Dépanner l'erreur " ; Catégorie non analysable = Erreur de message, Motif non analysable = Erreur d'archivage" ; dans le SEC

Table des matières

Introduction

Conditions préalables

- Exigences
- Composants utilisés

Informations générales

Problème

Environnement

Motif

Solution

- Avant de commencer : Vérification et sélection d'une option
- Option 1. Ajouter une balise d'objet aux pièces jointes non analysables
- Option 2. Mettre en quarantaine les messages non analysables dans la quarantaine des virus de stratégie et des attaques

Informations connexes

Introduction

Ce document décrit comment dépanner l'erreur "Unscannable Category = Message Error, Unscannable Reason = Archive Error : Dépassement de la limite de taille totale des « fichiers non archivés » dans un ESA Cisco.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Appliance de sécurisation de la messagerie Cisco (ESA)
- Cisco Advanced Malware Protection (AMP)

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations de ce document ont été créées à partir de périphériques dans un environnement de travaux pratiques spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Examiner l'impact potentiel de toute modification avant de l'appliquer dans un réseau de production.

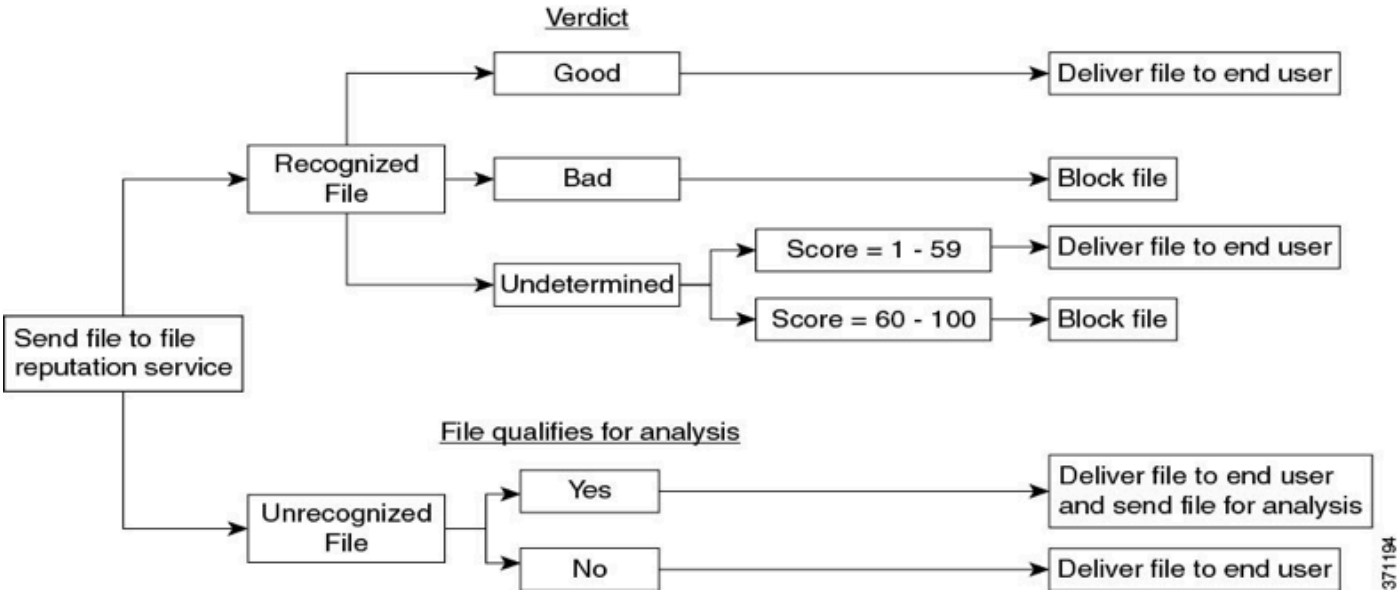
Informations générales

Lorsqu'un message avec une pièce jointe atteint Advanced Malware Protection (AMP) dans le pipeline de traitement du courrier, c'est-à-dire l'étape ESA où l'analyse des pièces jointes a lieu, ESA tente d'analyser la pièce jointe. ESA vérifie également la conformité des en-têtes de message avec le document RFC 2045 (Request for Comments) (RFC 2045). Si le message n'est pas entièrement conforme, ESA fait tout de même une tentative d'analyse de la pièce jointe.

ESA vérifie ensuite si la pièce jointe est un fichier d'archive. Si c'est le cas, ESA tente de le déballer. ESA évalue plusieurs facteurs afin d'estimer la taille non compressée et de s'assurer que l'archive est valide. ESA détecte également les archives suspectes, telles que les fichiers fortement compressés.

