Compliance with Compliments! Viable DB2 z/OS Workload Tracking

Ulf Heinrich
SOFTWARE ENGINEERING

Session Code: A09
On November 16, 2016 | at 08:30 | Platform: DB2 for z/OS

AGENDA

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

Security and data breach protection

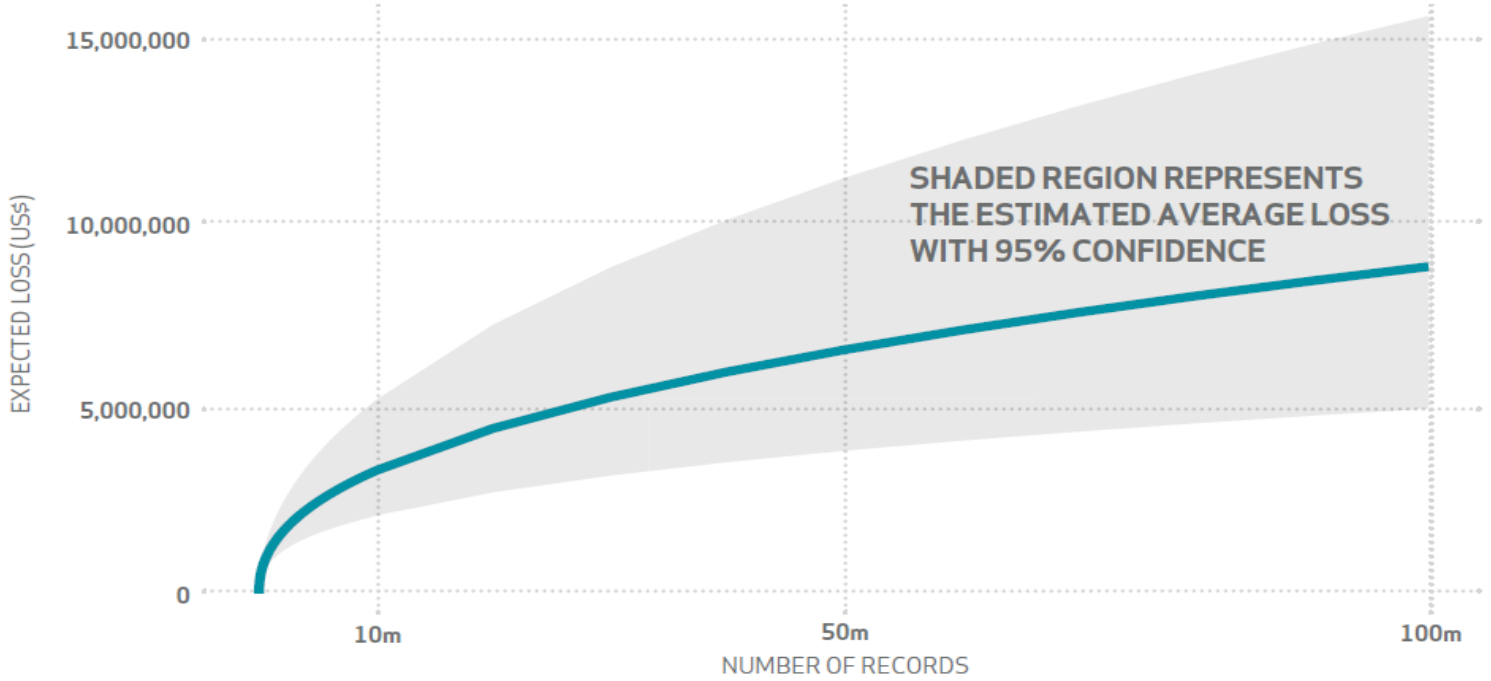
Source: 2015 Gemalto Breach Level Index http://bit.ly/1PUCspY

