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

AGENDA

1. Audit needs and musts
2. Solution overview and their Pros/Cons
3. WLX Audit
4. Customer results from the banking industry

Security and data breach protection

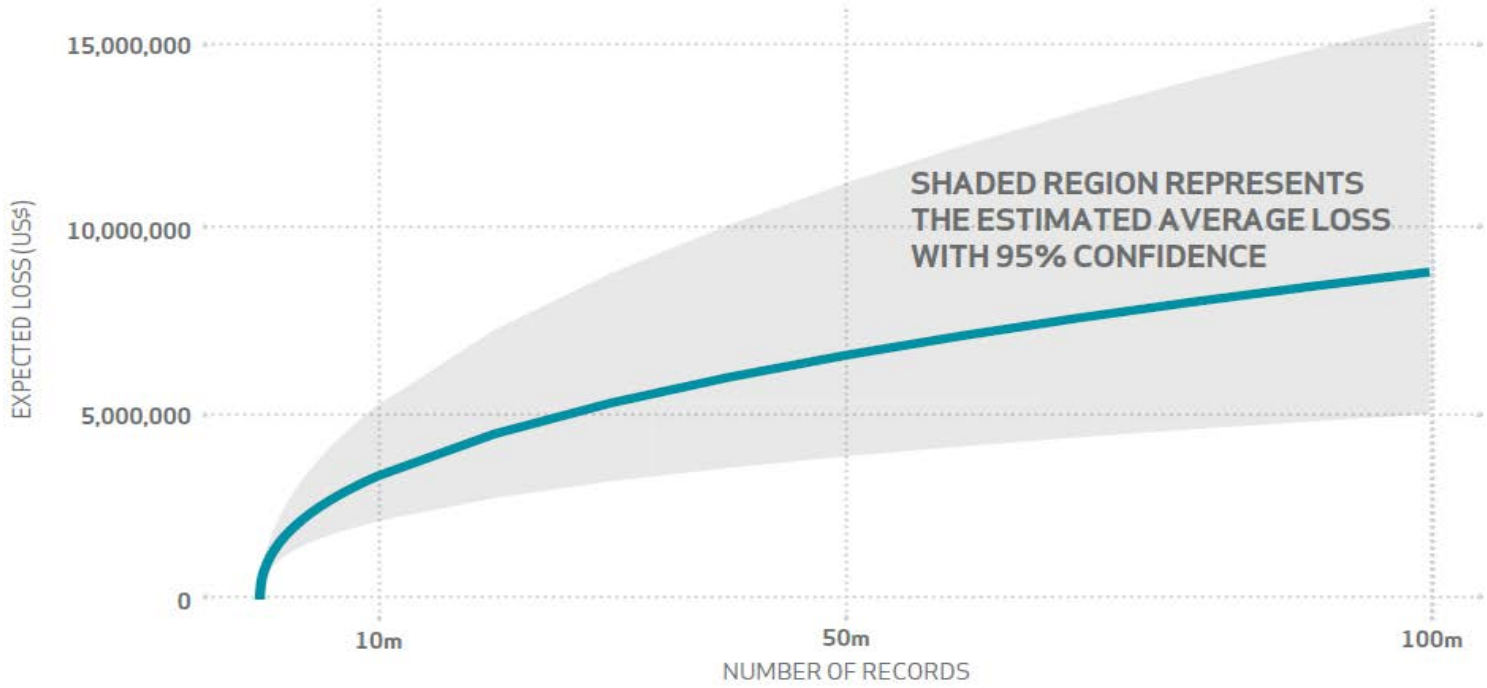
Source: 2015 Gemalto Breach Level Index
http://bit.ly/1PUCspY

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

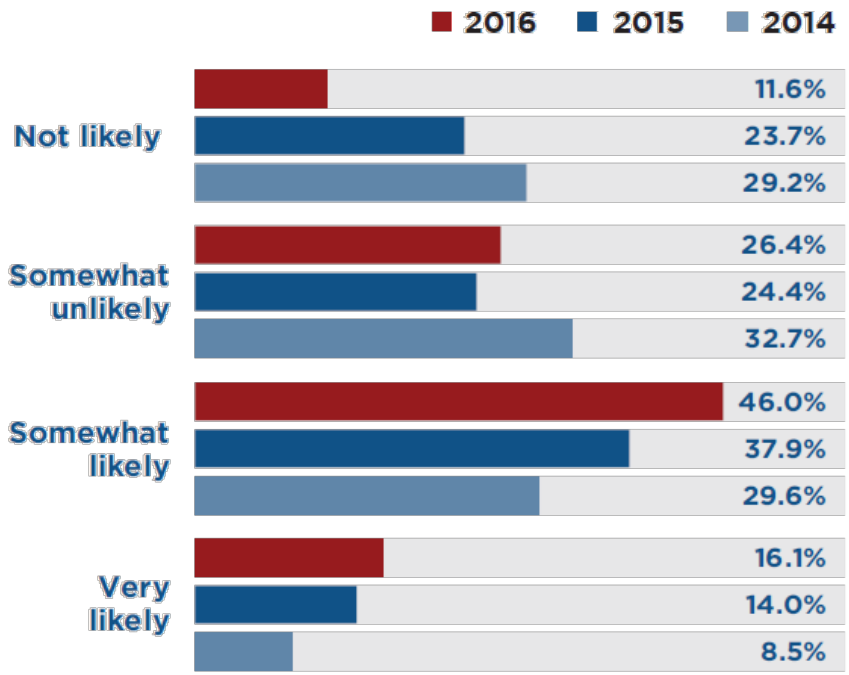
- Average loss for a breach of 1,000 records between $52,000 and $87,000
- Average loss for a breach affecting 10 million records between $2.1 million and $5.2 million

