AMP für Endgeräte: ClamAV-Virendefinitionsoptionen in Linux

Inhalt

Einführung

Ab Linux Connector Version 1.11.0 bietet AMP für Endgeräte jetzt zwei Konfigurationsoptionen für ClamAV-Virendefinitionen:

1. Nur Linux
2. Vollständige ClamAV

Bevor die Linux-Option verfügbar ist, hat der Linux Connector Dateien mit dem vollständigen ClamAV-Virendefinitionsset gescannt. Dieses Set enthält Malware-Signaturen für Linux, MacOS, Windows und Android. Dies bietet zwar umfassende Abdeckung, erfordert aber auch erhebliche Laufzeitressourcen (d. h. CPU-Zeit und Arbeitsspeicher). Einige Linux-Systeme können von der Konfiguration von AMP für die Verwendung des kleineren ClamAV-Virendefinitionssatzes für Linux profitieren.

Die Dateigröße der reinen Linux-Virendefinitionen beträgt weniger als 10 % des gesamten Satzes. Mit einem kleineren Satz wird der Computing-Overhead reduziert und die Ausführung von AMP auf Systemen mit eingeschränkten Ressourcen ermöglicht. Trotz der Leistungsvorteile ist diese Konfiguration aufgrund der geringeren Abdeckung für Malware, die nicht unter Linux läuft, nur für einige Anwendungen geeignet. Beispielsweise wäre es für Server geeignet, die nur Linux-Dateien hosten/speichern (z. B. Anwendungsserver), aber nicht für Server geeignet sind, die auch Nicht-Linux-Dateien hosten/speichern (z. B. FTP-, Mail- und SMB-Dateiserver). Der Systemadministrator muss diesen Kompromiss abwägen, um die passenden Virendefinitionen auszuwählen.

> **WICHTIG!**
>
> Es wird dringend empfohlen, dass alle Endgeräte auf Connector Version 1.11.0 oder höher aktualisiert werden, bevor die neue Virendefinitionsoption für Linux verwendet wird. Die neue Option wird zwar von Version 1.10.x und älteren Connector-Versionen akzeptiert, in einigen Fällen ist ihr Verhalten jedoch nicht intuitiv. Weitere Informationen finden Sie im Abschnitt *Abwärtskompatibilität*.

Abwärtskompatibilität

Vor der Konfiguration von Endpunkten zur Verwendung der neuen Virendefinitionsoption für Linux

muss ein wichtiges Problem der Abwärtskompatibilität beachtet werden: 1.10.x und ältere Connectors verwenden weiterhin die vollständige Virendefinition, wenn der vollständige Satz bereits heruntergeladen wurde. Wenn Connector für die Verwendung der neuen Virendefinitionsoption für Linux konfiguriert ist, beendet er die Aktualisierung des vollständigen Virusdefinitionssatzes und aktualisiert erst danach den Linux-Virendefinitionssatz. Dies kann dazu führen, dass Endgeräte aktuelle Linux-Virendefinitionen, aber veraltete MacOS-, Windows- und Android-Definitionen verwenden.

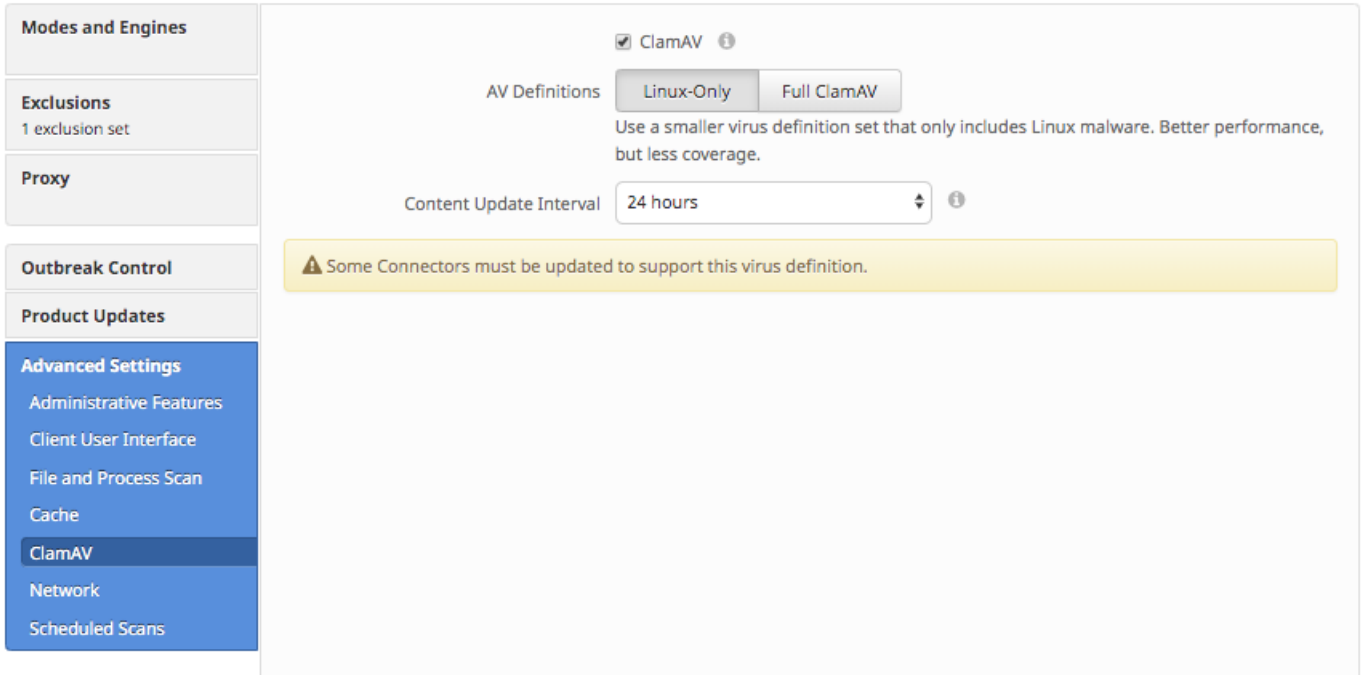
Es gibt zwei mögliche Auflösungen:

1. Aktualisieren Sie den Connector auf Version 1.11.0 oder höher.
2. Ändern Sie die ClamAV-Virendefinitionseinstellung wieder auf Full ClamAV.

Ändern der ClamAV-Virendefinitionsoption

Die ClamAV-Virendefinitionsoption kann über das Webportal von AMP für Endgeräte konfiguriert werden. Die Option für jede Richtlinie kann geändert werden, indem Sie zu:

> Management > Richtlinien > [Linux-Richtlinie] > Bearbeiten > Erweiterte Einstellungen > ClamAV



Nachdem die AV Definitions-Richtlinieneinstellungen geändert wurden, wird die neue Einstellung beim nächsten geplanten Update der Virendefinitionen auf den Endpunkten aktiviert. Diese Verzögerung wird durch die Einstellung "Content Update Internal" (Interne Inhaltsaktualisierung) geregelt.

Die Warnung "Einige Connectors müssen aktualisiert werden, um diese Virendefinitionen zu unterstützen" kann im Bildschirm "ClamAV Advanced Settings" angezeigt werden, wenn mindestens ein von der Richtlinie verwalteter Connector eine inkompatible Linux Connector-Version ausführt. Es wird dringend empfohlen, die Connectors zu aktualisieren und diese Warnung zu beheben, bevor die Linux-Definitionen verwendet werden.

Überprüfen der neuen Einstellung am Endpunkt

Wenn die Konfiguration für die Verwendung reiner Linux-Definitionen konfiguriert ist, sollte die kombinierte Größe des lokalen Arbeitsspeichers der beiden AMP Connector-Prozesse unter 100 MB liegen.

Dies kann mithilfe des folgenden Befehls überprüft werden:

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

Nachfolgend finden Sie eine Beispielausgabe: