配置高级流量收集器引擎自定义安全事件触发行为

目录

[简介](#)

[背景](#)

[自定义安全事件调试](#)

[默认流量收集器行为](#)

[cse_exec_interval_secs高级设置](#)

[性能影响](#)

- [测量classify_flows线程的持续时间](#)
- [性能期间的引擎状态](#)
- [SFI — 静态流索引](#)

[配置](#)

[确认更改](#)

[Congratulations!](#)

简介

本文档介绍两个流量收集器高级设置，这些设置可以更改SNA流量收集器触发自定义安全事件(CSE)的方式。

背景

传统early_check_age流量收集器高级设置以及新的cse_exec_interval_secs流量收集器高级设置确定流量收集器引擎触发自定义安全事件的方式。 流量收集器是SNA系统架构中第一个查看网络流量的设备，因此流量收集器引擎负责在流量缓存中监控流量的特性，并确定流量是否满足给定自定义安全事件的配置标准。 但是，这些流量收集器高级设置不会更改任何内置核心安全事件的触发特性。

自定义安全事件调试

在SNA 7.5.0及更高版本中，debug_custom_events流量收集器高级设置已增强以提供不同级别的调试

- debug_custom_events 1（调试最少 — 旨在能够在生产中运行，并深入了解生成CSE的确切流）
- debug_custom_events 2（更多调试）
- debug_custom_events 3（最详细的调试）

默认流量收集器行为

默认情况下，流量收集器early_check_age advanced设置配置为160秒。 这意味着流量收集器引擎在检查流量是否与配置的自定义安全事件匹配之前，至少要等待160秒进入该流量。 默认情况下，在流结束之前不会再次进行此检查。

之所以选择此160秒早期检查值，是因为如果使用最佳实践，必须将遥测导出器配置为每60秒发送一次遥测。 此默认值允许流量收集器在典型环境中有足够的时间查看与给定会话/流量两端相关的流量信息。 因此，early_check_age未在高级设置列表中预先定义。 这是有意设计的，未经咨询支持/工程，不得更改此值。 但是，当考虑较长且比较安静的流特性以及涉及字节或数据包计数的累积的自定义安全事件配置时，这种初始设计并不能很好地发挥作用。 这是创建cse_exec_interval_secs高级设置参数的原因。

cse_exec_interval_secs高级设置

在7.4.2中增加了cse_exec_interval_secs流量收集器高级设置，现在可指示引擎根据已配置的自定义安全事件定期检查其流量缓存中的流。 此高级设置对于长流特别有用，在长流中，给定流在默认160秒early_check_age的CSE标准上不匹配，但在流中较晚超过该阈值。 如果没有此高级设置，自定义安全事件在流结束之前不会触发，有时可能几天后才会触发。

性能影响

执行这些间隔CSE条件检查流生命中的流次数比默认值定义的流次数多，这确实需要更多CPU。 这些说明将指导您研究流量收集器引擎上的sw.log文件的内容，以在启用cse_exec_interval_secs参数之前确定性能基线。 如果您正在考虑启用此高级设置，并且希望TAC协助确认您的流量收集器运行状况以准备此更改，可以通过打开支持案例并将流量收集器诊断包附加到SR来完成。

测量classify_flows线程的持续时间

您可以执行的一项快速性能影响评估是从今天开始调查sw.log，并将激活设置之前“cf-”日志条目后列出的数字与应用设置之后的数字进行比较。

/lancope/var/sw/today/logs/grep "cf-" sw.log

20:43:21 I-flo-f0:classify_flows:流n-1744317 ns-178613 ne-188095 nq-0 nd-0 nx-0至–300 cf-21 ft-126473/792802/940383/14216

20:44:20 I-flo-f4:classify_flows:流n-1754296 ns-191100 ne-167913 nq-0 nd-0 nx-0至–300 cf-20 ft-122830/783378/949392/14928

20:44:21 I-flo-f2:classify_flows:流n-1773175 ns-191930 ne-169039 nq-0 nd-0 nx-0至–300 cf-20 ft-123055/788507/962264/15431

20:44:21 I-flo-f3:classify_flows:流n-1750066 ns-189197 ne-165940 nq-0 nd-0 nx-0至–300 cf-20 ft-122563/779792/944192/15154

20:44:21 l-flo-f5:classify_flows:流n-1753899 ns-190477 ne-168004 nq-0 nd-0 nx-0至–300 cf-20 ft-122261/783375/946651/15423

20:44:21 l-flo-f1:classify_flows:流n-1763952 ns-191342 ne-169518 nq-0 nd-0 nx-0至–300 cf-20 ft-122782/786822/955997/15175

20:44:21 l-flo-f7:classify_flows:流n-1757535 ns-188154 ne-166221 nq-0 nd-0 nx-0至–300 cf-20 ft-122808/781388/951528/14363

20:44:21 l-flo-f6:classify_flows:流n-1764211 ns-190964 ne-169013 nq-0 nd-0 nx-0至–300 cf-21 ft-122713/784446/954149/16320

20:44:21 l-flo-f0:classify_flows:流n-1764197 ns-189780 ne-168784 nq-0 nd-0 nx-0至–300 cf-21 ft-123290/787327/952186/14352

20:45:22 l-flo-f4:classify_flows:流n-1780277 ns-177512 ne-149843 nq-0 nd-0 nx-0至–300 cf-21 ft-129553/766777/964933/14864

