AMP para endpoints: Opções de definição de vírus ClamAV no Linux

Contents

Introduction

Começando com o conector Linux versão 1.11.0, o AMP para endpoints agora oferece duas opções de configuração de definição de vírus ClamAV:

1. Somente Linux
2. ClamAV completo

Antes da opção somente Linux se tornar disponível, o conector Linux digitalizava arquivos usando o conjunto completo de definições de vírus ClamAV. Esse conjunto inclui assinaturas de malware para Linux, macOS, Windows e Android. Embora isso forneça cobertura abrangente, também exige recursos significativos de tempo de execução (ou seja, tempo e memória da CPU). Alguns sistemas Linux podem se beneficiar com a configuração da AMP para usar o conjunto menor de definições de vírus da ClamAV apenas para Linux.

O tamanho do arquivo de definição de vírus somente Linux é inferior a 10% do conjunto completo. O uso de um conjunto menor reduz a sobrecarga de computação e torna possível executar o AMP em sistemas com recursos limitados. Apesar das vantagens de desempenho, a cobertura reduzida para malware não Linux torna essa configuração adequada apenas para alguns aplicativos. Por exemplo, ele seria adequado para servidores que hospedam/armazenam somente arquivos Linux (como servidores de aplicativos), mas não seria adequado para servidores que também hospedam/armazenam arquivos não Linux (como servidores de arquivos FTP, de correio e SMB). O administrador do sistema deve equilibrar essa compensação para escolher o conjunto apropriado de definições de vírus.

IMPORTANTE!

Éaltamente recomendável atualizar todos os endpoints para o Connector versão 1.11.0 ou mais recente antes de usar a nova opção de definição de vírus somente Linux. Embora as versões 1.10.x e mais antigas do Connector aceitem a nova opção, seu comportamento em alguns casos não será intuitivo. Consulte a seção *Compatibilidade com Versões Anteriores* para obter detalhes.

Compatibilidade com versões anteriores

Há um importante problema de compatibilidade com versões anteriores a ser considerado antes

de configurar endpoints para usar a nova opção de definição de vírus somente Linux: 1.10.x e conectores mais antigos continuarão a usar a definição completa do vírus se o conjunto completo já tiver sido baixado. Se configurado para usar a nova opção de definição de vírus somente para Linux, o Connector parará de atualizar o conjunto completo de definições de vírus e só atualizará a definição de vírus Linux posteriormente. Isso pode resultar no endpoint usando definições de vírus Linux atualizadas, mas definições de macOS, Windows e Android desatualizadas.

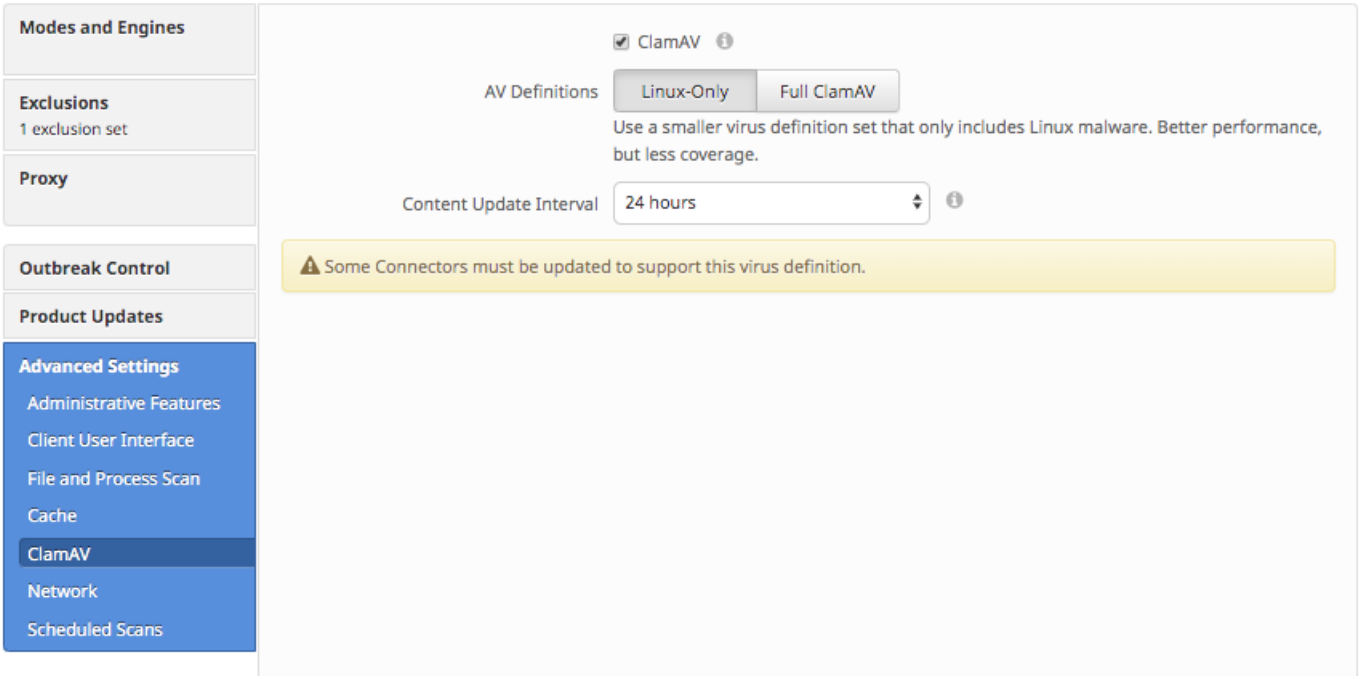
Há duas resoluções possíveis:

1. Atualize o conector para 1.11.0 ou posterior.
2. Altere a definição ClamAV Virus Definition para Full ClamAV.

Alteração da opção Definições de vírus ClamAV

A opção ClamAV Virus Definition pode ser configurada usando o portal da Web AMP para endpoints. A opção para cada política pode ser alterada navegando para:

> Gerenciamento > Políticas > [Política do Linux] > Editar > Configurações avançadas > ClamAV



Depois que a configuração da política Definições de AV é alterada, a nova configuração entra em vigor nos endpoints na próxima atualização programada da definição de vírus. Esse atraso é regido pela configuração de política "Content Update Internal" (Atualização de conteúdo interna).

O aviso "Alguns conectores devem ser atualizados para suportar essa definição de vírus" pode aparecer na tela Configurações avançadas do ClamAV se pelo menos um conector gerenciado pela diretiva estiver executando uma versão incompatível do conector Linux. É altamente recomendável atualizar os conectores e resolver esse aviso antes de usar a configuração de definições somente de Linux.

Verificando a nova configuração no endpoint

Quando configurado para usar definições somente Linux, o tamanho combinado da memória residente dos dois processos do conector AMP deve ser inferior a 100 MB.

Isso pode ser examinado usando o seguinte comando:

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

Veja a seguir um exemplo de saída: