Database Auditing
Who did what to which data when and how?
Authors

This presentation was prepared by:

Craig S. Mullins
Corporate Technologist

NEON Enterprise Software, Inc.
14100 Southwest Freeway
Sugar Land, TX 77479
Tel: 888.338.6366
Fax: 281.207.4973
E-mail: craig.mullins@neonesoft.com

This document is protected under the copyright laws of the United States and other countries as an unpublished work. This document contains information that is proprietary and confidential to NEON Enterprise Software, which shall not be disclosed outside or duplicated, used, or disclosed in whole or in part for any purpose other than to evaluate NEON Enterprise Software products. Any use or disclosure in whole or in part of this information without the express written permission of NEON Enterprise Software is prohibited. © 2006 NEON Enterprise Software (Unpublished). All rights reserved.
Agenda

Emergence of Enterprise Data Protection
Regulatory Compliance and Auditing
Database Auditing Capabilities
# DBA versus Data Management

<table>
<thead>
<tr>
<th>Database Administration</th>
<th>Data Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Security</td>
<td>Data Protection</td>
</tr>
<tr>
<td>Backup/Recovery</td>
<td>Data Privacy Protection</td>
</tr>
<tr>
<td>Disaster Recovery</td>
<td>Data Quality Improvement</td>
</tr>
<tr>
<td>Reorganization</td>
<td>Data Quality Monitoring</td>
</tr>
<tr>
<td>Performance Monitoring</td>
<td>Database Archiving</td>
</tr>
<tr>
<td>Application Call Level Tuning</td>
<td>Data Extraction</td>
</tr>
<tr>
<td>Data Structure Tuning</td>
<td>Metadata Management</td>
</tr>
<tr>
<td>Capacity Planning</td>
<td></td>
</tr>
</tbody>
</table>

Managing the database environment

Managing the content and uses of data
Top Data Protection Challenges

Where is my sensitive data located & who is using it?

How can I enforce access & change control policies for critical databases?

How do I simplify & automate compliance?
Security By the Numbers (per TechTarget)

- 54% of companies say security budgets are growing
- 69% of security pros said their job will be more strategic in 2008
- 75% of security pros said their job will involve more compliance work
- 62% of security pros said their company’s top IT person will care more about security in 2008
- 52% said their top priority will have something to do with network/security integration
- 80% said they would “prefer to purchase best of breed products and integrate them into my network so I have the strongest security possible for my budget.”
67% of 1,100 security pros said securing databases was an important or very important challenge for 2008

- #1 in a list of 13 data protection initiatives

45% of security pros will spend more time on data protection in 2008 vs. 2007.

- #3 on a list of 19 security activities

41% will spend more time on database security specifically
According to the Privacy Rights Clearinghouse, the total number of records containing sensitive personal information involved in security breaches in the U.S. since January 2005 is:

218,198,364

As of February 5, 2008

http://www.privacyrights.org/ar/ChronDataBreaches.htm
How Prevalent is this Problem?

68% of companies are losing sensitive data or having it stolen out from under them six times a year.

An additional 20% are losing sensitive data 22 times or more per year.

Sources: eWeek, March 3, 2007
IT Policy Compliance Group

Regulations Impacting Security
Governance vs. Privacy

Governance
1. Basel II
2. Sarbanes Oxley
3. OFAC
4. Turnbull Report

Privacy
1. EU DPD
2. AU/NZ NPP
3. SB 1386/AB 1950
4. GLBA
5. HIPAA
6. PCI
7. FCRA -- “Red Flag”

Protect and control the process

Protect the data
FCRA: “Red Flag” Rules

All federally regulated financial institutions must be in full compliance by Nov. 1, 2008, with the so-called "Red Flag" provisions of the Fair and Accurate Credit Transactions Act of 2003 (FACTA).

- Part of FCRA - the Fair Credit Reporting Act.

Requires that financial institutions and creditors develop and deploy an Identity Theft Prevention Program for combating ID theft on new and existing accounts.

