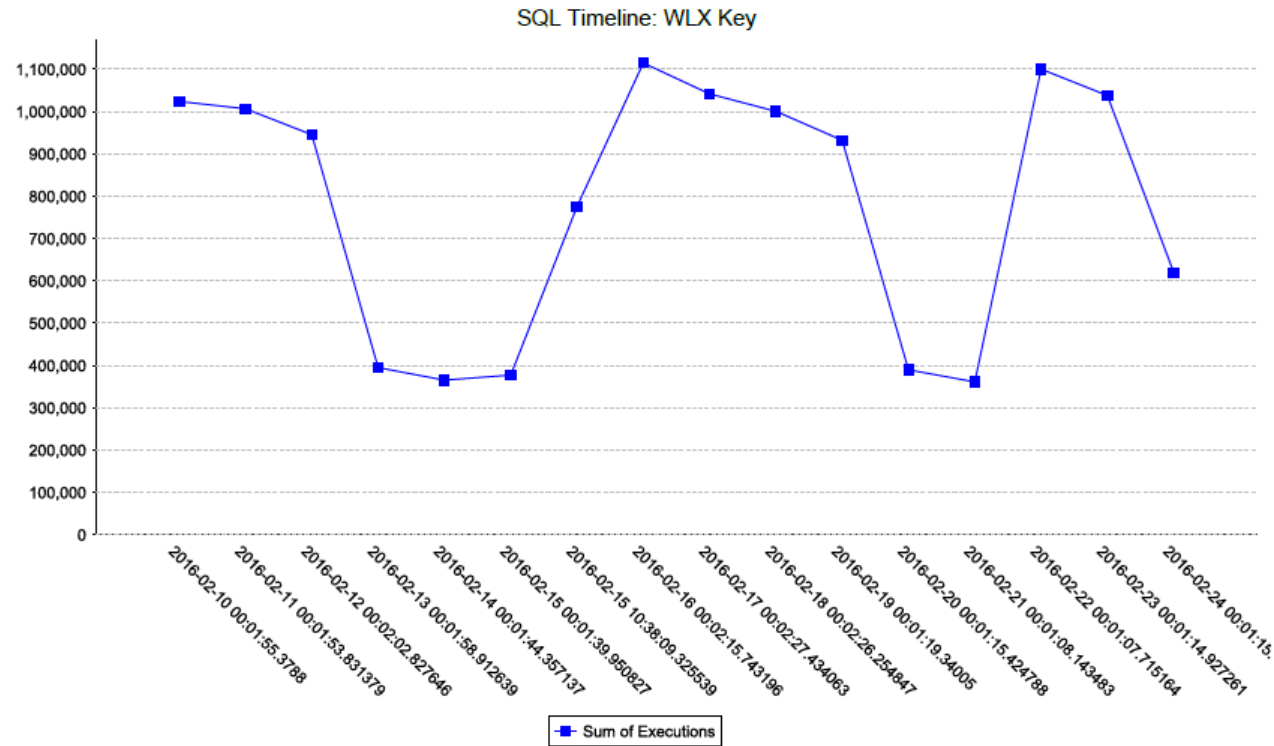
Label	Description
Statement Timestamp	The timestamp that this statement was written into the SSC c
WLB DB2 SSID	The WorkloadExpert Group or Subsystem DB2 name for this v
Primary Authorization ID	The Primary Authorization ID used to identify the applica
Package	The package used by the statement
Collection ID	The Collection ID used by the statement
Primary Authorization ID	The Primary Authorization ID used to identify the applica
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 signon or resignon
Package CONTOKEN	For Static SQL the CONTOKEN of the Package
Current SQL ID	The Current SQL ID that is running the statement
Qualifier	The Qualifier used at Bind time for unqualified objects
First referred Table Qualifier	The first tab
First referred Table Name	The first tab
Statement text	The comple
Query no.	Query numk
	User provided id string
	Authorization ID
	Job name or logon ID
	Connection name
	Plan name
	Initial authorization ID
	Connection type
	Accounting
	Work station user ID
	Transaction or application na...
	Workstation name
	Context name
	User provided id string
	Authorization ID
	Job name or logon ID
	Connection name
	Plan name
	Initial authorization ID
	Connection type that was used for an access
	Accounting token
	Work station user ID
	Transaction or application name
	The endusers workstation name
	Trusted context name



