对ESA中的“无法扫描的类别=消息错误，无法扫描的原因=存档错误：超过未存档文件总大小限制”错误进行故障排除

目录

简介

本文档介绍如何对邮件安全设备(ESA)中的错误“Unscannable Category = Message Error，Unscannable Reason = Archive Error: Exceeded the total size limit of the unarchived files”进行故障排除。

先决条件

要求

Cisco 建议您了解以下主题：

- ESA
- 思科高级恶意软件防护(AMP)

使用的组件

本文档中的信息基于以下软件和硬件版本：

- ESA AsyncOS 11.1.2-023。
- ESA AsyncOS 12.0.0-419。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

背景信息

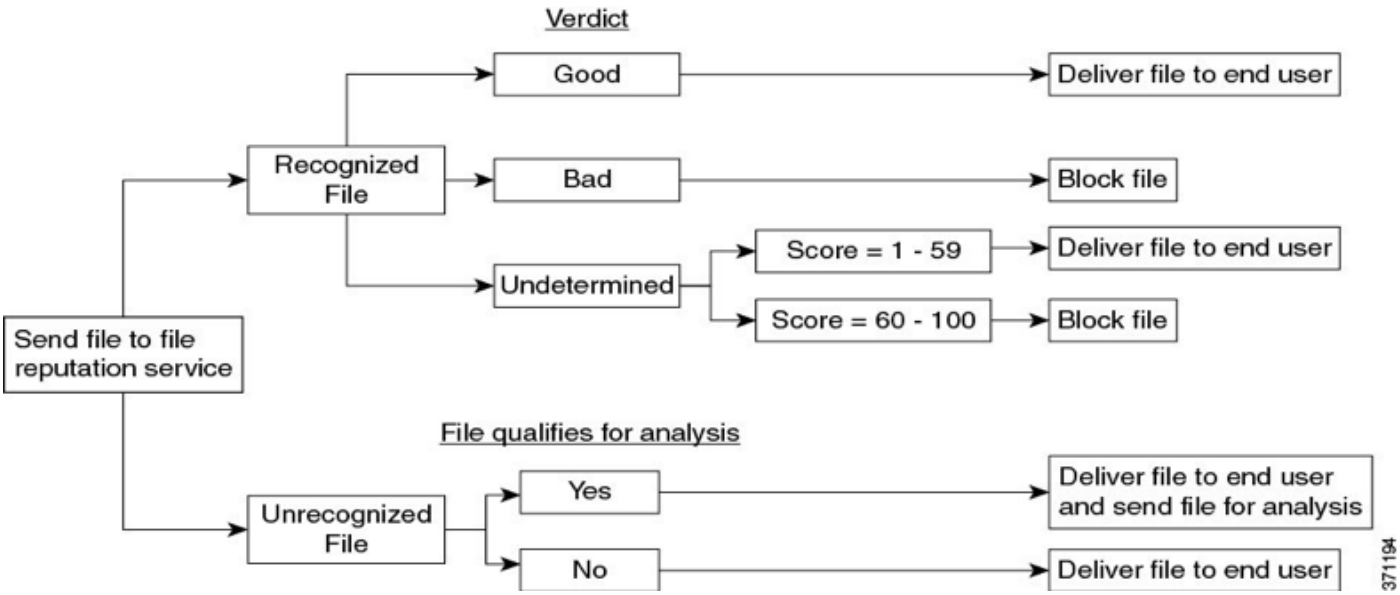
当带有附件的邮件到达管道中的AMP时，ESA尝试解析邮件中的附件并检查邮件信头(检查是否符合

RFC 2045)。 即使邮件不完全兼容，ESA仍会尽力解析附件。

下一步是检查附件是否为存档文件，如果是，ESA会尝试将其解包，它会考虑多个因素以确定压缩文件大小，以确保附件是合法的，而不是压缩文件。

如果找不到文件信誉，并且文件符合分析标准，则会将其隔离并上传到沙盒。

然后，ESA打开与AMP服务器的连接，上传文件并等待判定更新，如图所示：



ESA根据以下场景做出判断：

- 如果提取的文件之一为恶意文件，则文件信誉服务会针对压缩文件或存档文件返回判定为Malicious。
- 如果压缩或存档文件是恶意的，并且提取的所有文件都是干净的，则文件信誉服务会针对压缩或存档文件返回恶意判定。
- 如果任何提取文件的判定是未知的，则会选择性地发送提取的文件进行文件分析（如果已配置并支持文件类型进行文件分析）。
- 如果任何提取的文件或附件的判定风险较低，则不会发送该文件进行文件分析。
- 如果文件解压缩后解压缩失败，然后该文件被压缩或存档，则文件信誉服务会针对压缩或存档文件返回Unscannable判定。请记住，在此场景中，如果提取的其中一个文件是恶意的，则文件信誉服务会针对压缩文件或存档文件返回一个Malicious判定（Malicious判定优先于Unscannable判定）。

