

SQL WorkloadExpert for Db2 z/OS

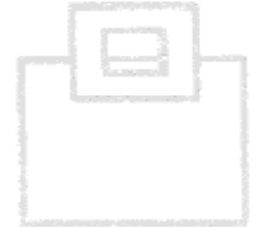
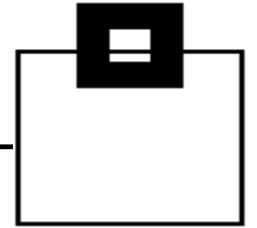
Compliance with compliments!

Audit Component



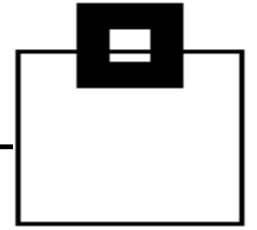
AGENDA

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

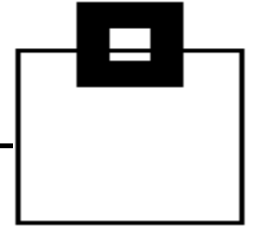


Audit – do you need it, do you care?!

- 61% of companies state that cybercrime and data theft are their most challenging threats
- 92% of respondents of a Lloyds Bank survey suffered a data breach in the past five years
- The number of attacks is growing each year
- Last year about ½ Billion records stolen
- Reputation is significantly affected by breaches
- The average cost of a data breach is \$5.4M+
- Fines, penalties and losses are \$105 - \$359 per data record → calculate your companies costs
- Securing environments is still a catch-up task:
 - Technology gets better, but attackers still find their way – sometimes from inside!
- 95% of the attacks start with a human error (website, or Email attachment)



Audit – do you need it, do you care?!



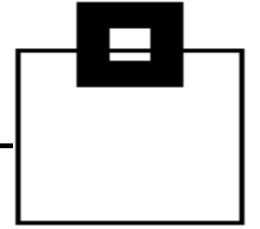
- Attackers use...
 - SQL injection
 - DDoS
 - Third-party software
 - XSS
 - Malware
 - Phishing
 - Watering holes/Honey pots
 - Physical access



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



Audit – do you need it, do you care?!



... the enterprises database servers are the target in 96% of the security breaches!

Because they contain your/your client's most valuable information...



- Customer personal information (PI, such as SSN)
- Detailed 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!



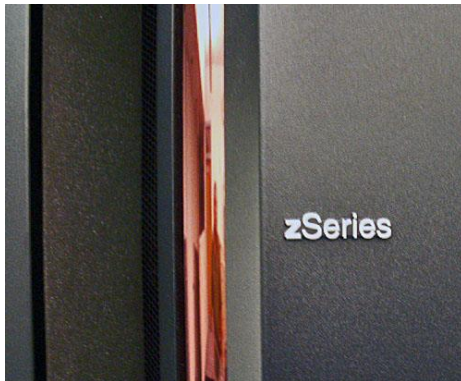
Audit – do you need it, do you care?!

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”

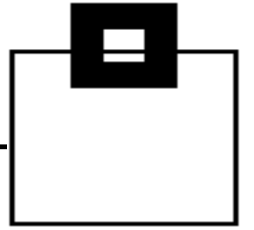
President, Mittal Technologies Inc.



Audit needs and musts

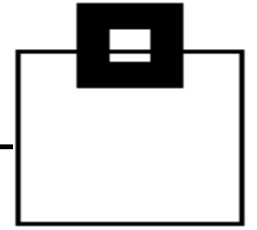
However, protecting and auditing is a major cost factor nowadays, thus the authorities had to force companies to pay attention:

- 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)

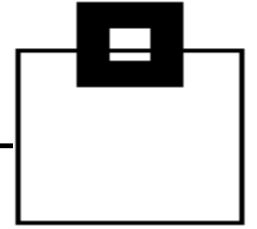


Audit needs and musts

- Chose your *favorite* one and/or use a reliable resource for guidance:
 - Center of Internet Security (CIS)
 - Department of Defense (DoD)
 - Security Technical Implementation Guide (STIG)
 - Common Vulnerability Exposure (CVE)
 - Bundesamt für Sicherheit in der Informationstechnik (BSI)



Audit needs and musts

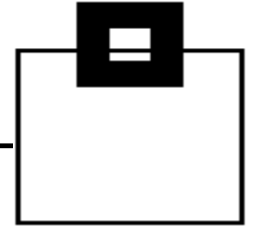


- Make sure you meet your business needs (e.g. PCI DSS):

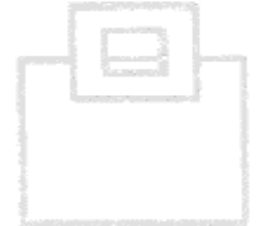
PCI DSS Requirement	Authentication, Authorization or Audit?
10.1 Establish a process for linking all access to system components to each individual user ...	Authentication, authorization AND audit
10.2.7 Log the creation and deletion of system level objects	Audit
10.3 Record audit trail entries for all system components for each event...	Audit
10.5 Secure audit trails so they cannot be altered.	Audit
10.6 Review logs for all system components related to security functions at least daily	Audit
10.7 Retain audit trail history for at least one year; at least three months of history must be immediately available for analysis	Audit



Audit needs and musts



- Critical activities that enterprises should be auditing
 - Privileged Users
 - Access/changes/deletion to critical data
 - Access using inappropriate channels
 - Schema modifications
 - Unauthorized addition of user accounts
 - End Users
 - Unusual access to excessive amounts of data
 - Access to data outside standard working hours
 - Access to data through inappropriate channels
 - Developers, Analysts and System Administrators
 - Access to live production systems
 - IT Operations
 - Inappropriate changes to DB/DB applications

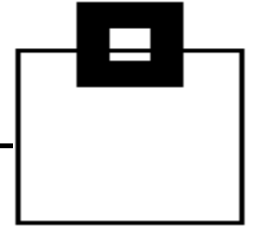


Audit needs and musts

- 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

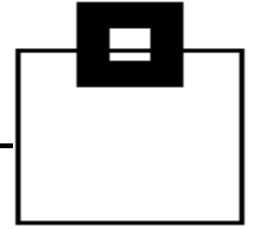
Audit needs and musts



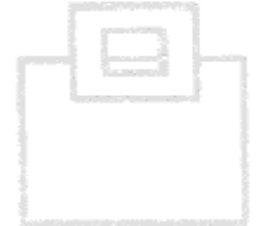
- ... or in other words:
Collect as much data as you can, because you probably don't know today what you'll need tomorrow
→ **breach patterns do change!!!**
- Make sure you include:
 - SELECTs (against sensitive data)
 - DDL
 - DML
 - DCL
 - Utilities (online + offline)
 - Commands
 - Assignment, or modification of a user ID/authorization – especially privileged users



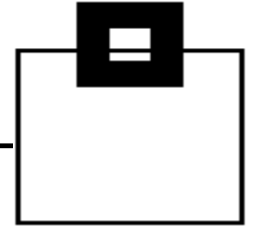
Audit needs and musts



- 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 cluster
- Also consider your INSTALL SYSADM/SYSOPR
 - Sorry DBAs, but Auditing requires a separation of duties



Audit needs and musts

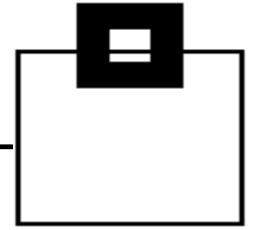


- Most Home-Grown Solutions are based on the Db2 Audit Trace
 - Class 1, 2, 7, 8 have very little overhead
 - Access violations
 - GRANTS/REVOKEs
 - Assignment, or modification of a user ID/authorization
 - Start of a Db2 online utility
 - Class 3 (IFCID 142) has very little overhead
 - DDL (only for TB having the AUDIT ALL attribute)
 - Class 4, 5 (IFCID 143, 144) has 15% - 20% overhead
 - 1st SELECT, INSERT/UPDATE/DELETE of a UOR
 - IFCID 90, 91 have very little overhead
 - Db2 Commands

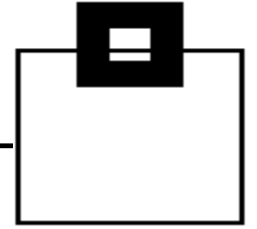


Solution overview and their Pros/Cons

- 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

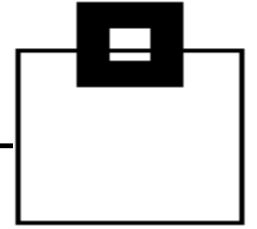


Db2 Log:

- 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)
 - Most companies have Log analysis tools they're already familiar with
- Cons:
 - Not all required data is logged
 - SELECTs are especially lacking



Solution overview and their Pros/Cons

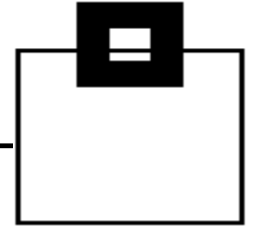


Db2 Trace:

- Pros:
 - Comes with Db2 and supports all versions
 - No additional costs (except for storing and processing the collected data)
 - Most companies have trace data analysis tools they're already familiar with
- Cons:
 - Depending on the scope (number of IFCIDs/classes), and the type (SMF, OPX, GTF, SRV), the overhead may be significant
 - You need to build your own repository



Solution overview and their Pros/Cons

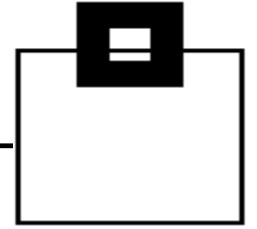


Db2 Trace:

- What are the differences:
 - There are different types of traces:
 - Statistics, Accounting, Audit, Monitor, Performance, Global
 - There are different classes
 - There are hundreds of individual IFCIDs
- Depending on your choice, the overhead is unmeasurable to significant
- A key difference in cost is the trace destination!
 - SMF, OPX, GTF, SRV



Solution overview and their Pros/Cons

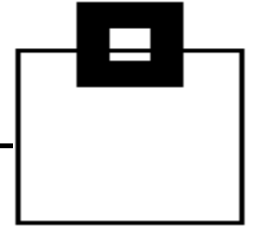


Db2 Trace:

- What are the differences:
 - Processing the data requires simple to more sophisticated knowledge:
 - SMF: System Management Facility:
Most commonly used, easy to process (use DSN1SMFP)
 - 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:
We have never seen it used



Solution overview and their Pros/Cons

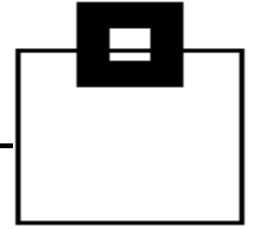


Db2 Memory (DSC/EDM):

- Pros:
 - Comes with Db2 and supports all versions
 - No additional overhead
 - No additional costs (except for storing and processing)
- Cons:
 - Not all required data is there
 - Usually you can't access it yourself, unless you hook into it
 - The information is volatile and can get lost quickly



Solution overview and their Pros/Cons

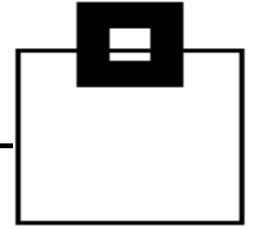


Db2 Exits:

- 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

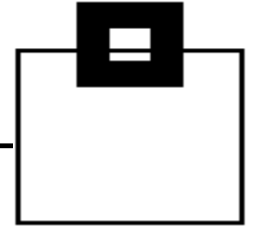


Additional Tools:

- 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

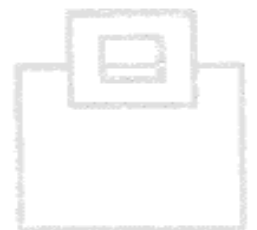
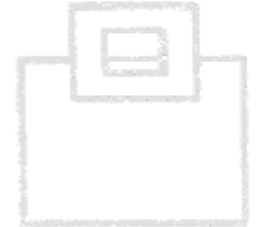


Solution overview and their Pros/Cons

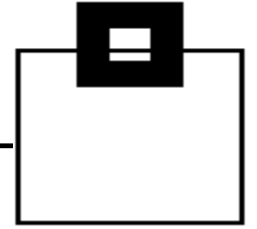


Additional Tools:

- What are the differences?
 - Good solutions have efficient data collectors and share repositories for Audit, Performance Management, Accounting, Analytics ...
 - Some solutions use hooks into the Db2 address space to capture SQL activity – errors can bring down Db2, or the entire LPAR, thus they try to protect Db2 by encapsulating the “foreign” code
 - Some solutions need additional appliances (easily up to 100+ virtual appliances)
→ all SQL captured is sent (unencrypted!) through the network. If the connection gets lost they try to cache it. Keep in mind that attackers do DDoS attacks!

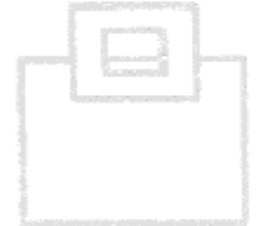
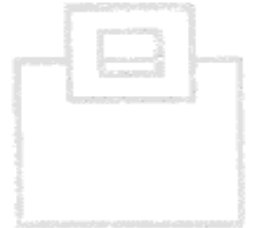


Solution overview and their Pros/Cons

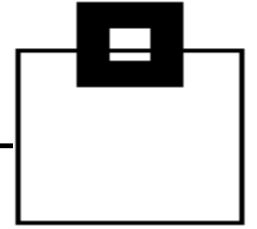


Additional Tools:

- 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!



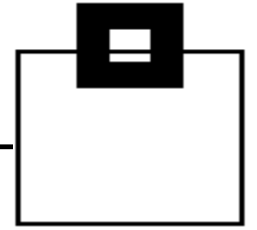
The viable way – let Db2 do the magic

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?



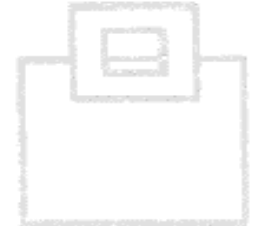
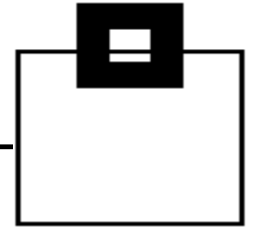
The viable way – let Db2 do the magic

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

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

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=DSSs)

55/83/87 SQLID setting

90/91 Commands and their completion status

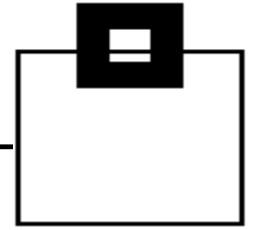
140 Authorization failures

141 Authorization changes

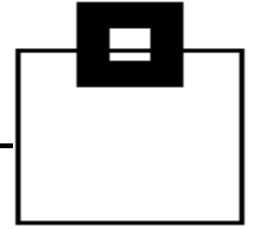
62/142 DDL/DDI for tables with audit changes/all

270/271 Trusted Context and Row Permission masks

Add the correlation headers to get detailed authentication data



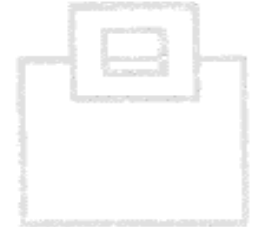
The viable way – let Db2 do the magic



BUT:

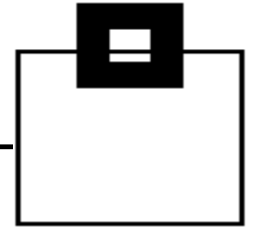
Make sure it's secure!

- 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

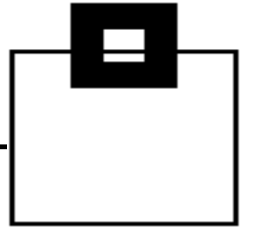


The viable way – let Db2 do the magic

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

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

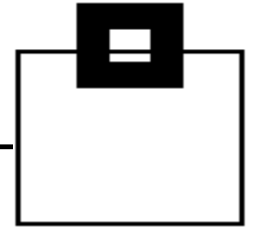
If you don't want to improve your Home Grown solution, find a vendor who exploits this technology



The viable way – let Db2 do the magic

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

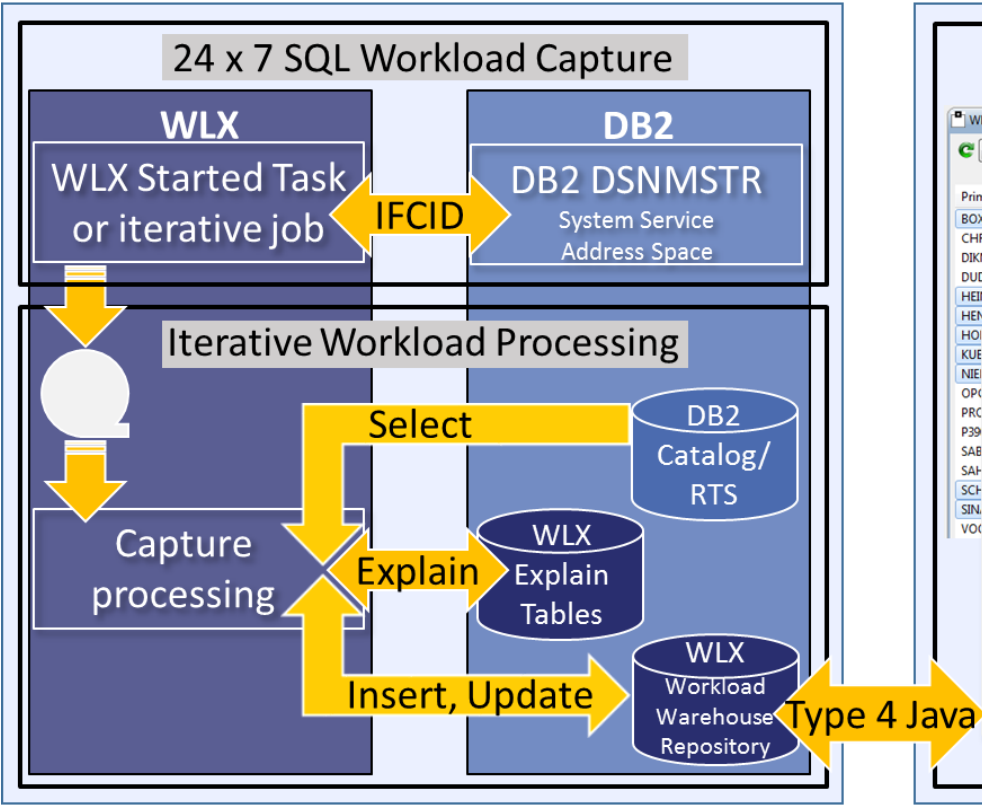
- SQL text
- Statement ID
- Date/time
- Current status
- Resource consumption
- Identification/environmental data



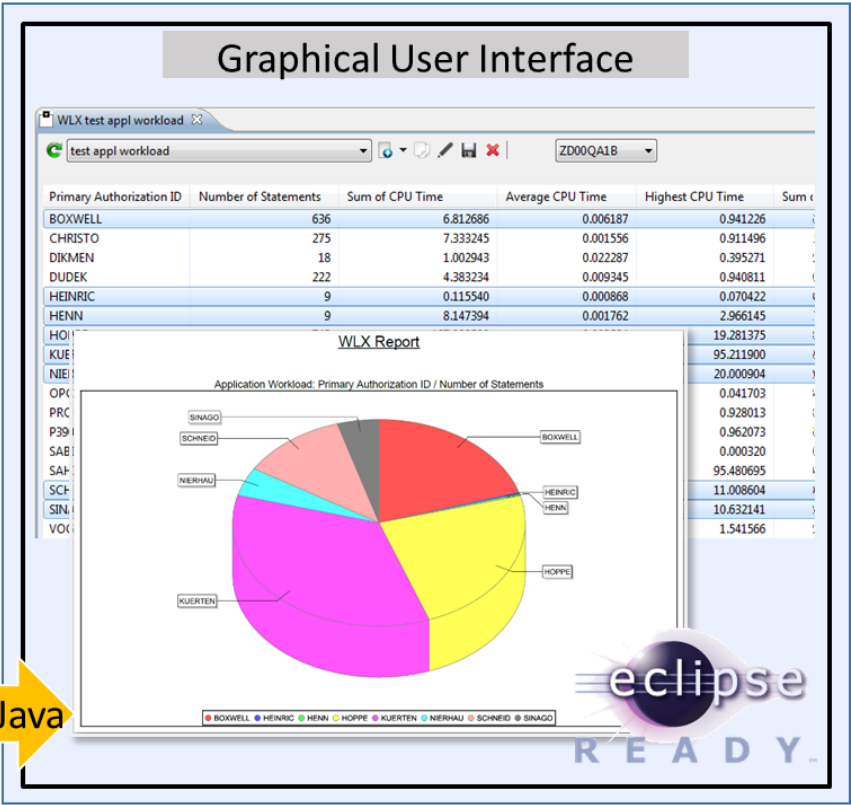
The viable way – let Db2 do the magic

Efficient data collector for your desired scope of Audit

Mainframe Engine



Workstation Engine



The viable way – let Db2 do the magic

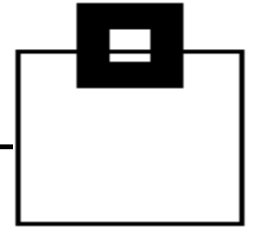
Capture the data e.g. using a STC:

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

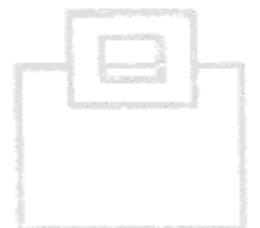
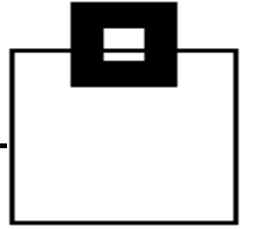


The viable way – let Db2 do the magic

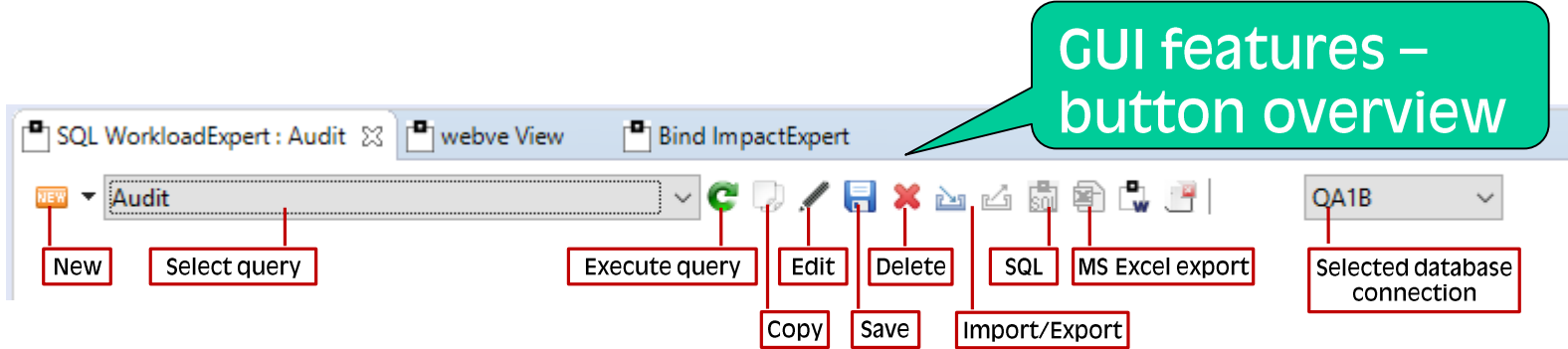
Use a GUI front end, preferably Eclipse:

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

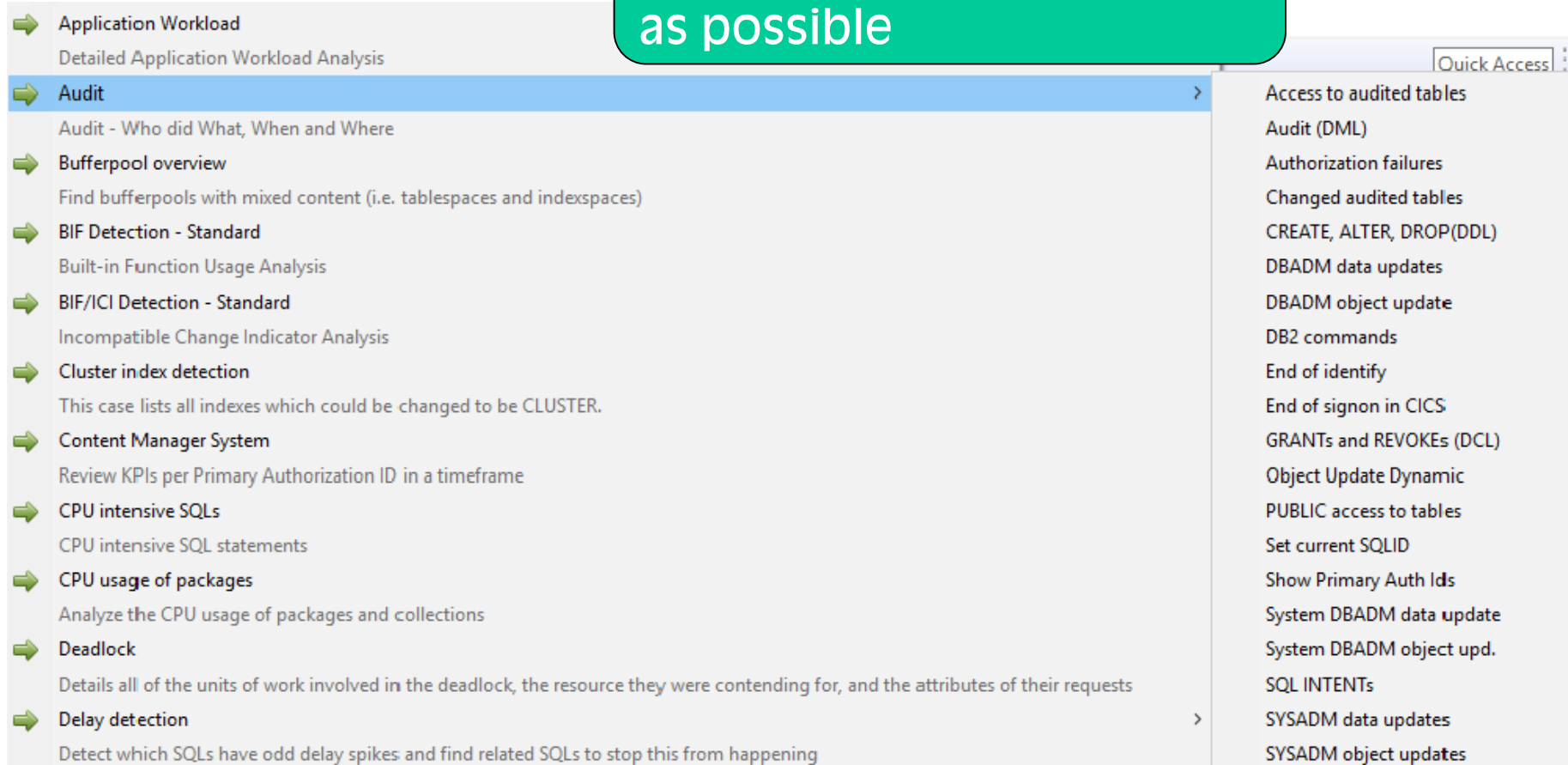


The viable way – let Db2 do the magic



The viable way – let Db2 do the magic

Delivered Use Cases make
using the product as easy
as possible



The viable way – let Db2 do the magic

Selection, Filtering and
Sorting makes the delivered
Use Cases easy to customize

Audit (DML)

Description:

Projection Selection Sorting

Label	Description
Transaction name	A value provided by the RRS signon ...
WLX Key	The WorkloadExpert key for this wor...
End User ID	A value provided by the RRS signon ...
WLX DB2 SSID	The WorkloadExpert Group or Subsy...
Workstation name	A value provided by the RRS signon ...
Statement ID	The DB2 internal Statement ID
Primary Authorization ID	The Primary Authorization ID used t...
Statement Origin	D for Dynamic SQL or S for Static SQL
Statement Timestamp ...	The timestamp that this statement ...
Package	The package used by the statement
Statement Type	N for No SQL statement text availab...
Collection ID	The Collection ID used by the state...
Min. INSERT timestamp	Minimal INSERT timestamp
Number of Users	The total number of Users of this st...
Max. UPDATE timestamp	Maximum UPDATE timestamp
Number of Copies	The total number of copies of this s...
Status of the Statement	Zero is Normal, 16 is invalidated by ...

>> > < <<

Label	Operator	Value	Description
WLX Key	=	newest	The WorkloadExpert key for this wor...
End User ID	=	SUSPECT	A value provided by the RRS signon ...

< >

↑ ↓

OK Cancel

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	
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:

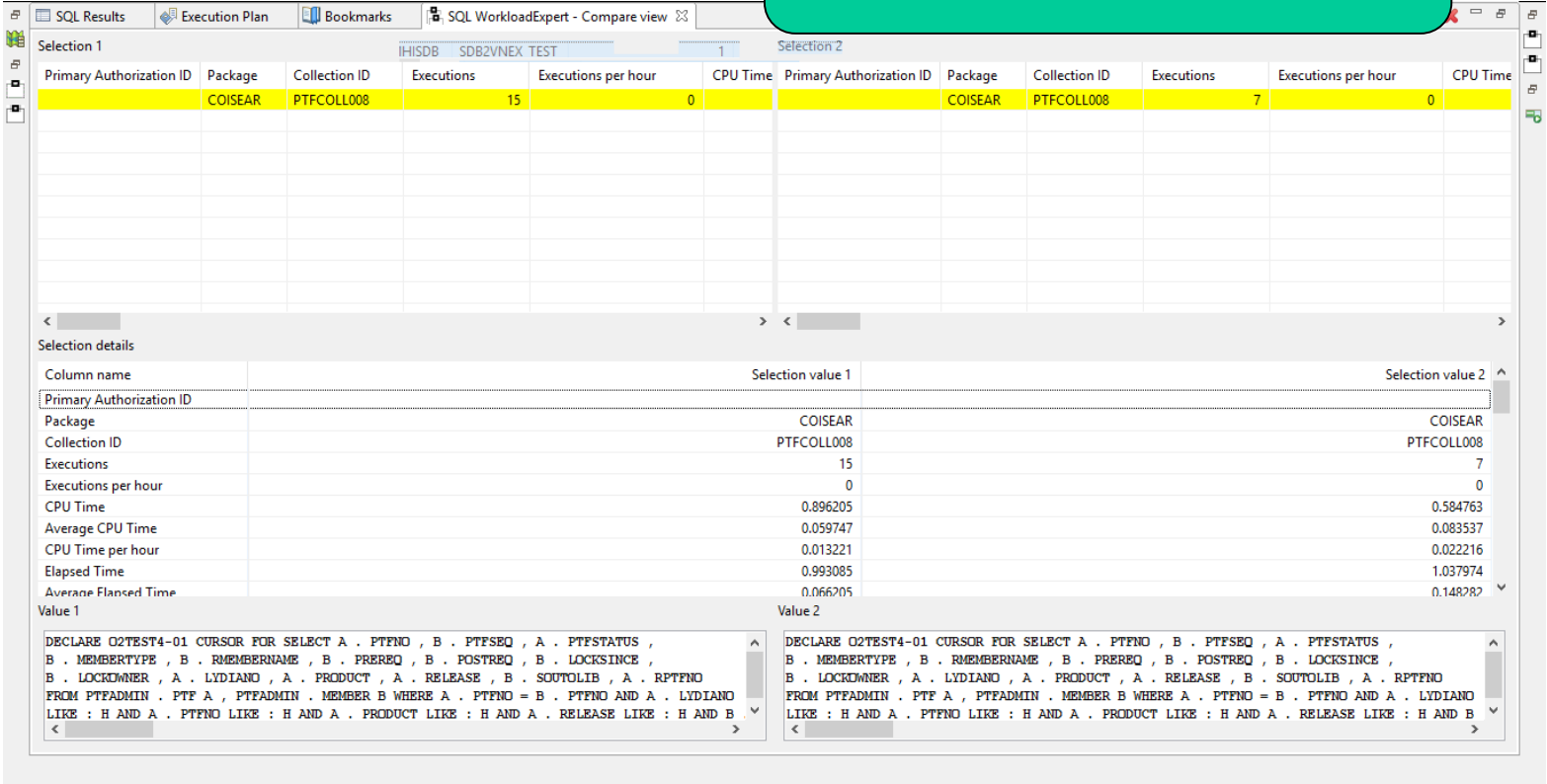
```
1 DECLARE SYSINDEXES_01 CURSOR FOR SELECT RTRIM ( IX . DBNAME ) , RTRIM ( IX . TBcreator ) , RTRIM ( IX . TBNAME ) ,
2 RTRIM ( IX . creator ) , RTRIM ( IX . NAME ) , IX . CLUSTERING , IX . CLUSTERED , CASE WHEN IX . CLUSTERRATIO > 0
3 THEN IX . CLUSTERRATIO WHEN IX . CLUSTERRATIO <= 0 THEN FLOAT ( IX . CLUSTERRATIO )
4 ELSE FLOAT ( IX . CLUSTERRATIO ) / 100 END AS CLUSTERRATIO , IX . FIRSTKEYCARD , IX . FULLKEYCARD , IX . NLEAF ,
5 IX . NLEVELS , IX . UNIQUERULE , IX . COLCOUNT , IX . INDEXTYPE , IX . PIECESIZE , IX . PADDED , IX . AVGKEYLEN ,
6 IX . STATTIME , IX . DATAPEATFACTOR , 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



The screenshot displays the SQL WorkloadExpert - Compare view interface. It compares two selections, Selection 1 and Selection 2, across various metrics. The top section shows a table with columns for Primary Authorization ID, Package, Collection ID, Executions, Executions per hour, and CPU Time. Below this, the 'Selection details' section provides a more granular comparison of metrics for both selections. At the bottom, the SQL statements for each selection are shown.

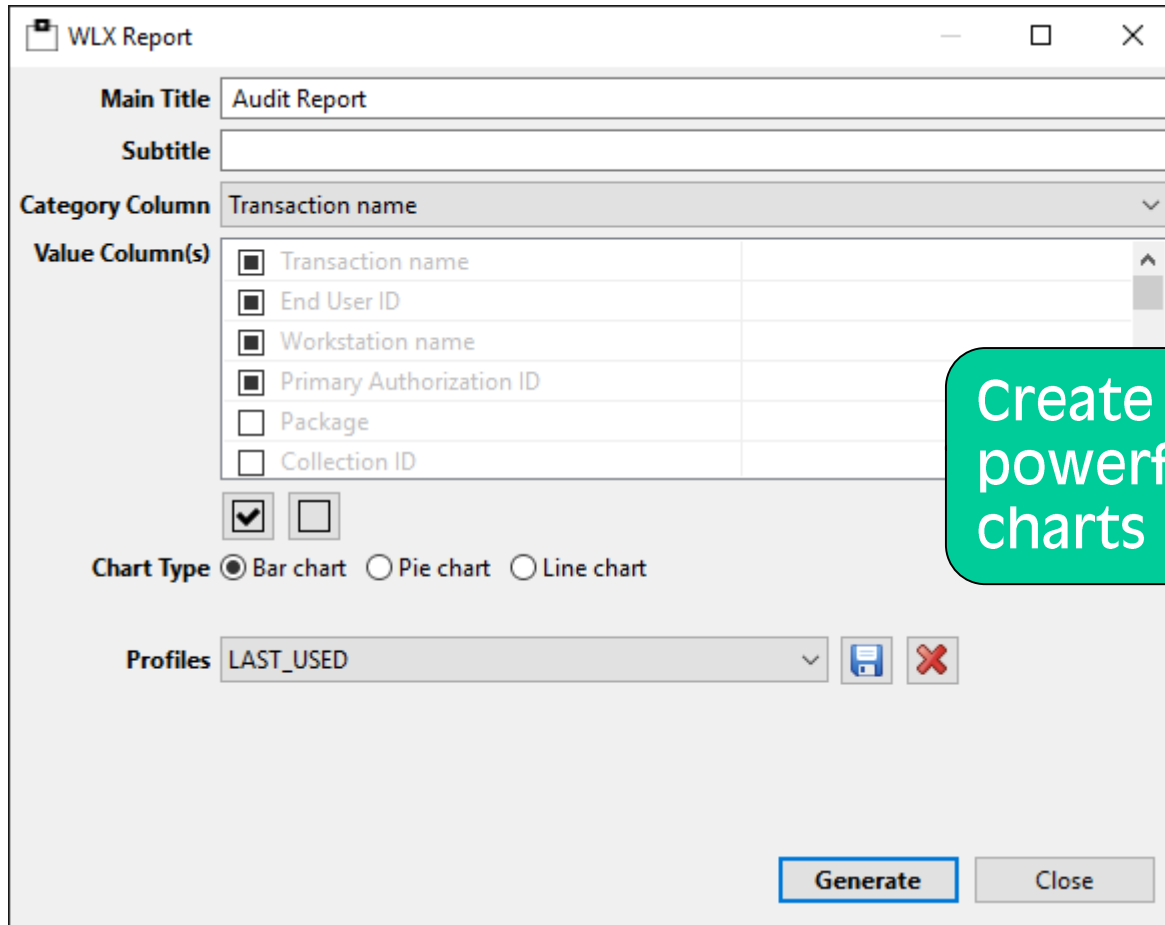
Selection 1	Selection 2
Primary Authorization ID	Primary Authorization ID
Package	Package
Collection ID	Collection ID
Executions	Executions
Executions per hour	Executions per hour
CPU Time	CPU Time

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 Flashed Time	0.066205	0.148282

Value 1
DECLARE Q2TEST4-01 CURSOR FOR SELECT A . PTENO , B . PTSEQ , A . PTSTATUS ,
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 . PTENO = B . PTENO AND A . LYDIANO
LIKE : H AND A . PTENO LIKE : H AND A . PRODUCT LIKE : H AND A . RELEASE LIKE : H AND B

Value 2
DECLARE Q2TEST4-01 CURSOR FOR SELECT A . PTENO , B . PTSEQ , A . PTSTATUS ,
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 . PTENO = B . PTENO AND A . LYDIANO
LIKE : H AND A . PTENO LIKE : H AND A . PRODUCT LIKE : H AND A . RELEASE LIKE : H AND B

The viable way – let Db2 do the magic



