恢复由安全终端隔离的文件

目录

简介

本文档介绍如何从安全终端控制台恢复由安全终端连接器隔离的文件。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科安全终端控制台

使用的组件

本文档中的信息基于以下软件版本：

- 安全终端控制台v5.4.2025030619

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。

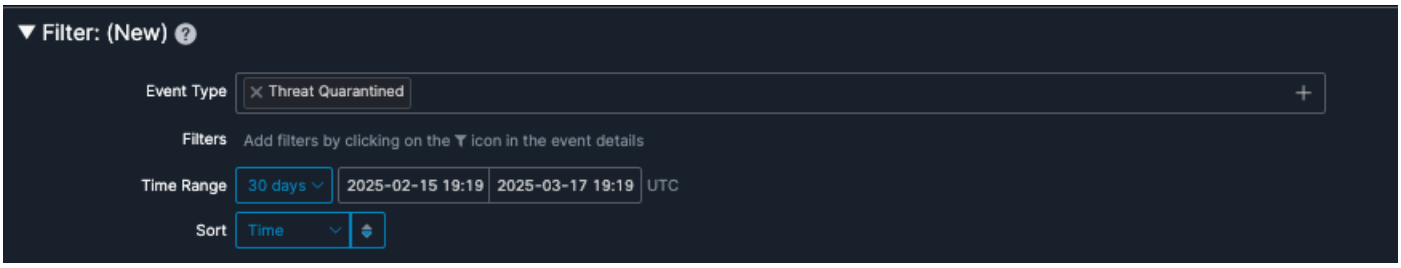
问题

当文件已知安全时，可以检索由安全终端(SE)连接器隔离的文件，以进行文件分析、误报提交或恢复。管理员可以直接从安全终端控制台执行此操作。

解决方案

1.导航到SE控制台上的Events页。

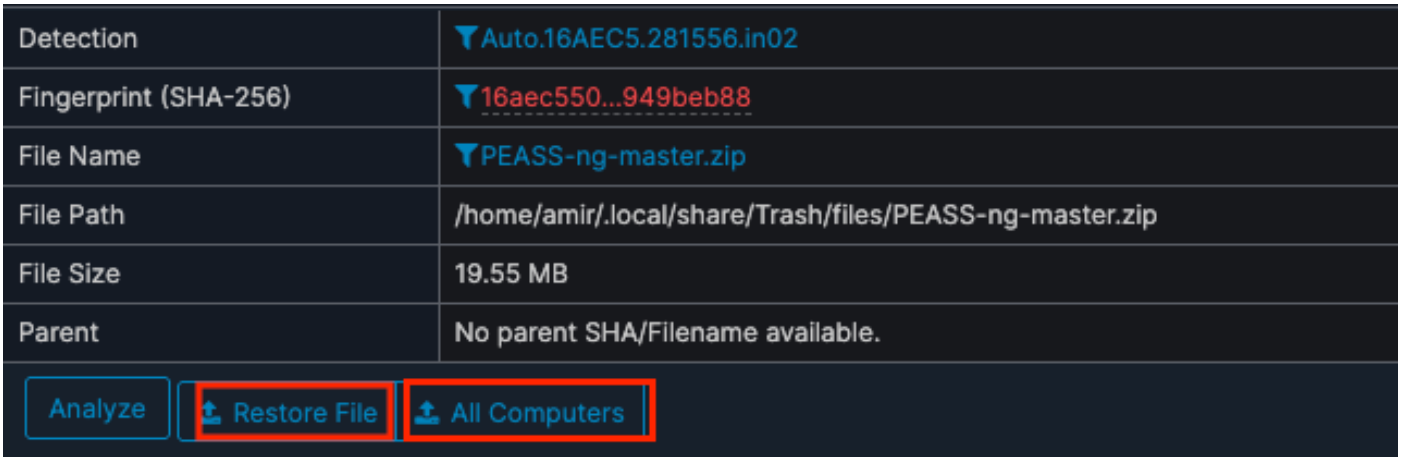
2.通过选择过滤器Event Type = Threat Quarantined，过滤事件以显示所有成功的隔离区。



威胁隔离事件类型

3.识别与需要还原的文件关联的检测事件。

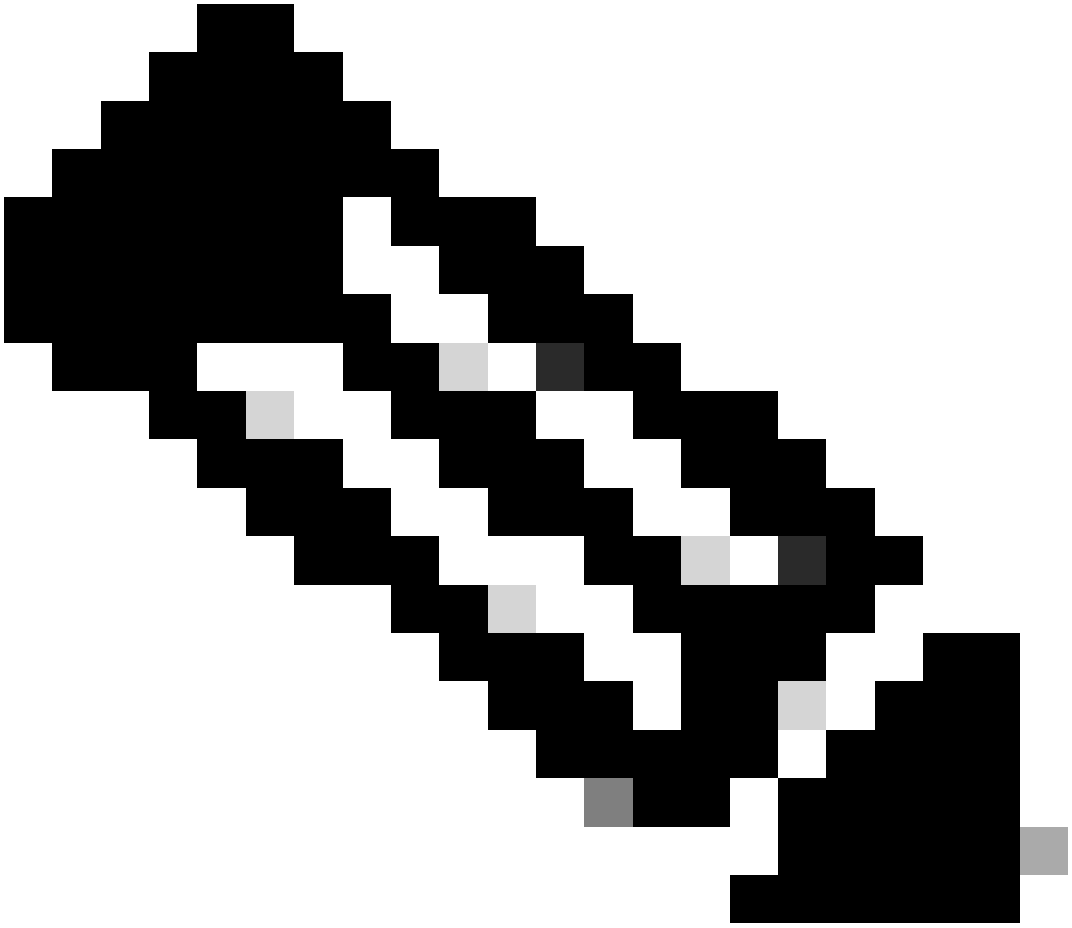
4.展开事件详细信息以访问还原文件选项。选择还原文件将在受影响的计算机上还原文件。选择All Computers将在所有文件被隔离的计算机上恢复文件。



