ManageEngine
Log360

A beginner's handbook on

database auditing

Introduction

As businesses grow, so do the challenges they face securing their enterprise. Data security is a top priority in IT, making database security a major concern for administrators, security analysts, and CIOs alike. Databases are an important component of application security, and it's hard to imagine a business today that could run without one.

Databases not only store confidential business-related information such as revenue and employee details, but also sensitive customer data including credit card information. This makes them prone to a variety of attacks from hackers that can stem from external as well as internal sources. A database breach can result in a hefty compliance penalty and also a loss of customer trust in the business. This handbook explains how organizations can secure their databases by monitoring database activity using an auditing solution.

Assessing your data security strategy

With compliance mandates stressing the importance of data protection, it's crucial to reassess your data security strategy and equip your IT with the right set of tools to be proactive about data protection. For example, the GDPR is pushing organizations to take stringent measures to protect personal data. If your enterprise falls under mandates like the GDPR and experiences a data breach, you need to have proper systems in place to tackle the breach and avoid hefty compliance penalties.

Administrators need to ensure data in their database is secure, that the right people are accessing it, that operations that change data are authorized, and know whether an attack is attempting to breach their database server. Enterprises can secure their databases by monitoring critical activity occurring on the database, including the database server and its front end application.

Despite the high stakes, many organizations still lack control over their databases, or only have primitive database security measures in place. Database activity monitoring (DAM) is a must not only from a compliance point of view, but also for preventing breaches and achieving tighter enterprise security.

Generating database audit trails

Auditing records information about every event that occurs in your database, generating what are known as audit trails. Audit policies are the set of rules that govern log generation for specific events. Enabling an audit policy for an event database means configuring the database to generate log entries which contain information on a specific event. Depending on the database you use, say MSSQL or Oracle, the exact process to configure auditing will vary, but the general idea remains the same.

Auditing can help you track every event of concern and helps answer questions such as who did what changes, when, and where. For example, if you take a particular operation performed by a user, auditing can capture the details of the user, the date and time of the operation, and more. This allows administrators to get vital information for forensic analysis, helping them file an incident report.

Auditing brings accountability to changes made to data, and that kind of liability is fundamental to meeting compliance regulations such as SOX and HIPAA. Auditing helps you keep track of actions performed by users, detect suspicious activity on your databases, and ensure your IT complies with regulatory compliance mandates.

Setting an optimal audit policy

It is important to clearly understand your requirements and analyze your security posture before setting up auditing. It would be unwise to audit every event occurring on your databases. This is because auditing is resource-intensive and puts an extra load on your system. Further, auditing all or most events results in a massive audit trail from which it would be extremely difficult to pick out specific events that are of concern to your security. For example, if you're only interested in tracking the deletion of a particular table, it's best to limit your auditing to just that and not bother with configuring auditing for creating or updating a table.

Leveraging audit trails with an auditing tool

Manually auditing a database without a tool can become cumbersome and inefficient. The challenge with auditing is that several database operations may be carried out on a given day. That makes it practically impossible for you to keep track of all of them and identify the operations that could pose a threat to your enterprise. This is a good point to reiterate the need for an optimal auditing configuration on your database.

An auditing solution like a security information and event management (SIEM) tool can help track activity on your database. It can collect the audit information generated by a database and give you a clear picture of what's going on, simplifying auditing. SIEM tools can help you run reports to easily visualize database activities of concern and also alert you about events that could pose a threat to your security.

It's crucial to have an auditing and alerting tool such as a SIEM solution in place to ensure your security operations can visualize the audit data they need. Further, in the event of a data breach, a SIEM tool can help you generate an incident report and furnish details of a breach or attack such as an SQL injection attack.

Enterprises often have a naive view about security threats. For example, many enterprises don't track internal threats to their database. Continuously monitoring database activity is a must to gain complete control over your databases, but enforcing database security goes beyond just auditing its contents. Users, privileges, data accesses, server activity, and other events on your database also need to be monitored to secure your database.

Log360, a comprehensive SIEM tool, audits MSSQL and Oracle databases, including database server activities, with exhaustive predefined reports and associated alert profiles. These on-the-fly resources help you easily audit and secure your database.

There are five aspects of database auditing that administrators need to continuously monitor in order to secure their database. These are:

1. DML (data manipulation language) auditing

The database schema, including its tables, is the building block of a database. DML auditing tracks the functional-level activities occurring on your database schema and ensures that important information pertaining to DML changes, such as tables being viewed, updated, deleted, and more, are checked by capturing their details in the audit trail.

Tip: Log360 provides a wide range of predefined DML audit reports such as "Selected tables," "Deleted tables," "Updated tables," and more that help you stay on top of every DML event of interest occurring in your database.

2. DDL (data definition language) auditing

DDL defines the entire structure of your database, and DDL operations can bring about changes to your data. DDL auditing records important information about changes made by database query executions, such as table and index creation, and, along with DML auditing, ensures that all database accesses and operations being carried out are authorized.

Tip: Log360 provides a wide range of predefined DDL audit reports to track changes to your tables, views, procedures, and triggers, and alerts you for specific DDL events.

3. Database account auditing

Privileged database users have the power to make critical changes that can threaten your database's integrity. Database account auditing helps you easily manage user accounts and track user creation and deletion, password changes, database role changes, and more. This ensures that permissions to sensitive data have been correctly assigned. Often, enterprises don't have proper measures in place to keep the actions performed by privileged users on their databases under control and account management gets overlooked, which can lead to internal attacks such as privilege abuse.

Tip: Log360 provides a wide range of reports to simplify your database account management with predefined reports for the above mentioned user account events and more. It can also alert you for threats such as an abuse of privilege or an account lockout.

4. Database server auditing

Database server auditing allows you to analyze trends in server activity and helps in identifying anomalies that could threaten your database. For example, an unauthorized login to your database server could possibly lead to access and exposure of confidential information stored in the database. Auditing your database server helps you track events such as server role changes, audit specifications, login failures, startups, shutdowns, and more.

Tip: Log360 gives you full control over your database server, allowing you to track critical server activity with predefined reports and alert profiles.

5. Auditing to mitigate attacks

Security auditing ensures that your databases are always up and running and secure from attacks. It helps track different security attacks such as DoS and SQL injection and empowers you to quickly take action. If a database server is compromised, audit information allows you to furnish a detailed forensic report for compliance. It is also important to remember that databases are typically accessible via a web application, making their monitoring equally important for ensuring security.

Tip: Log360 alerts you for attacks on your database, such as DoS and SQL injection, and also empowers you to furnish a detailed incident report for your internal audits as well as for compliance.

Conclusion

So, figure out your organization's strategy for data security, then establish an ideal policy for auditing. Once the groundwork is in place, staying on top of the five aforementioned aspects of database auditing can go a long way in securing your databases, ensuring your IT meets compliance requirements.

About the author

Siddharth Sharathkumar is a computer science engineer who works in ManageEngine's product marketing team. He writes IT security articles and technical guides, presenting webinars on key security topics to educate security professionals and help enterprises solve their security challenges as well.

Check out his blogs **here.**

About ManageEngine

ManageEngine delivers the real-time IT management tools that empower an IT team to meet an organization’s need for real-timeservices and support. Worldwide, more than 60,000 established and emerging enterprises — including more than 60 percent of the Fortune 500 — rely on ManageEngine products to ensure the optimal performance of their critical IT infrastructure, including networks, servers, applications, desktops and more. ManageEngine is a division of Zoho Corp. with offices worldwide, including the United States, United Kingdom, India, Japan and China.