Cisco Secure Firewall eStreamer 集成指南

版本 7.2
June 13, 2023

思科系统公司
www.cisco.com
思科在全球设有 200 多个办事处。
有关地址、电话号码和传真号码信息，
可查阅思科网站:
www.cisco.com/go/offices。

本手册中有关产品的规格和信息如有更改，恕不另行通知。本手册中的所有声明、信息和建议均准确可靠，但我们不为其提供任何明示或暗示的担保。用户必须承担使用产品的全部责任。

随附产品的软件许可和有限担保在随产品一起提供的信息包中提供，且构成本文的一部分。如果您无法找到软件许可或有限担保，请与思科代表联系以获取副本。

思科所采用的 TCP 信头压缩是加州大学伯克莱分校 (UCB) 开发的一个程序的改版，是 UCB 的 UNIX 操作系统公共域版本的一部分。保留所有权利。© 1981，加州大学董事会。

无论本手册中是否有任何其他担保，这些供应商的所有文档文件和软件均按“原样”提供，可能包含缺陷。思科和上述供应商不承诺所有明示或暗示的担保，包括（但不限于）对特定用途的适销性、适用性、非侵权性以及因交易、使用或商业惯例所产生的保证。

在任何情况下，对于任何间接、特殊、连带发生或偶发的损坏，包括（但不限于）因使用或无法使用本手册而导致的任何利润损失或数据损失或损坏?料及其供应商概不负责，即使思科及其供应商已获知此类损坏的可能性也不例外。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或注册商标。要查看思科商标列表，请转至此 URL：www.cisco.com/go/trademarks。文中提及的第三方商标为其相应所有者的财产。“合作伙伴”一词的使用并不意味着思科和任何其他公司之间存在合作伙伴关系。(1721R)

本文档中使用的任何互联网协议 (IP) 地址和电话号码并不代表实际地址和电话号码。本文档中所含的任何示例、命令显示输出、网络拓扑图和其他图形仅供说明之用。说明性内容中用到的任何真实 IP 地址或电话号码纯属巧合，并非有意使用。

目 录

CISCO SECURE FIREWALL 系统

简介

思科 Event Streamer（也称为 eStreamer）能让您通过流传输将 Cisco Secure Firewall 系统事件发送到外部客户端应用。您可以从管理中心通过流传输发送主机、发现、关联、合规性白名单、入侵、用户活动、文件、恶意软件和连接数据。

请注意，NGIPSv、Firepower 服务、Firepower Threat Defense Virtual 和 Firepower 威胁防御不支持 eStreamer。要从这些设备通过流传输发送事件，可以在这些设备向其报告的管理中心上配置 eStreamer。

eStreamer 使用自定义应用层协议与连接的客户端应用通信。因为 eStreamer 的目的只是返回客户端请求的数据，所以本指南主要介绍请求的数据的 eStreamer 格式。

创建 eStreamer 客户端并将其与 Cisco Secure Firewall 系统集成需要执行三个主要步骤：

1. 编写一个使用 eStreamer 应用协议与管理中心或受管设备交换消息的客户端应用。eStreamer SDK 包含一个标准客户端应用。
2. 配置一个管理中心或设备以将所需类型的事件发送到您的客户端应用。
3. 将您的客户端应用连接到管理中心或设备，并开始交换数据。

本指南为您提供需要的信息，帮助您成功创建和运行 eStreamer 版本 7.2 客户端应用。

eStreamer 版本 7.2的重大变更

添加了对接收完全限定事件的支持。请参阅 请求完全限定事件，第 2-4 页

已将基于 Python 的新参考客户端添加到 SDK。请参阅 运行 eStreamer Python 标准客户端，第 6-12 页

使用本指南

总体来看，eStreamer 服务是通过流传输将数据从 Cisco Secure Firewall 系统发送到发出请求的客户端的一种机制。该服务可以通过流传输发送以下类别的数据：

- 入侵事件数据和事件额外数据
- 关联（合规性）事件数据
- 发现事件数据
- 用户事件数据
- 事件的元数据

- 主机信息
- 恶意软件事件数据

本文主要介绍 eStreamer 返回的数据结构。本文的章节如下：

- 了解 eStreamer 应用协议，第 2-1 页，此章对 eStreamer 通信进行了概述，详细说明了编写 eStreamer 客户端应用的一些要求，并且介绍了用于向 eStreamer 服务发送命令和接收来自该服务的数据的四种类型的消息。
- 了解入侵和关联数据结构，第 3-1 页，此章介绍了用于返回由入侵检测和关联组件生成的事件数据的数据格式，以及用于描述入侵和关联事件的数据格式。
- 了解发现和连接数据结构，第 4-1 页，此章介绍了用于返回发现事件、用户事件和连接事件数据的数据格式。
- 了解主机数据结构，第 5-1 页，此章介绍了 eStreamer 在收到主机信息请求消息时用于返回完整主机信息数据的数据格式。
- 配置eStreamer，第 6-1 页，此章介绍了如何在管理中心或受管设备上配置 eStreamer。此章还介绍了 eStreamer 命令行开关，并且提供了手动启动和停止 eStreamer 服务以及配置管理中心或受管设备以自动启动 eStreamer 的说明。
- 数据结构示例，第 A-1 页，此章提供了二进制格式的 eStreamer 消息数据包示例。
- 了解旧版数据结构，第 B-1 页，此章介绍了当前产品不再使用、但是旧客户端可能使用的旧数据结构的结构。

必备条件

要了解此指南中的信息，您应大体上熟悉 Cisco Secure Firewall 系统的功能和术语以及其组件的功能，尤其应熟悉这些组件生成的不同类型的事件数据。对于不熟悉的术语或产品特定的术语，其定义通常可以从《*Cisco Secure Firewall eStreamer 集成指南*》获取。

Cisco Secure Firewall 系统发行版的产品版本

本指南通篇使用版本号来描述管理中心和受管设备生成的事件的数据格式。***Cisco Secure Firewall 系统产品版本***表按主要发行版列出了每个产品的版本。

表 1-1 Cisco Secure Firewall 系统产品版本

版本	管理中心版本	受管设备版本
3D 系统 5.0	管理中心 5.0	5.0
3D 系统 5.1	管理中心 5.1	5.1
3D 系统 5.1.1	管理中心 5.1.1	5.1.1
3D 系统 5.2	管理中心 5.2	5.2
3D 系统 5.3	管理中心 5.3	5.3
Cisco Secure Firewall 系统 5.3.1	管理中心 5.3.1	5.3.1
Cisco Secure Firewall 系统 5.4	管理中心 5.4	5.4
Cisco Secure Firewall 系统 6.0	管理中心 6.0	6.0
Cisco Secure Firewall 系统 6.1	管理中心 6.1	6.1

表 1-1　Cisco Secure Firewall 系统产品版本 （续）

版本	管理中心版本	受管设备版本
Cisco Secure Firewall 系统 6.2	管理中心 6.2	6.2
Cisco Secure Firewall 系统 6.2.1	管理中心 6.2.1	6.2.1
Cisco Secure Firewall 系统 6.2.2	管理中心 6.2.2	6.2.2
Cisco Secure Firewall 系统 6.2.2	管理中心 6.2.3	6.2.3
Cisco Secure Firewall 系统 6.3.0	管理中心 6.3.0	6.3.0
Cisco Secure Firewall 系统 6.4.0	管理中心 6.4.0	6.4.0
Cisco Secure Firewall 系统 6.5.0	管理中心 6.5.0	6.5.0
Cisco Secure Firewall 系统 6.6.0	管理中心 6.6.0	6.6.0
Cisco Secure Firewall 系统 6.7.0	管理中心 6.7.0	6.7.0
Cisco Secure Firewall 系统 7.0	管理中心 7.0	7.0
Cisco Secure Firewall 系统 7.1.0	管理中心 7.1.0	7.1.0

文档约定

eStreamer 消息数据类型约定表列出了本文中用于介绍 eStreamer 消息中采用的各种数据字段格式的名称。eStreamer 服务使用的数字常数通常为无符号整数值。除非另有说明，位字段使用低顺序位。例如，在包含五位标志数据的单字节字段中，低顺序五位将包含数据。

表 1-2　eStreamer 消息数据类型约定

数据类型	说明 (Description)
nn-位字段	nn 位的位字段
字节	包含任意格式数据的 8 位字节
int8	带符号 8 位字节
uint8	无符号 8 位字节
int16	带符号 16 位整数
uint16	无符号 16 位整数
int32	带符号 32 位整数
uint32	无符号 32 位整数
uint64	无符号 64 位整数
字符串	包含字符数据的变长字段
[n]	跟在以上任何数据类型后面的数组下标，表示该数据类型的 n 个实例，例如 uint8[4]
变量	各种数据类型的集合
BLOB	未指定类型的二进制对象，通常为从数据包捕获的原始数据

IP 地址

思科数据库以二进制格式将 IPv4 和 IPv6 地址存储在同一字段中。要获取 IPv6 地址，请转换为十六进制表示法，例如：`20010db80000000000000000000004321`。此数据库存储IPv4地址时遵循RFC，用 1 填充位 80-95，生成无效的 IPv6 地址。例如 IPv4 地址 10.5.15.1 会存储为 `00000000000000000000FFFF0A050F01`。

最佳实践

使用 eStreamer 时，思科给出了以下建议以最佳利用 API。

设计

- 考虑使用以 Python 编写的 Cisco 可插拔 eStreamer 客户端作为客户端基础，这样您只需构建一个插件即可设置 SIEM 方案的数据格式。
- 构建您的 eStreamer 客户端，以支持 API 可以提供的所有内容，因为方案的每一部分都至少对一小部分客户群很重要。
  - 了解消息结构 - 逐渐了解 eStreamer 集成指南。
  - 花时间获取在元数据和代码结构中定义的记录 - 其中很大一部分能够解析消息。
  - 从一般意义上了解元数据的工作方式，例如，元数据记录被提前发送。
  - 了解对象模型 - 记录如何相互关联以及哪些元数据与哪些记录相关。
- 实施强大的错误处理和日志记录，以便在出现问题时，您可以查看消息和导致问题的情况，而不必重现错误。
- 仔细挑选您的语言。解析似乎不需要进行大量计算，但当每秒钟有数千个事件时，一切都非常重要。诸如 C、C++、Go 等编译语言将比 Python/JavaScript 更快。 这种方法的缺点是缺乏可移植性。
- 如果您实施多线程处理 或常规处理，请明白处理元数据的任何方法都必须按顺序处理消息 - 这必须包括无序传送更正。
- 查看现有的 eStreamer 实施，了解其他人过去如何实现您的目标。访问以下某些资源：
  - https://splunkbase.splunk.com，并搜索 eStreamer
  - https://software.cisco.com/download/home/，在“选择产品”旁边，选择“浏览全部”，再选择“安全性”，然后依次选择“防火墙”、“防火墙管理”、“Firepower 管理中心虚拟设备”、“Firepower 系统工具和 API”。
  - https:/community.cisco.com，并搜索 “eNcoreCLI”。
- 确保与思科安全技术联盟团队合作，及时了解对 eStreamer 所做的更改以及与思科 Firepower 集成的其他方面。您可以通过 ask-csta-pm@cisco.com 与他们联系。

测试

- 当思科推出新版本的 Firepower 时，请立即针对它测试您的客户端，以确保您的客户端收集的数据不会更改。
- 拥有良好的测试平台，以便您可以轻松、频繁地进行测试。
- 如果您不希望构建自己的测试平台，请使用 dcloud 沙盒测试平台。思科安全技术联盟将提供资源来帮助设置和使用此平台。Dcloud 是免费的，并且支持全面测试。但是，它不一定是供您使用的完整平台，并且没有 100% 覆盖事件。此外，实例仅供短期使用。有关 dcloud 的详细信息，请访问 https://dcloud2-rtp.cisco.com

了解 eStreamer 应用协议

Cisco Secure Firewall 系统 Event Streamer (eStreamer) 使用面向消息的协议来将事件和主机配置文件信息通过流传输发送到您的客户端应用。您的客户端可以从管理中心请求事件数据和主机配置文件数据，从受管设备只能请求入侵事件数据。您的客户端应用可以通过提交请求消息（指定要发送的数据）启动数据流，然后在流传输开始后控制来自管理中心或受管设备的消息流。

在本文中，管理中心或受管设备上的 eStreamer 服务可能会称为 eStreamer 服务器或 eStreamer。

以下部分描述连接到 eStreamer 服务的要求，并介绍 eStreamer 协议中使用的命令和数据格式：

- 连接规格，第 2-1 页介绍了 eStreamer 服务与您的客户端之间的通信流，并且介绍了客户端是如何与其进行交互的。
- 了解 eStreamer 通信阶段，第 2-1 页介绍了用于客户端应用向 eStreamer 服务器提交数据请求以及 eStreamer 向客户端传送所请求的信息的通信协议。
- 了解 eStreamer 消息类型，第 2-8 页介绍了 eStreamer 协议中使用的消息类型；讨论了 eStreamer 用于向客户端返回入侵事件数据、发现事件数据、元数据和主机数据的数据包的基本结构；并提供了其他信息来帮助您编写能够解释 eStreamer 消息的客户端。

连接规格

eStreamer 服务：

- 使用 TCP 通过 SSL 连接进行通信（客户端应用必须支持基于 SSL 的身份验证）。
- 接受端口 8302 上的连接请求。
- 等待客户端启动所有通信会话。
- 按网络字节顺序（大端字节）编写所有消息字段。
- 以 UTF-8 格式进行文本编码。

了解 eStreamer 通信阶段

客户端与 eStreamer 服务之间的通信有四个主要阶段：

1. 客户端与 eStreamer 服务器建立连接，并且双方对连接进行身份验证。

   有关详细信息，请参阅建立经过身份验证的连接，第 2-2 页。

2. 客户端向 eStreamer 服务请求数据，并指定要流传输的数据类型。单个事件请求消息可以指定可用事件数据的任意组合，包括事件元数据。单个主机配置文件请求可以指定单个主机或多个主机。

   请求事件数据可采用两种请求模式：

   – 事件流请求 - 客户端提交包含请求标志（指定请求的事件类型和每个类型的版本）的消息，eStreamer 服务器则通过流传输所请求的数据作出响应。

   – 扩展请求 - 客户端提交请求（其消息格式与事件流请求相同），但是设置了扩展请求的标志。这将启动客户端与 eStreamer 服务器之间的消息交互，客户端可向此服务器请求通过事件流请求无法获得的额外信息和版本组合。

   有关请求数据的信息，请参阅向 eStreamer 请求数据，第 2-3 页。

3. eStreamer 与客户端建立请求的数据流。

   有关详细信息，请参阅接受来自 eStreamer 的数据，第 2-7 页。

4. 连接终止。
   有关详细信息， 请参阅终止连接，第 2-7 页。

建立经过身份验证的连接

客户端必须先与 eStreamer 服务建立支持 SSL 的 TCP 连接，才能向 eStreamer 请求数据。客户端可以在管理中心或受管设备上已配置的任何管理接口上发出请求。客户端连接对管理接口不实施流量信道配置，所以在选择您的连接接口时，可以忽略该配置。当客户端发起连接时，eStreamer 服务器响应，发起与客户端的 SSL 握手。作为SSL 握手的一部分，eStreamer 服务器请求客户端身份验证证书，并确认证书是有效的（由 eStreamer 服务器上的内部认证机构 [内部 CA] 签署）。

注释 思科建议您还要求您的客户端确认 eStreamer 服务器提供的证书已由受信任的认证机构签署。这是您向管理中心或受管设备注册新的 eStreamer 客户端时，思科提供的 PKCS#12 文件中包含的内部 CA 证书。有关详细信息，请参阅为 eStreamer 客户端添加身份验证，第 6-3 页。

在建立 SSL 会话后，eStreamer 服务器会另外对证书进行一次连接后验证。验证内容包括确认客户端连接是从证书中指定的主机发起的，并且证书的持有者名称包含适当的值。如果任一项连接后检查失败，则 eStreamer 服务器将关闭连接。必要时，您可以配置 eStreamer 服务，使其不执行客户端主机名称检查（有关更多信息，请参阅 eStreamer 服务选项，第 6-4 页）。

虽然不要求客户端执行连接后验证，但是，思科仍然建议客户端执行此验证步骤。身份验证证书的持有者名称包含以下字段值：

表 2-1　　证书持有者名称字段

字段	值
`title`	eStreamer
`generationQualifier`	`server`

完成连接后验证之后，eStreamer 服务器会等待客户端发出数据请求。

向 eStreamer 请求数据

您的客户端在管理数据请求时会执行以下高级任务：

- 初始化请求会话 - 请参阅建立会话，第 2-3 页。
- 从 eStreamer 事件存档请求事件 - 使用事件流请求和扩展请求启动事件流传输，第 2-3 页。
- 请求主机数据 - 请参阅请求主机数据，第 2-6 页。
- 更改请求 - 请参阅更改请求，第 2-6 页。
- 请求完全限定事件 - 请参阅 请求完全限定事件，第 2-4 页

建立会话

客户端通过向 eStreamer 服务发送初始事件流请求建立会话。

在此初始消息中，您可以添加数据请求标志，也可以在后续消息中提交数据请求。此初始事件流请求消息本身是所有 eStreamer 请求的前提条件，不管是请求事件数据还是主机数据，都是如此。有关使用事件流请求消息的信息，请参阅事件流请求消息格式，第 2-11 页。

注释　eStreamer 客户端可以在管理中心或受管设备上已配置的任何管理接口上发出请求。客户端连接对管理接口不实施流量信道配置，所以在选择您的连接接口时，可以忽略该配置。

使用事件流请求和扩展请求启动事件流传输

eStreamer 服务提供两种事件流传输的请求模式。您的请求可以组合不同模式。在两种模式中，您的客户端均利用一条事件流请求消息发起请求，但是对请求标志位进行的设置不同。有关事件流消息格式的详细信息，请参阅事件流请求消息格式，第 2-11 页。

当 eStreamer 收到一个事件流请求消息时，它对该客户端请求的处理如下：

- 如果该请求消息**未**设置请求标志字段中的位 30，则 eStreamer 开始流传输该请求标志字段中其他已设置的位请求的任何事件。有关信息，请参阅提交事件流请求，第 2-3 页。
- 如果事件流请求中的位 30 **已**设置，则 eStreamer 提供扩展的请求处理。如果此位已设置，则必须发送扩展请求标志。有关信息，请参阅提交扩展请求，第 2-4 页。请注意，eStreamer 会解决所有重复请求。如果您请求相同数据的多个版本，不管是通过多个标志还是多个扩展请求，系统都会采用最高版本。例如，如果 eStreamer 收到对发现事件版本 1 和 6 的标志请求，以及对版本 3 的扩展请求，则发送版本 6。

提交事件流请求

事件流请求的流程很简单：

- 您的客户端向 eStreamer 服务发送一条请求消息。该消息带有起始日期和时间，以及一个指定要在数据流中包含的事件及其版本级别的请求标志字段。
- eStreamer 通过流传输发送开始于指定时间的事件。有关流传输协议的信息，请参阅接受来自 eStreamer 的数据，第 2-7 页。

有关客户端的事件流请求消息格式和内容的信息，请参阅事件流请求消息格式，第 2-11 页。

有关客户端可以请求的事件的事件类型和版本的信息，请参阅表 2-6，第 2-13 页。

提交扩展请求

如果您在事件流请求消息的请求标志字段中设置了位 30，则您发起一个扩展请求，该请求启动与服务器之间的协商。如果此位已设置，则必须发送扩展请求标志。有关扩展请求可用的事件类型，请参阅表 2-22，第 2-34 页。

扩展请求的步骤如下：

- 您的客户端向 eStreamer 发送一条事件流请求消息，其中的请求标志位 30 设置为 1，表示这是扩展请求。有关消息格式详细信息，请参阅事件流请求消息格式，第 2-11 页。
- eStreamer 回复一条流传输信息消息，通告客户端可用的服务列表。有关流传输信息消息的详细信息，请参阅流传输信息消息格式，第 2-29 页。
- 客户端返回一条流传输请求消息。该消息指明其希望使用的服务，并且包含该服务中可用的事件类型和版本的请求列表。该请求列表对应于进行标准事件流请求时请求标志字段中的设置位。有关如何使用流传输请求消息来请求事件的详细信息，请参阅“扩展请求消息示例”节，第 2-36 页。
- eStreamer 处理客户端的流传输请求消息，并在消息中指定的时间开始流传输数据。有关流传输协议的信息，请参阅接受来自 eStreamer 的数据，第 2-7 页。

请求完全限定事件

我们建议您的客户端使用此选项来请求文本格式（例如 JSON 或 CSV）的完全限定事件，而不是以复杂的二进制格式接收事件。使用此选项时，本文档中介绍二进制格式的大部分内容都无关紧要。在 SDK 包中，python_client 子目录提供使用此选项的示例代码。

此选项当前仅支持请求几种事件类型的信息：连接事件、入侵事件、入侵数据包和文件事件。如果需要以二进制格式接收其他事件类型，则必须为完全限定和二进制事件格式使用单独的客户端连接。

要请求完全限定事件，请使用记录的“事件流请求消息”，并在消息末尾附加 JSON 格式的配置块。该请求将包括如下所示的五个二进制整数，后跟 JSON 格式的配置详细信息，例如：

```
<报头版本 (1)>
<消息类型 (2)>
<消息长度>
<初始时间戳>
<请求标志>
<JSON 格式配置块>
```

二进制消息长度字段必须包括二进制报头的长度以及 JSON 块的长度。在 JSON 块之后可以选择空字符终止，但如果包含空字符，则消息长度必须将空字符考虑在内。对于 Request Flags 字段，仅支持第 23 位（扩展事件报头）；所有其他位应为零，特别是位 30（扩展请求）必须为零。

在客户端发送请求消息后，如果已在服务器端 UI eStreamer 配置页面上启用了请求的事件类型，则 eStreamer 服务将立即开始发送事件数据。

JSON 文件的格式

此示例也可以在 eStreamer SDK 的 `json_request.json` 文件中找到。

```
{
"Events":
{
"ConnectionEvent":
{
"FieldSetDef":
{
"OutputFieldSet": ["HeaderFieldSet", "ConnectionKeySet", "DetailFieldSet"]
},
"Fields": ["OutputFieldSet"]
},
"IntrusionEvent":
{
"FieldSetDef":
{
"OutputFieldSet": ["HeaderFieldSet", "ConnectionKeySet", "DetailFieldSet", "Impact"]
},
"Fields": ["OutputFieldSet"]
},
"IntrusionPacket":
{
"FieldSetDef":
{
"OutputFieldSet": ["HeaderFieldSet", "DetailFieldSet"]
},
"Fields": ["OutputFieldSet"]
},
"FileEvent":
{
"FieldSetDef":
{
"OutputFieldSet": ["HeaderFieldSet", "ConnectionKeySet", "DetailFieldSet"]
},
"Fields": ["OutputFieldSet"]
}
},
"OutputFormat":
{
"Transform": "Text",
"TransformConfig": "JSON"
}
}
```

在`事件 (Events)` 部分中，为您希望客户端接收的每种事件类型指定一个块（仅支持三种示例类型：`ConnectionEvent`、`IntrusionEvent`、`IntrusionPacket` 和 `FileEvent`）。每个事件的 `FieldSetDef` 部分必须指定一个 `OutputFieldSet`，其中列出将包含在该事件类型的事件中的字段或字段集。示例文件仅指定字段集，但您可以使用字段名称和字段集的任意组合。

每种事件类型的可用字段列表以及预定义字段集可在 Firepower 管理中心的文件 `/etc/sf/EventHandler/EventCatalog/EventCatalog.json` 中找到。在文件末尾的字段部分中，查找所需的事件类型（例如 `IntrusionEvent`），然后查看 `Fields` 和 `FieldSetDef` 块，以查看可用于该事件类型的内容。

OutputFormat 部分包含输出设置。转换 (Transform) 字段始终为文本 (Text)，您可以使用 TransformConfig 字段指定输出转换格式。该示例显示 JSON，但您也可以指定 CSV。其他文本格式以及 FlatBuffer 均可用，但您需要请求这些格式的文档。

在 TransformConfig 中指定 JSON 输出时，输出将包含每个请求的字段的名称-值对，与事件无关的任何字段都将被跳过（例如，如果您请求了 SSL 字段，并且事件未使用 SSL，则输出将不包含这些字段）。

在 TransformConfig 中指定 CSV 输出时，输出将包含按配置中列出的顺序排列的所需字段。如果某个字段与事件无关，则 CSV 只会包含该字段的逗号。在请求 CSV 时，不要使用预定义的字段集，因为版本之间的字段集可能会发生变化，从而导致 CSV 不兼容。

完全限定事件消息

事件消息包含在捆绑包中，如 eStreamer 文档中“消息捆绑包格式”消息类型 4002 中所述。

如文档所述，客户端必须通过向 eStreamer 服务器发送一条空消息来确认每个接收到的数据包，从而表明已准备好接受更多数据。

对于所有受支持的事件类型，事件数据消息以二进制报头开头，如“关联记录报头”等 eStreamer 文档中所述。唯一的区别在于数据块格式是请求的格式（JSON、CSV 等）。基本结构的快速参考如下：

```
<报头版本 (1)>
<消息类型 (3)>
<消息长度>
<记录类型（可应要求包括可选的 Netmap ID）>
<记录长度>
<时间戳（在指定请求位 23 时）>
<保留（在指定请求位 23 时）>
<数据>
```

请求主机数据

建立会话后，您可以随时提交主机数据请求。eStreamer 从 Cisco Secure Firewall 系统网络映射生成有关所请求主机的信息。

更改请求

要更改已建立会话的请求参数，客户端必须断开连接，并请求建立新会话。

接受来自 eStreamer 的数据

注释 eStreamer 服务器不保留其发送的事件的历史记录。您的客户端应用必须检查是否存在重复事件。重复事件可能由于各种原因而意外出现。例如，启动新的流传输会话时，客户端指定为新会话起点的时间可能有多条消息，其中一些消息可能已经在前一个会话中发送，有些则没有。eStreamer 会发送所有符合指定请求条件的消息。您的应用应能够检测出产生的任何重复。

在非活动时段，eStreamer 会定期向客户端发送空消息，使连接保持开启状态。如果它从客户端或中间主机收到错误消息，则会关闭连接。

根据请求模式，eStreamer 以不同方式将请求的数据传输给客户端。

事件流请求

如果客户端提交事件流请求，eStreamer 会逐条消息返回数据。它可以接连发送多条消息，无需等待客户端确认。在某个点，它会暂停并等待客户端。客户端操作系统会缓存收到的数据，让客户端按照自己的节奏处理这些数据。

如果客户端请求中包含元数据请求，则 eStreamer 会先发送元数据。客户端应该将元数据存储在内存中，以便在处理后续事件记录时使用。

扩展请求

如果客户端提交扩展请求，eStreamer 会将消息排队，并捆绑发送。eStreamer 可以接连发送多个捆绑包，无需等待客户端确认。在某个点，它会暂停并等待客户端。客户端操作系统会缓存收到的数据，让客户端按照自己的节奏读取这些数据。

客户端会逐条消息地解开每个捆绑包，然后根据记录和块的长度解析每条消息。可以根据每个消息报头中的总消息长度计算出到达每条消息末尾的时间，根据总捆绑包长度确定到达捆绑包末尾的时间。捆绑包的正确解析并不需要其内容的索引。

有关消息捆绑机制的信息，请参阅消息捆绑包格式，第 2-37 页。

有关客户端能够用于额外流控制的空消息的信息，请参阅空消息格式，第 2-9 页。

终止连接

在关闭连接之前，eStreamer 服务器会尝试发送一条错误消息。有关错误消息的信息，请参阅错误消息格式，第 2-10 页。

eStreamer 服务器可出于以下原因关闭客户端连接：

- 在任何时候发送消息产生错误时。这包括事件数据消息以及 eStreamer 在非活动期间发送的空的保持连接消息。
- 处理客户端请求时出错。
- 客户端身份验证失败（不发送错误消息）。
- eStreamer 服务将要关闭（不发送错误消息）。

您的客户端可随时关闭与 eStreamer 服务器的连接，且应尝试使用错误消息格式告知 eStreamer 服务器原因。

了解 eStreamer 消息类型

eStreamer 应用协议采用的消息格式很简单：包含标准消息报头和各种子报头字段，后接包含消息负载的记录数据。所有 eStreamer 消息类型都采用相同的消息报头；有关更多信息，请参阅eStreamer 消息报头，第 2-9 页。

表 2-2　　eStreamer 消息类型

消息类型	名称	说明
0	“空消息” (Null message)	eStreamer 服务器和客户端都通过发送空消息来控制数据流。有关信息，请参阅空消息格式，第 2-9 页。
1	“错误消息” (Error message)	eStreamer 服务器和客户端使用错误消息来说明关闭连接的原因。有关信息，请参阅错误消息格式，第 2-10 页。
2	“事件流请求” (Event Stream Request)	客户端向 eStreamer 服务发送此消息类型以启动新的流传输会话和请求数据。有关信息，请参阅事件流请求消息格式，第 2-11 页。
4	“事件数据” (Event Data)	eStreamer 服务使用此消息类型向客户端发送事件数据和元数据。有关信息，请参阅事件数据消息格式，第 2-16 页。
5	“主机数据请求” (Host Data Request)	客户端向 eStreamer 服务发送此消息类型来请求主机数据。必须已经通过事件流请求消息开始会话。有关信息，请参阅主机请求消息格式，第 2-24 页。
6	“单主机数据” (Single Host Data)	eStreamer 服务使用此消息类型发送客户端请求的单主机数据。有关信息，请参阅主机数据和多主机数据消息格式，第 2-28 页。
7	“多主机数据” (Multiple Host Data)	eStreamer 服务使用此消息类型发送客户端请求的多主机数据。有关信息，请参阅主机数据和多主机数据消息格式，第 2-28 页。
2049	“流传输请求” (Streaming Request)	客户端在扩展请求中使用此消息类型来指定其需要流信息消息中的哪些通告事件。有关信息，请参阅扩展请求消息示例，第 2-36 页。
2051	“流传输信息” (Streaming Information)	eStreamer 在扩展请求中使用此消息类型来向客户端通告可用服务列表。有关信息，请参阅流传输信息消息格式，第 2-29 页。
4002	“消息捆绑包” (Message Bundle)	eStreamer 服务使用此消息类型对要通过流传输发送给客户端的消息进行打包。有关信息，请参阅消息捆绑包格式，第 2-37 页。

eStreamer 消息报头

所有 eStreamer 消息都以下图所示的消息报头开始。下表对这些字段进行了说明。

表 2-3　　标准eStreamer消息报头字段

字段	数据类型	说明 (Description)
报头版本 (Header Version)	uint16	表示消息使用的报头的版本。对于当前版本的 eStreamer，此值始终为。
消息类型 (Message Type)	uint16	表示传输的消息的类型。有关当前值的列表，请参阅表 2-2，第 2-8 页。
消息长度 (Message Length)	uint32	表示后续内容的长度，不包括消息报头本身的字节。带有报头但是没有数据的消息的消息长度为零。

空消息格式

客户端应用和 eStreamer 服务都会发送空信息。空消息的类型为 0，在消息报头之后不含数据。

客户端向 eStreamer 服务器发送空消息，表明自己已准备好接受更多数据。不传输数据时，eStreamer 服务向客户端发送空消息，使连接保持活动状态。空消息的消息长度值始终设置为 0。

提示　在本文的数据结构图中，括号内的整数（例如 (1) 或 (115)）表示恒定字段值。例如，报头版本 (1) 表示这里讨论的数据结构中的字段值始终为 1。

空消息格式如下所示。空消息中唯一的非零值为报头版本。

空消息的二进制格式示例如下。请注意，唯一的非零值位于第二个字节，表示报头版本值为 1。消息类型和长度字段（加阴影部分）的值都是 0。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

提示 本指南中的示例以二进制格式显示，以清楚地展示设置了哪些位。这对于某些消息非常重要，例如事件请求消息和事件影响字段。

错误消息格式

客户端应用和 eStreamer 服务都会使用错误信息。错误消息的消息类型为 1，并且包含报头、错误代码、错误文本长度和实际错误文本。错误文本可包含 0 至 65535 个字节。

为客户端应用创建自定义错误消息时，思科建议使用 -1 作为错误代码。

下图说明基本的错误消息格式。加阴影的字段是错误消息所特有的。

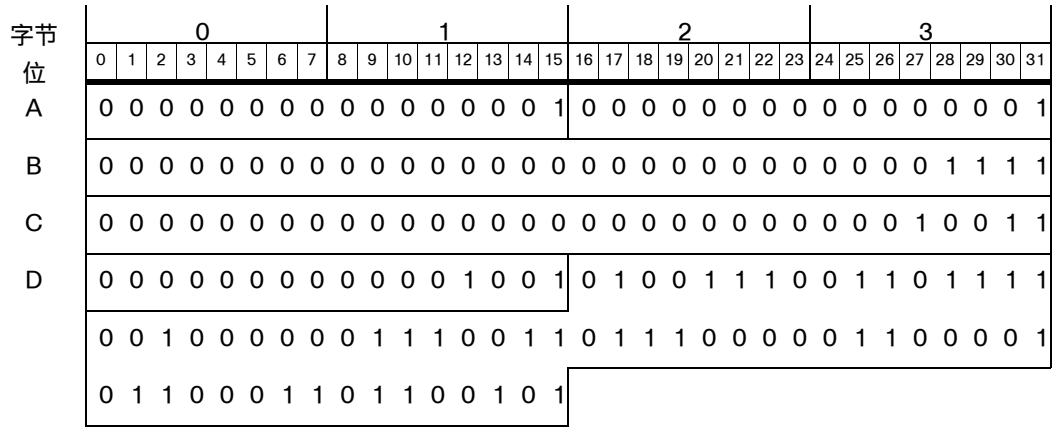
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (1) (Message Type (1))															
	消息长度 (Message Length)																															
	错误代码 (Error Code)																															
	错误文本长度 (Error Text Length)																错误文本... (Error Text...)															

下表介绍错误代码消息中的每个字段。

表 2-4　　错误消息字段

字段	数据类型	说明 (Description)
错误代码	int32	表示错误的号码。
错误文本长度 (Error Text Length)	uint16	错误文本字段中包含的字节数。
错误文本 (Error Text)	变量	错误消息。最多 65535 字节。

下图显示了一个错误消息示例：



在上一个实例中，出现以下信息：

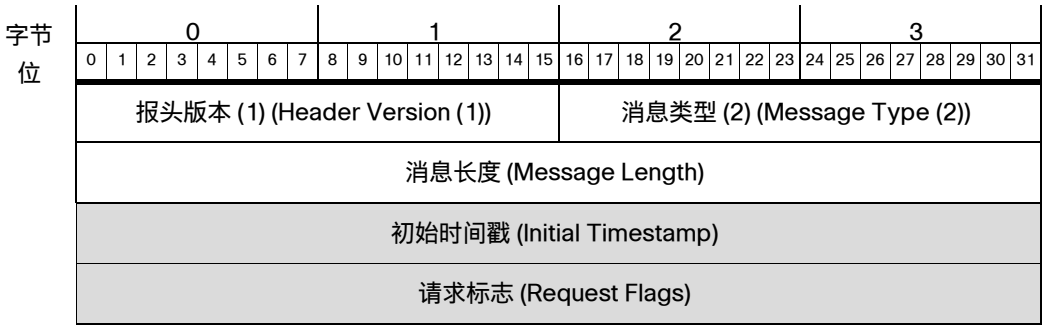
字母	说明
A	前两个字节表示标准报头值 1。接下来的两个字节显示值 1，说明传输的是错误消息。
B	此行表示后面的消息数据量。在本例中，后面是 15个字节（二进制为 1111）的数据。
C	此行显示错误代码。在本例中，该消息包含的值为 19 (10011)。因此，在消息中传输的是错误代码 19。
D	此行包含错误消息中的字节数（1001，或 9 个字节），错误消息本身在接下来的 9 个字节中。错误消息值，转换为 ASCII 文本时，等于“无空间”，这是错误代码为 19 的错误消息。

事件流请求消息格式

eStreamer 客户端使用事件流请求消息开始流传输会话。该请求消息包括开始时间和位标志字段，以此指定 eStreamer 服务应该包含的数据，这些数据可以是事件的任意组合，以及入侵事件额外数据和元数据。事件流请求消息可以发起事件流请求和扩展请求。消息类型为 2。

您必须为所有数据请求（包括专用于主机配置文件信息的请求）提交事件流请求消息。在这种情况下，您首先要提交事件流请求消息，然后提交主机请求消息（类型 5）来指定主机数据。

下图说明事件流请求消息格式。该消息使用标准报头。加阴影的字段是请求消息所特有的，后面的表格对此进行了介绍。



下表介绍事件流请求消息中的每个字段。

表 2-5　事件流请求消息字段

字段	数据类型	说明 (Description)
初始时间戳 (Initial Timestamp)	uint32	定义会话的开始。若要： ▪ 在客户端连接到 eStreamer 时开始，请将所有时间戳位设置为 1。 ▪ 从最早的可用数据开始，请将所有时间戳位设置为 0。 ▪ 在给定日期和时间开始，请指定 UNIX 时间戳（自 1970 年 1 月 1 日起经过的秒数）。 有关重要信息，请参阅下文的初始时间戳，第 2-12 页。
请求标志 (Request Flags)	bits[32]	指定要在事件流请求中返回的事件和元数据的类型和版本。有关标志定义，请参阅请求标志，第 2-12 页。 设置位 30 会发起一个扩展请求，该请求可以与事件流请求共存于同一个消息中。

初始时间戳

注释 提交事件流请求时，您的客户端应用应使用“初始时间戳”(Initial Timestamp) 字段中的存档时间戳，如下所述。这可以确保您不会意外地排除事件。设备使用具有传输延迟的“存储和转发”机制将数据传输到管理中心。如果您根据检测到事件的设备分配的生成时间戳来请求事件，则可能会漏掉延迟的事件。

开始会话时，最佳做法是从上一个会话的最后记录的存档时间戳（也称为“服务器时间戳”）开始。这并不是技术要求，但强烈建议这样做。 通过使用上次会话中最后一条记录的存档时间戳，eStreamer 服务不会重新发送之前的记录或元数据。在某些情况下，如果您使用生成时间戳，则您可能意外地将事件排除在新的流传输会话之外。

要将存档时间戳添加到您的流传输事件中，您必须在请求标志字段中设置位 23。

请注意，只有基于时间的事件才带有存档时间戳。如果在请求扩展事件报头时设置了位 23，则 eStreamer 生成的事件（例如元数据）的这个字段值为 0。

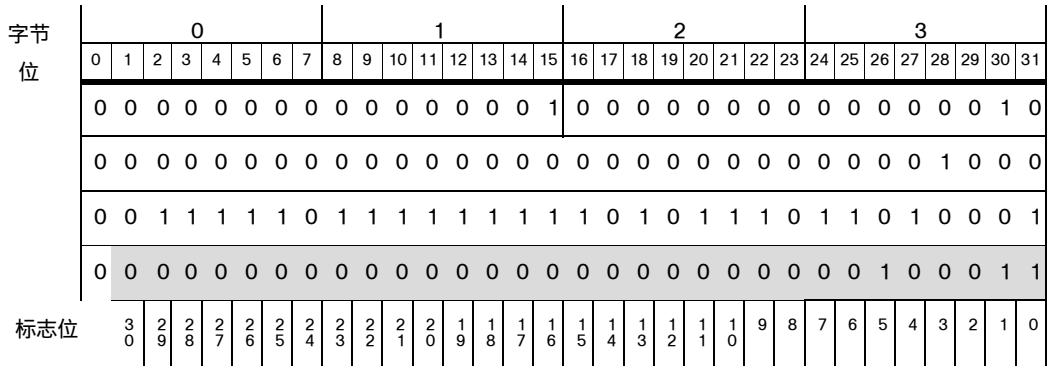
请求标志

在事件数据请求标志字段中设置位 0 至 29，以选择您希望 eStreamer 发送的事件的类型。设置位 30 可激活扩展请求模式。设置位 30 并不会直接请求任何数据。如果此位已设置，则必须发送扩展请求标志。您的客户端会在提交事件流请求消息后进行的服务器与客户端消息对话中请求数据。有关扩展请求的信息，请参阅向 eStreamer 请求数据，第 2-3 页。

有关请求标志字段中的位设置的定义，请参阅表 2-6，第 2-13 页。不同的标志请求不同版本的事件数据。例如，要获取 Cisco Secure Firewall 系统 4.9 格式而不是 4.10 格式的数据，您需要设置不同的标志位。有关在请求特定产品版本的数据时需使用的标志的具体信息，请参阅表 2-7，第 2-15 页。

请注意，您根据版本请求元数据，而不是根据具体元数据记录。有关每个受支持的元数据版本的信息，请参阅请求标志，第 2-12 页。

下图加阴影部分显示当前使用的标志字段中的位:



有关每个请求标志位的信息，请参阅下表。

表 2-6　　请求标志

位字段	说明 (Description)
位 0	请求传输与入侵事件相关的数据包数据。如果设置为 1，数据包数据随入侵事件传输。如果设置为 0，数据包数据不传输。
位 1	请求传输与入侵事件、发现事件、关联事件和连接事件相关的版本 1 元数据。如果设置为 1，版本 1 元数据随事件传输。如果设置为 0，版本 1 元数据不传输。 可以使用元数据解析事件中的编码字段和数字字段。有关 向客户端传输元数据的方式 （续）客户端如何利用元数据的一般信息，请参阅了解元数据，第 2-38 页。
位 2	请求传输入侵事件。如果位 2 和位 6 其中之一或两者都设置为 1，但是扩展请求标志（位 30）设置为 0，则系统将其解释为来自版本 4.x 客户端的请求，并发送记录类型 104/105。如果位 2 和位 6 其中之一或两者都设置为 1 时没有指定事件类型，而位 30 设置为 1，则系统将其解释为来自版本 5.0-5.1 客户端的请求，并发送记录类型 207/208。如果位 30 设置为 1，并且请求了特定的事件类型，则不管位 2 和 6 如何设置，都会发送入侵事件。 有关请求记录类型的详细信息，请参阅提交扩展请求，第 2-4 页。 如果位 2、位 6 和位 30 都设置为 0，则不发送入侵事件。 位 6 的使用方式与位 2 相同。可以将任意一个位设置为请求入侵事件。将这两个位中的一个设置为 0 不会覆盖另一个位；将位 2 设置为 0、位 6 设置为 1，或者将位 2 设置为 1、位 6 设置为 0，都会被解释为请求入侵事件。
位 3	请求传输发现数据版本 1（管理中心 3.2）。如果设置为 0，则不传输发现数据版本 1。 有关发现事件的详细信息，请参阅了解发现和连接数据结构，第 4-1 页。
位 4	请求传输关联数据版本 1（管理中心 3.2）。如果设置为 0，则不传输关联数据版本 1。
位 5	请求传输影响关联事件（入侵影响警报）。如果设置为 1，则传输入侵影响警报。如果设置为 0，则不传输入侵影响警报。 有关入侵影响警报的详细信息，请参阅入侵影响警报数据 5.3+，第 3-19 页。
位 6	位 6 的使用方式与位 2 相同。请参阅位 2，第 2-13 页。
位 7	如果设置为 1，则请求传输发现数据版本 2（管理中心 4.0 - 4.1）。如果设置为 0，则不传输发现数据版本 2。
位 8	如果设置为 1，则请求传输连接数据版本 1（管理中心 4.0 - 4.1）。如果设置为 0，则不发送连接数据版本 1。
位 9	如果设置为 1，则请求传输关联数据版本 2（管理中心 4.0 - 4.1.x）。如果设置为 0，则不传输关联策略数据版本 2。
位 10	如果设置为 1，则请求传输发现数据版本 3（管理中心 4.5 - 4.6.1）。如果设置为 0，则不传输发现数据版本 3。 有关旧版发现事件的详细信息，请参阅旧版发现数据结构，第 B-121 页。
位 11	禁用事件传输。
位 12	如果设置为 1，则请求传输连接数据版本 3（管理中心 4.5 - 4.6.1）。如果设置为 0，则不发送连接数据版本 3。
位 13	请求传输关联数据版本 3（管理中心 4.5 - 4.6.1）。如果设置为 0，则不传输关联数据版本 3。

表 2-6　　请求标志 （续）

位字段	说明 (Description)
位 14	请求传输与入侵事件、发现事件、关联事件和连接事件相关的版本 2 元数据。如果设置为 1，版本 2 元数据随事件传输。如果设置为 0，版本 2 元数据不传输。 有关 向客户端传输元数据的方式管理中心客户端如何利用元数据的一般信息，请参阅了解元数据，第 2-38 页。
位 15	请求传输与入侵事件、关联事件、发现事件和连接事件相关的版本 3 元数据。如果设置为 1，版本 3 元数据随事件传输。如果设置为 0，版本 3 元数据不传输。 有关 向客户端传输元数据的方式客户端如何利用元数据的一般信息，请参阅了解元数据，第 2-38 页。
位 16	未使用
位 17	请求传输发现数据版本 4（管理中心 4.7-4.8.x）。如果设置为 0，则不传输发现数据版本 4。
位 18	如果设置为 1，则请求传输连接数据版本 4（管理中心 4.7 - 4.9.0.x）。如果设置为 0，则不发送连接数据版本 4。 有关详细信息，请参阅连接区块消息，第 4-52 页。
位 19	请求传输关联数据版本 4（管理中心 4.7）。如果设置为 0，则不传输关联数据版本 4。 有关以管理中心 4.7 格式传输的关联事件的信息，请参阅旧版关联事件数据结构，第 B-347 页。
位 20	请求传输与入侵事件、发现事件、用户活动事件、关联事件和连接事件相关的版本 4 元数据。如果设置为 1，版本 4 元数据随事件传输。如果设置为 0，版本 4 元数据不传输。 版本 4 元数据包括: ▪ 关联（合规性）规则信息 ▪ 关联（合规性）策略信息 ▪ 指纹记录 ▪ 客户端应用记录 ▪ 客户端应用类型记录 ▪ 漏洞记录 ▪ 主机重要性记录 ▪ 网络协议记录 ▪ 主机属性记录 ▪ 扫描类型记录 ▪ 用户记录 ▪ 服务检测设备（版本 2）记录 ▪ 事件分类（版本 2）记录 ▪ 优先级记录 ▪ 规则信息（版本 2） ▪ 恶意软件信息 如果同时请求位 20 和位 22，则也会发送用户元数据。 有关 向客户端传输元数据的方式客户端如何利用元数据的一般信息，请参阅了解元数据，第 2-38 页。
位 21	请求传输版本 1 用户事件。有关用户事件的详细信息，请参阅用户记录，第 4-19 页。
位 22	请求传输关联数据版本 5（管理中心 4.8.0.2 - 4.9.1）。如果设置为 0，则不传输关联数据版本 5。 如果同时请求位 20 和位 22，则也会发送用户元数据。 有关旧版关联（合规性）事件的详细信息，请参阅旧版关联事件数据结构，第 B-347 页。
位 23	请求扩展事件报头。如果设置为 1，则随事件一起传输事件被存档（以便 eStreamer 服务器处理）时的时间戳，并且保留四个字节供未来使用。如果此字段设置为 0，则随事件一起发送仅包含记录类型和记录长度的标准事件报头。 有关事件消息报头的信息，请参阅eStreamer 消息报头，第 2-9 页。
位 24	请求传输发现数据版本 5（管理中心 4.9.0.x）。如果设置为 0，则不传输发现数据版本 5。 有关发现事件的详细信息，请参阅了解发现和连接数据结构，第 4-1 页。
位 25	请求传输发现数据版本 6（管理中心 4.9.1+）。如果设置为 0，则不传输发现数据版本 6。 有关发现事件的详细信息，请参阅了解发现和连接数据结构，第 4-1 页。

表 2-6　　请求标志 （续）

位字段	说明 (Description)
位 26	如果设置为 1，则请求传输连接数据版本 5（管理中心 4.9.1 - 4.10.x）。如果设置为 0，则不发送连接数据版本 5。 有关详细信息，请参阅连接区块消息，第 4-52 页。
位 27	请求额外数据记录中与入侵事件相关联的事件额外数据。 有关事件数据的详细信息，请参阅表 B-11入侵事件额外数据数据块字段，第 B-67 页。
位 28	请求传输发现数据版本 7（管理中心 4.10.0+）。如果设置为 0，则不传输发现数据版本 7。 有关发现事件的详细信息，请参阅了解发现和连接数据结构，第 4-1 页。
位 29	请求传输关联数据版本 6（管理中心 4.10 - 4.10.x）。如果设置为 0，则不传输关联策略数据版本 6。 如果同时请求位 20 和位 29，则也会发送用户元数据。 有关关联事件的详细信息，请参阅该产品的早期版本。
位 30	表示向 eStreamer 发出的一个扩展请求。如果此位已设置，则必须发送扩展请求标志。有关扩展请求的信息，请参阅提交扩展请求，第 2-4 页。

为了帮助您决定使用哪些标志来请求特定版本的数据，请参阅下表。对于版本 5.0 及更高版本，请参阅提交扩展请求，第 2-4 页了解有关使用位 30 的更多信息。

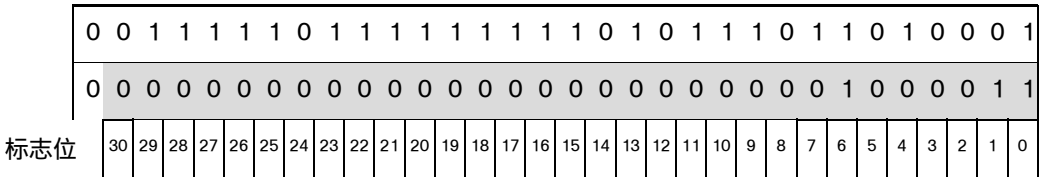
表 2-7　　按产品版本划分的事件请求标志

请求的数据的类型	4.9.0.x	4.9.1.x	4.10.x	5.0+	5.1	5.1.1+
数据包数据	位 0	位 0	位 0	位 0	位 0	位 0
入侵事件	位 2	位 2	位 2	位 2	位 2	位 30
元数据	位 20	位 20	位 20	位 20	位 20	位 20
发现事件	位 24	位 25	位 28	位 30	位 30	位 30
关联事件	位 22	位 22	位 29	位 30	位 30	位 30
事件额外数据	-	-	位 27	位 27	位 27	位 27
影响事件警报	位 5	位 5	位 5	位 5	位 5	位 5
连接数据	位 18	位 26	位 26	位 30	位 30	位 30
用户事件	位 21	位 21	位 21	位 30	位 30	位 30
恶意软件事件	-	-	-	-	-	位 30
文件事件	-	-	-	-	-	位 30

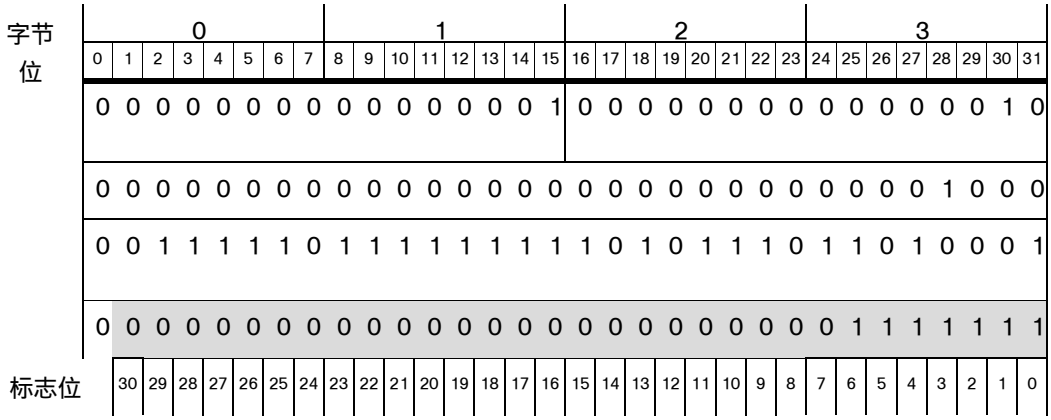
小心　在所有事件类型中，在版本 5.x 之前，标准客户端都将 `detection engine ID` 字段标记为 `sensor ID`。

以下示例请求类型为 7 的入侵事件（与 Cisco Secure Firewall 系统 3.2+ 兼容）以及版本 1 元数据和数据包标志：

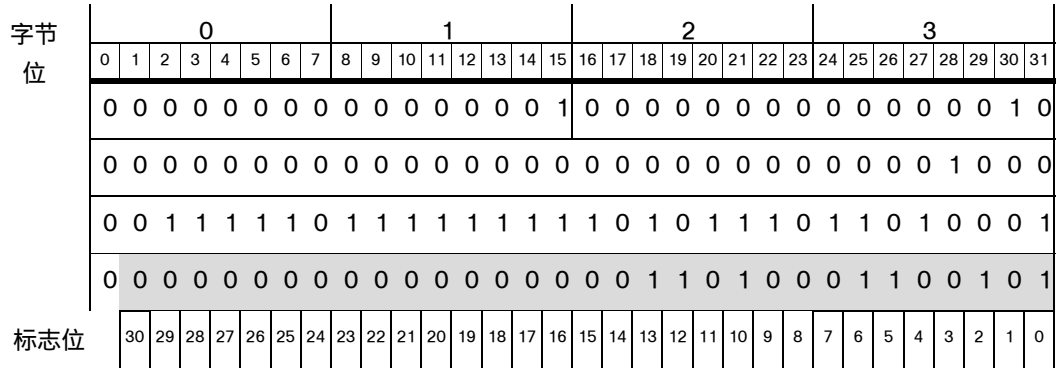
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0



要仅请求与 Cisco Secure Firewall 系统 3.2 兼容的数据（包括入侵事件、数据包、元数据、影响警报、策略违规事件和版本 2.0 事件），则使用：



要请求类型为 7 的入侵影响警报、关联事件、发现事件、连接事件和入侵事件，以及数据包和管理中心 4.6.1+ 格式的版本 3 元数据，则使用：



事件数据消息格式

在收到事件请求时，eStreamer 服务会将事件数据及相关元数据传输到客户端。事件数据消息的消息类型为 3。每条消息都包含单个带有事件数据或元数据的数据记录。

请注意，类型 3 消息只传送事件数据和元数据。eStreamer 以类型 6（单主机）和类型 7（多主机）消息传输主机信息。有关主机消息格式的信息，请参阅主机数据和多主机数据消息格式，第 2-28 页。

了解事件数据消息的组织

eStreamer 发送的事件数据和元数据消息包含以下部分：

- eStreamer 消息报头 - eStreamer 消息报头，第 2-9 页上定义的标准消息报头。
- 特定于事件的子报头 - 因事件类型而异的字段组，带有描述额外事件详细信息并确定后续负载数据结构的代码。
- 数据记录 - 多个固定长度的字段和一个数据块。

注释　客户端应根据字段长度对所有消息进行解包。

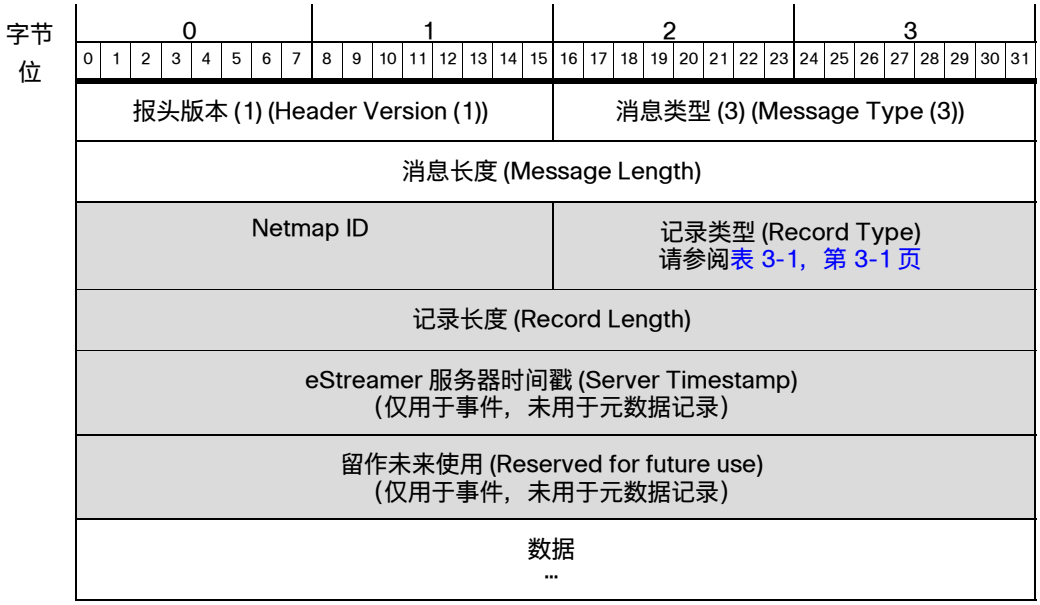
有关根据事件类型划分的事件消息格式，请参阅：

- 入侵事件和元数据消息格式，第 2-17 页，了解入侵事件数据记录和所有元数据记录。这些消息含有固定长度字段。
- 发现事件消息格式，第 2-19 页，了解含有发现事件或用户事件数据的消息。除了有标准 eStreamer 消息报头和与入侵事件消息相似的记录报头外，发现消息还有一个与众不同的含有事件类型和子类型字段的发现事件报头。发现事件消息中的数据记录打包在系列 1 数据块中。该数据块可包含可变长度字段和多层封装数据块。
- 连接事件消息格式，第 2-20 页，了解带有连接统计信息的消息。连接事件消息的一般结构与发现事件消息相同。但是它们的数据块类型是特定于连接统计信息的。
- 关联事件消息格式，第 2-20 页，了解带有关联（合规性）事件数据的消息。此类消息中的报头与入侵事件消息中的报头相同，但数据块是系列1 数据块。
- 事件额外数据消息格式，第 2-22 页，了解传输带有可变长度字段和多层嵌套数据块（例如入侵事件额外数据）的入侵相关记录类型的一系列消息。有关此消息系列的结构的一般信息，请参阅事件额外数据消息格式，第 2-22 页。有关此系列数据块结构（类似于系列 1 数据块，但是单独编号）的信息，请参阅数据块报头，第 2-23 页。

入侵事件和元数据消息格式

下图显示了入侵事件和元数据消息的一般结构。

下图显示了入侵事件和元数据消息格式的记录报头部分的详细信息。加阴影部分为记录报头字段。后面的表格定义这些字段。



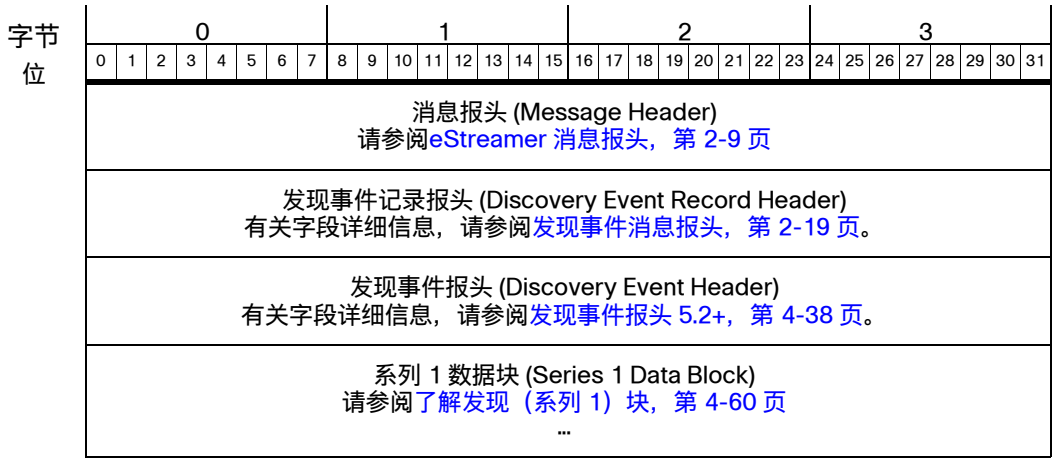
下表介绍入侵事件和元数据消息报头中的每个字段。

表 2-8　　入侵事件和元数据记录报头字段

字段	数据类型	说明 (Description)
Netmap ID	uint16	此字段的第一位是一个标志，表示该报头是否为含有存档时间戳的扩展报头。其余 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。如果不使用此字段，则字段显示为空。Netmap ID 根据元数据中的规定映射到域。
记录类型 (Record Type)	uint16	确定数据记录内容类型。有关记录类型的列表，请参阅表 3-1入侵事件与一般元数据记录类型，第 3-1 页。
记录长度 (Record Length)	uint32	记录报头后面的消息内容长度。不包括记录报头的 8 或 16 个字节。（记录长度加上记录报头的长度等于消息长度。）
eStreamer 服务器时间戳 (eStreamer Server Timestamp)	uint32	表示事件被 eStreamer 服务器存档时的时间戳。也称为存档时间戳。 只有设置了请求消息标志中的位 23，才存在此字段。
留作未来使用 (Reserved for future use)	uint32	已保留供将来使用。 只有设置了请求消息标志中的位 23，才存在此字段。

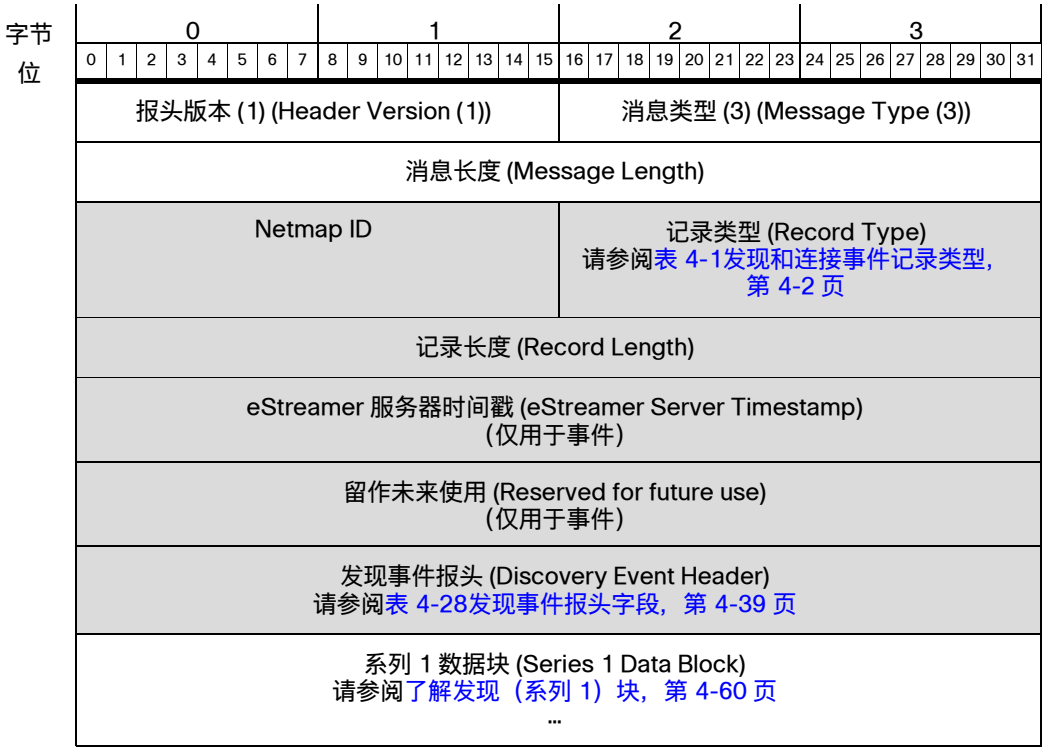
发现事件消息格式

下图显示了发现事件消息的结构。标准 eStreamer 消息报头和事件记录报头后面是仅在发现和用户事件消息中使用的发现事件报头。消息的发现事件报头部分包含发现事件类型和子类型字段。这些字段在一起构成后面的数据块的密钥。有关当前发现事件类型和子类型的信息，请参阅表 4-29按类型和子类型划分的发现与连接事件，第 4-40 页。



发现事件消息报头

下图中的加阴影部分显示了发现事件数据消息格式中的记录报头的字段，并且显示了后面的事件报头的位置。下表定义发现事件消息报头中的字段。



下表介绍发现事件消息的记录报头和事件报头中的字段。

表 2-9　　发现事件消息报头字段

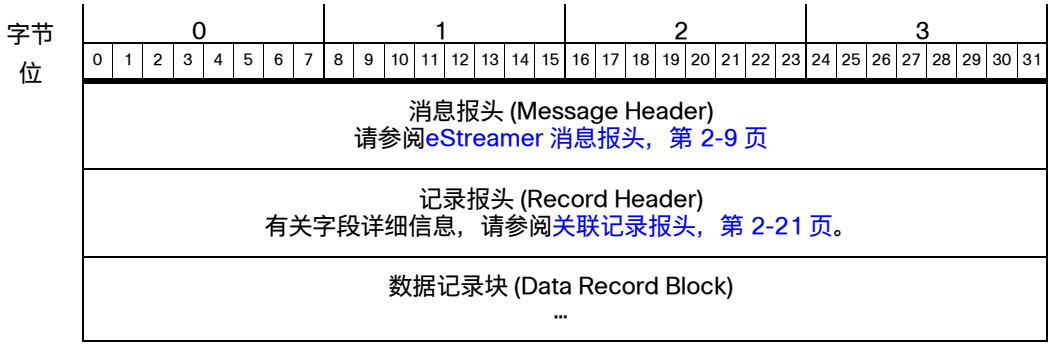
字段	数据类型	说明 (Description)
Netmap ID	uint16	此字段的第一位是一个标志，表示该报头是否为含有存档时间戳的扩展报头。其余 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。如果不使用此字段，则字段显示为空。Netmap ID 根据元数据中的规定映射到域。
记录类型 (Record Type)	uint16	确定数据记录内容类型。有关记录类型的列表，请参阅表 4-1发现和连接事件记录类型，第 4-2 页。
记录长度 (Record Length)	uint32	记录报头后面的消息内容长度。不包括记录报头的 8 或 16 个字节。（记录长度加上记录报头的长度等于消息长度。）
eStreamer 服务器时间戳 (eStreamer Server Timestamp)	uint32	表示事件被 eStreamer 服务器存档时的时间戳。也称为存档时间戳。只有在事件流请求的请求标志字段中设置了位 23，才存在此字段。
留作未来使用 (Reserved for future use)	uint32	已保留供将来使用。只有设置了请求消息标志中的位 23，才存在此字段。
发现事件报头 (Discovery Event Header)	视情况而定	包含大量字段，其中包括事件类型和子类型字段，这些字段在一起构成后面的数据结构的密钥。有关发现事件报头中的字段的定义，请参阅发现事件报头 5.2+，第 4-38 页。

连接事件消息格式

带有连接统计信息的消息的结构与发现事件消息相同。有关一般消息格式信息，请参阅发现事件消息格式，第 2-19 页。连接事件消息具有不同的数据块类型。

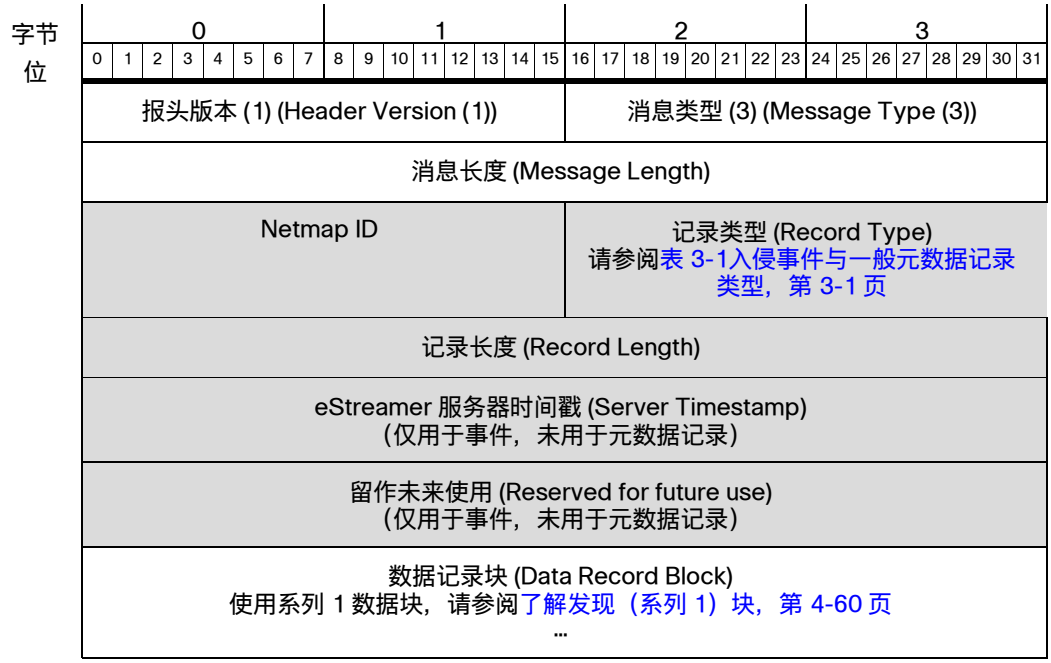
关联事件消息格式

下图显示了关联（合规性）事件消息的一般结构。标准 eStreamer 消息报头和记录报头后面紧跟着消息的数据记录部分中的数据块。关联消息使用系列 1 数据块。



关联记录报头

下图中的加阴影部分显示了关联事件消息中记录报头的字段。请注意，关联消息使用系列 1 数据块；但是它们没有发现事件消息中存在的发现报头。它们的报头字段与入侵事件消息的相似。下图后面的表格定义关联事件的记录报头字段。



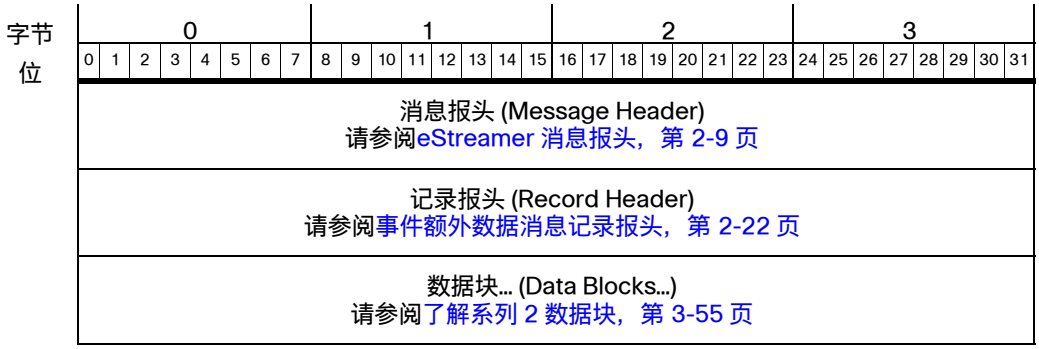
下表介绍关联事件消息的记录报头中的每个字段。

表 2-10　　关联事件消息记录报头字段

字段	数据类型	说明 (Description)
Netmap ID	uint16	此字段的第一位是一个标志，表示该报头是否为含有存档时间戳的扩展报头。其余 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。如果不使用此字段，则字段显示为空。Netmap ID 根据元数据中的规定映射到域。
记录类型 (Record Type)	uint16	确定数据记录内容类型。有关入侵、关联和元数据记录类型的列表，请参阅表 3-1，第 3-1 页。
记录长度 (Record Length)	uint32	记录报头后面的消息内容长度。不包括记录报头的 8 或 16 个字节。（记录长度加上记录报头的长度等于消息长度。）
eStreamer 服务器时间戳 (eStreamer Server Timestamp)	uint32	表示事件被 eStreamer 服务器存档时的时间戳。也称为存档时间戳。 只有设置了请求消息标志中的位 23，才存在此字段。 对于管理中心生成的数据（例如主机配置文件和元数据），此字段为零。
留作未来使用 (Reserved for future use)	uint32	已保留供将来使用。 只有设置了请求消息标志中的位 23，才存在此字段。

事件额外数据消息格式

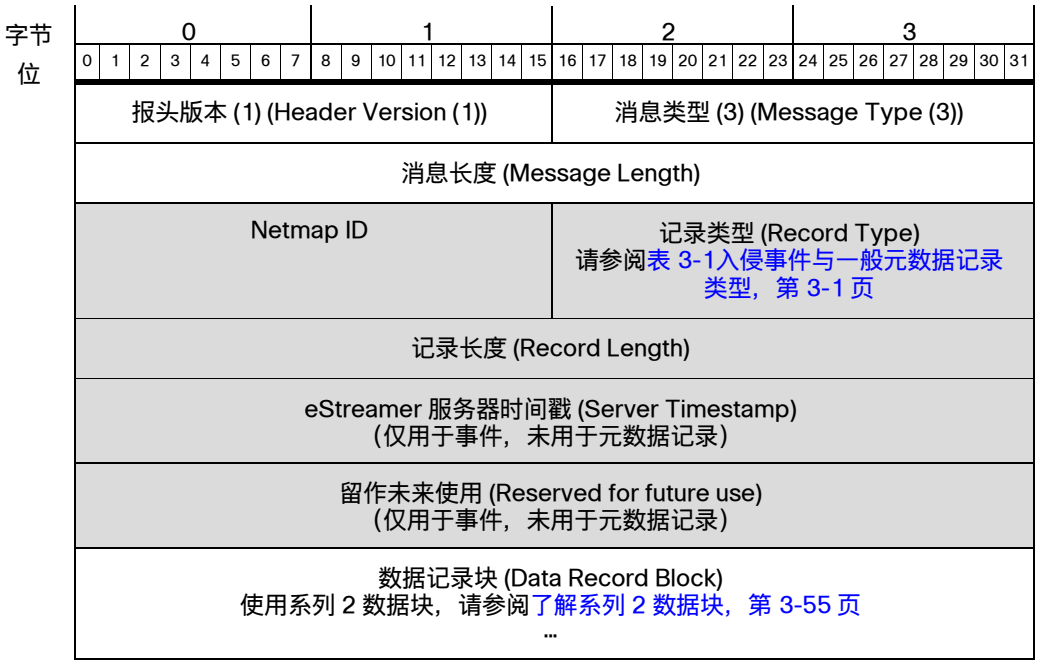
下图显示了事件额外数据消息的结构。此消息组的一个示例是入侵事件额外数据消息。



事件额外数据消息的格式与关联事件消息相同，在记录报头后面直接跟着数据块。和关联消息不同的是，它们使用具有单独编号顺序的系列 2 数据块而不是系列 1 数据块。有关系列 2 数据块类型的信息，请参阅了解系列 2 数据块，第 3-55 页。

事件额外数据消息记录报头

下图中的加阴影部分显示了事件额外数据消息中的记录报头的字段。后面的表格定义事件额外数据消息的记录报头字段。



下表介绍事件额外数据消息的记录报头中的每个字段。

表 2-11　事件额外数据消息记录报头字段

字段	数据类型	说明 (Description)
Netmap ID	uint16	此字段的第一位是一个标志，表示该报头是否为含有存档时间戳的扩展报头。其余 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。如果不使用此字段，则字段显示为空。Netmap ID 根据元数据中的规定映射到域。
记录类型 (Record Type)	uint16	确定数据记录内容类型。有关事件额外数据记录类型的列表，请参阅表 3-1入侵事件与一般元数据记录类型，第 3-1 页。
记录长度 (Record Length)	uint32	记录报头后面的消息内容长度。不包括记录报头的 8 或 16 个字节。（记录长度加上记录报头的长度等于消息长度。）
eStreamer 服务器时间戳 (eStreamer Server Timestamp)	uint32	表示事件被 eStreamer 服务器存档时的时间戳。也称为存档时间戳。 只有设置了请求消息标志中的位 23，才存在此字段。对于管理中心生成的事件，不存在此字段。
留作未来使用 (Reserved for future use)	uint32	已保留供将来使用。 只有设置了请求消息标志中的位 23，才存在此字段。对于管理中心生成的事件，不存在此字段。

数据块报头

系列 1 数据块和系列 2 数据块具有类似结构，但编号不同。这些数据块可以出现在发现、关联、连接或事件额外数据消息的数据部分中的任何位置。这些数据块在多个嵌套层级上封装其他数据块。

第一和第二系列的数据块都以下图中显示的报头结构开始。后面的表格提供有关报头字段的信息。报头后面紧跟着与数据块类型相关的数据结构。

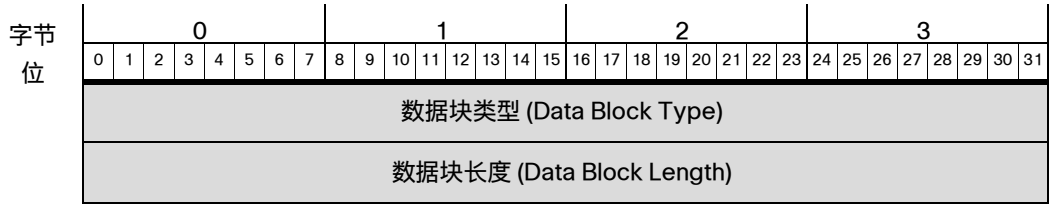


表 2-12

字段	数据类型	说明 (Description)
数据块类型 (Data Block Type)	uint32	对于系列 1 数据块类型，请参阅了解发现（系列 1）块，第 4-60 页。 对于系列 2 数据块类型，请参阅表 3-24系列 2 块类型，第 3-55 页。
数据块长度 (Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的

主机请求消息格式

要接收主机配置文件，您需提交主机请求消息。可以请求单个主机或 IP 地址范围定义的多个主机的数据。

请注意，对于所有数据请求（包括主机配置文件信息请求），都必须先通过提交事件流请求消息来初始化会话。要设置仅流传输主机数据，您可以在您的初始事件流请求消息中使用以下任意一个请求标志设置：

- 设置表示适当版本的元数据的位（这可能有助于流传输主机数据）
- 设置无请求标志
- 设置位 11（在使用旧版 eStreamer 时禁用任何默认事件流传输）

在初始消息后，使用主机请求消息（类型 5）以指定主机。

注释 对于带有默认事件流传输的旧版 eStreamer，如果想仅传输主机配置文件数据，则需要禁用默认事件消息。首先向服务器发送事件流请求消息（请求标志字段中的位 11 设置为 1）；然后，发送主机请求消息。

下图显示了主机请求消息的格式。加阴影的字段是主机请求消息格式特有的，后面的表格给出了这些字段的定义。前面的三个字段是标准消息报头。

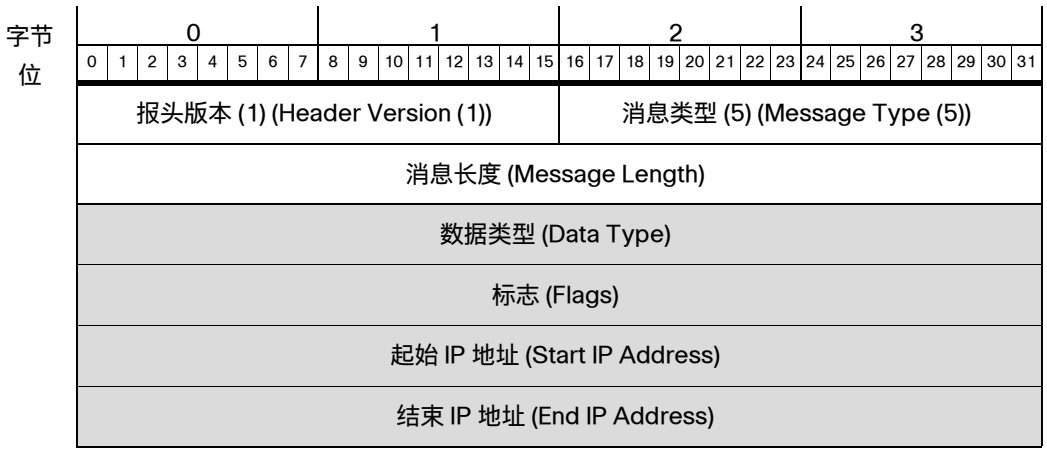
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (5) (Message Type (5))															
消息长度 (Message Length)																																
数据类型 (Data Type)																																
标志 (Flags)																																
起始 IP 地址 (Start IP Address)																																
起始 IP 地址 (Start IP Address)（续）																																
起始 IP 地址 (Start IP Address)（续）																																
起始 IP 地址 (Start IP Address)（续）																																
结束 IP 地址 (End IP Address)																																
结束 IP 地址 (End IP Address)（续）																																
结束 IP 地址 (End IP Address)（续）																																
结束 IP 地址 (End IP Address)（续）																																

下表对消息字段进行了说明。

表 2-13　主机请求消息字段

字段	数据类型	说明 (Description)
数据类型 (Data Type)	uint32	使用下列代码请求单个主机或多个主机的数据: ▪ 0 — 版本 3.5-4.6 数据，单主机。 ▪ 1 — 版本 3.5-4.6 数据，多主机（使用数据块 34）。 ▪ 2 — 版本 4.7-4.8 数据，单主机（使用数据块 47）。 ▪ 3 — 版本 4.7-4.8 数据，多主机（使用数据块 47）。 ▪ 4 — 版本 4.9 - 4.10 数据，单主机（使用数据块 92）。 ▪ 5 — 版本 4.9 - 4.10 数据，多主机（使用数据块 92）。 ▪ 6 — 版本 5.0.x .x 数据，单主机（使用数据块 111，请参阅完整主机配置文件数据块 5.0 - 5.0.2，第 B-363 页）。 ▪ 7 — 版本 5.0.x 数据，多主机（使用数据块 111，请参阅完整主机配置文件数据块 5.0 - 5.0.2，第 B-363 页）。 ▪ 8 — 版本 5.1.x 数据，多主机（使用数据块 111，请参阅完整主机配置文件数据块 5.1.1，第 B-372 页）。 ▪ 9 — 版本 5.1.x 数据，多主机（使用数据块 111，请参阅完整主机配置文件数据块 5.1.1，第 B-372 页）。 ▪ 10—规则文档数据（使用数据块27，请参阅规则文档消息格式，第 2-27 页） ▪ 11 — 版本 5.2x 数据，多主机（使用数据块 111，请参阅完整主机配置文件数据块 5.2.x，第 B-381 页）。 ▪ 12 — 版本 5.2.x 数据，多主机（使用数据块 111，参阅完整主机配置文件数据块 5.2.x，第 B-381 页）。 ▪ 13 — 版本 5.3+ 数据，多主机（使用数据块 111，参阅完整主机配置文件数据块 5.3+，第 5-1 页）。 ▪ 14 — 版本 5.3+ 数据，多主机（使用数据块 111，参阅完整主机配置文件数据块 5.3+，第 5-1 页）。
标志 (Flags)	32 位字段	▪ 0x00000001 - 使主机配置文件的“注释”字段填充（有关 Cisco Secure Firewall 系统中存储的主机的用户定义信息）。 ▪ 0x00000002 - 使服务块的“横幅”字段填充（为服务检测到的第一个数据包的前 256 个字节）。默认禁用横幅，只有配置后才能使用。
起始 IP 地址 (Start IP Address)	uint8[16]	应返回其数据的主机的 IP 地址（如果请求针对单主机），或 IP 地址范围的起始地址（如果请求针对多主机）。可以是 IPv4 或 IPv6 地址。
结束 IP 地址 (End IP Address)	uint8[16]	IP 地址范围的结束地址（如果请求针对多主机），或起始 IP 地址的值（如果请求针对单主机）。可以是 IPv4 或 IPv6 地址。

下图显示了旧版主机请求消息的格式。eStreamer 仍会响应此请求。与当前请求的唯一区别是 IPv4 地址字段较小。加阴影的字段是主机请求消息格式特有的，后面的表格给出了这些字段的定义。前面的三个字段是标准消息报头。



下表对消息字段进行了说明。

表 2-14 主机请求消息字段

字段	数据类型	说明 (Description)
数据类型 (Data Type)	uint32	使用下列代码请求单个主机或多个主机的数据: ▪ 0 - 版本 3.5-4.6 数据，单主机。 ▪ 1 - 版本 3.5-4.6 数据，多主机（使用数据块 34）。 ▪ 2 - 版本 4.7-4.8 数据，单主机（使用数据块 47）。 ▪ 3 - 版本 4.7-4.8 数据，多主机（使用数据块 47）。 ▪ 4 - 版本 4.9 - 4.10 数据，单主机（使用数据块 92）。 ▪ 5 - 版本 4.9 - 4.10 数据，多主机（使用数据块 92）。 ▪ 6 - 版本 5.0+ 数据，单主机（使用数据块 111，参阅完整主机配置文件数据块 5.3+，第 5-1 页）。 ▪ 7 - 版本 5.0+ 数据，多主机（使用数据块 111，参阅完整主机配置文件数据块 5.3+，第 5-1 页）。
标志 (Flags)	32 位字段	▪ 0x00000001 - 使主机配置文件的“注释”字段填充（有关 Cisco Secure Firewall 系统中存储的主机的用户定义信息）。 ▪ 0x00000002 - 使服务块的“横幅”字段填充（为服务检测到的第一个数据包的前 256 个字节）。默认禁用横幅，只有配置后才能使用。
起始 IP 地址 (Start IP Address)	uint8[4]	应返回其数据的主机的 IP 地址（如果请求针对单主机），或 IP 地址范围的起始地址（如果请求针对多主机）。以 IP 地址八位字节指定地址。
结束 IP 地址 (End IP Address)	uint8[4]	IP 地址范围的结束地址（如果请求针对多主机），或起始 IP 地址的值（如果请求针对单主机）。

