了解带有AMP的ESA上的警报“已达到上传限制”

目录

简介

本文档介绍当邮件安全设备(ESA)配置为使用高级恶意软件防护(AMP)功能扫描邮件时，引发的“已达到上传限制”警报。

先决条件

要求

Cisco 建议您了解以下主题：

- 邮件安全设备
- 高级恶意软件保护

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 运行软件12.x的邮件安全设备(ESA)

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

邮件安全设备(ESA)使用高级恶意软件防护(AMP)功能，该功能包含两个主要功能：

- 文件信誉
- 文件分析

File Analysis会将用于沙盒分析的邮件附件上传到ThreatGrid云服务器。

了解“已达到上传限制”警报

邮件跟踪可以显示高级恶意软件防护(AMP)未扫描邮件，因为它们已达到上传限制。

示例：

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

在新的ThreatGrid样本限制模型中，这些限制是基于每个组织允许设备上传以进行文件分析的样本数。所有集成设备（WSA、ESA、CES、FMC等）以及面向终端的AMP都有权每天获取200个样本，无论设备的数量是多少。

这是一个共享限制（不是每个设备的限制），适用于2017年1月12日之后购买的许可证。

> **注意：**此计数器不会每天重置，相反，它作为24小时滚动周期运行。

示例：

在具有200个上传样本限制的4个ESA集群中，如果ESA1在今天10:00上传80个样本，则从今天10:01到明天10:00（释放前80个插槽），4个ESA（共享限制）中仅可上传120个额外样本。

如何检查过去24小时内您的ESA上传的样本数量？

ESA:导航到**监控(Monitor)> AMP文件分析(AMP File Analysis)报**告，并选中**Files Uploaded for Analysis**部分。

SMA：导航至**邮件>报告> AMP文件分析报**告，并检查**Files Uploaded for Analysis**部分。

> **注意：**如果AMP File Analysis报告未显示准确数据，请查看《用户指南》中Cloud Are Incomplete部分的File Analysis Details。

> **警告：**有关详细信息，请参阅缺陷CSCvm10813。

或者，您可以从CLI运行**grep**命令以计算上传的文件数。

必须在每台设备上执行此操作。

示例：

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

您可以使用PCRE正则表达式来匹配日期和时间。

如何扩展上传限制？

请与您的思科客户经理或销售工程师联系。

相关信息

- 深入探讨AMP和Threat Grid与思科电邮安全的集成
- 检验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）。