AMP pour terminaux : Options de définition de virus ClamAV sous Linux

Contenu

Introduction

Àpartir de la version 1.11.0 du connecteur Linux, AMP for Endpoints offre désormais deux options de configuration de définition de virus ClamAV :

1. Linux uniquement
2. ClamAV complet

Avant que l'option Linux uniquement ne devienne disponible, le connecteur Linux a analysé les fichiers à l'aide de l'ensemble complet de définitions de virus ClamAV. Ce jeu inclut les signatures de programmes malveillants pour Linux, macOS, Windows et Android. Bien que cette couverture soit complète, elle nécessite également d'importantes ressources d'exécution (temps processeur et mémoire). Certains systèmes Linux peuvent bénéficier de la configuration d'AMP pour utiliser le plus petit jeu de définitions de virus ClamAV Linux uniquement.

La taille du fichier de définition de virus Linux uniquement est inférieure à 10 % de l'ensemble complet. L'utilisation d'un ensemble plus petit réduit la surcharge de calcul et permet d'exécuter AMP sur des systèmes à ressources limitées. Malgré les avantages en termes de performances, une couverture réduite pour les programmes malveillants autres que Linux rend cette configuration adaptée uniquement à certaines applications. Par exemple, il convient aux serveurs qui hébergent/stockent uniquement des fichiers Linux (tels que des serveurs d'applications) mais ne convient pas aux serveurs qui hébergent/stockent également des fichiers non Linux (tels que des serveurs FTP, de messagerie et de fichiers SMB). L'administrateur système doit équilibrer cette compensation pour choisir l'ensemble approprié de définitions de virus.

IMPORTANT !

Il est fortement recommandé de mettre à niveau tous les terminaux vers Connector version 1.11.0 ou ultérieure avant d'utiliser la nouvelle option de définition de virus Linux uniquement. Bien que les versions 1.10.x et antérieures de Connector acceptent la nouvelle option, son comportement dans certains cas ne sera pas intuitif. Reportez-vous à la section *Rétrocompatibilité* pour plus de détails.

Rétrocompatibilité

Il y a un problème de compatibilité descendante important à prendre en compte avant de

configurer les points de terminaison pour utiliser la nouvelle option de définition de virus Linux uniquement : 1.10.x et les connecteurs plus anciens continueront à utiliser la définition complète du virus si le jeu complet a déjà été téléchargé. S'il est configuré pour utiliser la nouvelle option de définition de virus Linux uniquement, le connecteur arrêtera de mettre à jour l'ensemble complet des définitions de virus et ne mettra à jour que la définition de virus Linux définie par la suite. Cela peut entraîner l'utilisation de définitions de virus Linux à jour, mais de définitions macOS, Windows et Android obsolètes.

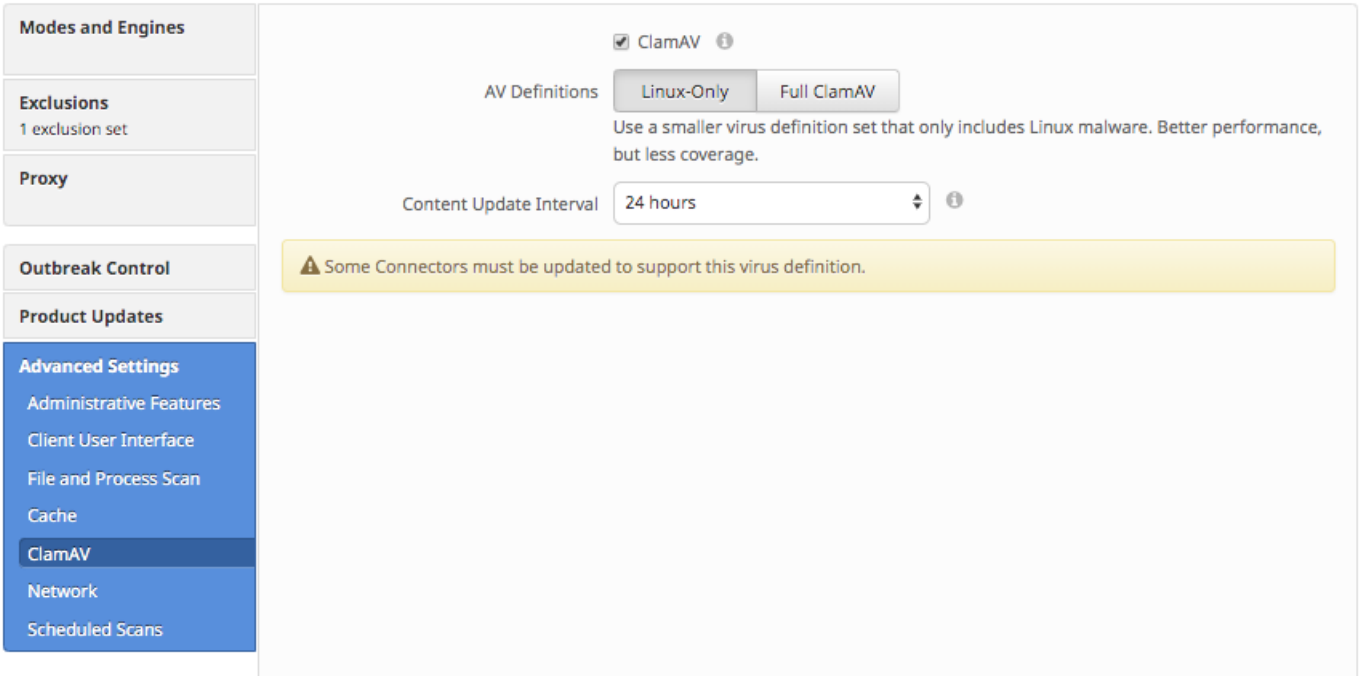
Il existe deux résolutions possibles :

1. Mettez à niveau le connecteur vers la version 1.11.0 ou ultérieure.
2. Remplacez le paramètre Définition du virus ClamAV par Full ClamAV.

Modification de l'option ClamAV Virus Definitions

L'option ClamAV Virus Definition peut être configurée à l'aide du portail Web AMP for Endpoints. Pour modifier l'option de chaque stratégie, accédez à :

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



Une fois le paramètre de stratégie Définitions AV modifié, le nouveau paramètre prend effet sur les points d'extrémité lors de la prochaine mise à jour planifiée de la définition de virus. Ce délai est régi par le paramètre de stratégie « Mise à jour du contenu interne ».

L'avertissement « Certains connecteurs doivent être mis à jour pour prendre en charge cette définition de virus » peut apparaître dans l'écran ClamAV Advanced Settings si au moins un connecteur géré par la stratégie exécute une version de connecteur Linux incompatible. Il est fortement recommandé de mettre à niveau les connecteurs et de résoudre cet avertissement avant d'utiliser le paramètre de définitions Linux uniquement.

Vérification du nouveau paramètre au point de terminaison

Lorsqu'elle est configurée pour utiliser des définitions Linux uniquement, la taille de mémoire résidente combinée des deux processus du connecteur AMP doit être inférieure à 100 Mo.

Vous pouvez l'examiner à l'aide de la commande suivante :

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

Voici un exemple de résultat :