规则文档消息格式

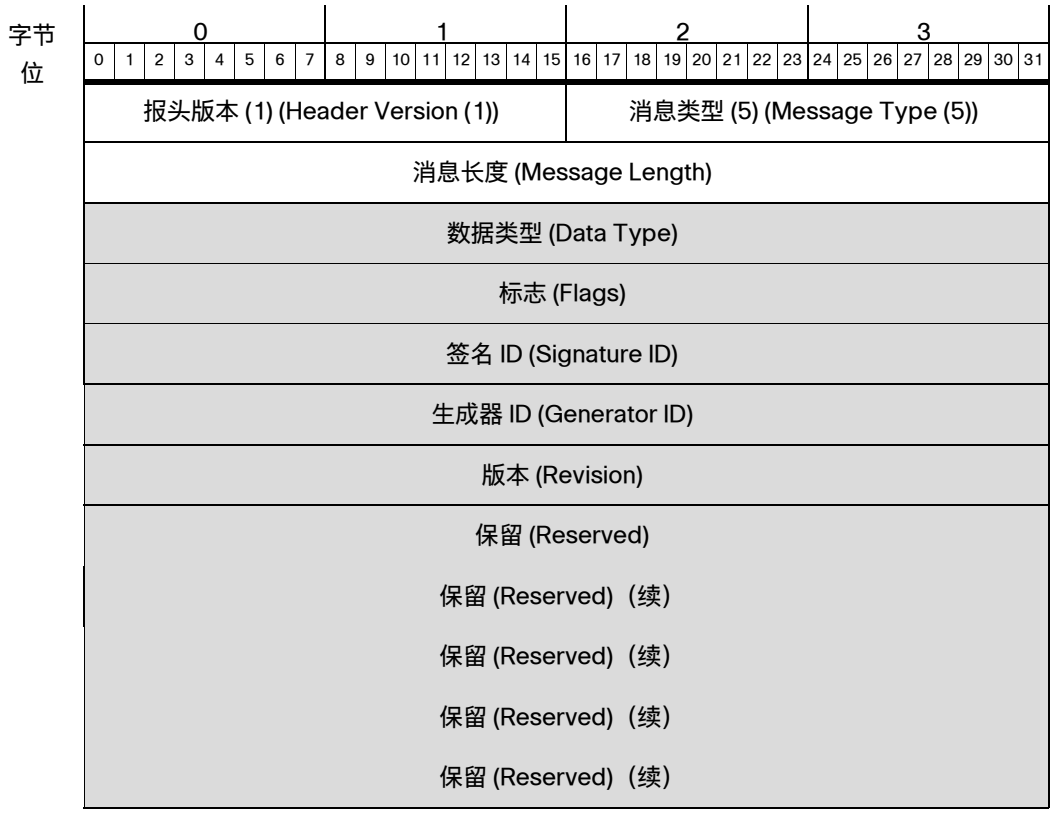
要接收规则文档配置文件，您需要提交规则文档消息。您可以按生成器 和版本请求这些规则文档配置文件。

请注意，对于所有数据请求（包括规则文档信息请求），都必须先通过提交事件流请求消息来初始化会话。要设置仅流传输主机数据，您可以在您的初始事件流请求消息中使用以下任意一个请求标志设置：

- 设置表示适当版本的元数据的位（这可能有助于流传输主机数据）
- 设置无请求标志
- 设置位 11（在使用旧版 eStreamer 时禁用任何默认事件流传输）

在初始消息后，使用规则文档消息（类型 10）来指定规则。

下图显示了规则文档消息的格式。加阴影的字段是规则文档消息格式特有的，后面的表格给出了这些字段的定义。前面的三个字段是标准消息报头。



下表对消息字段进行了说明。

表 2-15 规则文档消息字段

字段	数据类型	说明 (Description)
数据类型 (Data Type)	uint32	请求规则文档数据块的数据。值始终为 10。请参阅用于 5.2+ 的规则文档数据块，第 3-105 页。
标志 (Flags)	32 位字段	▪ 0x00000001 - 使规则文档数据块的“注释”(Notes) 字段被填充（有关 Cisco Secure Firewall 系统中存储的主机的用户定义信息）。 ▪ 0x00000002 - 使服务块的“横幅”字段填充（为服务检测到的第一个数据包的前 256 个字节）。默认禁用横幅，只有配置后才能使用。
签名 ID (Signature ID)	uint32	所请求规则的标识号。
生成器 ID (Generator ID)	uint32	所请求规则的 Cisco Secure Firewall 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
已预留	uint8[20]	当前不使用此字段。

主机数据和多主机数据消息格式

eStreamer 通过发送主机数据消息响应主机请求，每条消息都带有完整的主机配置文件数据块。eStreamer 为请求中指定的每个主机发送一条主机数据消息。eStreamer 使用类型 6 消息响应单主机配置文件请求，并使用类型 7 消息响应多主机请求。类型 6 和类型 7 消息的格式相同，只是消息类型不同。

主机数据消息没有记录类型字段。消息的结构通过消息中包含的完整主机配置文件的消息类型和数据块类型传输。完整主机配置文件数据块为一组数据块系列。

下图显示了主机数据消息的格式，后面的表格定义加阴影的字段：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (6	7) (Message Type (6	7))													
消息长度 (Message Length)																																
完整主机配置文件数据块类型 (Full Host Profile Data Block Type) 请参阅表 4-30主机发现和连接数据块类型，第 4-61 页																																
长度 (Length)																																
完整主机配置文件数据块 (Full Host Profile Data Block)																																

主机请求消息特有的字段如下：

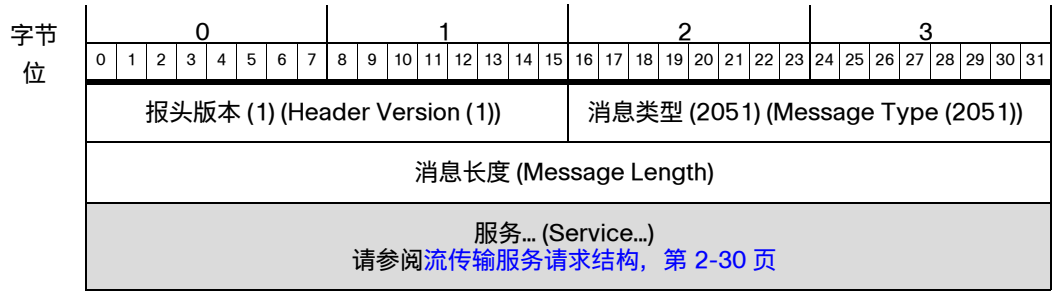
表 2-16

字段	数据类型	说明 (Description)
完整主机配置文件数据块类型 (Full Host Profile Data Block Type)	uint32	为消息中包含的完整主机配置文件数据指定数据块类型。请参阅表 4-30主机发现和连接数据块类型，第 4-61 页。
长度 (Length)	uint32	消息中完整主机配置文件数据的长度。
完整主机配置文件数据块 (Full Host Profile Data Block)	变量	主机数据。有关当前完整主机配置文件数据块的定义的链接，请参阅表 4-30主机发现和连接数据块类型，第 4-61 页。

流传输信息消息格式

当 eStreamer 服务收到需要一个扩展请求时，它会向客户端发送流传输信息消息，如下所述。此消息通告服务器的可用服务列表。目前，唯一的相关选项是 eStreamer 服务 (6667)，不过该消息可能会列出其他服务（应忽略这些服务）。通告的每项服务都由一个流传输服务请求结构（在流传输服务请求结构，第 2-30 页中介绍）表示。

下图说明流传输信息消息的格式。加阴影的字段是此消息类型所特有的。前面的三个字段是标准消息报头。



流传输信息消息的字段如下：

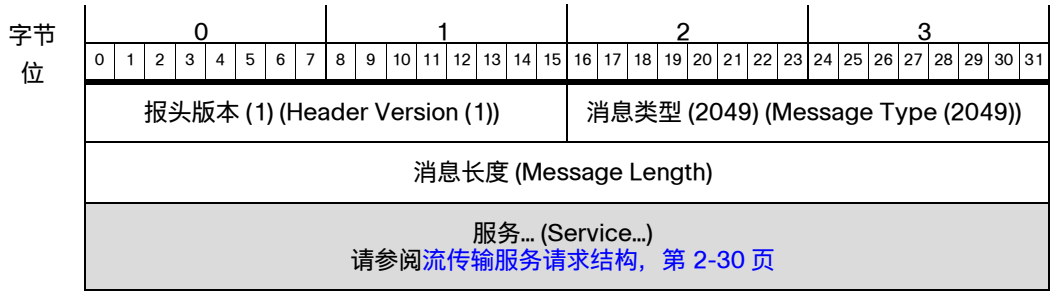
表 2-17　流传输信息消息字段

字段	数据类型	说明 (Description)
报头版本 (Header Version)	uint16	设置为 1。
消息类型 (Message Type)	uint16	eStreamer 消息类型。对于流传输请求消息，设置为 2051。
消息长度 (Message Length)	uint32	在消息报头后面的消息内容长度。不包括报头版本、消息类型和消息长度字段中的字节。
服务[] (Service[])	数组	可用服务的列表。请参阅流传输服务请求结构，第 2-30 页。

流传输请求消息格式

客户端使用流传输请求消息向 eStreamer 指定其要使用的流传输信息消息中的服务，后面跟着一组对要进行流传输的事件类型和版本的请求。下图显示该消息结构，后面的表格给出了字段的定义。请求的服务由一个流传输服务请求结构（在流传输服务请求结构，第 2-30 页中介绍）表示。

下图说明流传输信息消息的格式。加阴影的字段是此消息类型所特有的。前面的三个字段是标准消息报头。



流传输请求消息的字段如下：

表 2-18　　流传输请求消息字段

字段	数据类型	说明 (Description)
报头版本 (Header Version)	uint16	设置为 1。
消息类型 (Message Type)	uint16	eStreamer 消息类型。对于流传输请求消息，设置为 2049。
消息长度 (Message Length)	uint32	在消息报头后面的消息内容长度。不包括报头版本、消息类型和消息长度字段中的字节。
服务[] (Service[])	数组	请求的服务结构的列表。请参阅流传输服务请求结构，第 2-30 页。

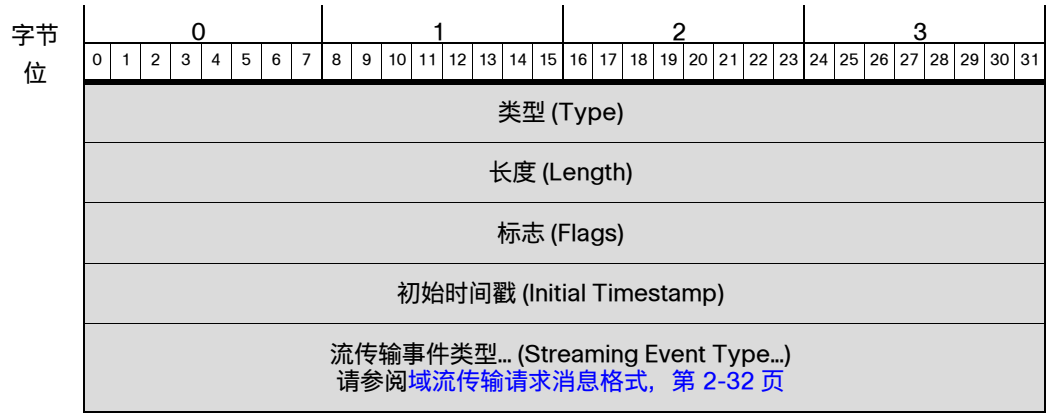
流传输服务请求结构

对于其通告的每项服务，eStreamer 服务都会在流传输信息消息中发送一个流传输服务请求数据结构。eStreamer 服务不使用流传输服务请求的最后一个字段。该字段用于要包含的事件类型列表。

客户端会处理来自 eStreamer 的流传输服务请求结构，并在其返回给服务器的响应中使用相同的结构。客户端向服务器发送的流传输服务请求首先包含一个对 eStreamer 通告的服务的请求，其次包含一个流传输事件类型结构列表（指定客户端希望接收的请求的事件类型）。

每个流传输事件类型结构包含两个字段，指定每个请求的事件类型的事件类型和版本。有关流传输事件类型结构的信息，请参阅域流传输请求消息格式，第 2-32 页。

下图显示了流传输服务请求结构的字段。后面的表格定义这些字段。



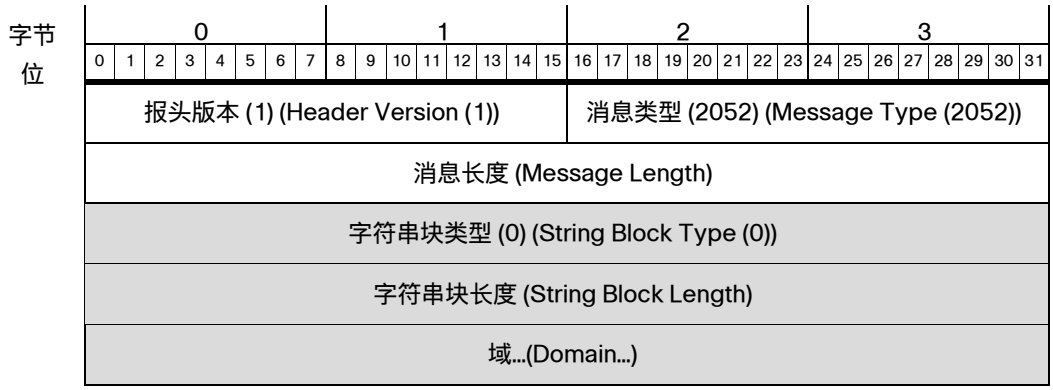
流传输服务请求结构的字段如下：

表 2-19　　流传输服务请求字段

字段	数据类型	说明
类型 (Type)	uint32	服务 ID。 在eStreamer服务器消息中，此字段通告一项可用服务。 在客户端消息中，此字段指定一项请求的服务。 当前有效选项： ▪ 6667（用于 eStreamer 服务）
长度 (Length)	uint32	服务请求长度。描述服务请求的长度，包括类型和长度。 请注意，长度必须包括消息中的所有流传输事件类型记录，加上终止记录。
标志 (Flags)	uint32	在 eStreamer 的流传输信息消息中：始终为 0。 在客户端的流传输请求消息中：复制原始事件流请求消息中的标志设置。
初始时间戳 (Initial Timestamp)	uint32	在 eStreamer 的流传输信息消息中：始终为 0。 在客户端的流传输请求消息中：复制原始事件流请求消息中的时间戳。
流传输事件类型 (Streaming Event Type)	数组	在 eStreamer 的流传输信息消息中： ▪ 已保留供将来使用。长度为 0。 在客户端的流传输请求消息中： ▪ 每个请求的事件类型各有一个流传输事件类型条目。请参阅域流传输请求消息格式，第 2-32 页。 ▪ 以 0 事件类型条目终止请求列表，事件类型和版本都设置为 0。 请参阅域流传输请求消息格式，第 2-32 页。

域流传输请求消息格式

客户端使用域流传输请求消息向 eStreamer 请求来自特定域的事件。下图显示该消息结构，后面的表格给出了字段的定义。加阴影的字段是此消息类型所特有的。前面的三个字段是标准消息报头。



域流传输请求消息的字段如下：

表 2-20 域流传输请求消息字段

字段	数据类型	说明 (Description)
报头版本 (Header Version)	uint16	设置为 1。
消息类型 (Message Type)	uint16	eStreamer 消息类型。对于域流传输请求消息，设置为 2052。
消息长度 (Message Length)	uint32	在消息报头后面的消息内容长度。不包括报头版本、消息类型和消息长度字段中的字节。
字符串块类型 (String Block Type)	uint32	启动包含域的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	域字符串数据块包含的字节数，包括数据块类型和报头字段的八个字节，加上域中的字节数。
域 (Domain)	字符串	请求流传输事件的域。如果留空，则服务将向客户端具有访问权限的所有域进行事件流传输。

流传输事件类型结构

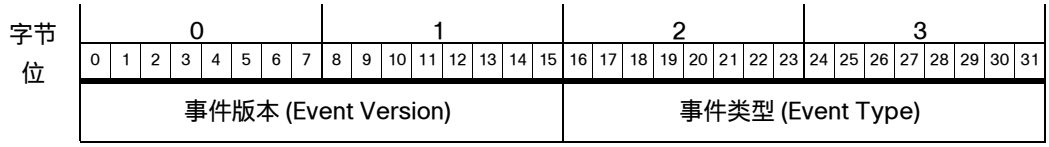
eStreamer 客户端使用流传输事件类型结构来指定事件的版本和类型。每个事件版本/类型组合构成一个事件流请求。

流传输事件类型结构的列表必须以一个所有字段都设置为零的结构终止。特点：

`Event Version = 0`

`事件类型 = 0`

下图说明流传输事件类型结构的格式。



流传输事件类型结构的字段如下：

表 2-21　　流传输事件类型字段

字段	数据类型	说明 (Description)
事件版本 (Event Version)	uint16	事件类型的版本号。有关每种事件类型的受支持版本的列表，请参阅表 2-22扩展请求的事件类型和版本，第 2-34 页。
事件类型 (Event Type)	uint16	请求的事件类型的代码。有关有效事件类型和版本代码的最新列表，请参阅表 2-22扩展请求的事件类型和版本，第 2-34 页。 要终止事件类型列表，应将事件类型和事件版本均设置为 0。

下表列出了客户端可以在扩展请求中指定的事件类型和版本。该表指出了与每种事件类型版本对应的管理中心软件版本。例如，要请求版本 4.8.0.2 - 4.9.1 中管理中心支持的关联事件，您应该请求事件类型 31、版本 5。如果事件被记录为不同的事件类型，它将被升级或降级，以符合请求的事件类型的格式。

表 2-22　　扩展请求的事件类型和版本

要请求...	使用此事件版本号...	以及此事件代码
入侵事件	1 — 4.8.x 及更早版本 2 — 4.9 - 4.10.x 3 — 5.0 - 5.1 4 — 5.1.1.x 5 — 5.2.x 6 — 5.3 7 — 5.3.1 8 — 5.4.x 9— 6.x 10— 7.0+	12
元数据	1 — 3.2 - 4.5.x 2 — 4.6.0.x 3 — 4.6.1 - 4.6.x 4 - 4.7+	21
关联和合规性允许列表事件	1 — 3.2 及更早版本 2 — 4.0 - 4.4.x 3 — 4.5 - 4.6.1 4 — 4.7 - 4.8.0.1 5 — 4.8.0.2 - 4.9.1.x 6 — 4.10.0 - 4.10.x 7 — 5.0 - 5.0.2 8 — 5.1 - 5.3.x 9 - 5.4+	31
发现事件	1 — 3.2 及更早版本 2 — 3.0 - 3.4.x 3 — 3.5 - 4.6.x 4 — 4.7 - 4.8.x 5 — 4.9.0.x 6 — 4.9.1 - 4.9.x.x 7 — 4.10.0 - 4.10.x 8 — 5.0.x 9 — 5.1.x 10 — 5.2 - 5.3 11 — 5.3.1+	61

表 2-22　　扩展请求的事件类型和版本 （续）

要请求...	使用此事件版本号...	以及此事件代码
连接事件	1 — 4.0 - 4.1 3 — 4.5 - 4.6.1 4 — 4.7 - 4.9.0.x 5 — 4.9.1 - 4.10.x 6 — 5.0.x 7 — 5.1.0.x 8 — 5.1.1.x 9 — 5.2.x 10 — 5.3 11 — 5.3.1 12 — 5.4 13 — 5.4.0.1-5.4.0.2 14 — 6.0.x 15 — 6.1.x 16 — 7.0.x 17 — 7.1+	71
用户事件	1 — 4.7 - 4.10.x 2 — 5.0.x 3 — 5.1-5.1.x 4 — 5.2 5— 6.0 6— 6.1 7— 6.2+	91
恶意软件事件	1 — 5.1.0.x 2 — 5.1.1.x 3 — 5.2.x 4 — 5.3 5 — 5.3.1 6 — 5.4.x 7— 6.x 8— 7.0+	101
文件事件	1 — 5.1.1 - 5.1.x 2 — 5.2.x 3 — 5.3 4 — 5.3.1 5 — 5.4.x 6 — 6.x 7 — 7.0+	111
影响关联事件	1 — 5.2.x 及更早版本 2 - 5.3+	131
终止列表中的事件类型	0	0

扩展请求消息示例

流传输信息消息

在以下示例中，服务器通告两项服务，一是类型 6667 (eStreamer)，二是类型 5000。在来自服务器的流传输信息消息中，标志字段和初始时间戳字段均为 0，该消息不指定事件类型。

表 2-23

报头版本:	1	/*始终为 1*/
消息类型:	2051	/*流传输信息消息*/
消息长度	32	/*消息内容字节数*/
服务[1].类型	6667	/*eStreamer 服务 ID*/
服务[1].长度	8	
服务[1].标志	0	/*没有来自服务器的标志*/
服务[1].初始时间戳	0	/*始终为 0*/
服务[2].类型	5000	/*服务-2 ID*/
服务[2].长度	8	
服务[2].标志	0	/*没有来自服务器的标志*/
服务[2].初始时间戳	0	/*始终为 0*/
报头版本:	1	/*始终为 1*/
消息类型:	2051	/*流传输信息消息*/

流传输请求消息

下面是一个流传输请求消息，其中客户端请求服务类型 6667 (eStreamer)，并指定了两个事件类型：版本 6 的连接事件（事件类型 71）和版本 4 的元数据（事件类型 21）。

表 2-24

报头版本:	1	/*始终为 1*/
消息类型:	2049	/*流请求消息*/
消息长度	28	/*负载字节*/
服务[1].类型	6667	/*eStreamer 服务 ID*/
服务[1].长度	20	
服务[1].标志	30	/*原始标志值*/
服务[1].初始时间戳	0	/*原始时间戳*/
服务[1].事件[1].版本	6	/*版本 6*/
服务[1].事件[1].类型	71	/*连接事件*/
服务[1].事件[2].版本	4	/* 版本 4*/
服务[1].事件[2].类型	21	/*元数据*/

表 2-24

服务[1].事件[3].版本	0	/*终止事件列表*/
服务[1].事件[3].类型	0	/*终止事件列表*/

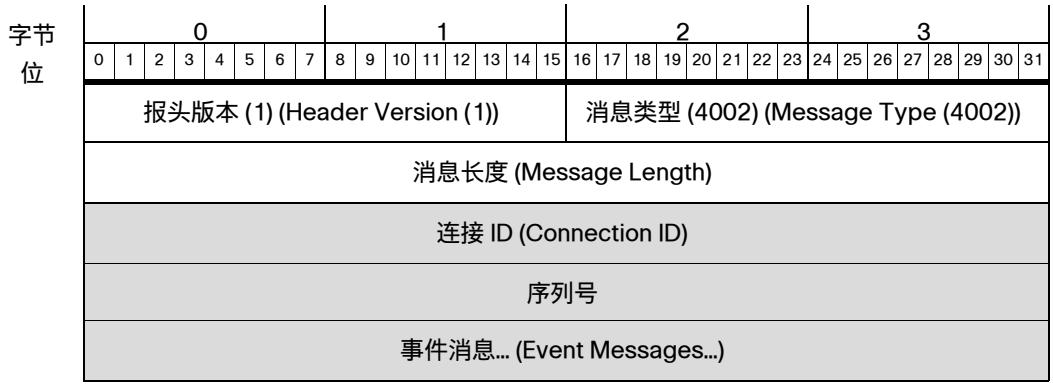
消息捆绑包格式

当客户端提交扩展请求时，eStreamer 服务器以捆绑包格式发送消息。

客户端回复空消息，确认收到整个捆绑包。客户端不应确认收到捆绑包内的单个消息。

消息捆绑包的消息类型应该为 4002。

下图显示消息捆绑包的结构。加阴影的字段是捆绑包消息类型所特有的。后面的表格介绍字段和数据结构的内容。



消息捆绑包消息的字段如下：

表 2-25　　消息捆绑包消息字段

字段	数据类型	说明 (Description)
报头版本 (Header Version)	uint16	始终为 1。
消息类型 (Message Type)	uint16	始终为 4002。
消息长度 (Message Length)	uint32	在消息报头后面的消息内容长度。不包括捆绑包的报头版本、消息类型和消息长度字段中的字节。 当客户端从捆绑包加载一条消息时，它会从此字段显示的长度中减去该消息的总长度（包括报头）。只要余数为正值，就有更多的消息要处理。
连接 ID (Connection ID)	uint32	与服务器建立的连接的唯一标识符。
序列号 (Serial Number)	uint32	从 1 开始，eStreamer 服务器每发送一个捆绑包，增加 1。
事件消息 [] (Event Messages [])	数组	服务器以捆绑包格式进行流传输的事件。每个消息都有全套报头，包括消息版本号 (1)、存档时间戳（如有请求）等等。

了解元数据

eStreamer 服务器可以将元数据与请求的事件记录一起提供。要接收元数据，您必须明确提出请求。有关如何请求给定版本的元数据的信息，请参阅表 2-6请求标志，第 2-13 页。元数据为事件记录中的代码和数字标识符提供情景信息。例如，入侵事件仅包含检测设备的内部标识符，而元数据则提供设备名称。

根据请求的元数据和环境，发送的元数据量可能有很大差异。

元数据传输

如果请求消息指定元数据，则 eStreamer 在发送任何相关的事件记录之前，先发送相关的元数据记录。

eStreamer 会记录已发送给客户端的元数据，不会重复发送相同的元数据记录。客户端应缓存收到的每个元数据记录。 如果客户端应用使用有限的缓存大小，则当缓存已满时，客户端应刷新缓存并重新连接到 eStreamer 服务，以确保客户端接收正在流传输的事件的所有数据值。从一个会话进入下一个会话后，eStreamer 不保留元数据传输历史记录，因此，当开始一个新会话，并且请求消息指定元数据时，eStreamer 会从头开始重新进行元数据流传输。 重新连接时，客户端可以在请求消息中指定“初始时间戳”，以避免事件重复或丢失事件。

章 节 3

了解入侵和关联数据结构

eStreamer 服务可传输多种数据记录类型，以向客户端交付请求的事件和元数据。本章介绍以下类型的事件数据的数据记录的结构：

- 受管设备生成的入侵事件数据和事件额外数据
- 管理中心生成的关联（合规性）事件
- 元数据记录

本章中的以下各节定义事件消息结构：

- 入侵事件和元数据记录类型，第 3-1 页。

有关 eStreamer 用于传输数据记录的消息格式的总体概述，请参阅事件数据消息格式，第 2-16 页。

入侵事件和元数据记录类型

下表列出了目前支持的入侵事件、入侵事件额外数据以及元数据消息的所有记录类型。这些记录类型的数据位于固定长度的字段中。相比之下，关联事件记录包含一个或多个层次的长度可变的嵌套数据块。下表提供了到定义关联数据记录结构的子节的链接。

对于有些记录类型，eStreamer 支持多个的版本。该表指示每个版本的状态（当前版本或旧版本）。当前记录是最新版本。旧记录已被较新的版本替代，但仍可以从 eStreamer 中请求旧记录。

表 3-1　　入侵事件与一般元数据记录类型

记录类型	块类型 (Block Type)	系列	说明 (Description)	记录状态	描述的数据格式...
2	不适用	不适用	数据包数据（版本 4.8.0.2+）	当前	数据包记录 4.8.0.2+，第 3-5 页
4	不适用	不适用	优先级元数据	当前	优先级记录，第 3-6 页
9	20	1	入侵影响警报	传统	入侵影响警报数据，第 B-63 页
9	153	1	入侵影响警报	当前	入侵影响警报数据 5.3+，第 3-19 页
62	不适用	2	用户元数据	当前	用户记录，第 3-22 页
66	不适用	不适用	规则消息元数据（版本 4.6.1+）	当前	用于 4.6.1+ 的规则消息记录，第 3-23 页
67	不适用	不适用	分类元数据（版本 4.6.1+）	当前	用于 4.6.1+ 的分类记录，第 3-25 页

表 3-1 入侵事件与一般元数据记录类型 （续）

记录类型	块类型 (Block Type)	系列	说明 (Description)	记录状态	描述的数据格式...
69	不适用	不适用	关联策略元数据（版本 4.6.1+）	当前	关联策略记录，第 3-26 页
70	不适用	不适用	关联规则元数据（版本 4.6.1+）	当前	关联规则记录，第 3-27 页
104	不适用	不适用	入侵事件 (IPv4) 记录 4.9 - 4.10.x	传统	产品的较早版本
105	不适用	不适用	入侵事件 (IPv6) 记录 4.9 - 4.10.x	传统	产品的较早版本
110	4	2	入侵事件额外数据（版本 4.10.0+）	传统模式	入侵事件额外数据记录，第 B-66 页
111	5	2	入侵事件额外数据元数据（版本 4.10.0+）	传统模式	入侵事件额外数据元数据，第 B-67 页
112	128	1	用于 5.1-5.3.x 的关联事件	传统	用于 5.1-5.3.x 的关联事件，第 B-355 页
112	156	1	用于 5.4+ 的关联事件	当前	用于 5.4+ 的关联事件，第 3-42 页
115	14	2	安全区名称元数据	当前	安全区名称记录，第 3-29 页
116	14	2	接口名称元数据	当前	接口名称记录，第 3-30 页
117	14	2	访问控制策略名称元数据	当前	访问控制策略名称记录，第 3-32 页
118	15	2	入侵策略名称元数据	当前	入侵策略名称记录，第 4-21 页
119	15	2	访问控制规则 ID 元数据	当前	访问控制规则 ID 记录元数据，第 3-33 页
120	不适用	不适用	访问控制规则操作元数据	当前	访问控制规则操作记录元数据，第 4-23 页
121	不适用	不适用	URL 类别元数据	当前	URL 类别记录元数据，第 4-24 页
122	不适用	不适用	URL 信誉元数据	当前	URL 信誉记录元数据，第 4-24 页
123	不适用	不适用	受管设备元数据	当前	受管设备记录元数据，第 3-34 页
不适用	64	2	访问控制策略名称数据块	当前	访问控制策略名称数据块，第 3-79 页
124	59	2	访问控制策略规则原因数据块	当前	用于 6.0+ 的访问控制策略规则原因数据块，第 3-77 页
125	不适用	2	恶意软件事件记录（版本 5.1.1+）	当前	恶意软件事件记录 5.1.1+，第 3-35 页
125	24	2	恶意软件事件（版本 5.1.1+）	传统模式	恶意软件事件数据块 5.1.1.x，第 B-74 页
125	33	2	恶意软件事件（版本 5.2.x）	传统	恶意软件事件数据块 5.2.x，第 B-80 页
125	35	2	恶意软件事件（版本 5.3）	传统	恶意软件事件数据块 5.3，第 B-87 页
125	44	2	恶意软件事件（版本 5.3.1）	传统	恶意软件事件数据块 5.3.1，第 B-94 页
125	47	2	恶意软件事件（版本 5.4.x）	传统模式	恶意软件事件数据块 5.4.x，第 B-101 页
125	62	2	恶意软件事件（版本 6.x）	传统模式	恶意软件事件数据块 6.x，第 B-111 页
125	80	2	恶意软件事件（版本 7.0+）	当前	恶意软件事件数据块 7.0+，第 3-92 页

表 3-1　　入侵事件与一般元数据记录类型 （续）

记录类型	块类型 (Block Type)	系列	说明 (Description)	记录状态	描述的数据格式...
127	14	2	思科高级恶意软件防护云名称元数据（版本 5.1+）	当前	思科高级恶意软件防护云名称元数据，第 3-36 页
128	不适用	不适用	恶意软件事件类型元数据（版本 5.1+）	当前	恶意软件事件类型元数据，第 3-37 页
129	不适用	不适用	恶意软件事件子类型元数据（版本 5.1+）	当前	恶意软件事件子类型元数据，第 3-38 页
130	不适用	不适用	面向终端的 AMP 检测器类型元数据（版本 5.1+）	当前	面向终端的 AMP 检测器类型元数据，第 3-39 页
131	不适用	不适用	面向终端的 AMP 文件类型元数据（版本 5.1+）	当前	面向终端的 AMP 文件类型元数据，第 3-40 页
132	不适用	不适用	安全情景名称	当前	安全情景名称，第 3-41 页
140	27	2	用于 5.2+ 的规则文档数据块	当前	用于 5.2+ 的规则文档数据块，第 3-105 页
207	不适用	不适用	入侵事件 (IPv4) 记录 5.0.x - 5.1	传统	入侵事件 (IPv4) 记录 5.0.x - 5.1，第 B-2 页
208	不适用	不适用	入侵事件 (IPv6) 记录 5.0.x - 5.1	传统	入侵事件 (IPv6) 记录 5.0.x - 5.1，第 B-6 页
260	19	2	ICMP 类型数据数据块	当前	ICMP 类型数据块，第 3-66 页
270	20	2	ICMP 代码数据块	当前	ICMP 代码数据块，第 3-67 页
282	不适用	2	用于 5.4.1+ 的安全情报类别元数据	当前	用于 5.4.1+ 的安全情报类别元数据，第 3-68 页
300	不适用	不适用	用于 6.0+ 的领域元数据	当前	用于 6.0+ 的领域元数据，第 3-69 页
301	58	2	用于 6.0+ 的终端配置文件	当前	用于 6.0+ 的终端配置文件数据块，第 3-70 页
302	不适用	不适用	用于 6.0+ 的安全组元数据	当前	用于 6.0+ 的安全组元数据，第 3-72 页
320	不适用	不适用	用于 6.0+ 的 DNS 记录类型元数据	当前	用于 6.0+ 的 DNS 记录类型元数据，第 3-72 页
321	不适用	不适用	用于 6.0+ 的 DNS 响应类型元数据	当前	用于 6.0+ 的 DNS 响应类型元数据，第 3-74 页
322	不适用	不适用	用于 6.0+ 的 Sinkhole 元数据	当前	用于 6.0+ 的 Sinkhole 元数据，第 3-75 页
350	不适用	不适用	用于 6.0+ 的 Netmap 域元数据	当前	用于 6.0+ 的 Netmap 域元数据，第 3-76 页
400	34	2	入侵事件记录 5.2.x	传统	入侵事件记录 5.2.x，第 B-12 页
400	41	2	入侵事件记录 5.3	传统	入侵事件记录 5.3，第 B-18 页
400	42	2	入侵事件记录 5.3.1	传统	入侵事件记录 5.3.1，第 B-29 页
400	45	2	入侵事件记录 5.4.x	传统	入侵事件记录 5.4.x，第 B-36 页
400	60	2	入侵事件记录 6.x	传统模式	入侵事件记录 6.x，第 B-45 页
400	81	2	入侵事件记录 7.0	传统模式	入侵事件记录 7.0，第 B-54 页
400	85	2	入侵事件记录 7.1+	当前	入侵事件记录 7.1+，第 3-7 页

表 3-1 入侵事件与一般元数据记录类型 （续）

记录类型	块类型 (Block Type)	系列	说明 (Description)	记录状态	描述的数据格式...
500	32	2	文件事件 （版本 5.2.x）	传统	用于 5.2 的文件事件，第 B-313 页
500	38	2	文件事件 （版本 5.3）	传统	用于 5.3 的文件事件，第 B-317 页
500	43	2	文件事件 （版本 5.3.1）	传统	用于 5.3.1 的文件事件，第 B-323 页
500	46	2	文件事件 （版本 5.4.x）	当前	7.0+ 的文件事件，第 3-82 页
502	32	2	文件事件 （版本 5.2.x）	传统	用于 5.2 的文件事件，第 B-313 页
502	38	2	文件事件 （版本 5.3）	传统	用于 5.3 的文件事件，第 B-317 页
502	43	2	文件事件 （版本 5.3.1）	传统	用于 5.3.1 的文件事件，第 B-323 页
502	46	2	文件事件 （版本 5.4.x）	传统模式	用于 5.4 的文件事件，第 B-329 页
502	56	2	文件事件 （版本 6.x）	传统模式	6.x 的文件事件，第 B-337 页
502	79	2	文件事件 （版本 7.0+）	当前	7.0+ 的文件事件，第 3-82 页
510	不适用	不适用	用于 5.3+ 的文件类型 ID 元数据	当前	用于 5.3+ 的文件类型 ID 元数据，第 3-104 页
511	26	2	用于 5.11-5.2.x 的文件事件 SHA 散列	传统	用于 5.1.1-5.2.x 的文件事件 SHA 散列，第 B-346 页
511	40	2	用于 5.3+ 的文件事件 SHA 散列	当前	用于 5.3+ 的文件事件 SHA 散列，第 3-102 页
515	不适用	不适用	用于 6.0+ 的文件日志存储元数据	当前	用于 6.0+ 的文件日志存储元数据，第 3-109 页
516	不适用	不适用	用于 6.0+ 的文件日志沙盒元数据	当前	用于 6.0+ 的文件日志沙盒元数据，第 3-109 页
517	不适用	不适用	用于 6.0+ 的文件日志 Spero 元数据	当前	用于 6.0+ 的文件日志 Spero 元数据，第 3-110 页
518	不适用	不适用	用于 6.0+ 的文件日志存档元数据	当前	用于 6.0+ 的文件日志存档元数据，第 3-111 页
519	不适用	不适用	用于 6.0+ 的文件日志静态分析元数据	当前	用于 6.0+ 的文件日志静态分析元数据，第 3-112 页
520	28	2	用于 5.2+ 的地理位置数据块	当前	用于 5.2+ 的地理位置数据块，第 3-113 页
530	不适用	不适用	用于 6.0+ 的文件策略名称	当前	用于 6.0+ 的文件策略名称，第 3-114 页
600	不适用	不适用	SSL 策略名称	当前	SSL 策略名称，第 3-115 页
601	51	2	SSL 规则 ID	当前	SSL 规则 ID，第 3-117 页
602	不适用	不适用	SSL 密码套件	当前	用于 5.4+ 的 SSL 证书详细信息数据块，第 3-124 页
604	不适用	不适用	SSL 版本	当前	SSL 版本，第 3-119 页
605	不适用	不适用	SSL 服务器证书状态	当前	SSL 服务器证书状态，第 3-120 页
606	不适用	不适用	SSL 实际操作	当前	SSL 实际操作，第 3-120 页
607	不适用	不适用	SSL 预期操作	当前	SSL 预期操作，第 3-121 页
608	不适用	不适用	SSL 流状态	当前	SSL 流状态，第 3-122 页

表 3-1　　入侵事件与一般元数据记录类型 （续）

记录类型	块类型 (Block Type)	系列	说明 (Description)	记录状态	描述的数据格式...
613	不适用	不适用	SSL URL 类别	当前	SSL URL 类别，第 3-123 页
614	50	2	用于 5.4+ 的 SSL 证书详细信息数据块	当前	用于 5.4+ 的 SSL 证书详细信息数据块，第 3-124 页
700	不适用	不适用	网络分析策略记录	当前	网络分析策略名称记录，第 3-129 页

数据包记录 4.8.0.2+

eStreamer 服务可传输与数据包记录中的事件相关的数据包数据，格式如下所示。当设置数据包标志（请求消息的“请求标志”(Request Flags) 字段中的位 0）时，发送数据包数据。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。请注意，“记录类型”(Record Type) 字段（出现在消息长度 (Message Length) 字段后面）的值为 2，表示数据包记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (2) (Record Type (2))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
设备 ID (设备 ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
数据包秒 (Packet Second)																																
数据包微秒 (Packet Microsecond)																																
链路类型 (Link Type)																																
数据包长度 (Packet Length)																																
数据包数据... (Packet Data...)																																