20:45:22 l-flo-f2:classify_flows:流n-1789285 ns-175763 ne-155809 nq-0 nd-0 nx-0至–300 cf-21 ft-129685/772482/976850/15289

20:45:22 l-flo-f3:classify_flows:流n-1774883 ns-177085 ne-149715 nq-0 nd-0 nx-0至–300 cf-22 ft-129067/764272/962000/15090

20:45:22 l-flo-f5:classify_flows:流n-1775998 ns-176898 ne-150682 nq-0 nd-0 nx-0至–300 cf-22 ft-128835/768374/963353/15347

20:45:22 l-flo-f1:classify_flows:流n-1786441 ns-175776 ne-151846 nq-0 nd-0 nx-0至–300 cf-22 ft-129255/770212/970360/15129

cf条目代表“Classify Flows”。 这表示线程通过它负责的Flow Cache部分所花费的秒数。 它位于“分类流”线程中，CSE应用于该流。 如果您看到这些数字在启用该功能后上升，这是衡量对性能整体影响的良好指标。

在添加此高级间隔设置后，预计会出现上升，但如果此数值接近60,请删除该设置，因为影响太大。 预计会增加几秒钟，并且认为很合理。

性能期间的引擎状态

您可以进行的另一个性能“before vs after”衡量方法是查看sw.log文件中的“Performance Period”部分，该部分每5分钟记录一次，以衡量该设置对流处理的影响。 您也可以使用grep来查找这些块。 如果引擎不堪重负，则必须禁用此高级设置间隔检查。

/lancope/var/sw/today/logs/ grep -A3 "性能周期" sw.log

注意除“引擎状态正常”以外的任何状态。

诸如“引擎状态输入速率过高”之类的状态表示classify_flows线程占用的CPU过多。

SFI — 静态流索引

表示分类线程无法通过流缓存完成它们的传递：它代表“静态流索引”，它表示分类流线程中存在挣扎。这本身并不是灾难，但它表明引擎开始达到极限，在当前cf级别下，性能开始下降。

sw.log:16:09:49 l-flo-f1:classify_flows:sfi:base(8388608)(10522745 ->
11014427)max(16777215)cod(1)(491681/8388608)---------->(5%)
sw.log:16:09:49 l-flo-f3:classify_flows:sfi:base(25165824)(27269277 ->
27754304)max(33554431)cod(1)(485026/8388608)---------->(5%)
sw.log:16:09:49 l-flo-f4:classify_flows:sfi:base(33554432)(35652656 ->
36138422)max(41943039)cod(1)(485765/8388608)---------->(5%)
sw.log:16:09:49 l-flo-f2:classify_flows:sfi:base(16777216)(18985626 ->
19499308)max(25165823)cod(1)(513681/8388608)---------->(6%)
sw.log:16:09:54 l-flo-f0:classify_flows:sfi:base(0)(1786480 ->
421161)max(8388607)cod(1)(7023288/8388608)---------->(83%)
sw.log:16:10:49 l-flo-f0:classify_flows:sfi:base(0)(421161 ->
1402189)max(8388607)cod(0)(981027/8388608)---------->(11%)
sw.log:16:10:49 l-flo-f2:classify_flows:sfi:base(16777216)(19499308 ->
17522620)max(25165823)cod(0)(6411919/8388608)---------->(76%)
sw.log:16:10:49 l-flo-f1:classify_flows:sfi:base(8388608)(11014427 ->
8976309)max(16777215)cod(0)(6350489/8388608)---------->(75%)
sw.log:16:10:49 l-flo-f3:classify_flows:sfi:base(25165824)(27754304 ->
25702968)max(33554431)cod(0)(6337271/8388608)---------->(75%)
sw.log:16:10:49 l-flo-f7:classify_flows:sfi:base(58720256)(58848913 ->
59630528)max(67108863)cod(0)(781614/8388608)---------->(9%)
sw.log:16:10:49 l-flo-f4:classify_flows:sfi:base(33554432)(36138422 ->
34064015)max(41943039)cod(1)(6314200/8388608)---------->(75%)
sw.log:16:10:49 l-flo-f5:classify_flows:sfi:base(41943040)(43310891 ->
44059251)max(50331647)cod(1)(748359/8388608)---------->(8%)
sw.log:16:10:49 l-flo-f6:classify_flows:sfi:base(50331648)(51714170 ->
52444661)max(58720255)cod(1)(730490/8388608)---------->(8%)
sw.log:16:11:49 l-flo-f5:classify_flows:sfi:base(41943040)(44059251 ->
42121104)max(50331647)cod(0)(6450460/8388608)---------->(76%)
sw.log:16:11:49 l-flo-f0:classify_flows:sfi:base(0)(1402189 ->
2373792)max(8388607)cod(1)(971602/8388608)---------->(11%)
sw.log:16:11:49 l-flo-f6:classify_flows:sfi:base(50331648)(52444661 ->
50483491)max(58720255)cod(1)(6427437/8388608)---------->(76%)
sw.log:16:11:49 l-flo-f3:classify_flows:sfi:base(25165824)(25702968 ->
26385879)max(33554431)cod(1)(682910/8388608)---------->(8%)
sw.log:16:11:49 l-flo-f1:classify_flows:sfi:base(8388608)(8976309 ->
9662167)max(16777215)cod(1)(685857/8388608)---------->(8%)
sw.log:16:11:49 l-flo-f4:classify_flows:sfi:base(33554432)(34064015 ->
34742593)max(41943039)cod(1)(678577/8388608)---------->(8%)
sw.log:16:11:50 l-flo-f7:classify_flows:sfi:base(58720256)(59630528 ->
60298366)max(67108863)cod(1)(667837/8388608)---------->(7%)
sw.log:16:11:50 l-flo-f2:classify_flows:sfi:base(16777216)(17522620 ->

