ManageEngine
EventLog Analyzer

# SQL Server 审计
# 使用EventLog Analyzer

www.eventloganalyzer.com

# 介绍

数据库是组织最重要的元素。
因为它们存储和处理公司的关键业务数据。

这些数据对网络犯罪分子来说具有很高的价值，他们正在每天都有新的针对性方法。除此之外，组织处理的数据量正在不断增长。

管理大量数据并保护其免受攻击是一项
这项艰巨的任务可能会暴露出不良的安全实践。这就是为什么数据库完整性、审计和安全性是许多组织。

# 数据库审计的重要性

您的数据库容易受到外部和内部攻击。攻击者善于寻找
漏洞允许他们找到进入您网络和数据库的途径。审计活动
数据库上发生的事件可以帮助你确保服务器上的一切顺利运行，
检测可能导致数据丢失的威胁。审计可帮助您找出以下事件：

- **错误更改：**如果没有严格的变更管理流程，大量
  数据库中可能会发生错误更改并破坏数据完整性。例如，如果
  多个用户对数据库具有写权限，重要数据可能会被覆盖
  错误的值。当对银行账户等关键列进行此类无效更改时
  数字，它可能会产生灾难性的后果。

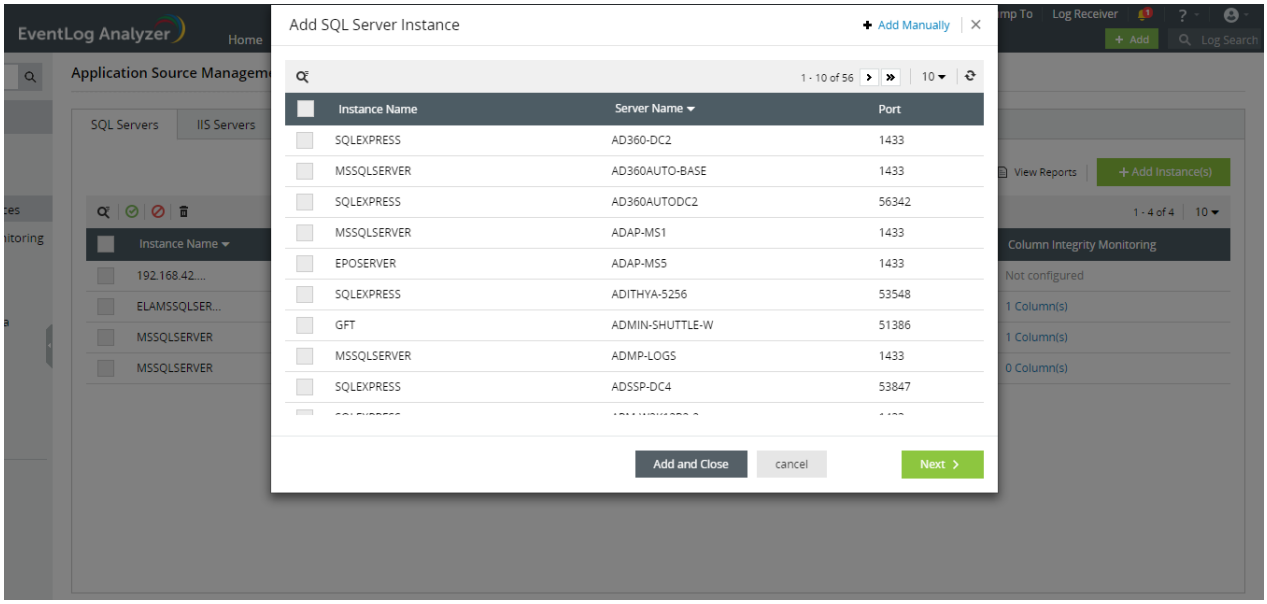
- **未经授权的活动：**当权限和用户账户管理不善时，用户
  可能会获得更高的权限和未经授权的敏感数据访问权，他们将能够
  修改。此外，外部攻击者可能会尝试使用窃取的凭证访问机密数据。
  他们使用的用户帐户可能没有足够的权限访问数据，从而导致
  未经授权的用户访问尝试。您需要监控所有此类事件，以阻止攻击
  最早阶段。

- **可疑的登录活动：**密码较弱的用户帐户很容易受到损害。
  攻击者可以通过暴力破解或其他方式轻松控制此类账户
  密码破解方法。如果这些账户具有特权并具有提升的访问权限，
  黑客可以自由地获取高度机密的数据。