Each institution must develop a program that will:

- Identify relevant patterns, practices, and specific forms of activity that are "red flags" signaling possible ID theft.
- Include a mechanism to detect red flags identified by the program.
- Quickly respond to detected red flags in a way to both prevent and mitigate ID theft.
- Be updated regularly to reflect changes in real world risks from ID theft.
## Top Regulations Impacting DB Security

<table>
<thead>
<tr>
<th>Audit Requirements</th>
<th>CobiT (SOX)</th>
<th>PCI DSS</th>
<th>HIPAA</th>
<th>CMS ARS</th>
<th>GLBA</th>
<th>ISO 17799 (Basel II)</th>
<th>NERC</th>
<th>NIST 800-53 (FISMA)</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Access to Sensitive Data (Successful/Failed SELECTs)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>3. Data Changes (DML) (Insert, Update, Delete)</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>4. Security Exceptions (Failed logins, SQL errors, etc.)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>5. Accounts, Roles &amp; Permissions (DCL) (GRANT, REVOKE)</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

**DDL** = *Data Definition Language* (aka schema changes)

**DML** = *Data Manipulation Language* (data value changes)

**DCL** = *Data Control Language*
Enterprise Data Protection

Cost associated with Non-Compliance & Breach of Data

Rapidly address auditors’ requirements

Simplify & automate compliance process

Protect enterprise data

Fines

Increased Staff

Loss/Out of Business

Tactical Need

Strategic Need

INTELLIGENCE. INNOVATION. INTEGRITY
Regulatory Compliance and...

**Impact:** upper-level management is keenly aware of the need to comply, if not all of the details that involves.

**Prosecution:** prosecution can result in huge fines and even imprisonment.

**Cost:** the cost of complete compliance can be significant.

**Durability:** although there have been discussions about scaling back some laws (e.g. SOX), increasing regulations and therefore increasing time, effort, and capital will be spent on compliance.

- *That is, the issue will not just disappear if you ignore it long enough!*
Why Audit & Secure Databases

Cost of Breach
- Identity theft, credit cards etc.

Regulatory Compliance
- Database monitoring is key requirement

Database Leak Prevention
- Sensitive data needs protection

Open Accessability
- Web 2.0 applications dissolving traditional perimeter controls
Data and Database Protection, Security, and Auditing Trends

- Data Protection Issues:
  - Volume of data
  - Increased accessibility of data
  - Regulatory compliance
  - Increased number and type of threats

Diagram:
- X-axis: Accessibility
- Y-axis: Amount of Data
- Line: Compliance Protection

INTELLIGENCE. INNOVATION. INTEGRITY
Database Auditing

In a world replete with regulations and threats, organizations have to go well beyond securing their data. Essentially, they have to perpetually monitor their data in order to know who or what did exactly what, when and how - to all their data.


HIPAA, for example, requires patients to be informed any time someone has even looked at their data.
What is Database Auditing?

There are many names used for basically the same thing.

I’ll call it database auditing, but you may also know it as:

- Data Access Auditing
- Data Monitoring
- Data Activity Monitoring (DAM)
Database Auditing definition

*Database Auditing:*
The process of monitoring access to and modification of selected database objects and resources within operational databases and retaining a detailed record of the access where said record can be used to proactively trigger actions and can be retrieved and analyzed as needed.
Key Stakeholder Requirements

SECURITY OPERATIONS
- Real-time policies
- Secure audit trail
- Data mining & forensics

COMPLIANCE AUDIT
- Separation of duties
- Best practices reports
- Automated controls

APPLICATION & DATABASE
- Minimal impact
- Change management
- Performance optimization

100% Visibility & Unified View
Database Auditing

Types of Database Auditing

Database Auditing Requirements

Database Auditing Challenges

Native DBMS Database Auditing?

Reporting and Analyzing the Audit Data
Types of Database Auditing

Authorization Auditing
- Who can do what.

Access Auditing
- Who did do what.
- Modifications: INSERT, UPDATE, DELETE
- Reads: SELECT
- Other: DDL (CREATE / DROP/ALTER), DCL (GRANT / REVOKE), Utilities, SQL errors, failed logins, etc.

Replication Auditing
- Who copied which data where.
Database Auditing Approaches

What methods are available?

