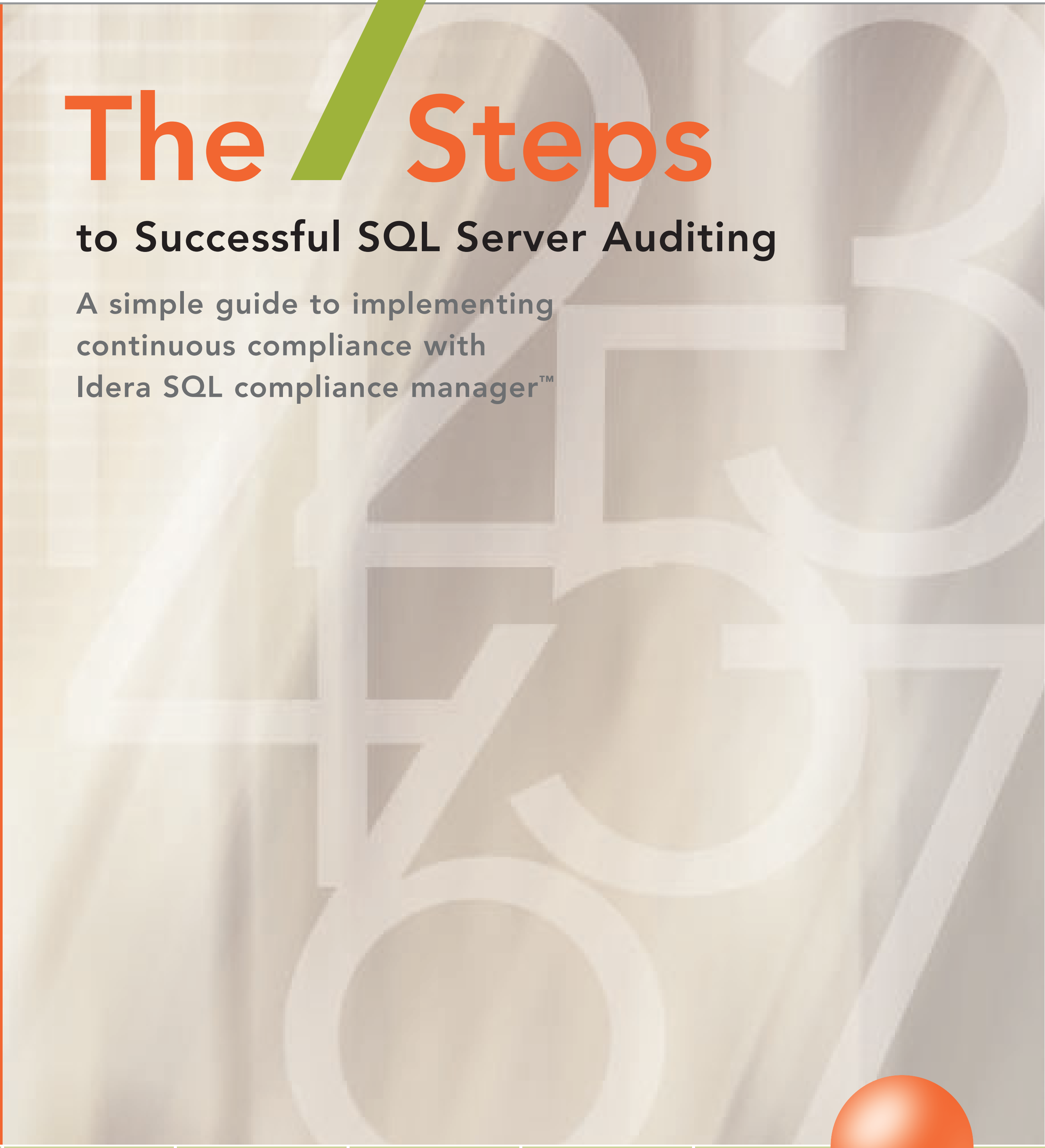
idera™

TOOLS FOR DATA MANAGEMENT

The 7 Steps

to Successful SQL Server Auditing

A simple guide to implementing
continuous compliance with
Idera SQL compliance manager™



01 02 03 04 05 06 07

> *"With the increasing deployment of SQL Server databases to hold mission-critical data, auditing and compliance have become critical issues. Organizations with large SQL Server infrastructure need a solution that is easy to deploy, easy to manage and that captures all the audit data required to ensure that compliance can be assessed on an on-going basis".*
>
> *—Mike Kelly, Partner at Ernst and Young LLP.*

INTRODUCTION

This paper provides an overview of the seven major steps involved in implementing an auditing and compliance solution for Microsoft SQL Server. If you are tasked with satisfying internal or external audit requirements on Microsoft SQL Server databases, this paper will provide you with practical guidelines. You'll also learn how continuous compliance is enabled and supported by Idera's SQL compliance manager product.

