ManageEngine
EventLog Analyzer

ManageEngine EventLog Analyzer采用的数据完整性技术和安全措施

EventLog Analyzer 在日志管理过程的每个阶段都采用了多种机制，以确保日志数据的安全性和完整性得以保持。本文详细阐述了 EventLog Analyzer 采用的数据完整性方法，用于保护已收集、处理和存档的日志数据。

1. 安全可靠的日志收集：

我们使用安全通信协议，如 WMI/DCOM、TLS 和 HTTPS（使用SSL/TLS保护的HTTP），将收集的日志数据从设备传输到 EventLog Analyzer 服务器。采用 TCP 通信协议来确保日志消息的可靠传递。

这些协议在您的环境中默认情况下未启用，需要单独配置。

A. 在传输中保护日志的安全性

我们采用不同的安全和加密技术，如 TLS、AES-26、SHA-256 等，来保护在传输中的日志数据。根据日志数据的类型，采用不同的技术。以下是我们根据日志收集模式和数据类型采用的安全方法。

a. WMI 配置

通过 WMI 配置收集的 Windows 事件日志会使用 RPC_C_AUTHN_LEVEL_PKT_INTEGRITY 进行保护，这个级别会验证和确认客户端和服务器之间传输的数据没有被篡改。

b. Syslog 配置

Syslog 数据在传输过程中会使用 TLS 协议进行保护。

c. 代理加密

位于 DMZ 区域的设备通常通过代理来收集日志数据。

Copyright © 2023 ManageEngine

另外，一些企业也为了各种其他目的而部署代理程序。这些代理程序收集的日志数据会使用AES-256算法进行加密。另外，还可以启用HTTPS以确保基于代理的日志数据的安全性。

d. ES 数据传输中的安全性

数据在传输过程中的完整性是通过使用Search Guard ES插件来确保的。这些传输数据会使用TLS协议以及当前JVM支持的密码来进行加密。如果需要，可以更新协议和密码。支持的TLS协议和密码套件的完整列表在这里列出。

B. 日志数据的安全存储

所谓的静态日志是指存储在存档、ES、数据库和临时文件中的日志数据。

存储在ES和存档中的日志数据是可变的。可以通过利用存储供应商的功能来实现不可变性。

保护存储在存档中的日志数据

EventLog Analyzer通过下面描述的技术来确保存档日志的完整性。该解决方案同时运行日志存档和分析过程。当接收到日志数据时，它会经由弹性搜索引擎进行处理，还会被加密并存档在用户指定的位置。

1. 使用哈希技术

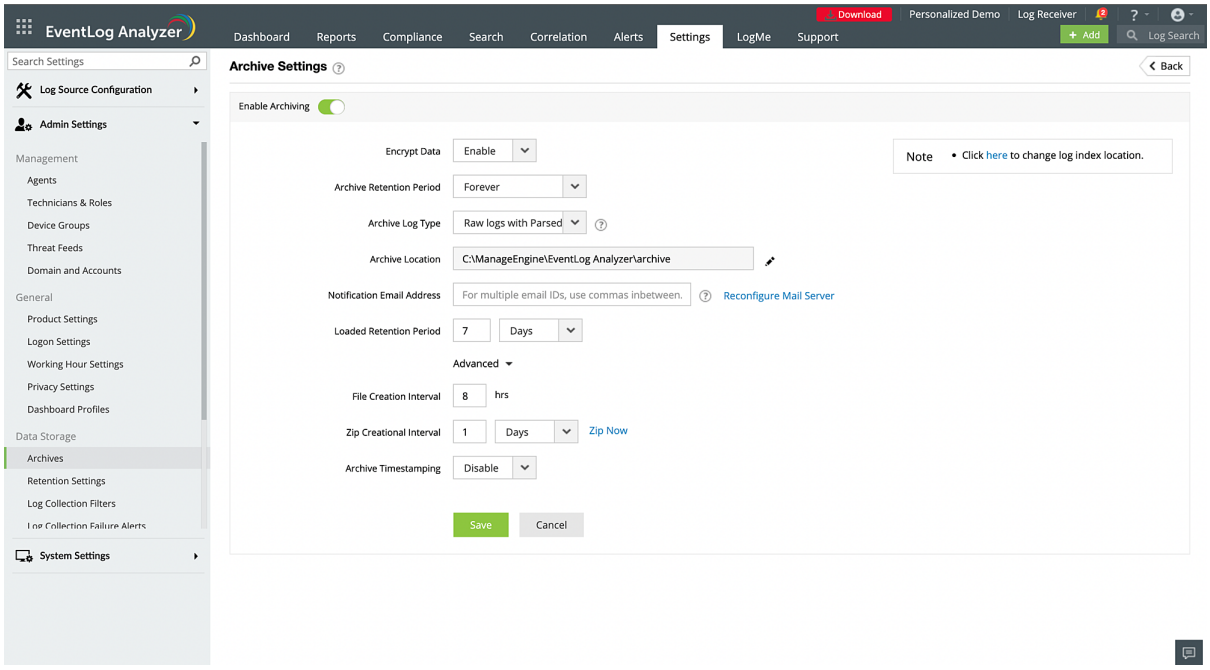
已存档的日志会使用SHA 256算法进行哈希处理，校验值会在数据库中维护。定期检查已存档文件的完整性，如果内容发生了修改，用户将在按计划或加载存档时收到通知。