Si aucun verdict de réputation de fichier n'est disponible à partir de la recherche de réputation dans le cloud et si le fichier répond aux critères d'analyse, ESA le met en quarantaine et le télécharge dans le sandbox AMP, c'est-à-dire dans l'environnement d'analyse de fichiers basé dans le cloud.

ESA ouvre ensuite une connexion aux serveurs AMP, télécharge le fichier et attend les mises à jour des verdicts, comme le montre l'image :



ESA fournit un verdict basé sur ces scénarios :

- Si l'un des fichiers extraits est malveillant, le service de réputation des fichiers renvoie le verdict « Malveillant » pour le fichier compressé ou le fichier d'archive.
- Si le fichier compressé ou le fichier d'archive est malveillant et que tous les fichiers extraits sont sains, le service de réputation des fichiers renvoie le verdict « Malveillant » pour le fichier compressé ou le fichier d'archive.
- Si le verdict de l'un des fichiers extraits est inconnu, les fichiers extraits sont éventuellement (s'ils sont configurés et si le type de fichier est pris en charge pour l'analyse de fichier) envoyés pour l'analyse de fichier.
- Si le verdict de l'un des fichiers extraits ou des pièces jointes est faible, le fichier n'est pas envoyé pour analyse.
- Si l'extraction d'un fichier compressé ou archivé échoue pendant la décompression, le service de réputation des fichiers renvoie un verdict d'analyse impossible pour ce fichier compressé ou archivé. Si l'un des fichiers extraits est malveillant dans ce scénario, le service de réputation des fichiers renvoie le verdict « Malveillant » pour le fichier compressé ou archivé. Le verdict malveillant a priorité sur le verdict impossible à analyser.

Les fichiers fortement compressés tels que CSV, XML et TXT peuvent dépasser la taille de fichier maximale codée en dur dans ESA. Des algorithmes de compression tels que Lempel-Ziv, génèrent une carte numérique qui compte le nombre et la position des caractères dans le document complet. Ce processus peut produire de très petites tailles de fichiers d'archive.

En revanche, les fichiers contenant des graphiques ou des formats tels que PDF, JPG et PNG ne sont pas compressés de la même manière. Par conséquent, ils restent généralement proches de leur taille de fichier d'origine.

Problème

ESA enregistre un verdict AMP non analysable pour une pièce jointe compressée avec la raison "Erreur d'archivage : Dépassement de la limite de taille totale des fichiers non archivés."

Environnement

- ESA Cisco
- AMP activé pour l'analyse des pièces jointes

Motif

La pièce jointe est une archive compressée qui s'étend au-delà de la limite codée en dur ESA pour la taille totale des fichiers non archivés. Les types de fichiers hautement compressibles (par exemple, CSV, XML et TXT) peuvent produire de petites archives qui s'étendent considérablement lorsqu'elles sont décompressées, ce qui peut déclencher un verdict « Unscan ».

Solution

Utilisez l'une de ces options en fonction de la gestion souhaitée : notification utilisateur, ou confinement et révision. Les étapes de vérification présentées permettent de déterminer l'option à utiliser.

Afin de confirmer la condition, localisez le type mentionné d'entrée de journal de messagerie.

Exemple d'entrée de journal de messagerie :

```
Info:   The attachment could not be scanned. File Name = 'ACTS Chopped ISO 88591 encod_NoSchema.XML.zip
```