THE COMPLIANCE CHALLENGE

SQL Server DBAs today are tasked with ensuring compliance to a wide range of external auditing standards such as Sarbanes-Oxley, GLBA, HIPAA, Basel II, The USA Patriot Act and more. Compliance with these standards and also internal auditing standards is not optional. DBAs must be able to:

- Provide meaningful audit reports on a regular basis to ensure that appropriate controls are in place, and are being enforced
- Provide an 'on-demand' audit trail identifying who did what, to which database objects, and when it was done,
- Detect breaches to defined controls and alert appropriate authorities,
- Retain audit data for a sufficient time to comply with mandated data retention standards – often many years,
- Provide flexible access to audit data for forensic analysis,
- Meet all of the above requirements while not substantially impacting performance on production servers.

WHY TRADITIONAL AUDITING APPROACHES HAVE FAILED

Traditional approaches to SQL Server auditing and compliance have typically fallen short of meeting these requirements as they have:

- Produced large amounts of script generated snapshot reports hoping that auditors would be satisfied by volume rather than meaningful content,
- Imposed unacceptable load on production servers,
- Been highly complex to implement and costly to maintain as they have required an undue amount of DBA effort to install, configure, and administer on an ongoing basis,
- Been unable to provide a 'trusted' source of audit data to external auditors, bringing into question the integrity of the entire auditing process.

DBA VS. AUDITOR NEEDS

To be effective a SQL Server audit and compliance solution must support two major user communities, each with different needs.

DBAs need a 'set it and forget it' solution that can be implemented quickly, requires minimal ongoing management, and imposes minimal overhead on production servers.

Internal or external auditors on the other hand have different requirements, they need:

- Regular compliance reports that document adherence to agreed controls
- A 'trusted source' of audit data, i.e. one that is provably correct, cannot be changed without detection, and is a complete audit trail of all database activity associated with a given set of controls
- Long term data retention as defined by audit standards
- The ability to perform unstructured forensic analysis in order to investigate and resolve compliance issues.

REAL-TIME AUDITING AND CONTINUOUS COMPLIANCE

To effectively meet the needs of auditors and DBAs and to dramatically reduce the cost and time associated with auditing and compliance, a new approach is necessary – Continuous Compliance. The Continuous Compliance approach is based on the principles of Continuous Auditing as advocated by J. Donald Warren, Ph.D., Professor of Accounting and Director, Center for Continuous Auditing, Rutgers University. This approach is based on the premise that:

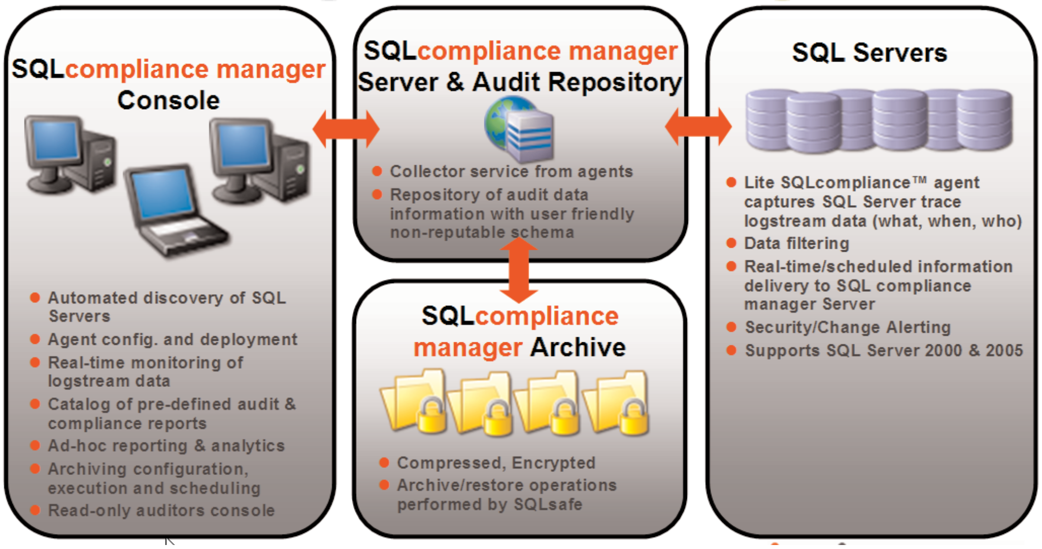
> "For internal auditors the classic audit model of a major yearly one time review performed on a cycle basis – has been done for years – may no longer be appropriate. Likewise for external auditors extending the audit throughout the year enhances audit effectiveness and efficiency. Using more continuous techniques is a logical response, as both internal and external auditors are finding that a more continuous audit process is both needed and expected." (1)
>
> "Continuous auditing is of great interest to internal auditors who appreciate it's potential as a solution to meeting the diverse demands of today's high-pressure, technologically complex business environments." (1)

