AMP for Endpoints: Opzioni di definizione dei virus ClamAV in Linux

Sommario

Introduzione

A partire da Linux Connector versione 1.11.0, AMP for Endpoints offre due opzioni di configurazione ClamAV Virus Definition:

1. Solo Linux
2. ClamAV completo

Prima che l'opzione solo Linux diventasse disponibile, il Connettore Linux eseguiva la scansione dei file usando il set completo di definizioni dei virus ClamAV. Questo set include firme malware per Linux, macOS, Windows e Android. Anche se questo fornisce una copertura completa, richiede anche notevoli risorse di runtime (ad esempio, tempo CPU e memoria). Alcuni sistemi Linux possono trarre vantaggio dalla configurazione di AMP per l'utilizzo del più piccolo set di definizioni di virus ClamAV solo per Linux.

Le dimensioni del file di definizione dei virus solo per Linux sono inferiori al 10% del set completo. L'utilizzo di un set più piccolo riduce il sovraccarico di elaborazione e consente di eseguire AMP su sistemi con risorse limitate. Nonostante i vantaggi in termini di prestazioni, una copertura ridotta per il malware non Linux rende questa configurazione adatta solo per alcune applicazioni. Ad esempio, è adatto per i server che ospitano/memorizzano solo file Linux (come i server applicazioni) ma non per i server che ospitano/memorizzano anche file non Linux (come i file server FTP, di posta e SMB). L'amministratore di sistema deve bilanciare questo compromesso per scegliere il set appropriato di definizioni dei virus.

> **IMPORTANTE!**
>
> Si consiglia di aggiornare tutti gli endpoint alla versione Connector 1.1.0 o successiva prima di utilizzare la nuova opzione di definizione dei virus solo Linux. Anche se la versione 1.10.x e le versioni precedenti di Connector accetteranno la nuova opzione, in alcuni casi il suo comportamento non sarà intuitivo. Per ulteriori informazioni, consultare la sezione *Compatibilità con le versioni precedenti*.

Compatibilità con le versioni precedenti

Prima di configurare gli endpoint per l'utilizzo della nuova opzione di definizione dei virus solo Linux, è necessario considerare un importante problema di compatibilità con le versioni

precedenti: La versione 1.10.x e le versioni precedenti di Connector continueranno a utilizzare la definizione di virus completa se è già stato scaricato il set completo. Se configurato per utilizzare la nuova opzione di definizione dei virus solo Linux, il Connettore interromperà l'aggiornamento dell'intero set di definizioni dei virus e aggiornerà solo il set di definizioni dei virus Linux. Ciò può determinare l'utilizzo da parte dell'endpoint di definizioni di virus Linux aggiornate ma di definizioni di macOS, Windows e Android non aggiornate.

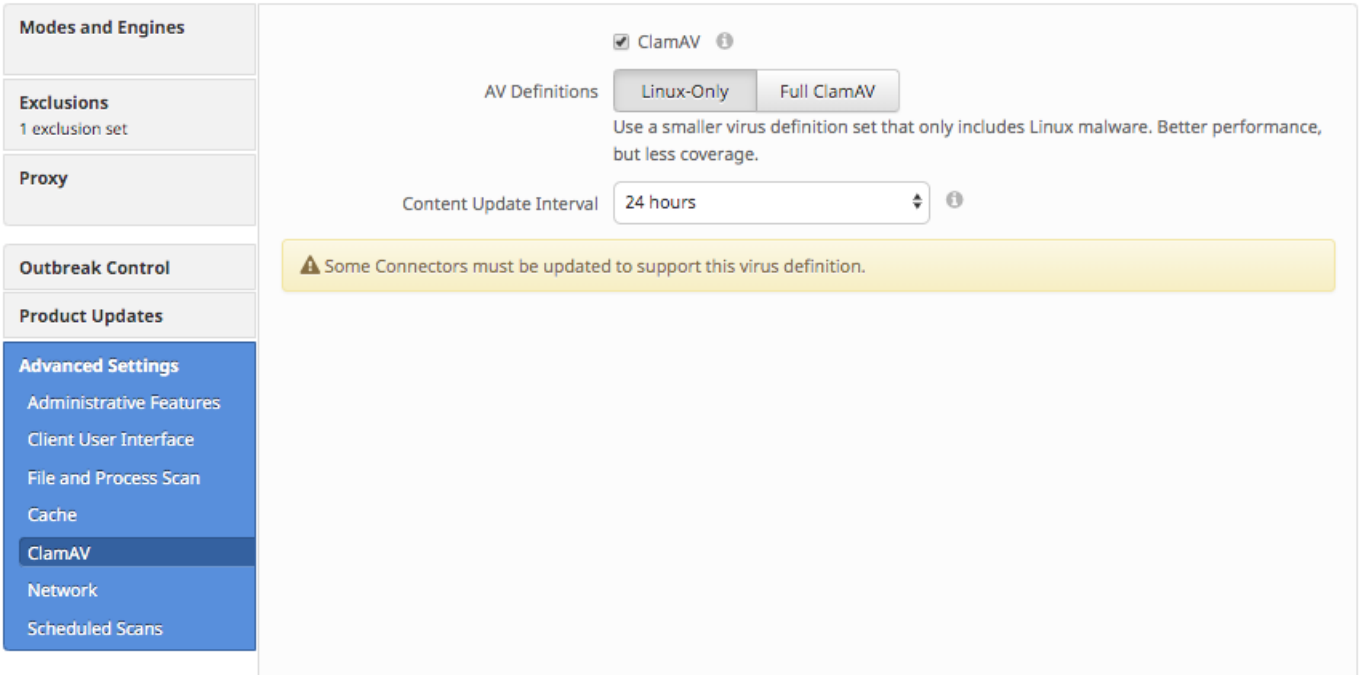
Esistono due possibili risoluzioni:

1. Aggiornare Connector alla versione 1.1.0 o successive.
2. Modificare l'impostazione ClamAV Virus Definition in Full ClamAV.

Modifica dell'opzione ClamAV Virus Definitions

L'opzione ClamAV Virus Definition può essere configurata utilizzando il portale Web AMP for Endpoints. È possibile modificare l'opzione per ogni criterio passando a:

Gestione > Criteri > [Criteri Linux] > Modifica > Impostazioni avanzate > ClamAV



Dopo la modifica dell'impostazione del criterio Definizioni AV, la nuova impostazione viene applicata agli endpoint al successivo aggiornamento pianificato delle definizioni dei virus. Tale ritardo è determinato dall'impostazione del criterio `Content Update Internal`.

L'avviso "Alcuni connettori devono essere aggiornati per supportare questa definizione di virus" può essere visualizzato nella schermata Impostazioni avanzate di ClamAV se almeno un connettore gestito dal criterio esegue una versione di Connettore Linux incompatibile. Si consiglia di aggiornare i connettori e risolvere questo avviso prima di utilizzare l'impostazione delle definizioni solo per Linux.

Verifica della nuova impostazione nell'endpoint

Se la configurazione prevede l'utilizzo di definizioni solo Linux, le dimensioni combinate della

memoria residente dei due processi del connettore AMP devono essere inferiori a 100 MB.

Èpossibile esaminare questa condizione utilizzando il seguente comando:

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

Di seguito viene riportato un esempio di output: