将ESA配置为跳过将未知MIME类型文件上传到文件分析服务器

目录

简介

本文档介绍跳过将未知MIME类型文件（应用程序/八位字节流）上传到思科ESA中的文件分析服务器的步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- ESA中的高级恶意软件防护(AMP)如何工作。
- 文件MIME类型的基础知识。

Cisco 建议您：

- 已安装物理或虚拟ESA。
- 许可证已激活或已安装。
- 安装向导已完成。

- 对ESA命令行界面(CLI)的管理访问。

使用的组件

本文档适用于AsyncOS 15.5.1、15.0.2及更高版本。

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。

MIME类型

介质类型，也称为多用途Internet邮件扩展(MIME)类型，用于标识文档、文件或字节集合的字符和结构。MIME类型的规范在Internet工程任务组(IETF) RFC 6838中建立并统一。

只要MIME实现知道如何处理字符集，则无法识别的“text”子类型必须被视为子类型“plain”。无法识别的子类型也指定了无法识别的字符集，必须将其视为“application/octet- stream”。

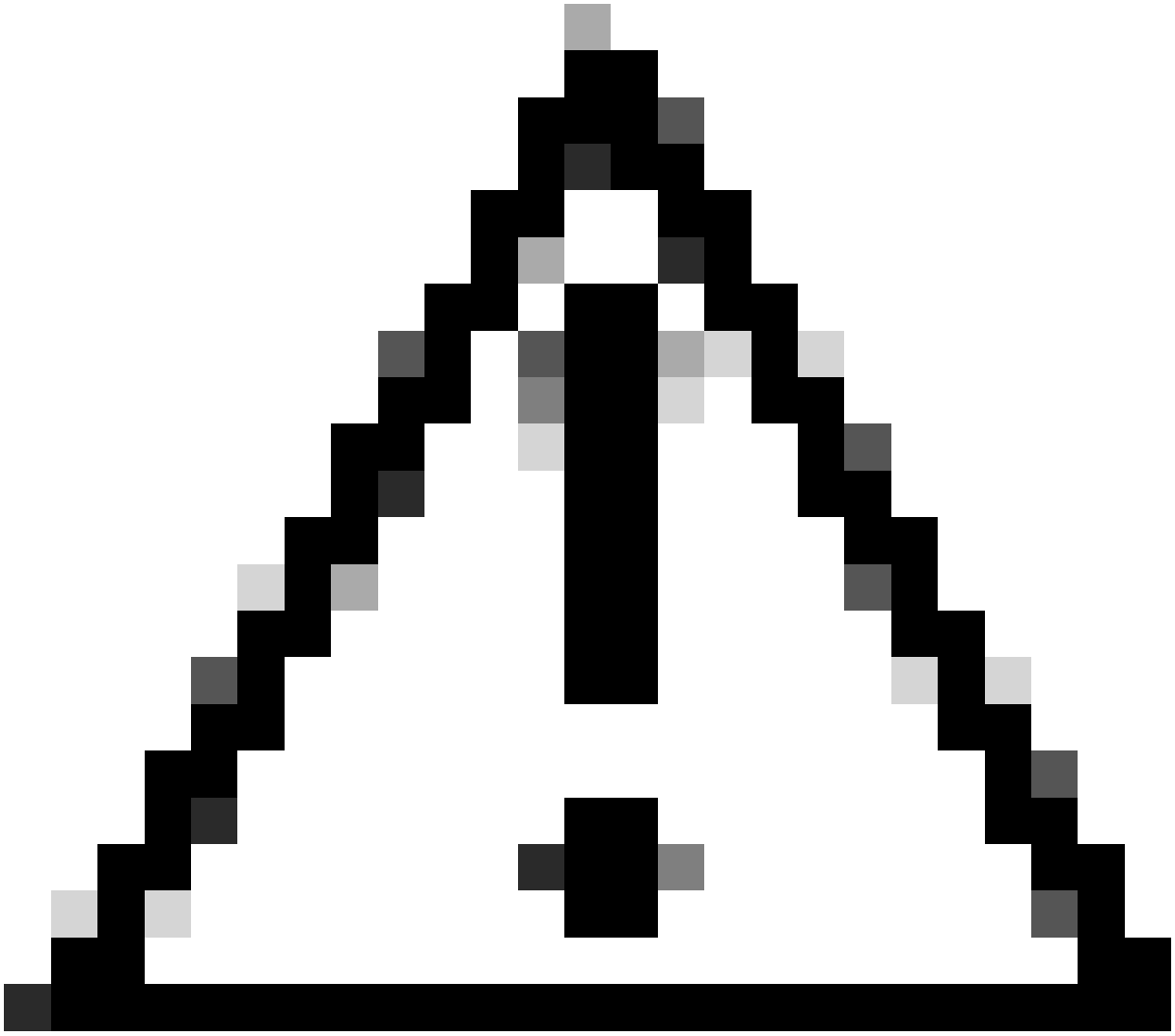
有关更多信息，请参阅RFC 2046 -多用途Internet邮件扩展(MIME)第2部分：媒体类型

ESA设备超过上传限制

如果已启用文件分析服务，并且信誉服务没有关于文件的信息，并且文件满足可分析文件的条件，则可以隔离邮件，并发送文件进行分析。如果尚未将设备配置为在发送附件以供分析时隔离邮件，或者未发送文件以供分析，则会将邮件释放给用户。

有关详情，请参阅“User Guide（用户指南）”。 思科安全邮件网关AsyncOS 15.0用户指南- GD（通用部署）-文件信誉过滤和文件分析[思科安全邮件网关] -思科