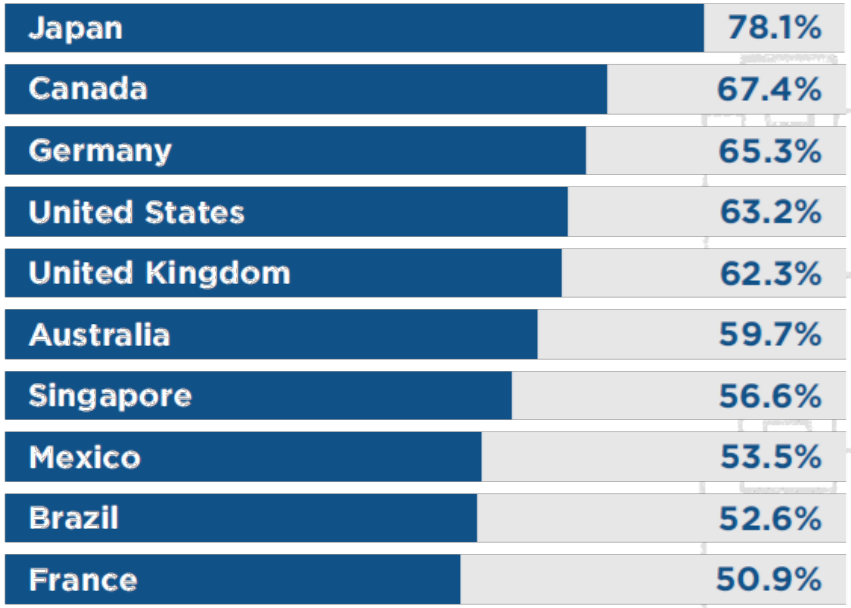


Number of cyber attacks likely to grow this year

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?

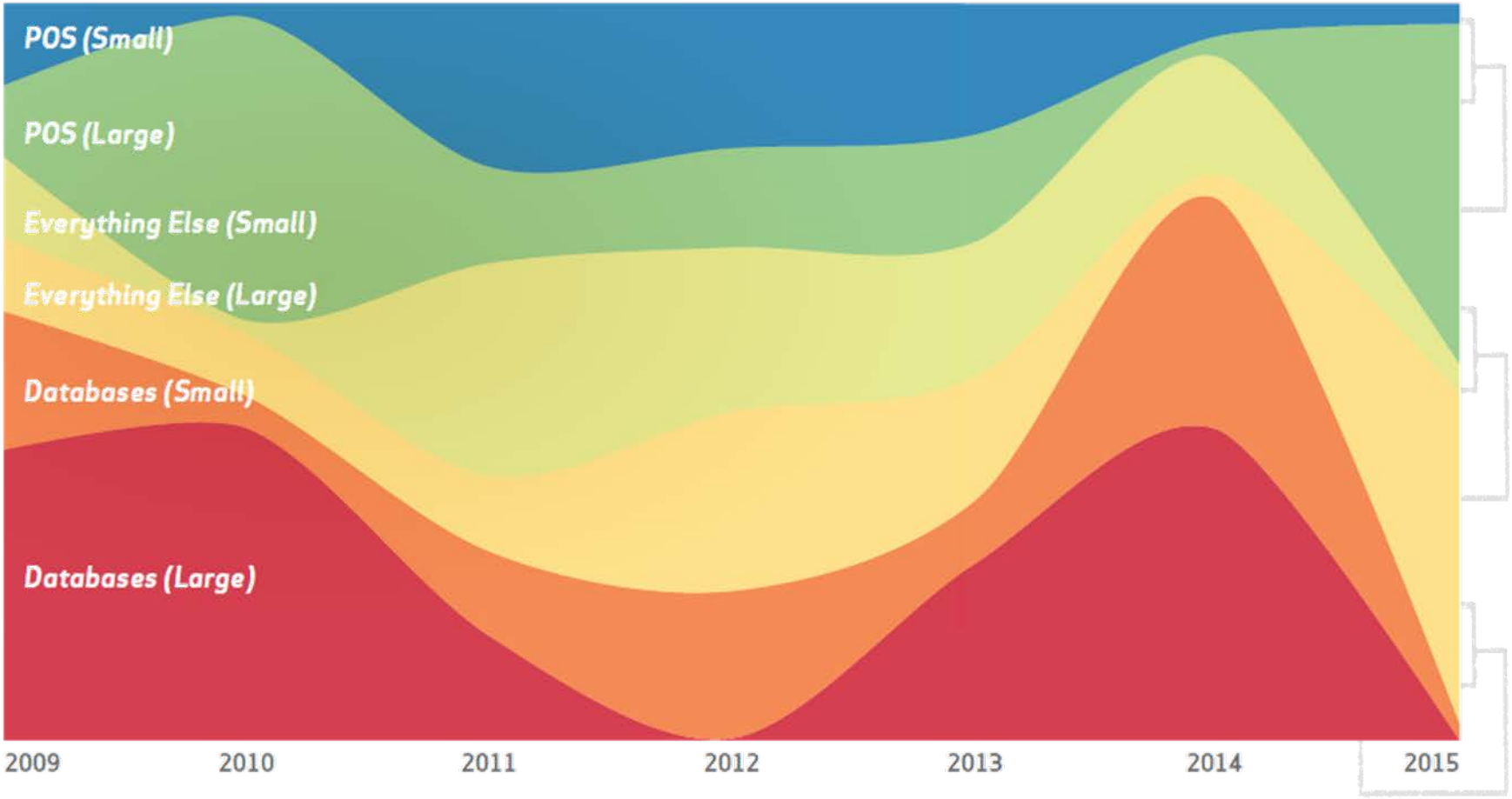
- Because they contain your/your clients most valuable information…
  - Personally identifiable information (PII, such as SSN)
  - SPI, or sensitive personal information
  - Personal financial data (PFI, also credit reporting)
  - Bank account/credit card information
  - Health information

… 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!

