在ESA中配置CEF日志条目和CEF报头

目录

简介

本文档介绍思科安全邮件网关(SEG)的通用事件格式(CEF)日志条目和报头的配置。

先决条件

要求

建议掌握下列主题的相关知识：

- 思科安全邮件网关/邮件安全设备(SEG/ESA)
- 内容过滤器知识
- 日志订阅知识

使用的组件

本文档中的信息基于以下软件和硬件版本：

- 电子邮件安全设备版本14.3

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

统一事件日志将每个消息事件汇总到一个日志行中。使用此日志类型以减少发送到安全信息和事件管理(SIEM)供应商或应用程序进行分析的数据（日志信息）字节数。日志采用大多数SIEM供应商广

泛使用的CEF日志消息格式。

添加CEF日志条目和CEF标头以提供跟踪和组织邮件事件的额外信息。

配置

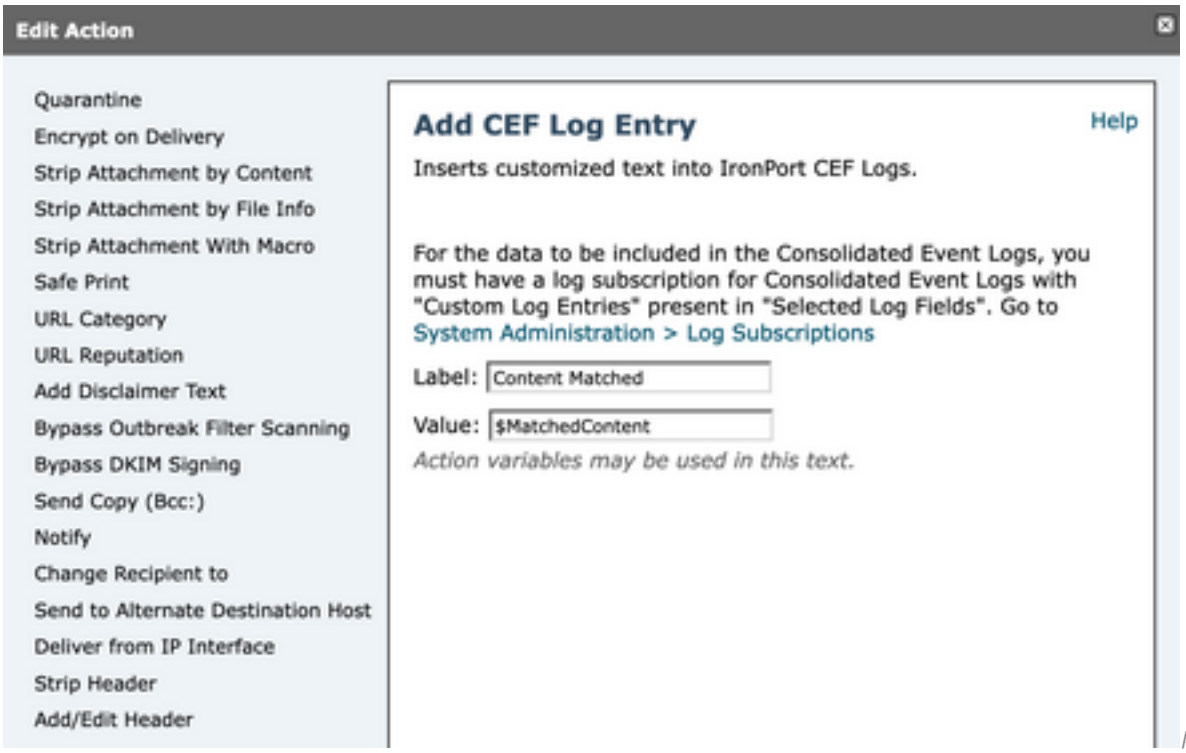
CEF日志条目

添加传入/传出内容过滤器

首先，在ESA上创建内容过滤器：

1. 转到 **Mail Policies > Incoming/Outgoing content filters**
2. 点击 **Add Filter**
3. 为过滤器命名
4. 需要添加条件
5. 点击 **Add Action**
6. 选择 **Add CEF Log Entry**
7. 命名标签并使用 **Action Variables** 对于值框
8. **Submit and Commit**

我们使用的文档示例 **$MatchedContent** 操作变量，如图所示：



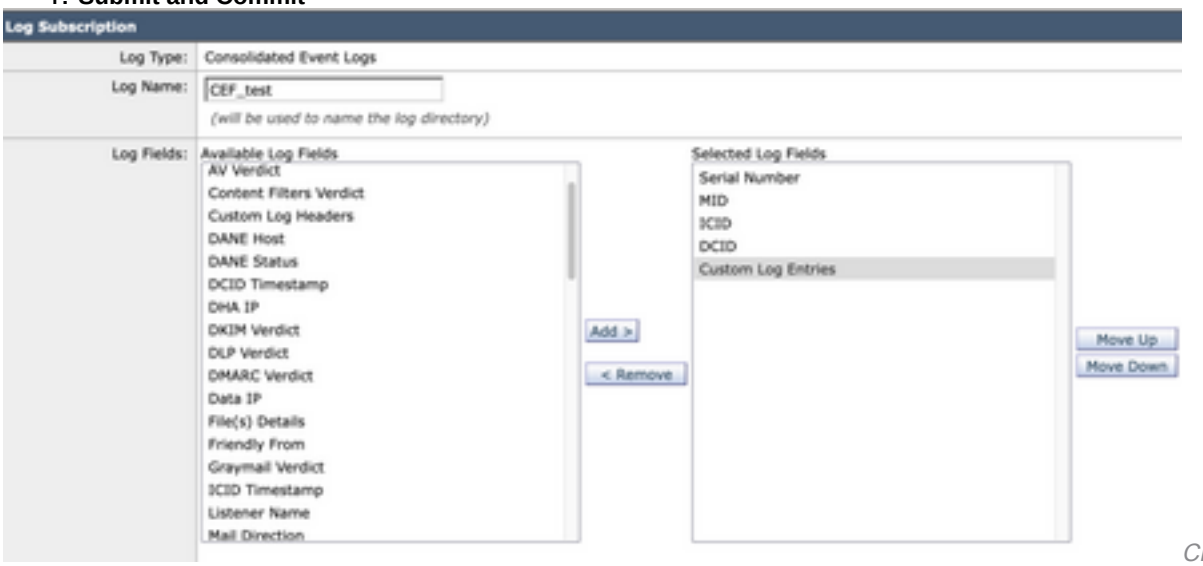
内容过滤器中的CEF日志条目操作

在整合事件日志订用中添加CEF日志条目

接下来，创建或修改统一事件日志订阅，以添加之前创建的CEF日志条目：

1. 转到 **System Administration > Log Subscriptions**
2. 添加或选择整合的事件日志
3. 选择 **Custom Log Entries** 并点击 **Add**

