ManageEngine
EventLog Analyzer

EventLog分析器：最佳实践指导

www.manageengine.cn/products/eventlog/

目录

本指南详细介绍了最佳实践，遵循这些最佳实践可确保顺利运行和最佳性能
EventLog Analyzer。

系统要求

硬件要求

日志管理解决方案是资源密集型的，选择正确的硬件起着
确保最佳性能方面发挥着重要作用。

下表显示了根据流程类型建议的硬件要求。

	低流量	正常流量	高流量
处理器内核	6	12	24
内存	16 GB	32 GB	64 GB
每秒输入/输出次数	150	750	1500 *
磁盘空间	1.2 TB	3 TB *	4 TB *
网卡容量	1 GB/秒	1 GB/秒	10 GB/秒
CPU 架构	64 位	64 位	64 位

笔记：

- 上述**值是近似值**建议先运行一个与生产环境类似的测试环境，并按照上表的设置细节进行操作。根据确切的流量和数据大小，可以对系统要求进行微调。

- 为了获得更高的 IOPS，我们可以使用 RAID 或 SSD。

使用下表确定您的实例的流量类型。

日志类型	大小（以字节为单位）	类别	日志单元 低流量 (每秒收益)	正常流量 (每秒收益)	高流量 (每秒收益)
Windows	900	Windows	300	1500	3000
Linux、HP、pfSense、瞻博网络	150	第 1 类 Syslog	2000	10000	20000
思科、Sonicwall、华为、Netscreen、Meraki、H3C	300	第 2 类 Syslog	1500	6000	12000
梭子鱼、Fortinet、Checkpoint	450	第 3 类 Syslog	1200	4000	7000
Palo Alto、Sophos、F5、Firepower 和其他系统日志	600	类型 4 Syslog	800	2500	5000

笔记：

- 单个安装服务器可以处理最多 3000 个 Windows 日志或任何高流量
  上表中提到的每种日志类型的流量值。
- 对于上表中未提及的日志类型，请根据以下情况选择适当的类别
  日志大小。例如，对于 SQL Server 日志，当字节大小为 900 字节时，EPS
  为 3000，则应视为高流量。
- 如果组合流量高于单个节点的处理能力，建议
  实施**分布式部署。**
- 如果需要高级威胁分析和大量
  已经使用了关联规则。

一般建议

虚拟机基础设施

- 为运行 EventLog Analyzer 的虚拟机分配 100% 的 RAM/CPU。共享内存
  /CPU 与同一主机上的其他虚拟机共享可能会导致 RAM/CPU 不足，并且可能
  对 EventLog Analyzer 的性能产生负面影响。
- 采用厚配置，因为精简配置会增加 I/O 延迟。对于 VMware，选择
  厚配置、积极归零和延迟归零的性能较低。
- 不建议启用虚拟机快照，因为主机会通过以下方式在多个块中复制数据：
  增加读写操作，导致 IO 延迟增加和性能下降。

CPU 和 RAM

- 为确保最佳性能，服务器 CPU 利用率应始终保持在 85% 以下。
- 应保留 50% 的服务器 RAM 供 Elasticsearch 以获得最佳性能。

磁盘

- 磁盘延迟极大地影响了 EventLog Analyzer 的性能。直连存储 (DAS)
  建议与具有接近零延迟和高吞吐量的 SSD 的吞吐量相当。
  企业存储区域网络 (SAN) 的速度比 SSD 更快。
- 目前 EventLog Analyzer 仅支持本地和远程（NAS）驱动器来存储实时
  搜索索引和档案数据。

补充说明：搜索索引需要快速随机访问索引文件，这是不可能的
使用 Blob 存储类型数据存储，例如 S3 和 Azure Blob 存储。

Web 浏览器

EventLog Analyzer 已测试支持以下浏览器和版本，且至少具有
1024x768 显示分辨率：

- **微软Edge**
- Firefox 4 及更高版本
- Chrome 8 及更高版本

数据库

EventLog Analyzer可以使用以下数据库作为其后端数据库。

与产品捆绑销售

- PostgreSQL

外部数据库

- Microsoft SQL 2012 及以上版本

请注意为 EventLog Analyzer 配置 MS SQL 数据库所需的硬件要求：

内存	中央处理器	每秒输入/输出次数	磁盘空间
8GB	6	300-500	300-500 GB

操作系统

EventLog Analyzer可以安装在运行以下操作系统和版本的机器上：

- Windows 7 及以上版本以及 Windows Server 2008 及以上版本
- Linux：Red Hat 8.0 及以上版本/RHEL、Mandrake/Mandriva、SUSE、Fedora 所有版本，CentOS、Ubuntu、Debian

安装服务器

- SIEM 解决方案需要大量资源。建议为其提供专用服务器
  最佳性能。
- Eventlog Analyzer 使用 Elasticsearch。Elasticsearch 进程预计会利用堆外内存
  以获得更好的性能。堆外内存由操作系统维护，并将释放
  必要时。

其他 Elasticsearch 节点建议

硬件	最低限度	受到推崇的
基本速度	2.4 GHz	3 GHz
核	12	16
内存	64	64
磁盘空间	1.2 TB	1.5 TB
每秒输入/输出次数	1500*	1500*

优化硬盘空间

硬盘空间占用的两个主要因素是数据库和存档文件。数据库（或索引文件包含最新的日志数据，可以报告和搜索，而存档文件包含较旧的历史日志数据。存档文件需要先加载到产品中，然后才能可供搜索或举报。

所需硬盘空间

存储日志所需的硬盘空间可以通过使用性能优化指南在 EventLog Analyzer 网站中

管理数据库大小

日志数据存储在数据库中，并定期压缩并存储在档案文件中。数据库中保留时间越长，所需的硬盘空间就越大，数据库性能。默认保留期为 32 天，可配置（设置 > 管理设置 > DB 保留设置）。最小化此值可获得最佳性能。

管理档案大小

存档文件会保留一段特定时间，然后被永久删除。因为它们甚至可以永久保存，存档文件夹的大小可能会无限增长。存档保留期限为永久保存，并可配置（设置 > 配置设置 > 查看存档文件 > 设置设置 > 管理设置 > 查看存档文件 > 设置）。还可以管理存档文件夹大小通过指定单独的专用驱动器作为存档位置，或手动将内容传输到磁带驱动器或大容量存储驱动器。

保护EventLog Analyzer

安装配置

安装和运行产品时使用的操作系统用户帐户必须相同，并且必须具有
对所有已安装文件夹和子文件夹的权限。虽然 root 帐户不需要
在Linux系统上使用，在Windows系统上，只需要使用默认的管理员账户。

用户配置

最好在 EventLog Analyzer Web 客户端中更改管理员和来宾用户帐户的默认密码（设置 > 管理员设置 > 管理技术人员）

SSL 认证

EventLog Analyzer 服务器-客户端通信可以使用 SSL（安全套接字层）协议进行保护。SSL 认证指南提供了有关如何获取 SSL 认证的详细步骤。

维护或升级

在进行任何维护或升级之前，请确保安装 EventLog Analyzer 的服务器关闭. 随后，进行备份。

数据库最佳实践

安全数据库

为了顺利无缝地安装，EventLog Analyzer 使用 MySQL 或 PostgreSQL
数据库默认 root/postgres 用户，无密码。建议为此用户分配密码
帐户以进一步保护数据库的安全。

对于 MS SQL，则不需要这样做，因为需要提供具有凭据的有效用户帐户
在安装过程中。

优化 PostgreSQL 数据库性能

要优化 PostgreSQL 数据库的性能：

- 停止EventLog Analyzer。
- 导航到 <EventLog Analyzer home>/pgsql/data/directory。
- 打开文件 postgres_ext.txt。
- 用下面提到的值替换参数的现有值。
- 保存并重新启动EventLog Analyzer。

范围	评论
共享缓冲区=128 MB	最低要求为 128 KB。
工作内存=12 MB	最低要求为 64 KB。
维护工作内存=100 MB	最低要求为 1 MB。
检查点段=15	每个日志文件段最小为 1 至 16 MB。
checkpoint_timeout=11 分钟	范围：30秒至1小时。
检查点完成目标=0.9	检查点目标持续时间为0.0 - 1.0。
顺序页成本=1.0	该参数以任意尺度来测量。
随机页面成本=2.0	该参数采用与上述相同的尺度来测量。
有效缓存大小=512MB	
同步提交=关闭	

优化 MySQL 数据库性能

要优化 MySQL 数据库的性能：

- 停止EventLog Analyzer。
- 导航到<EventLog Analyzer home>/bin。
- 打开文件 startDB.bat（如果是 Linux 机器，则打开 startDB.sh）。
- 将参数“--innodb_buffer_pool_size”的现有值替换为适合机器的 RAM 大小，如下表所示。例如，如果 RAM size为8GB，参数应为“--innodb_buffer_pool_size=3000M”。
- 保存并重新启动EventLog Analyzer。

RAM 大小	价值
1 GB	默认值（无需替换）
2 GB	1200米
3 GB	1500米
4GB	1500米
8 GB	3000米
16 GB	3000米

备份数据库

建议每两周备份一次 EventLog Analyzer 数据库，这样万一发生灾难，数据也不会丢失。数据库文件位于 <EventLog Analyzer home>/mysql 或 <EventLog Analyzer home>/pgsql 文件夹中，具体取决于版本号。要备份数据，请停止 EventLog Analyzer 服务，并复制该位置的所有文件和文件夹。这可以手动完成，也可以使用任何第三方备份软件。备份 MS SQL 数据库数据的过程可在此链接中找到。还建议保留存档文件的备份，存档文件位于 <EventLog Analyzer>/archive。如果从备份中恢复数据，请确保产品的版本号与备份时相同。