恢复文件选项

5. “检测信号间隔”是连接器呼叫总部以查看是否有任何文件由管理员恢复的频率。一旦受影响的计算机联机或发生下一个检测信号间隔，就会恢复文件。

6.如果文件受信任，请将其添加到允许列表，以防止再次隔离该文件。



注意：文件在隔离区中保留30天，或者在隔离文件夹达到100 MB时清除最旧的文件。清除隔离的文件后，无法再恢复这些文件。

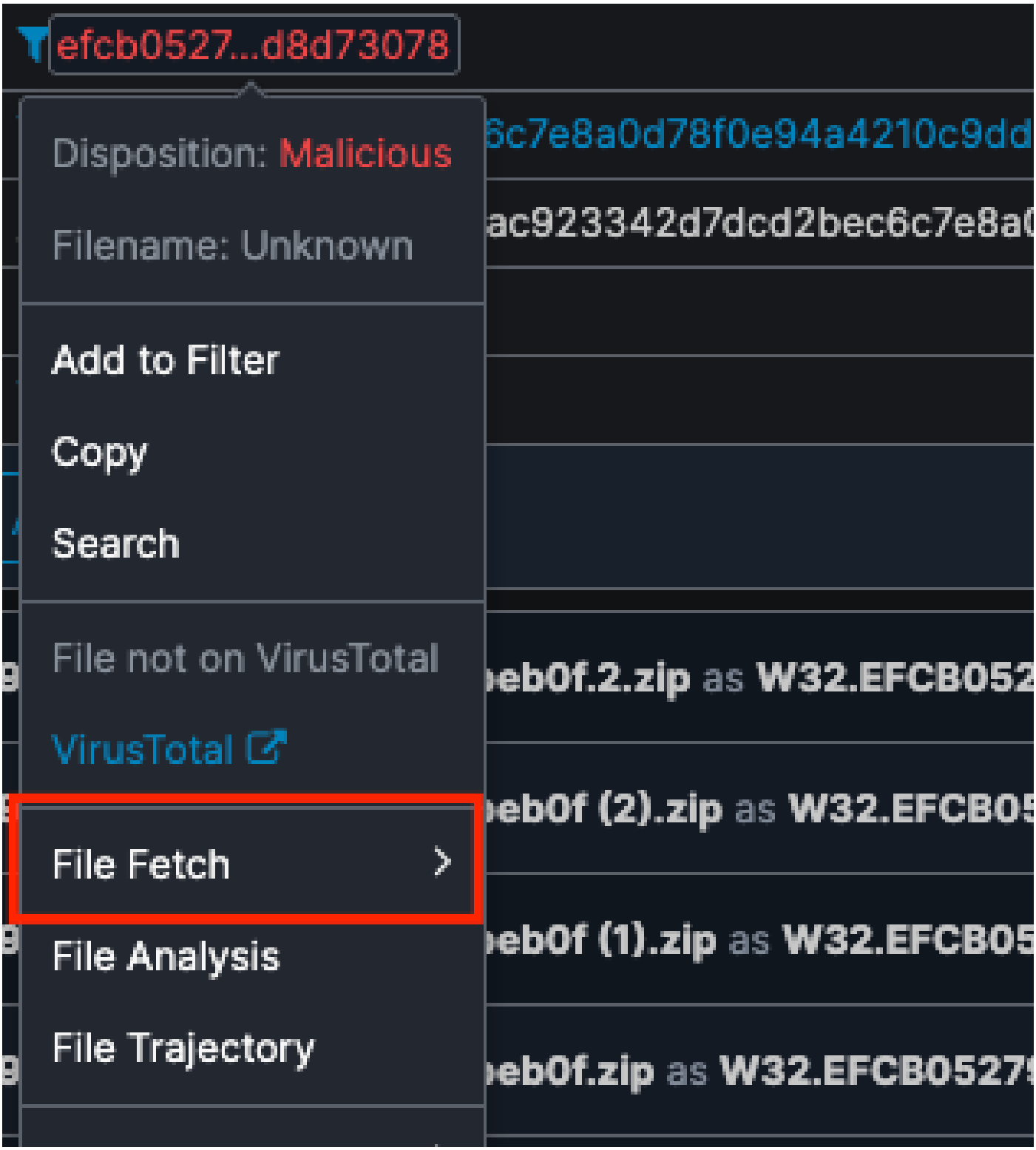
如果只需下载隔离文件以进行威胁分析或进行误报提交，而不将其还原到您的环境中，则可以使用文件获取功能。下载隔离文件的步骤：