诸如csv、xml、txt等高度压缩的文件可能会超过硬编码为ESA的最大文件大小，而压缩算法(如Lempel-Ziv*)会生成一个数字映*射，计算整个文档中的字符数量和位置，这样生成的文件大小非常小。

另一方面，包含图形、文本格式（如pdf、jpg、png）的文件不是以相同方式压缩的，因此它们几乎保留原始文件大小。

问题

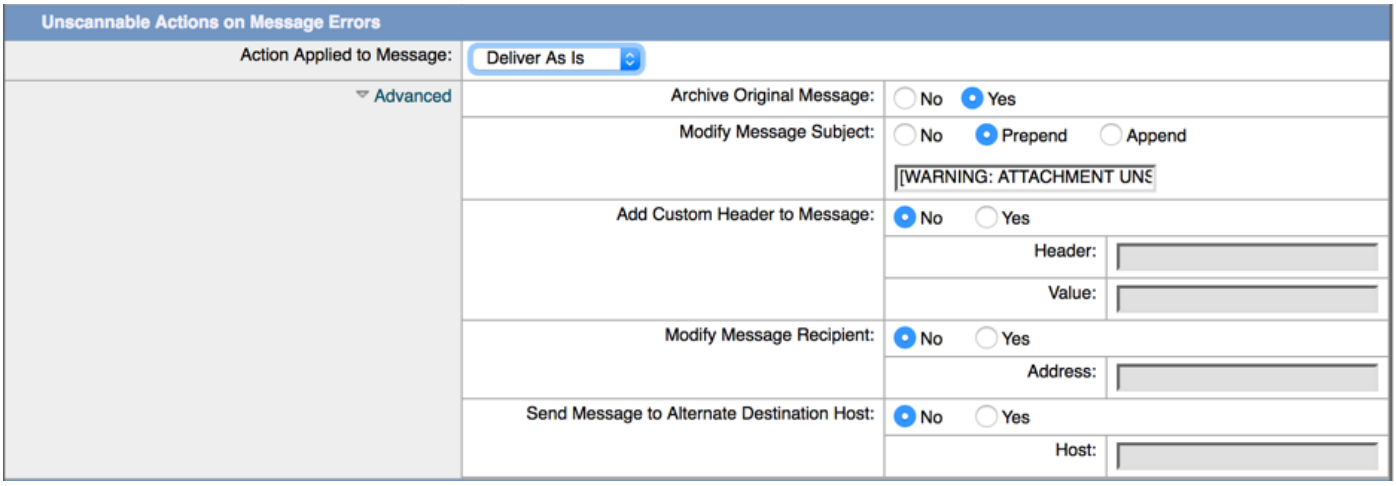
当ESA收到压缩附件中的邮件，且邮件超出最大压缩比，并且ESA无法计算附件的文件大小时，结

果会出现以下错误日志：

“Wed Feb 13 20:03:47 2019信息： 无法扫描附件。文件名= 'ACTS截断ISO 88591 encod_NoSchema.XML.zip',MID = 226,SHA256 =7efa6154b7519872055cff10a69067dcad88562f708b284a390a9abcf5e99b8f，不可扫描类别=消息错误，不可扫描原因=存档错误： 已超过未存档文件的大小限制”

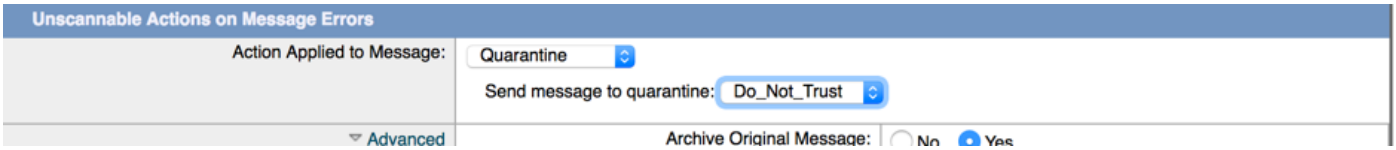
解决方案 1

在Subject中预置不可扫描的邮件，以提醒用户文件未由AMP服务分析，如图所示。



解决方案 2

无法扫描到策略病毒和爆发(PVO)隔离区，以进行进一步分析。如图所示.



相关信息

- 思科邮件安全设备AsyncOS 12.0用户指南 — GD（通用部署）
- 在内容安全产品上启用AMP(ESA/WSA)
- 验证ESA上的文件分析上传
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。