我们引入了一个新的CLI命令，以解决由于ESA提交过多的文件以供检查而导致文件提交配额受限的设备过早达到最大上传容量的问题。此增强功能从15.5.1版开始实施，并且正在合并到15.0.2维护版本(MR)及后续版本中。



注意：为了增强安全性，我们强烈建议按照建议上传所有文件。但是，如果您认为对于特定文件类型必须绕过此步骤，则所提供的命令允许您自行决定是否启用此选项。请谨慎行事，了解其中可能涉及的风险。

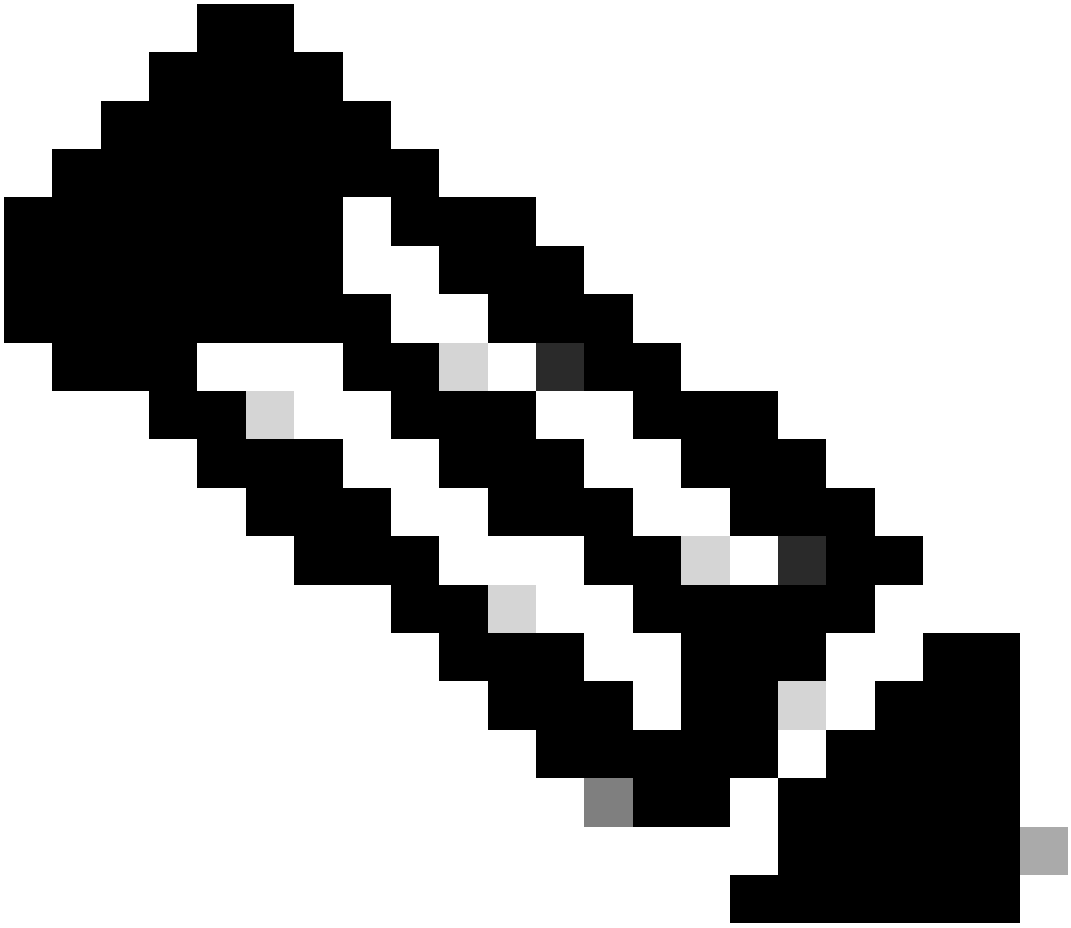
排除要上传到文件分析的应用程序/八位字节流MIME类型

要排除要上传到文件分析服务器进行扫描的应用/八位字节流MIME类型，请使用以下步骤：

步骤1:登录到CLI。

步骤2.运行ampconfig命令

第三步： 键入unknownmimeoverride并按Enter



注意：unknownmimeoverride是一个隐藏命令。

第四步：键入N以回答“Do you want to send unknown mime for analysis only if their extensions are selected ? ”[N]>“

第五步：按Enter键退出向导。

第六步：提交更改

```
ESA_CLI> ampconfig

File Reputation: Enabled
File Analysis: Enabled
Appliance Group ID/Name: Not part of any group yet


Choose the operation you want to perform:
- SETUP - Configure Advanced-Malware protection service.
- ADVANCED - Set values for AMP parameters (Advanced configuration).
```

```
- SETGROUP - Add this appliance to the group of appliances that can share File Analysis reporting
details.
- CACHESETTINGS - Configure the cache settings for AMP.
[]> unknownmimeoverride

Do you want to send unknown mime for analysis only if their extensions are selected? [Y]> N

ESA_CLI>  commit
```

关联缺陷和增强功能

由于以下功能请求和缺陷而引入此新功能：

- HTML和二进制八位数流文件上传到File Analysis中的行为更改会让客户困惑。思科漏洞ID CSCwh61317
- 即使未选择文件类型，也会将p7s文件上传到文件分析。思科漏洞ID CSCwh70476

参考

思科安全邮件网关AsyncOS 15.0用户指南- GD（通用部署）-文件信誉过滤和文件分析[思科安全邮件网关] -思科

RFC 2046 -多用途Internet邮件扩展(MIME)第2部分：媒体类型

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）。