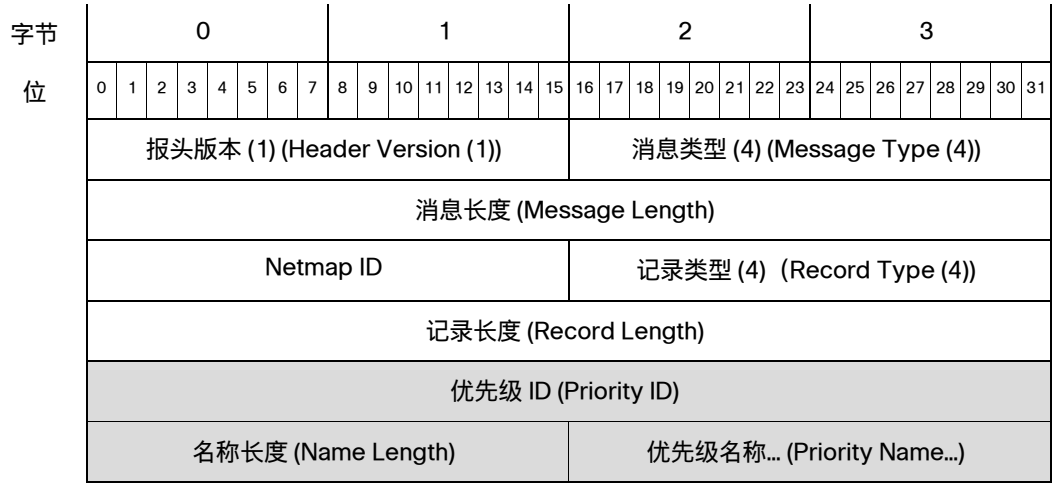
下表对数据包记录中的字段进行了说明。

表 3-2 数据包记录字段

字段	数据类型	说明
设备 ID (Device ID)	uint32	设备标识号。您可以通过请求版本 3 或版本 4 元数据获取与它们关联的设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件出现的秒数（从 1970/01/01 起）。
数据包秒 (Packet Second)	uint32	捕获数据包的秒数（从 1970/01/01 起）。
数据包微秒 (Packet Microsecond)	uint32	捕获数据包的微秒（一秒的百万分之一）增量。
链路类型 (Link Type)	uint32	链路层类型。目前，此值始终为 1（代表以太网层）。
数据包长度 (Packet Length)	uint32	数据包数据中包含的字节数。
数据包数据 (Packet Data)	变量	实际捕获的数据包数据（报头和负载）。

优先级记录

eStreamer 服务可传输与优先级记录中的事件相关的优先级信息，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送优先级信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 4，表示优先级记录。



下表对每个优先级特定字段进行了说明。

表 3-3　　优先级记录字段

字段	数据类型	说明 (Description)
优先级 ID (Priority ID)	uint32	表示优先级标识号。
名称长度 (Name Length)	uint16	优先级名称中包含的字节数。
优先级名称 (Priority Name)	变量	与优先级 ID 对应的优先级名称（1 - 高，2 - 中等，3 - 低）。

入侵事件记录 7.1+

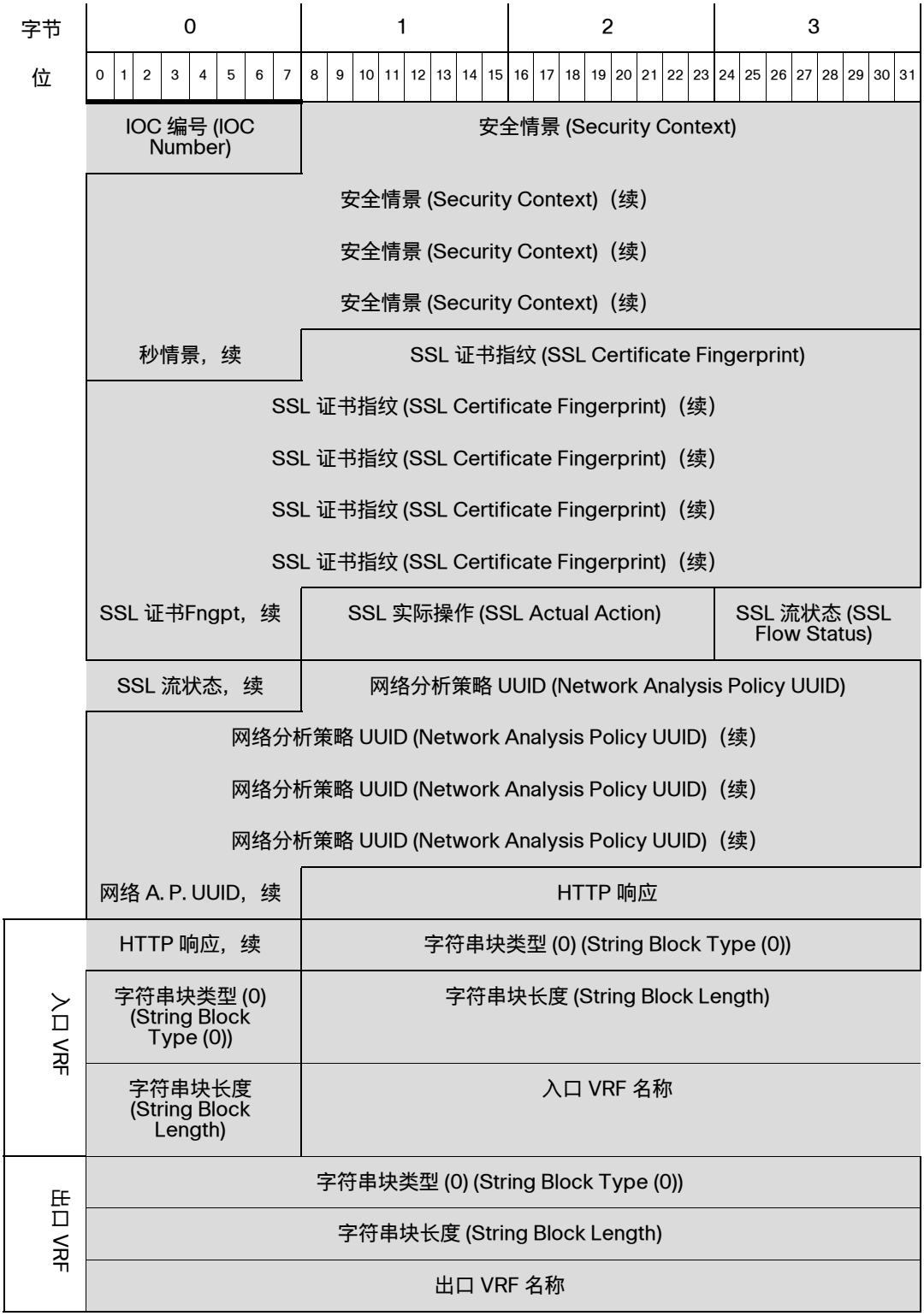
下图中的阴影部分表示入侵事件记录中的字段。此数据块的记录类型为系列 2 数据块组中的 400，块类型为系列 2 数据块组中的 85。它替代了块类型 81。添加了以前包含在额外事件数据中的 XFF 字段。

您可以通过扩展请求，仅从 eStreamer 请求 7.1+ 入侵事件，要提交扩展请求，您需要在流请求消息中请求事件类型代码 12 和版本代码 11（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
阻止类型 (85)																																
块长度 (Block Length)																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID（签名 ID）(Rule ID (Signature																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																
源 IP 地址 (Source IP Address) 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续）																																
目标 IP 地址 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址 (Destination IP Address)（续）																																
源端口或 ICMP 类型 (Source Port or ICMP Type)																	目标端口或 ICMP 代码 (Destination Port or ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								内联结果							
内联结果原因									MPLS 标签																							
MPLS 标签，续									VLAN ID																Pad							
填充位，续									策略 UUID (Policy UUID)																							
策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续）																																
策略 UUID (Policy UUID)（续）																									用户 ID							
用户 ID，续																									Web 应用 ID (Web Application ID)							
Web 应用 ID，续																									客户端应用 ID (Client Application ID)							
客户端应用 ID (Client Application ID)																									应用协议ID							


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
应用协议 ID，续
访问控制规则 ID
访问控制规则 ID，续
访问控制策略 UUID
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID (Access Control Policy UUID)（续）
接口入口 UUID
接口入口 UUID (Interface Ingress UUID)（续）
接口入口 UUID (Interface Ingress UUID)（续）
接口入口 UUID (Interface Ingress UUID)（续）
接口入口 UUID (Interface Ingress UUID)（续）
接口出口 UUID
接口出口 UUID (Interface Egress UUID)（续）
接口出口 UUID (Interface Egress UUID)（续）
接口出口 UUID (Interface Egress UUID)（续）
接口出口 UUID (Interface Egress UUID)（续）
秒区域入口UUID
安全区入口 UUID (Security Zone Ingress UUID)（续）
安全区入口 UUID (Security Zone Ingress UUID)（续）
安全区入口 UUID (Security Zone Ingress UUID)（续）
安全区入口 UUID (Security Zone Ingress UUID)（续）
秒区域出口UUID
安全区出口 UUID (Security Zone Egress UUID)（续）
安全区出口 UUID (Security Zone Egress UUID)（续）
安全区出口 UUID (Security Zone Egress UUID)（续）
安全区出口 UUID (Security Zone Egress UUID)（续）
连接时间戳
连接时间戳，续
连接实例ID
连接实例 ID
连接计数器 (Connection Counter)
源国家/地区 (Source Country)
源国家/地区 (Source Country)
目标国家/地区 (Destination Country)
IOC 编号 (IOC Number)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
IOC 编号 (IOC Number)
安全情景 (Security Context)
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
秒情景，续
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书Fngpt，续
SSL 实际操作 (SSL Actual Action)
SSL 流状态 (SSL Flow Status)
SSL 流状态，续
网络分析策略 UUID (Network Analysis Policy UUID)
网络分析策略 UUID (Network Analysis Policy UUID)（续）
网络分析策略 UUID (Network Analysis Policy UUID)（续）
网络分析策略 UUID (Network Analysis Policy UUID)（续）
网络 A. P. UUID，续
HTTP 响应
入口 VRF
HTTP 响应，续
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)
入口 VRF 名称
出口 VRF
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
出口 VRF 名称

下表对每个入侵事件记录数据字段进行了说明。

表 3-4 入侵事件记录 7.1+ 字段

字段	数据类型	说明 (Description)
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 85。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒（一秒的百万分之一）增量。
规则 ID（签名 ID） (Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的Cisco Secure Firewall 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标 IP 地址 (Destination IP Address)	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由
IP 协议 ID (IP Protocol ID)	uint8	IANA 指定的协议号。例如： ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP

表 3-4　　入侵事件记录 7.1+ 字段 （续）

字段	数据类型	说明 (Description)
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到管理中心上的特定优先级中。x 表示值可以为 0 或 1: ▪ 灰色（0，未知）：00X00000 ▪ 红色（1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）：00X0011X ▪ 黄色（3，当前不易受攻击）：00X0001X ▪ 蓝色（4，未知目标）：00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下: ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 - 灰色（未知影响）

表 3-4 入侵事件记录 7.1+ 字段 （续）

字段	数据类型	说明 (Description)
内联结果 (Inline Result)	uint8	表示内联结果的值。 ▪ 0 — 通过 ▪ 1 — 已丢弃 ▪ 2 — 将被丢弃（但配置不允许） ▪ 3— 已部分丢弃 ▪ 4— 阻止 ▪ 5— 将阻止 ▪ 6— 部分阻止 ▪ 7— 丢弃 ▪ 8— 将丢弃 ▪ 9— 拒绝 ▪ 10— 将拒绝 ▪ 11— 做出反应 ▪ 12— 将做出反应 ▪ 13— 重写 ▪ 14— 将重写
内联结果原因 (Inline Result Reason)	uint8	指示内联结果原因的值。 ▪ 1— 被动或分流模式下的接口 ▪ 2— “检测”检测模式下的入侵策略 ▪ 3— “检测”检测模式下的网络分析策略 ▪ 4— 连接超时 ▪ 5— 连接已关闭（内部使用） ▪ 6— 连接已关闭（内部使用） ▪ 7— 连接已关闭（内部使用）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID	uint32	用户的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。

表 3-4　　入侵事件记录 7.1+ 字段 （续）

字段	数据类型	说明 (Description)
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
接口入口 UUID (Interface Ingress UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
接口出口 UUID (Interface Egress UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
安全区入口 UUID (Security Zone Ingress UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
安全区出口 UUID (Security Zone Egress UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8[16]	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。

表 3-4 入侵事件记录 7.1+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 3-4　　入侵事件记录 7.1+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
网络分析策略 UUID (Network Analysis Policy UUID)	uint8[16]	创建入侵事件的网络分析策略的 UUID。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。
字符串块类型 (String Block Type)	uint32	启动包含入口 VRF 名称的字符串数据块。值始终为 0。

表 3-4 入侵事件记录 7.1+ 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“入口 VRF ”(Ingress VRF) 名称字段中的字节数。
入口 VRF 名称	字符串	用于流量进入网络的虚拟路由器。
字符串块类型 (String Block Type)	uint32	启动包含出口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“出口 VRF ”(Egress VRF) 名称字段中的字节数。
出口 VRF 名称	字符串	用于流量离开网络的虚拟路由器。
Snort 版本	uint8	Snort 版本号。
原始发起方 IP	uint16	包含连接的原始发起方的 IP 地址。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 主机名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 HTTP 主机名 (HTTP Hostname) 字段中的字节数。
HTTP 主机名 (HTTP Hostname)	字符串	包含在 HTTP 连接中找到的主机名。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP URI 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 HTTP URI 字段中的字节数。
HTTP URI	字符串	包含在 HTTP 连接中找到的通用资源指示器。
字符串块类型 (String Block Type)	uint32	启动包含 SMTP 附件名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 SMTP 附件 (SMTP Attachments) 字段中的字节数。
SMTP 附件 (SMTP Attachments)	字符串	包含提取自“MIME 内容性质”报头的 MIME 附件文件名。要填充此字段，必须启用 SMTP 预处理器记录 MIME 附件名称 (Log MIME Attachment Names) 选项。支持多个附件文件名。
字符串块类型 (String Block Type)	uint32	启动包含 SMTP 发件人地址的字符串数据块。此值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 SMTP 发件人 (SMTP From) 字段中的字节数。
SMTP 发件人 (SMTP From)	string	包含提取自 SMTP MAIL FROM 命令的邮件发件人的地址。要填充此字段，必须启用 SMTP 预处理器记录发件人地址 (Log From Address) 选项。支持多个发件人地址。
字符串块类型 (String Block Type)	uint32	启动包含 SMTP 报头的字符串数据块。值始终为 0。

表 3-4　　入侵事件记录 7.1+ 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 SMTP 报头 (SMTP Headers) 字段中的字节数。
SMTP 报头 (SMTP Headers)	string	包含提取自邮件报头的数据。 要将邮件报头与 SMTP 流量的入侵事件相关联，必须启用 SMTP 预处理器的记录报头 (Log Headers) 选项。
字符串块类型 (String Block Type)	uint32	启动包含 SMTP 收件人地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 SMTP 收件人 (SMTP To) 字段中的字节数。
SMTP 收件人 (SMTP To)	string	包含提取自 SMTP RCPT TO 命令的邮件收件人的地址。要填充此字段，必须启用 SMTP 预处理器记录收件人地址 (Log To Addresses) 选项。支持多个收件人地址。

入侵影响警报数据 5.3+

入侵影响警报 5.3+ 事件包含影响事件的相关信息。当将入侵事件与系统网络映射数据进行比较且影响已确定时，系统传输入侵影响警报数据。它使用记录类型为 9 的标准记录报头，接着是系列 1 数据块类型为系列 1 数据块组中的 153 的入侵影响警报数据块。（影响警报数据块是系列 1 类型的数据块。有关系列 1 数据块的详细信息，请参阅了解发现（系列 1）块，第 4-60 页。）

您可以通过在请求消息的标志字段中设置位 5 来请求 eStreamer 只传输入侵影响事件。有关请求消息的详细信息，请参阅事件流请求消息格式，第 2-11 页。这些警报的版本 1 只处理 IPv4。5.3 中引入的版本 2 除了处理 IPv4 之外，还处理 IPv6 事件。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (9) (Record Type (9))															
eStreamer 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
入侵影响警报块类型 (153)（Intrusion Impact Alert Block Type (153)）																																
入侵影响警报块长度 (Intrusion Impact Alert Block Length)																																
事件 ID (Event ID)																																
设备 ID (设备 ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	事件秒 (Event Second)																															
	影响 (Impact)																															
	源 IP 地址 (Source IP Address)																															
	源 IP 地址 (Source IP Address)（续）																															
	源 IP 地址 (Source IP Address)（续）																															
	源 IP 地址 (Source IP Address)（续）																															
	目标 IP 地址 (Destination IP Address)																															
	目标 IP 地址 (Destination IP Address)（续）																															
	目标 IP 地址 (Destination IP Address)（续）																															
	目标 IP 地址 (Destination IP Address)（续）																															
影响 (Impact) 说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明... (Description...)																															

下表对影响事件中的每个数据字段进行了说明。

表 3-5　　影响事件数据字段

字段	数据类型	说明 (Description)
入侵影响警报块类型 (Intrusion Impact Alert Block Type)	uint32	表示后面是入侵影响警报数据块。此字段的值始终为 153。请参阅入侵事件和元数据记录类型，第 3-1 页。
入侵影响警报块长度 (Intrusion Impact Alert Block Length)	uint32	表示入侵影响警报数据块的长度，包括后面的所有数据以及入侵影响警报块类型和长度的 8 个字节。
事件 ID (Event ID)	uint32	表示事件标识号。
设备 ID	uint32	表示受管设备标识号。
事件秒 (Event Second)	uint32	表示检测到事件的秒数（从 1970/01/01 起）。
影响 (Impact)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到管理中心上的特定优先级中。x 表示值可以为 0 或 1: ▪ 灰色（0，未知）：00X00000 ▪ 红色（1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）：00X0011X ▪ 黄色（3，当前不易受攻击）：00X0001X ▪ 蓝色（4，未知目标）：00X00001
源 IP 地址 (Source IP Address)	uint8[16]	与影响事件相关的主机的 IP 地址。可能包含 IPv4 地址或 IPv6 地址。有关详细信息，请参阅IP 地址，第 1-4 页。

表 3-5 影响事件数据字段 （续）

字段	数据类型	说明 (Description)
目标 IP 地址 (Destination IP Address)	uint8[16]	与影响事件相关的目标 IP 地址的 IP 地址（如适用）。可能包含 IPv4 地址或 IPv6 地址。有关详细信息，请参阅IP 地址，第 1-4 页。如果无目标 IP 地址，则此值为 0。
字符串块类型 (String Block Type)	uint32	启动包含影响名称的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-67 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数。这包括字符串块类型的四个字节，字符串块长度的四个字节以及说明中的字节数。
说明 (Description)	字符串	影响事件的说明。

用户记录

请求元数据时，您可以检索有关 Cisco Secure Firewall 系统中的组件生成的事件中引用的用户的信息。eStreamer 服务可传输包含用户记录中的事件的用户信息的元数据，格式如下所示。用户记录包含用户 ID 和相应的名称。用户元数据记录可用于通过将元数据与用户 ID 值相关联的方法来确定与事件相关联的用户名。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送用户信息。请参阅请求标志，第 2-12 页。）

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (62) (Record Type (62))															
记录长度 (Record Length)																																
用户 ID																																
名称长度 (Name Length)																																
名称...(Name...)																																

下表对用户记录中的字段进行了说明。

表 3-6　　用户记录字段

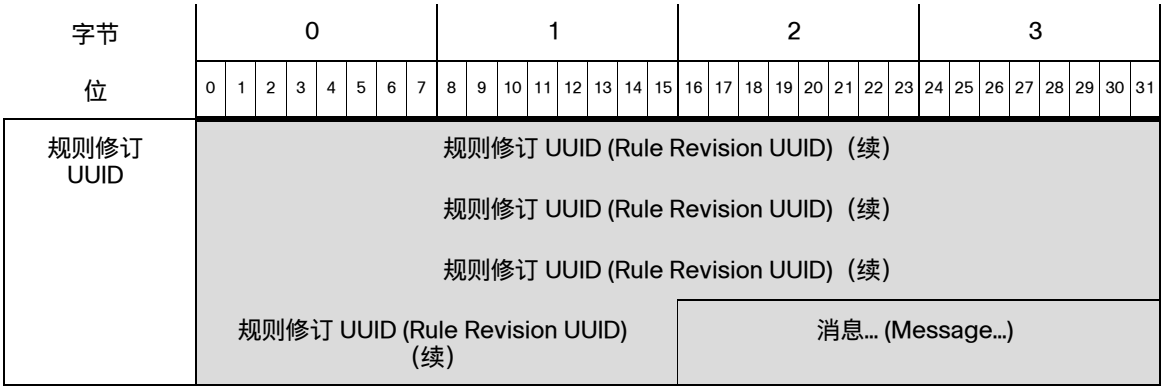
字段	数据类型	说明 (Description)
用户 ID (User ID)	uint32	用户 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	用户名称中包含的字节数。
名称 (Name)	字符串	用户的名称。

用于 4.6.1+ 的规则消息记录

系统通过规则消息记录传输事件的规则消息信息，格式如下所示。当您请求版本 2 或版本 3 元数据时，eStreamer 服务传输用于 4.6.1+ 的规则消息记录。用于 4.6.1+ 的规则消息记录包含用于 4.6 及更低版本的规则消息记录中包含的字段，但也具有新 UUID 和修订 UUID 字段。（当设置对应的元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 14（版本 2）、位 15（版本 3）或位 20（版本 4））时，发送版本 2、版? 或版本 4 元数据信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在消息长度 (Message Length) 字段后面）的值为 66，表示规则消息版本 2 记录。

根据防火墙配置，有成千上万条规则。每个规则都可能会生成单独的记录规则消息记录。如果缓存元数据并请求此记录，请确保分配足够的内存。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															
	Netmap ID																记录类型 (66) (Record Type (66))															
	记录长度 (Record Length)																															
签名密钥	生成器 ID (Generator ID)																															
	规则 ID (Rule ID)																															
	修订号 (Revision Number)																															
	呈现的签名 ID (Rendered Signature ID)																															
	消息长度 (Message Length)																规则 UUID (Rule UUID)															
规则 UUID	规则 UUID (Rule UUID)（续）																															
	规则 UUID (Rule UUID)（续）																															
	规则 UUID (Rule UUID)（续）																															
	规则 UUID (Rule UUID)（续）																规则修订 UUID (Rule Revision UUID)															



下表对每个规则特定字段进行了说明。

表 3-7 规则消息记录字段

字段	数据类型	说明 (Description)
生成器 ID (Generator ID)	uint32	生成器标识号。
规则 ID (Rule ID)	uint32	本地计算机的规则标别号。
规则修订 (Rule Revision)	uint32	规则修订号。目前，所有规则消息的此值均设置为 0。
呈现的签名 ID (Rendered Signature ID)	uint32	Cisco Secure Firewall 系统界面呈现的规则标识号。
消息长度 (Message Length)	uint16	规则文本中包含的字节数。
UUID	uint8[16]	充当规则的唯一标识符的规则 ID 号码。
修订 UUID (Correlation Rule UUID)	uint8[16]	充当修订的唯一标识符的规则修订 ID 号码。
消息 (Message)	变量	触发事件的规则消息。

用于 4.6.1+ 的分类记录

eStreamer 服务可传输用于 4.6.1+ 的分类记录中的事件的分类信息，格式如下所示。用于 4.6.1+ 的分类记录包含用于 4.6 及更低版本的分类记录中包含的字段，但也具有新 UUID 和修订 UUID 字段。（当设置版本 3 或版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 15 或位 20）时，发送分类信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 67，表示分类版本 2 记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															
	Netmap ID																记录类型 (67) (Record Type (67))															
	记录长度 (Record Length)																															
	分类 ID (Classification ID)																															
	名称长度 (Name Length)																名称...(Name...)															
	名称 (Name)（续）...																															
	说明长度 (Description Length)																说明... (Description...)															
	说明 (Description)（续）...																															
分类 UUID (Classification UUID)	分类 UUID (Classification UUID)																															
	分类 UUID (Classification UUID)（续）																															
	分类 UUID (Classification UUID)（续）																															
	分类 UUID (Classification UUID)（续）																															
分类修订 UUID (Classification Revision UUID)	分类修订 UUID (Classification Revision UUID)																															
	分类修订 UUID (Classification Revision UUID)（续）																															
	分类修订 UUID (Classification Revision UUID)（续）																															
	分类修订 UUID (Classification Revision UUID)（续）																															

下表对分类记录中的字段进行了说明。

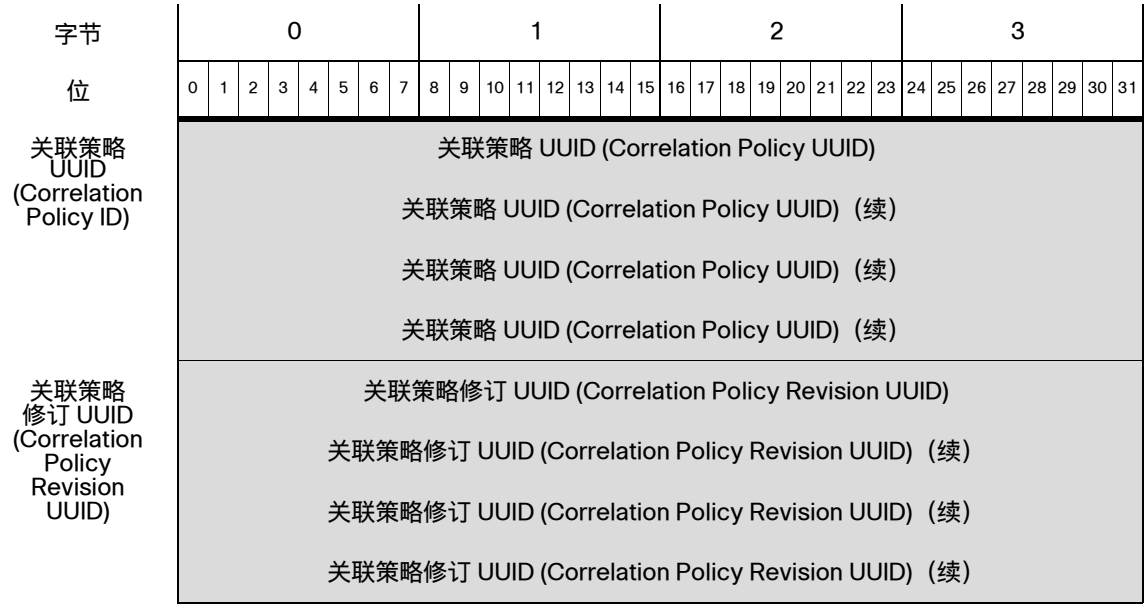
表 3-8 分类记录字段

字段	数据类型	说明 (Description)
分类 ID (Classification ID)	uint32	分类 ID 号码。
名称长度 (Name Length)	uint16	名称中包含的字节数。
名称 (Name)	字符串	分类名称。
说明长度 (Description Length)	uint16	说明中包含的字节数。
说明 (Description)	字符串	分类说明。
UUID	uint8[16]	充当分类的唯一标识符的分类 ID 号码。
修订 UUID (Correlation Rule UUID)	uint8[16]	充当分类修订的唯一标识符的分类修订 ID 号码。

关联策略记录

eStreamer 服务可传输包含关联策略记录中关联事件的关联策略的元数据，格式如下所示。（当设置版本 3 或版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 15 或位 20）时，发送关联策略信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 69，表示关联策略记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (69) (Record Type (69))															
记录长度 (Record Length)																																
关联策略 ID (Correlation Policy ID)																																
名称长度 (Name Length)																	名称...(Name...)															
说明长度 (Description Length)																	说明... (Description...)															



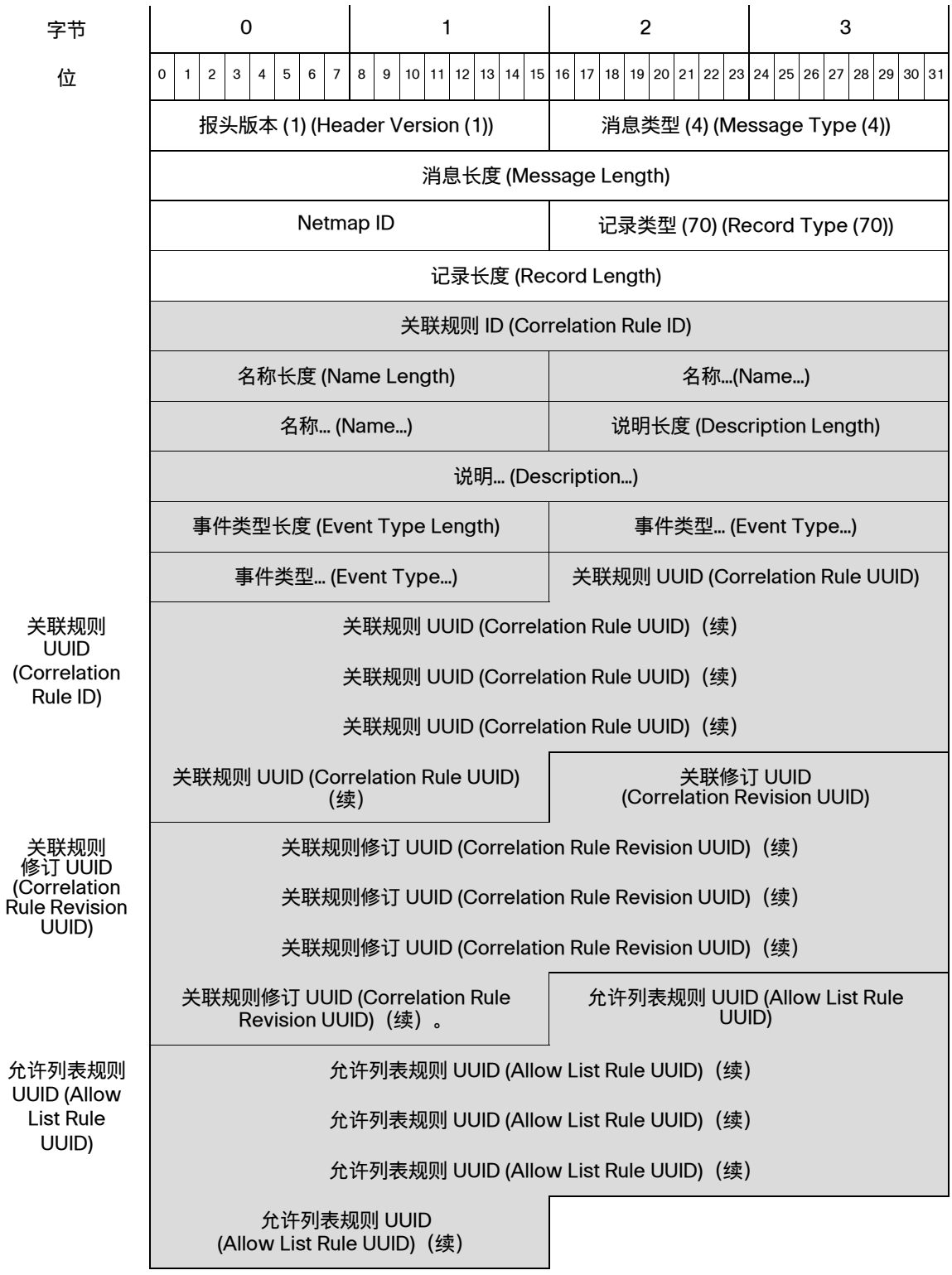
下表对关联策略记录中的字段进行了说明。

表 3-9　　关联策略记录字段

字段	数据类型	说明 (Description)
关联策略 ID	uint32	关联策略 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint16	关联策略名称中包含的字节数。
名称 (Name)	字符串	触发事件的关联策略的名称。
说明长度 (Description Length)	uint16	关联策略说明中包含的字节数。
说明 (Description)	字符串	触发事件的关联策略的说明。
UUID	uint8[16]	充当关联策略的唯一标识符的关联策略 ID 号码。
修订 UUID (Correlation Rule UUID)	uint8[16]	充当关联策略的唯一标识符的关联策略修订 ID 号码。

关联规则记录

eStreamer 服务可传输包含有关触发关联规则记录中的关联事件的关联规则的信息的元数据，格式如下所示。（当设置版本 3 或版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 15 或位 20）时，发送关联规则信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 70，表示关联规则记录。



下表对关联规则记录中的字段进行了说明。

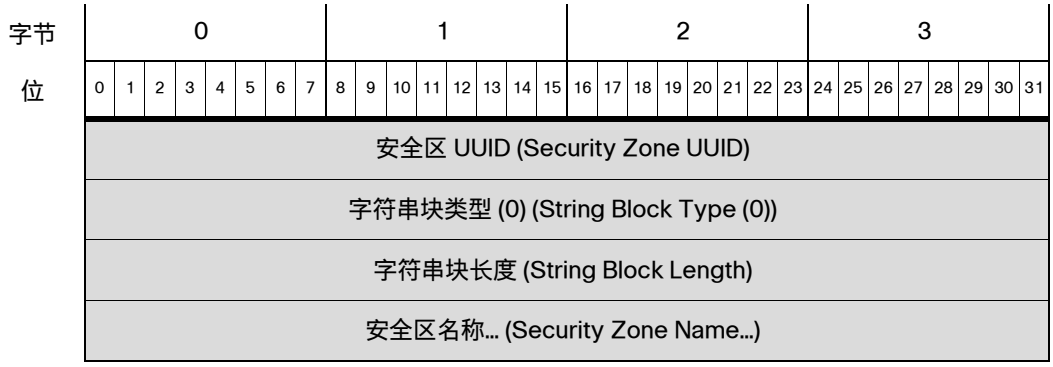
表 3-10　关联规则记录字段

字段	数据类型	说明 (Description)
关联规则 ID	uint32	关联规则 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint16	关联规则名称中包含的字节数。
名称 (Name)	字符串	触发事件的关联规则的名称。
说明长度 (Description Length)	uint16	关联规则说明中包含的字节数。
说明 (Description)	字符串	触发事件的关联规则的说明。
事件类型长度 (Event Type Length)	uint16	事件类型说明中包含的字节数。
事件类型 (Event Type)	字符串	触发关联规则的事件的说明。
UUID	uint8[16]	充当关联规则的唯一标识符的关联规则 ID 号码。
修订 UUID (Correlation Rule UUID)	uint8[16]	充当关联规则修订的唯一标识符的关联规则修订 ID 号码。
允许列表 UUID (Allow List UUID)	uint8[16]	充当作为允许列表违规结果发送的事件的唯一标识符的关联 ID 号码。

安全区名称记录

eStreamer 服务可传输包含有关与安全区名称记录中的入侵事件或连接事件关联的安全区的名称的信息的元数据，格式如下所示。（当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送安全区信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 115，表示安全区名称记录。它包含一个 UUID 字符串数据块，该数据块的块类型为系列 2 数据块组中的 14。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (115) (Record Type (115))															
记录长度 (Record Length)																																
安全区名称数据块 (14) (Security Zone Name Data Block (14))																																
安全区名称数据块长度 (Security Zone Name Data Block Length)																																



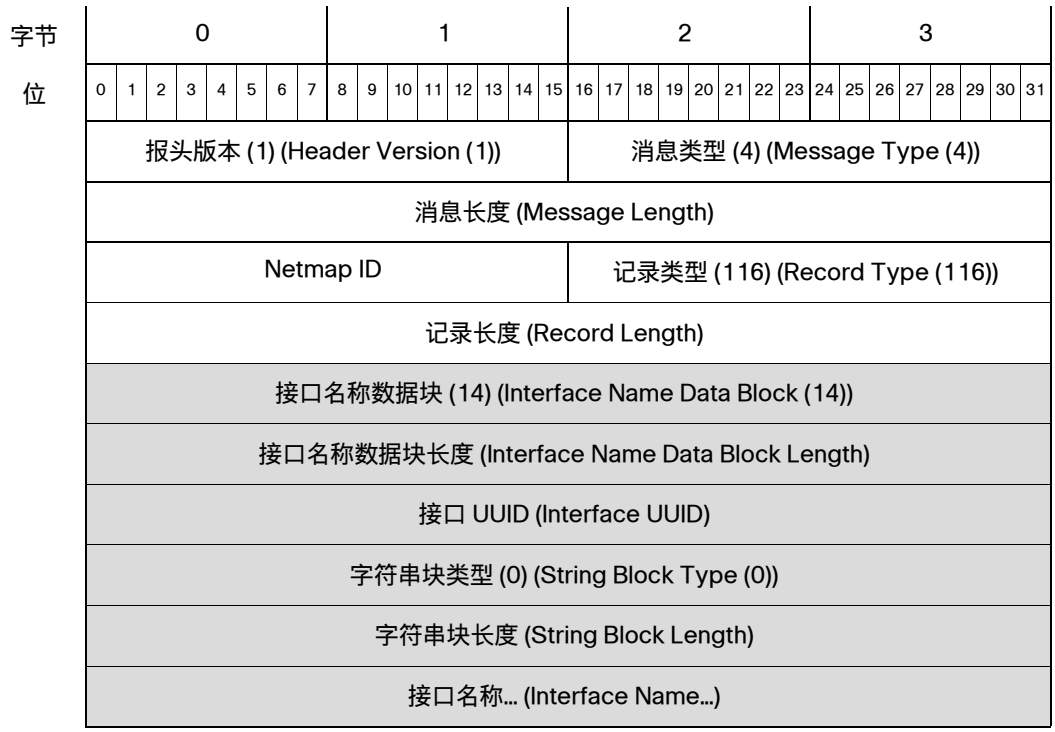
下表对安全区名称数据块中的字段进行了说明。

表 3-11 安全区名称数据块字段

字段	数据类型	说明 (Description)
安全区名称数据块类型 (Security Zone Name Data Block Type)	uint32	启动安全区名称数据块。值始终为 14。块类型为系列 2 数据块。
安全区名称数据块长度 (Security Zone Name Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的
安全区 UUID (Security Zone UUID)	uint8[16]	与连接事件相关的安全区的唯一标识符。 此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含安全区名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	安全区名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上名称中的字节数。
安全区名称 (Security Zone Name)	字符串	安全区名称。

接口名称记录

eStreamer 服务可传输包含有关与接口名称记录中的入侵事件或连接事件关联的接口的名称的信息的元数据，格式如下所示。（当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送接口名称信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 116，表示接口名称记录。它包含一个



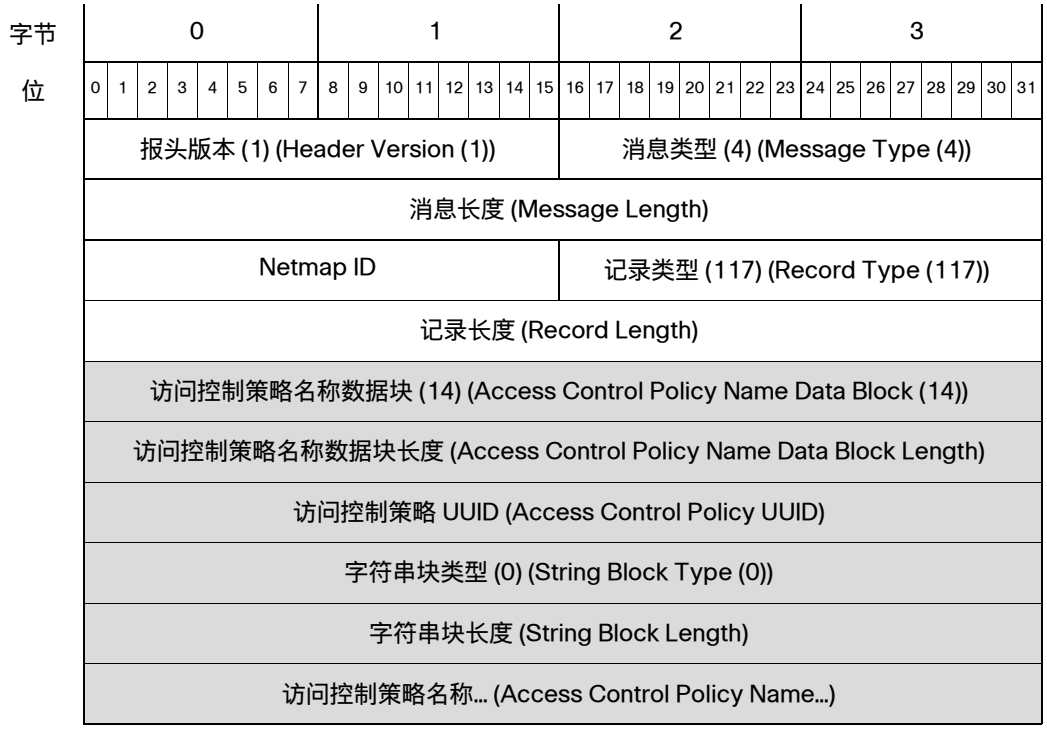
下表对接口名称数据块中的字段进行了说明。

表 3-12　　接口名称数据块字段

字段	数据类型	说明 (Description)
接口名称数据块类型 (Interface Name Data Block Type)	uint32	启动接口名称数据块。值始终为 14。块类型为系列 2 数据块。
接口名称数据块长度 (Interface Name Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的
接口 UUID (Interface UUID)	uint8[16]	充当与连接事件关联的接口的唯一标识符的接口 ID 号码。 此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含接口名字的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	接口名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上接口名称中的字节数。
接口名称 (Interface Name)	字符串	接口名称。

访问控制策略名称记录

eStreamer 服务可传输有关触发访问控制策略名称记录中的入侵事件或连接事件的访问控制策略的名称的元数据，格式如下所示。（当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送访问控制策略名称信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 117，表示访问控制策略名称记录。它包含一个



下表对访问控制策略名称数据块中的字段进行了说明。

表 3-13 访问控制策略名称数据块字段

字段	数据类型	说明 (Description)
访问控制策略名称数据块类型 (Access Control Policy Name Data Block Type)	uint32	启动访问控制策略名称数据块。值始终为 14。块类型为系列 2 数据块。
访问控制策略名称数据块长度 (Access Control Policy Name Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当与入侵事件或连接事件关联的访问控制策略的唯一标识符的 ID 号码。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含访问控制策略的名称的字符串数据块。值始终为 0。

表 3-13　访问控制策略名称数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	访问控制策略名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上访问控制策略名称中的字节数。
访问控制策略名称 (Access Control Policy Name)	字符串	访问控制策略名称。

访问控制规则 ID 记录元数据

eStreamer 服务可传输包含有关触发访问控制规则 ID 记录中的入侵事件或连接事件的访问控制规则的信息的元数据，格式如下所示。当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送访问控制规则元数据。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 119，表示访问控制规则 ID 记录。它包含一个规则 ID 数据块，该数据块的块类型为系列 2 数据块组中的 15。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															
	Netmap ID																记录类型 (119) (Record Type (119))															
	记录长度 (Record Length)																															
	访问控制规则 ID 数据块 (15) (Access Control Rule ID Data Block (15))																															
	访问控制规则 ID 数据块长度 (Access Control Rule ID Data Block Length)																															
AC 规则 UUID	访问规则策略 UUID (Access Rule Policy UUID)																															
	访问控制规则 UUID (Access Control Rule UUID)（续）																															
	访问控制规则 UUID (Access Control Rule UUID)（续）																															
	访问控制规则 UUID (Access Control Rule UUID)（续）																															
	访问控制规则 ID (Access Control Rule ID)																															
	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	访问控制规则名称... (Access Control Rule Name...)																															

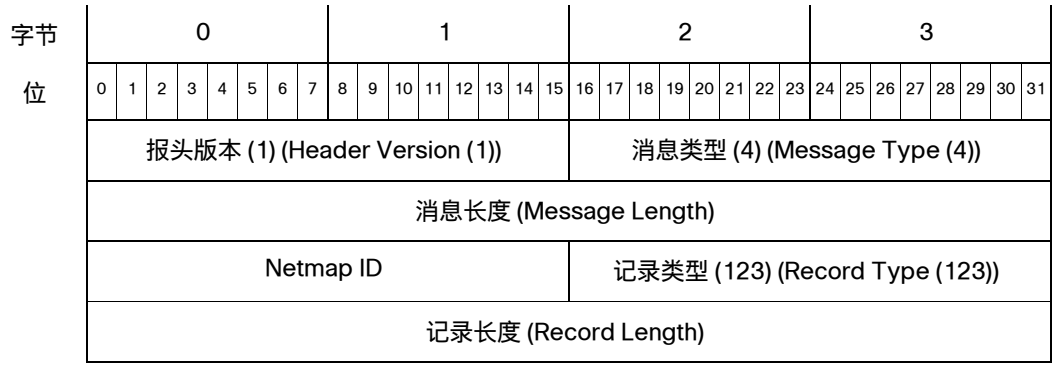
下表对访问控制规则 ID 数据块中的字段进行了说明。

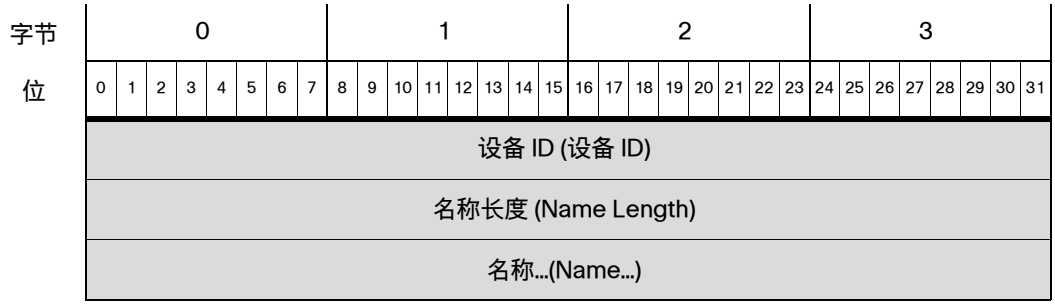
表 3-14 访问控制规则 ID 数据块字段

字段	数据类型	说明 (Description)
访问控制规则 ID 数据块类型 (Access Control Rule ID Data Block Type)	uint32	启动访问控制规则 ID 数据块。值始终为 15。块类型为系列 2 数据块。
访问控制规则 ID 数据块长度 (Access Control Rule ID Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的
访问控制规则 UUID (Access Control Rule UUID)	uint8[16]	访问控制规则的 UUID。此字段与访问控制规则 ID 一起是此记录的唯一密钥。
访问控制规则 ID (Access Control Rule ID)	uint32	充当与连接事件相关的访问控制策略中的规则的内部标识符。此字段与访问控制规则UUID一起是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含访问控制规则的名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上规则名称中的字节数。
访问控制规则名称 (Access Control Rule Name)	字符串	访问控制规则名称。

受管设备记录元数据

eStreamer 服务可传输包含有关与受管设备记录中的入侵事件相关的受管设备的信息的元数据，格式如下所示。当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送受管设备元数据。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 123，表示受管设备记录。





下表对受管设备记录中的字段进行了说明。

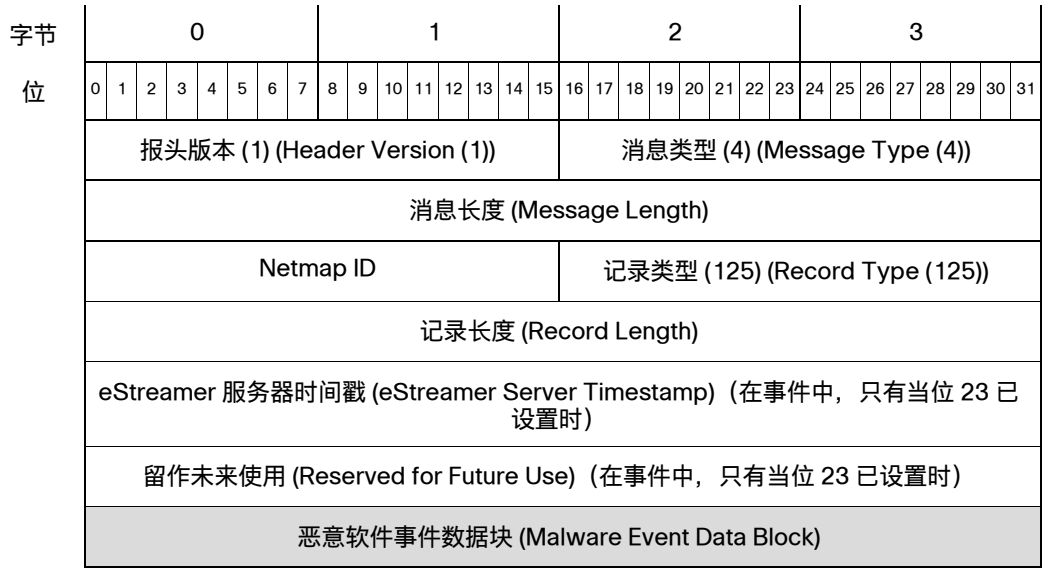
表 3-15　　受管设备记录字段

字段	数据类型	说明
设备 ID	uint32	受管设备的ID号码。此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	名称中包含的字节数。
名称 (Name)	字符串	受管设备名称。

恶意软件事件记录 5.1.1+

下图中的阴影部分表示恶意软件事件记录中的字段。记录类型为 125。

您可以通过在事件版本为 2 且事件代码为 101 的请求消息中设置恶意软件事件标志（“请求标志”(Request Flags) 字段中的位 30）请求恶意软件事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。它包含一个恶意软件事件数据块，该数据块的块类型为 24、33、35、44、47 或在系列 2 数据块组中。



下表对每个恶意软件事件记录数据字段进行了说明。

表 3-16 恶意软件事件记录字段

字段	数据类型	说明 (Description)
恶意软件事件数据块 (Malware Event Data Block)	变量	表示恶意软件事件数据块。有关详细信息，请参阅恶意软件事件数据块 7.0+，第 3-92 页。

思科高级恶意软件防护云名称元数据

eStreamer 服务可传输包含有关与思科高级恶意软件防护云名称记录中的入侵事件或连接事件相关的思科高级恶意软件防护云（简称 AMP 云或云）的名称的信息的元数据，格式如下所示。（当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送 AMP 云名称信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在消息长度 (Message Length) 字段后面）的值为 `127`，表示思科高级恶意软件防护云名称记录。它包含一个

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (127) (Record Type (127))															
记录长度 (Record Length)																																
思科高级恶意软件防护云名称数据块 (14) (思科高级恶意软件防护云 Name Data Block (14))																																
思科高级恶意软件防护云名称数据块长度 (思科高级恶意软件防护云 Name Data Block Length)																																
思科高级恶意软件防护云 UUID (思科高级恶意软件防护云 UUID) 思科高级恶意软件防护云 UUID (思科高级恶意软件防护云 UUID)（续） 思科高级恶意软件防护云 UUID (思科高级恶意软件防护云 UUID)（续） 思科高级恶意软件防护云 UUID (思科高级恶意软件防护云 UUID)（续）																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
思科高级恶意软件防护云 名称...(Name...)																																

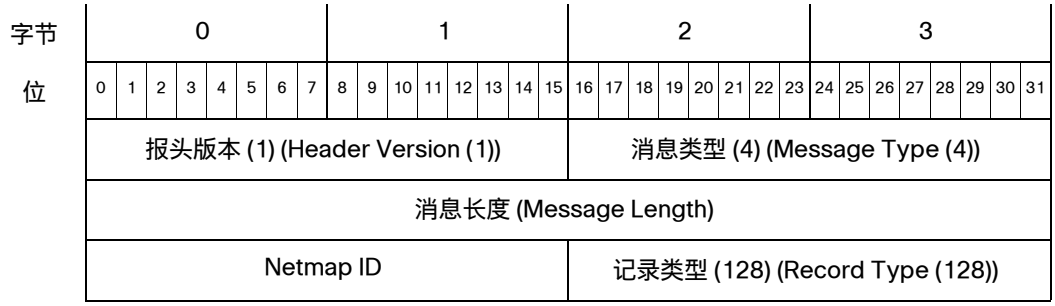
下表对思科高级恶意软件防护云名称数据块中的字段进行了说明。

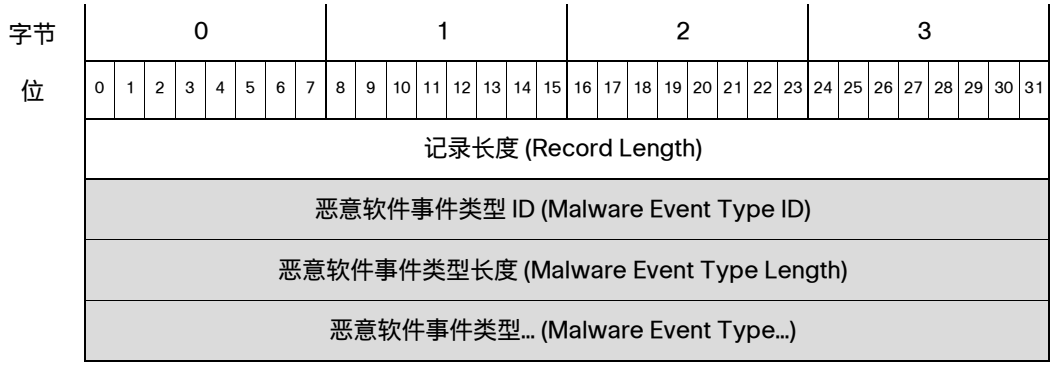
表 3-17　　思科高级恶意软件防护云名称数据块字段

字段	数据类型	说明 (Description)
思科高级恶意软件防护云名称数据块类型 (思科高级恶意软件防护云 Name Data Block Type)	uint32	启动思科高级恶意软件防护云名称数据块。值始终为 14。块类型为系列 2 数据块。
思科高级恶意软件防护云名称数据块长度 (思科高级恶意软件防护云 Name Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的
思科高级恶意软件防护云 UUID (思科高级恶意软件防护云 UUID)	uint8[16]	充当与连接事件关联的思科高级恶意软件防护云的唯一标识符的思科高级恶意软件防护云ID号码。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含思科高级恶意软件防护云名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	思科高级恶意软件防护云名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上思科高级恶意软件防护云名称中的字节数。
思科高级恶意软件防护云名称 (思科高级恶意软件防护云 Name)	字符串	思科高级恶意软件防护云 名称。

恶意软件事件类型元数据

eStreamer 服务可传输包含恶意软件事件类型记录中的事件的恶意软件事件类型信息的元数据，格式如下所示。（当设置元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 128，表示恶意软件事件类型记录。





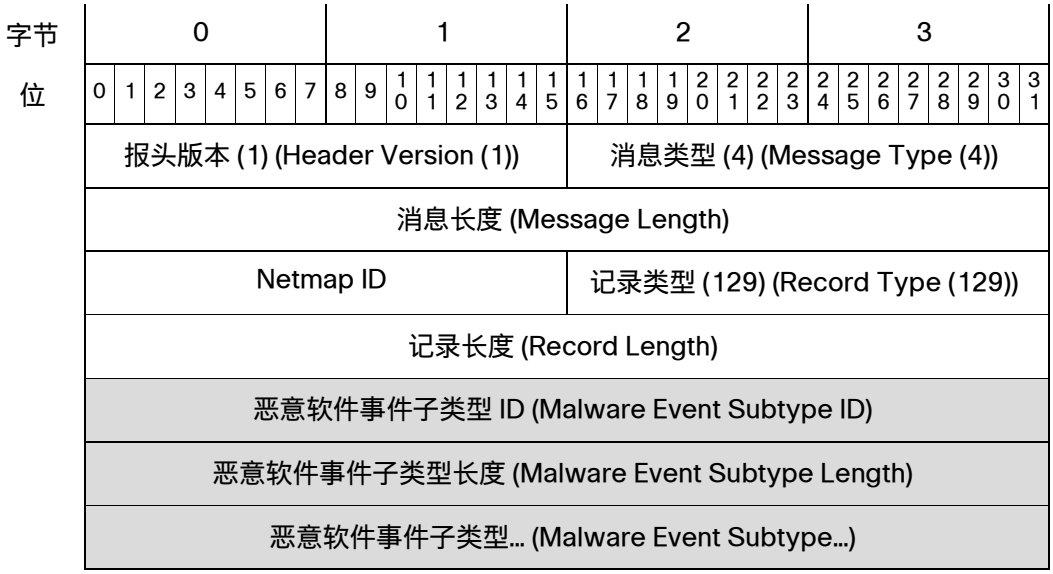
下表对恶意软件事件类型记录中的字段进行了说明。

表 3-18 恶意软件事件类型记录字段

字段	数据类型	说明 (Description)
恶意软件事件类型 ID (Malware Event Type ID)	uint32	恶意软件事件类型ID号码。此字段是此记录的唯一密钥。
恶意软件事件类型长度 (Malware Event Type Length)	uint32	恶意软件事件类型中包含的字节数。
恶意软件事件类型 (Malware Event Type)	字符串	恶意软件事件类型。

恶意软件事件子类型元数据

eStreamer 服务可传输包含恶意软件事件子类型记录中的事件的恶意软件事件子类型信息的元数据，格式如下所示。（当设置元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在消息长度 (Message Length) 字段后面）的值为 `129`，表示恶意软件事件子类型记录。



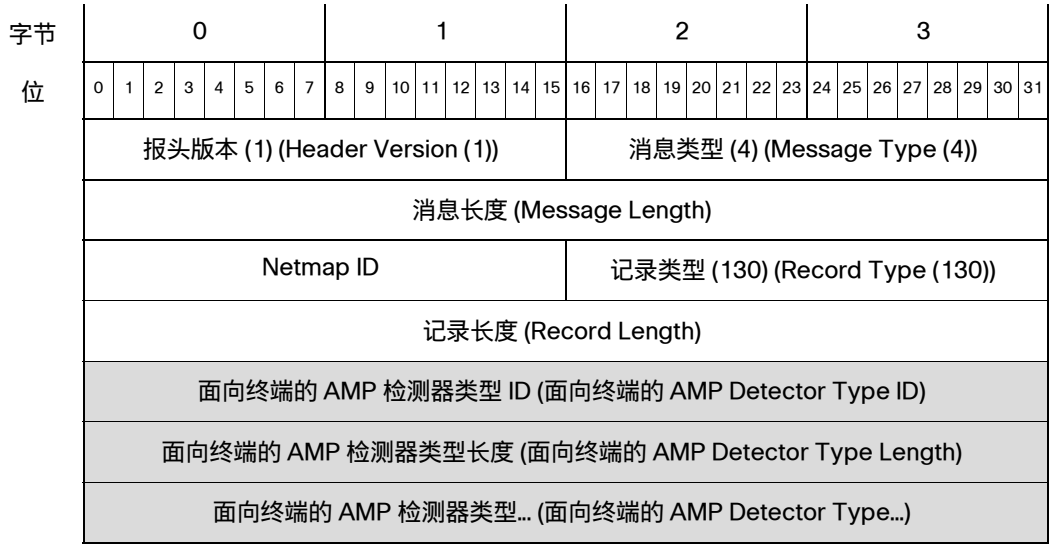
下表对恶意软件事件子类型记录中的字段进行了说明。

表 3-19　　恶意软件事件子类型记录字段

字段	数据类型	说明 (Description)
恶意软件事件子类型 ID (Malware Event Subtype ID)	uint32	恶意软件事件子类型 ID 号码。 此字段是此记录的唯一密钥。
恶意软件事件子类型长度 (Malware Event Subtype Length)	uint32	恶意软件事件子类型中包含的字节数。
恶意软件事件子类型 (Malware Event Subtype)	字符串	恶意软件事件子类型。

面向终端的 AMP 检测器类型元数据

eStreamer 服务可传输包含面向终端的 AMP 检测器类型记录中的事件的面向终端的 AMP 检测器类型信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送面向终端的 AMP 检测器类型信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在消息长度 (Message Length) 字段后面）的值为 130，表示面向终端的 AMP 检测器类型记录。



下表对面向终端的 AMP 检测器类型记录中的字段进行了说明。

表 3-20　　面向终端的 AMP 检测器类型记录字段

字段	数据类型	说明 (Description)
面向终端的 AMP 检测器类型 ID (面向终端的 AMP Detector Type ID)	uint32	面向终端的 AMP 检测器类型 ID 号码。 此字段是此记录的唯一密钥。

表 3-20 面向终端的 AMP 检测器类型记录字段 （续）

字段	数据类型	说明 (Description)
面向终端的 AMP 检测器类型长度 (面向终端的 AMP Detector Type Length)	uint32	面向终端的 AMP 检测器类型中包含的字节数。
面向终端的 AMP 检测器类型 (面向终端的 AMP Detector Type)	字符串	面向终端的 AMP 检测器的类型。

面向终端的 AMP 文件类型元数据

eStreamer 服务可传输包含面向终端的 AMP 文件类型记录中的事件的面向终端的 AMP 文件类型信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送面向终端的 AMP 文件类型信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在消息长度 (Message Length) 字段后面）的值为 131，表示面向终端的 AMP 文件类型记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (131) (Record Type (131))															
记录长度 (Record Length)																																
面向终端的 AMP 文件类型 ID (面向终端的 AMP File Type ID)																																
面向终端的 AMP 文件类型长度 (面向终端的 AMP File Type Length)																																
面向终端的 AMP 文件类型... (面向终端的 AMP File Type...)																																

下表对面向终端的 AMP 文件类型记录中的字段进行了说明。

表 3-21　面向终端的 AMP 文件类型记录字段

字段	数据类型	说明 (Description)
面向终端的 AMP 文件类型 ID (面向终端的 AMP File Type ID)	uint32	面向终端的 AMP 文件类型 ID 号码。 此字段是此记录的唯一密钥。
面向终端的 AMP 文件类型长度 (面向终端的 AMP File Type Length)	uint32	面向终端的 AMP 文件类型中包含的字节数。
面向终端的 AMP 文件类型 (面向终端的 AMP File Type)	字符串	被检测文件的类型。

安全情景名称

eStreamer 服务可传输包含安全情景名称信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送安全情景名称信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在消息长度 (Message Length) 字段后面）的值为 132，表示安全情景名称记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (132) (Record Type (132))															
记录长度 (Record Length)																																
安全情景 UUID (Security Context UUID) 安全情景 UUID (Security Context UUID)（续） 安全情景 UUID (Security Context UUID)（续） 安全情景 UUID (Security Context UUID)（续）																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
安全情景名称... (Security Context Name...)																																

下表对安全情景名称记录中的字段进行了说明。

表 3-22 安全情景名称记录字段

字段	数据类型	说明 (Description)
安全情景 UUID (Security Context UUID)	uint8[16]	安全情景的 UUID。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含安全情景名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	安全情景名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“安全情景名称”(Security Context Name) 中的字节数。
安全情景名称 (Security Context Name)	字符串	安全情景名称。

用于 5.4+ 的关联事件

关联事件（在 5.0 之前的版本中称为合规性事件）包含关联策略违规的相关信息。此消息使用标准 eStreamer 消息报头并指定记录类型为 112，随后是类型为系列 1 数据块组中的 156 的关联数据块。数据块类型 156 与其前身（块类型 128）的区别在于其包含 IPv6 支持。

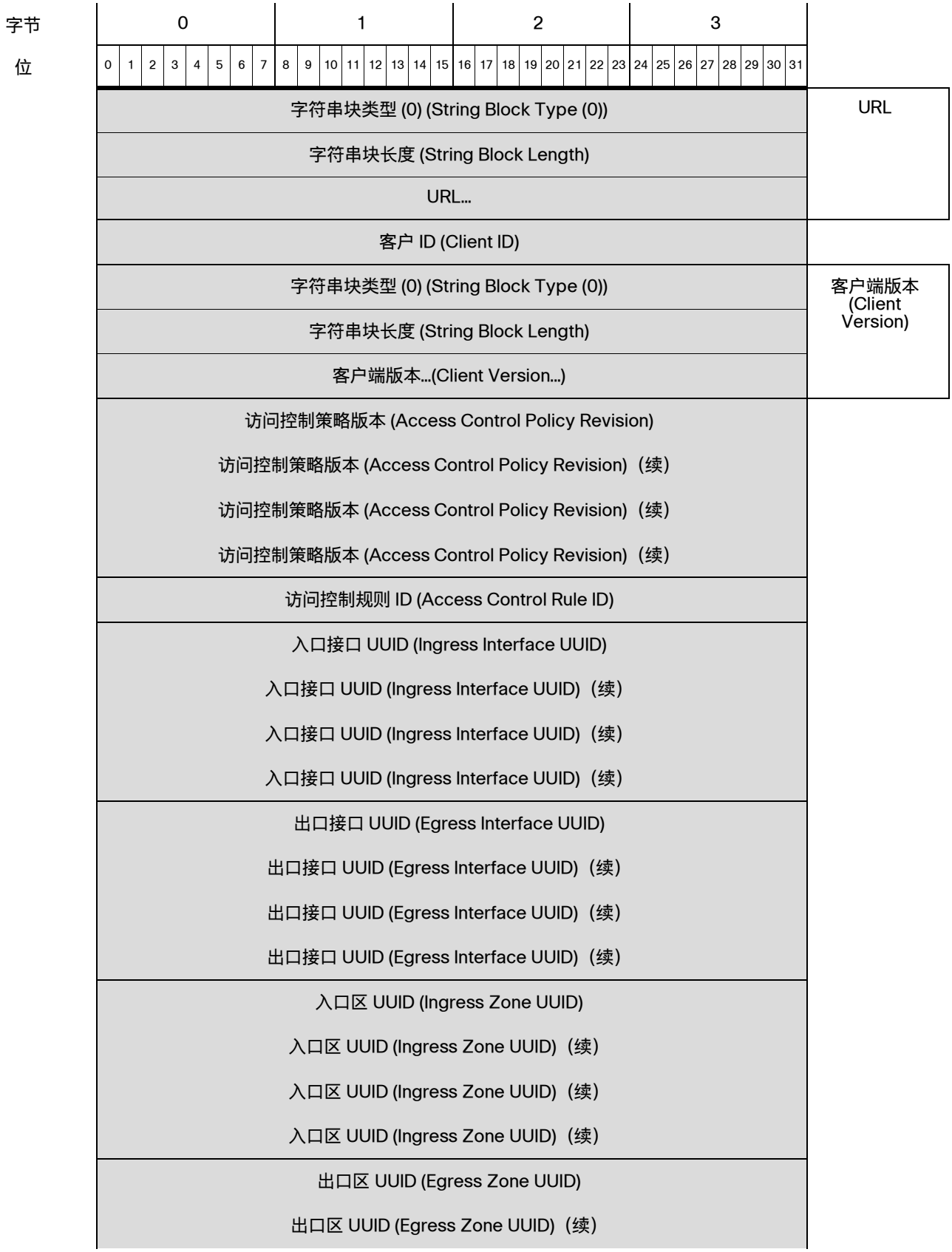
关联事件的 5.4+ 版本具有地理位置、安全情报以及 SSL 支持等新字段。

只需通过扩展请求，即可从 eStreamer 请求 5.4+ 关联事件，对于提交扩展请求，您需要在流请求消息中请求事件类型代码 31 和版本代码 9（请参阅 提交扩展请求，第 2-4 页 了解有关提交扩展请求的信息）。您可以选择启用初始事件流请求消息的标志字段中的位 23，以包含扩展事件报头。您也可以启用标志字段中的位 20，以包含用户元数据。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (112)（Record Type (112)）															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
关联块类型 (156) (Correlation Block Type (156))																																
关联块长度 (Correlation Block Length)																																
设备 ID (Device ID)																																


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
（关联）事件秒 ((Correlation) Event Second)
事件 ID (Event ID)
策略 ID (Policy ID)
规则 ID (Rule ID)
优先级 (Priority)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
说明... (Description...)
事件类型 (Event Type)
事件说明 (Event Description)
事件设备 ID (Event Device ID)
签名 ID (Signature ID)
签名生成器 ID (Signature Generator ID)
（触发器）事件秒 ((Trigger) Event Second)
（触发器）事件微秒 ((Trigger) Event Microsecond)
事件 ID (Event ID)
事件定义的掩码 (Event Defined Mask)
事件影响标志 (Event Impact Flags)
IP 协议 (IP Protocol)
网络协议 (Network Protocol)
源 IP (Source IP)
源主机类型 (Source Host Type)
源 VLAN ID (Source VLAN ID)
源操作系统指纹 UUID (Source OS Fprt UUID)
源操作系统指纹 UUID (Source OS Fprt UUID)
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源重要性 (Source Criticality)
源临界点 (Source Criticality)（续）
源用户 ID (Source User ID)


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
源用户 ID (Source User ID)（续）
源端口 (Source Port)
源服务器 ID (Source Server ID)
源服务器 ID (Source Server ID)（续）
目标 IP (Destination IP)
目标 IP (Destination IP)（续）
目标主机类型 (Host Type)
目标VLAN ID
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)
目标操作系统指纹 UUID (Dest OS Fingerprint UUID)
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标重要性 (Destination Criticality)
目标用户 ID
目标端口 (Destination Port)
目标服务器 ID (Destination Server ID)
目标服务器 ID (Destination Server ID)（续）
影响 (Impact)
已阻止 (Blocked)
入侵策略 (Intrusion Policy)
入侵策略 (Intrusion Policy)（续）
入侵策略 (Intrusion Policy)（续）
入侵策略 (Intrusion Policy)（续）
规则操作 (Rule Action)
字符串块类型 (0) (String Block Type (0))
NetBIOS 域 (NetBIOS Domain)
字符串块长度 (String Block Length)
NetBIOS 域...(NetBIOS Domain...)
URL 类别 (URL Category)
URL 信誉 (URL Reputation)


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
URL...
URL
客户 ID (Client ID)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
客户端版本...(Client Version...)
客户端版本 (Client Version)
访问控制策略版本 (Access Control Policy Revision)
访问控制策略版本 (Access Control Policy Revision)（续）
访问控制策略版本 (Access Control Policy Revision)（续）
访问控制策略版本 (Access Control Policy Revision)（续）
访问控制规则 ID (Access Control Rule ID)
入口接口 UUID (Ingress Interface UUID)
入口接口 UUID (Ingress Interface UUID)（续）
入口接口 UUID (Ingress Interface UUID)（续）
入口接口 UUID (Ingress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)
出口接口 UUID (Egress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)（续）
入口区 UUID (Ingress Zone UUID)
入口区 UUID (Ingress Zone UUID)（续）
入口区 UUID (Ingress Zone UUID)（续）
入口区 UUID (Ingress Zone UUID)（续）
出口区 UUID (Egress Zone UUID)
出口区 UUID (Egress Zone UUID)（续）

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出口区 UUID (Egress Zone UUID)（续）																																
出口区 UUID (Egress Zone UUID)（续）																																
源 IPv6 地址 (Source IPv6 Address)																																
源 IPv6 地址 (Source IPv6 Address)（续）																																
源 IPv6 地址 (Source IPv6 Address)（续）																																
源 IPv6 地址 (Source IPv6 Address)（续）																																
目的 IPv6 地址 (Destination IPv6 Address)																																
目标 IPv6 地址 (Destination IPv6 Address)（续）																																
目标 IPv6 地址 (Destination IPv6 Address)（续）																																
目标 IPv6 地址 (Destination IPv6 Address)（续）																																
源国家/地区 (Source Country)																	目标国家/地区 (Destination Country)														
安全情报 UUID (Security Intelligence UUID)																																
安全情报 UUID (Security Intelligence UUID)（续）																																
安全情报 UUID (Security Intelligence UUID)（续）																																
安全情报 UUID (Security Intelligence UUID)（续）																																
安全情景 (Security Context)																																
安全情景 (Security Context)（续）																																
安全情景 (Security Context)（续）																																
安全情景 (Security Context)（续）																																
SSL 策略 ID (SSL Policy ID)																																
SSL 策略 ID (SSL Policy ID)（续）																																
SSL 策略 ID (SSL Policy ID)（续）																																
SSL 策略 ID (SSL Policy ID)（续）																																
SSL 规则 ID (SSL Rule ID)（续）																																
SSL 实际操作 (SSL Actual Action)																																
SSL 流状态 (SSL Flow Status)																																

请注意，记录结构包含一个字符串块类型，该数据块为系列 1 中的数据块。有关系列 1 数据块的信息，请参阅了解发现（系列 1）块，第 4-60 页。

表 3-23　　关联事件 5.4+ 数据字段

字段	数据类型	说明 (Description)
关联块类型 (Correlation Block Type)	uint32	表示随后的关联事件数据块。此字段的值始终为 156。请参阅了解发现（系列 1）块，第 4-60 页。
关联块长度 (Correlation Block Length)	uint32	关联数据块的长度，包括关联块类型和长度的 8 个字节加上随后的关联数据。
设备 ID (Device ID)	uint32	生成关联事件的受管设备或管理中心的内部标识号。值 0 表示管理中心。您可以通过请求版本 3 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
（关联）事件秒 ((Correlation) Event Second)	uint32	表示生成关联事件的时间的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
事件 ID (Event ID)	uint32	关联事件标识号。
策略 ID (Policy ID)	uint32	违反的关联策略的标识号。有关如何从数据库获取策略标识号的信息，请参阅服务记录，第 4-14 页。
规则 ID (Rule ID)	uint32	触发策略违规事件的关联规则的标识号。有关如何从数据库获取策略标识号的信息，请参阅服务记录，第 4-14 页。
优先级 (Priority)	uint32	分配给事件的优先级。该项是从 0 到 5 的整数值。
字符串块类型 (String Block Type)	uint32	启动包含关联违规事件说明的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-67 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数，包括字符串块类型的四个字节，字符串块长度的四个字节加上说明中的字节数。
说明 (Description)	字符串	关联事件的说明。

表 3-23 关联事件 5.4+ 数据字段 （续）

字段	数据类型	说明 (Description)
事件类型 (Event Type)	uint8	表示关联事件是由入侵事件、主机发现事件还是用户事件触发的: ▪ 1 - 入侵 ▪ 2 - 主机发现 ▪ 3 - 用户
事件设备 ID (Event Device ID)	uint32	生成触发关联事件的事件的设备的标识号。您可以通过请求版本 3 元数据获取设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
签名 ID (Signature ID)	uint32	如果事件为入侵事件，则表示与事件对应的规则识别号。否则，该值为 0。
签名生成器 ID (Signature Generator ID)	uint32	如果事件为入侵事件，则表示生成事件的 Cisco Secure Firewall 系统预处理器或规则引擎的 ID 号码。
（触发器）事件秒 ((Trigger) Event Second)	uint32	表示事件触发关联策略规则的时间的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
（触发器）事件微秒 ((Trigger) Event Microsecond)	uint32	检测到事件的微秒（一秒的百万分之一）增量。
事件 ID (Event ID)	uint32	思科设备生成的事件的标识号。
事件定义的掩码 (Event Defined Mask)	bits[32]	此字段中的设置位表示后面消息中哪些是有效的字段。有关每个位值的列表，请参阅表 3-21，第 3-41 页。

表 3-23　关联事件 5.4+ 数据字段 （续）

字段	数据类型	说明 (Description)
事件影响标志	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到管理中心上的特定优先级中。x 表示值可以为 0 或 1: ▪ 灰色（0，未知）：`00X00000` ▪ 红色（1，易受攻击）：`XXXX1XXX`、`XXX1XXXX`、`X1XXXXXX`、`1XXXXXXX` （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）：`00X0011X` ▪ 黄色（3，当前不易受攻击）：`00X0001X` ▪ 蓝色（4，未知目标）：`00X00001`
IP 协议 (IP Protocol)	uint8	与事件关联的
网络协议 (Network Protocol)	uint16	与事件关联的网络协议（如适用）。
源 IP 地址 (Source IP Address)	uint8[4]	保留此字段，但不再填充。源 IPv4 地址存储在源 IPv6 地址字段中。有关详细信息，请参阅IP 地址，第 1-4 页。
源主机类型	uint8	源主机的类型: ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥
源 VLAN ID	uint16	源主机的 VLAN 标识号（如适用）。
源操作系统指纹 UUID (Source OS Fingerprint UUID)	uint8[16]	充当源主机操作系统的唯一标识符的指纹 ID 号码。 有关获取映射到指纹 ID 的值的信息，请参阅服务记录，第 4-14 页。

表 3-23 关联事件 5.4+ 数据字段 （续）

字段	数据类型	说明 (Description)
源重要性 (Source Criticality)	uint16	源主机的用户定义临界值: ▪ 0 - 无 ▪ 1 - 低 ▪ 2 - 中 ▪ 3 - 高
源用户 ID (Source User ID)	uint32	系统识别的登录源主机的用户的标识号。
源端口 (Source Port)	uint16	事件中的源端口。
源服务器 ID (Source Server ID)	uint32	源主机上运行的服务器的标识号。
目标 IP 地址 (Destination IP Address)	uint8[4]	保留此字段，但不再填充。目标 IPv4 地址存储在目标 IPv6 地址字段中。有关详细信息，请参阅IP 地址，第 1-4 页。
目标主机类型 (Destination Host Type)	uint8	目标主机的类型: ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥
目标 VLAN ID (Destination VLAN ID)	uint16	目标主机的 VLAN 标识号（如适用）。
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)	uint8[16]	充当目标主机操作系统的唯一标识符的指纹 ID 号码。 有关获取映射到指纹 ID 的值的信息，请参阅服务记录，第 4-14 页。
目标重要性 (Destination Criticality)	uint16	目标主机的用户定义临界值: ▪ 0 - 无 ▪ 1 - 低 ▪ 2 - 中 ▪ 3 - 高
目标用户 ID (Destination User ID)	uint32	系统识别的登录目标主机的用户的标识号。
目标端口 (Destination Port)	uint16	事件中的目标端口。
目标服务 ID (Destination Service ID)	uint32	源主机上运行的服务器的标识号。

表 3-23　关联事件 5.4+ 数据字段 （续）

字段	数据类型	说明 (Description)
影响 (Impact)	uint8	事件的影响标志值。其值如下： ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 - 灰色（未知影响）
已阻止 (Blocked)	uint8	表示触发入侵事件的数据包发生了什么情况的值。 ▪ 0 - 未丢弃入侵事件 ▪ 1 - 已丢弃入侵事件（当部署为内联、交换或路由式部署时丢弃） ▪ 2 - 如果已向在内联、交换或路由式部署中配置的设备应用入侵策略，则触发事件的数据包本应已丢弃。
入侵策略 (Intrusion Policy)	uint8[16]	与事件关联的入侵策略的 UUID。
规则操作 (Rule Action)	uint32	针对触发事件的规则在用户界面中选择的操作（允许、阻止等）。
字符串块类型 (String Block Type)	uint32	启动包含 NetBIOS 域的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-67 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数，包括字符串块类型的四个字节、字符串块长度的四个字节，加上 NetBIOS 域中的字节数。
NetBIOS 域 (NetBIOS Domain)	字符串	NetBIOS 域的名称
URL 类别 (URL Category)	uint32	指示 URL 类别的编号。有关详细信息，请参阅URL 类别记录元数据，第 4-24 页。
URL 信誉 (URL Reputation)	uint32	URL 信誉的 ID 号码。请参阅 URL 信誉记录元数据，第 4-24 页
字符串块类型 (String Block Type)	uint32	启动包含 URL 的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-67 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数，包括字符串块类型的四个字节、字符串块长度的四个字节，加上 URL 中的字节数。
URL	字符串	触发相关事件的 URL。
客户 ID (Client ID)	uint32	检测到事件的客户端的 ID 号码。
字符串块类型 (String Block Type)	uint32	启动包含客户端版本的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-67 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数，包括字符串块类型的四个字节、字符串块长度的四个字节，加上客户端版本中的字节数。

表 3-23 关联事件 5.4+ 数据字段 （续）

字段	数据类型	说明 (Description)
客户端版本 (Client Version)	字符串	检测到事件的客户端的版本。
访问控制策略版本 (Access Control Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号。
访问控制规则 ID (Access Control Rule ID)	uint32	触发事件的规则的内部标识符。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当与关联事件相关的入口接口的唯一标识符的接口 ID。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当与关联事件相关的出口接口的唯一标识符的接口 ID。
入口区 UUID (Ingress Zone UUID)	uint8[16]	充当与关联事件相关的入口安全区的唯一标识符的区域 ID。
出口区 UUID (Egress Zone UUID)	uint8[16]	充当与关联事件相关的出口安全区的唯一标识符的区域 ID。
源 IPv6 地址 (Source IPv6 Address)	uint8[16]	事件中源主机的 IP 地址，采用 IPv6 地址八位组。
目的 IPv6 地址	uint8[16]	事件中目标主机的 IP 地址，采用 IPv6 地址八位组。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint16	目标主机的国家/地区代码。
安全情报 UUID (Security Intelligence UUID)	uint8[16]	为安全情报配置的访问控制策略的 UUID。
安全情景 (Security Context)	uint8[16]	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 IDD 编号。

表 3-23　　关联事件 5.4+ 数据字段 （续）

字段	数据类型	说明 (Description)
SSL 实际操作 (SSL Actual Action)	uint32	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 3-23 关联事件 5.4+ 数据字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint32	SSL 流量的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。

了解系列 2 数据块

从版本 4.10.0 开始，eStreamer 服务使用第二系列数据块打包入侵事件额外数据等记录。有关该系列中的所有块类型列表，请参阅表 3-24，第 3-55 页。与系列 1 数据块一样，系列 2 数据块也支持可变长度字段和嵌套式数据块的层次结构。系列 2 数据块类型与系列 1 基元数据块类型一样，包括了具有的嵌套式内部块封装机制的基元数据块。但是，系列 2 块与系列 1 块具有不同的编号系统。

以下示例展示如何使用基元数据块。列表数据块（系列 2 块类型 31）定义一个操作系统指纹数组（每个指纹本身都是一个具有可变长度的类型 87 数据块）。类型 31 数据块的总体长度通过数据块长度 (Data Block Length) 字段进行自描述，包含消息的数据部分的长度，不包括块类型和块长度字段中的 8 个字节。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	列表数据块类型 (2) (List Data Block Type (2))																															
	数据块长度 (Data Block Length)																															
服务器指纹 (Server Fingerprints)	操作系统指纹块类型 (87) (Operating System Fingerprint Block Type (87))																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统服务器指纹数据... (Operating System Server Fingerprint Data...)																															

在下表中，“数据块状态”(Data Block Status) 字段指示该块是当前版本（最新版本）还是旧版本（在较旧的版本中使用，但仍可以通过 eStreamer 请求）。

表 3-24　　系列 2 块类型

类型 (Type)	内容	数据块状态	说明
0	字符串	当前	封装可变字符串数据。有关详细信息，请参阅字符串数据块，第 3-59 页。
1	BLOB	当前	封装二进制数据，专门用于横幅。有关详细信息，请参阅BLOB 数据块，第 3-60 页。
2	列表	当前	封装其他数据块列表。有关详细信息，请参阅列表数据块，第 3-61 页。
3	通用列表	当前	封装其他数据块列表。对于反序列化，它相当于列表数据块。有关详细信息，请参阅通用列表数据块，第 3-62 页。
4	事件额外数据	传统模式	包含入侵事件额外数据。有关详细信息，请参阅入侵事件额外数据记录，第 B-66 页。
5	额外数据类型	当前	包含额外数据元数据。有关详细信息，请参阅入侵事件额外数据元数据，第 B-67 页。

表 3-24　系列 2 块类型（续）

类型 (Type)	内容	数据块状态	说明
14	UUID 字符串映射	当前	各种元数据消息将 UUID 值映射到描述性字符串时使用的块。请参阅UUID 字符串映射数据块，第 3-62 页。
15	访问控制策略规则 ID 元数据	当前	包含访问控制规则的元数据。请参阅访问控制策略规则 ID 元数据块，第 3-64 页。
16	恶意软件事件	传统	包含恶意软件事件的信息，如在内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户。请参阅恶意软件事件数据块 5.1，第 B-70 页。被块 24 否决，恶意软件事件数据块 5.3.1，第 B-94 页。
19	ICMP 类型数据块	当前	包含描述 ICMP 类型的元数据。请参阅ICMP 类型数据块，第 3-66 页。
20	ICMP 代码数据块	当前	包含描述 ICMP 代码的元数据。请参阅ICMP 代码数据块，第 3-67 页。
21	访问控制策略规则原因数据块	当前	包含解释访问控制策略规则原因的信息。请参阅用于 6.0+ 的访问控制策略规则原因数据块，第 3-77 页。
22	IP 信誉类别数据块	当前	包含有关 IP 信誉类别（解释 IP 地址被阻止的原因）的信息。请参阅访问控制策略名称数据块，第 3-79 页。
23	文件事件	传统	包含有关文件事件的信息，如文件的源、SHA 散列以及处置情况。请参阅用于 5.1.1.x 的文件事件，第 B-309 页。它被块 32 替代，访问控制策略规则 ID 元数据块，第 3-64 页。
24	恶意软件事件	传统	包含恶意软件事件的信息，如在内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户。请参阅恶意软件事件数据块 5.1.1.x，第 B-74 页。否决块 16，恶意软件事件数据块 5.1，第 B-70 页。被块 33 否决，恶意软件事件数据块 5.3.1，第 B-94 页。
25	入侵事件	传统	包含有关入侵事件的信息，包括将入侵事件与连接事件和恶意软件事件匹配的信息。请参阅入侵事件记录 5.1.1.x，第 B-24 页。被块 34 否决，入侵事件记录 5.2.x，第 B-12 页。
26	文件事件 SHA 散列	传统	包含已识别为包含恶意软件的文件的 SHA 散列和名称。请参阅用于 5.1.1-5.2.x 的文件事件 SHA 散列，第 B-346 页。被块 40 否决，用于 5.3+ 的文件事件 SHA 散列，第 3-102 页。
27	规则文档数据块	当前	包含有关用于生成事件的规则的信息。有关详细信息，请参阅用于 5.2+ 的规则文档数据块，第 3-105 页。
28	地理位置数据块	当前	包含国家/地区代码及相应的国家/地区名称。请参阅用于 5.2+ 的地理位置数据块，第 3-113 页。

表 3-24　系列 2 块类型 （续）

类型 (Type)	内容	数据块状态	说明
32	文件事件	传统	包含有关文件事件的信息，如文件的源、SHA 散列以及处置情况。请参阅用于 5.2 的文件事件，第 B-313 页。它否决用于 5.1.1.x 的文件事件，第 B-309 页。被块 38 否决，用于 5.3 的文件事件，第 B-317 页。
33	恶意软件事件	当前	包含恶意软件事件的信息，如在内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户。请参阅恶意软件事件数据块 5.2.x，第 B-80 页。否决块 24，恶意软件事件数据块 5.1.1.x，第 B-74 页。被块 35 否决，恶意软件事件数据块 5.3，第 B-87 页。
34	入侵事件	传统	包含有关入侵事件的信息，包括将入侵事件与连接事件和恶意软件事件匹配的信息。请参阅入侵事件记录 5.2.x，第 B-12 页。否决块 25。被块 41 否决，入侵事件记录 5.3，第 B-18 页。
35	恶意软件事件	传统	包含有关恶意软件事件的信息，包括 IOC 信息。请参阅恶意软件事件数据块 5.3，第 B-87 页。否决块 33，恶意软件事件数据块 5.2.x，第 B-80 页。被块 44 否决，恶意软件事件数据块 5.3，第 B-87 页。
38	文件事件	传统	包含有关文件事件的信息，如文件的源、SHA 散列以及处置情况。请参阅用于 5.3 的文件事件，第 B-317 页。它否决块 32。被块 43 否决，恶意软件事件数据块 7.0+，第 3-92 页。
39	IOC 名称数据块	当前	包含有关 IOC 的信息。请参阅用于 5.3+ 的 IOC 名称数据块，第 4-35 页
40	文件事件 SHA 散列	当前	包含已识别为包含恶意软件的文件的 SHA 散列和名称。请参阅用于 5.3+ 的文件事件 SHA 散列，第 3-102 页。否决块 26，用于 5.1.1-5.2.x 的文件事件 SHA 散列，第 B-346 页。
41	入侵事件	传统	包含有关入侵事件的信息，包括将入侵事件与 IOC 匹配的信息。请参阅入侵事件记录 5.3，第 B-18 页。否决块 34。被块 42 否决，入侵事件记录 5.3.1，第 B-29 页。
42	入侵事件	传统模式	包含有关入侵事件的信息，包括将入侵事件与 IOC 匹配的信息。请参阅入侵事件记录 5.3.1，第 B-29 页。否决块 41，入侵事件记录 5.3，第 B-18 页。被块 45 否决，入侵事件记录 5.4.x，第 B-36 页。
43	文件事件	传统	包含有关文件事件的信息，如文件的源、SHA 散列以及处置情况。请参阅用于 5.3.1 的文件事件，第 B-323 页。否决块 38，用于 5.3 的文件事件，第 B-317 页。被块 46 否决，7.0+ 的文件事件，第 3-82 页
44	恶意软件事件	传统	包含有关恶意软件事件的信息，包括 IOC 信息。请参阅恶意软件事件数据块 7.0+，第 3-92 页。否决块 35，恶意软件事件数据块 5.3，第 B-87 页。被块 47 否决，恶意软件事件数据块 7.0+，第 3-92 页

表 3-24 系列 2 块类型 （续）

类型 (Type)	内容	数据块状态	说明
45	入侵事件	传统模式	包含有关入侵事件的信息。请参阅 入侵事件记录 5.4.x，第 B-36 页。否决块 42，入侵事件记录 5.3.1，第 B-29 页。被块 60 否决，入侵事件记录 6.x，第 B-45 页。
46	文件事件	传统模式	包含有关文件事件的信息，如文件的源、SHA 散列以及处置情况。请参阅恶意软件事件数据块 7.0+，第 3-92 页。否决块 43，用于 5.3.1 的文件事件，第 B-323 页。
47	恶意软件事件	当前	包含有关恶意软件事件的信息，包括 IOC 信息。请参阅恶意软件事件数据块 7.0+，第 3-92 页。否决块 44，恶意软件事件数据块 5.3.1，第 B-94 页。
50	SSL 证书详细信息 (SSL Certificate Details)	当前	包含有关 SSL 证书的信息。观察用于 5.4+ 的 SSL 证书详细信息数据块，第 3-124 页
51	SSL 规则 ID	当前	包含有关 SSL 规则的信息。请参阅 SSL 规则 ID，第 3-117 页
56	文件事件	传统模式	包含有关文件事件的信息。请参阅 6.x 的文件事件，第 B-337 页。否决块 46， 用于 5.4 的文件事件，第 B-329 页。 它被块类型 79 弃用， 恶意软件事件数据块 7.0+，第 3-92 页
57	用户记录	当前	包含有关用户的信息。请参阅 用户记录，第 3-22 页
58	终端配置文件	当前	包含有关网络终端的信息。请参阅 用于 6.0+ 的终端配置文件数据块，第 3-70 页
59	访问控制策略规则原因 (Access Control Policy Rule Reason)	当前	包含关于访问控制策略规则的信息。请参阅 用于 6.0+ 的访问控制策略规则原因数据块，第 3-77 页
60	入侵事件	传统模式	包含有关入侵事件的信息。请参阅 入侵事件记录 6.x，第 B-45 页。否决块 45，入侵事件记录 5.3.1，第 B-29 页。被块 81 否决，入侵事件记录 7.1+，第 3-7 页。
61	名称说明映射	当前	用于在许多情况下将名称映射到描述。请参阅 名称说明映射数据块，第 3-63 页
62	恶意软件事件	传统模式	包含有关恶意软件事件的信息。请参阅恶意软件事件数据块 6.x，第 B-111 页。否决块 44，恶意软件事件数据块 5.3.1，第 B-94 页。被块类型 80 否决， 恶意软件事件数据块 7.0+，第 3-92 页
64	访问控制策略名称 (Access Control Policy Name)	当前	包含关于访问控制策略名称的信息。请参阅 访问控制策略名称数据块，第 3-79 页

表 3-24　　系列 2 块类型 （续）

类型 (Type)	内容	数据块状态	说明
79	文件事件	当前	包含有关文件事件的信息。请参阅7.0+ 的文件事件，第 3-82 页。否决块 56， 6.x 的文件事件，第 B-337 页。
80	恶意软件事件	当前	包含有关恶意软件事件的信息。请参阅 恶意软件事件数据块 7.0+，第 3-92 页。否决块 62，恶意软件事件数据块 6.x，第 B-111 页。
81	入侵事件	当前	包含有关入侵事件的信息。请参阅 入侵事件记录 7.1+，第 3-7 页。否决块 60，入侵事件记录 6.x，第 B-45 页。

