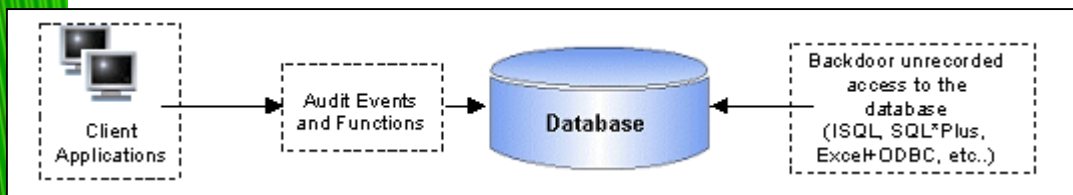# DB Audit
for Oracle, Microsoft SQL Server, Sybase ASE, Sybase ASA, and IBM DB2

Introduction

DB Audit is a professional database auditing solution enabling tracking and analysis of any database activity including database access, logons, security breaches, user and application activities, data creation, change or deletion. The database security tracking is essential for all organizations that must be able to comply – and document their compliance – with a range of federal laws including the Sarbanes-Oxley Act, Basel II, HIPAA and other regulations. DB Audit automates the collection and review of security events for all major database systems running on different platforms.

The Challenge

In addition to strong authorization controls, corporate security policy requires that audit trails be maintained at the database level to insure data integrity and to detect possible security breaches or intrusions. Although many third-party software applications using a relational database have built-in auditing capabilities, they are usually incomplete and only record events that take place through the application, thus leaving any backdoor access to the database unrecorded.

While most databases have built-in audit utilities, they are complex and do not provide enough detail to meet corporate auditing requirements. As a result, native database auditing utilities are often disabled. If they have been enabled, they usually are set to track a small subset of all the events required to meet corporate security policy due to a fear of creating performance problems or disk storage overhead. Logged audit events are rarely reviewed because the data are cryptic and too voluminous to be useful. There is no easy-to-use-reporting tool for filtering out irrelevant audit events or drilling down for more detail about suspicious activities. This also complicates the process of purging excess audit data and archiving significant audit events. These problems are compounded if multiple database audit trails must be maintained.

Another major problem with native database auditing utilities is the inability to track both "before" and "after" value detail on changes made to data within tables. This information is critical for creating a meaningful audit trail because it provides the means to determine if access rights have been abused. It also allows the correction of data that has been intentionally or accidentally modified in an unauthorized manner. In addition, the database does not provide a simple method for sending real-time alerts to the security console when time-sensitive critical audit events such as break-ins occur.
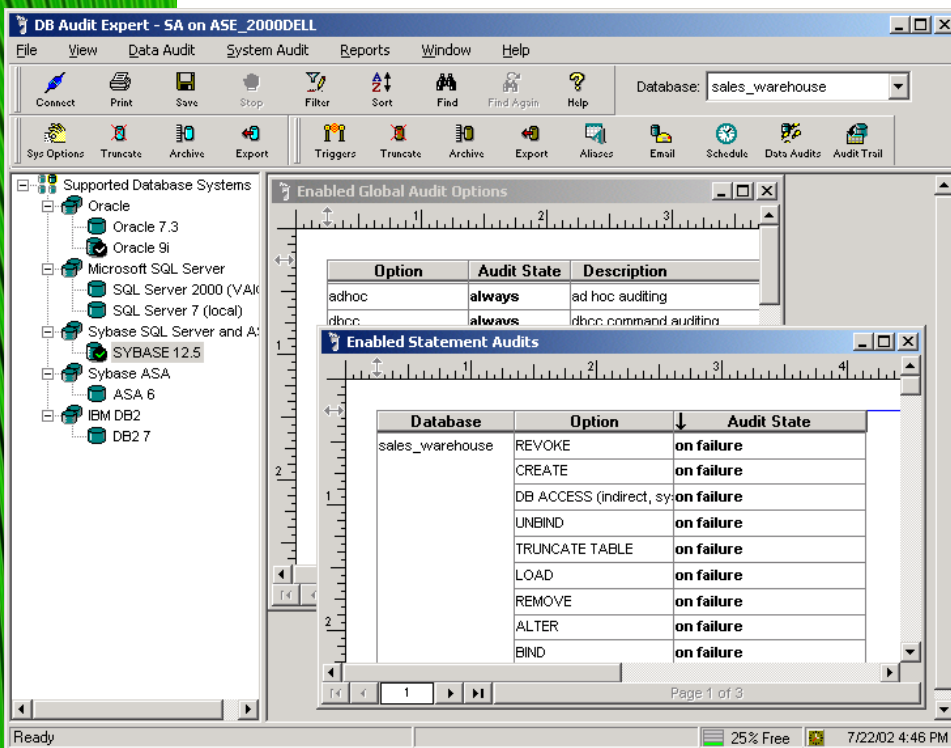
DB Audit
for Oracle, Microsoft SQL Server, Sybase ASE, Sybase ASA, and IBM DB2

An out-of-the-box auditing solution

DB Audit is a complete out-of-the-box auditing solution, which is easy to customize and does not require installation of any additional software or services on the database server and network. This solution is implemented completely on the database back-end thus eliminating any possibility of a backdoor access to the database unrecorded.

