IBM InfoSphere Guardium Data Activity Monitor for MongoDB

Proactively address regulatory compliance requirements and protect sensitive data in real time

Highlights

- Monitor and audit all data access activity for MongoDB
- Protect sensitive data with real-time alerting and blocking inappropriate access
- Build upon proven database monitoring technology
- Enforce separation of duties with a nonintrusive architecture
- Scale across the enterprise using a federated architecture

The proliferation of data from endpoint devices, growing user volumes, and new computing models like cloud, social business and big data have created demands for data access and analytics that can handle these staggering amounts of data. This has led to the rise of MongoDB and other NoSQL databases that offer performance and agility through the use of dynamic schemas.

IBM® InfoSphere® Guardium® has taken the lead in addressing data security and compliance concerns by delivering the first data monitoring and auditing solution for MongoDB.

Address data security and protection challenges

To address some fundamental security issues, MongoDB has recently delivered some enhancements for authorization and privileges; there is nothing here that relational databases haven't had for years. Audit and compliance requirements around the world require more robust accountability in terms of being able to log and verify who did what, and when, for a database transaction. This information must be stored for a defined period of time, sometimes years.

Beyond simple compliance, however, organizations have a responsibility to do whatever they can to avoid embarrassing or damaging data breaches. Demonstrating compliance is just one aspect, because when a breach does occur, being able to detect and react quickly—within minutes or hours rather than days or weeks—can mean the difference between a hugely damaging loss and a minor inconvenience.

For this reason, organizations using any combination of relational databases, Hadoop, or NoSQL databases such as MongoDB still need to implement best practices for auditing and compliance:

- Continuous real-time monitoring to ensure data access is protected and audited.
- Policy-based controls based on access patterns to rapidly detect unauthorized or suspicious activity and alert key personnel.
- Protection of sensitive data repositories against new threats or other malicious activity.
- Demonstrate compliance to pass audits: It's not enough to develop a holistic approach to data security and privacy; organizations must also demonstrate and prove compliance to internal and external auditors.

Understand the hidden costs and security risks of custom security solutions

How are organizations handling the requirements for audit and compliance for MongoDB? Because there has not been a good solution for this problem until now, it is likely that many organizations have not yet come to terms with the problem or are considering custom solutions such as creating shadow audit collections that store metadata about document changes based on the MongoDB oplog.
This is problematic in many ways:

- Read activity is not captured in the MongoDB oplog, which means unauthorized users can read as much data as they like—with no audit trail.
- Any approach that relies on log data or writes audit data to another collection within MongoDB does not comply with separation-of-duties (SOD) requirements because logs can be tampered with by a MongoDB privileged user or a hacker.
- Real-time alerting is not supported; any compliance infraction or data breach could take weeks or months to discover using custom approaches.
- There are no capabilities for real-time prevention of data breaches, such as blocking.

Organizations would need to spend significant IT resources working around these issues. In most cases, organizations are using MongoDB to give them leading-edge applications. However, creating custom-solution audit trails for compliance is not necessarily the best use of those resources.

Rely on a scalable enterprise-wide database security and compliance platform

InfoSphere Guardium has extended its market-leading[1] data activity monitoring solution to include leading-edge platforms, such as MongoDB, so that you can exploit these new capabilities without sacrificing performance and flexibility to meet audit and compliance requirements.

With its nonintrusive architecture (Figure 1), InfoSphere Guardium provides full visibility into data activity and provides full separation of duties by storing audit data into a separate, tamper-proof software or hardware appliance, known as a collector. This architecture requires no configuration changes to the MongoDB servers. Operating system software taps, called S-TAPs, are installed on the MongoDB nodes. The S-TAP streams the network packets to a hardened, tamper-resistant hardware or software appliance known as a collector for parsing, analysis, and logging, into its internal repository. Because processing of the network traffic occurs on the collector, overhead on the MongoDB cluster is very low. The InfoSphere Guardium repository is the heart of the system and enables rich reporting, real-time alerting, and automated workflow management.

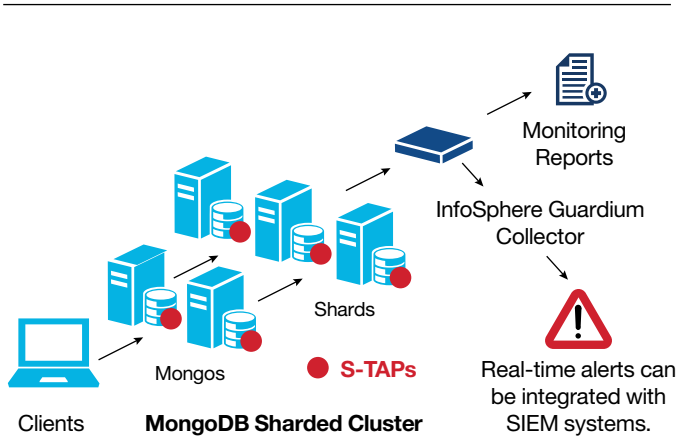

Figure 1: Architecture enforces separation of duties

Streamline compliance validation using automated, policy-based monitoring and auditing