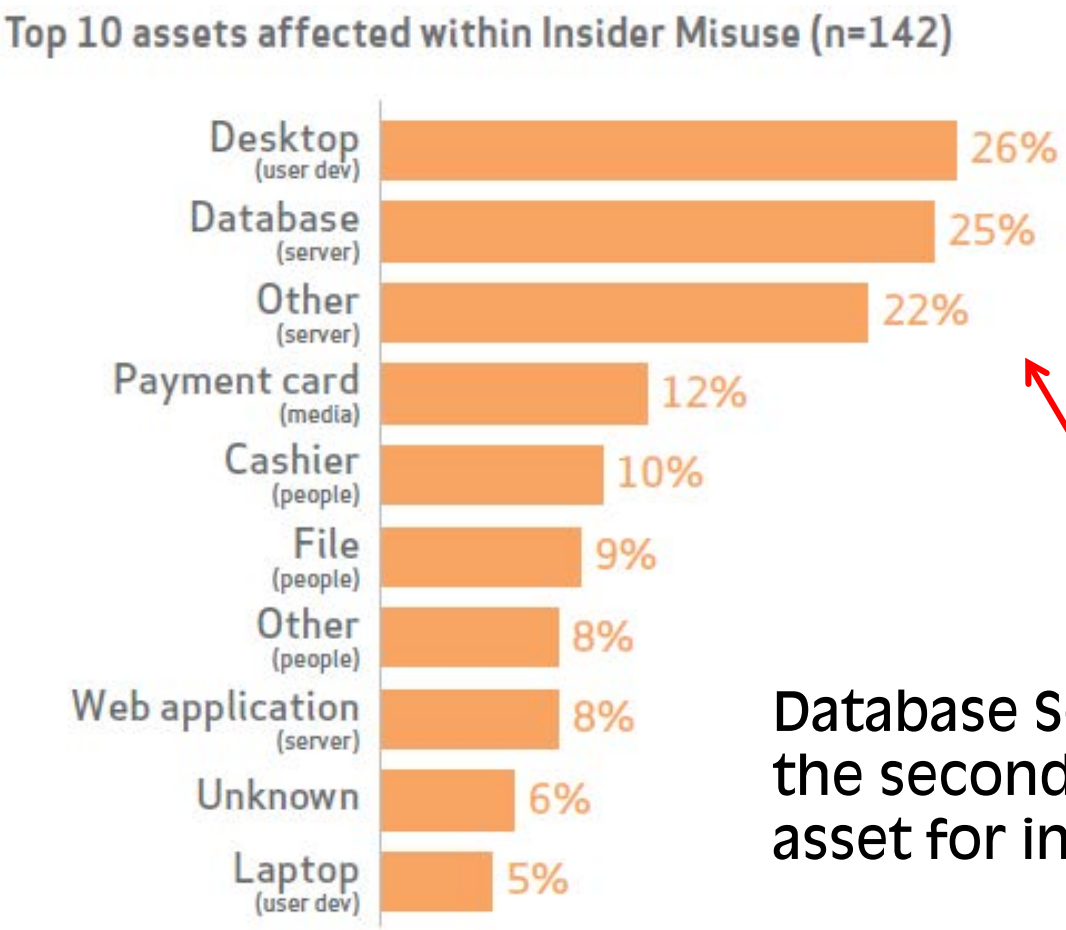
Databases are a significant target for attack

Small company = less than 1000 employee



 Source: 2015 Verizon Data Breach Investigation Report

Greatest inside misuse



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

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
    - 1st 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

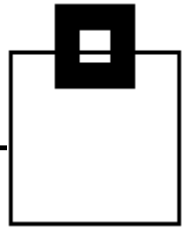
Additional Tools:

- What are the differences?

- Guess What?!

  → Several tools exploit the IFI collector!

WLX Audit



The most reliable/efficient solution, 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()

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=Listdef+220=DSs)
90/91	Commands and their completion status
140	Authorization failures
141	Authorization changes
62/142	DDL/DDL 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)

Adding the correlation headers provides detailed authentication data

We Make sure it's secure!

- By auditing access to the repository
- By alerting via WTO if someone messes with the IFCIDs
- By optionally cancelling threads of users violating the rules

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
- 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

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)

WLX Audit

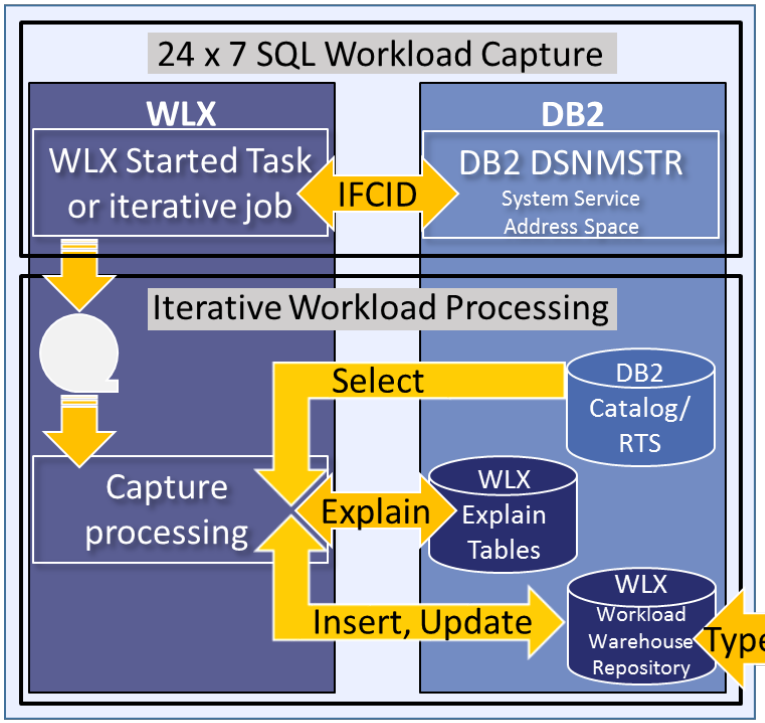
DSC and EDM provide detailed workload insights, including flushed statements:

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

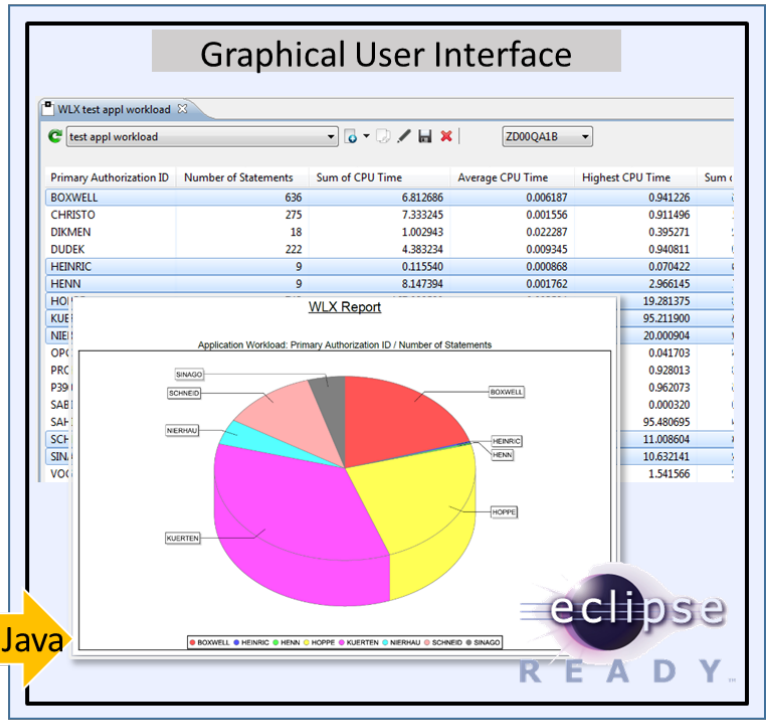
WLX Audit

Efficient data collector for your desired scope of Audit

Mainframe Engine



Workstation Engine



WLX Audit

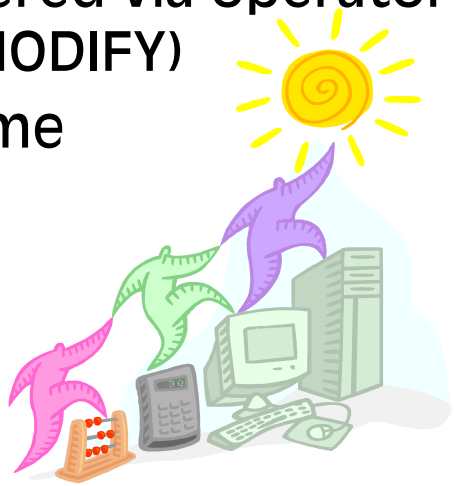
<u>Capturing the data using a STC:</u>

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

<u>Processing the workload:</u>

Externalize and process the data, e.g. every 60 min:

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



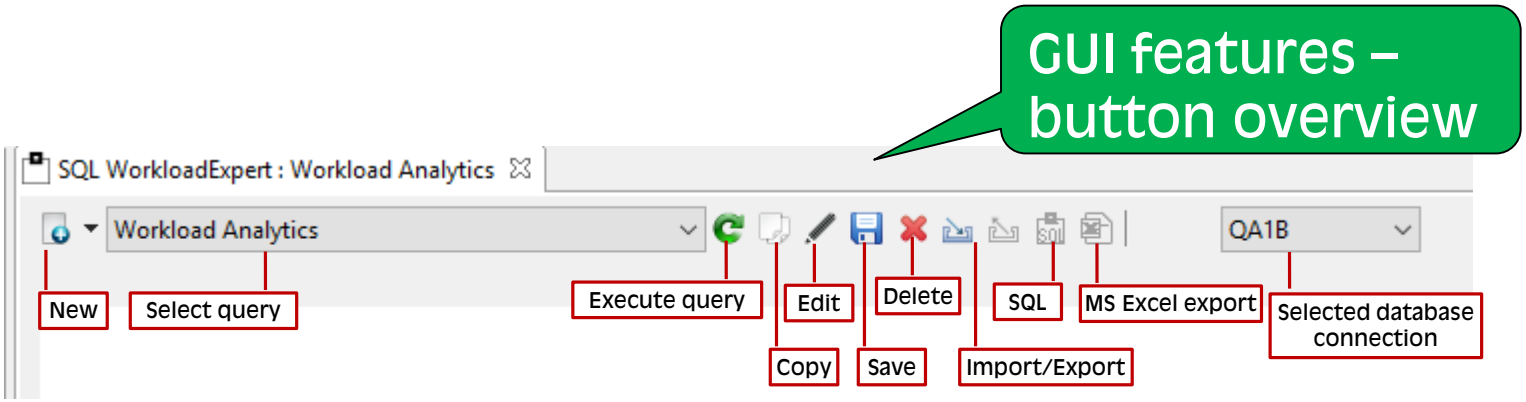
WLX Audit

<u>Integrates into a GUI front end:</u>

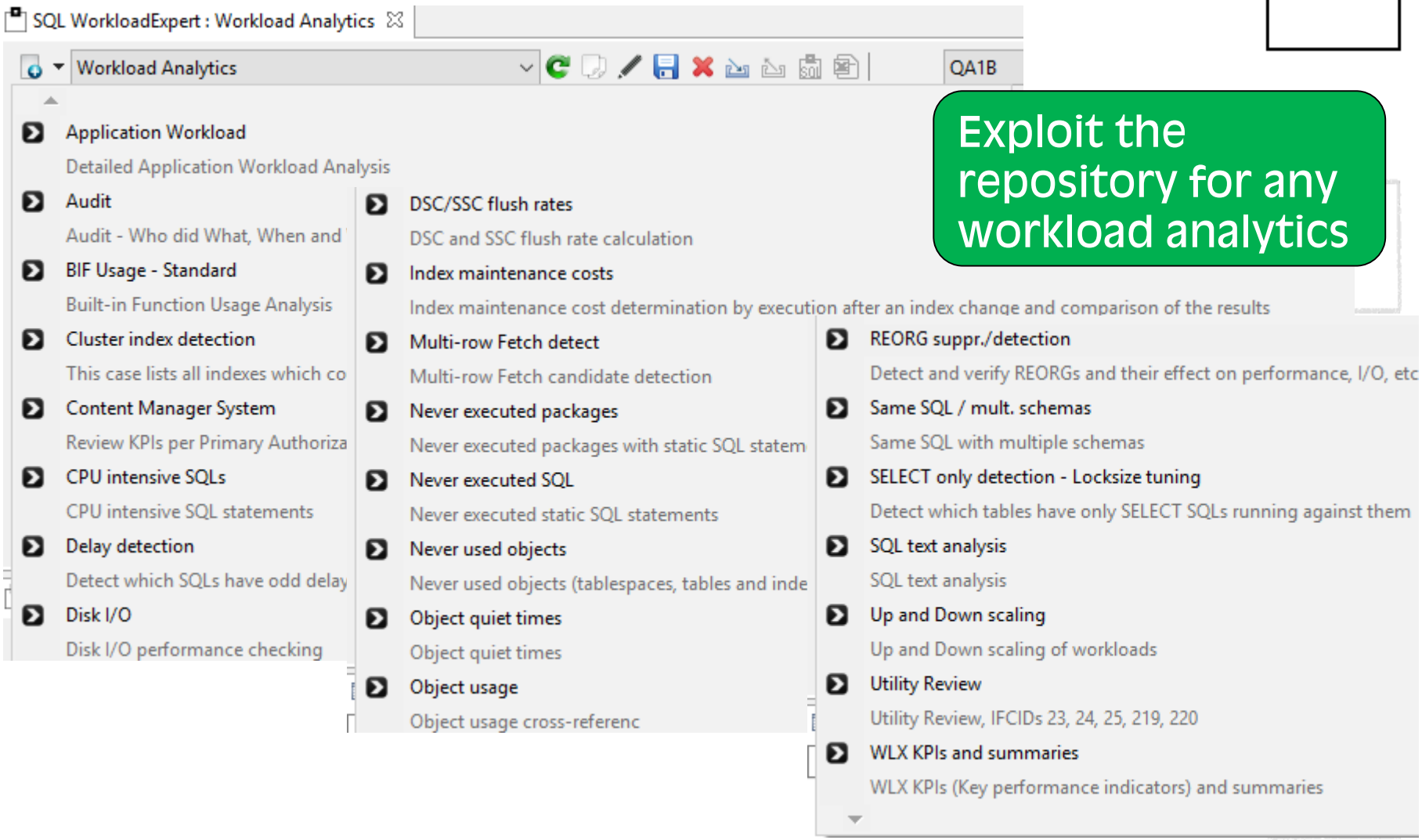
Exploits and integrates into Eclipse based GUI front ends

- 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

WLX Audit


GUI features – button overview
SQL WorkloadExpert : Workload Analytics
Workload Analytics
QA1B
New
Select query
Execute query
Edit
Delete
SQL
MS Excel export
Selected database connection
Copy
Save
Import/Export

WLX Audit



Exploit the repository for any workload analytics

WLX Audit

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	
DSN5EP2L	DSNTEP2	1	0.000712	0.000356	0.000712	0.000712	
DSNREXX	DSNREXX	2	0.038444	0.000573	0.024368	0.040348	
DSNTIAP	DSNTIAP	2	0.191846	0.000067	0.111507	0.219824	
DSNTIAUL	DSNTIB10	2	0.009314	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 . FIRSTKEYCARDF , IX . FULLKEYCARDF , IX . NLEAF ,
5    IX . NLEVELS , IX . UNIQUERULE , IX . COLCOUNT , IX . INDEXTYPE , IX . PIECESIZE , IX . PADDED , IX . AVGKEYLEN ,
6    IX . STATSTIME , IX . DATAREPEATFACTORF , 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
```

Writable | Insert | 10 : 26

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

WLX Audit

Compare workload and SQL to find anomalies

Database Development - Eclipse

File Edit Navigate Search Project Run Window Help

SQL Results | Execution Plan | Bookmarks | SQL WorkloadExpert - Compare view

Selection 1 — IHISDB SDB2VNEX TEST 1

Primary Authorization ID	Package	Collection ID	Executions	Executions per hour	CPU Time
	COISEAR	PTFCOLL008	15	0	

Selection 2

Primary Authorization ID	Package	Collection ID	Executions	Executions per hour	CPU Time
	COISEAR	PTFCOLL008	7	0	

Selection details

Column name	Selection value 1	Selection value 2
Primary Authorization ID		
Package	COISEAR	COISEAR
Collection ID	PTFCOLL008	PTFCOLL008
Executions	15	7
Executions per hour	0	0
CPU Time	0.896205	0.584763
Average CPU Time	0.059747	0.083537
CPU Time per hour	0.013221	0.022216
Elapsed Time	0.993085	1.037974
Average Elapsed Time	0.066205	0.148282

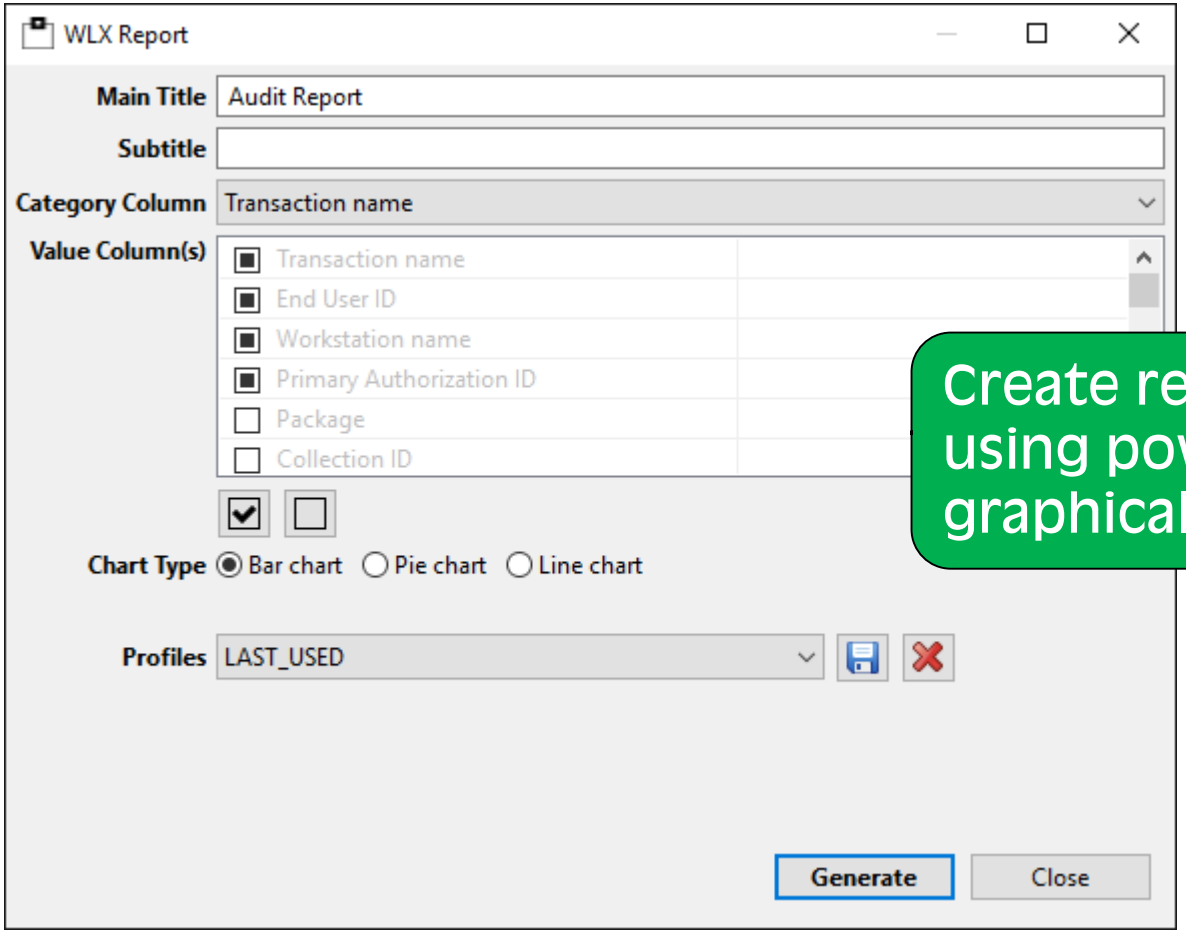
Value 1