系列 2 基元数据块

系列 2 和系列 1 块都包含一组用于封装可变长度块列表以及消息中的可变长度字符串和 BLOB 的基元。基元数据块具有在上文数据块报头，第 2-23 页中讨论的标准 eStreamer 块报头，但它们仅出现在其他数据块中。给定的块类型可以包含任何数字。有关这些块的结构的详细信息，请参阅以下内容:

- 字符串数据块，第 3-59 页
- BLOB 数据块，第 3-60 页
- 列表数据块，第 3-61 页
- 通用列表数据块，第 3-62 页
- UUID 字符串映射数据块，第 3-62 页
- 名称说明映射数据块，第 3-63 页

字符串数据块

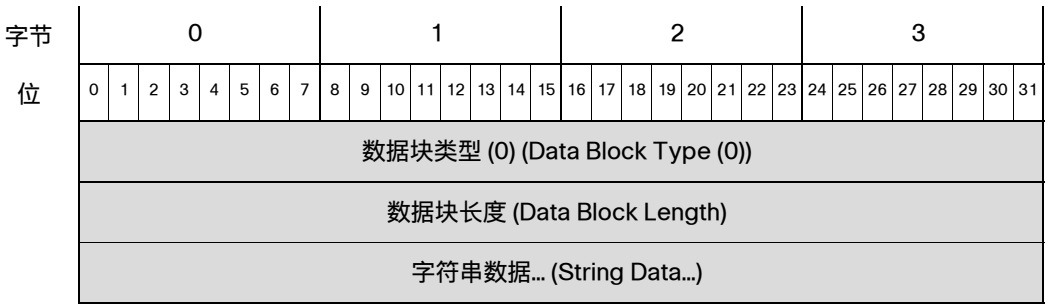
eStreamer 服务使用字符串数据块发送消息中的字符串数据。这些块常出现在其他数据块中，用于识别，例如，操作系统或服务器名称。

空字符串数据块（不包含任何数据，只有报头字段）的块长度为 8。eStreamer 在字符串值没有任何内容时使用空字符串数据块，出现这种情况的一个例子是，操作系统的供应商未知时操作系统数据块中的操作系统供应商字符串字段。

字符串数据块的块类型为系列 2 数据块组中的 0。

注释　此数据块中返回的字符串不总是以空值终止（即字符串字符后面不总是 0）。

下图显示字符串数据块的格式:



下表对字符串数据块的字段进行了说明。

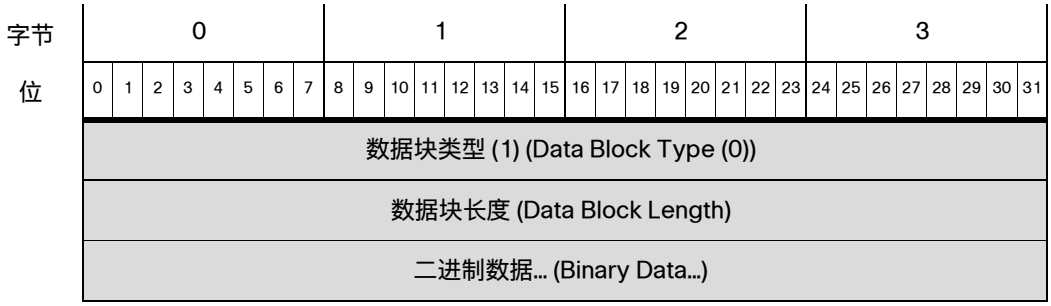
表 3-25 字符串块字段

字段	数据类型	说明 (Description)
数据块类型 (Data Block Type)	uint32	启动字符串数据块。值始终为 0。
数据块长度 (Data Block Length)	uint32	字符串数据块报头与字符串数据的总长度（字节数）。
字符串数据 (String Data)	字符串	包含字符串数据，且可能在字符串结尾包含一个终止字符（空字节）。

BLOB 数据块

eStreamer 服务使用 BLOB 数据块传送二进制数据。例如，主机发现记录使用 BLOB 块承载捕获的服务器横幅。BLOB 数据块的块类型为系列 2 数据块组中的 1。

下图显示 BLOB 数据块的格式:



下表对 BLOB 数据块的字段进行了说明。

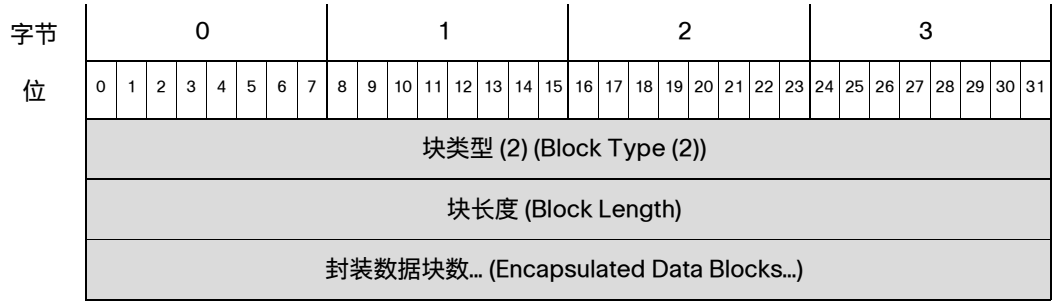
表 3-26　BLOB 数据块字段

字段	数据类型	说明 (Description)
数据块类型 (Data Block Type)	uint32	启动 BLOB 数据块。值始终为 1。
数据块长度 (Data Block Length)	uint32	BLOB 数据块中的字节数，包括 BLOB 块类型和长度字段的八个字节，加上随后的二进制数据的长度。
二进制数据 (Binary Data)	变量	包含服务器横幅等二进制数据。

列表数据块

eStreamer 服务使用列表数据块封装数据块列表。例如，eStreamer 可以使用列表数据块发送 TCP 服务器列表，每个 TCP 服务器本身就是一个数据块。列表数据块的块类型为系列 2 数据块组中的 2。

下图显示列表数据块的基本格式:



下表对列表数据块的字段进行了说明。

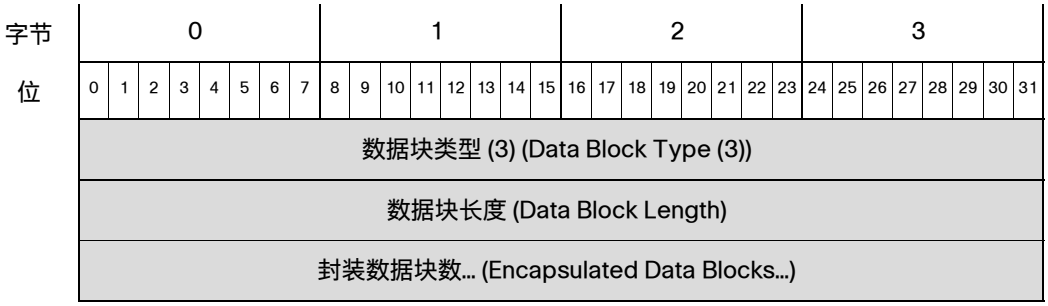
表 3-27　列表数据块字段

字段	数据类型	说明 (Description)
块类型 (Block Type)	uint32	启动列表数据块。值始终为 2。
块长度 (Block Length)	uint32	列表块和封装数据中的字节数。例如，如果列表中包含三个子服务器数据块，则此处的值包含子服务器数据块中的字节总数，加上列表块报头的八个字节。
封装数据块数 (Encapsulated Data Blocks)	变量	封装数据块数最多可以是列表块长度中的最大字节数。

通用列表数据块

eStreamer 服务使用通用列表数据块封装数据块列表。例如，主机配置文件数据块包含有关多个客户端应用的信息，并使用通用列表数据块在消息中嵌入客户端应用数据块列表。通用列表数据块的块类型为系列 2 数据块组中的 3。

下图显示通用列表数据块的基本结构：



下表对通用列表数据块的字段进行了说明。

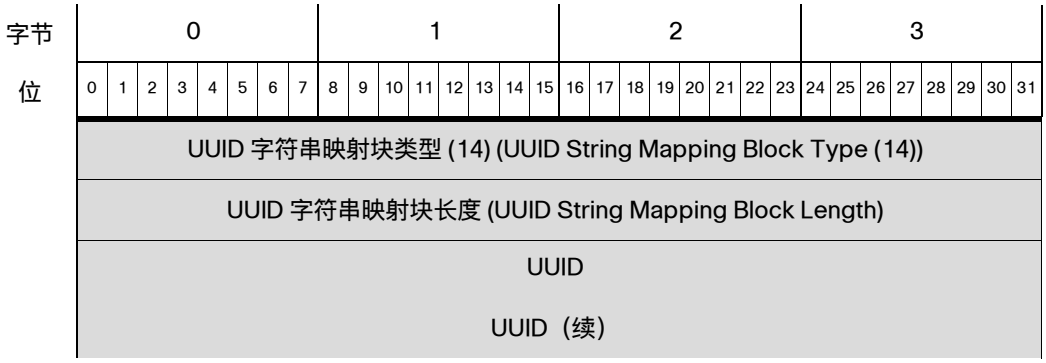
表 3-28 通用列表数据块字段

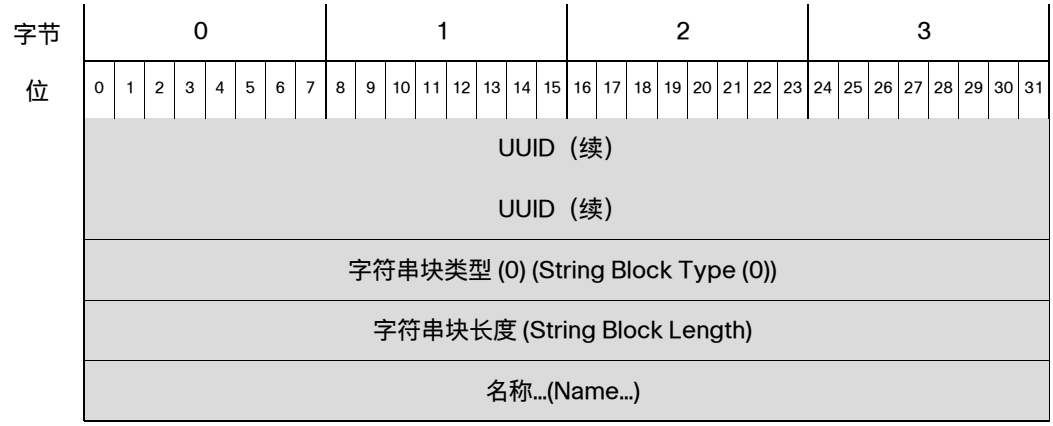
字段	字节数	说明 (Description)
数据块类型 (Data Block Type)	uint32	启动通用列表数据块。值始终为 3。
数据块长度 (Data Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节总数。
封装数据块数 (Encapsulated Data Blocks)	变量	封装数据块数最多可以是通用列表块长度中的最大字节数。

UUID 字符串映射数据块

eStreamer 服务使用各种元数据消息中的 UUID 字符串映射数据块，将 UUID 值映射到描述性字符串。UUID 字符串映射数据块的块类型为系列 2 中的 14。

下图显示 UUID 字符串映射数据块的结构。





下表对 UUID 字符串映射数据块中的字段进行了说明。

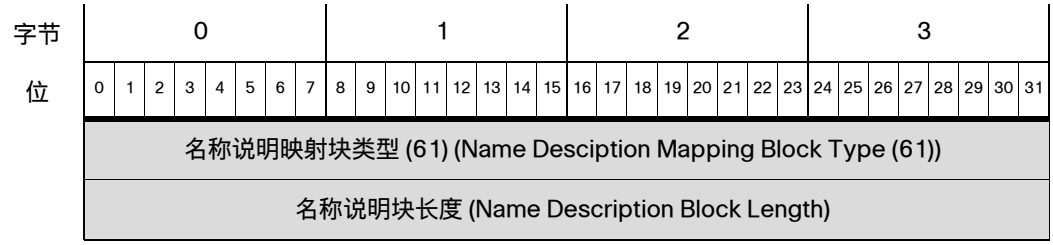
表 3-29　　UUID 字符串映射数据块字段

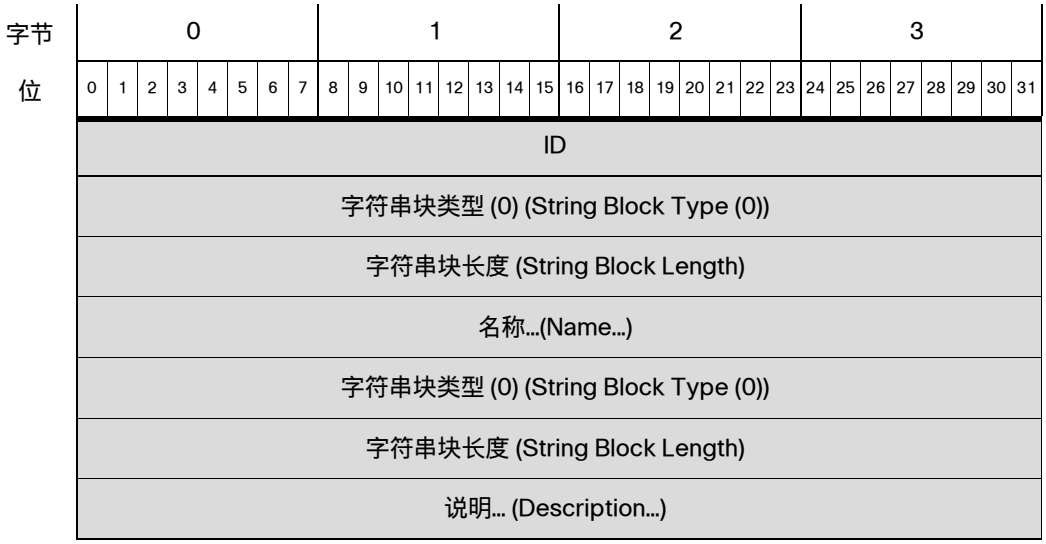
字段	数据类型	说明 (Description)
UUID 字符串映射块类型 (UUID String Mapping Block Type)	uint32	启动 UUID 字符串映射块。值始终为 14。
UUID 字符串映射块长度 (UUID String Mapping Block Length)	uint32	UUID 字符串映射块中的字节总数，包括 UUID 字符串映射块类型和长度字段的八个字节，加上随后的数据字节数。
UUID	uint8[16]	UUID识别的事件或其他对象的唯一标识符。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含与 UUID 相关的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
名称 (Name)	字符串	描述性名称。

名称说明映射数据块

eStreamer 服务使用各种元数据消息中的名称说明映射数据块，将 ID 值映射到名称和描述性字符串。名称说明映射数据块的块类型为系列 2 中的 61。

下图显示名称说明映射数据块的结构。





下表对名称说明映射数据块中的字段进行了说明。

表 3-30 名称说明映射数据块字段

字段	数据类型	说明 (Description)
名称说明映射块类型 (Name Description Mapping Block Type)	uint32	启动名称说明映射块。值始终为 61。
名称说明映射块长度 (Name Description Mapping Block Length)	uint32	名称说明映射块中的字节总数，包括名称说明映射块类型和长度字段的八个字节，加上随后的数据字节数。
ID	unit32	ID 识别的事件或其他对象的唯一标识符。 此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含与 ID 相关的名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
名称 (Name)	字符串	事件或对象的名称。
字符串块类型 (String Block Type)	uint32	启动包含与 ID 相关的说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“说明”(Description) 字段中的字节数。
说明 (Description)	字符串	对与 ID 相关的对象或事件的说明。

访问控制策略规则 ID 元数据块

eStreamer 服务用访问控制策略规则 ID 元数据块包含有关访问控制策略规则 ID 的信息。此数据块的块类型为系列 2 中的 15。

下图显示访问控制策略规则 ID 元数据块的结构。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	访问控制策略规则 ID 元数据块类型 (15) (Access Control Policy Rule ID Metadata Block Type (15))																															
	访问控制策略规则 ID 元数据块长度 (Access Control Policy Rule ID Metadata Block Length)																															
	修订版 (Revision) 修订版 (Revision)（续） 修订版 (Revision)（续） 修订版 (Revision)（续）																															
	规则 ID (Rule ID)																															
名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名称...(Name...)																															

下表对访问控制策略规则 ID 元数据块中的字段进行了说明。

表 3-31　　访问控制策略规则 ID 元数据块字段

字段	数据类型	说明 (Description)
访问控制策略规则 ID 元数据块类型 (Access Control Policy Rule ID Metadata Block Type)	uint32	启动访问控制策略规则 ID 元数据块。值始终为 15。
访问控制策略规则 ID 元数据块长度 (Access Control Policy Rule ID Metadata Block Length)	uint32	访问控制策略规则 ID 块中的字节总数，包括访问控制策略规则 ID 元数据块类型和长度字段的八个字节，加上随后的数据的字节数。
修订版 (Revision)	uint8[16]	与触发的关联事件相关的规则版本号。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符。 此字段是此记录的唯一密钥。

表 3-31　访问控制策略规则 ID 元数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含与访问控制策略规则相关的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
名称 (Name)	字符串	访问控制策略规则的描述性名称。

ICMP 类型数据块

eStreamer 服务使用 ICMP 类型数据块包含有关 ICMP 类型的信息。此数据块的记录类型为系列 2 中的 260，块类型为系列 2 中的 19。

下图显示 ICMP 类型数据块的结构。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															
	Netmap ID																记录类型 (260) (Record Type (260))															
	ICMP 类型数据块类型 (19) (ICMP Type Data Block Type (19))																															
	ICMP 类型数据块长度 (ICMP Type Data Block Length)																															
	类型 (Type)																协议 (Protocol)															
说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明... (Description...)																															

下表对 ICMP 类型数据块中的字段进行了说明。

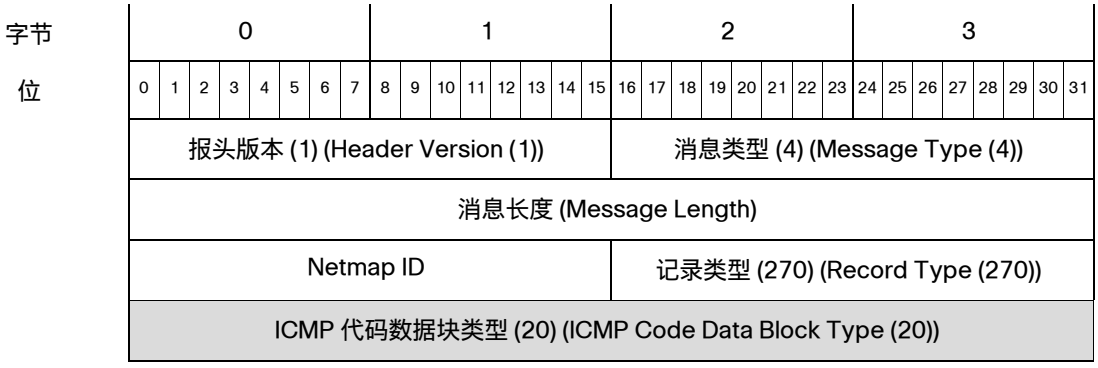
表 3-32　　ICMP 类型数据块字段

字段	数据类型	说明 (Description)
ICMP 类型数据块类型 (ICMP Type Data Block Type)	uint32	启动 ICMP 类型数据块。值始终为 19。
ICMP 类型数据块长度 (ICMP Type Data Block Length)	uint32	ICMP 类型数据块中的字节总数，包括 ICMP 类型数据块类型和长度字段的八个字节，加上随后的数据字节数。
类型 (Type)	uint16	事件的 ICMP 类型。
协议 (Protocol)	uint16	IANA 指定的协议号。例如: ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP
字符串块类型 (String Block Type)	uint32	启动包含对 ICMP 类型的说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上说明 (Description) 字段中的字节数。
说明 (Description)	字符串	对事件的 ICMP 类型的说明。

ICMP 代码数据块

eStreamer 服务用 ICMP 代码数据块包含有关访问控制策略规则 ID 的信息。此数据块的记录类型为系列 2 中的 270，块类型为系列 2 中的 20。

下图显示访问控制策略规则 ID 元数据块的结构。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	ICMP 代码数据块长度 (ICMP Code Data Block Length)																															
	代码 (Code)																类型 (Type)															
说明	协议 (Protocol)																字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0)) (续)																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length) (续)																说明... (Description...)															

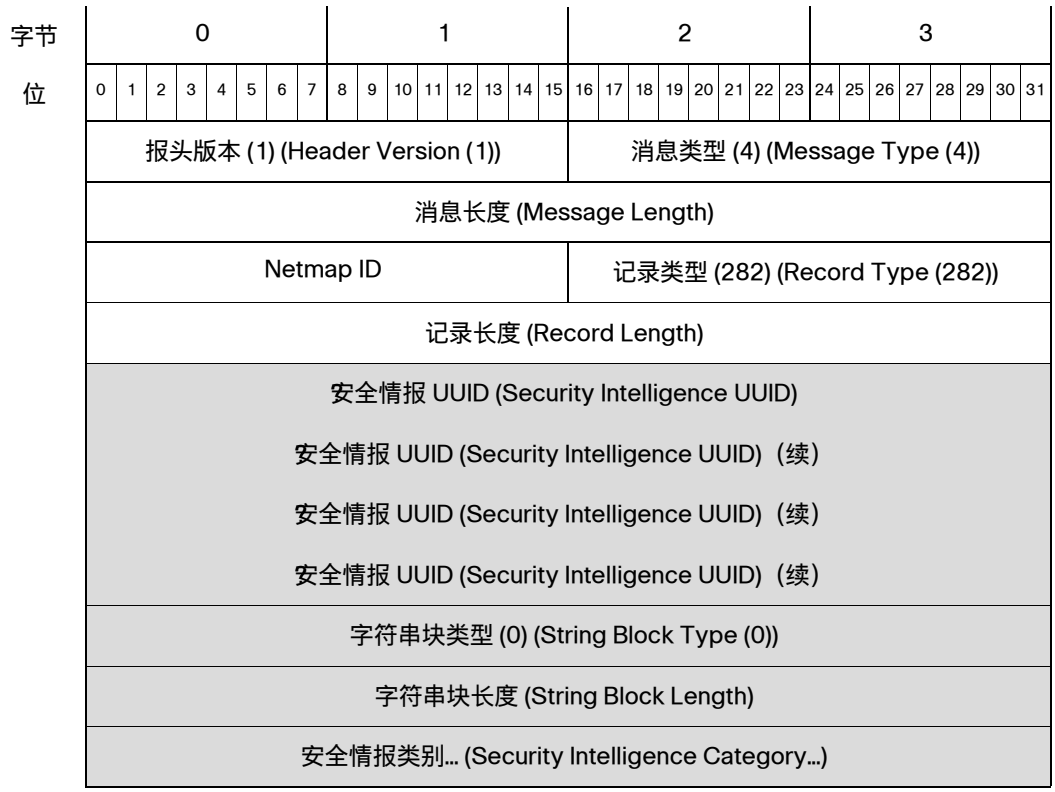
下表对 ICMP 代码数据块中的字段进行了说明。

表 3-33 ICMP 代码数据块字段

字段	数据类型	说明 (Description)
ICMP 代码数据块类型 (ICMP Code Data Block Type)	uint32	启动 ICMP 代码数据块。值始终为 20。
ICMP 代码数据块长度 (ICMP Code Data Block Length)	uint32	ICMP 代码数据块中的字节总数，包括 ICMP 代码数据块类型和长度字段的八个字节，加上随后的数据字节数。
代码 (Code)	uint16	事件的 ICMP 代码。
类型 (Type)	uint16	事件的 ICMP 类型。
协议 (Protocol)	uint16	IANA 指定的协议号。例如: ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP
字符串块类型(String Block Type)	uint32	启动包含对 ICMP 代码的说明的字符串数据块。值始终为 0。
字符串块长度(String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上说明 (Description) 字段中的字节数。
说明 (Description)	字符串	对事件的 ICMP 代码的说明。

用于 5.4.1+ 的安全情报类别元数据

eStreamer 服务可传输包含安全情报类别信息的元数据，格式如下所示。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 282，表示安全情报类别记录。



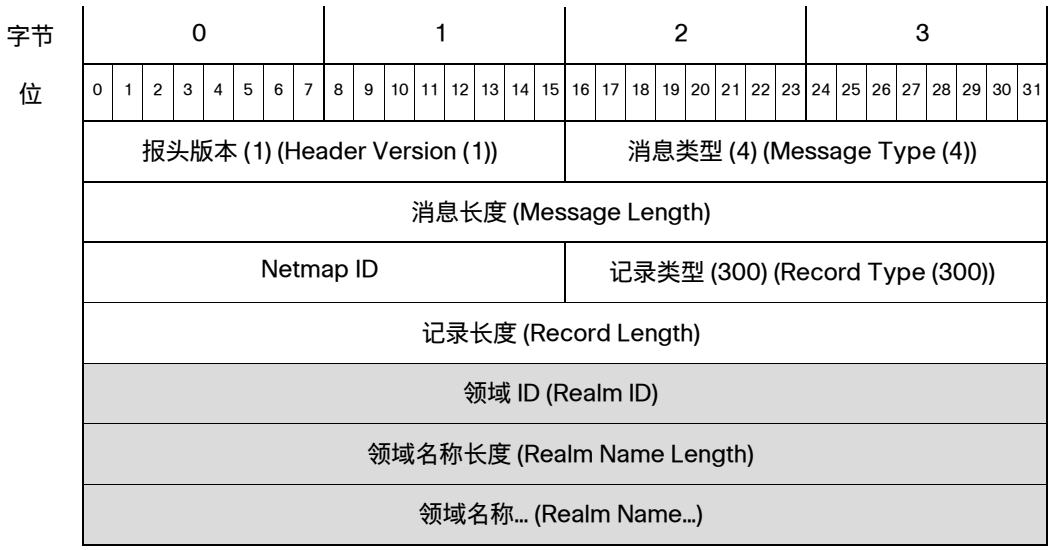
下表对安全情景名称记录中的字段进行了说明。

表 3-34　　安全情景名称记录字段

字段	数据类型	说明 (Description)
安全情报 UUID (Security Intelligence UUID)	uint8[16]	安全情报的 UUID。 此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含安全情报类别的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	安全情报类别字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“配置文件名称”(File Name) 字段中的字节数。
安全情报类别 (Security Intelligence Category)	字符串	安全情报类别。

用于 6.0+ 的领域元数据

eStreamer 服务可传输包含领域信息的元数据，格式如下所示。请注意，“记录类型”(Record Type) 字段（出现在消息长度 (Message Length) 字段后面）的值为 300，表示领域元数据记录。



下表对领域元数据记录中的字段进行了说明。

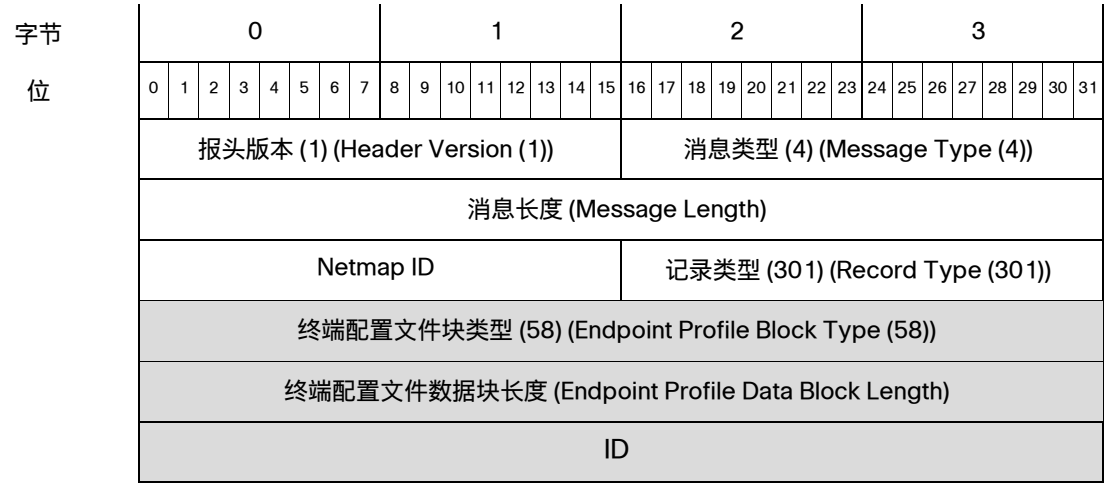
表 3-35 领域元数据记录字段

字段	数据类型	说明 (Description)
领域 ID (Realm ID)	uint32	领域的唯一 ID 号码。此字段是此记录的唯一密钥。
领域名称长度 (Realm Name Length)	uint32	“领域名称”(Realm Name) 中包含的字节数。
领域名称 (Realm Name)	字符串	领域名称

用于 6.0+ 的终端配置文件数据块

eStreamer 服务使用终端配置文件数据块来包含有关网络终端的信息。此数据块的记录类型为系列 2 中的 301，块类型为系列 2 中的 58。

下图显示访问控制策略规则 ID 元数据块的结构。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
配置文件名称 (Profile Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	配置文件名称... (Profile Name...)																															
全称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	全名...(Full Name...)																															

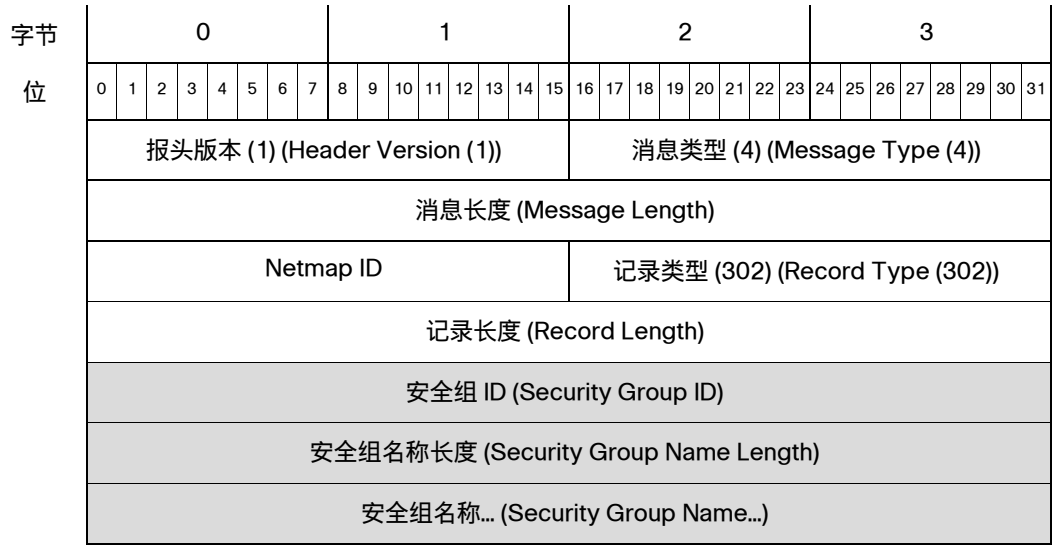
下表对终端配置文件数据块中的字段进行了说明。

表 3-36　　终端配置文件数据块字段

字段	数据类型	说明 (Description)
终端配置文件数据块类型 (Endpoint Profile Data Block Type)	uint32	启动终端配置文件数据块。值始终为 58。
终端配置文件数据块长度 (Endpoint Profile Data Block Length)	uint32	终端配置文件数据块中的字节总数，包括终端配置文件数据块类型和长度字段的八个字节，加上随后的数据字节数。
ID	uint32	终端的 ID 号码。
字符串块类型 (String Block Type)	uint32	启动包含终端的配置文件的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	配置文件名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“配置文件名称”(Profile Name) 字段中的字节数。
配置文件名称 (Profile Name)	字符串	终端配置文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含终端的全名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	全名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“全名”(Full Name) 字段中的字节数。
全称 (Full Name)	字符串	配置文件的完全限定名称，提供该类型终端的关系层次结构。

用于 6.0+ 的安全组元数据

eStreamer 服务可传输包含安全组信息的元数据，格式如下所示。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 302，表示安全组元数据记录。



下表对安全组元数据记录中的字段进行了说明。

表 3-37 安全组元数据记录字段

字段	数据类型	说明 (Description)
安全组 ID (Security Group ID)	uint32	安全组的 ID 号码。 此字段是此记录的唯一密钥。
安全组名称长度 (Security Group Name Length)	uint32	“安全组名称”(Security Group Name) 中包含的字节数。
安全组名称 (Security Group Name)	字符串	安全组名称

用于 6.0+ 的 DNS 记录类型元数据

eStreamer 服务可传输包含 DNS 记录类型信息的元数据，格式如下所示。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 320，表示 DNS 记录类型元数据记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Netmap ID																记录类型 (320) (Record Type (161))															
	记录长度 (Record Length)																															
	名称说明块类型 (61) (Name Description Block Type (61))																															
	名称说明数据块长度 (Name Description Data Block Length)																															
	DNS 记录 ID (DNS Record ID)																															
DNS 记录类型名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	DNS 记录类型名称... (DNS Record Type Name...)																															
DNS 记录类型说明	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	DNS 记录类型说明... (DNS Record Type Description...)																															

下表对 DNS 记录类型元数据记录中的字段进行了说明。

表 3-38　　DNS 记录类型元数据字段

字段	数据类型	说明 (Description)
名称说明数据块类型 (Name Description Data Block Type)	uint32	启动名称说明数据块。值始终为 61。
名称说明数据块长度 (Name Description Data Block Length)	uint32	名称说明数据块中的字节总数，包括名称说明数据块类型和长度字段的八个字节，加上随后的数据的字节数。
DNS 记录 ID (DNS Record ID)	uint32	DNS记录的ID号码。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含 DNS 记录类型名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	DNS 记录类型名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“DNS 记录类型名称” (DNS Record Type Name) 字段中的字节数。
DNS 记录类型名称 (DNS Record Type Name)	字符串	DNS 记录类型的名称。
字符串块类型 (String Block Type)	uint32	启动包含 DNS 记录类型说明的字符串数据块。值始终为 0。

表 3-38 DNS 记录类型元数据字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	DNS 记录类型说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“DNS 记录类型说明” (DNS Record Type Description) 字段中的字节数。
DNS 记录类型说明	字符串	DNS 记录类型的说明。

用于 6.0+ 的 DNS 响应类型元数据

eStreamer 服务可传输 DNS 响应类型元数据，格式如下所示。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 `321`，表示 DNS 响应类型元数据记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															
	Netmap ID																记录类型 (321) (Record Type (161))															
	记录长度 (Record Length)																															
	名称说明块类型 (61) (Name Description Block Type (61))																															
	名称说明数据块长度 (Name Description Data Block Length)																															
	DNS 响应 ID (DNS Response ID)																															
DNS 响应类型名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	DNS 响应类型名称... (DNS Response Type Name...)																															
DNS 响应类型说明	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	DNS 响应类型说明 (DNS Response Type Description...)																															

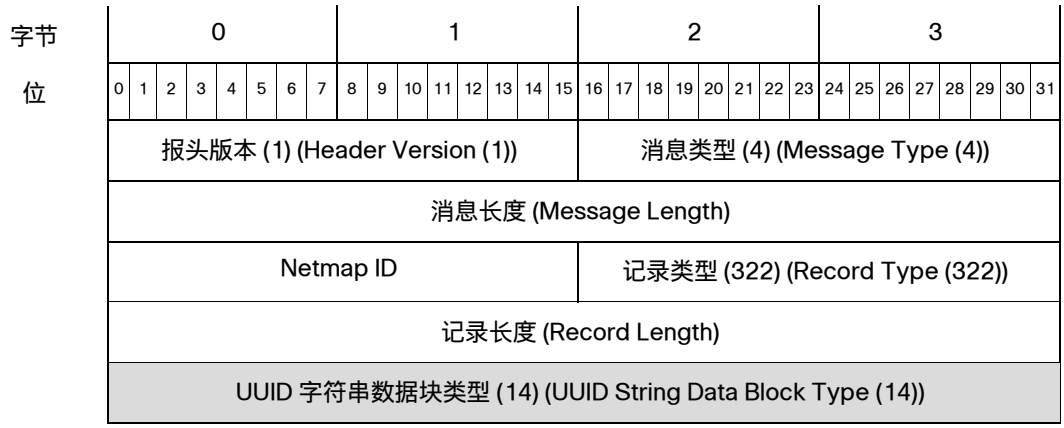
下表对 DNS 响应类型元数据记录中的字段进行了说明。

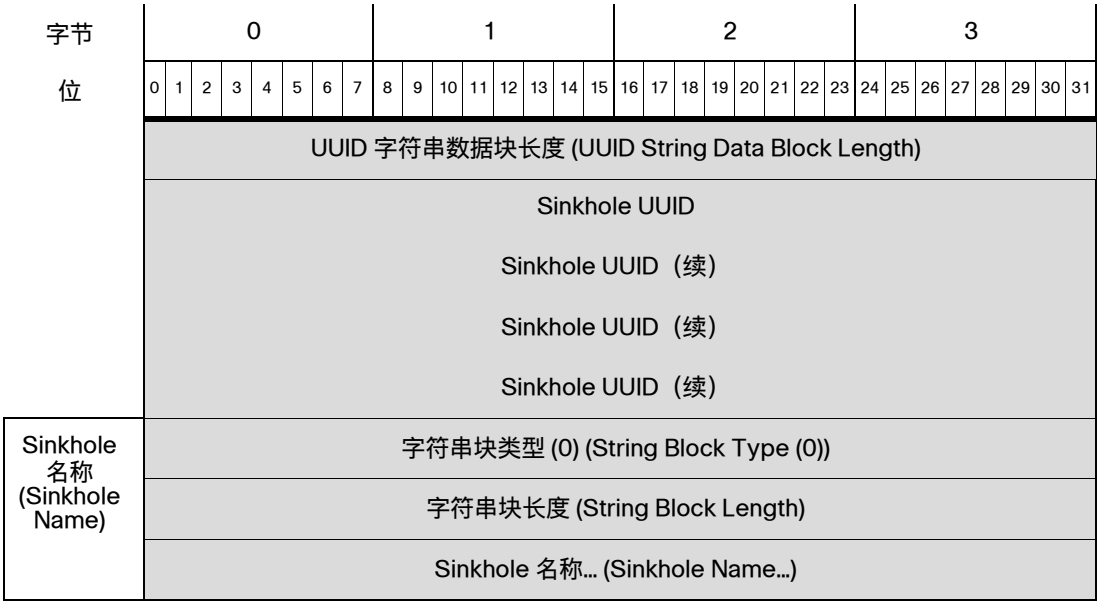
表 3-39　　DNS 响应类型元数据字段

字段	数据类型	说明 (Description)
名称说明数据块类型 (Name Description Data Block Type)	uint32	启动名称说明数据块。值始终为 61。
名称说明数据块长度 (Name Description Data Block Length)	uint32	名称说明数据块中的字节总数，包括名称说明数据块类型和长度字段的八个字节，加上随后的数据的字节数。
DNS 响应 ID (DNS Response ID)	uint32	DNS 响应的 ID 号码。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含 DNS 响应类型名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	DNS 响应类型名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“DNS 响应类型名称” (DNS Response Type Name) 字段中的字节数。
DNS 响应类型名称 (DNS Response Type Name)	字符串	DNS 响应类型的名称。
字符串块类型 (String Block Type)	uint32	启动包含 DNS 响应类型说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	DNS 响应类型说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“DNS 响应类型说明”(DNS Response Type Description) 字段中的字节数。
DNS 响应类型说明	字符串	DNS 响应类型的说明。

用于 6.0+ 的 Sinkhole 元数据

eStreamer 服务可传输包含 Sinkhole 信息的元数据，格式如下所示。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 322，表示 Sinkhole 元数据记录。





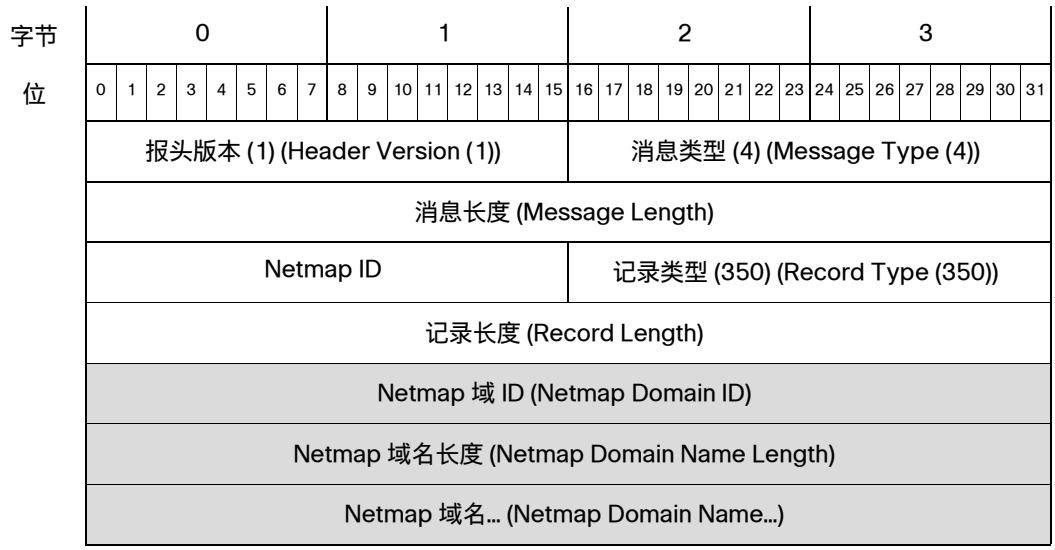
下表对 Sinkhole 元数据记录中的字段进行了说明。

表 3-40 Sinkhole 元数据记录字段

字段	数据类型	说明 (Description)
UUID 字符串数据块类型 (UUID String Data Block Type)	uint32	启动 UUID 字符串数据块。值始终为 14。
UUID 字符串数据块长度 (UUID String Data Block Length)	uint32	UUID 字符串数据块中的字节总数，包括 UUID 字符串数据块类型和长度字段的八个字节，加上随后的数据字节数。
Sinkhole UUID	uint8[16]	Sinkhole 的 UUID 号码。 此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含 Sinkhole 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	Sinkhole 名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“Sinkhole 名称”(Sinkhole Name) 字段中的字节数。
Sinkhole 名称 (Sinkhole Name)	字符串	Sinkhole 的名称。

用于 6.0+ 的 Netmap 域元数据

eStreamer 服务可传输包含 Netmap 域信息的元数据，格式如下所示。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 350，表示 Netmap 域元数据记录。



下表对 Netmap 域元数据记录中的字段进行了说明。

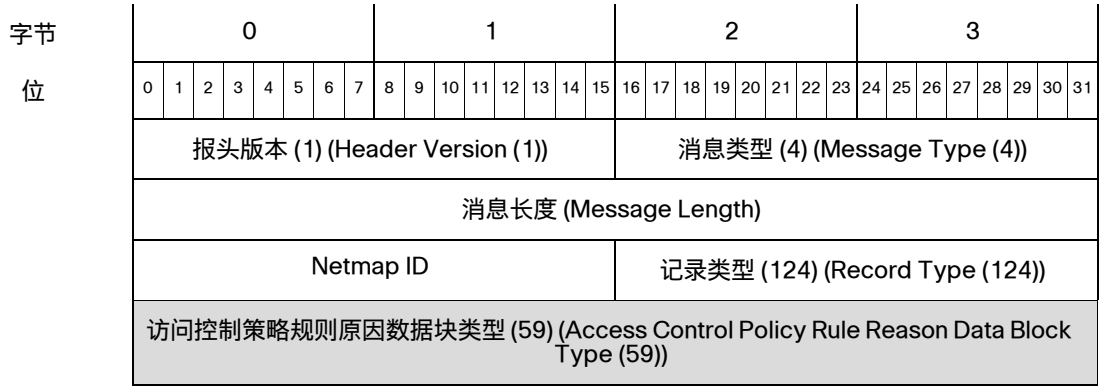
表 3-41　　Sinkhole 元数据记录字段

字段	数据类型	说明 (Description)
Netmap 域 ID (Netmap Domain ID)	uint32	Netmap 域的 ID 号码。此字段是此记录的唯一密钥。
Netmap 域名长度 (Netmap Domain Name Length)	uint32	“Netmap 域名”(Netmap Domain Name) 中包含的字节数。
Netmap 域名 (Netmap Domain Name)	字符串	Netmap 域名

用于 6.0+ 的访问控制策略规则原因数据块

eStreamer服务用访问控制规则策略规则原因数据块包含有关访问控制策略规则 ID 的信息。此数据块的记录类型为系列 2 中的 124，块类型为系列 2 中的 59。它替代了块类型 21。“原因”(Reason) 字段已从 16 位增加至 32 位。

下图显示访问控制策略规则 ID 元数据块的结构。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	访问控制策略规则原因数据块长度 (Access Control Policy Rule Reason Data Block Length)																															
	原因 (Reason)																															
说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明... (Description...)																															

下表对访问控制策略规则原因数据块中的字段进行了说明。

表 3-42 访问控制策略规则原因数据块字段

字段	数据类型	说明 (Description)
访问控制策略规则原因数据块类型 (Access Control Policy Rule Reason Data Block Type)	uint32	启动访问控制策略规则原因数据块。值始终为 59。
访问控制策略规则原因数据块长度 (Access Control Policy Rule Reason Data Block Length)	uint32	访问控制策略规则原因数据块中的字节总数，包括访问控制策略规则原因数据块类型和长度字段的八个字节，加上随后的数据的字节数。

表 3-42　访问控制策略规则原因数据块字段 （续）

字段	数据类型	说明 (Description)
原因 (Reason)	uint32	触发事件的规则的原因编号。 规则原因是一个可以在其中设置多个位的二进制位图。规则可能有多种原因。位值如下： ▪ **1** - IP 阻止 ▪ **2** - IP 监控 ▪ **4** - 用户绕行 ▪ **8** - 文件监控 ▪ **16** - 文件阻止 ▪ **32** - 入侵监控 ▪ **64** - 入侵阻止 ▪ **128** - 阻止继续传输文件 ▪ **256** - 允许继续传输文件 ▪ **512** - 文件自定义检测 ▪ **1024** - SSL 阻止 ▪ **2048** - DNS 阻止 ▪ **4096** - DNS 监控 ▪ **8192** - URL 阻止 ▪ **16384** - URL 监控 ▪ **32768** - 内容限制 ▪ **65536** - 智能应用绕行 ▪ **131072** - WSA 威胁
字符串块类型 (String Block Type)	uint32	启动包含访问控制策略规则原因的说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上说明 (Description) 字段中的字节数。
说明 (Description)	字符串	规则原因的说明。

访问控制策略名称数据块

eStreamer 服务用访问控制策略名称数据块包含有关访问控制策略名称的信息。此数据块的块类型为系列 2 中的 64。

下图显示访问控制策略名称元数据块的结构。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	访问控制策略名称数据块类型 (64) (Access Control Policy Name Data Block Type (64))																															
	访问控制策略名称数据块长度 (Access Control Policy Name Data Block Length)																															
	访问控制策略 UUID (Access Control Policy UUID)																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	传感器 ID (Sensor ID)																															
名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名称...(Name...)																															

下表对访问控制策略名称元数据块中的字段进行了说明。

表 3-43 访问控制策略策略名称数据块字段

字段	数据类型	说明 (Description)
访问控制策略名称数据块类型 (Access Control Policy Name Data Block Type)	uint32	启动访问控制策略名称数据块。值始终为 64。
访问控制策略名称数据块长度 (Access Control Policy Name Data Block Length)	uint32	访问控制策略名称数据块中的字节总数，包括访问控制策略名称数据块类型和长度字段的八个字节，加上随后的数据的字节数。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	访问控制策略的 UUID
传感器 ID (Sensor ID)	uint32	与访问控制策略关联的传感器的 ID 号码
字符串块类型 (String Block Type)	uint32	启动包含访问控制策略的名称的字符串数据块。值始终为 0。

表 3-43　访问控制策略策略名称数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
名称 (Name)	字符串	访问控制策略的名称

IP 信誉类别数据块

eStreamer 服务使用 IP 信誉类别数据块包含有关信誉类别的信息。此数据块的块类型为系列 2 中的 22。

下图显示 IP 信誉类别数据块的结构。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IP 信誉类别数据块类型 (22) (IP Reputation Category Data Block Type (22))																															
	IP 信誉类别数据块长度 (IP Reputation Category Data Block Length)																															
	规则 ID (Rule ID)																															
	策略 UUID (Policy UUID) 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续）																															
说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	类别名称... (Category Name...)																															

下表对 IP 信誉类别数据块中的字段进行了说明。

表 3-44 IP 信誉类别数据块字段

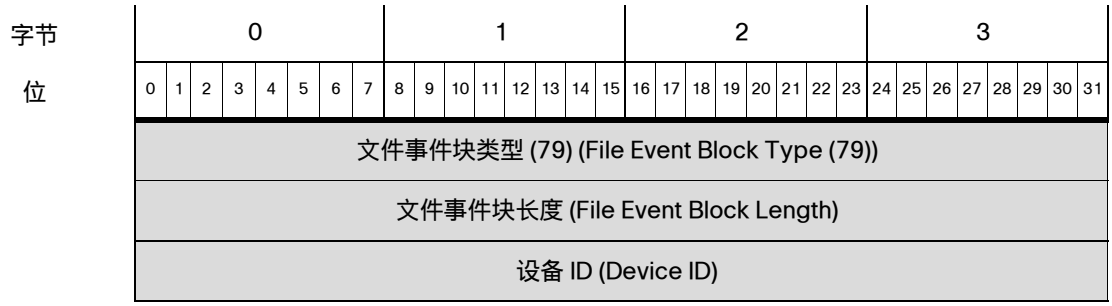
字段	数据类型	说明 (Description)
IP 信誉类别数据块类型 (IP Reputation Category Data Block Type)	uint32	启动 IP 信誉类别数据块。值始终为 22。
IP 信誉类别数据块长度 (IP Reputation Category Data Block Length)	uint32	IP 信誉类别数据块的字节总数，包括 IP 信誉类别数据块类型和长度字段的八个字节，加上随后的数据字节数。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符。
策略 UUID (Policy UUID)	uint8[16]	触发事件的策略的 UUID。
字符串块类型 (String Block Type)	uint32	启动包含对 IP 信誉类别的说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	类别名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“类别名称”(Category Name) 字段中的字节数。
类别名称 (Category Name)	字符串	规则的类别名称。

7.0+ 的文件事件

文件事件数据块包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 79。它替代了块类型 56。虚拟路由和转发的字段。

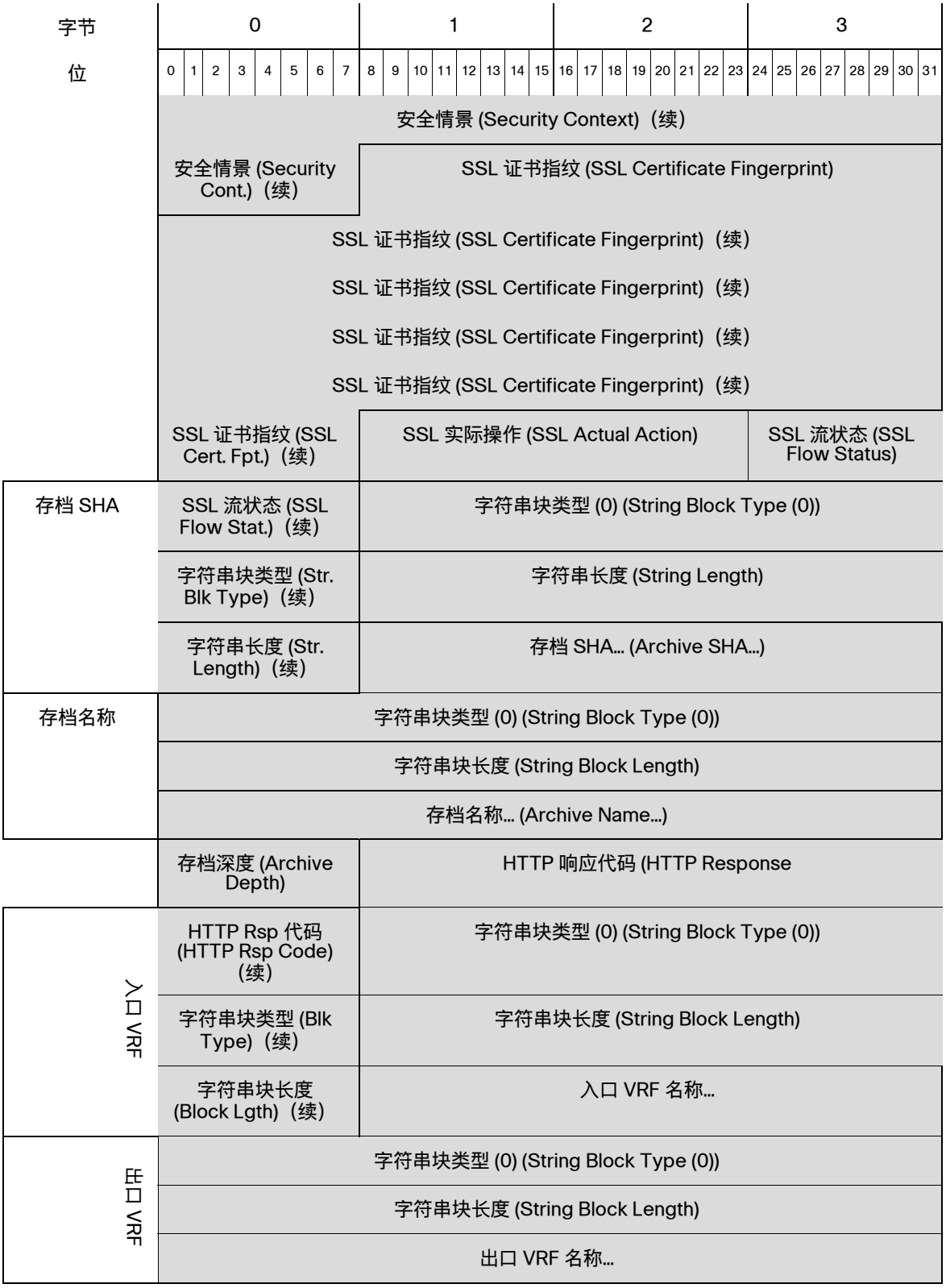
您可以通过在事件版本为 7 且事件代码为 111 的请求消息中设置文件事件标志（“请求标志”(Request Flags) 字段中的位 30）请求文件事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

下图显示文件事件数据块的结构。



<table>
<tr><td>字节</td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>位</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td></td><td colspan="16">连接实例 (Connection Instance)</td><td colspan="16">连接计数器 (Connection Counter)</td></tr>
<tr><td></td><td colspan="32">连接时间戳 (Connection Timestamp)</td></tr>
<tr><td></td><td colspan="32">文件事件时间戳 (File Event Timestamp)</td></tr>
<tr><td></td><td colspan="32">源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）
源 IP 地址 (Source IP Address) （续）</td></tr>
<tr><td></td><td colspan="32">目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）
目标 IP 地址 (Destination IP Address) （续）</td></tr>
<tr><td></td><td colspan="8">处理结果 (Disposition)</td><td colspan="8">SPERO 处置情况 (SPERO Disposition)</td><td colspan="8">文件存储状态 (File Storage Status)</td><td colspan="8">文件分析状态 (File Analysis Status)</td></tr>
<tr><td></td><td colspan="8">本地恶意软件分析统计信息 (Local Malware Analysis Stat.)</td><td colspan="8">存档文件状态 (Archive File Status)</td><td colspan="8">威胁评分 (Threat Score)</td><td colspan="8">操作 (Action)</td></tr>
<tr><td></td><td colspan="32">SHA 散列 (SHA Hash)
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）
SHA 散列 (SHA Hash) （续）</td></tr>
<tr><td></td><td colspan="32">文件类型 ID (File Type ID)</td></tr>
<tr><td rowspan="3">文件名</td><td colspan="32">字符串块类型 (0) (String Block Type (0))</td></tr>
<tr><td colspan="32">字符串块长度 (String Block Length)</td></tr>
<tr><td colspan="32">文件名... (File Name...)</td></tr>
</table>

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	文件大小 (File Size)																															
	文件大小，续																															
	方向 (Direction)								应用 ID (Application ID)																							
	应用 ID (App ID)（续）								用户 ID																							
URI	用户 ID (User ID)（续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0))（续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)（续）								URI...																							
签名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	签名... (Signature...)																															
	源端口 (Source Port)																目的端口															
	协议 (Protocol)								访问控制策略 UUID (Access Control Policy UUID)																							
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (AC Pol UUID)（续）								源国家/地区 (Source Country)																目标国家/地区							
	目标国家/地区 (Dst. Country)（续）								Web 应用 ID (Web Application ID)																							
	Web 应用ID (Web App. ID)（续）								客户端应用 ID (Client Application ID)																							
	客户端应用ID (Client App. ID)（续）								安全情景 (Security Context)																							
	安全情景 (Security Context)（续）																															
	安全情景 (Security Context)（续）																															



下表对文件事件数据块中的字段进行了说明。

表 3-45 用于 7.0+ 的文件事件数据块字段

字段	数据类型	说明 (Description)
文件事件块类型 (File Event Block	uint32	启动文件事件数据块。此值始终为 79。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE 文件包含恶意软件。 ▪ 4 - UNAVAILABLE 软件无法向 AMP 云发送请求以了解处置情况，或 AMP 云服务未响应此请求。 ▪ 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
SPERO 处置情况 (SPERO Disposition)	uint8	表示文件分析中是否使用了 SPERO 签名。如果值为 1、2 或 3，则表示使用了 SPERO 分析。如果是任何其他值，则表示未使用 SPERO 分析。

表 3-45　用于 7.0+ 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
文件存储状态 (File Storage Status)	uint8	文件的存储状态。可能的值如下： ▪ 1 - 文件已存储 ▪ 2 - 文件已存储 ▪ 3 - 无法存储文件 ▪ 4 - 无法存储文件 ▪ 5 - 无法存储文件 ▪ 6 - 无法存储文件 ▪ 7 - 无法存储文件 ▪ 8 - 文件太大 ▪ 9 - 文件太小 ▪ 10 - 无法存储文件 ▪ 11 - 文件未存储，无法获取处置情况

表 3-45 用于 7.0+ 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
文件分析状态 (File Analysis Status)	uint8	是否已发送该文件进行动态分析。可能的值如下: ▪ 0 - 未发送文件进行分析 ▪ 1 - 已发送进行分析 ▪ 2 - 已发送进行分析 ▪ 4 - 已发送进行分析 ▪ 5 - 发送失败 ▪ 6 - 发送失败 ▪ 7 - 发送失败 ▪ 8 - 发送失败 ▪ 9 - 文件太小 ▪ 10 - 文件太大 ▪ 11 - 已发送进行分析 ▪ 12 - 分析完成 ▪ 13 - 故障（网络问题） ▪ 14 - 故障（速率限制） ▪ 15 - 故障（文件太大） ▪ 16 - 故障（文件读取错误） ▪ 17 - 故障（内部库错误） ▪ 19 - 文件未发送，无法获取处置情况 ▪ 20 - 故障（无法运行文件） ▪ 21 - 故障（分析超时） ▪ 22 - 已发送进行分析 ▪ 23 - 文件传输文件容量已处理 - 由于无法将文件提交到沙盒进行分析而导致文件容量已处理（存储到传感器上） ▪ 25 - 文件传输服务器限制超出容量已处理 - 服务器上的速率限制导致文件容量已处理 ▪ 26 - 通信故障 - 云连接故障导致文件容量已处理 ▪ 27 - 未发送 - 因配置原因导致文件未发送 ▪ 28 - 预分类不匹配 - 未发送文件进行动态分析，因为预分类在文件中未找到任何嵌入式或可疑对象 ▪ 29 - 传输已发送沙盒私有云 - 已将文件发送到私有云进行动态分析 ▪ 30 - 传输未发送沙盒私有云 - 未将文件发送到私有云进行分析
本地恶意软件分析状态 (Local Malware Analysis Status)	uint8	文件的恶意软件分析状态。可能的值包括: ▪ 0 - 文件未分析 ▪ 1 - 分析完成 ▪ 2 - 分析失败 ▪ 3 - 手动分析请求

表 3-45　用于 7.0+ 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
存档文件状态 (Archive File Status)	uint8	正在被检测的存档的状态。可能会有以下值： ▪ 0 - 不适用 - 文件没有被作为存档进行检测 ▪ 1 - 待处理 - 正在检测存档 ▪ 2 - 提取 - 已成功检测，且无任何问题 ▪ 3 - 失败 - 检测失败，系统资源不足 ▪ 4 - 超出深度 - 成功，但存档超出了嵌套的检测深度 ▪ 5 - 加密 - 部分成功，存档已加密或包含加密的存档 ▪ 6 - 无法检出 - 部分成功，文件可能已变形或损坏
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表 ▪ 6 - 云查找超时 ▪ 7 - 自定义检测 ▪ 8 - 自定义检测阻止 ▪ 9 - 存档阻止（超出深度） ▪ 10 - 存档阻止（已加密） ▪ 11 - 存档阻止（检查失败）
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-40 页。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小（字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值： ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。

表 3-45 用于 7.0+ 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
用户 ID	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。
签名	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 3-45　用于 7.0+ 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
字符串块类型 (String Block Type)	uint32	启动包含存档 SHA 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档 SHA 字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。

表 3-45 用于 7.0+ 的文件事件数据块字段 （续）

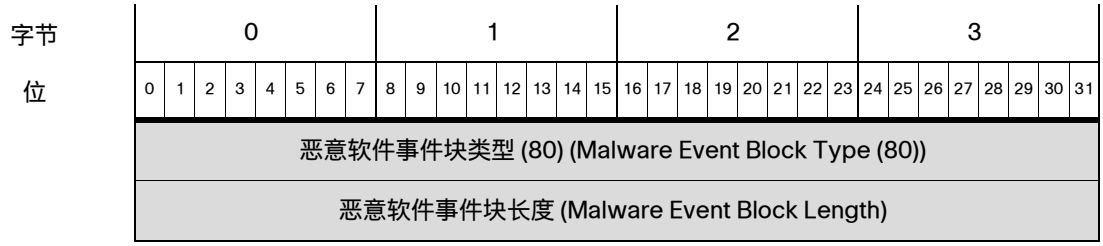
字段	数据类型	说明 (Description)
存档 SHA (Archive SHA)	字符串	包含该文件的父存档的 SHA1 散列。
字符串块类型 (String Block Type)	uint32	启动包含“存档名称”(Archive Name) 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上入侵策略名称中的字节数。
存档名称 (Archive Name)	字符串	父存档的名称。
存档深度 (Archive Depth)	uint8	嵌套文件的层数。例如，如果文本文件位于压缩存档中，则此值为 1。
HTTP 响应代码 (HTTP Response	uint32	HTTP 响应代码。
字符串块类型 (String Block Type)	uint32	启动包含入口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“入口 VRF ”(Ingress VRF) 名称字段中的字节数。
入口 VRF 名称	字符串	用于流量进入网络的虚拟路由器。
字符串块类型 (String Block Type)	uint32	启动包含出口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“出口 VRF ”(Egress VRF) 名称字段中的字节数。
出口 VRF 名称	字符串	用于流量离开网络的虚拟路由器。

恶意软件事件数据块 7.0+

eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 80。它替代了块 62。已添加虚拟路由和转发字段。

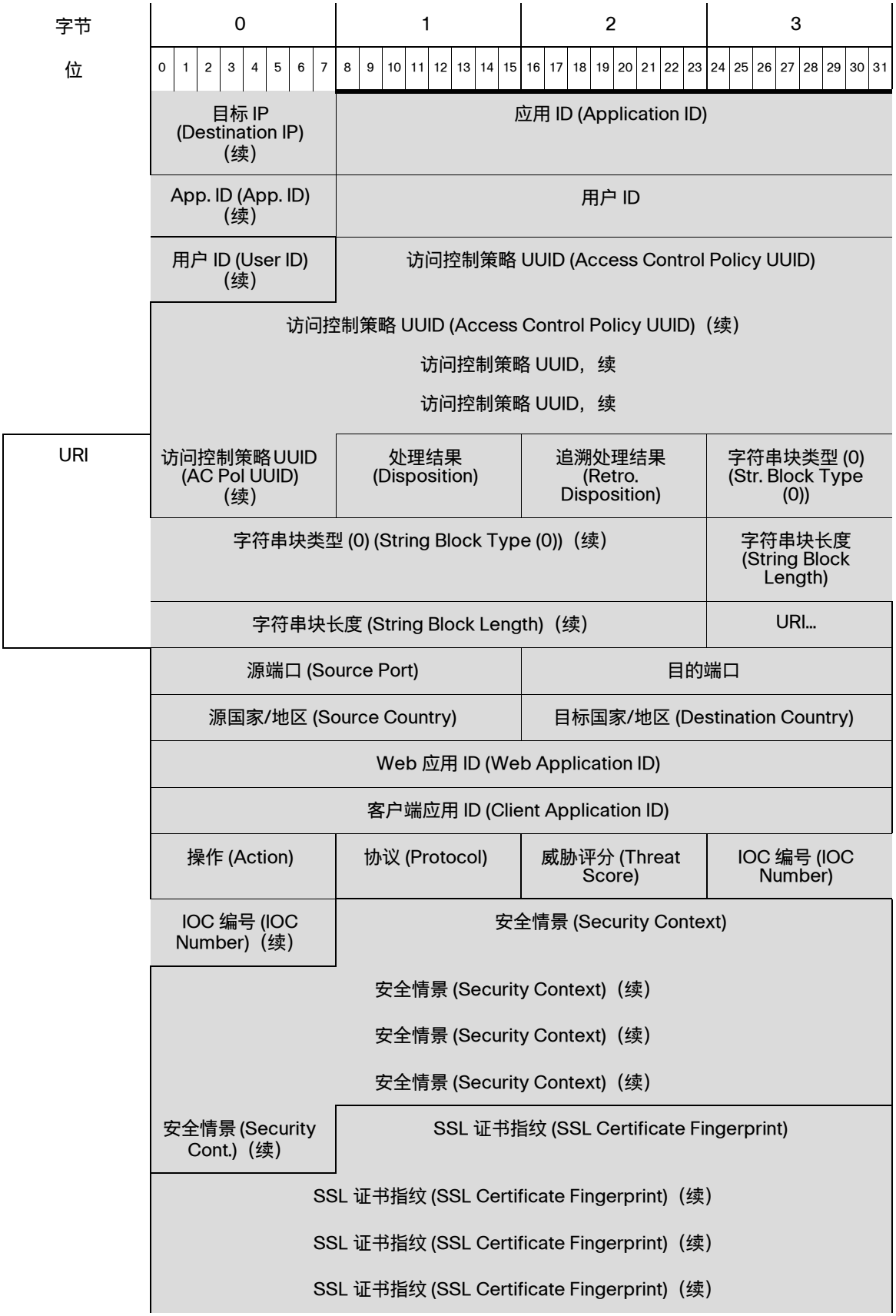
您可以通过在事件版本为 8 且事件代码为 101 的请求消息中设置恶意软件事件标志（“请求标志”(Request Flags) 字段中的位 30），将该事件作为恶意软件事件记录的一部分进行请求。

下图显示恶意软件事件数据块的结构。



字节	0				1			
位	0 1 2 3 4 5 6 7				8 9 10 11 12 13 14 15			
	代理 UUID (Agent UUID)							
	代理 UUID (Agent UUID)（续）							
	代理 UUID (Agent UUID)（续）							
	代理 UUID (Agent UUID)（续）							
	云 UUID (Cloud UUID)							
	云 UUID (Cloud UUID)（续）							
	云 UUID (Cloud UUID)（续）							
	云 UUID (Cloud UUID)（续）							
	恶意软件事件时间戳 (Malware Event Timestamp)							
	事件类型 ID (Event Type ID)							
	事件子类型 ID (Event Subtype ID)							
检测名称 (Detection Name)	检测器 ID (Detector ID)				字符串块类型 (0) (String Block Type (0))			
	字符串块类型 (0) (String Block Type (0))（续）				字符串块长度 (String Block Length)			
	字符串块长度 (String Block Length)（续）				检测名称... (Detection Name...)			
用户	字符串块类型 (0) (String Block Type (0))							
	字符串块长度 (String Block Length)							
	用户... (User...)							
文件名	字符串块类型 (0) (String Block Type (0))							
	字符串块长度 (String Block Length)							
	文件名... (File Name...)							
文件路径	字符串块类型 (0) (String Block Type (0))							
	字符串块长度 (String Block Length)							
	文件路径... (File Path...)							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列... (File SHA Hash...)																															
	文件大小 (File Size)																															
	面向终端的 AMP 文件类型 (File																															
	文件时间戳 (File Timestamp)																															
父文件名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件名... (Parent File Name...)																															
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列... (Parent File SHA Hash...)																															
事件说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件说明... (Event Description...)																															
	设备 ID (Device ID)																															
	连接实例 (Connection Instance)																连接计数器 (Connection Counter)															
	连接事件时间戳 (Connection Event Timestamp)																															
	方向 (Direction)								源 IP 地址 (Source IP Address)																							
	源 IP 地址 (Source IP Address)（续）																															
	来源 IP 地址，续																															
	来源 IP 地址，续																															
	源 IP (Source IP)（续）								目标 IP 地址 (Destination IP Address)																							
	目标 IP 地址 (Destination IP Address)（续）																															
	目标 IP 地址，续																															
	目标 IP 地址，续																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
目标 IP (Destination IP) (续)
应用 ID (Application ID)
App. ID (App. ID) (续)
用户 ID
用户 ID (User ID) (续)
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID，续
访问控制策略 UUID，续
URI
访问控制策略 UUID (AC Pol UUID) (续)
处理结果 (Disposition)
追溯处理结果 (Retro. Disposition)
字符串块类型 (0) (Str. Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
URI...
源端口 (Source Port)
目的端口
源国家/地区 (Source Country)
目标国家/地区 (Destination Country)
Web 应用 ID (Web Application ID)
客户端应用 ID (Client Application ID)
操作 (Action)
协议 (Protocol)
威胁评分 (Threat Score)
IOC 编号 (IOC Number)
IOC 编号 (IOC Number)（续）
安全情景 (Security Context)
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Cont.)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															
	SSL 证书指纹 (SSL Cert Fpt)（续）								SSL 实际操作 (SSL Actual Action)																SSL 流状态 (SSL Flow Status)							
存档 SHA	SSL 流状态 (SSL Flow Stat.)（续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (Str. Blk Type)（续）								字符串块类型 (0) (String Block Type (0))																							
	字符串长度 (Str. Length)（续）								存档 SHA... (Archive SHA...)																							
存档名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	存档名称... (Archive Name...)																															
	存档深度 (Archive Depth)								HTTP 响应 (HTTP Response)																							
入口 VRF	HTTP 响应 (HTTP Resp.)（续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (续)								字符串块长度 (String Block Length)																							
	字符串块长度 (Block Lgth)（续）								入口 VRF 名称																							
出口 VRF	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	出口 VRF 名称																															

下表对恶意软件事件数据块中的字段进行了说明。

表 3-46　用于 7.0+ 的恶意软件事件数据块字段

字段	数据类型	说明 (Description)
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。此值始终为 80。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的 AMP 云的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint32	导致恶意软件检测的操作的内部 ID。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“检测名称”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户”(User) 字段中的字节数。
用户	字符串	安装思科代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件名”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件路径”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。

表 3-46 用于 7.0+ 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件 SHA 散列”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小（字节）。
面向终端的 AMP 文件类型 (File	uint32	被检测或隔离文件的文件类型。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-40 页。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件名”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件 SHA 散列”(Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件说明”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。

表 3-46　用于 7.0+ 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值: ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE 文件包含恶意软件。 ▪ 4 - UNAVAILABLE 软件无法向 AMP 云发送请求以了解处置情况，或 AMP 云服务未响应此请求。 ▪ 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与“处置情况”(Disposition) 字段包含的值相同。可能值与“处置情况”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。

表 3-46 用于 7.0+ 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值: ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表 ▪ 6 - 云查找超时 ▪ 7 - 自定义检测 ▪ 8 - 自定义检测阻止 ▪ 9 - 存档阻止（超出深度） ▪ 10 - 存档阻止（已加密） ▪ 11 - 存档阻止（检查失败）
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 3-46　用于 7.0+ 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
字符串块类型 (String Block Type)	uint32	启动包含存档 SHA 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档 SHA 字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。

表 3-46 用于 7.0+ 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
存档 SHA (Archive SHA)	字符串	包含该文件的父存档的 SHA1 散列。
字符串块类型 (String Block Type)	uint32	启动包含“存档名称”(Archive Name) 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上入侵策略名称中的字节数。
存档名称 (Archive Name)	字符串	父存档的名称。
存档深度 (Archive Depth)	uint8	嵌套文件的层数。例如，如果文本文件位于压缩存档中，则此值为 1。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。
字符串块类型 (String Block Type)	uint32	启动包含入口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“入口 VRF ”(Ingress VRF) 名称字段中的字节数。
入口 VRF 名称	字符串	用于流量进入网络的虚拟路由器。
字符串块类型 (String Block Type)	uint32	启动包含出口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“出口 VRF ”(Egress VRF) 名称字段中的字节数。
出口 VRF 名称	字符串	用于流量离开网络的虚拟路由器。

用于 5.3+ 的文件事件 SHA 散列

eStreamer 服务使用文件事件 SHA 散列数据块以包含文件的 SHA 散列到其文件名的映射的元数据。块类型为系列 2 数据块列表中的 40。如果已在扩展请求中请求文件日志事件（事件代码为 111）且已设置位 20 或已请求元数据（事件版本为 5，事件代码为 21），则可以请求它。

下图显示文件事件散列数据块的结构：

下表对文件事件 SHA 散列数据块中的字段进行了说明。

表 3-47　　文件事件 SHA 散列块字段

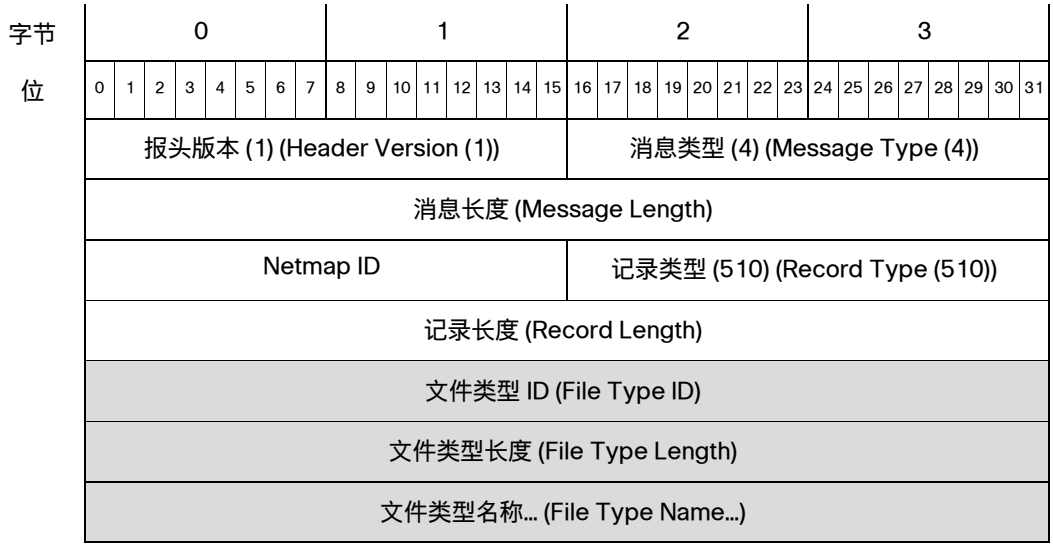
字段	数据类型	说明 (Description)
文件事件 SHA 散列块类型 (File Event SHA Hash Block Type)	uint32	启动文件事件 SHA 散列块。值始终为 40。
文件事件 SHA 散列块长度 (File Event SHA Hash Block Length)	uint32	文件事件 SHA 散列块中的字节总数，包括文件事件 SHA 散列块类型和长度字段的八个字节，加上随后的数据的字节数。
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
字符串块类型 (String Block Type)	uint32	启动包含与文件相关的描述性名称的字符串数据块。值始终为 0。

表 3-47 文件事件 SHA 散列块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
文件名或处置情况 (File Name or Disposition)	字符串	文件的描述性名称或处置情况。如果文件是安全的，则值为 `Clean`。如果文件的处置情况未知，则值为 `Neutral`。如果文件包含恶意软件，则提供文件名。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ `1` - CLEAN 文件是安全的，不包含恶意软件。 ▪ `2` - UNKNOWN 不确定文件是否包含恶意软件。 ▪ `3` - MALWARE 文件包含恶意软件。 ▪ `4` - UNAVAILABLE 软件无法向 AMP 云发送请求以了解处置情况，或 AMP 云服务未响应此请求。 ▪ `5` - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理
用户定义 (User Defined)	uint8	指示文件名提供的方式: ▪ `0` - 由 AMP 定义 ▪ `1` - 用户定义

用于 5.3+ 的文件类型 ID 元数据

eStreamer 服务可传输包含具有文件类型 ID 的事件的文件类型信息的元数据，格式如下所示。此记录将文件类型 ID 映射到文件类型名称。当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，则发送文件类型 ID 信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在消息长度 (Message Length) 字段后面）的值为 `510`，表示文件类型 ID 记录。



下表对文件类型 ID 记录中的字段进行了说明。

表 3-48　　文件类型 ID 记录字段

字段	数据类型	说明 (Description)
文件类型 ID (File Type ID)	uint32	文件类型 ID 号码。 此字段是此记录的唯一密钥。
文件类型长度 (File Type Length)	uint32	文件类型名称中包含的字节数。
文件类型名称 (File Type Name)	字符串	文件类型的描述性名称。

用于 5.2+ 的规则文档数据块

eStreamer 服务使用规则文档数据块包含用于生成警报的规则的相关信息。块类型为系列 2 数据块组中的 27。它可以通过类型为 10 的主机请求消息进行请求。有关详细信息，请参阅主机请求消息格式，第 2-24 页。

下图显示规则文档数据块的结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	规则文档块类型 (27) (Rule Documentation Block Type (27))																															
	规则文档块长度 (Rule Documentation Block Length)																															
	签名 ID (Signature ID)																															
	生成器 ID (Generator ID)																															
	修订 (Revision)																															
摘要	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	摘要... (Summary...)																															
影响 (Impact)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	影响... (Impact...)																															
详细信息 (Detailed Info)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	详细信息 (Detailed Information)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
受影响系统 (Affected Systems)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	受影响系统... (Affected Systems...)																															
攻击情景 (Attack Scenarios)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	攻击情景... (Attack Scenarios...)																															
易攻击性 (Ease of Attack)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	易攻击性... (Ease of Attack...)																															
误报率	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	错误的正误差率... (False Positives...)																															
错误的负误差率 (False Negatives)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	错误的负误差率... (False Negatives...)																															
纠正措施 (Corrective Action)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	纠正措施... (Corrective Action...)																															
贡献者	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	参与者... (Contributors...)																															
其他参考资料	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	其他参考资料... (Additional References...)																															

下表对规则文档数据块中的字段进行了说明。

表 3-49　　规则文档数据块字段

字段	数据类型	说明 (Description)
规则文档数据块类型 (Rule Documentation Data Block Type)	uint32	启动规则文档数据块。值始终为 27。
规则文档数据块长度 (Rule Documentation Data Block Length)	uint32	规则文档数据块中的字节总数，包括规则文档数据块类型和长度字段的八个字节，加上随后的数据字节数。
规则 ID（签名 ID) (Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Cisco Secure Firewall 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的摘要的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“摘要”(Summary) 字段中的字节数。
摘要 (Summary)	字符串	威胁或漏洞的说明。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的影响的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上影响 (Impact) 字段中的字节数。
影响 (Impact)	字符串	使用此漏洞的威胁可能影响各种系统的程度。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的详细信息的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“详细信息”(Detailed Information) 字段中的字节数。
详细信息 (Detailed Information)	字符串	有关潜在漏洞、规则实际针对的对象、受影响的系统的信息。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的受影响系统列表的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“受影响系统”(Affected Systems) 字段中的字节数。
受影响系统 (Affected Systems)	字符串	受漏洞影响的系统。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的可能攻击情景的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“攻击情景”(Attack Scenarios) 字段中的字节数。

表 3-49 规则文档数据块字段 （续）

字段	数据类型	说明 (Description)
攻击情景 (Attack Scenarios)	字符串	可能的攻击的示例。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的易攻击性的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“易攻击性”(Ease of Attack) 字段中的字节数。
易攻击性 (Ease of Attack)	字符串	攻击是被视为简单、中等、困难还是艰难，以及是否可以使用脚本执行此攻击。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的可能错误的正误差率的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“错误的正误差率”(False Positives) 字段中的字节数。
误报率 (False Positives)	字符串	可能导致误报的示例。默认值为 None Known。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的可能错误的负误差率的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“错误的负误差率”(False Negatives) 字段中的字节数。
错误的负误差率 (False Negatives)	字符串	可能导致漏报的示例。默认值为 None Known。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的纠正措施的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“纠正措施”(Corrective Action) 字段中的字节数。
纠正措施 (Corrective Action)	字符串	有关补丁、升级，或其他消除或缓解漏洞的信息。
字符串块类型 (String Block Type)	uint32	启动包含规则的参与者的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“参与者”(Contributors) 字段中的字节数。
贡献者 (Contributors)	字符串	规则和其他相关文档的作者的联系信息。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的其他参考资料的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“其他参考资料”(Additional References) 字段中的字节数。
其他参考资料 (Additional References)	字符串	更多信息和参考。

用于 6.0+ 的文件日志存储元数据

eStreamer 服务可传输包含文件日志存储信息的元数据。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 515，表示文件日志存储元数据记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (515)（Record Type (515))															
记录长度 (Record Length)																																
文件日志存储状态 (Filelog Storage Status)																																
文件日志存储状态说明长度 (Filelog Storage Status Description Length)																																
文件日志存储状态说明... (Filelog Storage Status Description...)																																