Put simply, in the SQL Server world the Continuous Auditing or Compliance approach involves:

- Real-time data collection
- Continuous monitoring and auditing of data to ensure compliance with defined controls
- Reporting and alerting of anomalies
- A trusted, 'immutable' (i.e. not subject or susceptible to change) store of audit data

IDERA'S SQL compliance manager™ SOLUTION

As illustrated in the diagram below, Idera's SQL compliance manager™ was designed from the ground up to implement the concepts of continuous compliance for SQL Server databases.



SQLcompliance manager Console

- Automated discovery of SQL Servers
- Agent config. and deployment
- Real-time monitoring of logstream data
- Catalog of pre-defined audit & compliance reports
- Ad-hoc reporting & analytics
- Archiving configuration, execution and scheduling
- Read-only auditors console

SQLcompliance manager Server & Audit Repository

- Collector service from agents
- Repository of audit data information with user friendly non-reputable schema

SQLcompliance manager Archive

- Compressed, Encrypted
- Archive/restore operations performed by SQLsafe

SQL Servers

- Lite SQLcompliance™ agent captures SQL Server trace logstream data (what, when, who)
- Data filtering
- Real-time/scheduled information delivery to SQL compliance manager Server
- Security/Change Alerting
- Supports SQL Server 2000 & 2005

THE SEVEN STEPS TO SUCCESSFUL SQL SERVER AUDITING AND CONTINUOUS COMPLIANCE

The steps below outline a simple approach to setting up a continuous compliance solution. While this is a practical step by step guide that can be applied to almost any auditing scenario, all of the steps below can be facilitated and automated using Idera's SQL compliance manager™.

Furthermore, please note that although the steps below are in sequential order, auditing SQL Server is not necessarily a linear process. Idera SQL compliance manager™ is easy to deploy, and configure and DBAs can start auditing in literally minutes, then later streamline, refine, and customize auditing controls with ease, based on visible results and changing needs.

01 Define Controls

02 Design the Compliance Environment

03 Configure Environment

04 Deploy Collection Agents

05 Monitor Execution

06 Report and Review

07 Refine and Improve

01

DEFINE CONTROLS

The first step involves working with the internal and/or external audit team to understand the controls required to support the defined internal or external audit standards. Specific attention should be paid to what is required to be audited by applications and what is required to be audited at the database level.

01 02 03 04 05 06 07

02

DESIGN THE COMPLIANCE ENVIRONMENT

Once an understanding of the controls has been obtained the next step is to design how the controls will be turned into actual auditing 'rules' used to monitor compliance.

In doing this, the team needs to consider:

a. The audit rules that must be applied globally to all databases. For example, monitoring changes in security permissions or access rights are typically applied on a global basis,

b Which databases should be audited, it is often only necessary to audit databases that are critical to key business processes or that hold sensitive data,

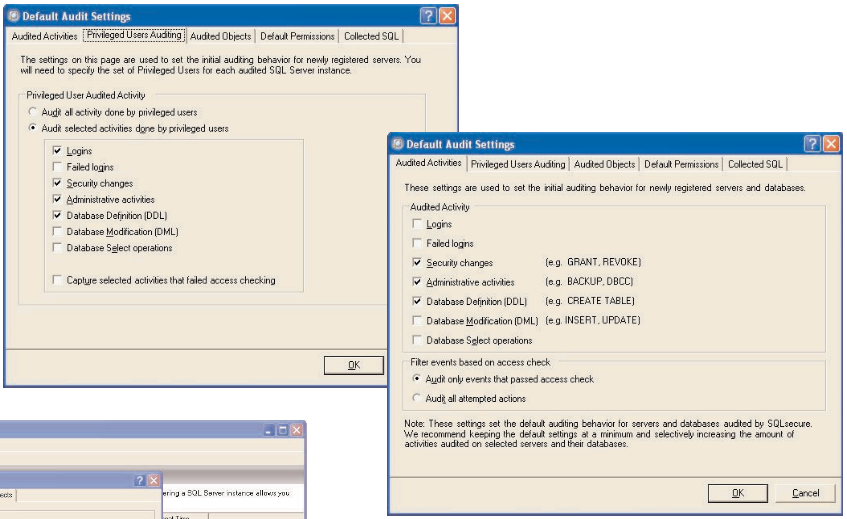
c. Which activities should be audited for each database, for example: logins, security changes, database definition (DDL), database modification (DML), Select statements, Privileged user (SA) activity, and Bulk data movement activities are all candidates for auditing. The choice depends heavily on the database type and contents,

