ManageEngine
EventLog Analyzer

高可用配置向导

www.eventloganalyzer.com

文档的目的

本文解释了高可用性配置 EventLog Analyzer 的好处、工作方式和步骤。

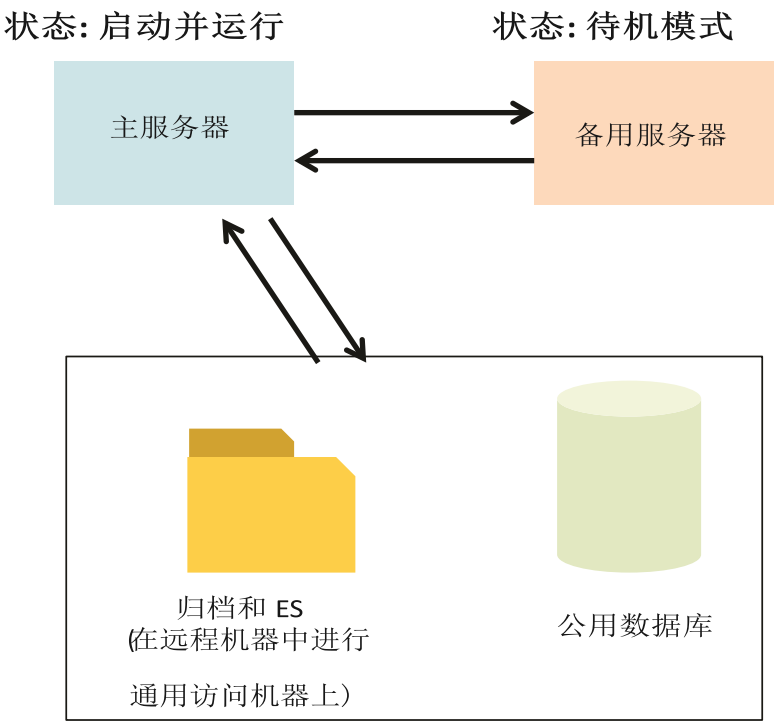
为什么需要确保 EventLog Analyzer 的高可用性?

作为一个网络安全解决方案，EventLog Analyzer 不断监视日志数据，查找异常和攻击模式，验证威胁，并帮助打击安全攻击。

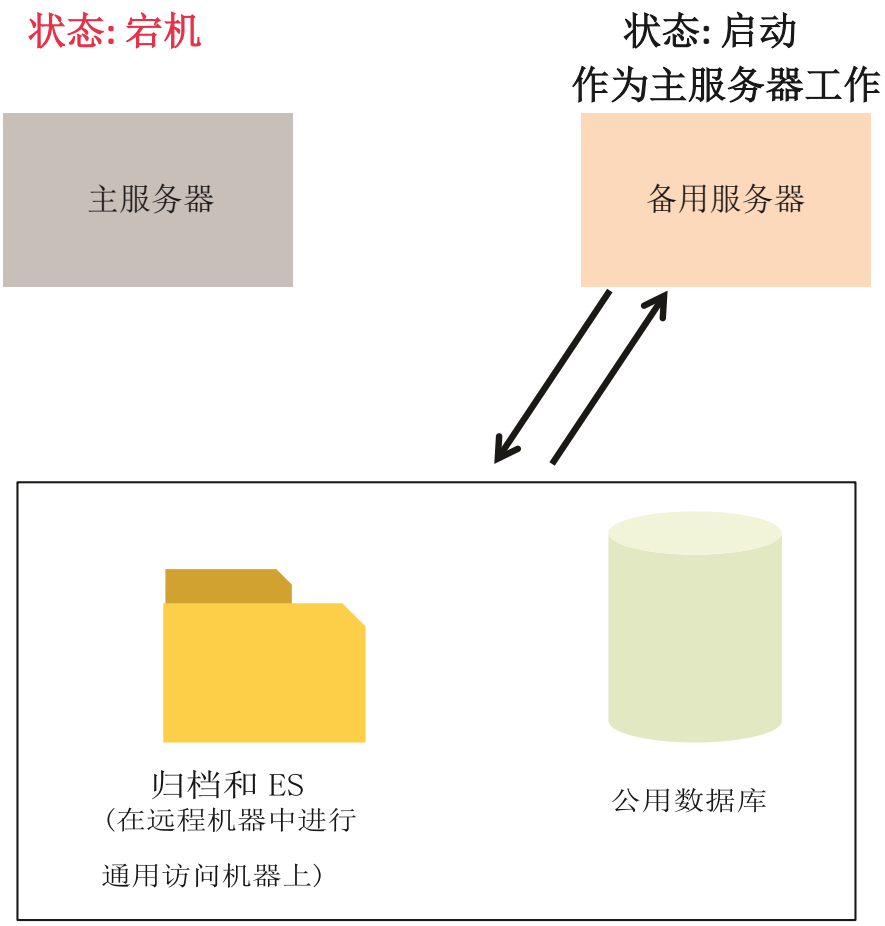
如果 EventLog Analyzer 服务器宕机，将导致日志数据收集和分析的中断。这可能导致无法识别安全事件，进而导致严重的数据泄露。这种违规行为不仅会造成巨大的财务损失和违规处罚，还会造成信誉和声誉的损失。因此，建议确保 EventLog Analyzer 的高可用性，从而保持它一直运行。

