对错误"；无法扫描的类别=消息错误，无法扫描的原因=存档错误"；进行故障排除在ESA中

目录

[简介](#)

[先决条件](#)

- [要求](#)
- [使用的组件](#)

[背景信息](#)

[问题](#)

[环境](#)

[原因](#)

[解决方案](#)

- [开始使用前:验证并选择选项](#)
- [选项1.为不可扫描的附件预置主题标签](#)
- [选项2.隔离策略病毒和爆发隔离区中无法扫描的邮件](#)

[相关信息](#)

简介

本文档介绍如何对错误“无法扫描的类别=消息错误，无法扫描的原因=存档错误：已超过思科ESA中未存档文件“ ”的总大小限制。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科邮件安全设备(ESA)
- 思科高级恶意软件防护(AMP)

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息在特定实验室环境设备上创建。用于本文的所有设备从已清除的配置开始。在将任何更改应用于生产网络之前，请审查更改的潜在影响。

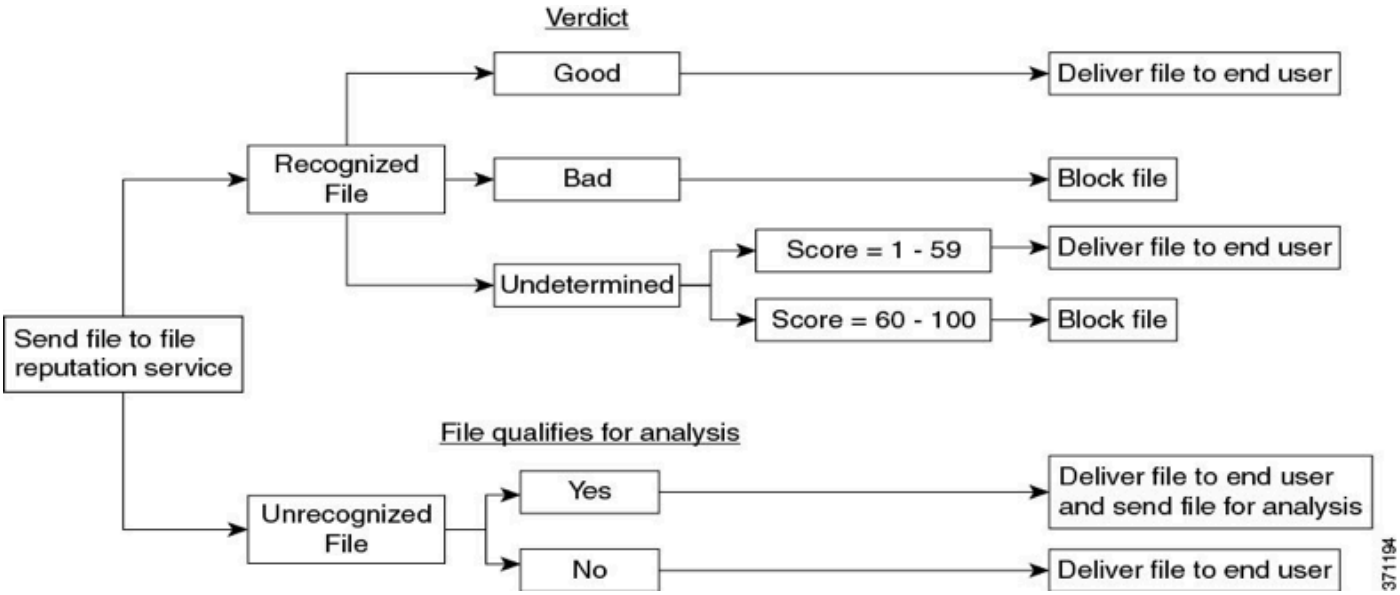
背景信息

当带有附件的邮件到达邮件处理管道中的高级恶意软件防护(AMP)（即进行附件扫描的ESA阶段）时，ESA会尝试解析附件。ESA还会检查邮件报头是否符合请求注解(RFC)2045(RFC 2045)。 如果邮件不完全兼容，ESA仍会尽力尝试解析附件。

接下来，ESA检查附件是否为存档文件。如果是，ESA会尝试将其解包。ESA评估多个因素以估计未压缩的大小并确保存档有效。ESA还会检测可疑存档，例如高度压缩的文件。

如果云信誉查找中没有可用的文件信誉判定，并且文件符合分析标准，则ESA会隔离该文件并将其上传到AMP沙盒（即基于云的文件分析环境）。

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“恶意”判定。
- 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（如果已配置且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。

- 如果解压缩期间对压缩或存档文件的解压缩失败，文件信誉服务会对该压缩或存档文件返回无法扫描的判定。如果提取的其中一个文件在此情况下是恶意的，则文件信誉服务会针对压缩或存档文件返回“恶意”判定。恶意裁决优先于不可扫描的裁决。

高度压缩的文件（如CSV、XML和TXT）可能会超过硬编码到ESA的最大文件大小。压缩算法（如Lempel-Ziv）生成数字地图，计算整个文档中的字符数量和位置。此过程可以产生非常小的存档文件大小。

相反，包含图形或格式（如PDF、JPG和PNG）的文件不会以相同方式压缩。因此，它们通常保持接近其原始文件大小。

问题

ESA记录压缩附件的AMP不可扫描判定，原因为“存档错误：已超出未存档文件的大小限制。"

