ASA トラブルシューティング ガイド： Syslog 宛先の口グがない

目次

概要

このドキュメントでは、syslog をさまざまな宛先に送信する適応型セキュリティ アプライアンス（ASA）の機能に関する問題、さらに具体的には、次のような症状が見られる問題をトラブルシューティングする方法について説明します。

- Adaptive Security Device Manager（ASDM）へのリアルタイム ログインに時間がかかる。
- 1 つ以上の syslog の宛先で断続的に syslog が欠落する。

はじめに

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

このドキュメントの情報は、Cisco ASA に基づいており、特定の ASA ソフトウェア バージョンには限定されません。

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

機能情報

他のほとんどのシスコ デバイスと同様、ASA は複数の syslog の宛先へ syslog を送信できます。一般的に使用される宛先の一部を次に示します。

実行可能な数の宛先を使用することには、実際の利点があります。 注意深く選ぶならば、ここに示すように、これらはその目的に基づいて、大きく 2 つの主なカテゴリに分類できます。

- Archival
- リアルタイムのデバッグ/トラブルシューティング

ほとんどのネットワークでは、1 つ以上のデバッグ宛先が必要な場合を除いて、アーカイブ宛先が有効であれば十分です。 同時に、また頻繁に、情報（レベル 6）以上のような高いログ レベルで複数の syslog の宛先を同時に有効にすることにより問題が発生します。

トラブルシューティング方法

1 つ以上の宛先で syslog 情報の損失が生じる問題が発生する場合、2 つの点を調べる必要があります。

- syslog 設定（**show run logging** の出力）を確認します。
- **show logging queue** の出力を調べます。

データ分析

syslog 設定の確認

次の手順を実行します。

1. 検索する syslog メッセージが **no logging message <ID>** コマンドによって無効にされていないことを確認します。
2. 確認できたら、有効にされている syslog の宛先の数、および各ログがそれぞれに送信されるレベルを確認します。 そのような設定の例を次に示します。`logging enable`
   ```
   logging timestamp
   logging standby
   logging console informational
   logging buffered informational
   logging trap informational
   logging asdm informational
   logging device-id hostname
   logging host inside 172.16.110.32
   ```

この例では、ASA は情報レベル（レベル 6）で 4 つの異なる宛先に syslog を送信しています。

show logging queue の出力

上記のような設定を使用した場合に、複数の宛先が大量のログ メッセージを受信すると、ロギング キューのオーバーフローのために ASA が syslog メッセージをドロップする状態が生じる可能性があります。 このような場合、次のような出力が表示されます。

```
ciscoasa# show logging queue Logging Queue length limit : 512 msg(s) 2352325 msg(s) discarded
due to queue overflow 0 msg(s) discarded due to memory allocation failure Current 512 msg on
```

`queue, 512 msgs most on queue`
デフォルトでは、ロギング キューは 512 個のメッセージを保持します。

一般的な問題

syslog メッセージが記録されていない問題が発生する場合は、次のオプションを検討します。

- コンソール ロギングを無効にします。 コンソールへのロギングは通常の運用では有効に**すべきではありません**。 コンソール ロギングを使用するのは、ロギング レベルが低いまたはトラフィックが少ない状況でリアルタイム トラブルシューティングを行う場合に限定する必要があります。 高いレートでコンソールへのロギングが行われると、ロギング プロセスでメッセージが大幅にレート制限されます。 コンソールでは 9600 bps でしかメッセージをロギングすることができず、コンソールが画面に出力できる量よりも多くのログをコンソールにダンプしようとするまでログを記録しません。 この場合、ログはロギング キューにバッファされ始めます。 ロギング キューがいっぱいになると、メッセージはテールドロップされます。
- ロギング キューのサイズを 512 より大きくします。 最大ロギング キューは、ASA-5505 では 1024、ASA-5510 では 2048、それ以外のプラットフォームでは 8192 です。 注： ロギング キューは syslog の「バースト」に使用されます。 syslog の持続レートが、ASA が複数の宛先に転送できるレートよりも速い場合、ロギング キューの制限がなくても十分な大きさになります。
- アーカイブの対象にしない個々の syslog メッセージを無効にします。 no logging message <syslog_id> コマンドを発行して、個々の syslog を無効にします。
- ASA のディスク（フラッシュ）へのロギング メッセージに注意してください。 フラッシュへの書き込みは、非常に時間のかかる処理になります。 フラッシュへの過剰なロギングによって、ASA はメモリに syslog ファイルをバッファするようになり、最終的に使用可能なすべてのメモリ（RAM）を使い果たしてしまいます。 さらに、フラッシュへの大量の syslog メッセージのロギングによって、CPU が上昇することもあります。 フラッシュへのロギングはレベル 1 のメッセージのみにすることをお勧めします（これで重要なシステム イベントには対応できます）。

関連情報

- テクニカルサポートとドキュメント - Cisco Systems