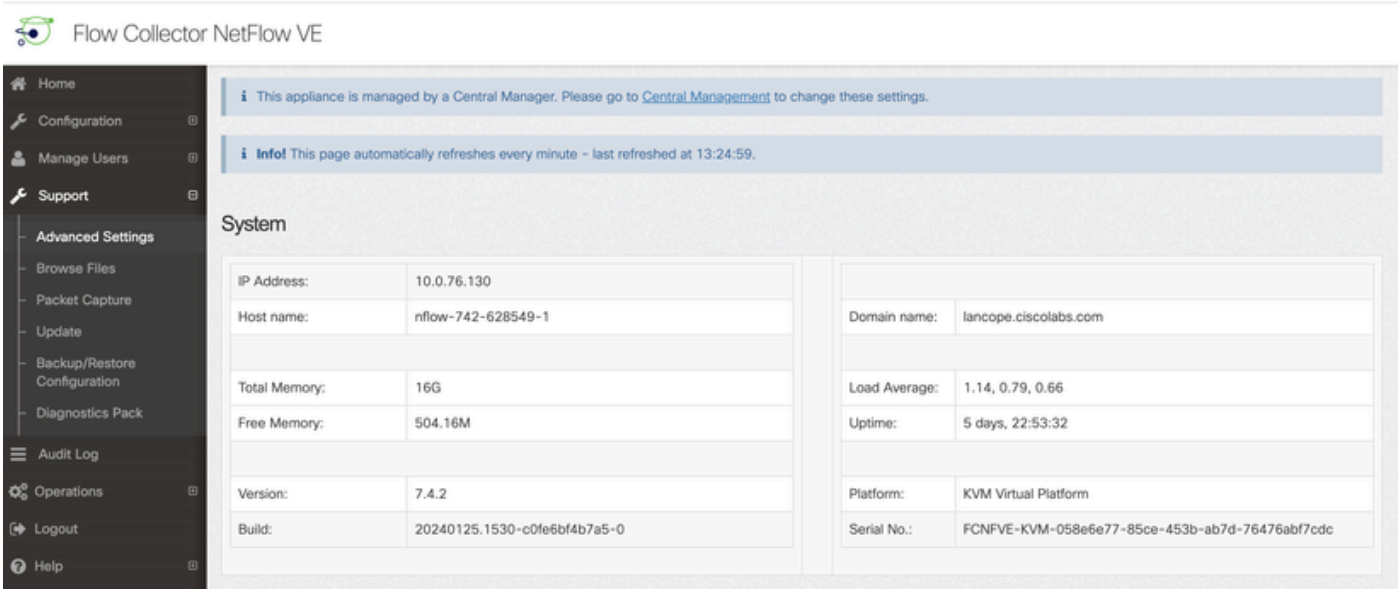
18202249)max(25165823)cod(1)(679628/8388608)---------->(8%)

