ManageEngine
EventLog Analyzer

SQL Server auditing with **EventLog Analyzer**

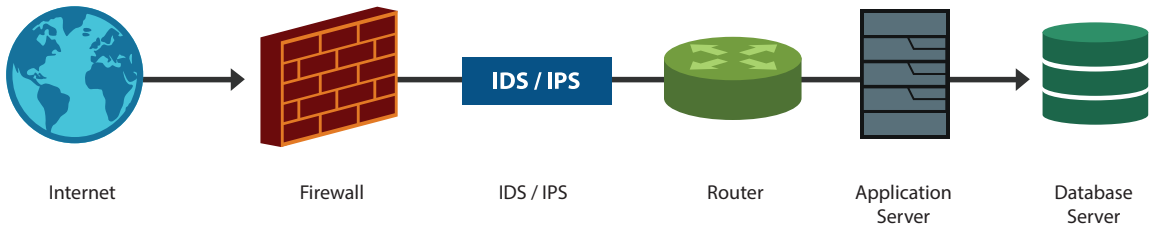
www.eventloganalyzer.com

SQL Server auditing with EventLog Analyzer

Databases form the backbone of an organization's network infrastructure. Today, organizations are collecting, processing, and storing more data than ever before. Database security thus becomes extremely pertinent given the growth in database size, complexity, and increasingly sophisticated attack methods.

How database attacks occur

Here is a quick overview of how a data breach usually occurs:



From outside the organization, databases are usually accessed via a front-end application, typically a web application hosted on the company's web server. Malicious users disguise themselves as valid network traffic in order to cross all perimeter security devices such as the firewalls and intrusion detection and prevention systems. They then proceed to find and manipulate a vulnerability in the application to gain control of the database, a process known as SQL injection. Attackers can also flood the database with seemingly valid requests, making its services unavailable to other users. This is another common type of attack known as denial of service.

From inside the organization, users with the appropriate permissions can directly breach the database or even cause physical damage to the servers and other storage media.

Attackers are adept at finding weak spots in your database security policy. When left unchecked, your database integrity could be severely compromised due to several factors, including:

- **Unauthorized changes:** If there is no stringent change management process in place, a multitude of unauthorized changes can occur in your database and can disrupt data integrity.
- **Unauthorized users:** When permissions are not properly assigned, unauthorized users can access a database.
- **Guest users:** Guest users must be disabled from using sensitive databases unless explicitly granted access.

- **Weak password policy:** User account passwords which are weak or not changed often are susceptible to attacks.

- **Irregular updates:** Failure to apply updates and patches released by your database vendor can make your server susceptible to viruses and other attacks.

- **Irregular backups:** Without a good backup policy in place, you can lose a lot of data if your server goes down for any reason.

Auditing databases: the need for a database reporting tool

Employing a good security policy is just part of a fully secured database server. Continuous monitoring of database transactions, user accesses, account changes, server level changes, etc. using database logs is necessary to ensure everything is running smoothly. It is also a security measure in itself, as it catches all attack attempts or indicators of compromise in your database, enabling you to take immediate corrective action and fine tune your security policy if necessary.

Due to the volume of logs generated, though, it is virtually impossible to go through them manually. Database vendors do not usually provide extensive reporting or alerting mechanisms. The use of a third-party tool such as EventLog Analyzer can solve this problem by providing the log analysis necessary to protect your databases.

Audit Microsoft SQL Server with EventLog Analyzer

EventLog Analyzer is an auditing and IT compliance management tool which can import and analyze SQL database logs with ease. The tool provides extensive reports and alerts for Microsoft SQL Server to improve its security. To monitor SQL server logs with EventLog Analyzer, you must:

- Enable logging on your Microsoft SQL Server.
- Import the logs to the EventLog Analyzer server.