   For example: Many databases exist only to support a single packaged application. These databases often require monitoring of only privileged user activity as all other types of control are handled via the application itself. Multi-application databases or databases that are subject to specific compliance regulations e.g. securities, financial reporting, aircraft maintenance, typically require auditing of access, update and modifications.

d. How long the audit data should be kept for each database. How long should the data be kept available on-line vs. archived and when can it be deleted? The data retention policy depends heavily on the audit standard and controls being applied (for example, SEC regulations mandate seven years).

CONFIGURE ENVIRONMENT

Once the design has been established, audit rules and the data retention policy must be configured. SQL compliance manager™ can be quickly and easily configured to apply and establish audit rules, as shown in the illustrations below.



Default Audit Settings

Audited Activities | Privileged Users Auditing | Audited Objects | Default Permissions | Collected SQL

The settings on this page are used to set the initial auditing behavior for newly registered servers. You will need to specify the set of Privileged Users for each audited SQL Server instance.

Privileged User Audited Activity

○ Audit all activity done by privileged users
● Audit selected activities done by privileged users

☑ Logins
☐ Failed logins
☑ Security changes
☑ Administrative activities
☑ Database Definition (DDL)
☐ Database Modification (DML)
☐ Database Select operations

☐ Capture selected activities that failed access checking

Default Audit Settings

Audited Activities | Privileged Users Auditing | Audited Objects | Default Permissions | Collected SQL

These settings are used to set the initial auditing behavior for newly registered servers and databases.

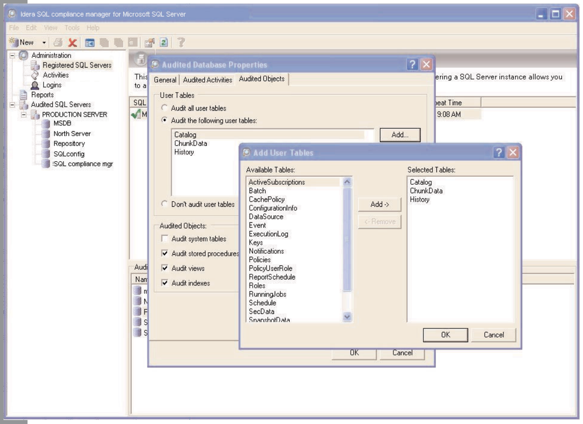
Audited Activity

☐ Logins
☐ Failed logins
☑ Security changes (e.g. GRANT, REVOKE)
☑ Administrative activities (e.g. BACKUP, DBCC)
☑ Database Definition (DDL) (e.g. CREATE TABLE)
☐ Database Modification (DML) (e.g. INSERT, UPDATE)
☐ Database Select operations

Filter events based on access check

● Audit only events that passed access check
○ Audit all attempted actions

Note: These settings set the default auditing behavior for servers and databases audited by SQLsecure. We recommend keeping the default settings at a minimum and selectively increasing the amount of activities audited on selected servers and their databases.



Idera SQL compliance manager for Microsoft SQL Server

Audited Database Properties

General | Audited Activities | Audited Objects

User Tables

○ Audit all user tables
● Audit the following user tables:

Catalog
ChunkData
History

○ Don't audit user tables

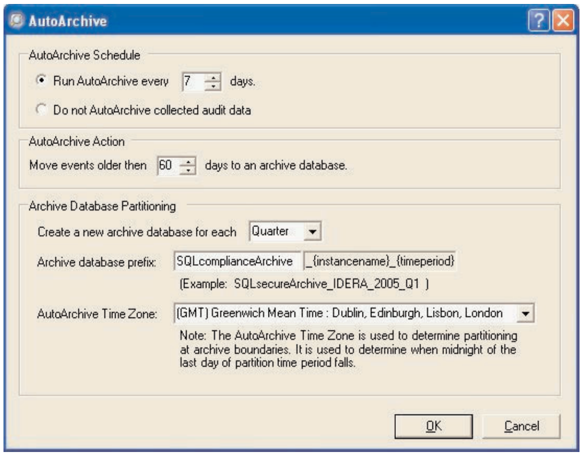
Audited Objects:

☐ Audit system tables
☑ Audit stored procedures
☑ Audit views
☑ Audit indexes

Add User Tables

Available Tables: ActiveSubscriptions, Batch, CachePolicy, ConfigurationInfo, DataSource, Event, ExecutionLog, Keys, Notifications, Policies, PolicyUserRole, ReportSchedule, Roles, RunningJobs, Schedule, SecData, SnapshotData

Selected Tables: Catalog, ChunkData, History



AutoArchive

AutoArchive Schedule

● Run AutoArchive every 7 days.
○ Do not AutoArchive collected audit data

AutoArchive Action

Move events older then 60 days to an archive database.

