AMP pour des points finaux : Options de définition de virus de ClamAV dans le Linux

Contenu

Introduction

Commençant par la version 1.11.0 de connecteur de Linux, l'AMP pour des points finaux offre maintenant deux options de configuration de définition de virus de ClamAV :

1. réservé à la Linux
2. Plein ClamAV

Avant l'option réservée à la Linux devenant disponible, le connecteur de Linux a analysé des fichiers utilisant le plein positionnement de définition de virus de ClamAV. Ce positionnement inclut des signatures de malware pour le Linux, le MaOS, le Windows et l'Android. Bien que ceci fournisse la couverture complète, il exige également les ressources d'exécution importantes (c.-à-d., temps- CPU et mémoire). Quelques systèmes Linux peuvent tirer bénéfice de configurer l'AMP pour utiliser le positionnement réservé à la Linux plus petit de définition de virus de ClamAV.

La taille de fichier réservée à la Linux de définition de virus est moins de 10% de l'ensemble complet. Utilisant un plus petit positionnement réduit calculer le temps système et permet pour exécuter l'AMP sur les systèmes contraints par ressource. En dépit des avantages de représentation, la couverture réduite pour le malware de non-Linux rend cette configuration seulement appropriée à quelques applications. Par exemple, il conviendrait aux serveurs qui hébergent seulement/les fichiers Linux de mémoire (tels que des serveurs d'applications) mais ne conviendrait pas aux serveurs qui hébergent également/les fichiers non-Linux de mémoire (tels que le FTP, la messagerie et les serveurs de fichiers PME). L'administrateur système doit équilibrer ce compromis pour choisir l'ensemble approprié de définitions de virus.

> **IMPORTANT !**
>
> On le recommande fortement que tous les points finaux soient améliorés à la version 1.11.0 ou plus récentes de connecteur avant d'utiliser la nouvelle option de définition réservée à la Linux de virus. Tandis que 1.10.x et versions plus anciennes de connecteur recevront la nouvelle option, son comportement dans certains cas ne sera pas intuitif. Référez-vous *ascendant à la* section de *compatibilité* pour des détails.

Ascendant compatibilité

Il y a un important vers l'arrière problème de compatibilité à considérer avant de configurer des

points finaux pour utiliser la nouvelle option de définition réservée à la Linux de virus : 1.10.x et connecteurs plus anciens continueront à utiliser la définition complète de virus si l'ensemble complet avait été déjà téléchargé. Si configuré pour utiliser la nouvelle option de définition réservée à la Linux de virus, le connecteur cessera de mettre à jour la définition complète de virus réglée et mettra à jour seulement la définition de virus de Linux réglée ensuite. Ceci peut avoir comme conséquence le point final utilisant les définitions à jour de virus de Linux mais le MaOS périmé, les définitions de Windows, et d'Android.

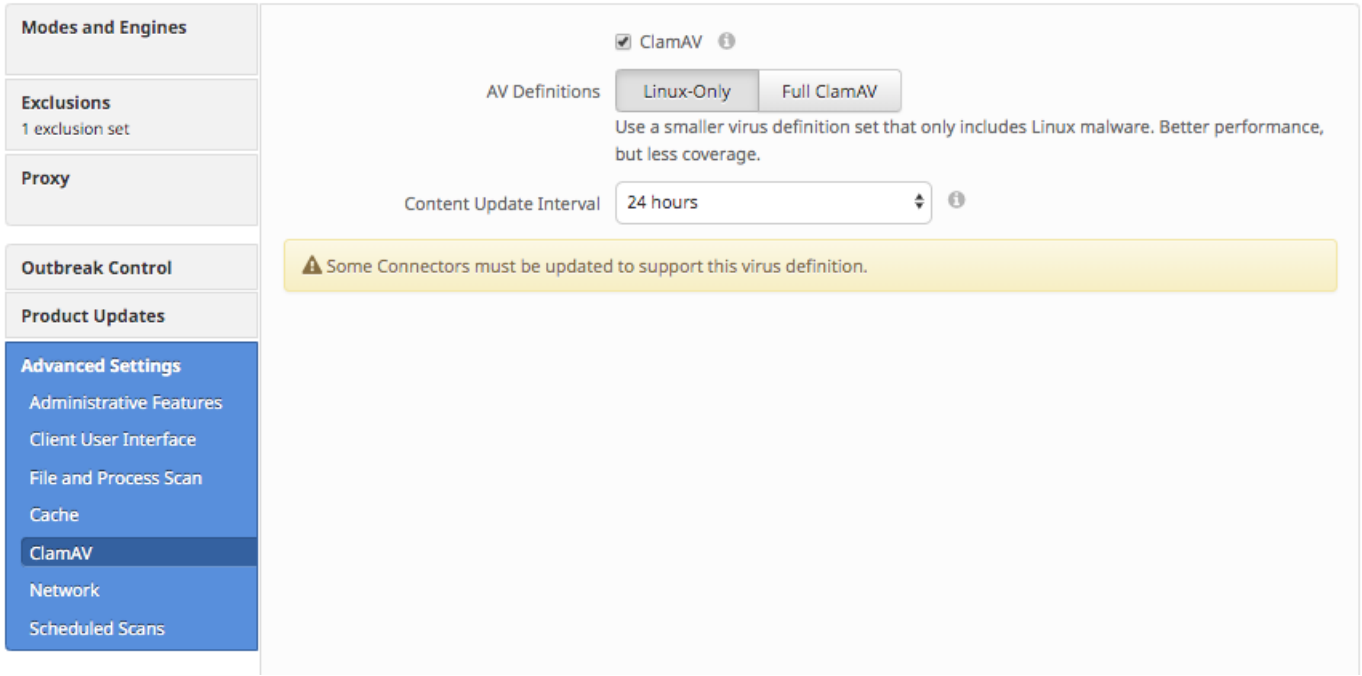
Il y a deux résolutions possibles :

1. Améliorez le connecteur à 1.11.0 ou plus tard.
2. Changez la configuration de définition de virus de ClamAV de nouveau à plein ClamAV.

Changer l'option de définitions de virus de ClamAV

L'option de définition de virus de ClamAV peut être configurée utilisant l'AMP pour le portail web de points finaux. L'option pour chaque stratégie peut être changée en naviguant vers :

> La Gestion > les stratégies > [stratégie de Linux] > éditent > des paramètres avancés > ClamAV



Après que le paramètre de la stratégie de définitions poids du commerce soit changé, le nouveau paramètre le prend effet sur les points finaux à la prochaine mise à jour programmée de définition de virus. Ce retard est régi par le paramètre de la stratégie interne de `de mise à jour de contenu de `.

Les « quelques connecteurs doivent être mis à jour pour prendre en charge ce virus que la définition » avertissant peut apparaître dans l'écran de paramètres avancés de ClamAV si au moins un connecteur géré par la stratégie exécute une version incompatible de connecteur de Linux. Il est fortement recommandé pour améliorer les connecteurs et pour résoudre cet avertissement avant d'utiliser l'établissement réservé à la Linux de définitions.

Vérifier le nouveau paramètre au point final

Une fois configurée pour utiliser des définitions réservées à la Linux, la taille de la mémoire résidente combinée des deux processus de connecteur d'AMP devrait être en-dessous de 100 Mo.

Ceci peut être examiné utilisant la commande suivante :

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

Ce qui suit est un résultat témoin :