配置

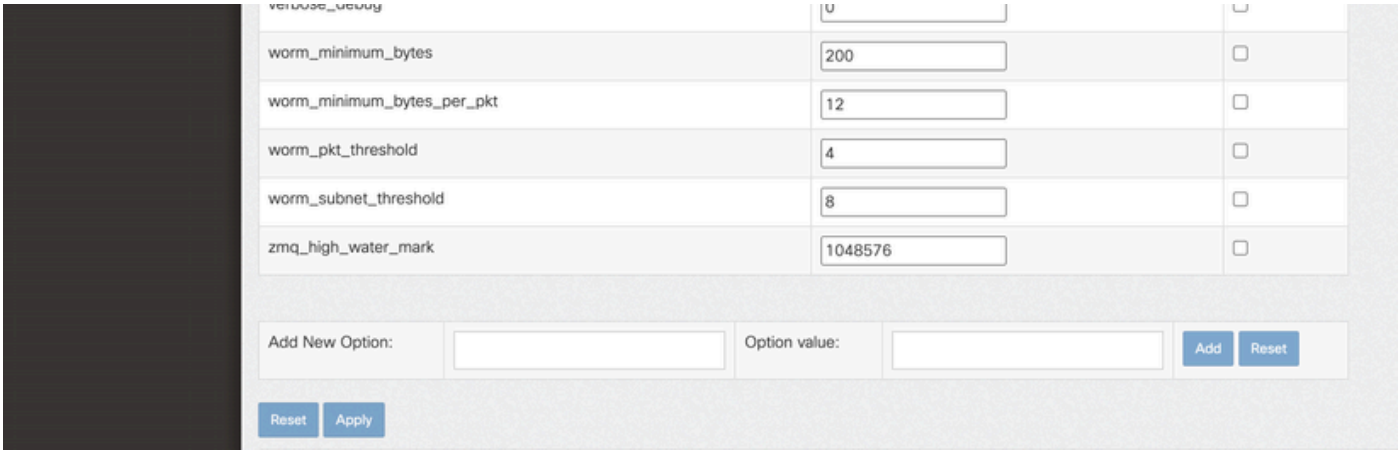
打开Web浏览器并直接导航到流量收集器设备IP。 以本地管理员用户身份登录。



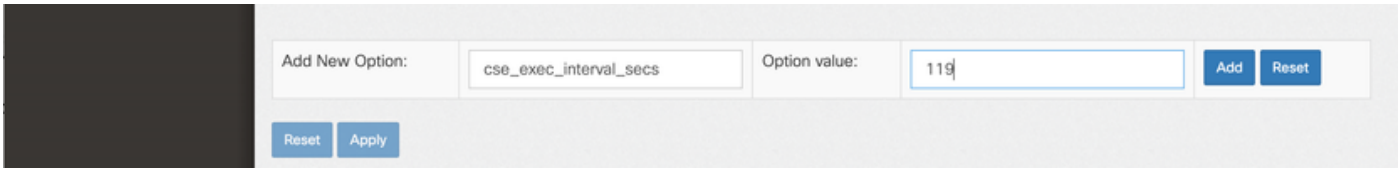
导航至Support（支持）— > Advanced Settings（高级设置）



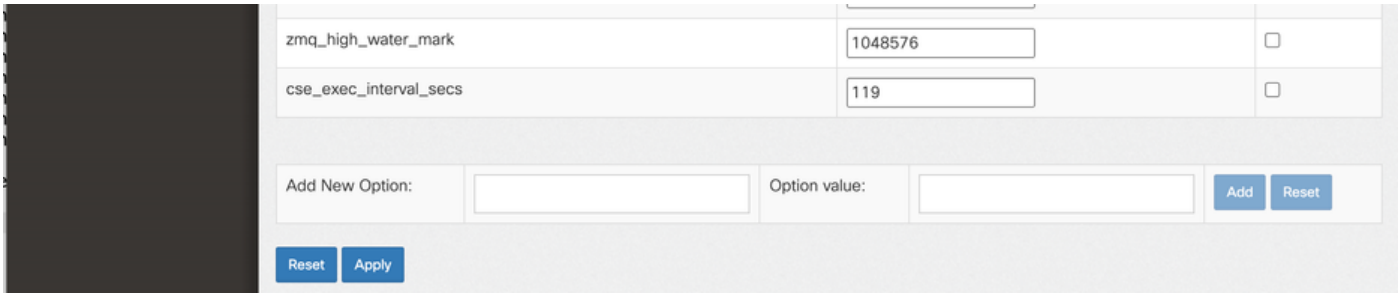
向下滚动Advanced Setting（高级设置）屏幕，显示列表底部的Add New Option（添加新选项）配置框



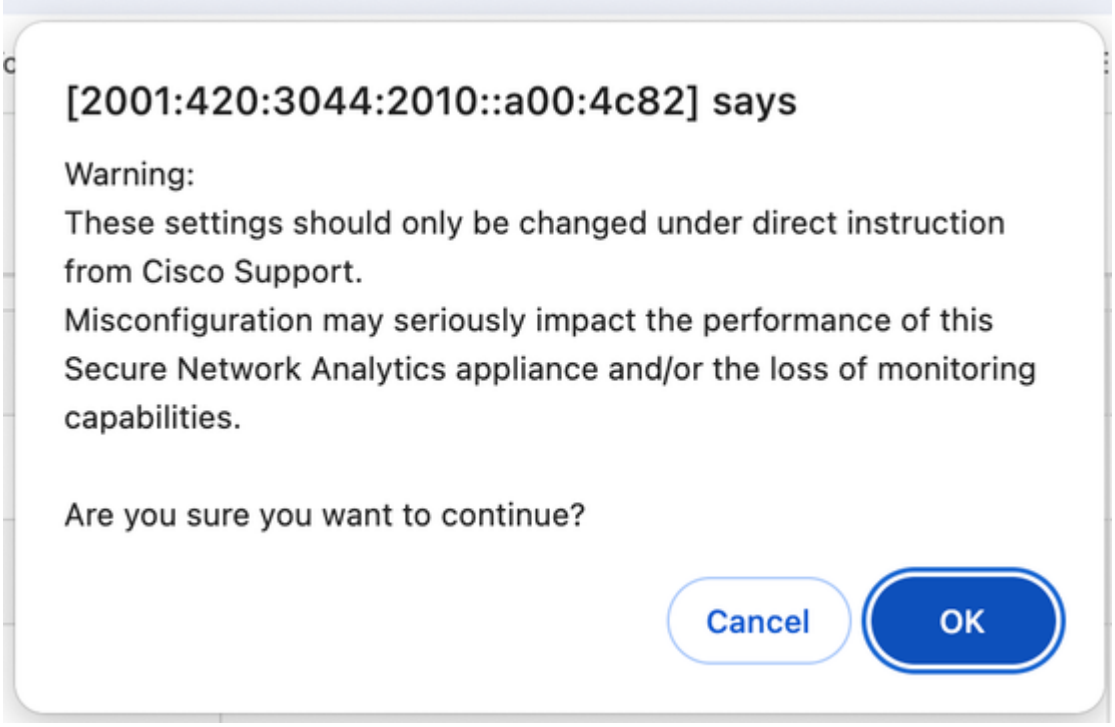
在添加新选项：编辑框中输入cse_exec_interval_secs，并在Option value:编辑框输入119。 编辑这些框将启用添加按钮。 在添加新选项中输入cse_exec_interval_secs后，按Add按钮：选项值中的编辑框和119:编辑框。



