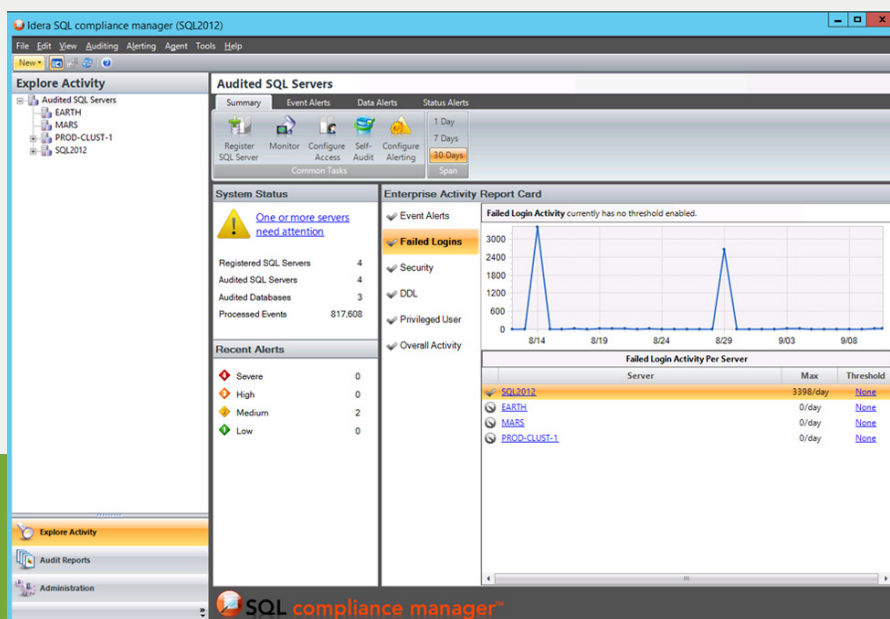# SQL Compliance Manager

MONITOR, AUDIT, AND ALERT ON SQL SERVER USER ACTIVITY & DATA CHANGES

SQL Compliance Manager is a comprehensive auditing solution that uses policy-based algorithms to track changes to your SQL Server objects and data. SQL Compliance Manager gives you detailed visibility to determine who did "what", "when", "where", and "how", whether the event is initiated by privileged users or hackers. SQL Compliance Manager also helps ensure compliance with regulatory and data security requirements such as SOX, PCI, FERPA, and HIPAA. SQL Compliance Manager goes beyond traditional auditing approaches by providing real-time monitoring, alerting, and auditing of all data access, selects, updates, schema modifications and permission changes to SQL Server databases.

WHY SQL COMPLIANCE MANAGER?

Data security and regulatory compliance requirements have become increasingly stringent. As a result, DBAs are tasked with the monumental job of providing an accurate audit trail of SQL Server activities such as database access, update actions, schema changes, and security changes. Unfortunately, auditing and reporting this information can often require weeks or months of custom development or in some cases the employment of a full-time DBA staff to provide scheduled or on-demand reports to auditors. SQL Compliance Manager eliminates this overhead by providing real-time monitoring, alerting, and auditing of SELECT statements (including column level granularity), DML, schema changes, permissions, and logins, giving quick, easy, accurate, and trusted answers to what has transpired on your servers. SQL Compliance Manager provides the best SQL Server auditing, alerting, and reporting solution which ensures all server access and exceptions are tracked to comply with internal and external audits. Furthermore, to ease the research and configuration required to comply with HIPAA, FERPA, SOX and PCI, SQL Compliance Manager delivers templates with pre-configured audit settings that align with regulatory citations.

Start for FREE!

IDERA

idera@konto.hr
+385.42.300.910
IDERA.com

PRODUCT HIGHLIGHTS

- **Audit Sensitive Data** Get detailed visibility of who did what, when, where and how
- **Improve Visibility** Web-based dashboard simplifies access from any browser
- **Track and Detect Changes** Monitor and audit all data access, failed logins, and schema and permission changes
- **Uncover Security Threats** Customize alerts and be notified of suspect activity by privileged users or hackers
- **Quickly Satisfy Audits** Demonstrate compliance with built-in PCI, HIPAA, FERPA and SOX templates
- **Easily Generate Reports** Deliver over 25 out-of-the-box reports to validate SQL Server audit trails
- **Minimize Overhead** Reduce impact on audited servers via a lightweight data collection mechanism

KEY BENEFITS

Continuous, Flexible Auditing
SQL Compliance Manager goes beyond traditional auditing approaches by providing real-time monitoring and auditing of all data access, updates, data structure modifications and changes to security permissions. The type and detail of audit data collected is highly configurable and may be defined at the server, database and object level. No changes to applications or production databases are required.

Immediate Notification of Suspect Activity
SQL Compliance Manager can be configured to alert DBAs of suspect server activity, either via e-mail or the event log. The alerting engine includes powerful features such as flexible alert definition, alert templates, custom messaging, and alert reporting, and alerts can be applied across the board, or to specific servers, databases, or tables, for more fine-grained control.