1.导航到SE控制台上的Events页。

2.通过选择过滤器Event Type = Threat Quarantined，过滤事件以显示所有成功的隔离区。

3.识别与需要下载的文件关联的检测事件。

4.单击隔离文件的SHA-256值以显示File Fetch选项。



文件获取

这提供了文件提取的状态、启动提取的选项以及在文件存储库中查看文件的访问权限。

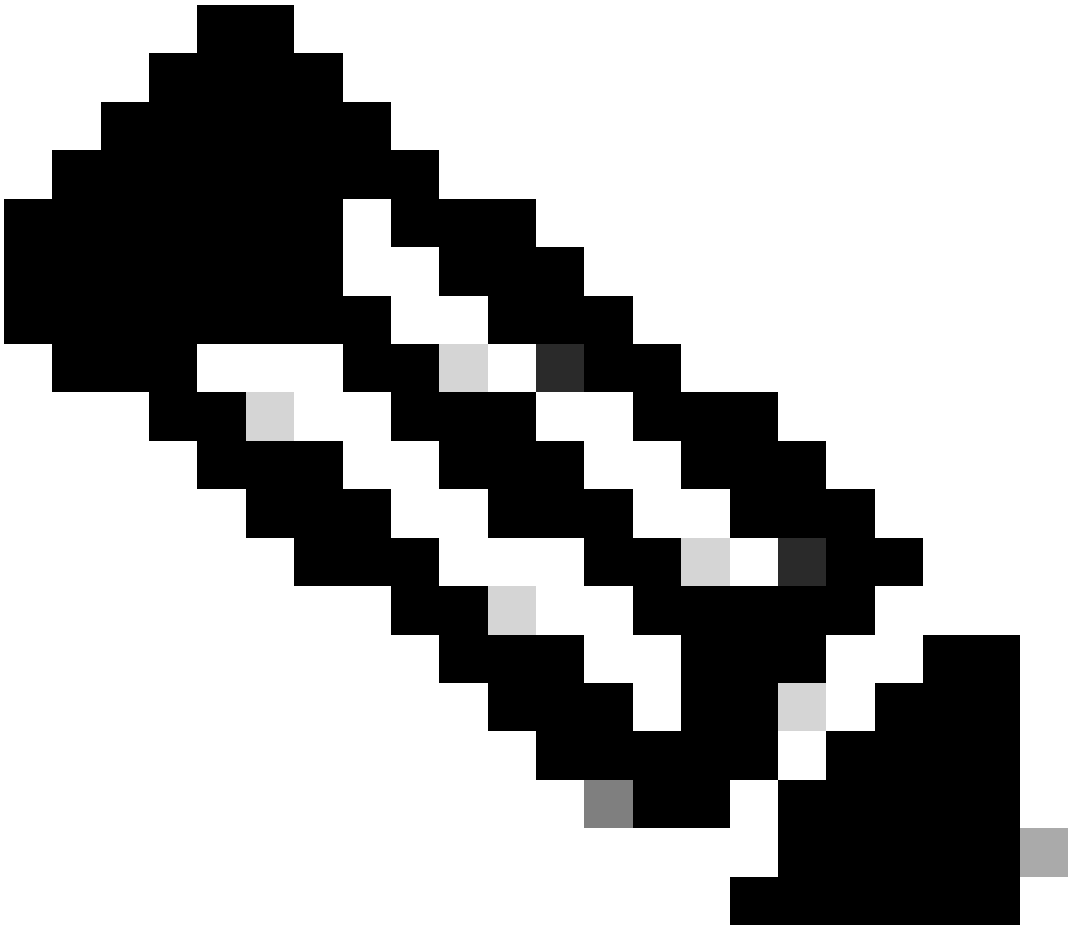
5.单击Fetch File，选择要从中检索文件的计算机，然后单击Fetch进行确认。