EventLog Analyzer 高可用性的工作方式

EventLog Analyzer 的高可用性设置包括两个独立的安装。其中一个充当主服务器，另一个充当备用服务器。两个安装都指向同一个数据库。归档日志数据和 ES 数据将在公共网络共享中可用。



默认情况下，主服务器将交付所有所需的服务。备用服务器也将启动，但仍将保持备用模式。但它将持续监视主服务器的状态。每当主服务器出现故障时，备用服务器就会启动并接管主服务器的角色。它将开始收集日志以防止任何数据丢失，并继续执行主服务器的所有功能，直到实际的主服务器恢复服务。



前提条件:

配置 EventLog Analyzer 高可用之前，请确保您有两个静态 IP 和一个虚拟 IP 地址。

配置步骤:

在 EventLog Analyzer 中配置高可用性非常简单。以下步骤就是如何来配置:

1 在两个独立的服务器上安装 EventLog Analyzer。

注意: 主服务器和备用服务器都应该在同一个网段中。

执行<EventLog_Analyzer 安装目录>\tools 文件夹中的 changeDBserver.bat 文件，将其中一台服务器的数据库改为 SQL。在弹出的对话框中，输入所需信息并保存。

在另外一台服务器上运行 **changeDBserver.bat** 文件，并指向相同的数据库。

注意:

(a) 当您运行该文件时，将弹出一个错误消息，说“数据库已经存在”。这个错误消息可以忽略。

(b) 在第二台服务器执行 **changeDBserver.bat** 文件时，请确保第一台服务器已停机。

2 请注意主服务器以及备份服务器都应该有静态 IP。配置静态 IP 地址的方式：

- **开始 > 控制面板 > 网络和共享中心 >以太网(本地连接)。**
- 选择**属性**菜单。
- 取消勾选 **Internet 协议版本 6 (TCP/IPv6)。**
- 选择 **Internet 协议版本 4 (TCP/IPv4)** 并点击 **属性。**
- 选择**使用以下 IP 地址。**
- 输入静态 IP 以及子网掩码。
- 最好，点击**确定**保存配置。

同样需要在备用服务器上执行上面的步骤，为其配置一个静态 IP 地址。

3 然后，在 **wrapper.conf** 文件中添加以下条目，该文件位于*<EventLog Analyzer_Home>\server\conf* 文件夹。

在主服务器中，添加以下条目：

wrapper.java.additional.x+1=-DremoteIp=<Secondary Server IP>

wrapper.java.additional.x+2=-DlocalIp=<Primary Server IP>

wrapper.java.additional.x+3=-DvirtualIp=<Virtual IP>

在备份服务器中，添加以下条目：

wrapper.java.additional.x+1=-DremoteIp=<Primary Server IP>

wrapper.java.additional.x+2=-DlocalIp=<Standby Server IP>

wrapper.java.additional.x+3=-DvirtualIp=<Virtual IP>

wrapper.java.additional.x+4=-DSecondary=true

注意: 主服务器和备份服务器都应该配置相同的虚拟 IP 地址。

x 的值随组织中的设置而变化。通过以下方式，找到 x 的值：

- 打开<EventLog Analyzer_Home>\server\conf\wrapper.conf，搜索 "wrapper.java.additional."。
- 导航至最后一次出现，记录下"wrapper.java.additonal."旁边的值。这就是要找的 x 的值。
- 根据这个 x 值添加主服务器和辅助服务器的命令。