The InfoSphere Guardium web console provides centralized management of alerts, report definitions, compliance workflow processes, and settings (such as archiving schedules) without the involvement of MongoDB administrators, thus providing the SOD required by auditors and streamlining compliance activities. A broad range of management functions can be executed across the entire database infrastructure, including:

- Defining granular security policies, using indicators of possible risk (appropriate for the particular environment), including the file or data object, type of access (reading, accessing, deleting), and user ID.
- Defining actions in response to policy violations, such as generating alerts and logging full incident details (Figure 2)
- Blocking access to sensitive data from privileged users or hackers
- Automating compliance workflow for routine activities and incident responses, including steps such as sign-offs, commenting and escalation
- Ready-to-use reports for compliance and a rich customizable reporting capability

With InfoSphere Guardium, you gain full visibility into MongoDB data activity, making it possible to identify unauthorized activities, like data tampering or hacking, and address them in real time. The report excerpt in Figure 3, for example, shows how read activity on a collection (a MongoDB find) is reported in InfoSphere Guardium, including the name of the database user.

Automation of the entire security and compliance lifecycle helps reduce labor costs, facilitate communication throughout the organization, and streamline audit preparation[2].

Policy Violations / Incident Management

Start Date: 2013-03-13 22:51:41 End Date: 2013-03-21 22:51:41
Aliases: OFF

Violation Log Id	Timestamp	Category Name	Access Rule Description	Client IP	Server IP	DB User Name	Full SQL String
551	2013-03-20 23.07.21.0		Excessive credit card download alert	9.70.144.201	9.70.145.249	NO_AUTH	test.credit_card.find({})

Figure 2: Real-time alerts can be color coded based on severity level

```
db.CreditCard.find()
```

My MongoDB Report

Start Date: 2013-06-03 21:01:45 End Date: 2013-06-05 21:01:45
Aliases: OFF DB_USER: LIKE %

Timestamp	Server Type	DB User Name	Details	Object Name	Command
2013-06-04 21:01:22.0	MONGODB	INDRANI	test.CreditCard.find({})	CreditCard	find

Figure 3: Monitoring reports showthe detailed activity of who did what

Supported MongoDB releases and capabilities

Guardium capabilities	**MongoDB 2.0, 2.2, 2.4**
Supports separation of duties using a role-based interface and a separate hardened hardware or software appliance for storing audit data	√
Activity monitoring, including privileged users and sensitive data access	√
Monitor mongos and shard servers to protect against privileged user access	√
Monitor users, including those using Kerberos	√ (2.4 Enterprise Edition or later releases)
Integrate audit results with other monitored databases for enterprise-wide reporting	√
Real-time alerts	√
Policy-based security for consistency across heterogeneous environments	√
Ready-to-use and customizable reports	√
Blocking privileged user access to sensitive data	√
Federated architecture for scalability	√
Compliance workflow and automation	√
Full set of administration APIs for automation and scripting	√

**For an updated list of supported data platforms for monitoring, see*
http://www.ibm.com/support/docview.wss?&uid=swg27035836

About IBM InfoSphere Guardium

InfoSphere Guardium is part of the IBM InfoSphere integrated platform and the IBM Security Systems Framework. The InfoSphere Integrated Platform defines, integrates, protects and manages trusted information in your systems. The InfoSphere Platform provides all the foundational building blocks of trusted information, including data integration, data warehousing, master data management, and information governance, all integrated with a core of shared metadata and models. The portfolio is modular, so you can start anywhere and mix and match InfoSphere software building blocks with components from other vendors, or choose to deploy multiple building blocks together for increased acceleration and value. The InfoSphere platform is an enterprise-class foundation for information-intensive projects, providing the performance, scalability, reliability and acceleration needed to simplify difficult challenges and deliver trusted information to your business faster.

For more information

To learn more about IBM Guardium, visit **ibm.com**/guardium

IBM is a 10gen Authorized Partner, and IBM InfoSphere Guardium Data Activity Monitor for MongoDB has been validated by 10gen.

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
June 2013

1 Gartner: "IBM InfoSphere Guardium is the market leader in terms of revenue and number of clients. Its offering has the widest platform coverage and the most robust set of features, and the company has demonstrated the ability to leverage the IBM sales model with its DAP offering."

Source: Database Activities You Should Be Monitoring. March 2012 Gartner, Inc. | G00231531

2 IBM United States Software Announcement 212-351 October 9, 2012

Please Recycle

IMD14432-USEN-00