Security and data breach protection

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

The cost of a data breach

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

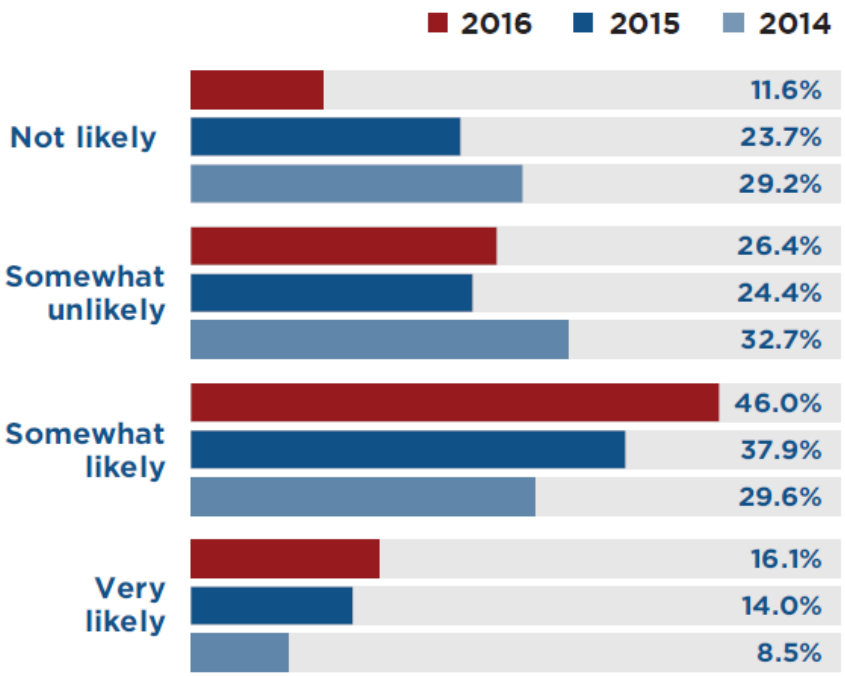


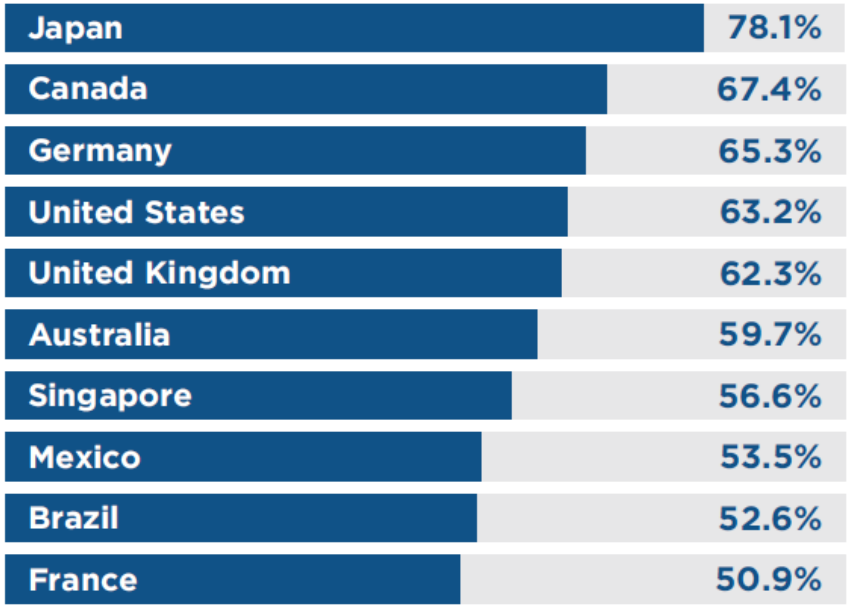
Source: 2015 Verizon Data Breach Investigation Report

Number of cyber attacks likely to grow this year

Future Likelihood of Successful Cyberattacks

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





Source: 2016 Cyberthreat Defense Report, CyberEdge Group

Audit – do you need it, do you care?!

Attackers use…

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

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

Audit – do you need it, do you care?!