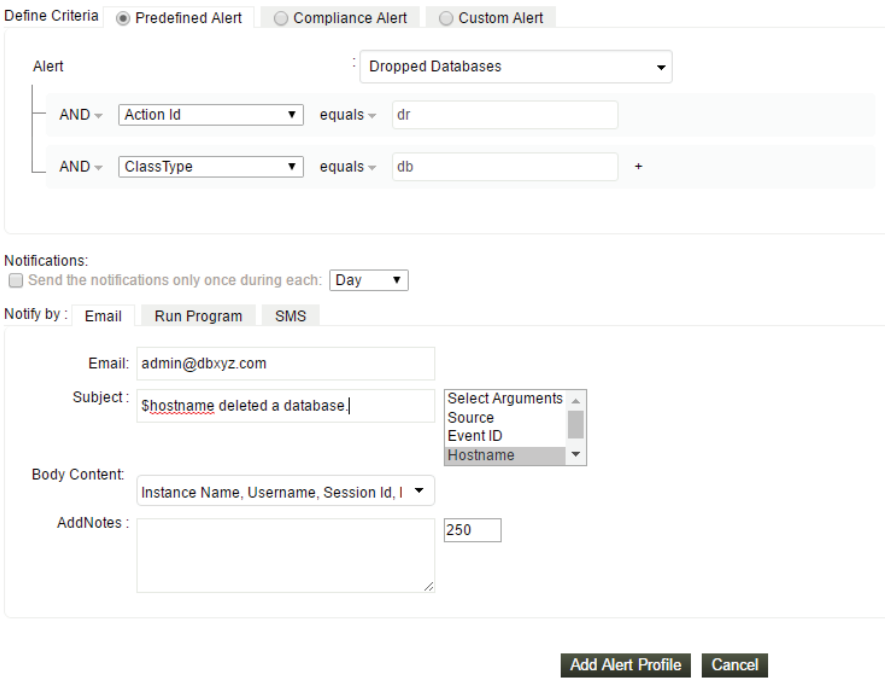
You can then proceed to view the instantly generated reports. You can also create custom reports or set up alert profiles and receive real-time SMS or email notifications about specific SQL Server events. The reports are provided in an intuitive graphical format, making it easier to understand the events on your database server. All reports can be customized, scheduled, distributed via email, or exported to PDF and CSV formats.

SQL Server reports and alerts are classified into five groups, allowing you to analyze the events of your choice with ease.

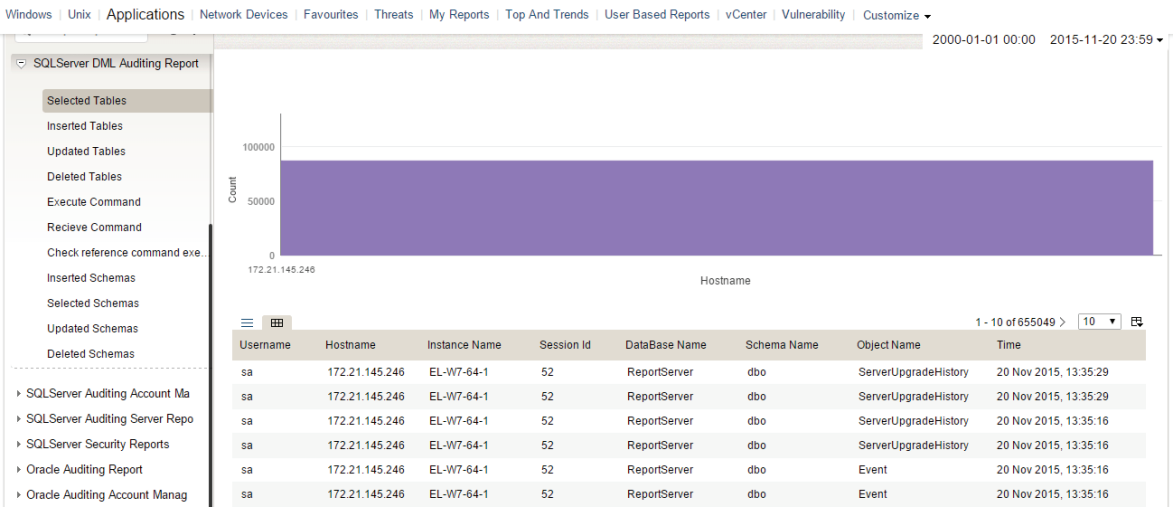
- **SQL Server DDL auditing:** Monitor and track the changes happening at the database structural level, such as changes to the tables, views, procedures, triggers, schema, and more. Easily discover the details of who made what change, when, and from where.

SQL Server auditing with EventLog Analyzer

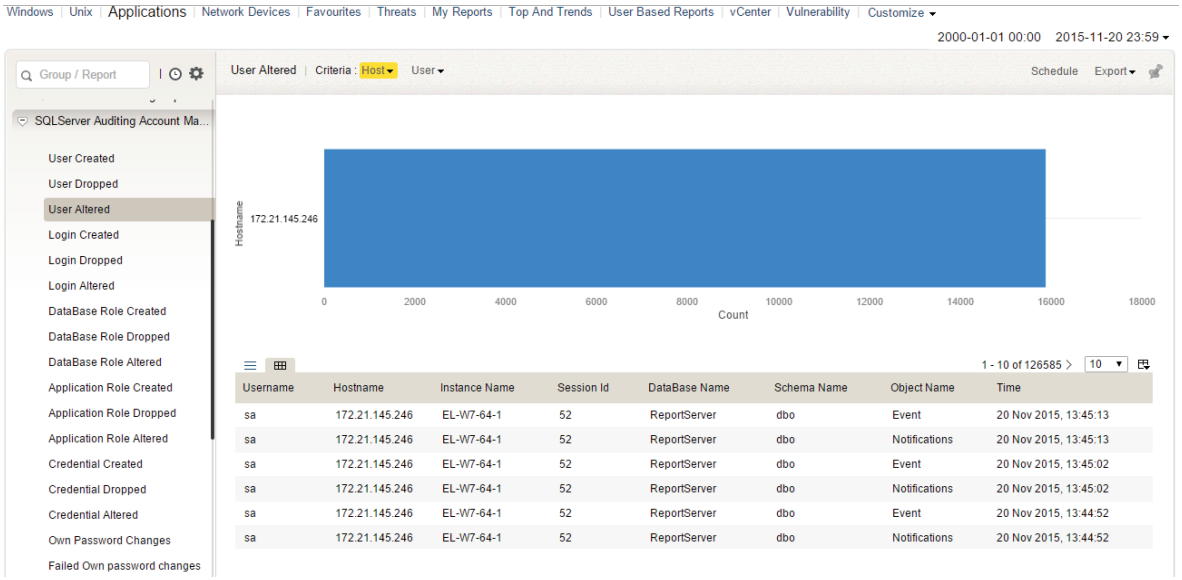
- **Scenario**: With an alert for dropped databases, the administrator is instantly notified of a major amount of data being deleted. If this is not expected, they can take immediate corrective action to restore the data and identify the user responsible.



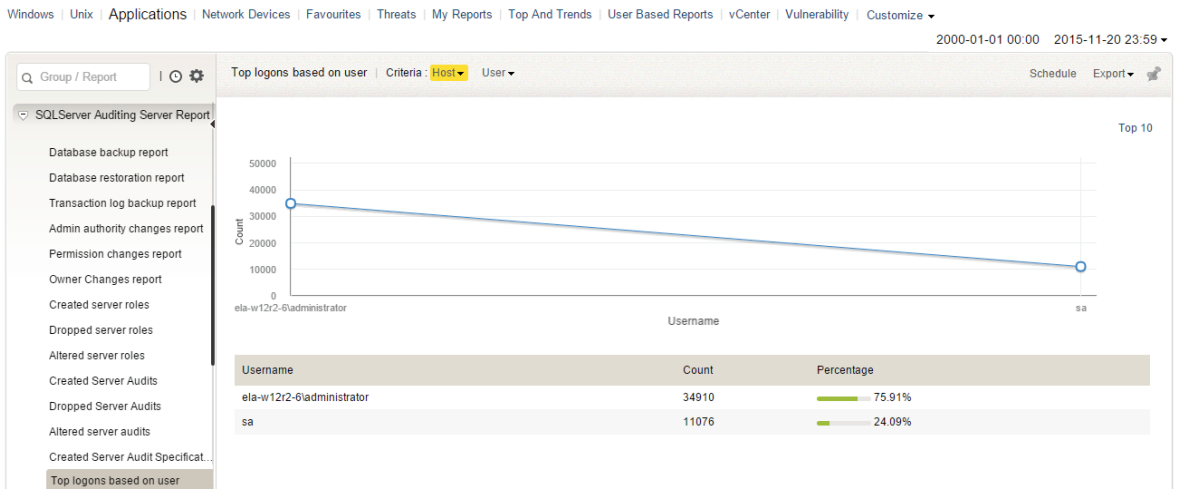
- **SQL Server DML auditing:** Audit all functional-level activities happening in the database. Find out when functional queries are executed, who executed them, and from where. Instantly track all change activity on confidential data such as data being viewed, updated, deleted, or new entries being made.
    - **Scenario**: The selected tables report helps an administrator understand which data is being viewed on the database.