例如，搜索"wrapper.java.additional."最后一次出现的结果为 "wrapper.java.additional.36"。在该场景中，x 的值为 36，并且您需要在主服务器中添加的条目为：
wrapper.java.additional.37=-DremoteIp=123.456.789.123

wrapper.java.additional.38=-DlocalIp=123.456.789.124

wrapper.java.additional.39=-DvirtualIp=123.456.789.125

备份服务器中添加的条目为：

wrapper.java.additional.37=-DremoteIp=123.456.789.124

wrapper.java.additional.38=-DlocalIp=123.456.789.123

wrapper.java.additional.39=-DvirtualIp=123.456.789.125

wrapper.java.additional.40=-DSecondary=true

同时，请确保，

- 虚拟 IP 地址在本地网络 IP 范围内。使用这个 IP 地址，高可用性脚本将在产品启动和关闭期间自动添加或删除虚拟 IP。

- EventLog Analyzer 进程绑定到虚拟 IP。在进行 syslog 监视时，应该将 syslog 设备配置为将其日志数据转发到这个虚拟 IP 地址。

6 然后，编辑并更新主、备份服务器的接口名称(*interfaceName* 字段)和虚拟 IP 子网掩码(*VirtualIPNetMask 字段*)，这些字段位于*<EventLog Analyzer_Home>\tools* 中的 **StartHA.vbs** 和 **StopHA.vbs** 文件。*interfaceName* 字段的值应该是在**网络共享中心**中找到的连接名。*VirtualIPNetMask* 字段应该是虚拟 IP 的子网掩码。

7 编辑*<EventLog Analyzer_Home\ES\Config* 文件夹中的 **elasticsearch.yml** 文件，找到 *path.data*。path.data 字段的值应该是公用共享位置，因此它可以在 ES 数据中存储主服务器和备用服务器的日志。

注意: 请确保主服务器和备用服务器都具有共享文件夹的完全控制权限。

8 启动 EventLog Analyzer 时，请确保它已被安装为服务。如果尚未安装为服务，请在*<EventLog Analyzer_Home>\bin* 目录中打开命令行，执行 **service.bat –i**，将该产品安装为服务。