Minimal Performance Impact
SQL Compliance Manager employs a very efficient, low-overhead data collection mechanism to minimize impact on audited servers. A lightweight agent monitors the SQL Server extended events files, collects the audit data and sends it back to the repository. SQL Compliance Manager does not use high-overhead approaches that can impact server performance such as profiling, 'heavy' tracing options or log scraping.

Powerful Reporting and Analytics
SQL Compliance Manager provides out-of-the-box reports to address a broad range of auditing and security reporting needs. These reports were developed in conjunction with industry experts in security, compliance and auditing policies, such as Ernst and Young and Information Shield Inc. All reports may be easily customized, plus the user-friendly schema of the audit data repository enables rapid development of ad-hoc queries and reports for detailed forensic analysis.

ENTERPRISE MANAGEMENT FEATURES

Central Management Console
The flexibility to utilize either a Windows interface or web-based console provides enterprises with options to deploy and manage compliance based on their IT environment and needs. This enables rapid configuration and deployment of SQL Compliance Manager agents as well as real-time monitoring of agent activity and the audit data stream. This makes it easy to manage and track audit activity over a large number of servers.

Guided Instance Install
Guided installation wizard makes registering new SQL Server instances with SQL Compliance Manager fast and easy. This ensures permissions and rights are set correctly to monitor the new instance.

Dynamic Deployment Technology
Automatically deploys and configures the SQL Compliance Manager agents, enabling rapid deployment and eliminating the need for time consuming software installs on your SQL servers.

Central Data Repository
A central repository houses all audit data. The published, user-friendly repository schema enables easy development of queries and custom reports. In addition, multiple repositories may be used where required for security partitioning purposes.

Efficient Data Archive
Built-in archiving mechanisms enable archiving to be scheduled on any frequency and archives can easily be restored to the current audit data repository or a separate repository. Additionally, you can easily leverage SQL Safe Backup, IDERA's high-performance backup solution, to compress and encrypt audit data archives.

Availability Group Support
Automatically switches the auditing from primary to the secondary replica in the event of failure as well as failback to primary when it comes back online. No loss of audit data trail in the event of failure.

POWERFUL SQL SERVER AUDITING

Customizable HIPAA, FERPA, SOX and PCI Templates
Easily apply the right auditing settings to your servers and databases for Payment Card Industry (PCI), Family Educational Rights and Privacy Act (FERPA), Sarbanes Oxley Act (SOX), and Health Insurance Portability and Accountability Act (HIPAA) regulations. Extensive research is no longer required as you can simply define the objects and apply the included customizable templates.

Sensitive Column Search
Discover the location of sensitive data that needs to be audited using the integrated sensitive column search. The data search parameters are based on a user-selectable combination of pre-populated and custom defined search strings.

Sensitive Column Auditing and Alerting
Audit any combination of columns and track who has issued "SELECT" statements against any table whether they are end-users or privileged users. Additionally, you can be alerted when any combination of columns is accessed.

Data Auditing
Audit data changes on any table so you can compare before and after data values resulting from inserts, updates and deletions.

Extended Events Auditing
Monitor and audit SQL Server Extended Events (XEvents) for SELECT and DML events, to enable more efficient processing of large numbers of events and event types.

Audit Privileged Users
Allows you to include user-defined events (custom SQL Server event types) selected from a list in audited activities. You can audit, alert on, and filter user-defined events. Privileged user auditing is key to ensure all access to databases can be tracked and reported.

Low-Overhead Data Collection
A lightweight agent captures data from the SQL Server extended events files and extracts the selected events for auditing. The data collected can be streamed to the repository in real time or in scheduled batches.

Tamper-Proof Audit Data Repository
Guarantees the integrity of audit data by providing an immutable repository – any attempts at changing or tampering with the audit data can be detected. In addition, powerful self-auditing features capture and alert on all changes to auditing policies and data collection parameters.

FLEXIBLE ALERTING

Auditor's Mode
Users can be granted auditor privileges only. Users in the auditor role have read-only permission. This supports report and query execution as well as self-audit, integrity reporting, and alerting of changes to configuration and data collection parameters.

Fine-Grained Filtering
Powerful filtering capabilities enable you to collect only what is important for audit and compliance, reducing data collection, transmission and storage overhead.

Customized Alerting
Provides customized alerting for over 200 specific SQL Server event types, allowing you to define rules to receive immediate notification when critical SQL Server events occur. These events are stored in the audit repository, can be emailed directly to a user and/or written to an event log that feeds an in-house operations monitor system (e.g. SCOM).

Threshold Alerting
Configure multiple event threshold levels and set alerts. Be alerted through email, Windows event log, or SNMP when they are exceeded.

Database Auditing
Supports comprehensive auditing of database events. For example, events can be captured for data changes resulting from INSERT, UPDATE, or DELETE activity on tables, or additional application context can be included within your audit trail.

User-Defined Event Auditing
Allows you to include user-defined events (custom SQL Server levent types) selected from a list in audited activities. You can audit, alert on, and filter user-defined events.

IMPROVE ANY SQL SERVER AUDIT

Regionalni distributer: KONTO d.o.o. Požega
www.idera.konto.hr idera@konto.hr +385.42.300.910