- Audit within the DBMS (traces)
  - Must start performance trace
    - Overhead as trace records are written by the DBMS
  - DDL changes required to traced tables?

- Audit from the database transaction log files
  - Modifications are on the log anyway so...

- Audit over the network
  - Capture SQL requests as they are sent over the network
  - What about non-network requests? (e.g. CICS w/DB2)

- Audit directly against the DBMS server (*software tap*)
Native DBMS Audit

The native DBMS audit capability may not be optimal:

- Separation of duties - logging typically is turned on and off by DBAs, who need to be audited
- Overhead - many require traces to be started, which can consume precious resources (as much as 10% overhead?)
- Comprehensive capture - may not capture everything that needs to be captured for compliance
DB2’s Native Audit Trace

The DB2 Audit Trace can record:

- Changes in authorization IDs
- Changes to the structure of data (such as dropping a table)
- Changes to data values (such as updating or inserting data)
- Access attempts by unauthorized IDs
- Results of GRANT statements and REVOKE statements
- Mapping of Kerberos security tickets to IDs
- Other activities that are of interest to auditors

CREATE TABLE . . . **AUDIT ALL** . . .

-START TRACE (AUDIT) CLASS (4,6) DEST (GTF) LOCATION (*)

FYI: Audit Trace Classes are listed on page 287, IBM DB2 Admin Guide
Limitations of DB2 Audit

The DB2 audit trace does not record everything. Consider the following limitations:

- The trace does not record old data after it is changed (the database transaction log records old data).
- If an agent or transaction accesses a table more than once in a single unit of recovery, the audit trace records only the first access.
- Although plan and authid can be used to limit audited data, wildcarding is not supported, so starting appropriate traces is prohibitive.
- Must start audit traces that have to be set up to go to an appropriate trace destination: requires system programmer assistance.
- The audit trace does not record accesses if you do not start the audit trace for the appropriate class of events.
- The audit trace does not audit some utilities. The trace audits the first access of a table with the LOAD utility, but it does not audit access by the COPY, RECOVER, and REPAIR utilities. The audit trace does not audit access by stand-alone utilities, such as DSN1CHKR and DSN1PRNT.
- Limitations exist as to what tables can be audited: you cannot audit access to auxiliary tables or to the system catalog tables.
What About Using the Log?

Database transaction log(s) capture ALL* changes made to data.

*Well, maybe not all changes, all the time.
Issues With Database Log Auditing & Analysis

- Log format is proprietary
- Volume can be an issue
- Easy access to online and archive logs?
  - But how long do you keep your archive logs?
- Dual usage of data could cause problems?
  - Recovery and protection
  - Audit
- Tracks database modifications, but what about reads?
  - Transaction logs do not record information about SELECT.
- And what about non-logged operations?
  - LOAD LOG NO, REORG LOG NO
  - Non-logged table spaces (new feature in DB2 9 for z/OS)
- Cannot invoke real-time actions using log-based auditing
Database auditing via network sniffing captures SQL requests as they go across the network.

- But not all requests go across the wire
  - Mainframe applications
  - DBA access directly on the server

- Be careful, many third-party database auditing solutions use this approach
A Better Approach

- Audit database calls at the server
  - Capture *all* SQL requests at the server
  - All SQL access is audited, not just network calls
  - Retain all pertinent audited information
    - No reliance on the DBMS
  - No need to keep the active/archive log files
  - No need to start a DBMS trace
  - No need to modify the database schema
  - Requires purchasing additional ISV software
<table>
<thead>
<tr>
<th>Enterprise DBMS Platforms</th>
<th>Local Access</th>
<th>IP Network Access</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Distributed Environments</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>Bequeath/IPC</td>
<td>✓</td>
</tr>
<tr>
<td>DB2</td>
<td>Shared Memory</td>
<td>✓</td>
</tr>
<tr>
<td>SQL Server</td>
<td>Named Pipes/Shared Memory</td>
<td>✓</td>
</tr>
<tr>
<td>Sybase</td>
<td>TLI</td>
<td>✓</td>
</tr>
<tr>
<td>Informix</td>
<td>Shared Memory/TLI</td>
<td>✓</td>
</tr>
<tr>
<td><strong>Mainframe Environments</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DB2, IMS</td>
<td>CICS, MQ, IMS/TM, TSO, RRSAF, etc.</td>
<td>DB2 Connect/JDBC</td>
</tr>
</tbody>
</table>

Visibility Across all DB Activities, Platforms, and Access Methods
Server-Based Database Auditing Requirements

Surveillance Mechanism

- Selective - must be rules-based to enable the capture of audit details only on the specific data that requires auditing.