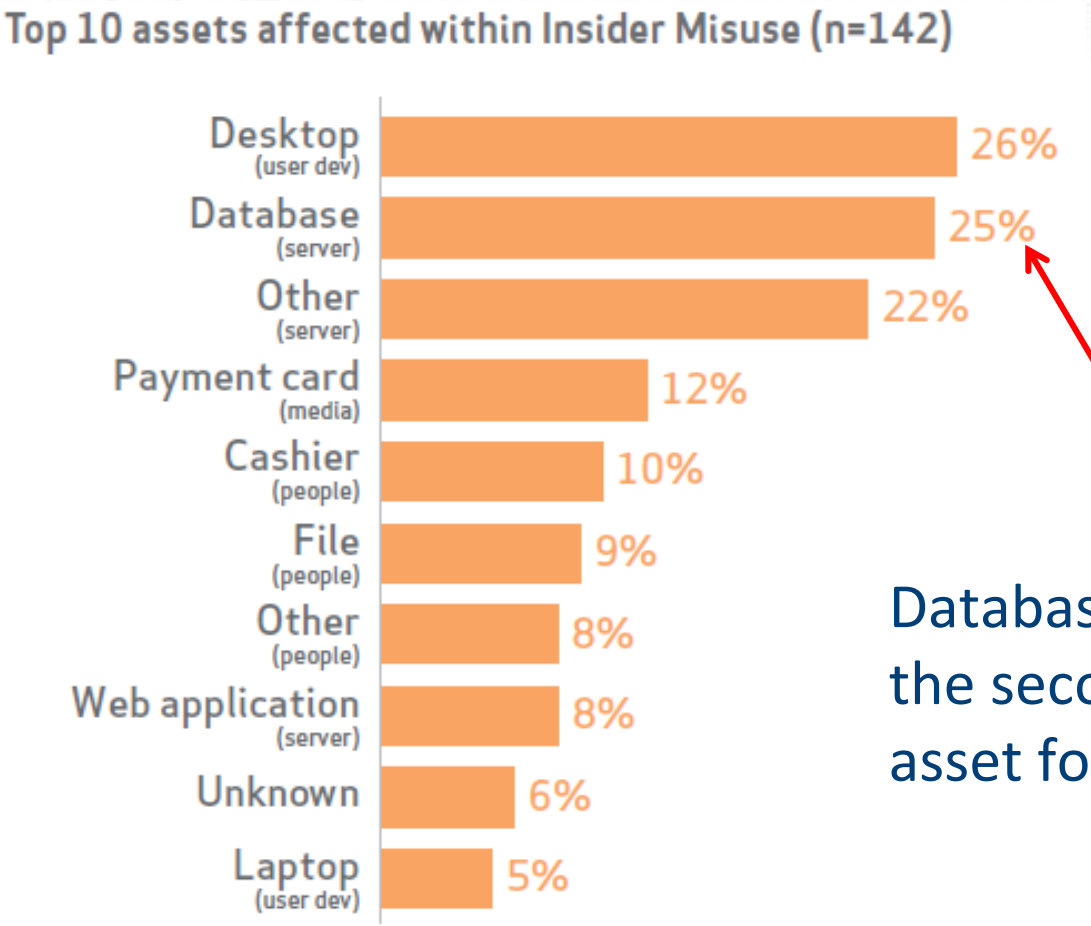
Enterprise database servers are a primary target of many security breaches! Why?

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

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

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

Greatest inside misuse



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

Source: 2014 Verizon Data Breach Investigation Report

Audit – do you need it, do you care?!

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

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

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

President, Mittal Technologies Inc.

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

Audit needs and musts

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

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

Audit needs and musts

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

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

Audit needs and musts

Focusing on the major areas of concern – the database server:

Audit Logging Requirements	Cobit (SOX) FIEL	PCI DSS	HIPAA	CMS ARS	GLBA	ISO 17799 27001	NERC	NIST 800-53 FISMA
SELECTs against sensitive data		X	X	X	X	X		X
Insert, Update, Delete	X			X		X		
Access violations	X	X	X	X	X	X	X	X
Schema Changes	X	X	X		X	X	X	X
Grants/Revokes	X	X	X	X	X	X	X	X