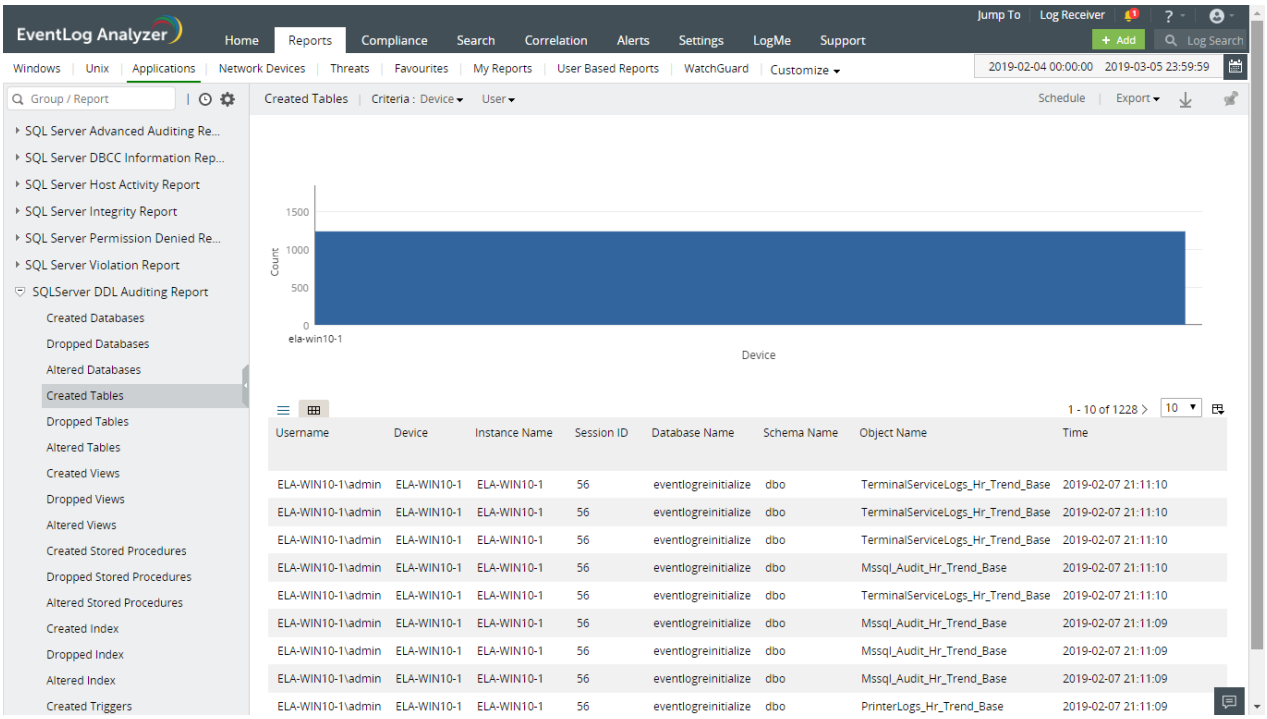
- **不一致的更新：**未能应用数据库供应商发布的更新和补丁
  会使您的服务器容易受到病毒和其他攻击。
  备份不一致：如果没有良好的备份策略，您可能会丢失大量数据，如果您的
  服务器由于某种原因瘫痪。

