AMP لنقاط النهاية: خيارات تعريف فيروس ClmAV في نظام التشغيل Linux

المحتويات

المقدمة
التوافق مع الإصدارات السابقة
تغيير خيار تعريفات فيروس ClamAV
التحقق من العداد الجديد في نقطة النهاية

المقدمة

بدءا من الإصدار 1. 11. 0 من موصل Linux، توفر AMP لنقاط النهاية الآن خياريني لتهيئة تعريف فيروس ClmAV:

1. لينكس فقط
2. كامل ClamAV

قبل أن يصبح خيار لينكس فقط متاحا، قام موصل ليونكس بمسح الملفات باستخدام مجموعة التعريف الكاملة للفيروس ClmAV. تتضمن هذه المجموعة توقيعات برامج ضارة لنظام التشغيل Linux و MacOS و Windows و Android. وعلى الرغم من أن ذلك يوفر تغطية شاملة، إلا أنه يتطلب أيضا مواردك كبيرة وقت التشغيل (مثل وقت وحدة المعالجة المركزية والذاكرة). يمكن لبعض أنظمة ليونكس الاستفادة من تكوين AMP لاستخدام مجموعة تعريفات فيروسات ClmAV الصغيرة التي تستخدم نظام ليونكس فقط.

حجم ملف تعريف الفيروس فقط ل Linux أقل من 10٪ من المجموعة الكاملة. يؤدي إستخدام مجموعة أصغ إلى تقليل متطلبات الحوسبة، كما يجعل من الممكن تشغيل برنامج لوكول على الأنظمة ذات الموارد المحدودة. على الرغم من ميزات الأداء، إلا أن تقليل التغطية AMP للبرامج الضارة يخلق نظام التشغيل Linux هذا التكوين مناسبا لبعض التطبيقات فقط. على سبيل المثال، ستكون ملائمة للملفات التي تستضيف/تخزن ملفات Linux فقط (مثل ملفات التطبيقات) لكنها لن تكون مناسبة للملفات التي تقوم أيضا باستضافة/تخزين الملفات غير الخاصة بنظام التشغيل Linux (مثل ملفات FTP والبريد و SMB). يجب على مسؤول النظام موازنة هذه المقايضة لاختيار المجموعة المناسبة من تعريفات الفيروسات.

ملاحظة!

يوصى بشدة بترقية جميع نقاط النهاية إلى الإصدار 1.11.0 من الموصل أو إصدار أحدث قبل إستخدام خيار تعريف الفيروس الجديد على نظام التشغيل Linux فقط. في حين أن إصدارات موصل 1.10.x والإصدارات الأقدم تقبل الخيار الجديد، إلا أنه سلوكها في بعض الحالات لن يكون بديهيا. راجع قسم *التوافق مع الإصدارات السابقة* للحصول على تفاصيل.

التوافق مع الإصدارات السابقة

هناك مشكلة توافق تراجعي مهمة ألخذها بعين الاعتبار قبل تكوين نقاط النهاية

لاستخدام خيار تعريف الفيروس الجديد على نظام التشغيل Linux: سيستمر تطبيق التعريف الكامل للفيروس على 1.10.x والموصلات الأقدم إذا تم تنزيل المجموعة الكاملة بالفعل. إذا تم تكوين استخدام خيار تعريف الفيروس الجديد على لينوكس فقط، سيقوم الموصل بإيقاف تحديث مجموعة تعريف الفيروسات بالكامل وسيقوم بتحديث تعريف فيروس لينوكس فقط الذي تم تعيينه بعد ذلك. يمكن أن يؤدي ذلك إلى إستخدام نقطة النهاية تعريفات فيروسات Linux الحديثة ولكن تعريفات MacOS و Windows و Android قديمة.

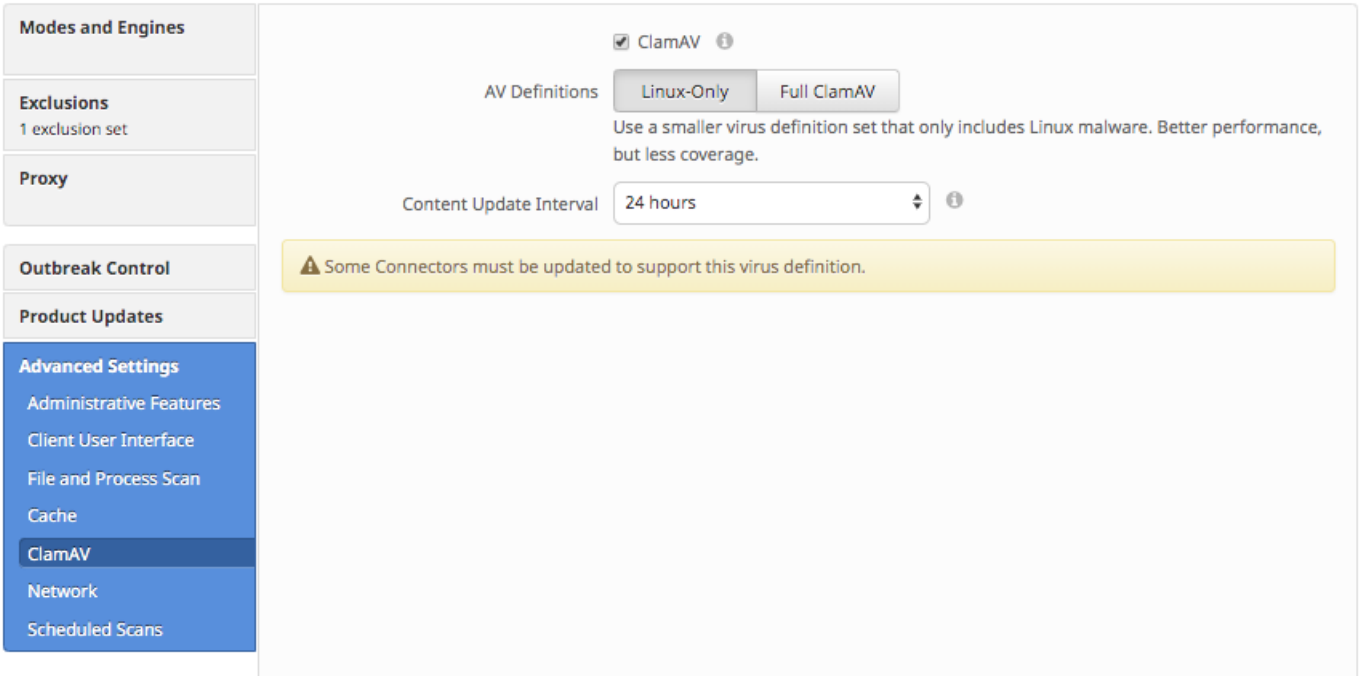
هناك قراران محتملان:

1. قم بترقية الموصل إلى 1.11.0 أو إصدار أحدث.
2. قم بتغيير إعداد تعريف فيروس ClamAV مرة أخرى إلى ClmAV الكامل.

تغيير خيار تعريفات فيروس ClamAV

يمكن تكوين خيار تعريف فيروس ClamAV باستخدام AMP لبوابة نقاط النهاية على الويب. يمكن تغيير الخيار لكل نهج عن طريق الانتقال إلى:

الإدارة > السياسات > [سياسة Linux] > تحرير > إعدادات متقدمة > ClmAV



بعد تغيير إعداد نهج تعريفات AV، يسري الإعداد الجديد على نقاط النهاية في التحديث التالي الموجود لتعريف الفيروسات. يتم التحكم في هذا التأخير من خلال إعداد النهج الداخلي "تحديث المحتوى".

قد يظهر التحذير "بعض الموصلات التي يجب تحديثها لدعم تعريف الفيروس هذا" في شاشة "إعدادات ClamAV المتقدمة إذا كان هناك موصل واحد على الأقل تتم إدارته بواسطة النهج يقوم بتشغيل إصدار غير متوافق من موصل Linux. يوصى بشدة بتحديث الموصلات وحل هذا التحذير قبل إستخدام إعداد التعريفات الخاصة بنظام التشغيل Linux فقط.

التحقق من الإعداد الجديد في نقطة النهاية

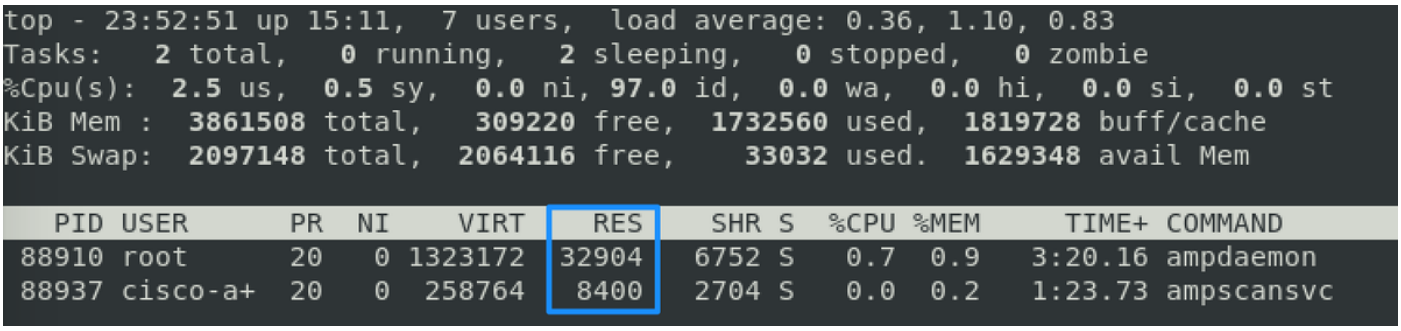
عند تكوين استخدام تعريفات نظام التشغيل Linux فقط، يجب أن يكون حجم الذاكرة

المقيم المجمع لكل من عمليتي AMP Connector أقل من 100 ميجابايت.

يمكن فحص ذلك باستخدام الأمر التالي:

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

وفيما يلي عينة من المخرجات:



حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).