# Customer results from the banking industry

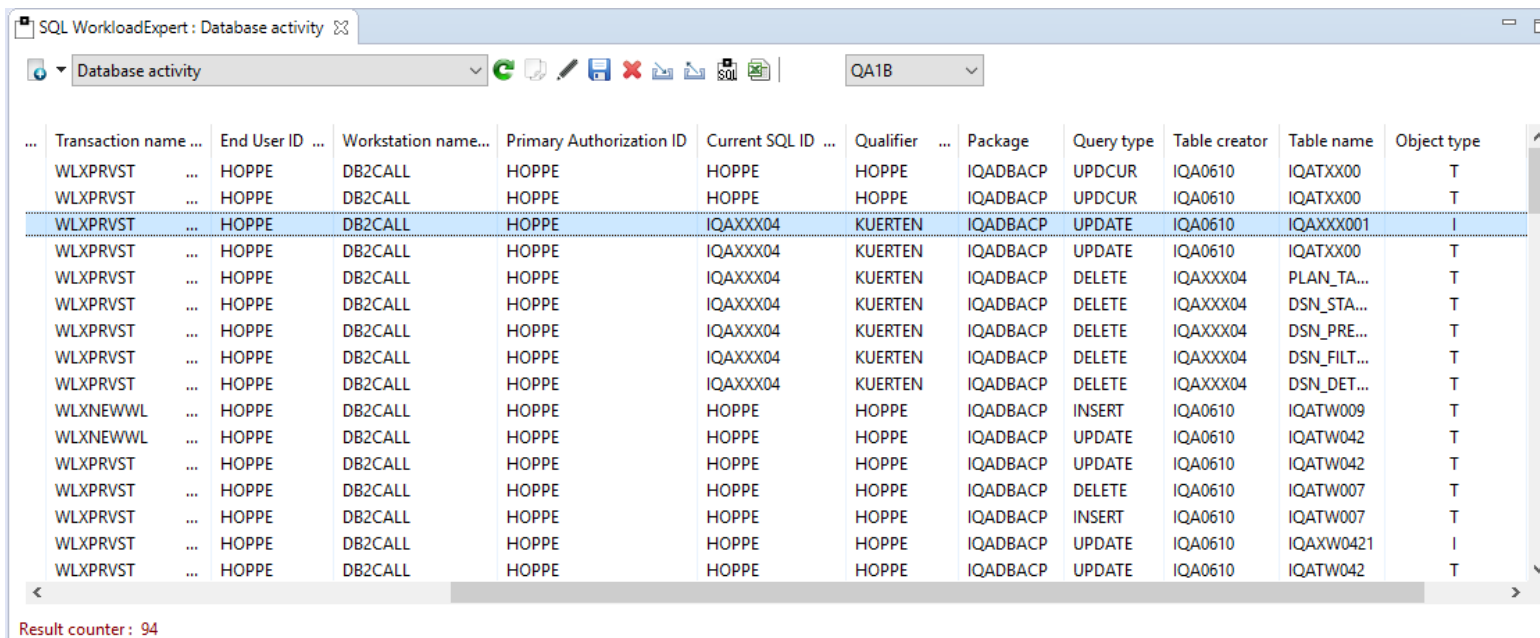
Detected anomalies: suspicious increase in SQL executions:

## WLX Report



# Customer results from the banking industry

*Show logon id as well as functional id:*

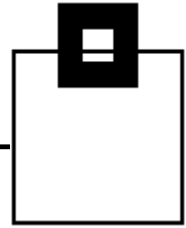


Transaction name ...	End User ID ...	Workstation name...	Primary Authorization ID	Current SQL ID ...	Qualifier ...	Package	Query type	Table creator	Table name	Object type
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	UPDCUR	IQA0610	IQATXX00	T
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	UPDCUR	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

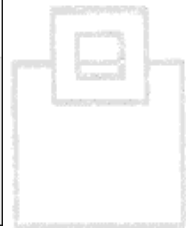
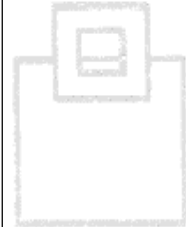
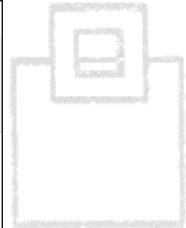
# Customer results from the banking industry

## *Generate daily audit reports matching given filters*



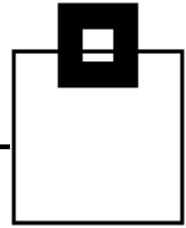
The screenshot shows the 'Object Update Dynamic' dialog box. The 'Description' field is set to 'Database activity'. The 'Projection' tab is active, showing a list of filters on the left and a table of results on the right.