Audit needs and musts

- It is important to match your data collection requirements to the regulations that apply to your business
- You may need more to satisfy business requirements
- *Breach patterns do change, so you probably won't know today what you could need tomorrow*
- Make sure have a way to collect:
  - SELECTs (against sensitive data)
  - Modifications (INS/UPD/DEL)
  - DDL
  - DCL
  - Utilities (online + offline)
  - Commands
  - Assignment, or modification of a user ID/authorization – especially privileged users

Audit needs and musts

- Be careful what happens outside of a table:
  - Consider clones
  - Consider backups
  - Consider extended statistics in catalog tables, like SYSCOLDIST + SYSKEYTGTDIST
  - Consider utility output (REORG, RUNSTATS)
  - Consider UNLOADs
  - Consider Replication
  - Consider access to the underlying VSAM data sets
- Also consider your INSTALL SYSADM/SYSOPR

  → Separation of duties

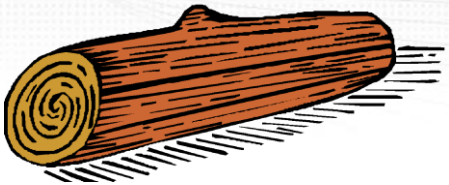
Audit needs and musts

- Most Home-Grown Solutions are based on the DB2 Audit Trace
  - Class 1, 2, 7, 8 have very little overhead
    - Access violations
    - GRANTs/REVOKEs
    - Assignment, or modification of a user ID/authorization
    - Start of a DB2 online utility
  - Class 3 has very little overhead
    - DDL (only for TB having the AUDIT ALL attribute)
  - Class 4, 5 up to 15% - 20% overhead
    - 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!

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

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

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)

Add the correlation headers to get detailed authentication data

The viable way – let DB2 do the magic

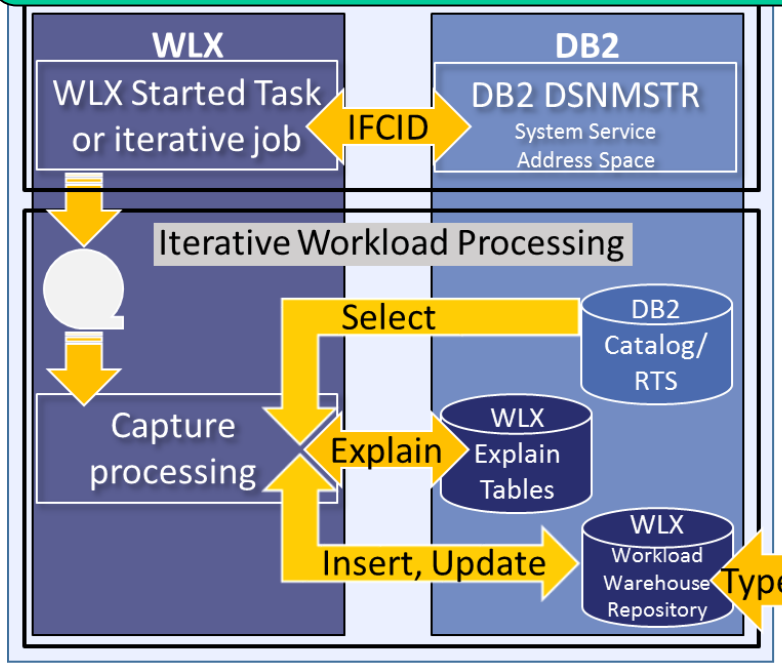
- All IFCIDs listed have a much smaller footprint than AUDIT CHANGES/ALL
- This is integrated, reliable DB2 technology
- OPX is the right target for efficient capturing
- Store it in a repository and protect it using proven technology (e.g. RACF, ACF2, Top Secret)
- Using DB2 compression reduces storage requirements exploiting proven, integrated technology

→ No new vulnerabilities:

  - Black Box appliance
  - Massive sensitive data transmissions over the network

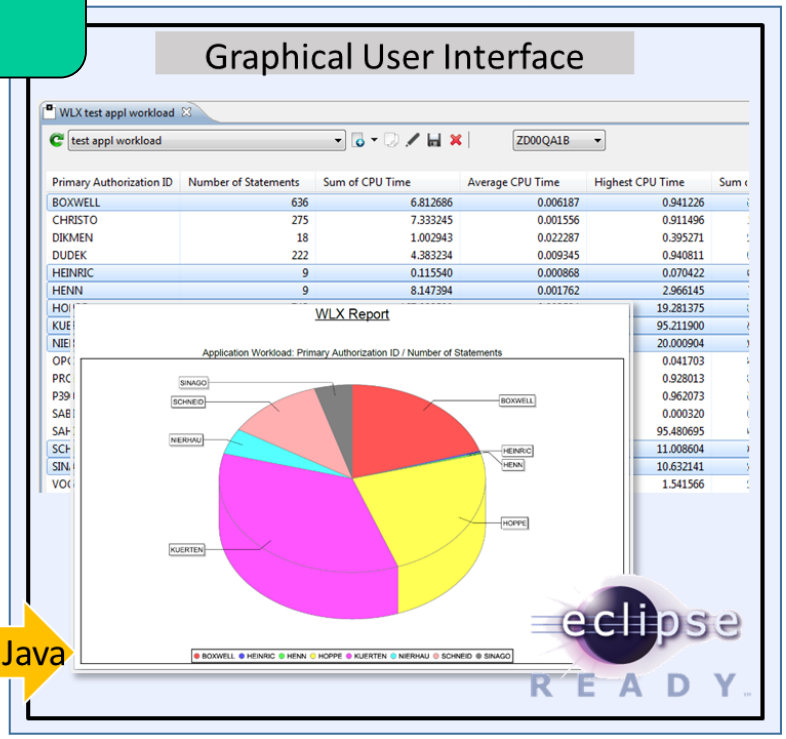
The viable way – let DB2 do the magic

Efficient data collector for your desired scope of Audit



Type 4 Java

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

…and:

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

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

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

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:

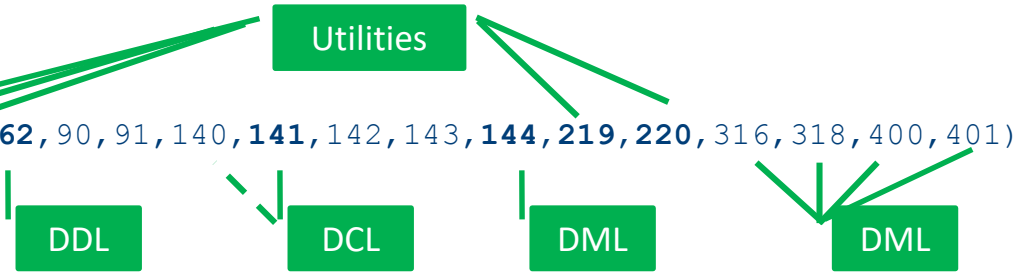
- WLX STC HA implementation
  - STC at the LPAR/DB2 DS member level to assure continuous capturing even during LPAR restart
- Workload processing once a day to generate daily audit reports
  - Automated via job scheduler
  - All DB2 systems merged into a common report
  - Objects and activity (DML, DDL,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



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

Appendix

- DB2 APARs to check for:
  - PI30040 DB2 11 UI26407 – Forward fit SQLCODE 420
  - PI33409 DB2 10 UI26352 – REVOKE MQT
  - PI35766 DB2 11 UI31693 – Elapsed time incorrect for parallel queries
  - PI46967 DB2 10 UI31646 DB2 11 UI31647 – Invalid IFCID 401 after IDAA APAR PI23083/PI30005
  - PI48100 DB2 10 UI32273 – Abend S0C4 in Pre V8 packages

Ulf Heinrich

SOFTWARE ENGINEERING

u.heinrich@seg.de

Please fill out your session evaluation before leaving!

Session A09

Compliance with Compliments!
Viable DB2 z/OS Workload Tracking

Photo by Steve from Austin, TX, USA