在Winevent log事件时间和Splunk索引时间之间报告的索引延迟

适用范围

Splunk企业

描述

如何识别

首先确认事件时间(_time)与Splunk indextime(_indextime)之间的增量，然后根据受影响的索引和源类型修改以下内容。此示例正在查询安全通道事件日志记录：

```
index=<splunk_index> sourcetype="WinEventLog:Security" host=<splunk_forwarder>
| fields _time, _indextime, host
| eval delay=(_indextime - _time)/60
| timechart avg(delay) by host
```

调查

要验证的重要事项：

- 索引延迟首次出现是在什么时候？
- 在延迟首次出现时，部署的位置发生了哪些变化（如果有）？
- 延迟是否随时间增加（线性）或波动？

确认最大和平均每秒事件(eps)数：

```
index=_internal source=*metrics.log* security per_source_thruput host=<splunk_forwarder>
```

```
| timechart max(eps) max(max_age)
```

如果延迟随时间变化，则高EPS值可能表示数据吞吐量的瓶颈。

分辨率

快速修复

此选项仅适用于想要获取当前事件而不关心缺少历史数据的情况。对于每个问题转发器，必须逐个执行以下步骤：

1. 在$SPLUNK_HOME\etc\system\local\inputs.conf中设置`current_only = 1`:

```
[WinEventLog://Security]
current_only = 1
```

2. 停止转发器
3. 重命名过时的检查点文件：

```
ren "C:\Program Files\SplunkUniversalForwarder\var\lib\splunk\modinput\WinEventLog\Securit
```

4. 启动转发器
5. 确保生成新的安全检查点文件
6. 确认检查点和安全日志相互之间具有几百个事件
7. 重命名`$SPLUNK_HOME\etc\system\local\inputs.conf`文件以将`current_only=1`设置恢复为默认值。
8. 重新启动Splunk
9. 搜索以确认数据正在接收

为什么执行常规UF重启不太可能有所帮助

重新启动UF会强制它重新读取检查点并短暂地清空内存缓冲区。由于事件生成速率超过处理/吞吐量限制，转发器将在重新启动后的几分钟内立即重新开始累积延迟。

长期解决方案

快速修复方案需要对每个受影响的UF进行手动干预，这在大型部署中通常是不可行的（并且某些管理员没有命令行访问UF）。除此之外，UF很有可能再次落后。您的最佳选择可能是提供长期解决方案。由于每个环境都不同，因此没有简单的设置可以应用于每个场景。但是，此知识库中的建议应适用于许多使用案例。本文中的所有配置建议都要求在UF上重新启动Splunk才能生效，因此请确保已选中部署服务器上的自定义应用重新启动Splunkd。

首先尝试此操作(limits.conf)

打开maxKBps

在调整以下选项之前，请查看`limits.conf/[thruput]maxKBps`。UF的默认设置为256KB/s，这限制了转发器每天的网络传输总量约为22 GB。繁忙的生成安全日志的服务器很容易产生256 KB/s以上的流量，这使得转发器实际上无法跟上。

所以，首先：在`limits.conf`中将此值设置为0（无限制），以取消网络带宽限制：

```
[thruput]
maxKBps = 0
```

由于大多数通用转发器正在通过电话回传到部署服务器，最佳实践是通过部署应用设置此配置，以便所有转发器一次接收它（如果可能，首先在测试环境中，然后在生产环境中）。 如果测试环境不可用，另一个选择是部署到包含小批UF的“测试”服务器类并监控之后再应用到任何地方。这同样适用于此知识库文章中提供的所有建议。

其它选项

如果打开转发器的推动力不足以完全解决问题，请考虑以下因素：

特定于`inputs.conf/[WinEventLog://Security]`

选项#1 — 更改批大小

默认情况下，Splunk会抓取小批中的事件（10个事件），并频繁更新磁盘上的检查点文件。在繁忙的主机上，检查点文件上的磁盘I/O成为主要的阻塞点。设置`batch_size = 500`，将磁盘同步延迟到600秒(`checkpointInterval = 600`)，以及设置`suppress_checkpoint = true`显着增加了`splunk-winevtlog.exe`的EPS（每秒事件）吞吐量。

```
batch_size = 500
suppress_checkpoint = true
checkpointInterval = 600
```

