安全终端Linux连接器故障排除18

目录

简介

本文档介绍安全终端Linux连接器上的故障18。

故障18：连接器事件监控超载

行为保护引擎提高了连接器对系统活动的可视性。随着可视性的提高，连接器的系统活动监控可能会被系统上的活动量所淹没.如果发生这种情况，连接器将引发故障18并进入降级模式。有关故障18的详细信息，请参阅Cisco安全终端Linux连接器故障文章。在Linux连接器上， status 命令可用于安全终端Linux CLI，以查看连接器是否以降级模式运行，以及是否出现任何故障。如果发生故障18，则运行 status 命令Linux CLI显示故障，其严重性可能为以下两种之一：

1. 故障18（严重性为严重）

```
ampcli> status
Status:                  Connected
Mode:                    Degraded
Scan:                    Ready for scan
Last Scan:               2023-06-19 02:02:03 PM
Policy:                  Audit Policy for FireAMP Linux (#1)
Command-line:            Enabled
Orbital:                 Disabled
Behavioural Protection: Protect
Faults:                  1 Major
Fault IDs:      18
                ID 18 - Major: Connector event monitoring is overloaded. Investigate the most acti
```

2. 故障18（严重性为严重）

```
ampcli> status
```

```
Status:                 Connected
Mode:                   Degraded
Scan:                   Ready for scan
Last Scan:              2023-06-19 02:02:03 PM
Policy:                 Audit Policy for FireAMP Linux (#1)
Command-line:           Enabled
Orbital:                Disabled
Behavioural Protection: Protect
Faults:                 1 Critical
Fault IDs:      18
                ID 18 - Critical: Connector event monitoring is overloaded. Investigate the most a
```

连接器事件监控超载：严重性

当以严重性引发故障18时，这意味着连接器事件监视超载，但仍可以监视较小的一组系统事件。连接器可切换为主要严重性，监控的事件少于早于1.22.0的连接器中所提供的监控。如果系统事件泛洪时间较短，并且事件监控负载下降回可接受的范围，则清除故障18，连接器重新开始监控所有系统事件。如果系统事件的泛洪变差，并且事件监控负载增加至临界量，则故障18将升高为严重性级别，并且连接器将切换到严重严重级别。

连接器事件监控超载：严重性

当故障18严重性为严重时，这意味着连接器所经历的系统事件数量极大，将连接器置于风险之中。连接器切换为更严格的严重性临界连接器。在此状态下，连接器仅监控关键事件，以允许连接器进行清理并专注于恢复。 如果事件泛洪最终减少回更可接受的范围，则故障将完全清除，连接器将恢复监控所有系统事件。

故障操作指南

如果连接器出现过严重程度为严重或严重的故障18，则必须采取一些步骤来调查和解决该问题。解决故障18的步骤因故障出现的时间和原因而异：

1. Linux连接器的全新安装引发了故障18
2. 故障18是在最近对操作系统进行更改后引发的
3. 故障18是自发发出的

4. 故障18是在重新调配已安装Linux连接器的计算机或将连接器更新到版本1.22.0+时引发的

案例1：全新安装

如果在全新安装Linux连接器时观察到故障18和降级模式，则必须首先确保系统满足最低系统要求。在验证要求是否符合或超过最低要求后，如果故障仍然存在，您必须调查系统上最活跃的进程。您可以使用 top 命令（或类似）。 如果已知消耗最多的CPU的进程是良性的，则可以创建新的进程排除项来排除这些进程被监控。

示例 情景:

假设全新安装后，通过安全终端Linux CLI显示故障18和降级模式。R运行 top Ubuntu计算机中的命

令显示以下活动进程：

```
Tasks: 223 total,   5 running, 218 sleeping,   0 stopped,   0 zombie
%Cpu(s): 29.4 us, 34.3 sy,  0.0 ni, 36.2 id,  0.0 wa,  0.0 hi,  0.1 si,  0.0 st
MiB Mem :   7943.0 total,   3273.9 free,   2357.6 used,   2311.5 buff/cache
MiB Swap:   2048.0 total,   2048.0 free,      0.0 used.   5141.2 avail Mem

    PID USER      PR  NI    VIRT    RES    SHR S  %CPU  %MEM     TIME+ COMMAND
  34896 user1     20   0   18136   3292   3044 R  96.7   0.0   0:04.89 trusted_process
   4296 user1     20   0  823768  52020  38900 R  48.0   0.6   0:10.90 gnome-terminal-
    117 root      20   0       0      0      0 I  12.3   0.0   0:01.86 kworker/u64:6-events_unbound
  34827 root      20   0       0      0      0 I  10.3   0.0   0:00.47 kworker/u64:2-events_unbound
   1880 user1     20   0  353080 101600  70164 S   6.3   1.2   0:30.37 Xorg
  34576 root      20   0       0      0      0 R   6.3   0.0   0:01.46 kworker/u64:1-events_unbound
   2089 user1     20   0 3939120 251332 104008 S   3.0   3.1   0:23.25 gnome-shell
    132 root      20   0       0      0      0 I   1.3   0.0   0:02.67 kworker/2:2-events
   6951 root      20   0 1681560 213536  74588 S   1.3   2.6   0:41.30 ampdaemon
    741 root      20   0  253648  13352   9280 S   0.3   0.2   0:01.54 polkitd
    969 root      20   0  153600   3788   3512 S   0.3   0.0   0:00.36 prlshprint
   2291 user1     20   0  453636  29388  20060 S   0.3   0.4   0:03.75 prlcc
      1 root      20   0  169608  13116   8524 S   0.0   0.2   0:01.95 systemd
      2 root      20   0       0      0      0 S   0.0   0.0   0:00.01 kthreadd
      3 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_gp
      4 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 rcu_par_gp
      5 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 slub_flushwq
      6 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 netns
      8 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 kworker/0:0H-events_highpri
     10 root       0 -20       0      0      0 I   0.0   0.0   0:00.00 mm_percpu_wq
```

我们看到有一个非常活跃的进程，称为 trusted_process 在本例中。在本例中，我熟悉此流程，而且受信任，因此没有理由对此流程产生怀疑。要清除故障18，可以将受信任的进程添加到门户中的进程排除项中。 请参阅配置和识别Cisco安全终端排除文章，了解创建排除的最佳实践。

案例2：最近更改

如果最近对操作系统进行了更改（例如安装新程序），则如果这些新更改增加了系统活动，则可能会出现故障18和降级模式。使用全新安装中概述的相同补救策略但是，案例会查找与最近更改相关的进程，例如新安装的程序运行的新进程。

案例3：恶意活动

行为保护引擎会增加受监控的系统活动类型。这使连接器对系统有了更广阔的视角，并具备检测更复杂行为攻击的能力。但是，对大量系统活动的监控也会使连接器面临更大的拒绝服务(DoS)攻击风险。如果连接器系统活动过多，进入故障为18的降级模式，它仍会继续监控系统关键事件，直到整体系统活动减少。 系统事件可见性的这种损失降低了连接器保护您计算机的能力。 请务必立即调查系统是否存在恶意进程。请使用 top 命令（或类似命令）查看当前活动的进程，并在发现任何可能存在的恶意进程时采取适当措施进行补救。

案例4：连接器要求

行为保护引擎可提高连接器保护计算机活动的能力，但是要这样做，它必须比先前版本消耗更多的资源。如果故障18频繁发生，则说明没有良性进程造成大量负载，并且计算机上似乎不存在任何恶意进程，您必须确保系统满足最低系统要求。

另请参阅

- 使用安全终端Mac/Linux CLI
- 思科安全终端Linux连接器故障
- 配置和确定思科安全终端例外项
- 安全终端用户指南(PDF)

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）。