6.文件上传到文件存储库后，系统会发送电子邮件通知。

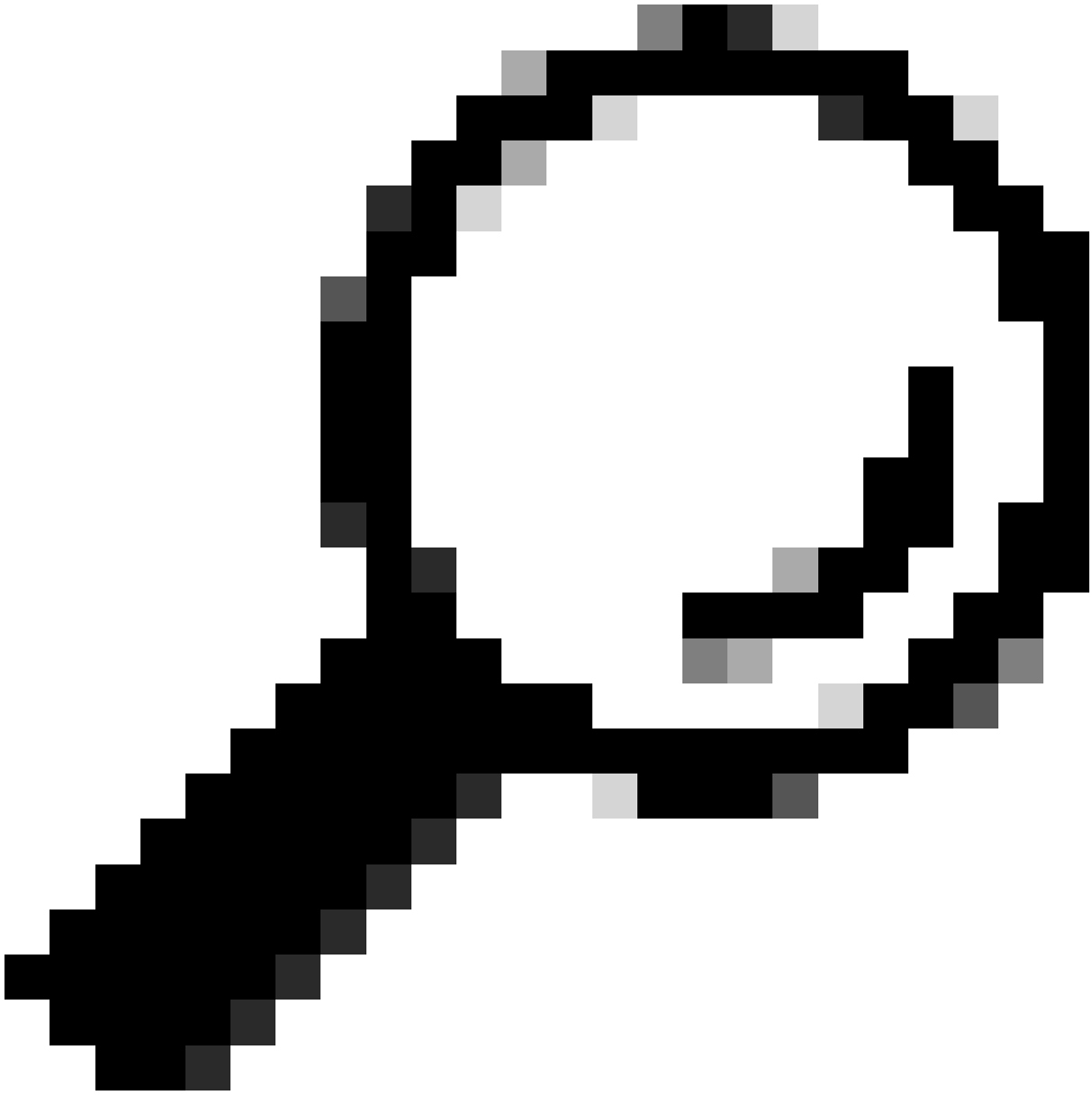
7.文件可用后，您就可以在Analysis >“文件存储库”中看到该文件以及下载该文件的选项。

下载文件

从文件存储库下载的所有文件都经过压缩且受密码保护。



注意：要使文件获取正常工作，必须允许网络流量访问基于云区域的相应文件获取服务器：欧洲:rff.eu.amp.cisco.com北美：rff.amp.cisco.com 亚太地区、日本和中国：rff.apjc.amp.cisco.com。此外，请确保为管理员帐户启用双因素身份验证(2FA)，因为成功启动文件获取请求需要该身份验证。



提示：可以使用Event Type = Quarantined Restore Failed和Event Type = File Fetch Failed过滤事件，以识别失败并分别检查还原和文件提取操作的相应原因。

如果无法按照上述步骤恢复文件，请联系思科TAC并提供位于C:\Program Files\Cisco\AMP\Quarantine目录中的.qrt文件。

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）。