选项#2 — 使用renderXML减少API调用的数量

默认情况下，Splunk为事件中的每个字段发出API调用。相反，启用renderXml将针对每个事件发出API调用，这有可能提高性能：[以XML显示Windows事件日志事件]

```
renderXml = true
```

选项#3 — 过滤抑制哪些字段以减少数据负载

该选项对原始速度有效，但是请确保它符合审核要求（如果适用）。

这些设置在发送前从原始事件中删除报头字段，以减少字节大小和API呈现调用。如果其SIEM、CIM模型或合规性控制面板依赖`Keywords`（例如，Audit Success/Failure）、`TaskCategory`或`Opcode`，则丢弃这些字段将中断这些检测。

```
suppress_sourcename = true
suppress_keywords = true
suppress_type = true
suppress_task = true
suppress_opcode = true
```

选项#4 — 在输入模式下启用FormatMessage()API

`evtFormatMessage()`是大多数Windows部署中的默认API，与之前的FormatMessage()API相比，前者增加了处理开销。恢复到旧的API可能会缓解索引延迟。

如果**renderXml = true**，则不要设置此值。传统FormatMessage() API仅在解析经典纯文本多行日志(renderXml = false)时速度更快，因为它绕过繁重的evtFormatMessage() DLL字符串查找。使用renderXml = true时，Splunk已经以结构化格式直接从现代EVTX API(EvtRender)读取，而不调用消息格式化DLL。

```
use_old_eventlog_api = true
```

增加UF接收管道(server.conf)

默认情况下，转发器运行单个解析和接收管道。对于接收较重事件量的多核计算机，可以增加流水线集以允许并行处理。这会控制转发器使用多少个内部线程从本地Windows API读取数据、打包数据并将其推送到网络。

在UF上，与索引器或重转发器相比，将摄入管道1增加到2的资源占用空间非常轻便，因为UF仅执行轻量读取、批处理和网络输出（无正则表达式转换、字段提取或到磁盘的索引）。

如果Windows服务器至少具有4个CPU核心和8 GB RAM，则设置parallelIngestionPipelines = 2通常是安全的，可以显着帮助清除大量事件积压并防止未来延迟。CPU使用率可能会在UF被捕获时增加，但是一旦摄入恢复正常水平，CPU使用率将再次下降。

```
[general]
parallelIngestionPipelines = 2
```

Outputs.conf队列大小

如果将输入批处理调整为500，请考虑确保TCP输出队列具有足够的内存缓冲区，以便网络层不会阻止输入工作进程：

```
[tcpout:myindexers]
maxQueueSize = 50MB
```

检查Windows Defender/防病毒例外项

安全终结点代理（例如，Defender、CrowdStrike、Carbon Black）可以主动检查`splunk-winevtlog.exe`并锁定`$SPLUNK_HOME\var\lib\splunk\modinput\WinEventLog\`目录。请确保从实时文件系统检查中排除整个`$SPLUNK_HOME`目录和`splunk-winevtlog.exe`。

域控制器相关性/网络路由：

如果问题UF在域控制器上运行或处理高Active Directory流量，请确保没有本地防火墙或网络速率限制将Splunk TCP端口（默认`9997`）限制在接收层（HF或索引器）上。

相关链接

- Splunk文档：
  - 使用Splunk Enterprise监控Windows事件日志数据
  - 通用转发器的高级配置
  - 规格文件：server.conf、inputs.conf、outputs.conf
- Splunk知识库文章
  - 排除UF或HF延迟日志故障
  - UF未向Splunk发送安全日志
- Splunk Lantern文章：性能调整转发层

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。