ManageEngine
EventLog Analyzer

EventLog Analyzer提供满足PCI DSS要求的数据完整性技术和安全措施

PCI DSS要求10.5规定审计跟踪必须要保证安全和防篡改。日志数据的完整性 对于确保事件信息可用于取证调查非常重要。

EventLog Analyzer有多种机制来确保在日志管理过程的每个阶段维护日志数 据的安全性和完整性。本文档阐述了EventLog Analyzer为保护收集、处理和 归档的日志数据而采用的数据完整性方法。

日志收集

- 日志收集过程安全可靠:使用安全的通信协议- WMI/DCOM、TLS和HTTPS(使用SSL/TLS保护HTTP)来确保数据的安全。TCP通信协议确保了日志信息的可靠传递。这些协议(WMI/DCOM除外)默认情况下不启用，需要单独配置。

- 峰值日志量的科学处理:在峰值日志量期间，EventLog Analyzer使用“数据缓冲区”来存储超过其阈值的日志。当日志量减少时，会处理这些日志，从而避免有日志被删除。

- 高可用性: EventLog Analyzer 允许您指定一个辅助服务器在主服务器出现故障时接管，从而避免丢失任何日志数据。

其他安全措施

- 安全web通信: EventLog Analyzer是一个基于web的解决方案，具有web客户端，可以从网络中的任何位置访问。启用HTTPS协议可以确保所有web通信的安全。

- 基于角色的访问控制(RBAC): EventLog Analyzer允许您在产品的技术人员之间划分您的数据。提供了三种访问级别:管理员、操作员和访客，以限制用户对特定功能和设备信息的访问和控制。这样，您可以确保只有经过授权的人员才能访问数据。

- 审计EventLog Analyzer技术人员操作:EventLog Analyzer提供了一个内置选项来生成产品中执行的所有用户操作的审计跟踪。这允许您确保解决方案本身的责任。

- 空闲时间后的会话终止:PCI DSS要求8.1.8中规定的会话终止要求。声明，“如果会话空闲超过15分钟，要求用户重新进行身份验证以重新激活终端或会话。”使用EventLog Analyzer，您可以设置会话到期时间，如果会话空闲时间超过10分钟(这是最短时间)，则会话将被终止。用户可以按照以下步骤将会话到期的默认设置30分钟更改为10分钟:

  1.以管理员身份登录EventLog Analyzer Web控制台。 2. 导航至 设置选项卡>系统设置>连接设置>常规设置。
  3.在“会话到期时间字段”中，提供属性值为“10”。

管理归档

EventLog Analyzer通过下面描述的三个关键技术措施来确保归档日志的完整性。该解决方案同时运行归档和分析日志过程。当接收到日志数据时，由弹性搜索引擎进行处理，并且还被加密并存档在用户指定的位置。

- 存档加密:存档数据使用AES 256加密机制进行保护。启用存档数据的加密方法如下:

1. 导航至设置>管理设置>管理归档。
2. 点击“设置”图标。
3. 选择与加密存档数据对应的启用选项。

2 时间戳:EventLog Analyzer通过使用时间戳技术来确保日志数据不会被篡改。归档数 据启用时间戳方法如下:

1. 导航至设置>管理设置>管理归档。
2. 点击设置＞高级的。
3. 选择与归档时间戳对应的启用选项

有关详细信息，请联系支持部门:support@manageengine.cn

ManageEngine
EventLog Analyzer

EventLog Analyzer是一个基于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可帮助企业满足不同的审计需求。它还提供开箱即用的合规性报表和告警，轻松满足严格的IT法规 要求。有关EventLog Analyzer的更多信息，请访问 https://www.manageengine.cn./products/eventlog/。

Get Quote Download