- Comprehensive - must be able to capture the complete scenario of auditable information.

- Non-invasive - must be able to audit access to data without incurring expensive performance degradation.
Selective

Rules-based Policies

- Database, Table
  - Identify referentially related tables
- Users
- Access Type
  - ALLACCESS
  - READ
  - WRITE
  - DELETE
  - CONNECT
  - DISCONNECT
- Success / Failure

Database, Table — Identify referentially related tables

Users

Access Type
- ALLACCESS
- READ
- WRITE
- DELETE
- CONNECT
- DISCONNECT

Success / Failure
Comprehensive

What Must be Captured?

- Collect data from a variety of environments
  - Any Supported Connection
  - Web, App Server, CICS, IMS TM, Batch, etc.
  - As well as multiple data access/update types
    - INSERT, UPDATE, DELETE
    - SELECT - capture information about queries
    - Database Commands, DDL, DCL
    - Database Utilities: REORG, RUNSTATS, COPY, RECOVER, etc.
What Must be Captured?

Environmental Data
- DBMS Related Information
- DBMS Data Object Descriptions

DBMS Specific Data
- System Information
- User Information
- Information dependent upon DBMS
  - For example: IMS TM/DB Transaction Data Collected
  - Or, for DB2: DBRM Information
Data Captured?

Modification
- Before and After Image of Data
  - May require access to transaction logs

Access
- Specifics of request (with host variables)
- Image of all data accessed?
- Number of rows accessed?
Database Auditing needs to be implementable with as little interference to the production environment as possible:

- Should not require modifications to the database schema
- Should not require application changes
- Should be performance-sensitive
  - That is, you can’t “dim the lights” when you start auditing database accesses
Additional Issues

Audit Trails in Tables

DBA Auditing

Non-standard Data Access

Discarding Audit Data

Proactive Database Security?
Audit Trails in Tables

Sometimes people add “audit columns” to tables, such as LAST_MODIFIED_DATE

Auditors don’t like this; it is a problem because:

- Audit trails should be kept outside of the database (because if you delete the row you lose the audit data)
- Can you guarantee that LAST_MODIFIED_DATE is accurate?
  - Couldn’t someone have set it by accident (or nefariously)?
DBA Auditing

One of the biggest needs for database auditing is privileged user (ie. DBA) auditing?

In other words, who watches the watchers?

Super users (SYSADM, DBADM)

- Can do anything to any data
- Database auditing can be used to verify the integrity and accuracy of the DBA group
Non-Standard Access?

File-level snooping as opposed to going through the DBMS interface

System-level zapping (IMS pointers)

Copy, tweak, rename?
Long-Term Retention and Discard

- **Why:**
  - Need to be able to find who accessed data long after the database logs would be recycled
  - But there could be a legal exposure for data kept too long

- **Implications:**
  - Data must be kept long enough to be useful, but not beyond a specific retention period
  - Must be removed with no exposure to forensic software

- **How:**
  - Long-term storage mechanism
  - Policy based discard
  - Tightly controlled and audited
  - True “zero out” capability
Audit Analysis

Access and analyze the audit details to produce multiple useful reports on database activities:

- Who did what to which piece of data when
- Pattern analysis and trending
Example: Any Changed Data Structures?