The screenshot shows a software window titled "WLX Report". It contains several input fields and a list of columns. The "Main Title" field is set to "Audit Report". The "Category Column" dropdown is set to "Transaction name". The "Value Column(s)" section has a list of columns with checkboxes: "Transaction name" (checked), "End User ID" (checked), "Workstation name" (checked), "Primary Authorization ID" (checked), "Package" (unchecked), and "Collection ID" (unchecked). Below this list are two small checkboxes, the first of which is checked. The "Chart Type" section has three radio buttons: "Bar chart" (selected), "Pie chart", and "Line chart". The "Profiles" dropdown is set to "LAST_USED". At the bottom right, there are "Generate" and "Close" buttons.

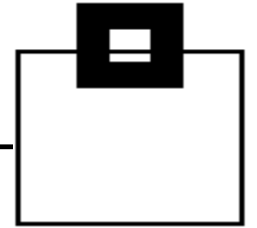
Value Column(s)	Selected
Transaction name	<input checked="" type="checkbox"/>
End User ID	<input checked="" type="checkbox"/>
Workstation name	<input checked="" type="checkbox"/>
Primary Authorization ID	<input checked="" type="checkbox"/>
Package	<input type="checkbox"/>
Collection ID	<input type="checkbox"/>

Create reports using powerful graphical charts

The viable way – let Db2 do the magic

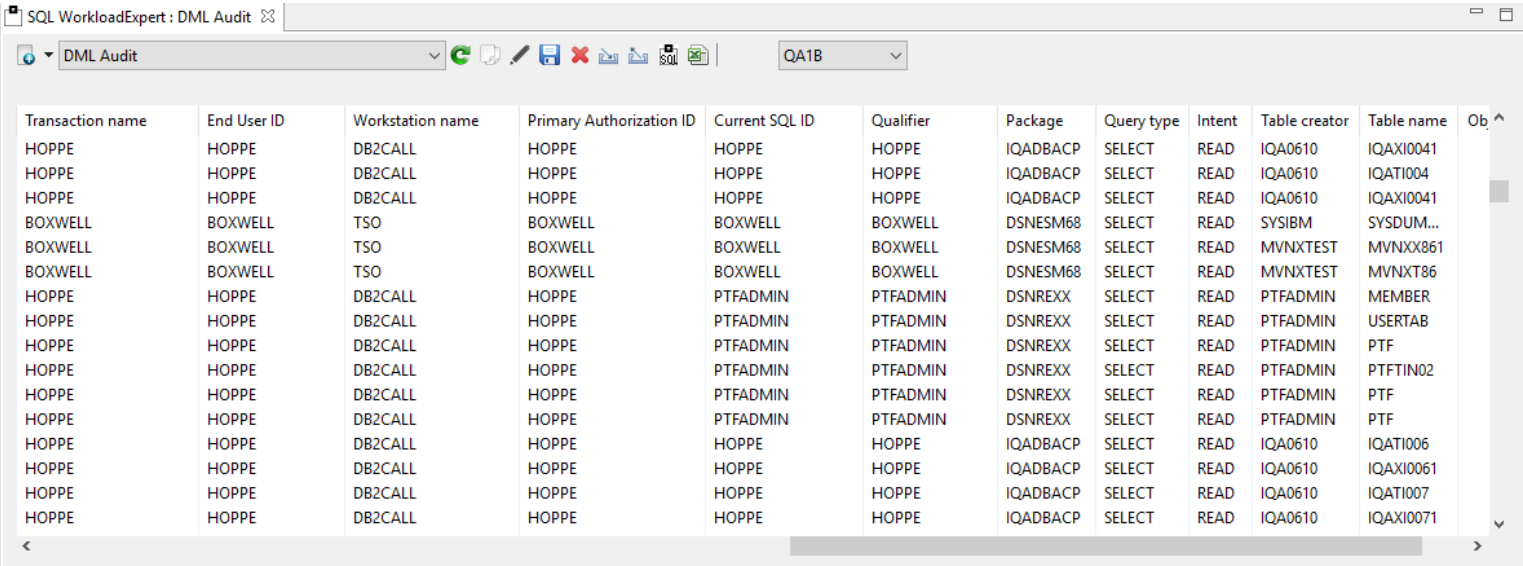
Choose how you'd like
to find out who did
what and when...

- Access to audited tables
- Audit (DML)
- Authorization failures
- Changed audited tables
- CREATE, ALTER, DROP(DDL)
- DBADM data updates
- DBADM object update
- DB2 commands
- End of identify
- End of signon in CICS
- GRANTs and REVOKEs (DCL)
- Object Update Dynamic
- PUBLIC access to tables
- Set current SQLID
- Show Primary Auth Ids
- System DBADM data update
- System DBADM object upd.
- SQL INTENTs
- SYSADM data updates
- SYSADM object updates



The viable way – let Db2 do the magic

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

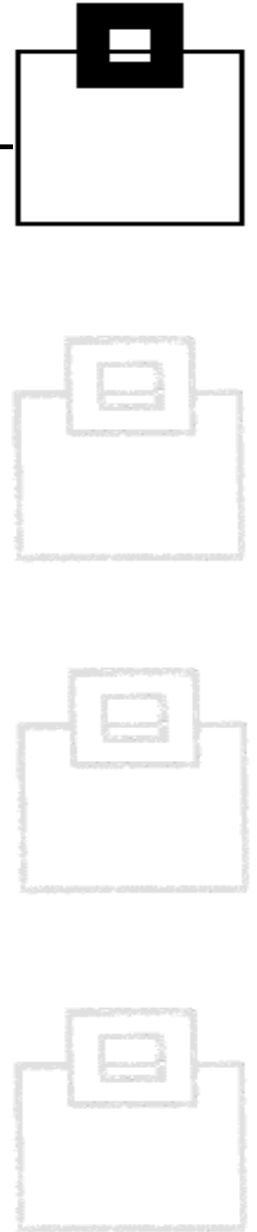
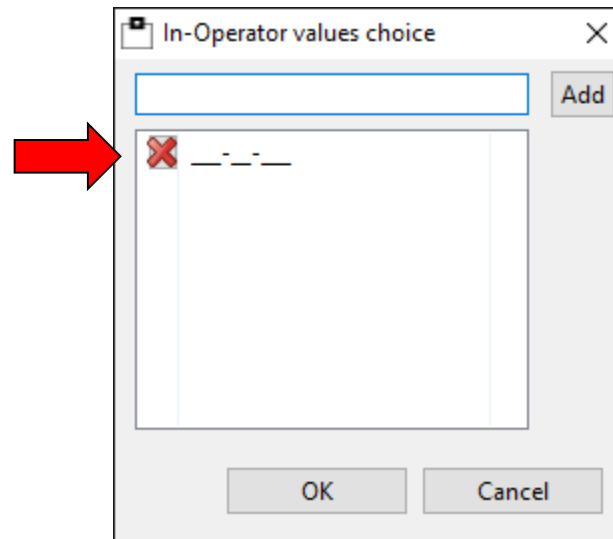


The screenshot shows the 'SQL WorkloadExpert: DML Audit' window. The 'DML Audit' tab is selected, and the filter 'QA1B' is applied. The table below lists various database transactions and their details.

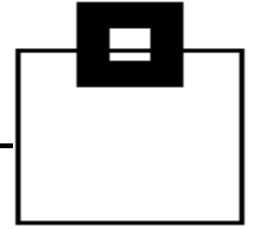