添加新选项：和选项值：编辑框清除以准备在要输入多个新Advanced Settings的情况下输入另一个条目。 新添加的Advanced Settings会在列表底部进行添加时进行标记。 这样用户就可以检查该条目。 Advanced Setting的准确拼写与案例一样重要。 所有高级设置都以小写形式显示。



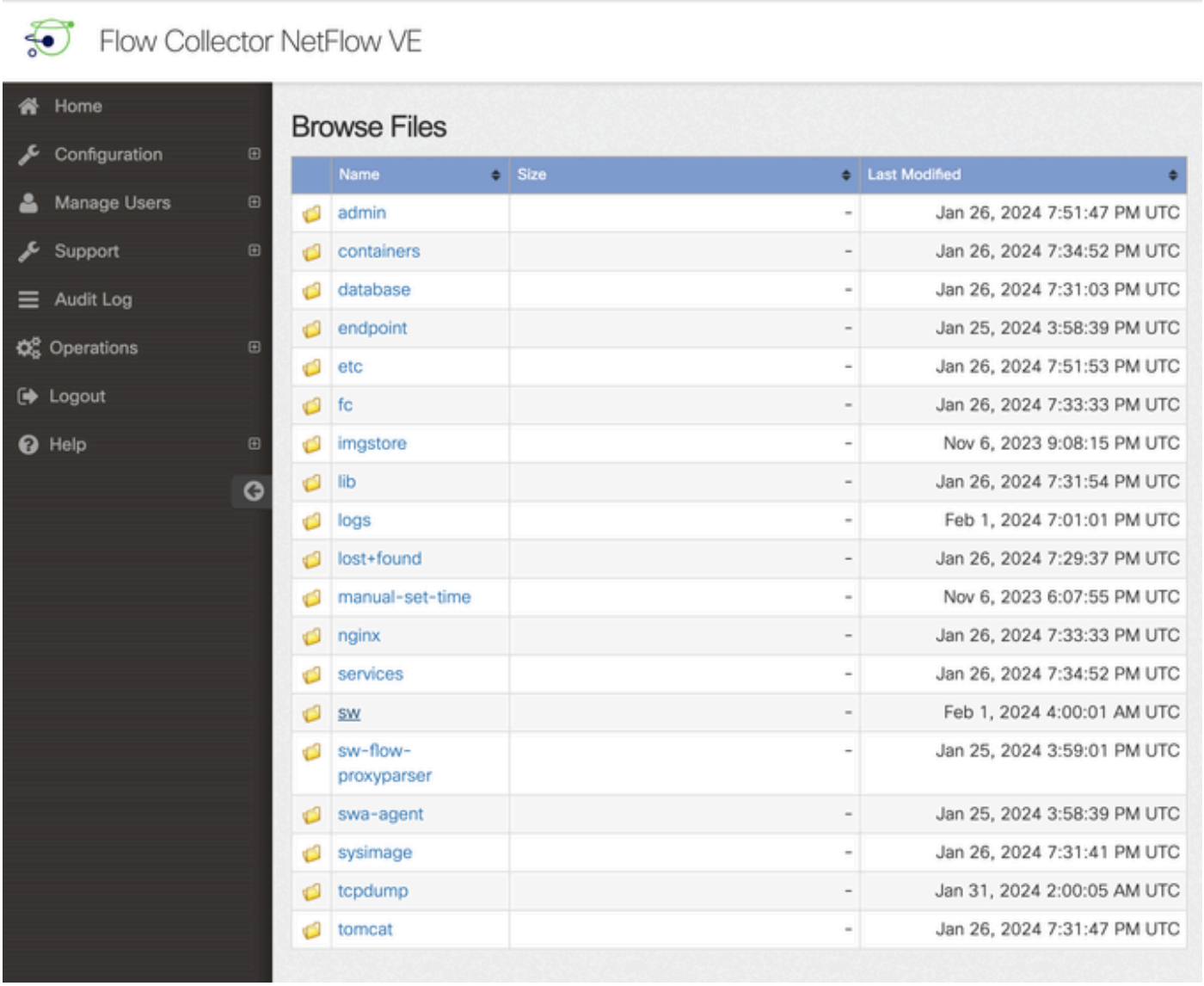
正确输入Advanced Setting后，请按Apply按钮。 请注意，有时Apply按钮未启用。 要启用它，请点击添加新选项：编辑框，然后单击Apply按钮。 出现此弹出窗口时，按“确定”按钮以提交新的高级设置和值。