```
DECLARE O2TEST4-01 CURSOR FOR SELECT A . PTFNO , B . PTFSEQ , A . PTFSTATUS ,
B . MEMBERTYPE , B . RMEMBERNAME , B . PREREQ , B . POSTREQ , B . LOCKSINCE ,
B . LOCKOWNER , A . LYDIANO , A . PRODUCT , A . RELEASE , B . SOUTOLIB , A . RPTFNO
FROM PTFADMIN . PTF A , PTFADMIN . MEMBER B WHERE A . PTFNO = B . PTFNO AND A . LYDIANO
LIKE : H AND A . PTFNO LIKE : H AND A . PRODUCT LIKE : H AND A . RELEASE LIKE : H AND B
```

Value 2

```
DECLARE O2TEST4-01 CURSOR FOR SELECT A . PTFNO , B . PTFSEQ , A . PTFSTATUS ,
B . MEMBERTYPE , B . RMEMBERNAME , B . PREREQ , B . POSTREQ , B . LOCKSINCE ,
B . LOCKOWNER , A . LYDIANO , A . PRODUCT , A . RELEASE , B . SOUTOLIB , A . RPTFNO
FROM PTFADMIN . PTF A , PTFADMIN . MEMBER B WHERE A . PTFNO = B . PTFNO AND A . LYDIANO
LIKE : H AND A . PTFNO LIKE : H AND A . PRODUCT LIKE : H AND A . RELEASE LIKE : H AND B
```

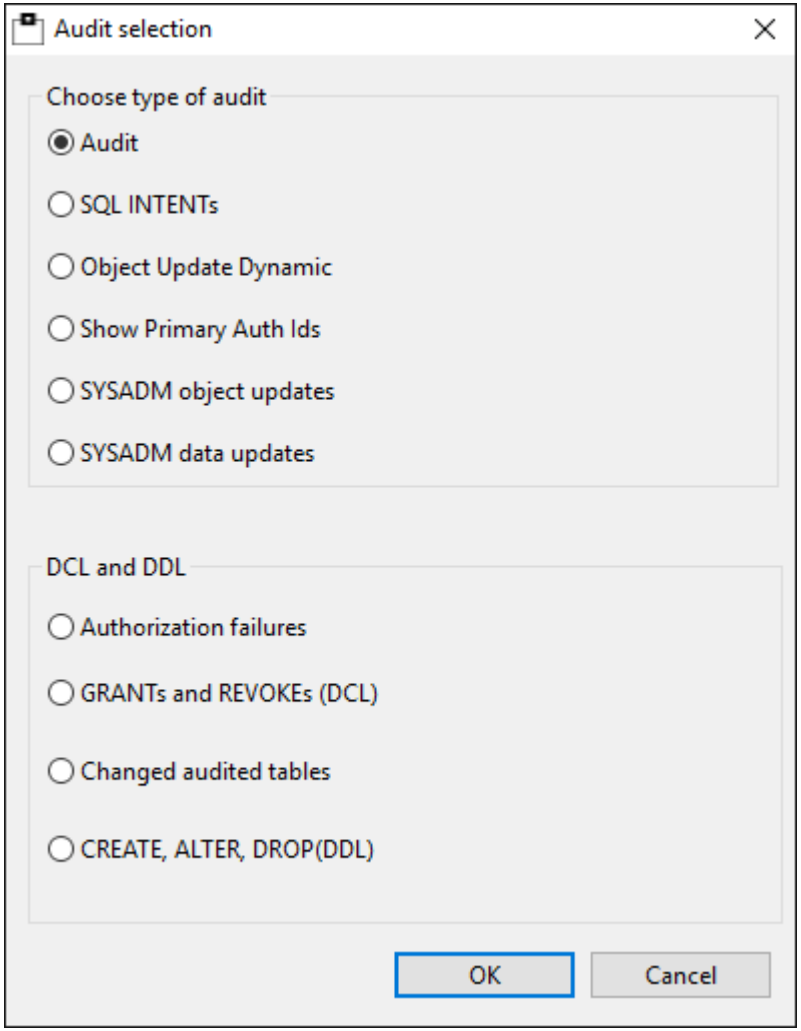
WLX Audit



Create reports using powerful graphical charts

WLX Audit

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



WLX Audit

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

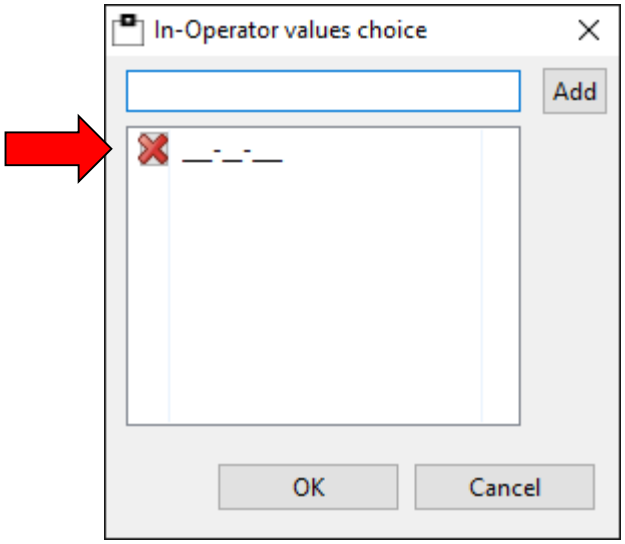
SQL WorkloadExpert : DML Audit

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	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	MVNXX861	
BOXWELL	BOXWELL	TSO	BOXWELL	BOXWELL	BOXWELL	DSNESM68	SELECT	READ	MVNXTEST	MVNXT86	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	MEMBER	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	USERTAB	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	PTF	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	PTFTIN02	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	PTF	
HOPPE	HOPPE	DB2CALL	HOPPE	PTFADMIN	PTFADMIN	DSNREXX	SELECT	READ	PTFADMIN	PTF	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQATI006	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQAXI0061	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQATI007	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQAXI0071	

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*

