安全終端Linux聯結器故障排除18

目錄

簡介

本文檔介紹安全終端Linux聯結器上的故障18。

故障18：聯結器事件監控超載

行為保護引擎提高了聯結器對系統活動的可視性。隨著可視性的增加，聯結器的系統活動監控可能會被系統上的活動量所淹沒.如果發生這種情況，聯結器將引發故障18並進入降級模式。有關故障18的詳細資訊，請參閱Cisco安全終端Linux聯結器故障文章。在Linux聯結器上， status 命令可用於Secure Endpoint Linux CLI，檢視聯結器是否正在降級模式下運行以及是否出現了任何故障。如果引發故障18，則運行 status 命令在Secure Endpoint Linux CLI中顯示故障，其嚴重性可能是以下兩種之一：

1. 故障18（嚴重性為嚴重）

```
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（嚴重性為嚴重）

```
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
```

聯結器事件監控超載：嚴重性

當以嚴重程度引發故障18時，這意味著聯結器事件監控超載，但仍然能夠監控較小的一組系統事件。聯結器切換到嚴重級別並監視較少事件，這些事件等效於在早於1.22.0的聯結器上可用的監視。如果系統事件的泛洪較短，並且事件監視負載減小到可接受的範圍，則清除故障18，聯結器恢復監視所有系統事件。如果系統事件的泛洪變差，並且事件監視負載增加至臨界量，則故障18將升高至臨界嚴重性，並且聯結器將切換至臨界嚴重性。

聯結器事件監視超載：嚴重性

如果故障18的嚴重程度為嚴重，則意味著聯結器正在經歷數量龐大的系統事件，將聯結器置於風險之中。聯結器切換成更嚴格的嚴重性。在此狀態下，聯結器僅監控關鍵事件，以允許聯結器進行清理並專注於恢復。 如果事件泛洪最終減小到更可接受的範圍，那麼故障將完全清除，聯結器將恢復監控所有系統事件。

故障操作指南

如果聯結器曾引發嚴重或嚴重程度為故障18，則必須採取一些步驟來調查和解決該問題。根據故障出現的時間和原因，解決故障18的步驟有所不同：

1. Linux聯結器的全新安裝引發了故障18
2. 故障18是在最近對作業系統進行更改後出現的
3. 故障18是自發發出的

4. 在重新調配已安裝Linux聯結器的電腦或將聯結器更新到1.22.0+版時引發了故障18

案例1：全新安裝

如果在全新安裝的Linux聯結器上觀察到故障18和降級模式，則必須首先確保系統滿足最低系統要求。在驗證要求是否符合或超過最低要求後，如果故障仍然存在，您必須調查系統上最活躍的進程。您可以使用 top 命令（或類似命令）。 如果已知佔用最高CPU量的進程是良性的，則可以建立新的進程排除項以排除那些進程不受監視。

範例情境：

假設在全新安裝之後，通過Secure Endpoint Linux CLI顯示故障18和降級模式。R運行 top ubuntu電

腦中的命令顯示以下活動進程：

```
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
```

我們看到有一個非常活躍的流程，稱為 trusted_process 在本例中。在這種情況下，我熟悉這個過程，而且它值得信任，我沒有理由懷疑這個過程。要清除故障18，可將受信任的進程新增到門戶中的進程排除中。 請參閱配置和確定思科安全終端排除一文，瞭解建立排除的最佳實踐。

案例2：最近更改

如果最近對作業系統進行了更改（例如安裝新程式），則如果這些新更改增加了系統活動，則會出現故障18和降級模式。使用全新安裝中概述的相同補救策略但是，請查詢與最近更改相關的進程，如新安裝的程式運行的新進程。

案例3：惡意活動

行為保護引擎會增加受監控的系統活動型別。這使聯結器對系統有更廣闊的視角，並具備檢測更複雜行為攻擊的能力。但是，對大量系統活動的監控也會增加聯結器遭受拒絕服務(DoS)攻擊的風險。如果接頭系統活動過多，並進入故障為18的降級模式，它仍會繼續監控系統嚴重事件，直到整體系統活動減少。 系統事件可見性的損失降低了聯結器保護電腦的能力。 請立即調查系統是否存在惡意進程，這一點非常重要。使用 top 命令（或類似命令）來檢視當前活動的進程，並在發現任何可能惡意的進程時採取適當措施進行補救。

案例4：聯結器要求

行為保護引擎可提高聯結器保護電腦活動的能力，但要想這樣做，它必須消耗比先前版本更多的資源。如果故障18頻繁發生，則沒有良性進程導致高負荷，並且電腦上似乎沒有任何惡意進程，則必須確保系統滿足最低系統要求。

另請參閱

- 使用安全終端Mac/Linux CLI
- Cisco安全終端Linux聯結器故障
- 配置和確定思科安全終端排除
- 安全終端使用手冊(PDF)

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。