Transaction name	End User ID	Workstation name	Primary Authorization ID	Current SQL ID	Qualifier	Package	Query type	Intent	Table creator	Table name	Ob
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQAXI0041	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQATI004	
HOPPE	HOPPE	DB2CALL	HOPPE	HOPPE	HOPPE	IQADBACP	SELECT	READ	IQA0610	IQAXI0041	
BOXWELL	BOXWELL	TSO	BOXWELL	BOXWELL	BOXWELL	DSNESM68	SELECT	READ	SYSIBM	SYSDDUM...	
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	

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

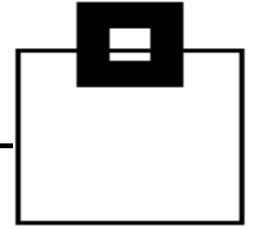


Requirements:

- 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:

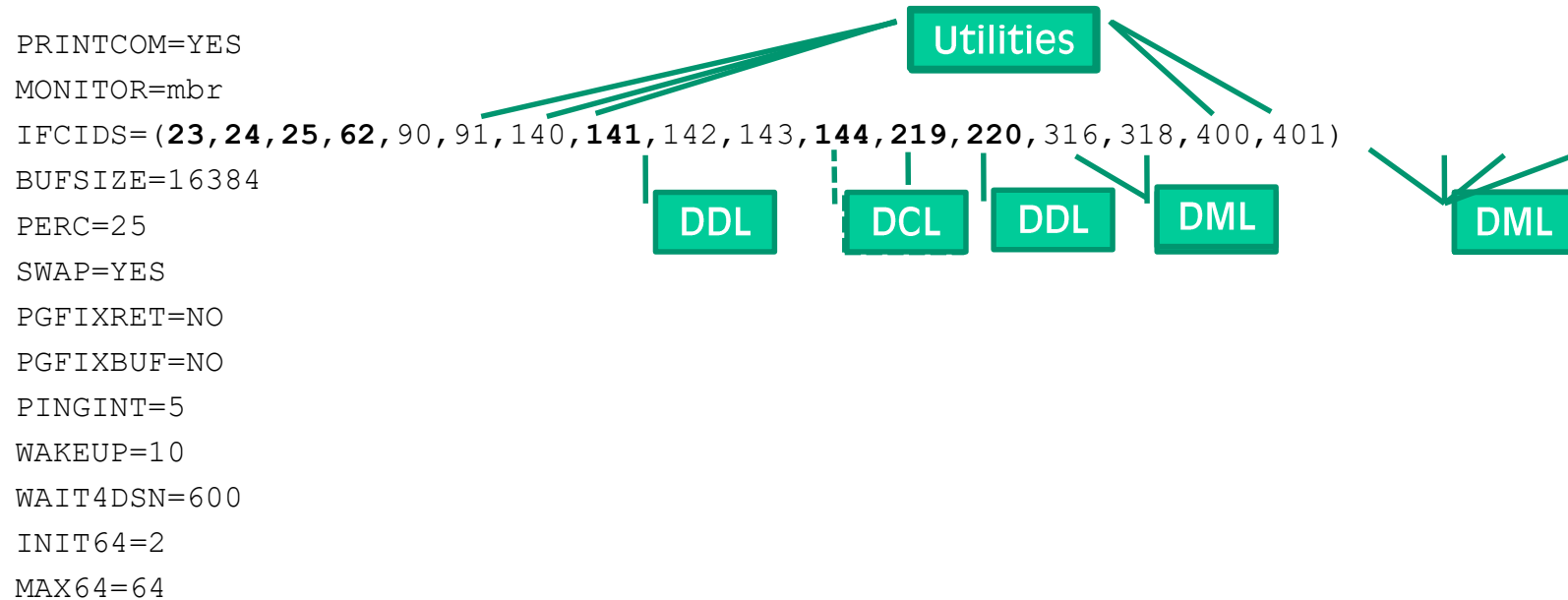
- WLX STC HA implementation
 - STC at the LPAR/Db2 DS member level to assure continuous capturing even during LPAR restart
- Workload processing once a day to generate daily audit reports
 - Automated via job scheduler
 - All Db2 systems merged into a common report
 - Objects and activity (DML, DDL, 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*



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=DSSs)

90/91 Commands and their completion status

140 Authorization failures

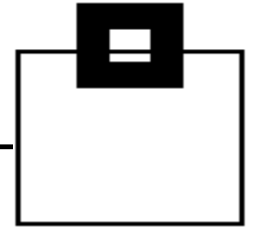
141 Authorization changes

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



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

<

>

© 2018 SEGUS & SOFTWARE ENGINEERING GMBH

49

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)

Projection

- Label
- WLX Key
- WLX DB2
- IFCID Tim
- IFCID No
- Audit ob
- Privilege
- DBID
- Access ty
- OBID
- Authoriz
- Multi-Le
- Reason a
- SQL Cod
- Row con
- Audit ob
- Grant cre
- SQL text

OK Cancel

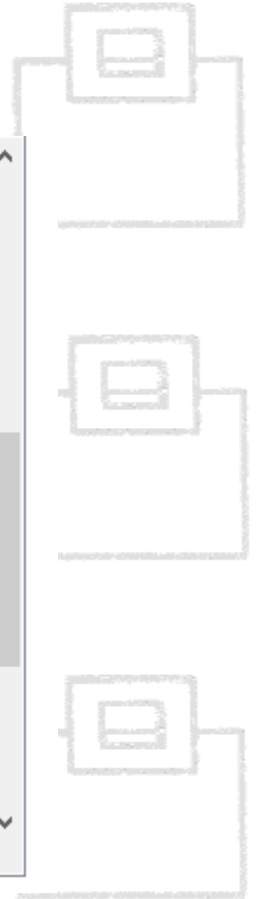
GRANTS and REVOKEs (DCL)

Description

Projection Selection **Sorting**

Label	Description
WLX Key	The WLX Key
WLX DB2 SSID	WLX DB2 SSID
IFCID Timestamp	IFCID Timestamp
IFCID No.	IFCID No.
Audit object type	Audit object type
Privilege check	Privilege check
DBID	DBID
Access type	Access type
OBID	OBID
Authorization type	Authorization type
Multi-Level Security	Multi-Level Security
Reason access	Reason access
SQL Code	SQL Code
Row control	Row control
Audit object type	Audit object type
Grant creator	Grant creator
SQL text length	SQL text length