```
PRINTCOM=YES
MONITOR=mbr
IFCIDS=(23,24,25,62,90,91,140,141,142,143,144,219,220,316,318,400,401)
BUFSIZE=16384
PERC=25
SWAP=YES
PGFIXRET=NO
PGFIXBUF=NO
PINGINT=5
WAKEUP=10
WAIT4DSN=600
INIT64=2
MAX64=64
```

Utilities

DDL

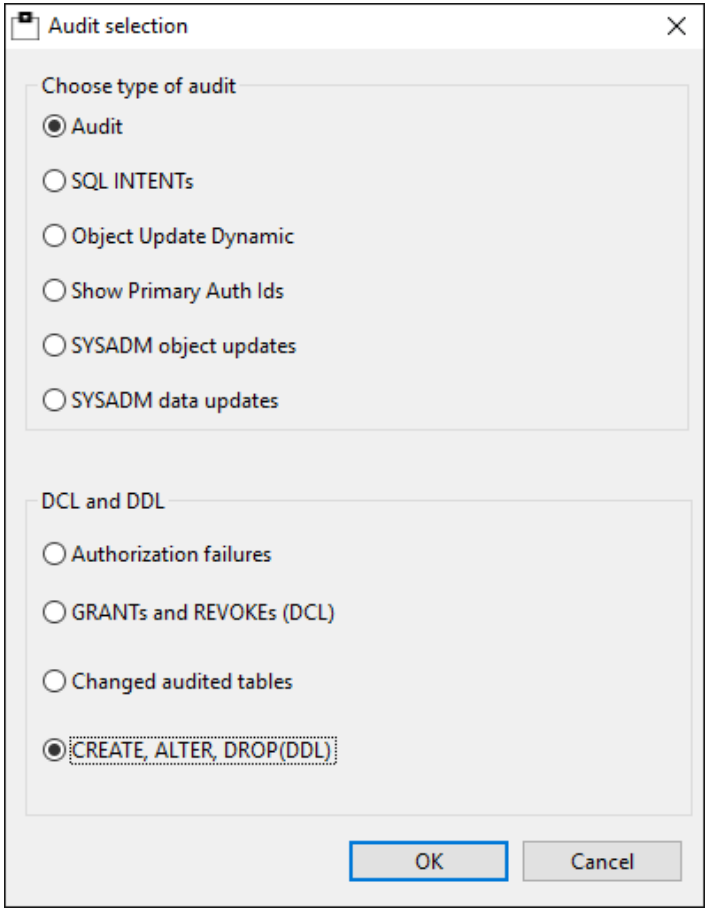
DCL

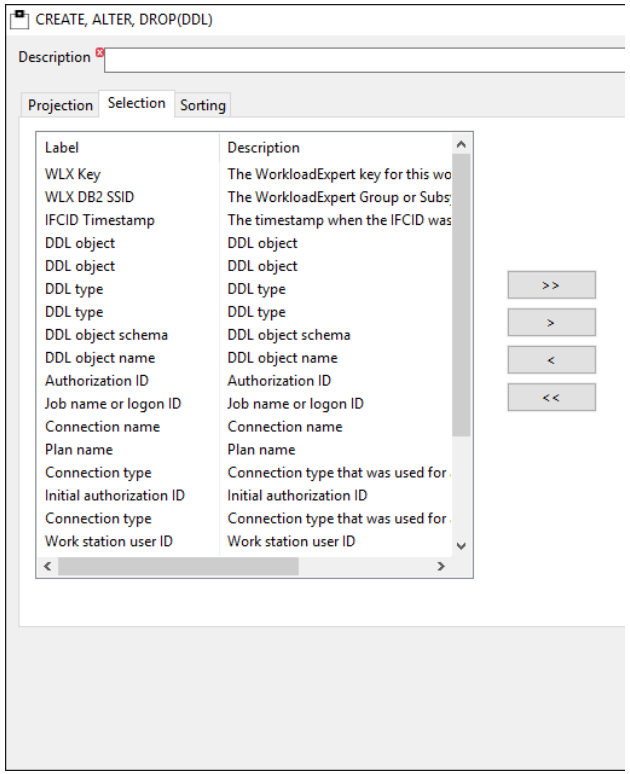
DML

DML

Customer results from the banking industry

Show DDL activities:





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 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

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

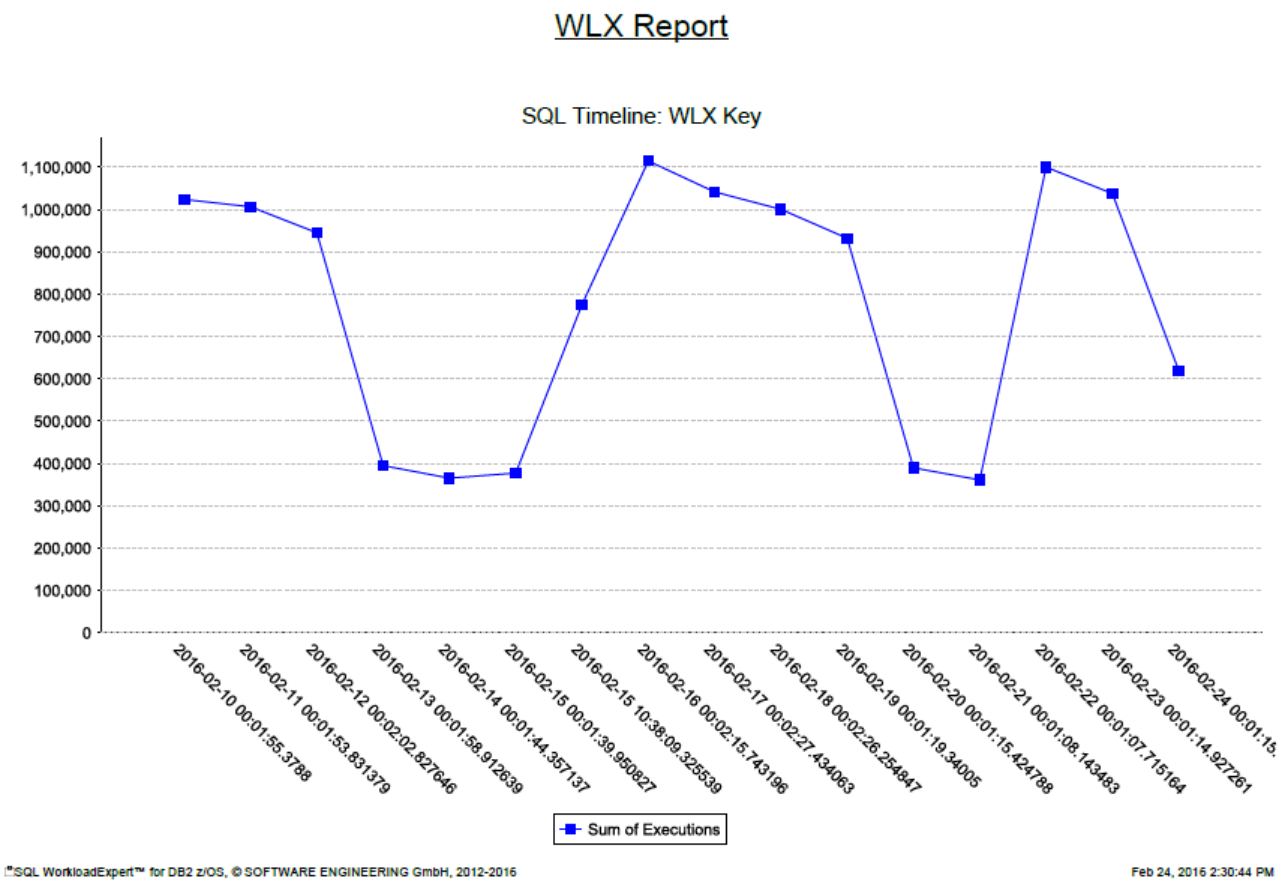
DML Reporting:

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 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 numl

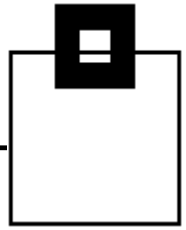
User provided id string	User provided id string
Authorization ID	Authorization ID
Job name or logon ID	Job name or logon ID
Connection name	Connection name
Plan name	Plan name
Initial authorization ID	Initial authorization ID
Connection type	Connection type that was used for an access
Accounting	Accounting token
Work station user ID	Work station user ID
Transaction or application na...	Transaction or application name
Workstation name	The endusers workstation name
Context name	Trusted context name

Customer results from the banking industry

Detected anomalies: suspicious increase in SQL executions:

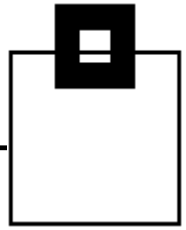


Customer results from the banking industry



Show logon id as well as functional id:

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 tha
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

Generate daily audit reports matching give filters

Project Run Window Help

SQL WorkloadExpert : Database activity

Database activity

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

Result counter : 94

SQL Results | Execution Plan | Bookmarks

Type query expression here | Status

Status	Operation	Date	Connectio...

SQL statement

```
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.QBLOCK_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.QBLOCK_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
- 3rd party applications with update intent, but should actually be read

WLX Audit at a glance

WLX Audit for DB2 z/OS

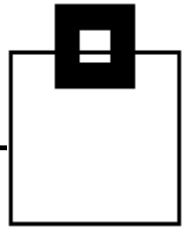
- Collects all SQL running on your PLEX (static and dynamic) via STC (64 bit high level ASM)
- Supports System Automation via STC Neartime Alerting
- Exploits IFI – Technology in a resource-saving way
- Covers all levels of SQL: DDL, DML, and DCL including the SQL Text
- Reports about IBM utilities, 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)

WLX typical use cases

<u>Application Development:</u>

- 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

WLX functional packages of use cases

<u>Audit and Security:</u>

- 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.)