Archive Database Partitioning

Create a new archive database for each: Quarter

Archive database prefix: SQLcomplianceArchive _{instancename}_{timeperiod}

(Example: SQLsecureArchive_IDERA_2005_Q1)

AutoArchive Time Zone: (GMT) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

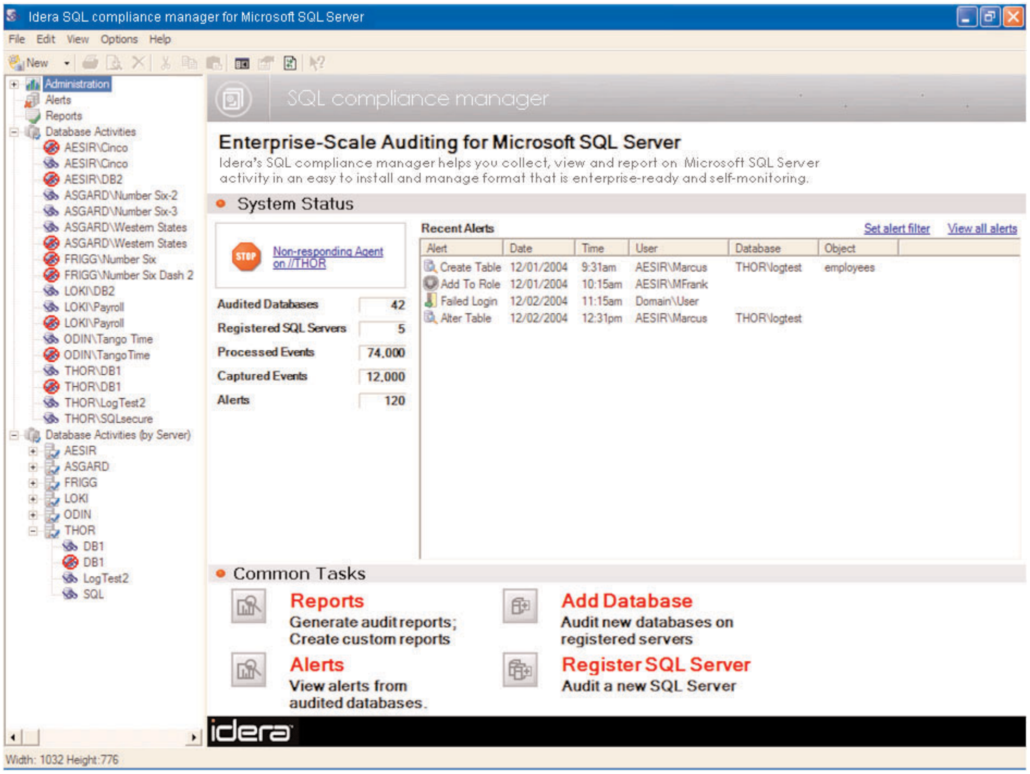
Note: The AutoArchive Time Zone is used to determine partitioning at archive boundaries. It is used to determine when midnight of the last day of partition time period falls.

Using SQL compliance manager's central console, you can quickly configure and manipulate global audit rules, privileged user audit rules, specific server audit rules, or audit data archiving rules -- with just a few simple clicks.

04

DEPLOY COLLECTION AGENTS

Deploy the configured collection agents to the SQL Server instances to be monitored. With SQL compliance manager™ the agents are auto-deployed across the network eliminating the need to manually install and configure each server.



Enterprise-Scale Auditing for Microsoft SQL Server

Idera's SQL compliance manager helps you collect, view and report on Microsoft SQL Server activity in an easy to install and manage format that is enterprise-ready and self-monitoring.

System Status

STOP Non-responding Agent on //THOR

Audited Databases	42
Registered SQL Servers	5
Processed Events	74,000
Captured Events	12,000
Alerts	120

Recent Alerts — Set alert filter — View all alerts

Alert	Date	Time	User	Database	Object
Create Table	12/01/2004	9:31am	AESIR\Marcus	THOR\logtest	employees
Add To Role	12/01/2004	10:15am	AESIR\MFrank		
Failed Login	12/02/2004	11:15am	Domain\User		
Alter Table	12/02/2004	12:31pm	AESIR\Marcus	THOR\logtest	

Common Tasks

Reports
Generate audit reports;
Create custom reports

Add Database
Audit new databases on
registered servers

Alerts
View alerts from
audited databases.

Register SQL Server
Audit a new SQL Server

Width: 1032 Height:776

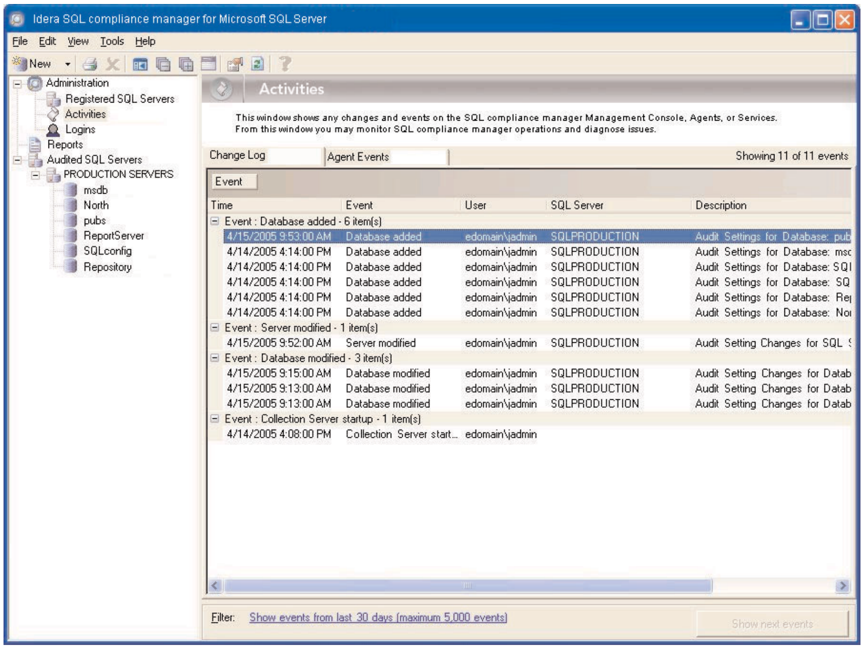
SQL compliance manager's enterprise console enables rapid deployment of SQL compliance agents™. All monitoring of agent activity and the audit data stream can then be done in real time from this central console, making it easy to manage and track audit activity over a large number of servers. SQL compliance agents™ are "lite" agents that require very low overhead and do not use triggers, profiling, “heavy” tracing, or log scraping.

MONITOR EXECUTION

From a DBA's perspective, monitoring the execution of compliance system simply involves using the SQL compliance manager™ console to:

a. Review the 'self-auditing' capabilities to ensure that auditing is proceeding as planned and that no intentional or unintentional attempts to subvert the audit and compliance process have taken place. Any attempts to subvert the compliance process will generate alerts, so the effort required to prove the integrity of the audit data tends to be minimal and somewhat reactive in nature,

b. Monitor audit data transaction rates and audit data repository growth rates to ensure that the system is optimally configured.



This window shows any changes and events on the SQL compliance manager Management Console, Agents, or Services.
From this window you may monitor SQL compliance manager operations and diagnose issues.

Showing 11 of 11 events

Time	Event	User	SQL Server	Description
Event : Database added - 6 item(s)				
4/15/2005 9:53:00 AM	Database added	edomain\jadmin	SQLPRODUCTION	Audit Settings for Database: pub
4/14/2005 4:14:00 PM	Database added	edomain\jadmin	SQLPRODUCTION	Audit Settings for Database: msc
4/14/2005 4:14:00 PM	Database added	edomain\jadmin	SQLPRODUCTION	Audit Settings for Database: SQI
4/14/2005 4:14:00 PM	Database added	edomain\jadmin	SQLPRODUCTION	Audit Settings for Database: SQ
4/14/2005 4:14:00 PM	Database added	edomain\jadmin	SQLPRODUCTION	Audit Settings for Database: Re|
4/14/2005 4:14:00 PM	Database added	edomain\jadmin	SQLPRODUCTION	Audit Settings for Database: Noı
Event : Server modified - 1 item(s)				
4/15/2005 9:52:00 AM	Server modified	edomain\jadmin	SQLPRODUCTION	Audit Setting Changes for SQL !
Event : Database modified - 3 item(s)				
4/15/2005 9:15:00 AM	Database modified	edomain\jadmin	SQLPRODUCTION	Audit Setting Changes for Datab
4/15/2005 9:13:00 AM	Database modified	edomain\jadmin	SQLPRODUCTION	Audit Setting Changes for Datab
4/15/2005 9:13:00 AM	Database modified	edomain\jadmin	SQLPRODUCTION	Audit Setting Changes for Datab
Event : Collection Server startup - 1 item(s)				
4/14/2005 4:08:00 PM	Collection Server start...	edomain\jadmin		

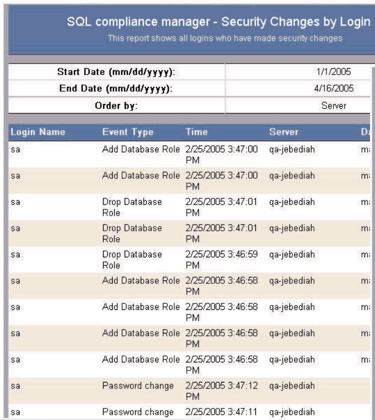
Filter: Show events from last 30 days (maximum 5,000 events)

A central repository houses all audit data gathered with SQL compliance manager. Then, powerful self-auditing features ensure that users are alerted to any attempts to change audit data collection policies or attempts to tamper with the contents of the audit data repository. Thus, SQL compliance manager provides a trusted, immutable source of audit data, significantly reducing the time required for audit data collection and verification.

REPORT AND REVIEW

From an auditors perspective, all reports and reviews can be done by interacting with SQL compliance manager™. This may include:

a. Reviewing compliance reports, identifying any compliance issues
b. If required, using the SQL compliance manager™ console to perform forensic analysis to determine the root cause of issues.
c. Reviewing the 'self-auditing' capabilities of SQL compliance manager™ to ensure that controls are being applied as specified.

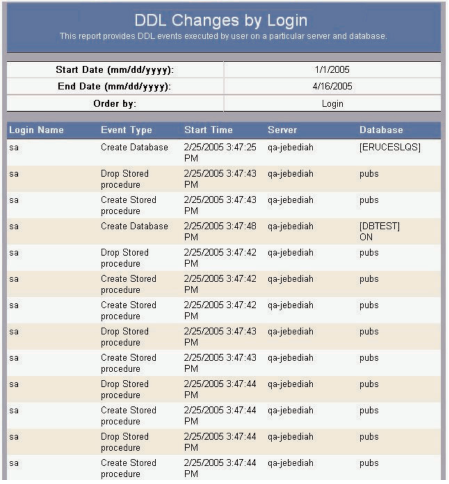


SQL compliance manager - Security Changes by Login

This report shows all logins who have made security changes

Start Date (mm/dd/yyyy):	1/1/2005
End Date (mm/dd/yyyy):	4/16/2005
Order by:	Server

Login Name	Event Type	Time	Server	Da
sa	Add Database Role	2/25/2005 3:47:00 PM	qa-jebediah	ma
sa	Add Database Role	2/25/2005 3:47:00 PM	qa-jebediah	ma
sa	Drop Database Role	2/25/2005 3:47:01 PM	qa-jebediah	ma
sa	Drop Database Role	2/25/2005 3:47:01 PM	qa-jebediah	ma
sa	Drop Database Role	2/25/2005 3:46:59 PM	qa-jebediah	ma
sa	Add Database Role	2/25/2005 3:46:58 PM	qa-jebediah	ma
sa	Add Database Role	2/25/2005 3:46:58 PM	qa-jebediah	ma
sa	Add Database Role	2/25/2005 3:46:58 PM	qa-jebediah	ma
sa	Add Database Role	2/25/2005 3:46:58 PM	qa-jebediah	ma
sa	Password change	2/25/2005 3:47:12 PM	qa-jebediah	
sa	Password change	2/25/2005 3:47:11	qa-jebediah	
		/2005 3:47:11	qa-jebediah	
		/2005 3:47:00	qa-jebediah	ma

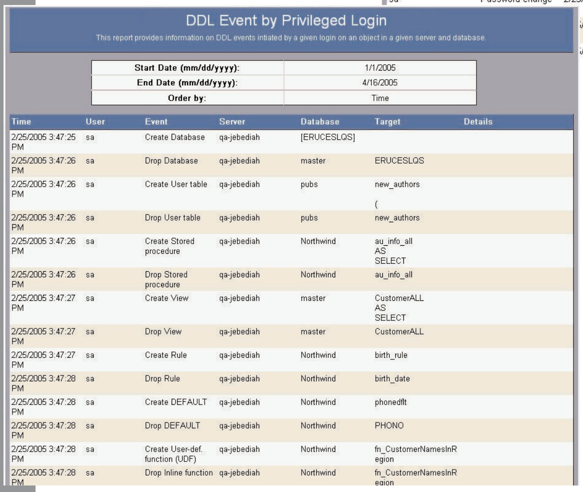


DDL Changes by Login

This report provides DDL events executed by user on a particular server and database.

