AMP para terminales: Opciones de definición de virus ClamAV en Linux

Contenido

Introducción

A partir de la versión 1.11.0 del conector Linux, AMP para terminales ahora ofrece dos opciones de configuración de definición de virus ClamAV:

1. Sólo Linux
2. ClamAV completo

Antes de que la opción de Linux-only estuviera disponible, Linux Connector escaneaba los archivos usando el conjunto completo de definición de virus ClamAV. Este conjunto incluye firmas de malware para Linux, MacOS, Windows y Android. Aunque esto proporciona una cobertura completa, también requiere importantes recursos en tiempo de ejecución (es decir, tiempo de CPU y memoria). Algunos sistemas Linux pueden beneficiarse de la configuración de AMP para utilizar el conjunto de definición de virus ClamAV más pequeño sólo para Linux.

El tamaño del archivo de definición de virus sólo para Linux es inferior al 10% del conjunto completo. El uso de un conjunto más pequeño reduce la sobrecarga informática y permite ejecutar AMP en sistemas con recursos limitados. A pesar de las ventajas de rendimiento, la reducción de la cobertura del malware que no es de Linux hace que esta configuración sólo sea adecuada para algunas aplicaciones. Por ejemplo, sería adecuado para servidores que sólo alojan/almacenan archivos Linux (como servidores de aplicaciones) pero no sería adecuado para servidores que también alojan/almacenan archivos que no son de Linux (como FTP, correo y servidores de archivos SMB). El administrador del sistema debe equilibrar esta compensación para elegir el conjunto adecuado de definiciones de virus.

> **¡IMPORTANTE!**
>
> Se recomienda encarecidamente actualizar todos los terminales a la versión 1.11.0 o posterior del conector antes de utilizar la nueva opción de definición de virus sólo para Linux. Aunque las versiones 1.10.x y anteriores de Connector aceptarán la nueva opción, su comportamiento en algunos casos no será intuitivo. Consulte la sección *Compatibilidad con versiones anteriores* para obtener más detalles.

Compatibilidad con versiones anteriores

Antes de configurar los terminales para utilizar la nueva opción de definición de virus sólo Linux,

debe tenerse en cuenta un importante problema de compatibilidad con versiones anteriores: 1.10.x y los conectores más antiguos seguirán utilizando la definición completa de virus si el conjunto completo ya se ha descargado. Si se configura para utilizar la nueva opción de definición de virus sólo Linux, el conector dejará de actualizar el conjunto completo de definiciones de virus y sólo actualizará la definición de virus Linux establecida a partir de entonces. Esto puede dar como resultado que el terminal utilice definiciones de virus Linux actualizadas pero definiciones de MacOS, Windows y Android obsoletas.

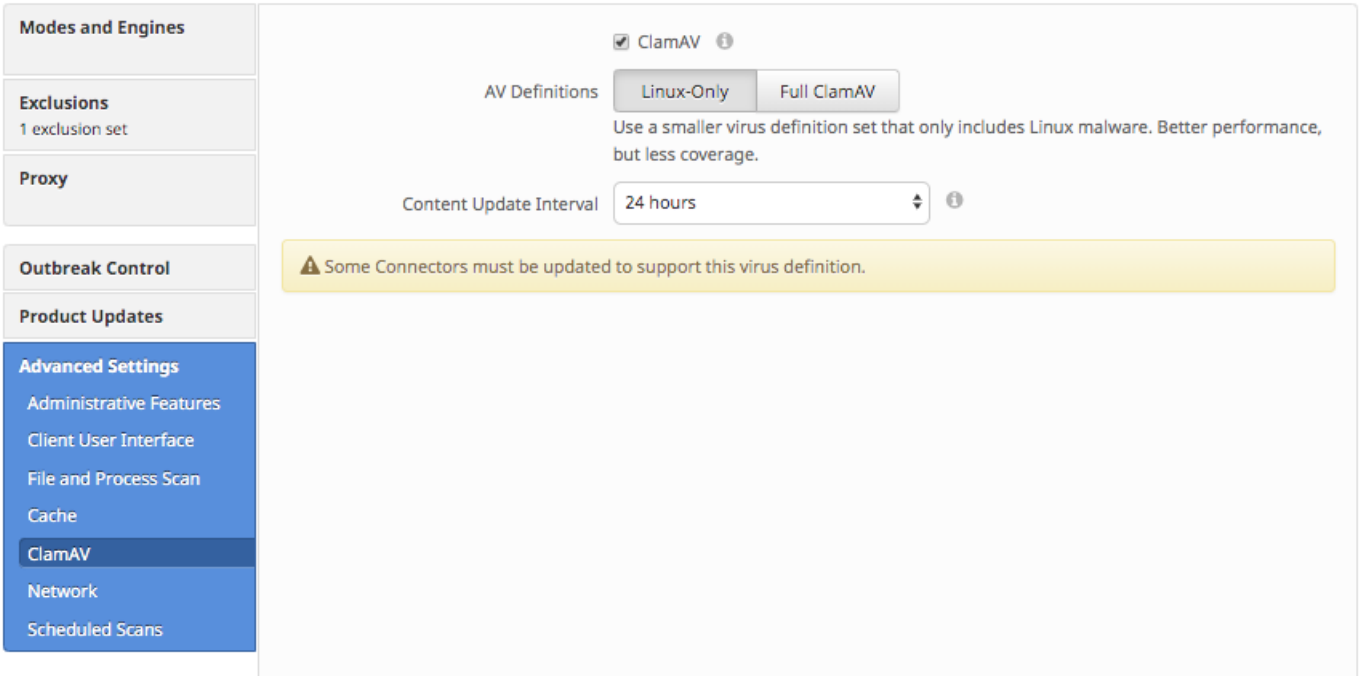
Hay dos posibles resoluciones:

1. Actualice el conector a 1.11.0 o posterior.
2. Vuelva a cambiar la configuración de definición de virus ClamAV a Full ClamAV.

Cambio de la opción de definiciones de virus ClamAV

La opción ClamAV Virus Definition se puede configurar mediante el portal web de AMP para terminales. La opción para cada política se puede cambiar navegando a:

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



Después de cambiar la configuración de la política de definiciones AV, la nueva configuración se aplica a los terminales en la próxima actualización programada de la definición de virus. Esa demora se rige por la configuración de la política `Actualización de contenido interna'.

La advertencia "Algunos conectores deben actualizarse para admitir esta definición de virus" puede aparecer en la pantalla Configuración avanzada de ClamAV si al menos un conector administrado por la política está ejecutando una versión de conector Linux incompatible. Se recomienda encarecidamente actualizar los conectores y resolver esta advertencia antes de utilizar la configuración de definiciones de Linux solamente.

Verificación de la Nueva Configuración en el Extremo

Cuando se configura para utilizar definiciones de sólo Linux, el tamaño de memoria residente combinado de los dos procesos de conector de AMP debe ser inferior a 100 MB.

Esto se puede examinar con el siguiente comando:

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

A continuación se incluye un ejemplo de salida: