Sourcefire アプライアンスの過剰なディスク使用率のトラブルシューティング

内容

概要

FireSIGHT Management Center または Firepower アプライアンスは、さまざまな理由でディスク容量を使い果たしてしまうことがあります。この事態が発生すると、高いディスク使用率によりヘルス アラートがトリガーされるか、ソフトウェア アップデートの試行が失敗することがあります。この記事では、過剰なディスク使用率の根本原因と、いくつかのトラブルシューティング手順について説明します。

確認手順

高使用率のパーティションを判別します。次のコマンドは、ディスク使用率を示します。

FireSIGHT Management Centerでは –

```
admin@3DSystem:~# df -TH
```

7000および8000シリーズアプライアンスおよびNGIPS仮想デバイスでは、

```
> show disk
```

どちらのコマンドも、次のような出力を示します。

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/sda5 2.9G 566M 2.2G 21% /
```

```
/dev/sda1 99M 16M 79M 17% /boot
/dev/sda7 52G 8.5G 41G 18% /Volume
none 11G 20K 11G 1% /dev/shm
/dev/sdb1 418G 210M 395G 1% /var/storage
```

注：ディスクのサイズと使用率は、さまざまなアプライアンスモデルによって異なります。NGIPS仮想デバイスの場合は、パーティションのサイズが最小ディスク領域要件に準拠していることを確認します。

注意：上記に示されていない追加パーティションはサポートされていません。

7000および8000シリーズアプライアンスおよびNGIPS仮想デバイスでは、次のコマンドを実行して、詳細なディスク使用率の統計情報を表示できます。

```
> show disk-manager
```

出力例：

```
> show disk-manager
Silo Used Minimum Maximum
Temporary Files 143.702 MB 402.541 MB 1.572 GB
Action Queue Results 0 KB 402.541 MB 1.572 GB
Connection Events 17.225 GB 3.931 GB 23.586 GB
User Identity Events 0 KB 402.541 MB 1.572 GB
UI Caches 587 KB 1.179 GB 2.359 GB
Backups 0 KB 3.145 GB 7.862 GB
Updates 13 KB 4.717 GB 11.793 GB
Other Detection Engine 0 KB 2.359 GB 4.717 GB
Performance Statistics 72.442 MB 805.082 MB 9.435 GB
Other Events 669.819 MB 1.572 GB 3.145 GB
IP Reputation & URL Filtering 0 KB 1.966 GB 3.931 GB
Archives & Cores & File Logs 1.381 GB 3.145 GB 15.724 GB
RNA Events 0 KB 3.145 GB 12.579 GB
File Capture 12.089 MB 4.717 GB 14.152 GB
IPS Events 3.389 GB 7.076 GB 15.724 GB
```

/Volume Partitionが一杯の場合

古いバックアップファイル

- 大量の古いバックアップファイルをシステムに保存すると、ディスクの空き容量が増える可能性があります。

トラブルシューティングの手順

- Webユーザインターフェイスを使用して、古いバックアップファイルを削除します。バックアップファイルを削除するには、[System] > [Tools] > [Backup/Restore]に移動します。

  ヒント：FireSIGHTシステムでは、リモートストレージを設定して大きなバックアップファイルを保存できます。

古いソフトウェアのアップデートとパッチファイル

- 以前のソフトウェアアップデート、アップグレード、およびパッチファイル（5.0や5.1など）を常に保持している場合、システムのディスク領域が不足する可能性があります。

トラブルシューティングの手順

- 不要になった古い更新ファイルとパッチファイルを削除します。これらを削除するには、[System] > [Updates]に移動します。

過剰なイベントファイルが保存される

- 管理対象デバイスまたはセンサーがFireSIGHT Management Centerへのイベントの送信を停止した可能性があります。
- デバイスが生成するイベントの数が、Management Centerが受信するように設計されている（1秒あたりの）数を超える場合があります。
- 管理対象デバイスと管理センターの間に通信の問題がある可能性があります。

トラブルシューティングの手順

- イベントに関連するポリシーを再適用します。たとえば、接続イベントが表示されない場合は、アクセスコントロールポリシーを再適用し、新しいイベントが管理センターで受信されているかどうかを確認します。
- FireSIGHT Management Centerが新しいIPSイベントを受信できない場合は、管理対象デバイスと管理センターの間に通信の問題があるかどうかを確認してください。

過剰な不明ファイル

- FireSIGHTシステムは、未知のネットワーク検出データ（OS、ホスト、およびサービス情報）を保存します。

トラブルシューティングの手順

- システムがネットワーク上のホストのオペレーティングシステムを判別できない場合は、Nmapを使用してホストをアクティブにスキャンできます。Nmapは、スキャンから取得した情報を使用して、可能なオペレーティングシステムを評価します。次に、ホストのオペレーティングシステムIDとして最高評価のオペレーティングシステムを使用します。
- システムが不明なオペレーティングシステムを持つホストを検出したときにトリガーされる相関規則を作成します。
  このルールは、検出イベントが発生し、ホストのOS情報が変更され、次の条件を満たす場合にトリガーされます。OS名が不明です。

イベントを格納する大規模データベース

- データベースイベントの制限をガイドラインまたはベストプラクティスを超えて増やすと、FireSIGHT Management Centerのディスク領域が不足する可能性があります。

トラブルシューティングの手順

- データベース制限の値を確認します。ディスクの使用率とパフォーマンスを向上させるには、定期的に作業するイベントの数に応じてイベントの制限を調整する必要があります。一部のイベントタイプでは、ストレージを無効にできます。
- データベースの制限を変更するには、[システムポリシー]ページに移動し、システムポリシーの名前の横にある[編集]をクリックし、左側にある[データベース]をクリックします。[システ

ムポリシー]**ページにアク**セスするには、[システム] > [ロー**カル] > [システムポリシー]に移動します**。

ディスク使用率85 %以上のヘルスアラートを受信

考えられる原因

- イベントレートが非常に高い可能性があります。したがって、デバイスは多数のイベントを生成して保存しています。
- 管理対象デバイスとFireSIGHT Management Center間の通信の問題。

トラブルシューティングの手順

- アラートしきい値レベルを87 %（警告）および92 %（重大）に変更することは、頻繁にヘルスアラートを出す簡単なソリューションです。
- リリースノートを参照して、プルーニングシステムに既知の問題があったかどうかを確認してください。ソリューションが利用可能になった時点で、この問題に対処するために、ソフトウェアバージョンを最新リリースにアップデートしてください。

/var/log/messagesファイルには、24時間以上、または25MBを超えるデータが含まれています

考えられる原因

- Logrotateデーモンが正しく動作していない可能性があります。

トラブルシューティングの手順

- この問題が発生した場合は、FireSIGHTシステムのソフトウェアバージョンを最新リリースにアップデートしてください。最新バージョンを実行しているにもかかわらず、この問題が発生する場合は、Cisco Technical Assistance Center(TAC)にお問い合わせください。

ルート(/)パーティションがいっぱいである場合

ルート(/)パーティションにユーザファイルが保存される

考えられる原因

- ルート(/)パーティションは固定サイズで、個人用ストレージ用ではありません。
- /var/tmpディレクトリは、/var/commonディレクトリの代わりに、手動で一時ストレージに使用されます。

トラブルシューティングの手順

- /root、/home、および/tmpフォルダに不要なファイルがないかチェックしてください。これらのフォルダは個人用ストレージ用に作成されないため、rmコマンドを使用して任意の個人用ファイルを削除することができます。

サポートされていないプロセスがルート(/)パーティションに書き込んでいます

考えられる原因

- ルート(/)パーティションにファイルを作成するサードパーティ製ソフトウェアをインストールすると、ディスク使用率が高い場合にヘルスアラートが発生することがあります。

トラブルシューティングの手順

- サポートされていないパッケージがインストールされているかどうかを確認します。次のコマンドを実行して、インストールされているパッケージを検索します。

```
admin@3DSystem:~$ rpm -qa --last
```

- pstreeとtopをチェックして、サポートされていないプロセスが実行されているかどうかを確認します。次のコマンドを実行します。

```
admin@3DSystem:~$ pstree -ap

admin@3DSystem:~$ top
```