Avant de commencer : Vérification et sélection d'une option

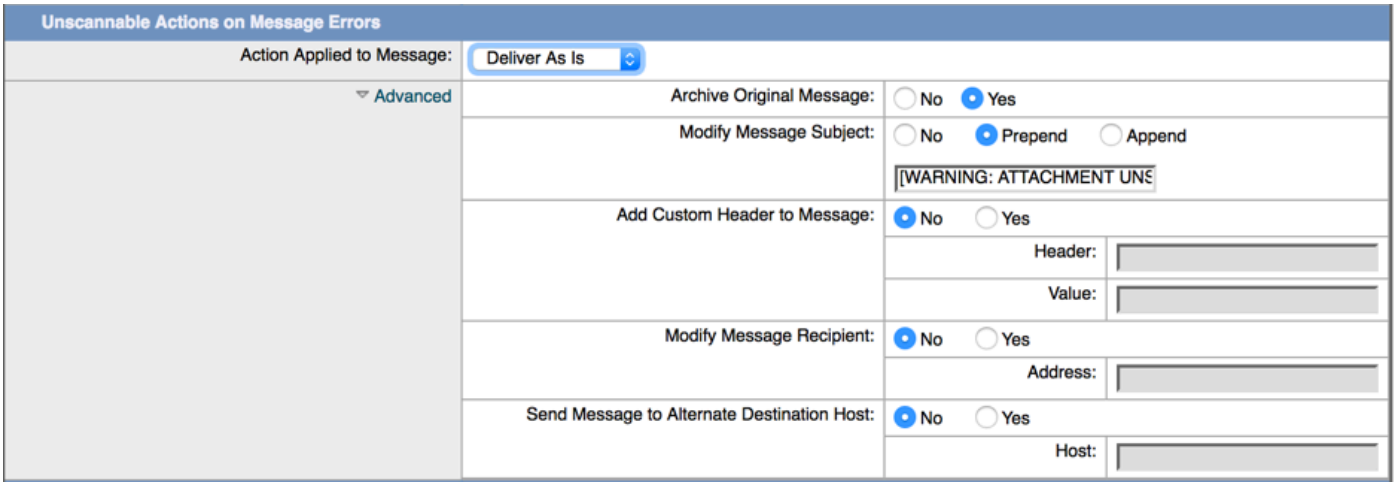
1. Dans ESA, accédez à Monitor > Mail Logs.
2. Recherchez l'ID de message (MID) qui indique Motif de l'impossibilité d'analyse = Erreur d'archivage : Dépassement de la limite de taille totale des fichiers non archivés.
3. Vérifiez que la pièce jointe est une archive compressée, par exemple un fichier .zip, et qu'elle s'étend de manière significative lorsqu'elle est décompressée.
4. Choisissez l'option 1 si le message doit être remis et que le destinataire n'a besoin que d'un avertissement dans la ligne d'objet.

5. Choisissez l'option 2 si le message doit être contenu pour révision dans la quarantaine Virus de stratégie et attaque (PVO).
6. Après avoir appliqué la modification, envoyez un message test avec une archive représentative. Vérifiez le comportement attendu dans Monitor > Mail Logs et, s'il est utilisé, dans la quarantaine Policy Virus and Outbreak (PVO) .

Option 1. Ajouter une balise d'objet aux pièces jointes non analysables

1. Dans ESA, accédez à Politiques de messagerie > Politiques de messagerie entrante ou Politiques de messagerie sortante, selon l'endroit où l'analyse AMP est activée.
2. Cliquez sur la stratégie qui gère le message affecté.
3. Dans les paramètres AMP de la stratégie, recherchez l'action Unscannable attachments.
4. Définissez Modify Message Subject sur Prepend.
5. Dans le champ d'objet, saisissez le préfixe [AMP Unscannable] ou une autre balise d'avertissement approuvée.
6. Cliquez sur Submit et validez la modification.
7. Envoyez un message de test avec une archive représentative et vérifiez que l'ESA envoie le message avec la balise d'objet ajoutée.

Remarque : Utilisez cette option lorsque la remise du message doit continuer mais que les destinataires doivent recevoir un avertissement clair indiquant qu'AMP n'a pas analysé la pièce jointe.



Option 2. Mettre en quarantaine les messages non analysables dans la quarantaine des virus de stratégie et des attaques

1. Dans ESA, accédez à Politiques de messagerie > Politiques de messagerie entrante ou Politiques de messagerie sortante, selon l'endroit où l'analyse AMP est activée.

2. Cliquez sur la stratégie qui gère le message affecté.
3. Dans les paramètres AMP de la stratégie, recherchez l'action Unscannable attachments.
4. Définissez l'action de message non analysable sur Quarantaine.
5. Sélectionnez la quarantaine Virus de stratégie et attaques (PVO) comme destination de quarantaine.
6. Cliquez sur Submit et validez la modification.
7. Envoyez un message test avec une archive représentative et vérifiez que ESA place le message dans la quarantaine des virus et des attaques de stratégie (PVO) pour examen par un analyste.



Remarque : Utilisez cette option lorsque le message doit être contenu pour une analyse plus approfondie au lieu d'être remis au destinataire.

Informations connexes

- Guide des meilleures pratiques pour la protection avancée contre les programmes malveillants sur ESA
- Vérification des chargements d'analyse de fichier sur ESA
- Dépannage de l'erreur « Le service de réputation de fichiers n'est pas accessible » sur Cisco ESA
- Assistance technique de Cisco et téléchargements

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.