# 使用 EventLog Analyzer 进行 SQL Server 审计的亮点

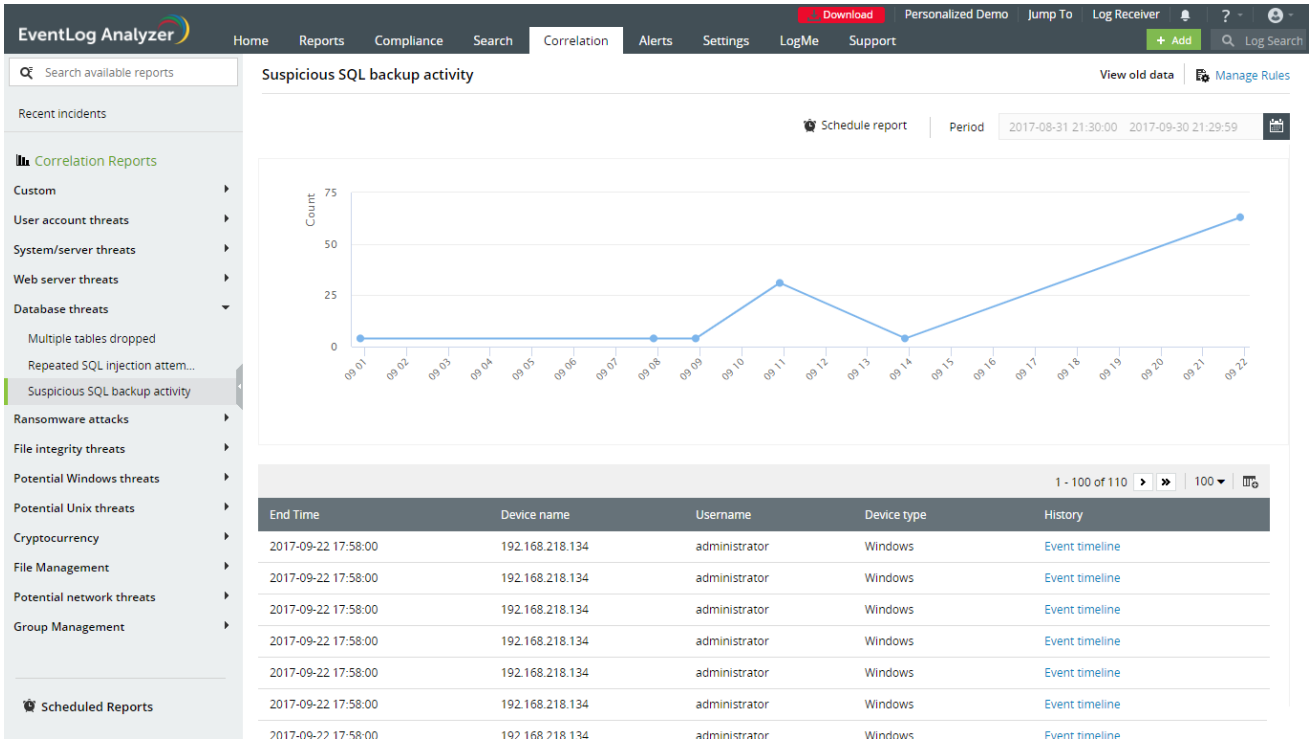
EventLog Analyzer 是一款日志管理、审计和 IT 合规性管理解决方案，轻松分析数据库日志。此工具为 Microsoft SQL 提供广泛的报告和警报服务器可帮助您增强安全状况。EventLog Analyzer 提供了许多功能，包括：