环境

- 思科ESA
- AMP已启用附件扫描

原因

附件是一种压缩存档，其扩展超出了ESA硬编码限制中未存档文件总大小。高度可压缩的文件类型（例如，CSV、XML和TXT）可以生成在解压缩时显着扩展的小型存档，这可能触发“无法扫描”判定。

解决方案

根据所需的处理使用以下选项之一：用户通知，或包容和审查。显示的验证步骤有助于确定要使用的选项。

要确认情况，请找到上述类型的邮件日志条目。

邮件日志条目示例：

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

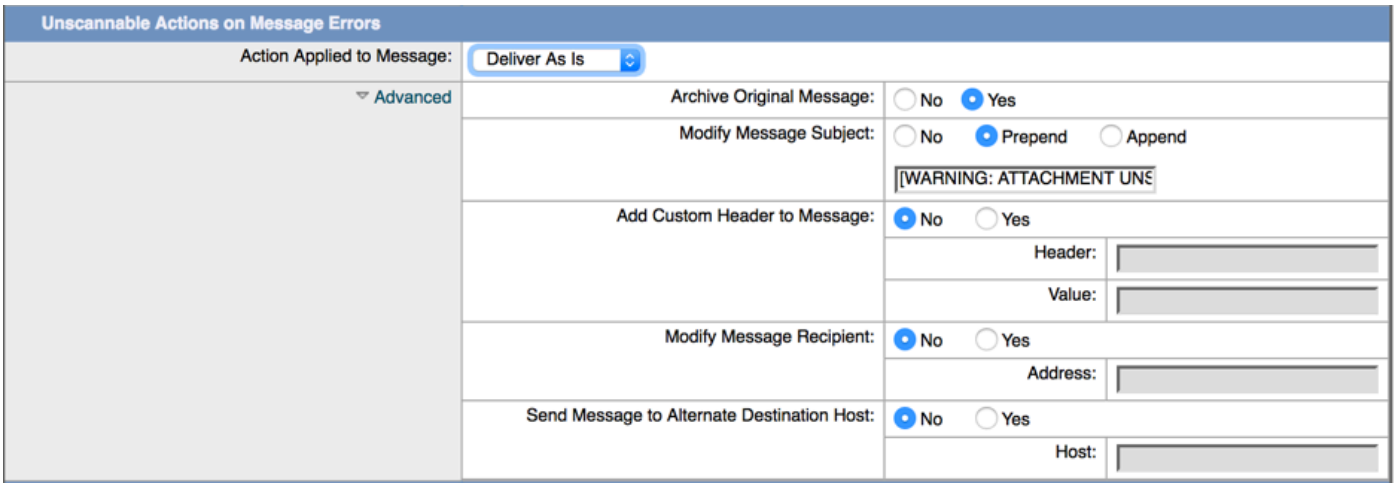
开始使用前:验证并选择选项

1. 在ESA中，导航到监控> 邮件日志。
2. 找到显示Unscannable Reason = Archive Error的消息ID(MID):已超出未存档文件的大小总限制。
3. 确认附件是压缩的存档文件（例如.zip文件），并在解压缩时大幅扩展。
4. 如果必须传送邮件，并且收件人只需要主题行中有警告，请选择Option 1。
5. 如果必须在策略病毒和爆发(PVO)隔离区中查看邮件，请选择Option 2。
6. 应用更改后，发送带有代表性存档的测试消息。验证监控> 邮件日志中的预期行为，如果使用，请验证策略病毒和爆发(PVO)隔离区中的预期行为。

选项1.为不可扫描的附件预置主题标签

1. 在ESA中，根据启用AMP扫描的位置，导航到邮件策略> 传入邮件策略或传出邮件策略。
2. 单击处理受影响邮件的策略。
3. 在策略的AMP设置中，找到Unscannable附件操作。
4. 将修改邮件主题设置为预置。
5. 在主题文本字段中，输入前缀[AMP Unscannable]或其他批准的警告标记。
6. 单击Submit并提交更改。
7. 发送带有代表性存档的测试消息，并验证ESA是否发送带有预先设置的主题标记的消息。

注意：当邮件传送必须继续，但收件人需要明确警告AMP未分析附件时，请使用此选项。



选项2.隔离策略病毒和爆发隔离区中无法扫描的邮件

1. 在ESA中，根据启用AMP扫描的位置，导航到邮件策略> 传入邮件策略或传出邮件策略。

2. 单击处理受影响邮件的策略。
3. 在策略的AMP设置中，找到Unscannable附件操作。
4. 将不可扫描邮件操作设置为Quarantine。
5. 选择Policy Virus and Outbreak(PVO)隔离区作为隔离目标。
6. 单击Submit并提交更改。
7. 发送带有代表性存档的测试邮件，并验证ESA是否将该邮件放在Policy Virus and Outbreak(PVO)隔离区，以供分析人员查看。



注意：当必须包含邮件以供进一步分析而非将邮件传送给收件人时，请使用此选项。

相关信息

- ESA高级恶意软件防护最佳实践指南
- 检验ESA上的文件分析上传
- 对Cisco ESA上的“The File Reputation Service Is Not Reachable”错误进行故障排除
- 思科技术支持和下载

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）。