DDL

<table>
<thead>
<tr>
<th>Timestamp</th>
<th>DB User Name</th>
<th>Source Program</th>
<th>Full Sql</th>
</tr>
</thead>
<tbody>
<tr>
<td>2007-01-22</td>
<td>SCOTT</td>
<td>C:\ORACLE\PRODUCT10.2.0\DB_1</td>
<td>alter table tickets drop column ticket_no</td>
</tr>
<tr>
<td>2007-01-22</td>
<td>SCOTT</td>
<td>C:\ORACLE\PRODUCT10.2.0\DB_1</td>
<td>alter table tickets add ticket varchar(30)</td>
</tr>
<tr>
<td>2007-01-22</td>
<td>SCOTT</td>
<td>C:\ORACLE\PRODUCT10.2.0\DB_1</td>
<td>alter table tickets</td>
</tr>
<tr>
<td>2007-01-22</td>
<td>SCOTT</td>
<td>C:\ORACLE\PRODUCT10.2.0\DB_1</td>
<td>create table tickets(ticket_no varchar(10), bus_unit varchar(16), description varchar(255), approver_id int)</td>
</tr>
<tr>
<td>2007-01-22</td>
<td>RBNRON</td>
<td>SQL QUERY ANALYZER</td>
<td>create table t1(i int)</td>
</tr>
<tr>
<td>2007-01-22</td>
<td>RBNRON</td>
<td>SQL QUERY ANALYZER</td>
<td>drop table t1</td>
</tr>
<tr>
<td>2007-01-22</td>
<td>RBNRON</td>
<td>SQL QUERY ANALYZER</td>
<td>drop table t3</td>
</tr>
<tr>
<td>2007-01-22</td>
<td>RBNRON</td>
<td>SQL QUERY ANALYZER</td>
<td>create table t3(i int)</td>
</tr>
<tr>
<td>2007-01-22</td>
<td>RBNRON</td>
<td>SQL QUERY ANALYZER</td>
<td>create table t1(i int)</td>
</tr>
<tr>
<td>2007-01-22</td>
<td>RBNRON</td>
<td>SQL QUERY ANALYZER</td>
<td>drop table t1</td>
</tr>
</tbody>
</table>

Records: 1 To 10 From 10
Proactive Database Security?

- Baselining to identify anomalous behavior
- Automatically suggests rules based on profiling
Provide insight such as . . .

- Who is changing database schemas or dropping tables?
- When are there any unauthorized source programs changing data?
- What are DBAs or outsourced staff doing to the databases?
- How many failed login attempts have occurred?
- Who is extracting credit card data?
- What data is being accessed from which network node?
- What data is being accessed by which application?
- How is data being accessed?
- What are the access patterns based on time of day?
- What database errors are being generated?
- What is the exposure to sensitive objects?
- When is someone attempting an SQL injection attack?
Gartner Recommendations

Implement Data Access Monitoring (DAM) functionality to mitigate the high levels of risk resulting from database vulnerabilities and to address audit findings in such areas as database segregation of duties (SOD) and change management.

Use DAM technology when there is a need for granular monitoring, or the overhead of database audit functions is unacceptable.

Use security information and event management (SIEM) technology when the additional resource consumption associated with native auditing is acceptable, and there is no need for advanced, database-focused analytics.

If specialized DAM technology is required, then the evaluation should encompass data capture methods, connection-pooling support, exception analysis, data retention, compliance reporting, blocking capabilities and incident management/workflow support.

Examples of related functions that may be provided by a DAM vendor include: Database vulnerability assessment and configuration audit, data loss prevention (discovery and control of sensitive structured data at rest and in motion), database change discovery and reconciliation to change management records.

Source: Gartner Research Report G00153063 (November 2007)
Summary Points

- Database auditing requirements go far beyond the capabilities of today’s DBMS software.
- Log analysis software does not solve access auditing requirements.
- Network sniffing does not provide sufficient auditability for mainframe databases.
- Long-term proof of database access not viable without archival of audit surveillance details.
- Audit details must be continuously managed:
  - Copying data for storage problems (e.g. media rot)
  - Copying data for system changes
  - Copying data for data encoding standard changes
  - Logging, auditing, and monitoring
Craig S. Mullins
NEON Enterprise Software, Inc.
craig.mullins@neonesoft.com
www.neonesoft.com
www.craigmullins.com
www.DB2portal.com

Intelligent Solutions for Enterprise Data. Depend On It.

http://www.neonesoft.com