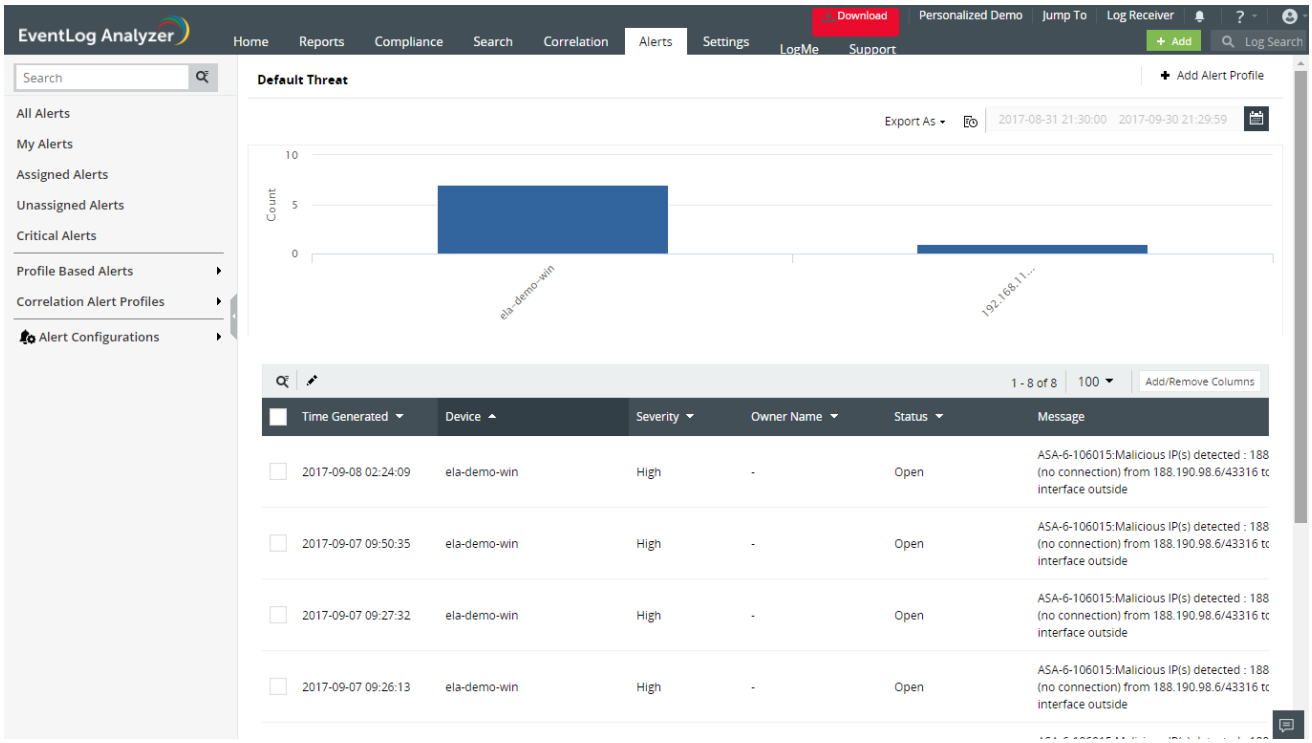

- **SQL Server 实例的自动发现：**自动发现所有 SQL Server 实例您的网络，以便您可以立即开始审核它们。



- **深入的审计报告和警报：**获取有关以下方面的详细信息：
  - **DDL 和 DML 活动：**了解数据库和表是如何被使用和修改的。
  - **SQL Server 活动：**跟踪 SQL Server 的启动和关闭，并跟踪对用户帐户和服务器级对象（如审计和审计规范对象）所做的更改。
  - **低级数据库活动：**通过有关数据库进程、安全更改、连接的应用程序等的高级审计报告深入了解数据库活动。
  - **柱完整性：**保护数据库中的关键列，防止其被篡改或错误修改。跟踪对数据值所做的更改并维护整体数据完整性。




- **事件关联：**通过事件关联获取有关 SQL 服务器上事件的更多背景信息。这该功能将 SQL Server 和其他应用程序和设备上发生的事件关联起来发现可疑的活动模式。例如，预定义的可疑 SQL Server 备份规则识别出可能对 Windows 计算机进行暴力破解的攻击，然后使用 SQL 備份事件。




**威胁情报：**根据最新威胁源接收通知并识别已知恶意行为者试图与您的数据库进行交互。

## 数据库审计场景

EventLog Analyzer 为 Microsoft SQL Server 提供超过 120 种预定义报表和警报。其中一些最常用的报告及其用途如下所列：

| 报告/警报名称 | 类别 | 用例 |
|---|---|---|
| 删除数据库 | DDL 审计 | **检测异常或大量数据删除：** 立即启动恢复工作，确保关键数据不会永远丢失。 |
| 选定的表 | DML 审计 | **跟踪数据库访问：**了解哪些数据正在被访问以及由谁访问。 |
| 用户账户被修改 | 帐户管理 | **管理数据库用户：**防止未经授权的帐户访问敏感数据。 |
| 根据用户排名的热门登录 | 服务器审计 | **发现服务器登录趋势：**识别最活跃的用户，并在活动异常频繁的情况下检测可能受到损害的帐户。 |

| | | |
|---|---|---|
| 可疑的 SQL 服务器备份 | 安全 | **检测可疑的备份活动：**获得未经授权的数据库备份通知。 |
| 已修改列 | 色谱柱完整性监测 | **维护数据完整性：**跟踪对敏感数据库列的值所做的更改。 |
| 连接的应用程序 | 高级审计 | **跟踪相关应用程序：**审核与数据库交互的所有应用程序，并确保没有未经授权的应用程序获得访问权限。 |

EventLog Analyzer 具有全面的审计和告警功能，是完美的工具监控活动，获取见解并发现和防止对 SQL 服务器的入侵尝试。

## 我们的产品

AD360 | Log360 | ADAudit Plus | Exchange Reporter Plus | DataSecurity Plus | SharePoint Manager Plus

ManageEngine
# EventLog Analyzer

EventLog Analyzer 是一款基于 Web 的实时日志管理和 IT 合规性解决方案，可抵御网络安全攻击。凭借全面的日志管理功能，EventLog Analyzer 可帮助组织满足其多样化的审计需求。它还提供现成的合规性报告和警报，可轻松满足严格的 IT 监管要求。

$ 获取报价　下载


直接拨打号码
4006608680

support@manageengine.cn

https://www.manageengine.cn/products/eventlog/