エンドポイント向けAMP:LinuxでのClamAVウイルス定義オプション

内容

概要

Linux Connectorバージョン1.11.0以降、AMP for Endpointsには2つのClamAV Virus Definition設定オプションが用意されています。

1. Linuxのみ
2. フルClamAV

Linuxのみのオプションが利用可能になる前に、Linux Connectorは完全なClamAVウイルス定義セットを使用してファイルをスキャンしました。このセットには、Linux、macOS、Windows、およびAndroid用のマルウェアシグニチャが含まれています。これは包括的なカバレッジを提供しますが、CPUの時間やメモリなどの重要なランタイムリソースも必要です。 一部のLinuxシステムでは、より小さいLinuxのみのClamAVウイルス定義セットを使用するようにAMPを設定する利点があります。

Linuxのみのウイルス定義ファイルのサイズは、フルセットの10 %未満です。小さいセットを使用すると、コンピューティングのオーバーヘッドが軽減され、リソースに制約のあるシステムでAMPを実行できます。パフォーマンス上の利点にもかかわらず、Linux以外のマルウェアのカバレッジが減少しているため、この設定は一部のアプリケーションにのみ適しています。例えば、Linuxファイル（アプリケーションサーバなど）をホスト/ストアするサーバには適していますが、Linux以外のファイル（FTP、メール、SMBファイルサーバなど）もホスト/ストアするサーバには適していません。 適切なウイルス定義セットを選択するには、システム管理者がこのトレードオフのバランスを取る必要があります。

重要：

新しいLinuxのみのウイルス定義オプションを使用する前に、すべてのエンドポイントをConnectorバージョン1.11.0以降にアップグレードすることを強く推奨します。1.10.x以前のバージョンのConnectorは新しいオプションを受け入れますが、場合によっては直感的に動作しない場合があります。詳細は、「下位互換性」セクションを参照してください。

下位互換性

新しいLinuxのみのウイルス定義オプションを使用するようにエンドポイントを設定する前に、下位互換性に関する重要な問題を考慮する必要があります。1.10.xおよびそれ以前のコネクタは、完全なセットがすでにダウンロードされている場合、引き続き完全なウイルス定義を使用します

。新しいLinuxのみのウイルス定義オプションを使用するように設定されている場合、Connectorは完全なウイルス定義セットの更新を停止し、それ以降はLinuxのウイルス定義セットのみを更新します。これにより、エンドポイントでは最新のLinuxウイルス定義が使用されますが、古いmacOS、Windows、およびAndroidの定義が使用される可能性があります。