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



# Customer results from the banking industry

*Generate daily audit reports matching given filters*



The screenshot displays the SQL WorkloadExpert interface. On the left, a table titled 'Database activity' shows a list of transactions. A red arrow points from the 'SQL' icon in the toolbar to the 'SQL statement' window on the right.

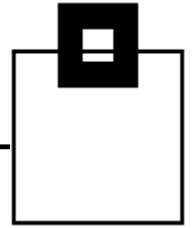
Transaction name...	End User ID ...	Workstation name...	Primary Authorization ID	Current SQL
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04
WLXPRVST	HOPPE	DB2CALL	HOPPE	IQAXXX04
WLXNEWWL	HOPPE	DB2CALL	HOPPE	HOPPE
WLXNEWWL	HOPPE	DB2CALL	HOPPE	HOPPE
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE
WLXPRVST	HOPPE	DB2CALL	HOPPE	HOPPE

```
SELECT STMT_GROUP_SSID, STMT_ID, STMT_TIMESTAMP, STMT_TYPE, TRANSACTION, END_USERID, WORKSTATION, PRIM_AUTHO
SELECT
A.WLX_TIMESTAMP
,A.STMT_GROUP_SSID
,A.STMT_ID
,A.STMT_ORIGIN
,A.STMT_TIMESTAMP
,A.STMT_TYPE
,A.EXECUTIONS
,A.GETP_OPERATIONS
,A.CPU_TIME
,A.STMT_STATS_UPD
,A.TRANSACTION
,A.END_USERID
,A.WORKSTATION
,A.PRIM_AUTHOR
,A.CUR_SQLID
,A.QUALIFIER
,A.PROGRAM
,A.PACKAGE_COLLID
,B.QLBLOCK_TYPE
,B.CREATOR
,B.NAME
,B.TYPE
FROM IQA0610.WLXT001 A
INNER JOIN IQA0610.WLXT006 B
ON A.STMT_ORIGIN = 'D'
AND A.WLX_TIMESTAMP = B.WLX_TIMESTAMP
AND A.STMT_GROUP_SSID = B.STMT_GROUP_SSID
AND A.STMT_ID = B.STMT_ID
AND A.STMT_ORIGIN = B.STMT_ORIGIN
AND A.STMT_TIMESTAMP = B.STMT_TIMESTAMP
AND A.STMT_TYPE = B.STMT_TYPE
WHERE ((1 = 1) And (A.WLX_TIMESTAMP = (SELECT MAX(WLX_TIMESTAMP) FROM
IQA0610.WLXT009 WHERE WLX_TYPE = 'X'))))
AND B.QLBLOCK_TYPE IN ('DELCUR', 'DELETE', 'INSERT', 'MERGE',
'SELUPD', 'TRUNCA', 'UPDATE', 'UPDCUR')
AND A.WLX_TIMESTAMP = (SELECT Z.WLX_TIMESTAMP FROM
IQA0610.WLX_WORKLOADS Z
WHERE Z.WLX_TIMESTAMP = A.WLX_TIMESTAMP AND Z.WLX_TYPE = 'X')
ORDER BY 5 ASC ) w
WHERE (WLX_TIMESTAMP = (SELECT MAX(WLX_TIMESTAMP) FROM
```



# Customer results from the banking industry

---



## Runtime & Costs:

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

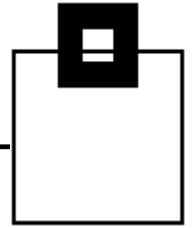
## Results:

- 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



# WLX Audit at a glance

---



## 📄 **WLX Audit for DB2 z/OS**

- Collects all SQL running on your PLEX (static and dynamic) via STC (64 bit high level ASM)
- Supports System Automation via STC Near-time Alerting
- Exploits IFI – Technology in a resource-saving way
- Covers all levels of SQL: DDL, DML, and DCL including the SQL Text
- Reports about IBM utilities, commands, Authorization failures
- Supports standard AUDIT features of the DBMS
- Provides GUIs for Eclipse native or an integration in IBM Data Studio
- Enables visualization of anomalies (SQL usage and execution rate)



# Questions???

---

Many thanks for your attention and now....