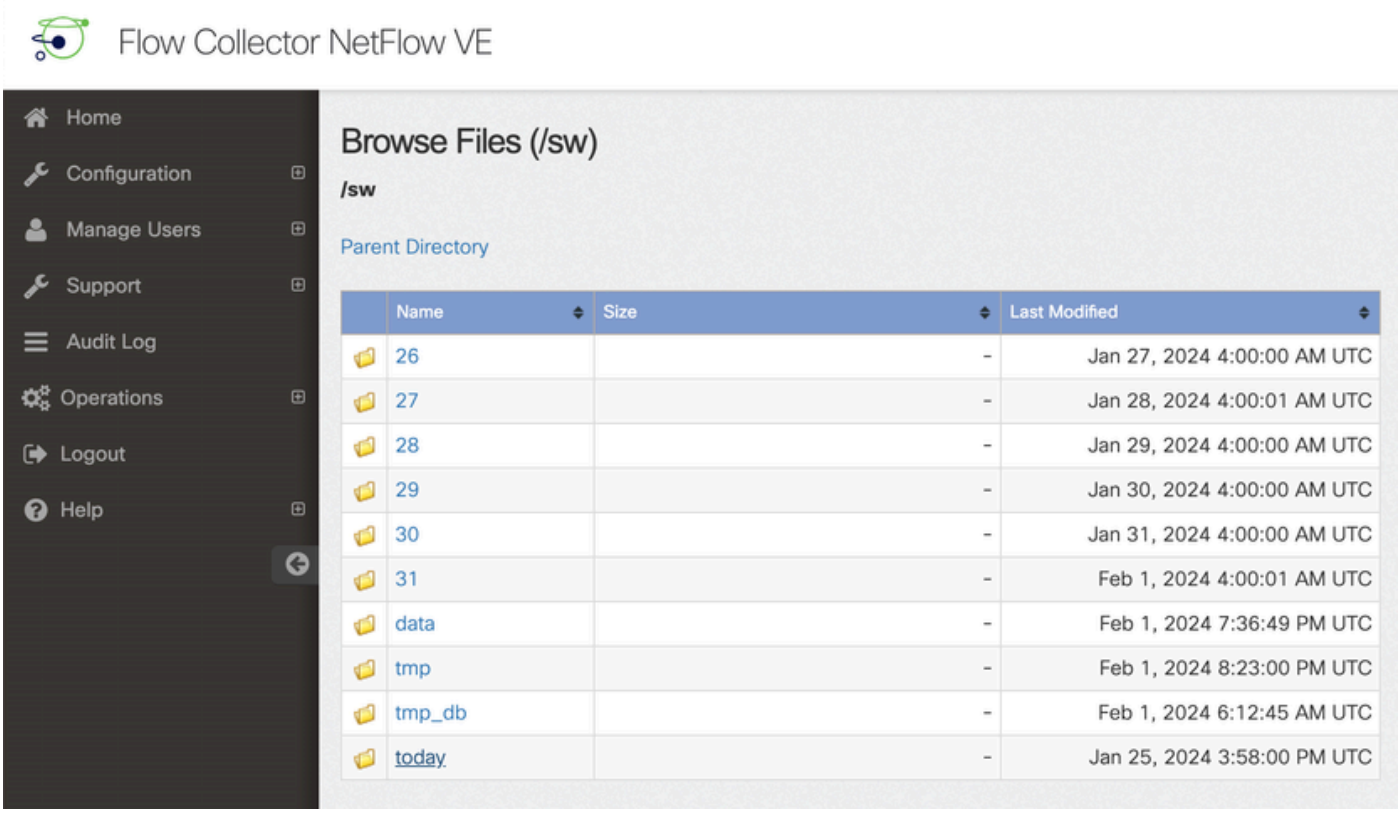
确认更改

此最终验证是最重要的。再次单击Support菜单并选择Browse Files。

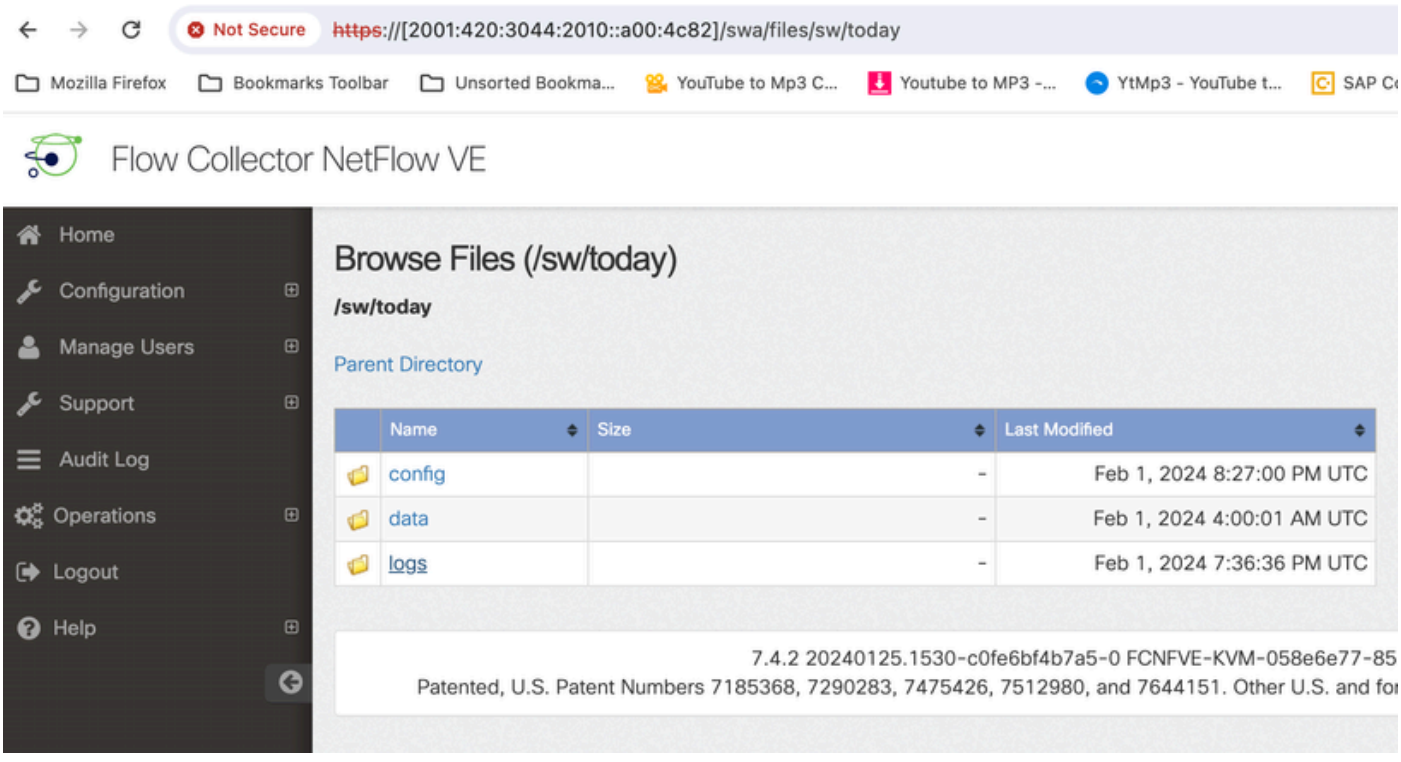
这会将您引导到FC上的文件系统。点击sw。


Flow Collector NetFlow VE
Home
Configuration
Manage Users
Support
Audit Log
Operations
Logout
Help
Browse Files
Name
Size
Last Modified
admin - Jan 26, 2024 7:51:47 PM UTC
containers - Jan 26, 2024 7:34:52 PM UTC
database - Jan 26, 2024 7:31:03 PM UTC
endpoint - Jan 25, 2024 3:58:39 PM UTC
etc - Jan 26, 2024 7:51:53 PM UTC
fc - Jan 26, 2024 7:33:33 PM UTC
imgstore - Nov 6, 2023 9:08:15 PM UTC
lib - Jan 26, 2024 7:31:54 PM UTC
logs - Feb 1, 2024 7:01:01 PM UTC
lost+found - Jan 26, 2024 7:29:37 PM UTC
manual-set-time - Nov 6, 2023 6:07:55 PM UTC
nginx - Jan 26, 2024 7:33:33 PM UTC
services - Jan 26, 2024 7:34:52 PM UTC
sw - Feb 1, 2024 4:00:01 AM UTC
sw-flow-proxyparser - Jan 25, 2024 3:59:01 PM UTC
swa-agent - Jan 25, 2024 3:58:39 PM UTC
sysimage - Jan 26, 2024 7:31:41 PM UTC
tcpdump - Jan 31, 2024 2:00:05 AM UTC
tomcat - Jan 26, 2024 7:31:47 PM UTC

