Comprendre l'alerte « Limite de chargement atteinte » sur ESA avec AMP

Contenu

Introduction

Ce document décrit l'alerte « Limite de chargement atteinte » lancée par l'appliance de sécurité de la messagerie électronique (ESA) lorsqu'elle est configurée pour analyser les e-mails avec la fonctionnalité Advanced Malware Protection (AMP).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Dispositif de sécurité de la messagerie
- Protection avancée contre les programmes malveillants

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Appareil de sécurité de la messagerie (ESA) exécutant le logiciel 12.x

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

L'appliance de sécurisation de la messagerie (ESA) utilise la fonctionnalité Advanced Malware

Protection (AMP) qui contient deux fonctions principales :

- Réputation des fichiers
- Analyse de fichiers

L'analyse des fichiers télécharge les pièces jointes des messages pour l'analyse sandbox sur les serveurs ThreatGrid Cloud.

Comprendre l'alerte « Limite de chargement atteinte »

Le suivi des messages peut indiquer que les e-mails n'ont pas été analysés par Advanced Malware Protection (AMP) car ils ont atteint la limite de téléchargement.

Exemple :

```
02 Dec 2019 14:11:36 (GMT +01:00) Message 12345 is unscannable by Advanced Malware Protection engine. Reason: Upload Limit Reached
```

Dans le nouveau modèle de limites d'échantillon ThreatGrid, ces limites correspondent au nombre d'échantillons que les périphériques sont autorisés à télécharger pour l'analyse de fichiers par organisation. Tous les périphériques intégrés (WSA, ESA, CES, FMC, etc.) ainsi qu'AMP for Endpoints ont droit à 200 échantillons par jour, quel que soit le nombre de périphériques.

Il s'agit d'une limite partagée (et non d'une limite par périphérique), qui s'applique aux licences achetées après le 12/1/2017.

> **Note**: Ce compteur n'est pas réinitialisé tous les jours, mais fonctionne comme une période de 24 heures.

Exemple :

Dans une grappe de 4 ESA avec une limite de 200 échantillons téléchargés, si l'ESA1 télécharge 80 échantillons à 10:00 aujourd'hui, alors seulement 120 échantillons supplémentaires peuvent être téléchargés parmi les 4 ESA (limite partagée) d'aujourd'hui à 10:01 jusqu'à demain à 10:00, lorsque les 80 premiers emplacements sont libérés.

Comment pouvez-vous vérifier le nombre d'échantillons que vos ESA ont téléchargés au cours des dernières 24 heures ?

ESA : Accédez à **Monitor > AMP File Analysis** report et cochez la section **Files Uploaded for Analysis**.

SMA : accédez à **Email > Reporting > AMP File Analysis** report et cochez la section **Files Uploaded for Analysis**.

> **Note**: Si le rapport d'analyse de fichier AMP ne contient pas de données précises, consultez la section Détails de l'analyse de fichier dans le cloud sont incomplets du Guide de l'utilisateur.

Avertissement : Référez-vous à la CSCvm10813 défectueuse pour les informations supplémentaires.

Vous pouvez également exécuter une commande **grep** à partir de l'interface de ligne de commande pour compter le nombre de fichiers téléchargés.

Cette opération doit être effectuée sur chaque appliance.

Exemple :

```
grep "Dec 20.*File uploaded for analysis" amp -c
grep "Dec 21.*File uploaded for analysis" amp -c
```

Vous pouvez utiliser des expressions régulières PCRE pour faire correspondre la date et l'heure.

Comment pouvez-vous étendre la limite de téléchargement ?

Contactez votre responsable de compte ou votre ingénieur commercial Cisco.

Informations connexes

- Approfondissement de l'intégration d'AMP et de Threat Grid avec Cisco Email Security
- Vérification des chargements d'analyse de fichier sur ESA
- Support et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.