Secure Endpoint Linuxコネクタの障害のトラブルシューティング18

内容

はじめに

このドキュメントでは、Secure Endpoint Linuxコネクタの障害18について説明します。

障害18：コネクタイベント監視が過負荷です

動作保護エンジンは、コネクタのシステムアクティビティに対する可視性を向上させます。このように可視性が向上すると、コネクタのシステムアクティビティ監視がシステムのアクティビティ量によって圧倒される可能性が高くなりますを参照。これが発生すると、コネクタは障害18を発生させ、縮退モードに入ります。障害18の詳細については、「Cisco Secure Endpoint Linux Connectorの障害」を参照してください。Linuxコネクタでは、 status コマンドをSecure Endpoint Linux CLIで使用して、コネクタが縮退モードで動作しているかどうか、およびエラーが発生しているかどうかを確認できます。障害18が発生した場合は、 status コマンドをSecure Endpoint Linux CLIで実行すると、次のいずれかの重大度でエラーが表示されます。

1. 障害18（重大な重大度）

```
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. 障害18 (重大な重大度)

```
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
```

コネクタイベント監視が過負荷です：重大な重大度

重大な重大度で障害18が発生した場合は、コネクタイベント監視が過負荷になっているものの、比較的小さなシステムイベントのセットを監視できることを意味します。コネクタはメジャーな重大度に切り替わり、1.22.0よりも前のコネクタで使用可能だったモニタリングと同等のイベントよりも少ないイベントをモニタリングします。システムイベントのフラッドが短く、イベントモニタリングの負荷が許容範囲内まで減少した場合、障害18がクリアされ、コネクタはすべてのシステムイベントのモニタリングを再開します。システムイベントのフラッディングが悪化し、イベントモニタリングの負荷がクリティカルなレベルまで増加した場合、障害18がクリティカルな重大度で起動し、コネクタがクリティカルな重大度に切り替わります。

コネクタイベント監視が過負荷です：重大な重大度

重大な重大度で障害18が発生した場合、これはコネクタに過剰なシステムイベントが発生しており、コネクタが危険にさらされていることを意味します。コネクタがより限定的な重大度に切り替わります。この状態では、コネクタは重大なイベントのみを監視し、コネクタがクリーンアップしてリカバリに集中できるようにします。 イベントのフラッディングが最終的により許容可能な範囲まで減少した場合、障害は完全にクリアされ、コネクタはすべてのシステムイベントの監視を再開します。

障害対応ガイダンス

コネクタで重大度がmajorまたはcriticalのエラー18が発生する場合は、問題を調査して解決するためにいくつかの手順を実行する必要があります。障害18を解決する手順は、障害がいつ、なぜ発生したかによって異なります。

1. 障害18は、Linuxコネクタの新規インストール時に発生しました
2. 障害18は、オペレーティングシステムに対する最近の変更の後に発生しました
3. フォールト18は自然に発生しました

4. Linuxコネクタがすでにインストールされているマシンを再プロビジョニングするか、コネ

クタをバージョン1.22.0+に更新すると、障害18が発生します

ケース1：新規インストール

Linuxコネクタの新規インストールで障害18およびデグレードモードが発生する場合、最初にシステムが最小システム要件を満たしていることを確認する必要があります。要件が最小要件を満たしているか、それを超えていることを確認した後、障害が続く場合は、システム上で最もアクティブなプロセスを調査する必要があります。Linuxシステム上の現在アクティブなプロセスを表示するには、 top コマンド（または類似のコマンド）を実行します。 最も多くのCPUを消費しているプロセスが良性であることが判明している場合は、新しいプロセス除外を作成して、それらのプロセスを監視から除外できます。

サンプル シナリオ:

新規インストール後に、障害18および縮退モードがSecure Endpoint Linux CLIを介して表示されたとします。Rを実行 top コマンドをUbuntuマシンで実行すると、次のアクティブプロセスが表示されます。

```
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
```

非常にアクティブなプロセスがあり、 trusted_process この例の場合は.この場合、私はこのプロセスに精通しており、それが信頼されており、私がこのプロセスを疑う理由はありません。障害18をクリアするために、信頼できるプロセスをポータルのプロセス除外に追加できます。 除外を作成する際のベストプラクティスについては、「Cisco Secure Endpoint除外の設定と特定」を参照してください。

ケース2：最近の変更

新しいプログラムのインストールなど、オペレーティングシステムに対して最近の変更を行った場合、これらの新しい変更によってシステムアクティビティが増加すると、fault 18およびdegradedモードが発生することがあります。新規インストールと同じ修復戦略を使用します。ただし、新しくインストールされたプログラムによって実行される新しいプロセスなど、最近の変更に関連するプロセスを探します。

ケース3：悪意のあるアクティビティ

動作保護エンジンは、監視するシステムアクティビティの種類を増やします。これにより、コネクタはシステムをより広い視野で捉え、より複雑な動作攻撃を検出できるようになります。ただし、より多くのシステムアクティビティを監視すると、コネクタがサービス拒否(DoS)攻撃にさらされるリスクも高くなります。コネクタがシステムアクティビティで過負荷になり、障害18で縮退モードに入った場合でも、システムアクティビティ全体が低下するまで、システムの重要なイベントを監視し続けます。 システムイベントの可視性が失われると、マシンを保護するコネクタの機能が低下します。 悪意のあるプロセスがないか、システムをすぐに調査することが重要です。 top コマンド（または類似のコマンド）をLinuxシステムで実行して、現在アクティブなプロセスを表示し、悪意のある可能性のあるプロセスが特定された場合に状況を修復するための適切な措置を講じます。

ケース4：コネクタの要件

動作保護エンジンは、マシンアクティビティを保護するコネクタの機能を改善しますが、そのためには以前のバージョンよりも多くのリソースを消費する必要があります。エラー18が頻繁に発生し、負荷の大きい問題を引き起こす良性プロセスがなく、マシン上で動作している悪意のあるプロセスがないと思われる場合は、システムが最小システム要件を満たしていることを確認する必要があります。

以下も参照のこと

- セキュアエンドポイントMac/Linux CLIの使用
- Cisco Secure Endpoint Linuxコネクタの障害
- Cisco Secure Endpointの除外の設定と特定
- セキュアエンドポイントユーザガイド(PDF)

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。