4. **Submit and Commit**



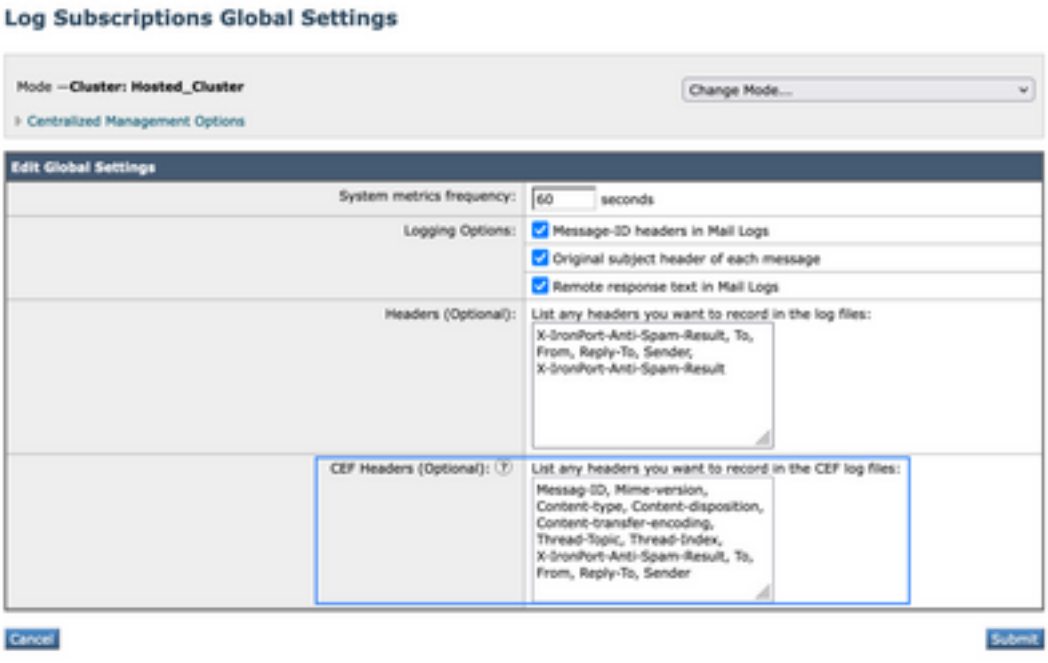
CEF日志订阅中的自定义日志条目

CEF报头

将CEF报头添加到日志中：

首先在ESA中添加CEF报头

1. 转到 **System Administration > Logs Subscription**
2. 点击 **Edit Settings** 在Global Settings下
3. 在CEF信头下，列出要记录的信头
4. **Submit and Commit**



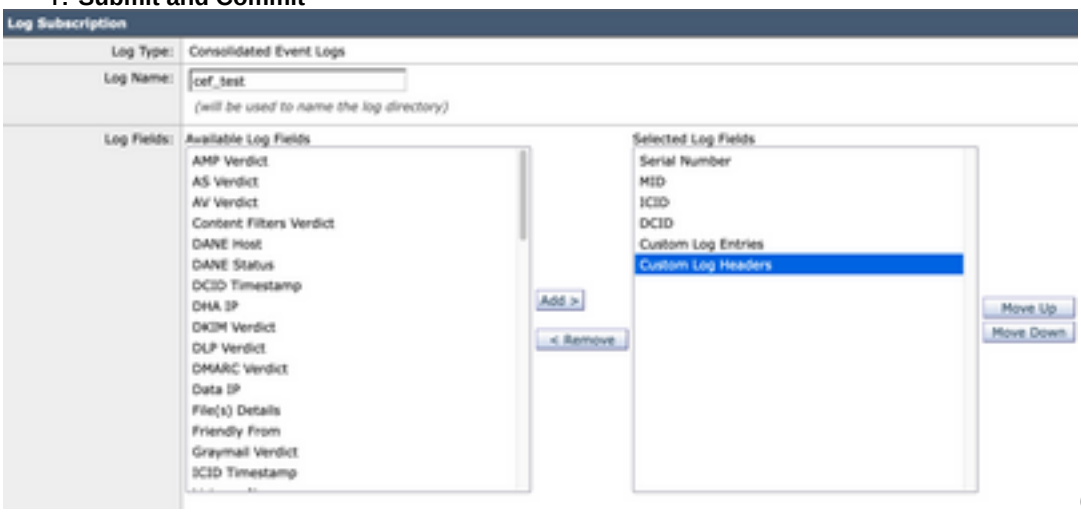
CEF报头配置

在整合事件日志订用中添加CEF日志条目

接下来，创建或修改统一事件日志订阅，以添加之前记录的CEF标头：

1. 转到 **System Administration > Logs Subscription**
2. 添加或选择整合的事件日志

3. 选择 **Custom Log Entries** 并点击 **Add**
4. **Submit and Commit**



CEF日志订阅中的CEF日志信头

相关信息

- 最终用户指南ESA 14.3
- 发行说明ESA 14.3
- 技术支持 - 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）。