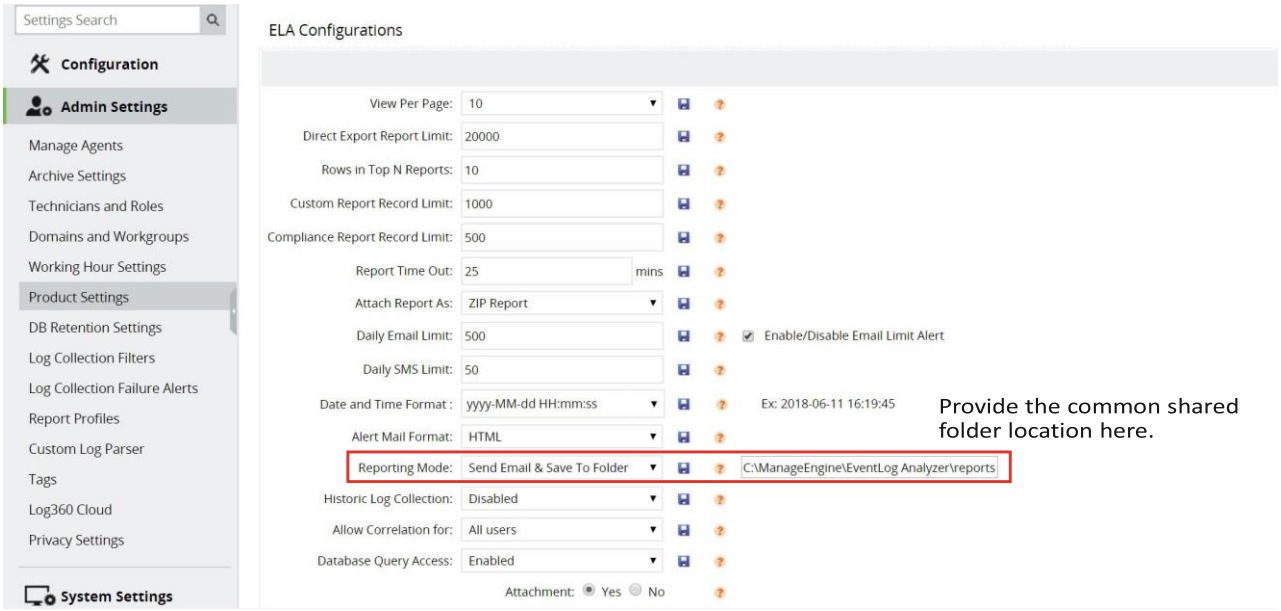
9 从 Windows 服务控制台中启动主服务。

注意: 在主、备份服务器中，请使用管理员凭证启动 EventLog Analyzer 服务。

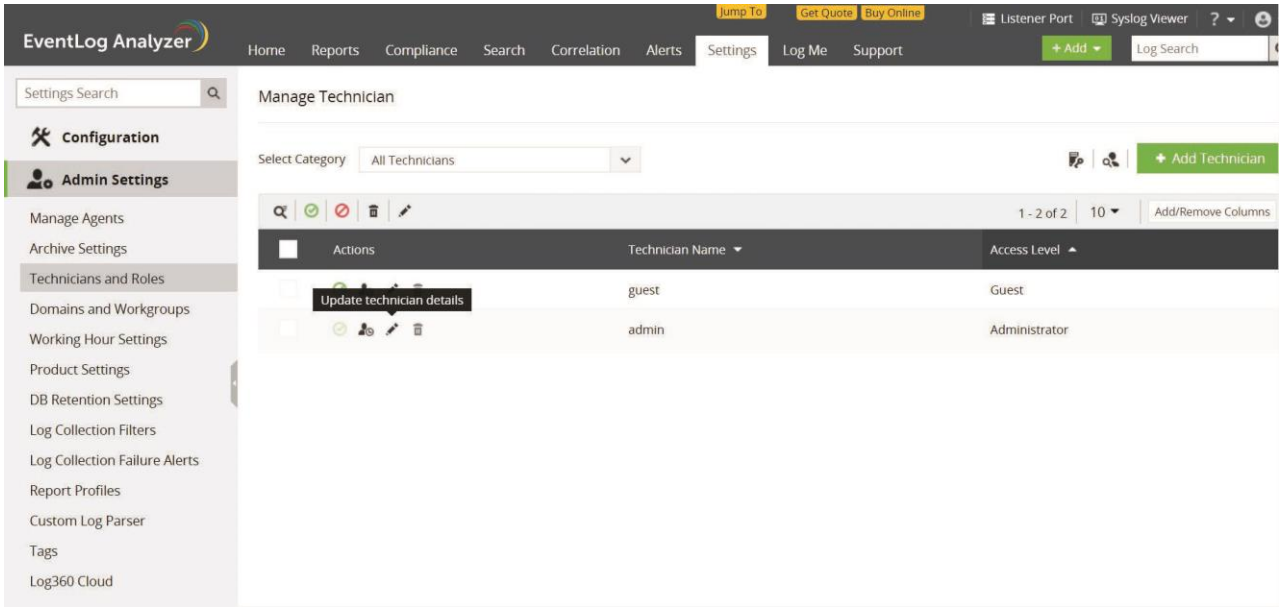
10 然后在 EventLog Analyzer 中，进入**设置> 归档> 设置，**提供确切的 UNC 路径，将归档日志数据的位置更改为公用共享文件夹。

11 您还需要更改自定义报表的存储位置。点击**设置> 管理设置> 产品设置。**在 **ELA 配置**页面，在*报表发送模式*字段中输入公用共享文件夹位置(UNC 路径)。

注意: *报表发送模式*字段应选择 发送邮件并保存。



12 邮件通知将发送到具有管理员权限的产品用户。改变 admin 用户的邮件地址，请点击**设置>管理设置>技术员和角色**。这将显示产品的技术人员及其相应的角色。点击 admin 用户的编辑按钮，打开*更新技术员明细*的对话框，在这里您可以编辑 admin 的邮件地址。



自动激活备份服务器的步骤

- 主服务器启动并运行时，在备份服务器中尝试启动 EventLog Analyzer 服务，该服务启动将会失败，但是这将会触发一个叫 **wscript.exe** 的进程，来开始监控主服务器的可用性。

- 一旦主服务器宕机，备用服务器将自动启动，电子邮件通知将立即发送给管理员。

- 主服务器宕机时进行故障排除。完成故障排除后，手动关闭备用服务器，然后启动主服务器。

- 当主服务器启动并运行时，执行步骤 1 在备用服务器中初始化脚本。

任何进一步的咨询，请联系 **mes@zohocorp.com.cn**.