Cancel



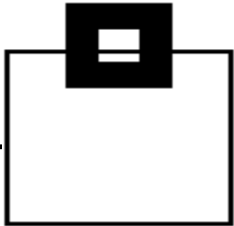
Customer results from the banking industry

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:

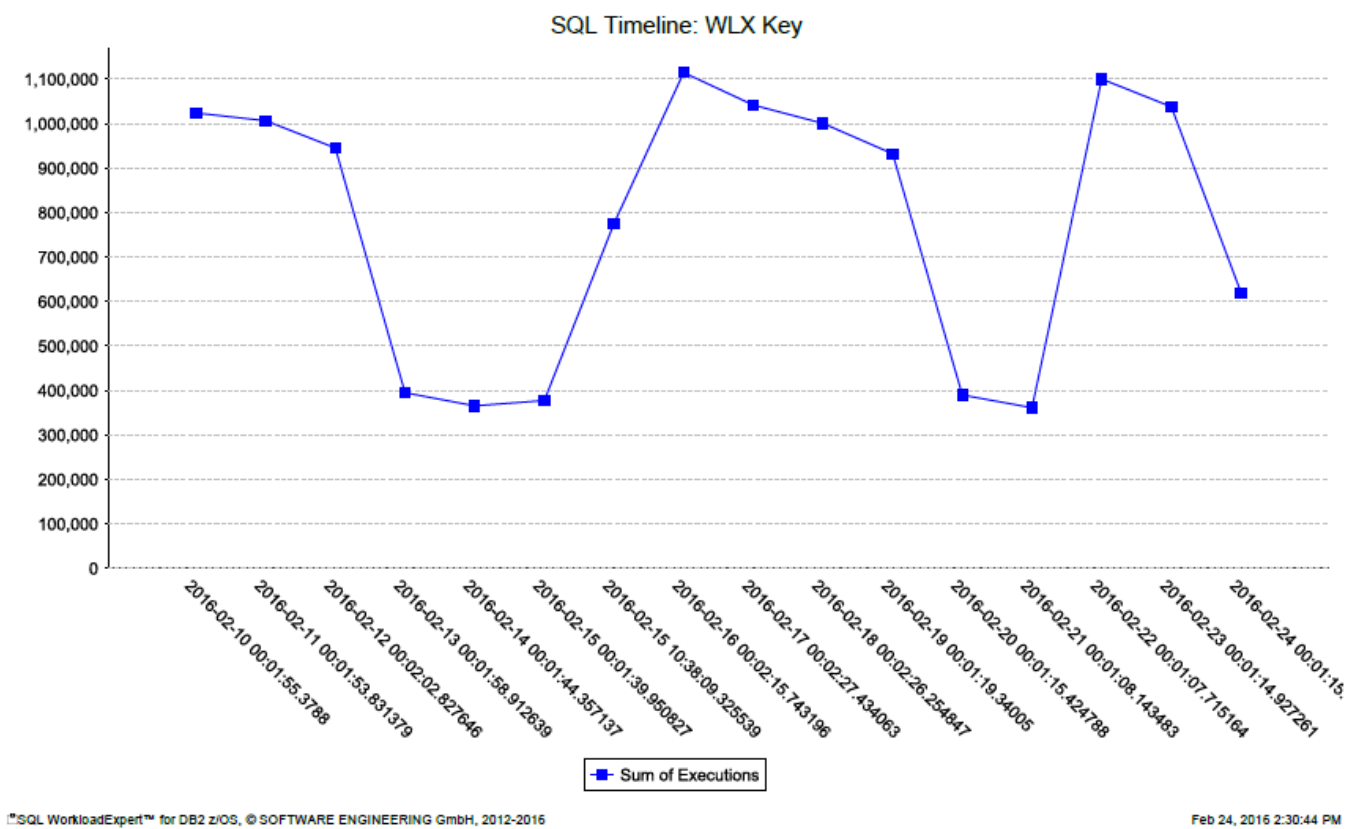
Label	Description	
Statement Timestamp	The timestamp that this statement was written into the SSC c	
WLX DB2 SSID	The WorkloadExpert Group or Subsystem DB2 name for this v	
Primary Authorization ID	The Primary Authorization ID used to identify the application	
Package	The package used by the statement	
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 ur	User provided id string
First referred Table Qualifier	The first table Qualifier in the statem	Authorization ID
First referred Table Name	The first table name in the statement	Job name or logon ID
Statement text	The complete text for the SQL statem	Connection name
Query no.	Query number	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:

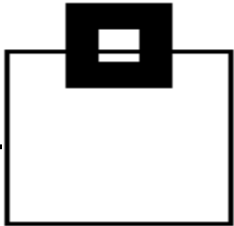
SQL WorkloadExpert : Database activity

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...

>> > < <<

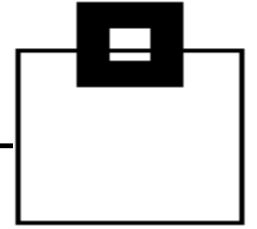
Label	Operator	Value	Description
WLX Key	=	newest	The WorkloadExpert k...
Statement Times...	=	2016-03-07-13.57.24.772000	The timestamp that th...
WLX DB2 SSID ...	=	DB2P	The WorkloadExpert G...
Primary Authoriz...	NOT LIKE	SA%	The Primary Authoriza...
Table name	IN	%CUST%, %PAYMNT%, %TRSACT%	Table name
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 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



Runtime & Costs:

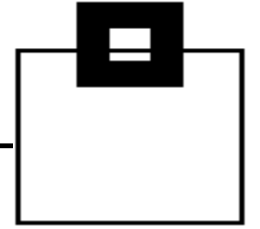
- Capture STC < 15sec. CPU/month (3-way DS)
- 150k stmt. < 3min processing

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



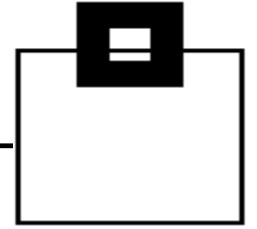
SQL WorkloadExpert for Db2 z/OS




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



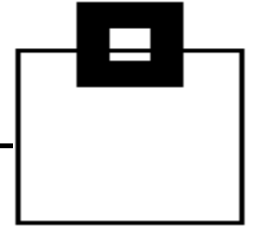


Application Development:

- 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
- Find unused (orphaned) SQL



WLX typical use cases

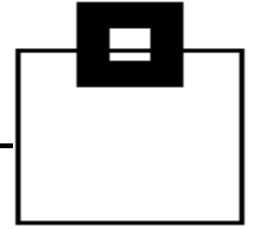


Workload/Performance management:

- 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.)



Questions???

Many thanks for your attention and now....