Start Date (mm/dd/yyyy):	1/1/2005
End Date (mm/dd/yyyy):	4/16/2005
Order by:	Login

Login Name	Event Type	Start Time	Server	Database
sa	Create Database	2/25/2005 3:47:25 PM	qa-jebediah	[ERUCESLQS]
sa	Drop Stored procedure	2/25/2005 3:47:43 PM	qa-jebediah	pubs
sa	Create Stored procedure	2/25/2005 3:47:43 PM	qa-jebediah	pubs
sa	Create Database	2/25/2005 3:47:48 PM	qa-jebediah	[DBTEST] ON
sa	Drop Stored procedure	2/25/2005 3:47:42 PM	qa-jebediah	pubs
sa	Create Stored procedure	2/25/2005 3:47:42 PM	qa-jebediah	pubs
sa	Create Stored procedure	2/25/2005 3:47:42 PM	qa-jebediah	pubs
sa	Drop Stored procedure	2/25/2005 3:47:43 PM	qa-jebediah	pubs
sa	Create Stored procedure	2/25/2005 3:47:43 PM	qa-jebediah	pubs
sa	Drop Stored procedure	2/25/2005 3:47:44 PM	qa-jebediah	pubs
sa	Create Stored procedure	2/25/2005 3:47:44 PM	qa-jebediah	pubs
sa	Drop Stored procedure	2/25/2005 3:47:44 PM	qa-jebediah	pubs
sa	Create Stored procedure	2/25/2005 3:47:44 PM	qa-jebediah	pubs



DDL Event by Privileged Login

This report provides information on DDL events intiated by a given login on an object in a given server and database.

Start Date (mm/dd/yyyy):	1/1/2005
End Date (mm/dd/yyyy):	4/16/2005
Order by:	Time

Time	User	Event	Server	Database	Target	Details
2/25/2005 3:47:25 PM	sa	Create Database	qa-jebediah	[ERUCESLQS]		
2/25/2005 3:47:26 PM	sa	Drop Database	qa-jebediah	master	ERUCESLQS	
2/25/2005 3:47:26 PM	sa	Create User table	qa-jebediah	pubs	new_authors (	
2/25/2005 3:47:26 PM	sa	Drop User table	qa-jebediah	pubs	new_authors	
2/25/2005 3:47:26 PM	sa	Create Stored procedure	qa-jebediah	Northwind	au_info_all AS SELECT	
2/25/2005 3:47:26 PM	sa	Drop Stored procedure	qa-jebediah	Northwind	au_info_all	
2/25/2005 3:47:27 PM	sa	Create View	qa-jebediah	master	CustomerALL AS SELECT	
2/25/2005 3:47:27 PM	sa	Drop View	qa-jebediah	master	CustomerALL	
2/25/2005 3:47:27 PM	sa	Create Rule	qa-jebediah	Northwind	birth_rule	
2/25/2005 3:47:28 PM	sa	Drop Rule	qa-jebediah	Northwind	birth_date	
2/25/2005 3:47:28 PM	sa	Create DEFAULT	qa-jebediah	Northwind	phonedflt	
2/25/2005 3:47:28 PM	sa	Drop DEFAULT	qa-jebediah	Northwind	PHONO	
2/25/2005 3:47:28 PM	sa	Create User-def. function (UDF)	qa-jebediah	Northwind	fn_CustomerNamesInRegion	
2/25/2005 3:47:28 PM	sa	Drop Inline function	qa-jebediah	Northwind	fn_CustomerNamesInRegion	

SQL compliance manager provides "out of the box" auditing and compliance reports that were developed in conjunction with industry experts in security, compliance and auditing such as Ernst and Young. All reports can be easily customized. Also, a user-friendly schema within the repository enables easy ad-hoc queries and reports for forensic analysis.

07

REFINE AND IMPROVE

Once experience is gained with the continuous compliance approach organizations will typically tune the controls, the audit rules and the actual system itself to optimize performance. As mentioned in the introduction to the seven steps above, deploying and configuring SQL compliance manager™ is quick and easy so the concept of continuous improvement is straightforward to implement.

01 02 03 04 05 06 07

idera
TOOLS FOR DATA MANAGEMENT

CONTACTS

Idera Worldwide Headquarters
802 Lovett Boulevard
Houston, Texas 77006
Phone: 713.523.4433
Toll Free: 1.877.GO.IDERA (464.3372)
Fax 713.862.5210
info@idera.com
www.idera.com