Administrators can utilize state-of-the art DB Audit Management Console graphical interface to easily and quickly configure audit settings on multiple database systems from a single location. The Management Console provides unified interface for different database systems hiding the complexity of database native functions while providing full access to all database supported audit options. The configured native audit functions can be used to record various events that have or will occur in the monitored database, primarily for auditing and improving system security, detecting penetration of the system and misuse of resources.

The DB Audit Management Console allows setting up mechanisms and functions for tracing value detail on changes made to data within tables (data-change audit). The data-change audit functions can be used to capture data-change events in database tables and record the "before" and "after" values as well as who, when and how made the changes. DB Audit Expert also allows setting up automated email alerts that can notify data owners about the data-change events.

In addition, DB Audit provides numerous pre-built analytical reports that can reduce large amounts of audit data to comprehensive summaries thus enabling to easily identify various database security violations.

DB Audit also provides administrators with tools for creating custom reports and report filters. Those custom reports can be distributed to the end-users using the Report Viewer utility without giving to end-users access to the DB Audit Management Console.

State-of-the-art DB Audit graphical user interface allows centralized auditing of multiple database systems from a single location.

DB Audit

for Oracle, Microsoft SQL Server, Sybase ASE, Sybase ASA, and IBM DB2

Key Benefits

➤ Provides totally transparent system-level and data-change auditing of any existing applications without requiring any changes to be made in those applications.

➤ Improves system security and ensures system accountability.

➤ Features centralized auditing control of multiple database systems from a single location providing ease of management.

➤ Features a unified auditing graphical interface that shortens the learning curve and is easy to use.

➤ Provides analytical reports that reduce large amounts of audit data to comprehensive summaries thus enabling to easily identify various database security violations.

➤ Provides analytical reports that help to identify which processes and users are hogging system resources.

➤ Provides audit trail details that are normally unavailable from standard database audit utilities.

➤ Frees DBA from the need to create and manage finely tuned database triggers for data-change auditing purposes.

➤ Provides ability to generate real-time email alerts to key personnel when changes occur to sensitive data.

➤ Full compatibility with all host Operation Systems on which the supported Database Management Systems can run, including but not limited to Windows NT, UNIX, Linux, VMS, OS/390, z/OS.

DB Audit
for Oracle, Microsoft SQL Server, Sybase ASE, Sybase ASA, and IBM DB2

Audit Features by DBMS

DBMS Name and Version / Function	Oracle				Microsoft SQL Server			Sybase SQL Server (Adaptive Server Enterprise)				Sybase Adaptive Server Anywhere			IBM DB2		
	7.3	8.0	8i	9i - 10g	6.5	7	2000 - 2005	10.x	11.0 -11.1	11.5 -11.9	12.0 - 12.x	6.x	7.x	8.x	5.x	6.x	7.x - 9.x
System Audit GUI	X	X	X	X	N/A		X		X⁴	X	X	N/A	N/A	N/A		X⁵	X⁵
Data-Change Audit	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Data-Change Audit for Key-less Tables	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Data-Change Audit BLOB columns	X				X			X	X	X	X	X	X	X	X	X	X
Email Alerts			X	X	X	X	X		X¹	X¹		X²	X²	X		X³	X³
Disable Triggers	X	X	X	X		X	X				X						X
Schedule Data Audit Trail Purge	X	X	X	X		X	X				X	X	X	X		X	X
Schedule System Audit Trail Purge	X	X	X	X			X									X⁵	X⁵
System Audit Trail Archival	X	X	X	X			X		X	X	X					X⁵	X⁵
System Audit Trail Export	X	X	X	X			X		X	X	X					X⁵	X⁵
Data Audit Trail Archival	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Data Audit Trail Export	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

1 -   For ASE databases hosted on Windows NT platforms DB Audit uses xp_sendmail extended stored procedure. For ASE database hosted on UNIX platforms DB Audit uses the host Operation System's mail command executed via the ASE xp_cmdshell extended stored procedure.
2 -   Supported only with ASA running on Windows platforms.
3 -   Supported if JavaMail package is installed on the system.
4 -   Limited support.
5 -   DB2 UDB for Linux, Unix and Windows only.
N/A - System auditing is not supported by DBMS

DB Audit
for Oracle, Microsoft SQL Server, Sybase ASE, Sybase ASA, and IBM DB2

Additional Information

For additional information about DB Audit and to download a free evaluation version please visit http://www.softtreetech.com/idbaudit.htm

About SoftTree Technologies, Inc.

Founded in 1997, SoftTree Technologies provides advanced software, services, solutions and technologies for business computing. Today we are focused on developing powerful tools for database management, monitoring, auditing, tuning, and coding. We are also developing enterprise strength software task scheduling and automation tools.

Our software is carefully designed for mission critical applications. That is why many organizations all around the world have chosen our products. Among them are 3M, AT&T, IBM, JP Morgan Chase, Hewlett- Packard, Shell, Sony, USA Army, NASA and many others.

Trademarks

DB Audit Expert, DB Tools for Oracle, DB Mail for Oracle, 24x7 Automation Suite and 24x7 Scheduler are trademarks of SoftTree Technologies, Inc. in the United States and other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.