优化日志搜索性能

1. 为 Elasticsearch 提供足够的空间

为了确保公平的性能，请将堆与数据的比率保持在 1:60。这意味着您可以为 Elasticsearch 节点中的每 60GB 数据分配大约 1GB 的内存（堆）（最大比率）。但为了获得更好的性能，您可以降低此比率（即 1:30 优于 1:60）并提高速度。

笔记：在较旧的 Build 12320 中，空间与数据比为 1:30。

Elasticsearch 还使用文件系统缓存来提供更快的搜索。建议在 RAM 上留出足够的可用空间，相当于为 Elasticsearch 分配的堆内存。如果这不可行，请确保服务器 RAM 至少有 30% 是空闲的。操作系统将使用此空闲 RAM 来缓存 Elasticsearch 的索引，以提供更好的性能。

笔记：分配给 Elasticsearch 的空间不应超过 32GB。

例子：

假设我们有**100GB的搜索数据，**

那么 Elasticsearch 的空间大小至少应该为→ **100/30 ~ 4GB**

堆不足是导致多种性能问题的根本原因，例如：

- 日志处理/索引性能缓慢
- 缓存记录
- 搜索结果延迟
- 搜索失败

了解 Elasticsearch 中存储的数据总大小

Elasticsearch 可以在共享公共实例 (<ManageEngine>/elasticsearch/ES) 或本地实例中运行（<事件日志分析器>/ES）

确定Elasticsearch位置（ES目录）的步骤：

- 当 EventLog Analyzer 作为独立应用程序安装时（即，不通过 Log360 运行）本地 ES 将处于使用状态，位于**<事件日志分析器>\ES**目录。

- 如果 EventLog Analyzer 已与 Log360 一起安装，则默认 Elasticsearch 配置（通用 ES）将被使用，位于**<管理引擎>\elasticsearch\ES**目录。

检查 Elasticsearch 数据大小的步骤：

1. 导航至**<ES 目录 >\config。**
2. 打开**elasticsearch.yml**配置文件夹中的文件。
3. 寻找**路径数据**在此文件中设置。

导航到**路径数据**设置并检查文件夹的大小。

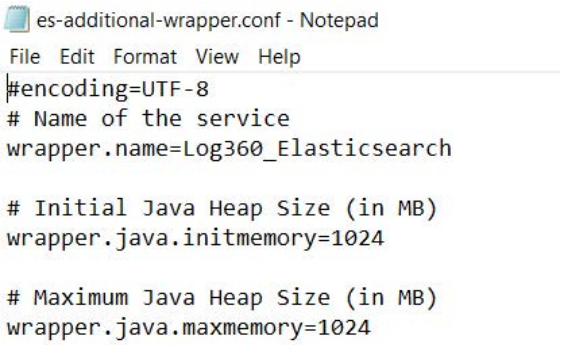
为了确保最佳性能，请定期监控和维护您的 Elasticsearch 数据，并限制单个ES节点大小在1.5TB-1.9TB之间。

笔记：在较旧的 Build 12320 中，ES 可以容纳 800GB-1.2TB 的数据。

调整堆（内存）的步骤：

1. 根据构建环境是独立版本还是捆绑版本，导航至 ES 目录构建（使用 Log360）。
2. 导航至**/ES/配置。**
3. 打开配置文件→ **es-additional-wrapper.conf**并查看堆大小。

笔记：确保登录的用户有写入权限。



4. 堆大小以 MB 为单位。

a. wrapper.java.initmemory 和 wrapper.java.maxmemory 都需要设置为相同的值。

这里设置为1024，即Elasticsearch的内存设置为（1024 MB/1024）= 1GB。

b. 如果必须增加到 25 GB，则我们需要将两个值都设置为 25 * 1024 = 25600

增加 ES 堆大小的步骤：

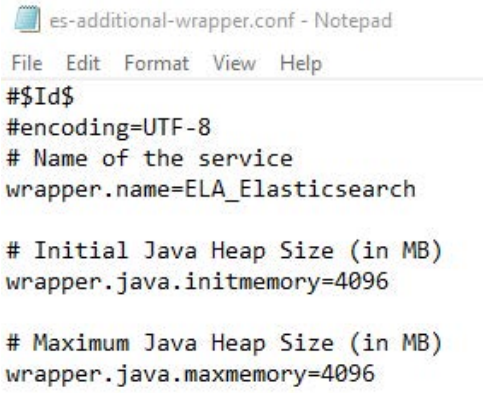
1.打开配置文件→ **es-additional-wrapper.conf**。

2. 编辑**包装器.java.initmemory**和**包装器.java.最大内存**值来增加堆大小。

3. 确保wrapper.java.initmemory和wrapper.java.maxmemory的值
否则产品将无法正常启动。

4. 如果产品正在运行，请通过以下方式停止 Elasticsearch：**ES/箱**然后运行**停止ES脚本**使用
管理员命令提示符或只是重新启动 EventLog Analyzer。这将重新启动 Elasticsearch
使用新的堆。

5. 如果**<管理引擎>\elasticsearch\ES**堆已更新，您需要手动运行
停止ES脚本命令来自**<ManageEngine>\elasticsearch\ES\bin**重启之前
EventLog 分析器。



笔记：

- 如果**内存不足**和**低内存**错误，Elasticsearch 堆将自动
扩展到机器可用 RAM 的三分之一。

- 值得注意的是，增加堆大小并不总是提高性能的解决方案。
除了堆之外，磁盘和 CPU 等其他因素也可能导致性能问题。确保
即系统要求得到满足。

- 定期监控内存使用情况也很重要，以确保系统正常运行
并根据需要调整设置。

- 请记住，增加 Elasticsearch 堆大小应经过深思熟虑
您的机器上的可用资源。

确保磁盘不是瓶颈：

如果服务器正在生成缓存记录（即日志处理速度很慢）或者搜索速度很慢，

然后你可以：

a. 使用更快的存储，如系统要求页。

b.检查存储数据的磁盘是否没有碎片。

c. 在**Windows 资源监视器，**您可以检查**磁盘**选项卡。如果**磁盘活动**显示**最高活跃时间**始终为 100%，则表明磁盘可能有问题或不够快。

2. 使用额外的搜索节点来分配搜索/索引负载以获得更好的性能

您可以使用**搜索引擎管理**Log360 中的功能（Log360 → 管理员 → SearchEngineManagement）添加额外的 Elasticsearch 节点来分发搜索和索引使用额外的机器加载。

a. 如果数据量对于单个节点来说太大，最好添加额外的节点来分散搜索/索引负载。

b.如果搜索性能不够好，则添加额外的节点。

c. 更多节点有助于更快地处理日志。

搜索的最佳实践：

- 在 Eventlog Analyzer 中，**保留期默认为 32 天**（可以增加**设置 → 数据库设置**在 UI 中）。如果更新为 90 天，则 32 天的数据将存储为实时数据，可以快速访问。超出此范围的数据将存储为冷数据，需要解压并加载到搜索引擎。因此，搜索超出实时数据的范围将比平时花费更多时间。

- 在搜索数据时，堆（分配给 Elasticsearch 的内存）和非堆（系统上的可用 RAM）都会被使用。系统上的可用 RAM 允许 Elasticsearch 更快地读取索引。因此，建议在服务器上保留至少与提供给 Elasticsearch 的堆相同的 RAM 量以获得更好的性能。如果这不可行，则确保服务器 RAM 的至少 30% 是可用的。操作系统将使用此可用 RAM 来缓存 Elasticsearch 的索引以提供更好的性能。

有必要拥有具有良好顺序和随机读取速度的磁盘，因为搜索过程涉及遍历大量文件，这是一项 IO 密集型操作。SSD 是首选，因为它可以减少 I/O 负载并且 I/O 等待并有助于充分利用 CPU 的能力。

支持最佳实践

创建支持信息文件 (SIF)

当需要支持时，创建一个支持信息文件 (SIF) 发送给支持团队 (eventloganalyzer-support@manageengine.com) 会很有帮助，而且可以节省时间。要从 Web 客户端创建 SIF，请转到产品的支持选项卡。单击“创建支持信息文件”，等待 30-40 秒，然后再次单击支持选项卡。单击下载并将下载的 SIF 发送给支持团队，或单击“上传到 FTP 服务器”，提供所需的详细信息并提交。如果服务器或 Web 客户端不工作，请压缩在 <EventLog Analyzer Home>/server/default/log 中找到的文件，然后在此 FTP 链接中上传 zip 文件。

关于EventLog Analyzer

EventLog Analyzer 是一款全面的 IT 合规性和 SIEM 日志管理软件。它以报告的形式提供对机器日志的详细洞察，以帮助缓解威胁，从而实现完整的网络安全。

关于ManageEngine

ManageEngine 提供实时 IT 管理工具，使 IT 团队能够满足组织对实时服务和支持的需求。全球有超过 60,000 家成熟和新兴企业（包括 60% 以上的财富 500 强企业）依靠 ManageEngine 产品来确保其关键 IT 基础设施（包括网络、服务器、应用程序、桌面等）的最佳性能。ManageEngine 是 Zoho Corp. 的一个部门，在美国、英国、印度、日本和中国等世界各地设有办事处。