- **SQL Server account management:** Managing and monitoring database server accounts is very critical in setting up authorizations for resources both inside and outside of the database. Track every change made to accounts such as privileged account creation, logons and logoffs, passwords, and more.
    - **Scenario**: The user altered report helps the administrator keep track of user permissions. If a user gains access to a sensitive database, the administrator can take immediate corrective action.

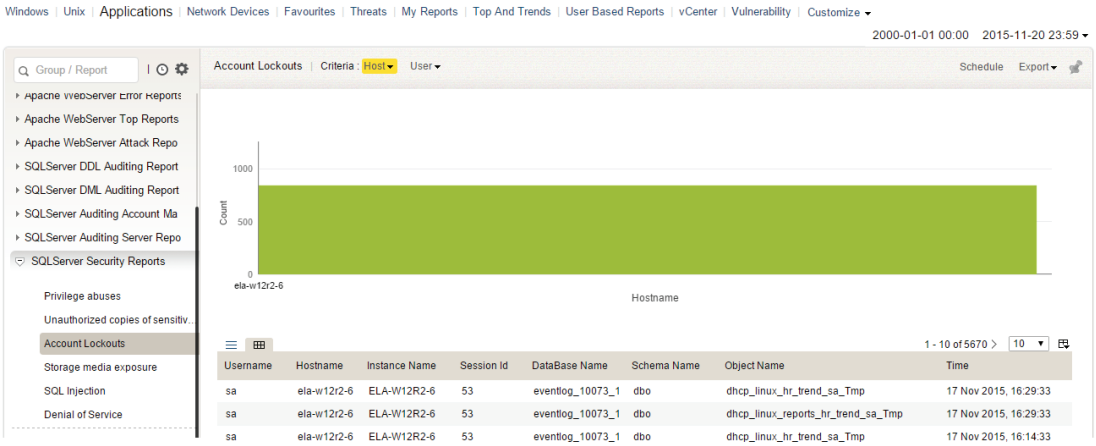


- **SQL Server auditing:** Audit SQL Server activities such as startups, shutdowns, logons, and logon failures. Also, obtain detailed reports on database backup, restoration, audit, audit specifications, administrator authorities, and more. Learn the top logon activities in the database, and visualize trend patterns of any logon failures.
    - **Scenario**: Top logons based on user is a trend report that helps an administrator understand who is most active in the database. A higher than expected value for any user could also indicate an account being compromised.



- **SQL Server account management:** SQL Server security: EventLog Analyzer helps mitigate external and internal security breaches by providing detailed reports on various security attacks that can occur in a database such as SQL injection and denial of service attacks. These help the administrator conduct detailed forensic analysis on how the attack happened. One can also track account lockouts, privilege abuses, unauthorized copying of sensitive data, and more, helping them instantly react to security breaches.

    - **Scenario**: Multiple account lockouts in a short span of time, as identified by the account lockouts report, could be indicative of hackers trying to gain access to the database.



With its comprehensive auditing and alerting capabilities, EventLog Analyzer serves as the perfect tool to monitor the activity, gain insights, and discover and prevent breach attempts on your SQL Server.

About EventLog Analyzer

EventLog Analyzer is a comprehensive IT compliance and log management software for SIEM. It provides detailed insights into your machine logs in the form of reports to help mitigate threats to help you achieve complete network security.

https://blogs.manageengine.com/eventloganalyzer

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 o□ces worldwide, including the United States, United Kingdom, India, Japan and China.