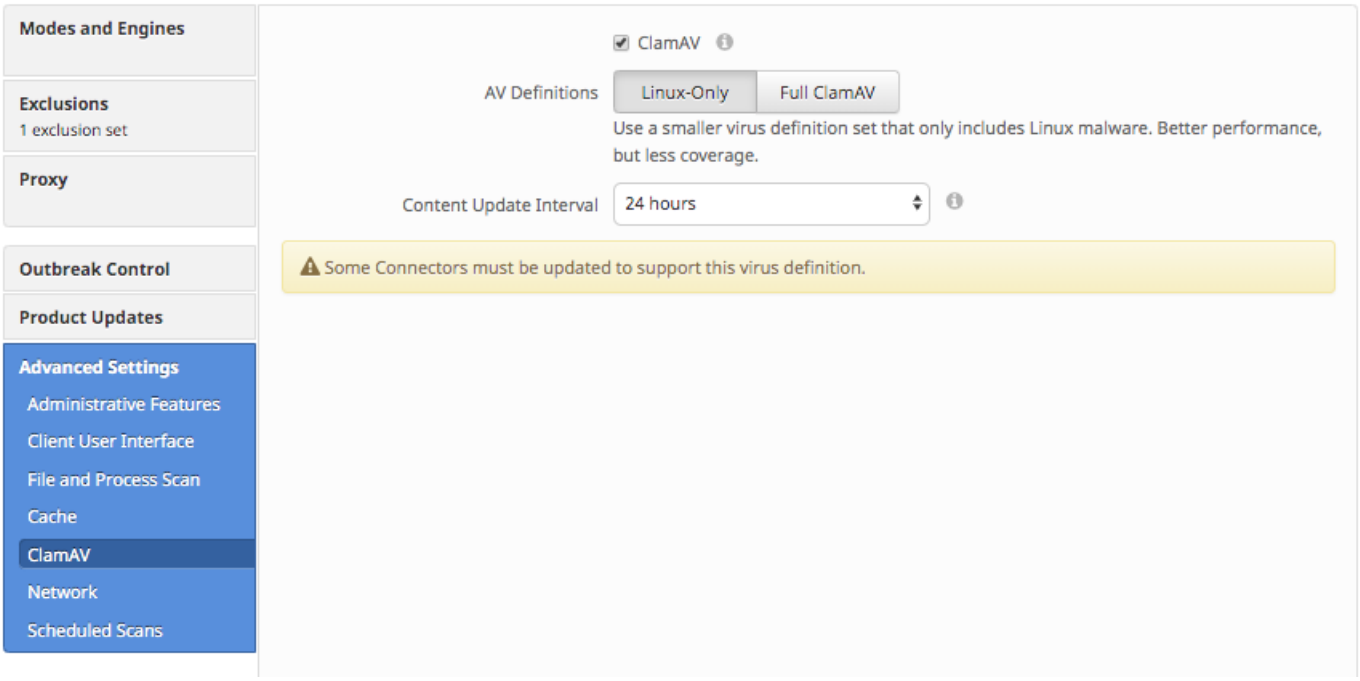
考えられる解決策は2つあります。

1. コネクタを1.11.0以降にアップグレードします。
2. [ClamAV Virus Definition]設定を[Full ClamAV]に戻します。

ClamAVウイルス定義オプションの変更

ClamAV Virus Definitionオプションは、AMP for Endpoints Webポータルを使用して設定できます。各ポリシーのオプションは、次の項目に移動して変更できます。

Management > Policies > [Linux Policy] > Edit > Advanced Settings > ClamAV



AV Definitionsポリシー設定が変更された後、スケジュールされた次回のウイルス定義の更新時に、新しい設定がエンドポイントに適用されます。この遅延は、[Content Update Internal]ポリシー設定によって制御されます。

ポリシーで管理されている少なくとも1つのコネクタが互換性のないLinux Connectorバージョンを実行している場合、[ClamAV Advanced Settings]画面に「Some Connectors must be updated to support this virus definition」という警告が表示されることがあります。Linux専用の定義設定を使用する前に、コネクタをアップグレードし、この警告を解決することを強く推奨します。

エンドポイントでの新しい設定の確認

Linuxのみの定義を使用するように設定されている場合、2つのAMPコネクタプロセスのメモリの合計サイズは100 MB未満である必要があります。

これは、次のコマンドを使用して確認できます。

```
top -p `pidof ampdaemon` -p `pidof ampscansvc`
```

次に出力例を示します。

```
top - 23:52:51 up 15:11,  7 users,  load average: 0.36, 1.10, 0.83
Tasks:   2 total,   0 running,   2 sleeping,   0 stopped,   0 zombie
%Cpu(s):  2.5 us,  0.5 sy,  0.0 ni, 97.0 id,  0.0 wa,  0.0 hi,  0.0 si,  0.0 st
KiB Mem :  3861508 total,   309220 free,  1732560 used,  1819728 buff/cache
KiB Swap:  2097148 total,  2064116 free,    33032 used.  1629348 avail Mem

  PID USER      PR  NI    VIRT    RES    SHR S  %CPU %MEM     TIME+ COMMAND
88910 root      20   0 1323172  32904   6752 S   0.7  0.9   3:20.16 ampdaemon
88937 cisco-a+  20   0  258764   8400   2704 S   0.0  0.2   1:23.73 ampscansvc
```