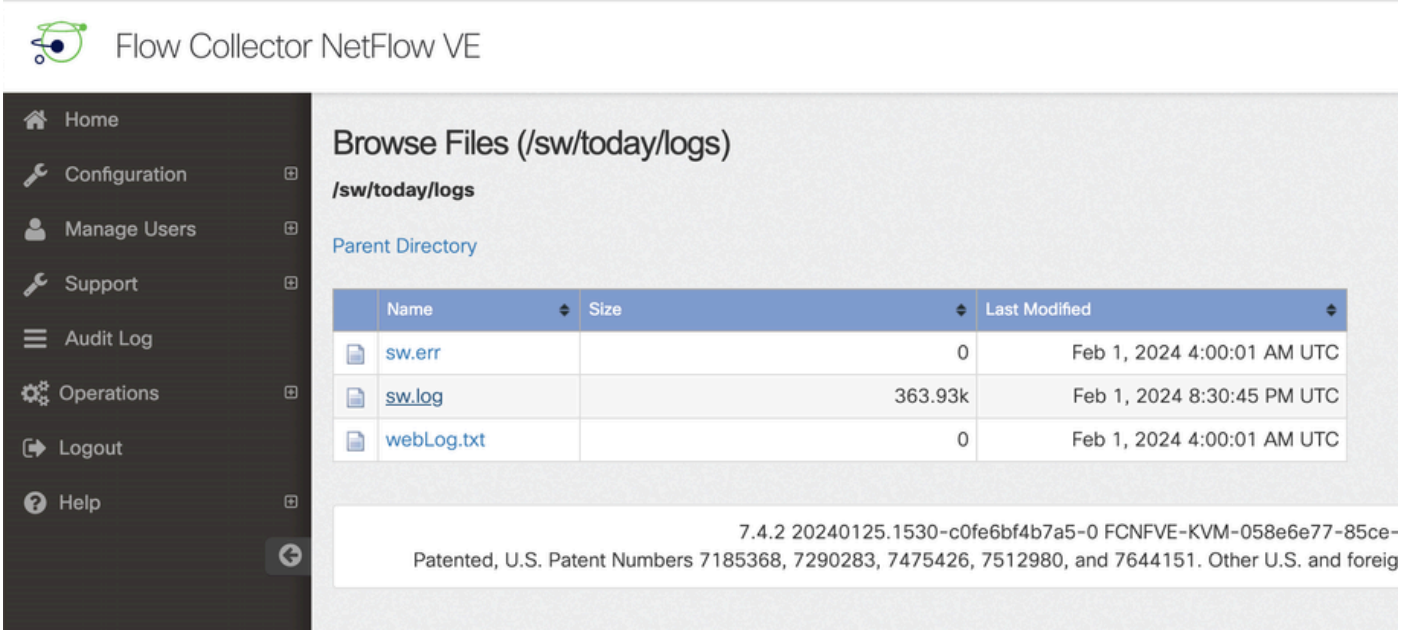
立即点击



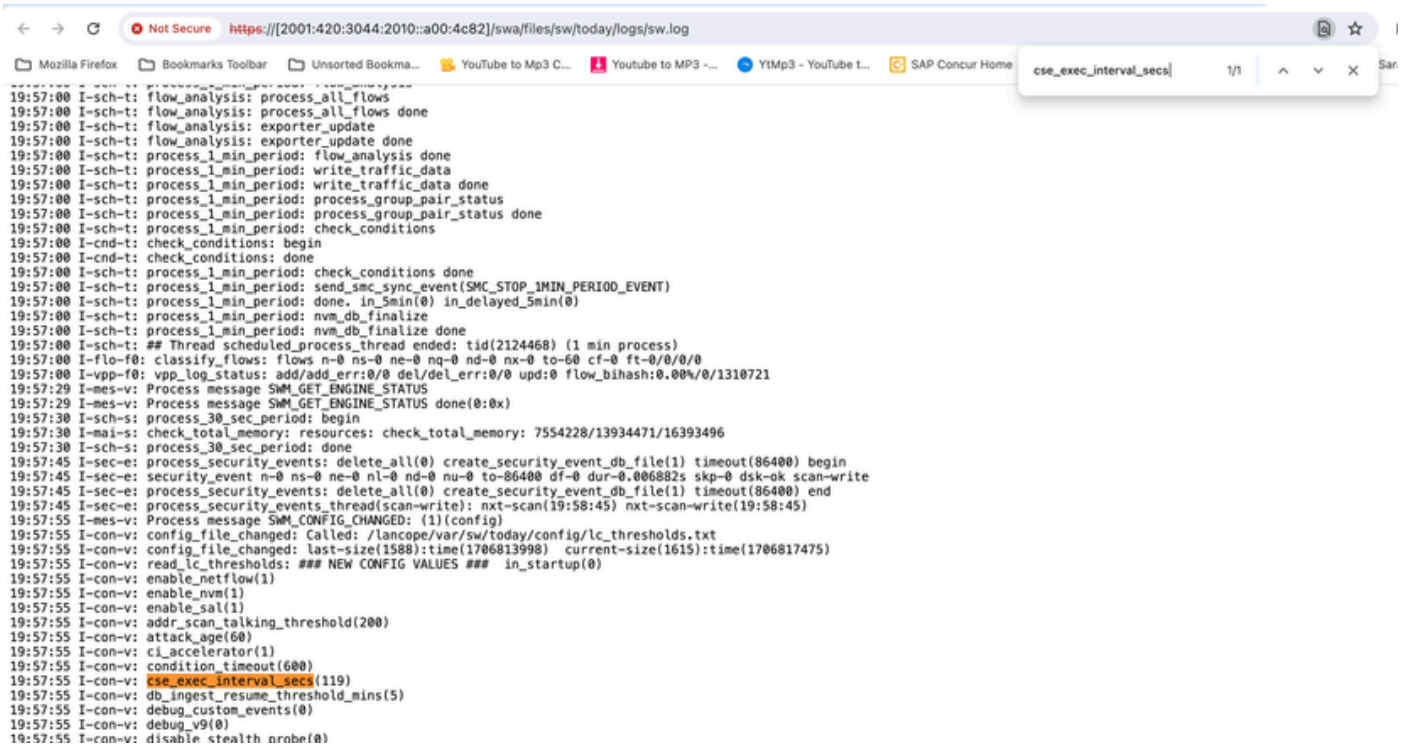
单击logs。



单击sw.log



在浏览器页面中执行搜索，在搜索框中输入cse_exec_interval_secs以查找Advanced Setting



已接受的高级设置如屏幕截图所示列出。

未接受的值按如下所示列为“不是输入配置的一部分”，在本例中，这是由于用户错误拼写了设置所致。这就是为什么在进行此类配置更改后必须检查日志的原因。

```
20:41:52 I-con-v: read_lc_thresholds: ### NEW CONFIG VALUES ###  in_startup(0)
20:41:52 I-con-v: enable_netflow(1)
20:41:52 I-con-v: enable_nvm(1)
20:41:52 I-con-v: enable_sal(1)
20:41:52 I-con-v: addr_scan_talking_threshold(200)
20:41:52 I-con-v: attack_age(60)
20:41:52 I-con-v: ci_accelerator(1)
20:41:52 I-con-v: condition_timeout(600)
20:41:52 I-con-v: (cse_exec_interval_sec) not part of input configuration
20:41:52 I-con-v: cse_exec_interval_secs(119)
```

Congratulations!

您刚刚输入了一个新的高级设置，并已验证引擎是否接受了该设置。

现在，启用该功能可在流到达early_check_age(默认为160秒)后大约每2分钟对流运行CSE逻辑。

如果CSE规则涉及累积一段时间的字节计数，此功能将改进CSE在与所定义的标准匹配的流上触发的时序。

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）。