2. 使用时间戳技术

当存档文件被压缩时，如果启用了时间戳功能，会创建一个扩展名为 .sgn 的独立文件，并存储在压缩文件内。具有 .sgn 扩展名的文件将包含一个经过编码的签名字符串（哈希值），使用我们的公钥进行签名。哈希处理采用SHA-1和RSA算法完成。如果文件具有 .sgn 扩展名，它将在进行完整性检查的同时进行时间戳检查。哈希值会定期与私钥进行交叉验证，以确保文件未被篡改。如果日志内容发生了修改，用户将在按计划或加载存档时收到通知。

Copyright © 2023 ManageEngine

此外，存档可以使用AES-256进行加密。这个方法会使文件变得不可读。如果文件被修改，它会变得损坏。您可以在设置 -> 管理员设置 -> 数据存储 -> 存档 -> 设置中启用此功能。默认情况下，还启用了篡改检测。



保护存储在数据库中的数据

EventLog Analyzer 可以使用 PostgreSQL 和 Microsoft SQL（2012 及以上版本）数据库作为其后端数据库。EventLog Analyzer 的配置数据存储在数据库中。默认情况下，EventLog Analyzer 将以 PostgreSQL 作为其后端数据库进行安装。通过为每个安装生成的独特密钥来保护它，该密钥安全地存储在应用程序中。这个 AES-256 加密密钥将用于加密包括密码在内的机密数据。捆绑的 Postgres 数据库也只设计用于接受本地主机连接。

用户还可以根据其需求选择迁移到 Microsoft SQL 服务器。在 MS SQL 中，为数据库创建了主密钥、证书和对称密钥。这个对称密钥用于加密和解密数据。

Copyright © 2023 ManageEngine

2. 高峰日志量处理：

在高峰日志量期间，EventLog Analyzer 使用一个“数据缓冲区”来存储超过阈值的日志。这些日志在日志量下降时进行处理，从而确保不会丢失任何日志。

3. 高可用性：

EventLog Analyzer 允许您指定一个备用服务器，在主服务器出现故障时接管，以确保不会丢失任何日志数据。

关于 EventLog Analyzer

EventLog Analyzer 是一个基于Web的实时日志管理和IT合规解决方案，用于抵御网络安全攻击。具备全面的日志管理功能，EventLog Analyzer 帮助组织满足各种审计需求。它还提供开箱即用的合规报告和警报，轻松满足IT法规要求。

关于 ManageEngine

ManageEngine 是 Zoho Corporation 旗下的企业IT管理部门。已建立和新兴企业，包括每10个财富100强组织中的9个，都依赖于 ManageEngine 的实时IT管理工具，以确保其IT基础架构的最佳性能，包括网络、服务器、应用程序、终端等。ManageEngine 在全球范围内设有办事处，包括美国、阿拉伯联合酋长国、荷兰、印度、哥伦比亚、墨西哥、巴西、新加坡、日本、中国和澳大利亚，还有200多个全球合作伙伴，以帮助组织紧密对齐业务和IT。

Copyright © 2023 ManageEngine