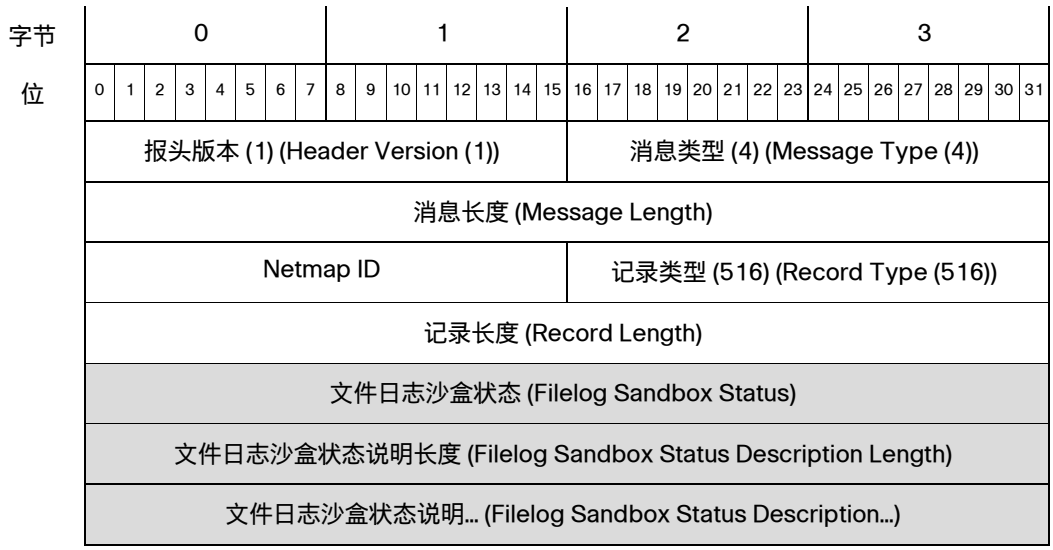
下表对文件日志存储元数据记录中的字段进行了说明。

表 3-50　　文件日志存储元数据记录字段

字段	数据类型	说明 (Description)
文件日志存储状态 (Filelog Storage Status)	uint32	指示文件日志存储状态的数字。此字段是此记录的唯一密钥。
文件日志存储状态说明长度 (Filelog Storage Status Description Length)	uint32	文件日志存储状态说明 (Filelog Storage Status Description) 中包含的字节数。
文件日志存储状态说明 (Filelog Storage Status Description)	字符串	文件日志存储状态的描述性名称。

用于 6.0+ 的文件日志沙盒元数据

eStreamer 服务可传输包含文件日志沙盒信息的元数据。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 516，表示文件日志沙盒元数据记录。



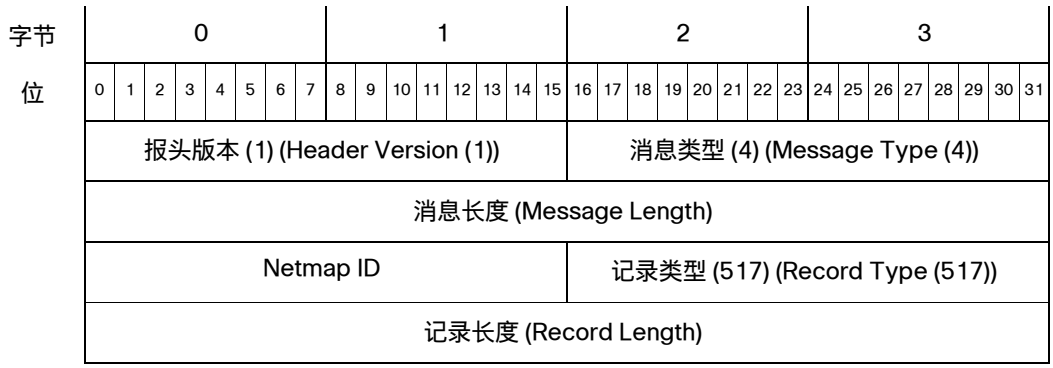
下表对文件日志沙盒元数据记录中的字段进行了说明。

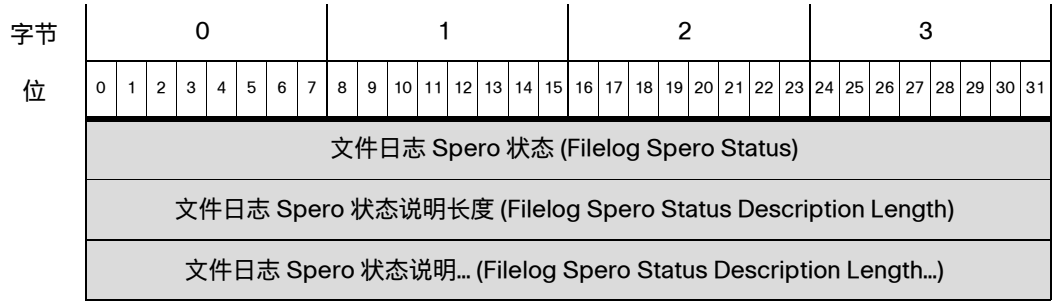
表 3-51 文件日志沙盒元数据记录字段

字段	数据类型	说明 (Description)
文件日志沙盒状态 (Filelog Sandbox Status)	uint32	指示文件日志沙盒状态的数字。此字段是此记录的唯一密钥。
文件日志沙盒状态说明长度 (Filelog Sandbox Status Description Length)	uint32	“文件日志沙盒状态说明”(Filelog Sandbox Status Description) 中包含的字节数。
文件日志沙盒状态说明 (Filelog Sandbox Status Description)	字符串	文件日志沙盒状态的描述性名称。

用于 6.0+ 的文件日志 Spero 元数据

eStreamer 服务可传输包含文件日志 spero 信息的元数据。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 `517`，表示文件日志 spero 元数据记录。





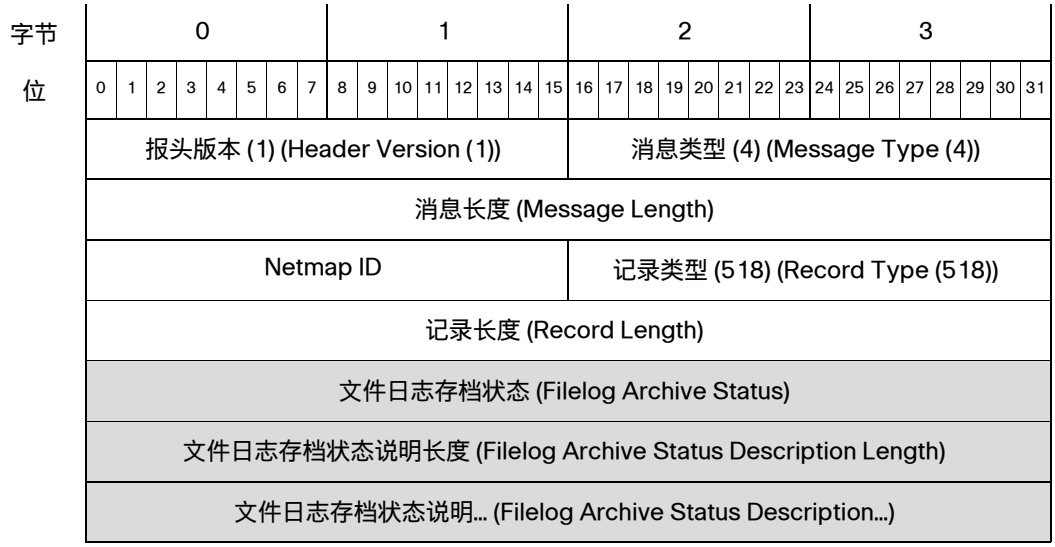
下表对文件日志 Spero 元数据记录中的字段进行了说明。

表 3-52　　文件日志 Spero 元数据记录字段

字段	数据类型	说明 (Description)
文件日志 Spero 状态 (Filelog Spero Status)	uint32	指示文件日志 spero 状态的数字。此字段是此记录的唯一密钥。
文件日志 Spero 状态说明长度 (Filelog Spero Status Description Length)	uint32	“文件日志 Spero 状态说明”(Filelog Spero Status Description Length) 中包含的字节数。
文件日志 Spero 状态说明 (Filelog Spero Status Description Length)	字符串	文件日志 spero 状态的描述性名称。

用于 6.0+ 的文件日志存档元数据

eStreamer 服务可传输包含文件日志存档信息的元数据。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 `518`，表示文件日志存档元数据记录。



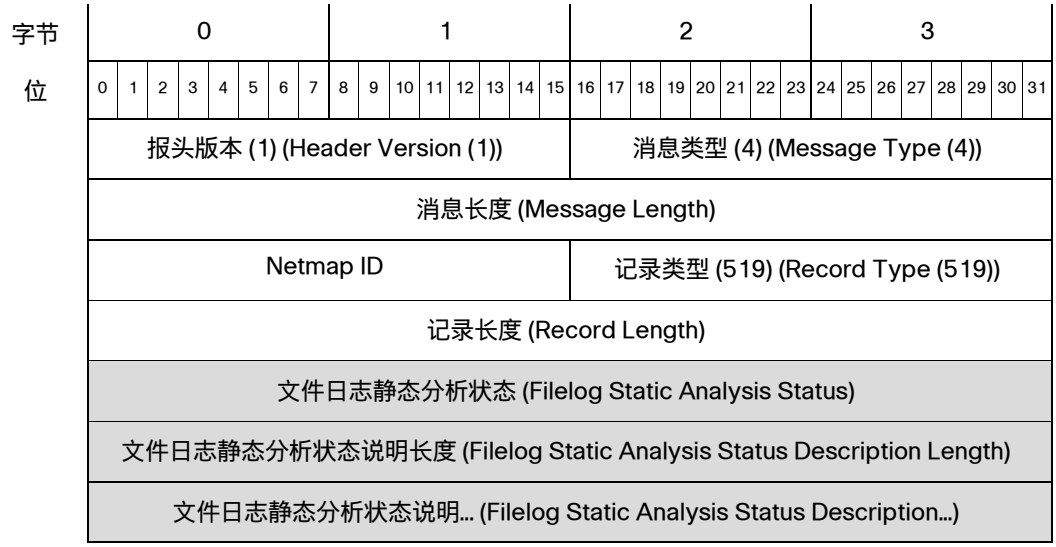
下表对文件日志存档元数据记录中的字段进行了说明。

表 3-53 文件日志存档元数据记录字段

字段	数据类型	说明 (Description)
文件日志存档状态 (Filelog Archive Status)	uint32	指示文件日志存档状态的数字。此字段是此记录的唯一密钥。
文件日志存档状态说明长度 (Filelog Archive Status Description Length)	uint32	“文件日志存档状态说明”(Filelog Archive Status Description) 中包含的字节数。
文件日志存档状态说明 (Filelog Archive Status Description)	字符串	文件日志存档状态的描述性名称。

用于 6.0+ 的文件日志静态分析元数据

eStreamer 服务可传输包含文件日志静态分析信息的元数据。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 519，表示文件日志静态分析元数据记录。



下表对文件日志静态分析元数据记录中的字段进行了说明。

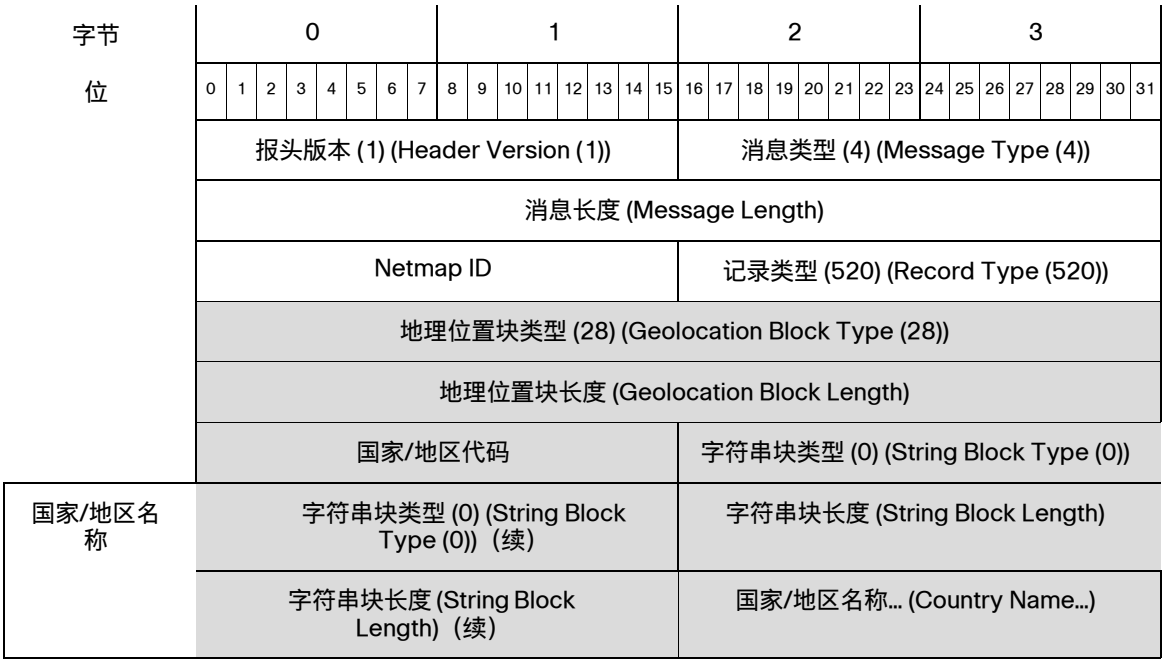
表 3-54　　文件日志静态分析元数据记录字段

字段	数据类型	说明 (Description)
文件日志静态分析状态 (Filelog Static Analysis Status)	uint32	指示文件日志静态分析状态的数字。此字段是此记录的唯一密钥。
文件日志静态分析状态说明长度 (Filelog Static Analysis Status Description Length)	uint32	文件日志静态分析状态说明 (Filelog Static Analysis Status Description) 中包含的字节数。
文件日志静态分析状态说明 (Filelog Static Analysis Status Description)	字符串	文件日志静态分析状态的描述性名称。

用于 5.2+ 的地理位置数据块

这是包含国家/地区代码到国家/地区名称的映射的数据块。此数据块的记录类型为系列 2 中的 520，块类型为系列 2 中的 28。它作为任何具有地理位置信息的事件的元数据显示。如果请求元数据，且事件中有国家/地区代码值，则系统将此数据块与其他元数据一起返回。

下图显示地理位置数据块的结构：



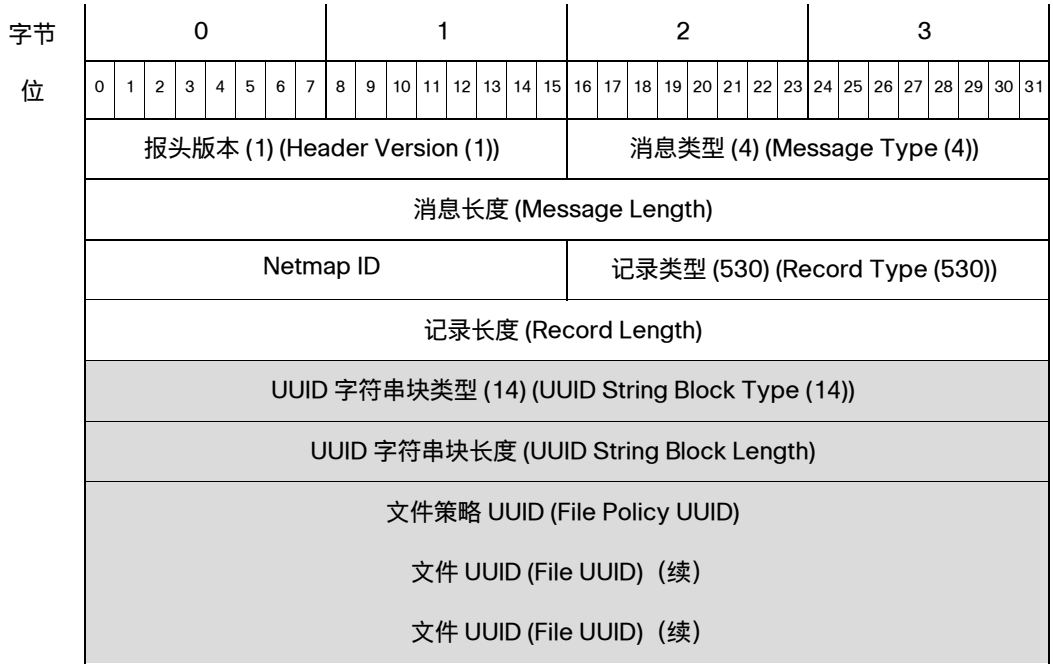
下表对地理位置数据块中的字段进行了说明。

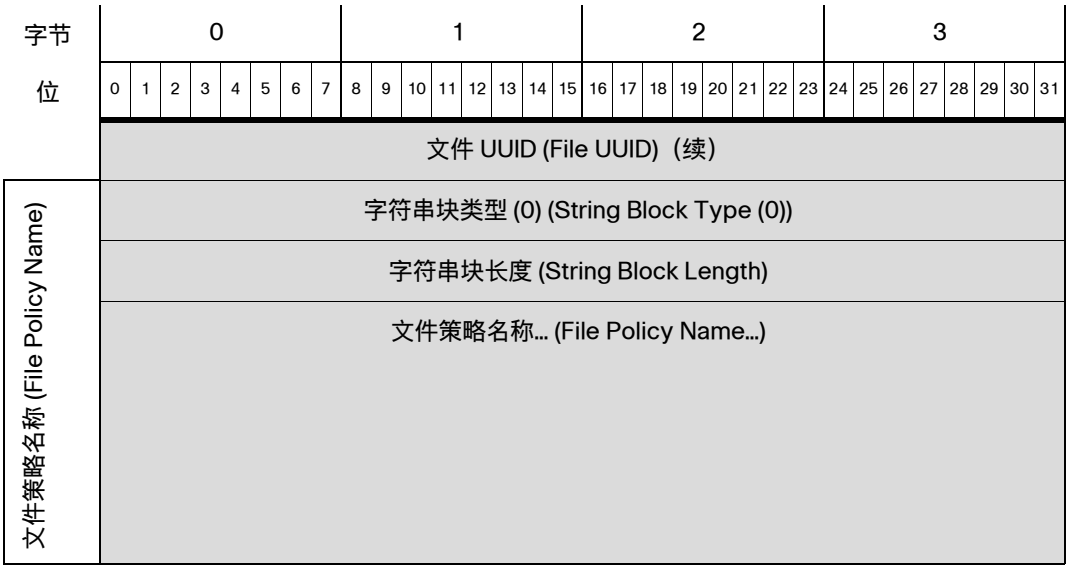
表 3-55　　地理位置数据块字段

字段	数据类型	说明 (Description)
地理位置数据块类型 (Geolocation Data Block Type)	uint32	启动地理位置数据块。值始终为 28。
地理位置数据块长度 (Geolocation Data Block Length)	uint32	地理位置数据块中的字节总数，包括地理位置数据块类型和长度字段的八个字节，加上随后的数据字节数。
国家/地区代码 (Country Code)	uint16	国家/地区代码。
字符串块类型 (String Block Type)	uint32	启动包含与国家/地区代码相关的国家/地区名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“国家/地区名称”(Country Name) 字段中的字节数。
国家/地区名称 (Country Name)	字符串	与国家/地区代码相关的国家/地区的名称。

用于 6.0+ 的文件策略名称

eStreamer 服务可传输包含文件策略名称信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送文件策略名称信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 530，表示文件策略名称记录。





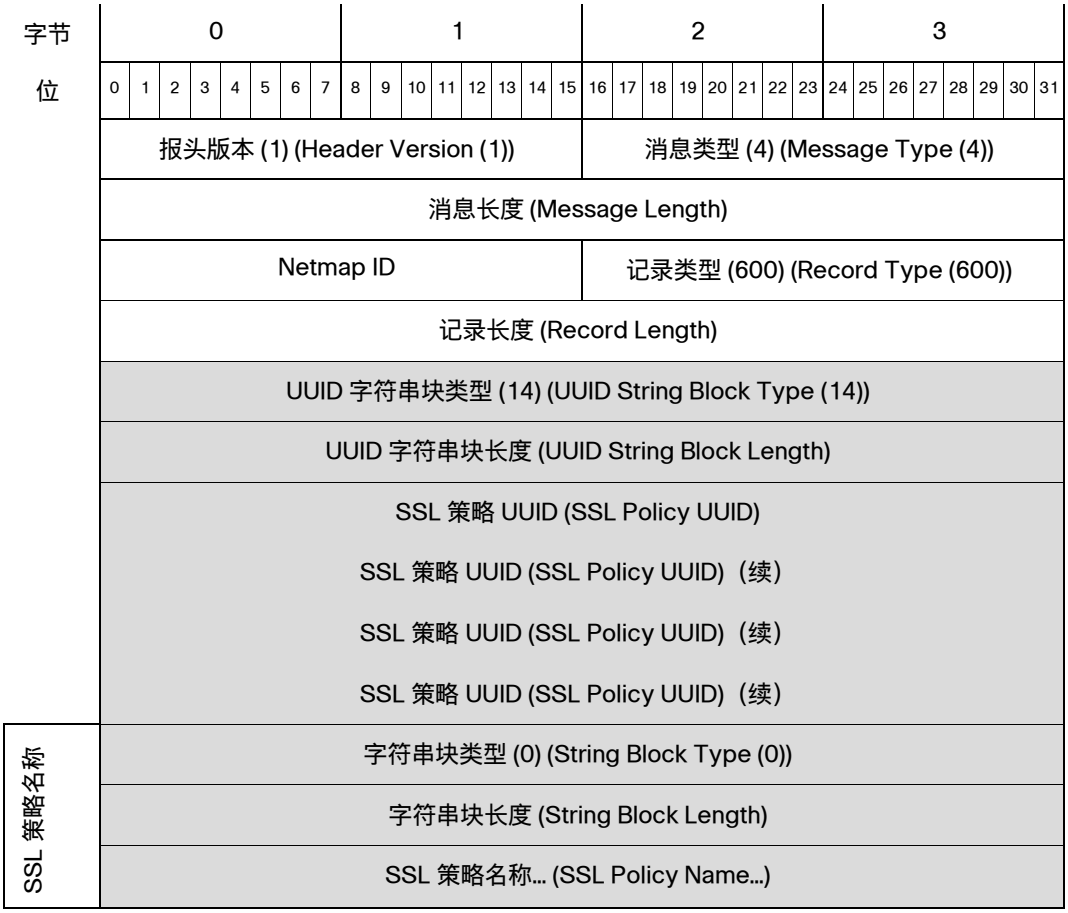
下表对文件策略名称记录中的字段进行了说明。

表 3-56　　文件策略名称字段

字段	数据类型	说明 (Description)
UUID 字符串数据块类型 (UUID String Data Block Type)	uint32	启动 UUID 字符串数据块。值始终为 14。
UUID 字符串数据块长度 (UUID String Data Block Length)	uint32	UUID 字符串数据块中的字节总数，包括 UUID 字符串数据块类型和长度字段的八个字节，加上随后的数据字节数。
文件策略 UUID (File Policy UUID)	uint8[16]	文件策略的 UUID。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含文件策略名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 文件策略字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上文件策略名称中的字节数。
文件策略名称 (File Policy Name)	字符串	文件策略的名称。

SSL 策略名称

eStreamer 服务可传输包含 SSL 策略名称信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送 SSL 策略名称信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 600，表示 SSL 策略名称记录。



下表对 SSL 策略名称记录中的字段进行了说明。

表 3-57 SSL 策略名称记录字段

字段	数据类型	说明 (Description)
UUID 字符串数据块类型 (UUID String Data Block Type)	uint32	启动 UUID 字符串数据块。值始终为 14。
UUID 字符串数据块长度 (UUID String Data Block Length)	uint32	UUID 字符串数据块中的字节总数，包括 UUID 字符串数据块类型和长度字段的八个字节，加上随后的数据字节数。
SSL 策略 UUID (SSL Policy UUID)	uint8[16]	SSL 策略的 UUID。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含 SSL 策略名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 策略名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 SSL 策略名称中的字节数。
SSL 策略名称 (SSL Policy Name)	字符串	SSL 策略的名称。

SSL 规则 ID

eStreamer 服务可传输包含 SSL 规则 ID 信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送 SSL 规则 ID 信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 601，表示 SSL 规则 ID 记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															
	Netmap ID																记录类型 (601) (Record Type (601))															
	记录长度 (Record Length)																															
	SSL 规则 ID 块类型 (51) (SSL Rule ID block type (51))																															
	SSL 规则 ID 块长度 (SSL Rule ID block length)																															
	修订版 (Revision)																															
	修订版 (Revision)（续）																															
	修订版 (Revision)（续）																															
	修订版 (Revision)（续）																															
	规则 ID (Rule ID)																															
规则名称 (Rule Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	规则名称... (Rule Name...)																															

下表对 SSL 规则 ID 记录中的字段进行了说明。

表 3-58　　SSL 策略名称记录字段

字段	数据类型	说明 (Description)
SSL 规则 ID 块类型 (SSL Rule ID Block Type)	uint32	SSL 规则 ID 数据块的块类型。值始终为 51•
SSL 规则 ID 块长度 (SSL Rule ID Block Length)	uint32	SSL 规则 ID 数据块中的字节数，包括块类型和报头字段的 8 个字节，加上 SSL 规则 ID 块中的字节数。

表 3-58 SSL 策略名称记录字段 （续）

字段	数据类型	说明 (Description)
修订版 (Revision)	uint8[16]	SSL 规则修订的 UUID。此字段与“规则 ID” (Rule ID) 一起构成此记录的唯一密钥。
规则 ID (Rule ID)	uint32	SSL 规则的 ID 号码。此字段与“修订” (Revision) 一起构成此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含 SSL 规则名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 规则名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 SSL 规则名称中的字节数。
SSL 规则名称	字符串	SSL 规则的名称。

SSL 密码套件 (SSL Cipher Suite)

eStreamer 服务可传输包含具有 SSL 密码 ID 的事件的 SSL 密码套件信息的元数据，格式如下所示。此记录将 SSL 密码 ID 映射到 SSL 密码套件名称。当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送 SSL 密码套件信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 602，表示 SSL 密码套件记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (602) (Record Type (602))															
记录长度 (Record Length)																																
SSL 密码 ID (SSL Cipher ID)																																
SSL 密码套件名称长度 (SSL Cipher Suite Name Length)																																
SSL 密码套件名称... (SSL Cipher Suite Name...)																																

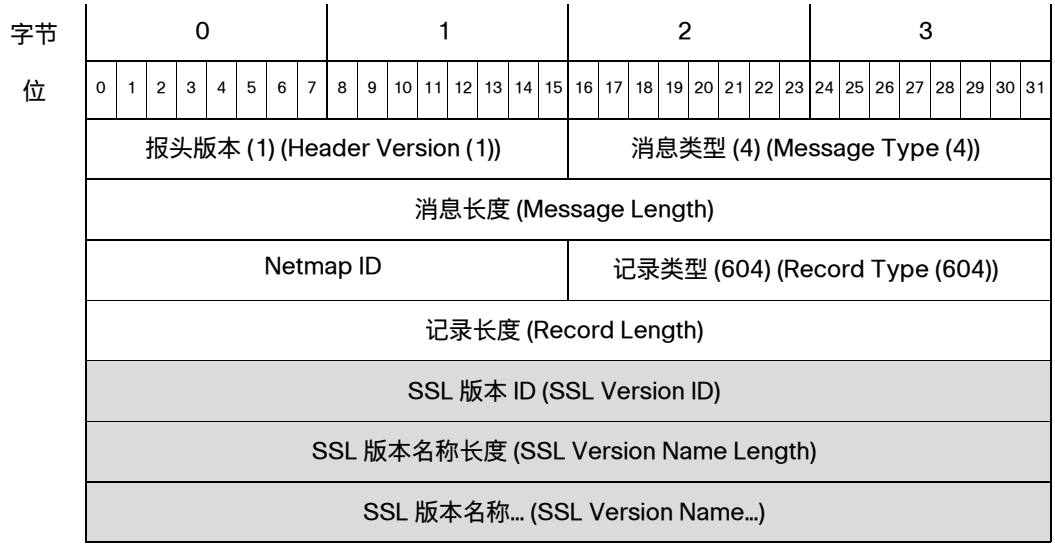
下表对 SSL 密码套件记录中的字段进行了说明。

表 3-59　SSL 密码套件字段

字段	数据类型	说明 (Description)
SSL 密码 ID (SSL Cipher ID)	uint32	SSL 密码 ID 号码。 此字段是此记录的唯一密钥。
SSL 密码套件名称长度 (SSL Cipher Suite Name Length)	uint32	SSL 密码套件名称中包含的字节数。
SSL 密码套件名称 (SSL Cipher Suite Name)	字符串	SSL 密码套件的描述性名称。

SSL 版本

eStreamer 服务可传输包含具有 SSL 版本的事件的 SSL 版本信息的元数据，格式如下所示。此记录将 SSL 版本 ID 映射到 SSL 版本名称。当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送 SSL 密码套件信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度” (Message Length) 字段后面）的值为 `604`，表示 SSL 版本记录。



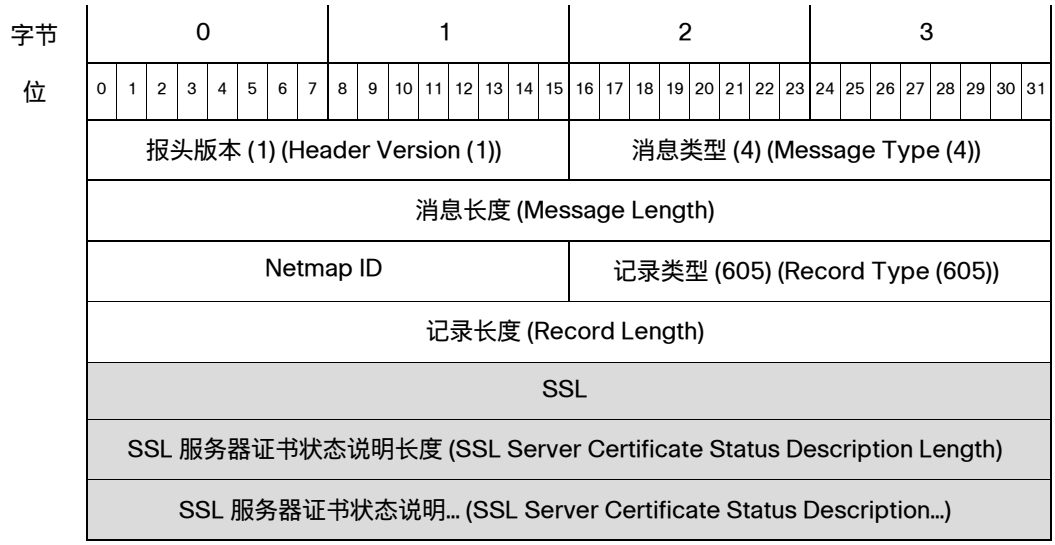
下表对 SSL 版本记录中的字段进行了说明。

表 3-60　SSL 版本字段

字段	数据类型	说明 (Description)
SSL 版本 ID (SSL Version ID)	uint32	SSL 版本 ID 号码。 此字段是此记录的唯一密钥。
SSL 版本名称 (SSL Version Name)	uint32	SSL 版本名称 (SSL Version Name) 中包含的字节数。
SSL 密码套件名称 (SSL Cipher Suite Name)	字符串	SSL 版本的描述性名称。

SSL 服务器证书状态

eStreamer 服务可传输包含 SSL 服务器证书状态信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送 SSL 服务器证书状态信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 605，表示 SSL 服务器证书状态记录。



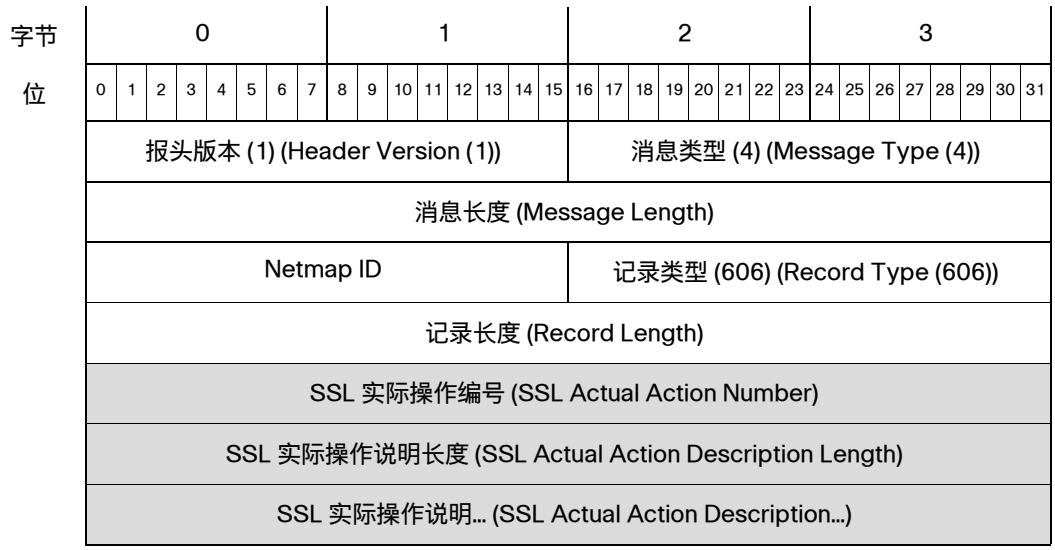
下表对 SSL 服务器证书状态记录中的字段进行了说明。

表 3-61 SSL 服务器证书状态记录字段

字段	数据类型	说明 (Description)
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 服务器证书状态编号。此字段是此记录的唯一密钥。
SSL 服务器证书状态说明长度 (SSL Server Certificate Status Description Length)	uint32	SSL 服务器证书状态说明 (SSL Server Certificate Status Description) 中包含的字节数。
SSL 服务器证书状态说明 (SSL Server Certificate Status Description)	字符串	对 SSL 服务器证书状态的说明。

SSL 实际操作

eStreamer 服务可传输包含 SSL 实际操作信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送 SSL 实际操作信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 606，表示 SSL 实际操作记录。



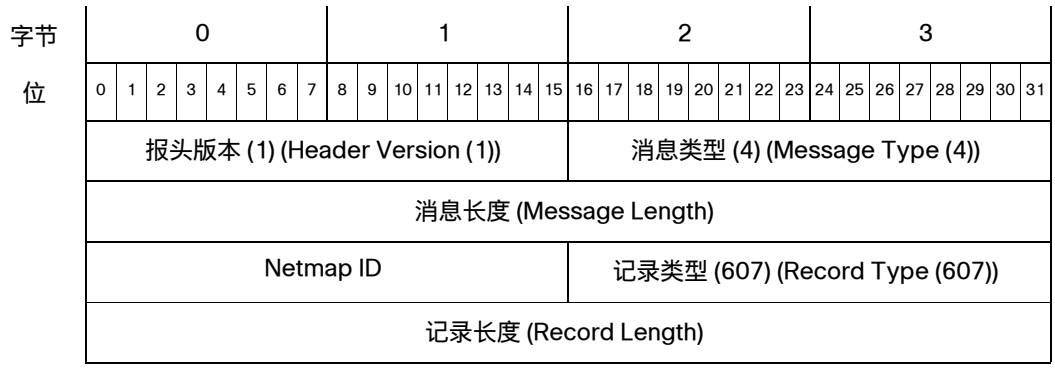
下表对 SSL 实际操作记录中的字段进行了说明。

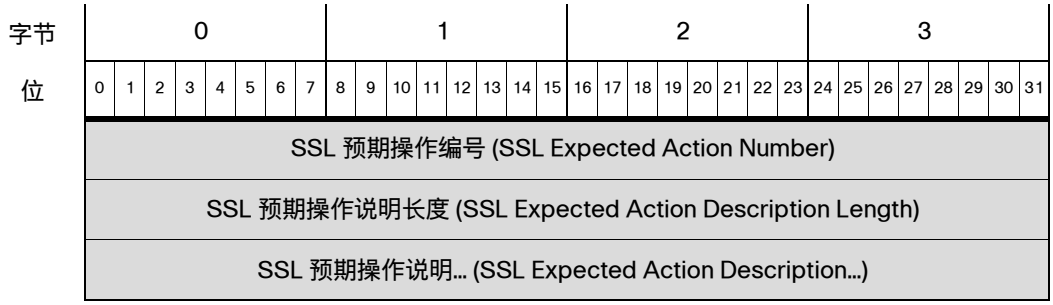
表 3-62　　SSL 实际操作字段

字段	数据类型	说明 (Description)
SSL 实际操作编号 (SSL Actual Action Number)	uint32	指示 SSL 实际操作的编号。此字段是此记录的唯一密钥。
SSL 实际操作说明长度 (SSL Actual Action Description Length)	uint32	SSL 实际操作说明 (SSL Actual Action Description) 中包含的字节数。
SSL 实际操作说明 (SSL Actual Action Description)	字符串	对 SSL 实际操作的说明。

SSL 预期操作

eStreamer 服务可传输包含 SSL 预期操作信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送 SSL 预期操作信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 `607`，表示 SSL 预期操作记录。





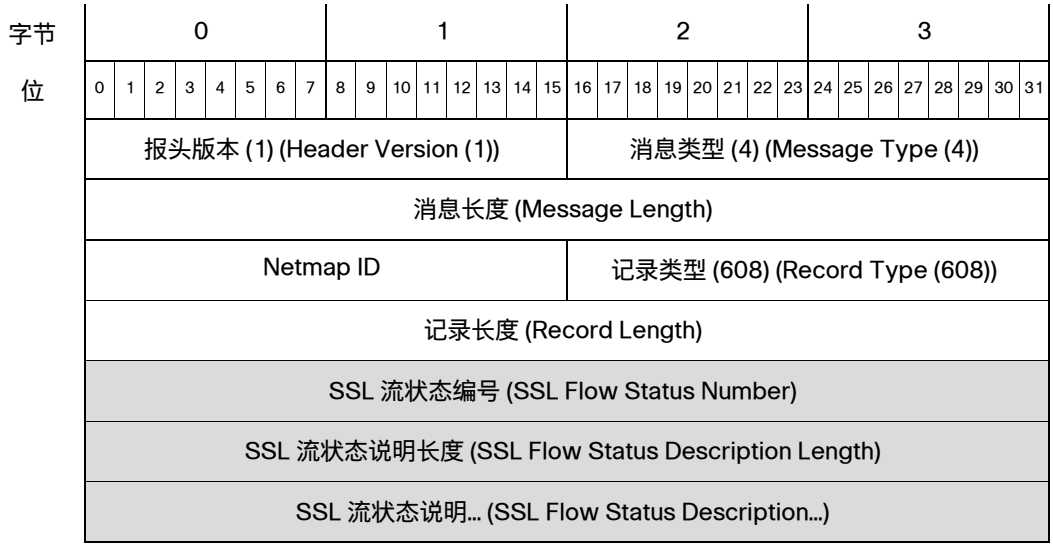
下表对 SSL 预期操作记录中的字段进行了说明。

表 3-63 SSL 实际操作字段

字段	数据类型	说明 (Description)
SSL 预期操作编号 (SSL Expected Action Number)	uint32	指示 SSL 预期操作的编号。此字段是此记录的唯一密钥。
SSL 预期操作说明长度 (SSL Expected Action Description Length)	uint32	SSL 预期操作说明 (SSL Expected Action Description) 中包含的字节数。
SSL 预期操作说明 (SSL Expected Action Description)	字符串	对 SSL 预期操作的说明。

SSL 流状态

eStreamer 服务可传输包含 SSL 流状态信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送 SSL 流状态信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 `608`，表示 SSL 流状态记录。



下表对 SSL 流状态记录中的字段进行了说明。

表 3-64　　SSL 流状态字段

字段	数据类型	说明 (Description)
SSL 流状态编号 (SSL Flow Status Number)	uint32	指示SSL流状态的编号。此字段是此记录的唯一密钥。
SSL 流状态说明长度 (SSL Flow Status Description Length)	uint32	SSL 流状态说明 (SSL Flow Status Description) 中包含的字节数。
SSL 流状态说明 (SSL Flow Status Description)	字符串	对 SSL 流状态的说明。

SSL URL 类别

eStreamer服务可传输包含SSL URL类别信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送 SSL URL 类别信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 613，表示 SSL URL 类别记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (613) (Record Type (613))															
记录长度 (Record Length)																																
SSL URL 类别编号 (SSL URL Category Number)																																
SSL URL 类别说明长度 (SSL URL Category Description Length)																																
SSL URL 类别说明... (SSL URL Category Description...)																																

下表对 SSL URL 类别记录中的字段进行了说明。

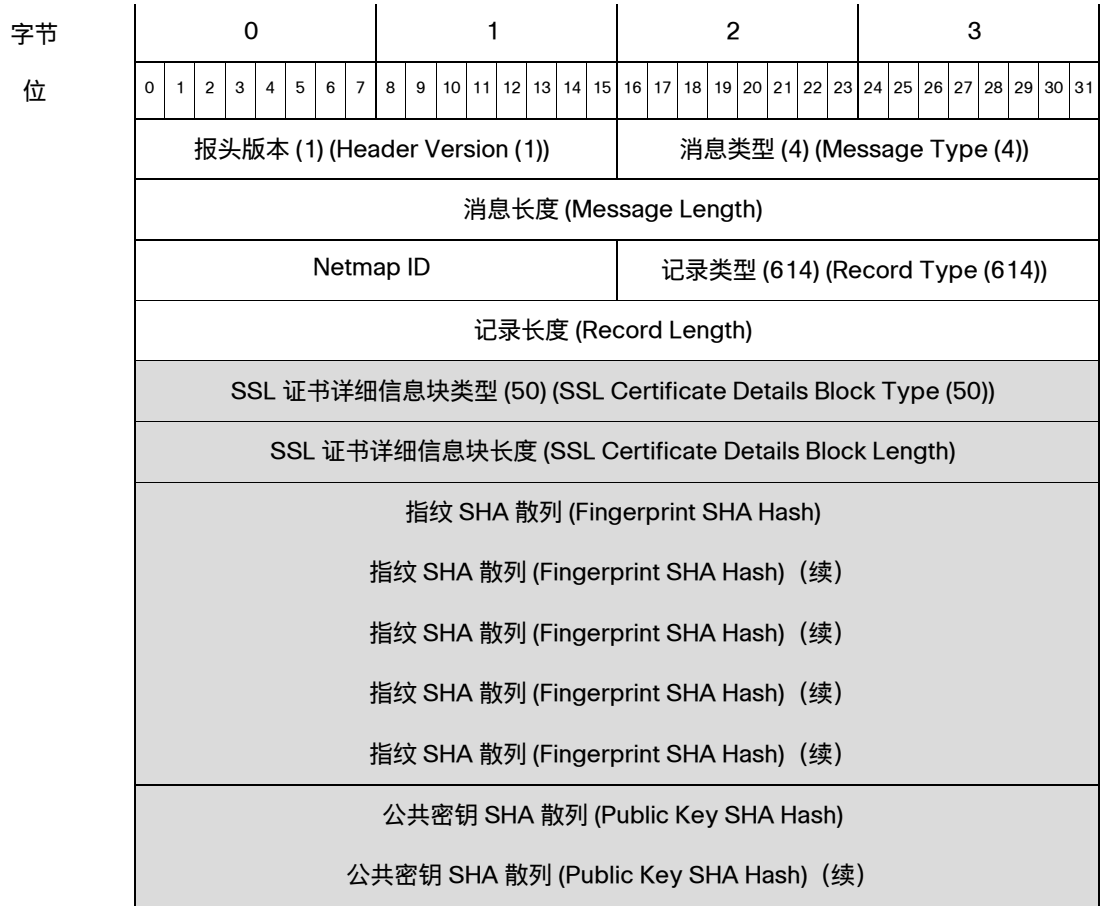
表 3-65 SSL URL 类别字段

字段	数据类型	说明 (Description)
SSL URL 类别编号 (SSL URL Category Number)	uint32	指示 SSL URL 类别的编号。此字段是此记录的唯一密钥。
SSL URL 类别说明长度 (SSL URL Category Description Length)	uint32	SSL 服务器 URL 类别说明中包含的字节数。
SSL URL 类别说明 (SSL URL Category Description)	字符串	对 SSL URL 类别的说明。

用于 5.4+ 的 SSL 证书详细信息数据块

此数据块提供有关 SSL 证书的详细信息。此数据块的记录类型为系列 2 中的 614，块类型为系列 2 中的 50。它作为任何具有 SSL 信息的事件的元数据显示。这些包括恶意软件事件、文件事件、入侵事件、连接事件以及关联事件。

下图显示 SSL 证书详细信息数据块的结构：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	公共密钥 SHA 散列 (Public Key SHA Hash)（续）																															
	公共密钥 SHA 散列 (Public Key SHA Hash)（续）																															
	公共密钥 SHA 散列 (Public Key SHA Hash)（续）																															
	序列号 (Serial Number)																															
	序列号 (Serial Number)（续）																															
	序列号 (Serial Number)（续）																															
	序列号 (Serial Number)（续）																															
	序列号 (Serial Number)（续）																															
	序列号长度 (Serial Number Length)																															
持有者常用名 (Subject Common Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	持有者常用名... (Subject Common Name...)																															
持有者组织 (Subject Organization)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	持有者组织... (Subject Organization...)																															
持有者组织单位 (Subject Organization Unit)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	持有者组织单位.... (Subject Organization Unit....)																															
持有者国家/地区 (Subject Country)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	持有者国家/地区... (Subject Country...)																															
颁发者常用名 (Issuer Common Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	颁发者常用名... (Issuer Common Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
颁发者组织 (Issuer Organization)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	颁发者组织... (Issuer Organization...)																															
颁发者组织单位 (Issuer Organizational Unit)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	颁发者组织单位... (Issuer Organizational Unit...)																															
颁发者国家/地区 (Issuer Country)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	颁发者国家/地区... (Issuer Country...)																															
	有效开始日期 (Valid Start Date)																															
	有效结束日期 (Valid End Date)																															

下表对 SSL 证书详细信息数据块中的字段进行了说明。

表 3-66 SSL 证书详细信息数据块字段

字段	数据类型	说明 (Description)
SSL 证书详细信息数据块类型 (SSL Certificate Details Data Block Type)	uint32	启动 SSL 证书详细信息数据块。值始终为 50。
SSL 证书详细信息数据块长度 (SSL Certificate Details Data Block Length)	uint32	SSL 证书详细信息数据块的字节总数，包括 SSL 证书详细信息数据块类型和长度字段的八个字节，加上随后的数据字节数。
指纹 SHA 散列 (Fingerprint SHA Hash)	uint8[20]	SSL 服务器证书的 SHA1 散列。
公共密钥 SHA 散列 (Public Key SHA Hash)	uint8[20]	用于对证书内所含公钥进行身份验证的 SHA 哈希值。
序列号 (Serial Number)	uint8[20]	由发行 CA 分配的序列号。尽管序列号的长度不能超过 20 个字节，但根据“序列号长度”(Serial Number Length) 字段中的规定，此值可能小于 20 个字节。

表 3-66　SSL 证书详细信息数据块字段 （续）

字段	数据类型	说明 (Description)
序列号长度 (Serial Number Length)	uint32	序列号的长度，以字节为单位。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的类别的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“类别”(Category) 字段中的字节数。
持有者常用名 (Subject Common Name)	字符串	SSL证书的持有者常用名。这通常是证书持有者的主机和域名，但也可能包含其他信息。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的事件类型的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件类型”(Event Type) 字段中的字节数。
持有者组织 (Subject Organization)	字符串	证书持有者的组织。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的事件类型的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件类型”(Event Type) 字段中的字节数。
持有者组织单位 (Subject Organization Unit)	字符串	证书持有者的组织单位。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的事件类型的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件类型”(Event Type) 字段中的字节数。
持有者国家/地区 (Subject Country)	字符串	证书持有者所在的国家/地区。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的类别的字符串数据块。值始终为 0。

表 3-66 SSL 证书详细信息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“类别”(Category) 字段中的字节数。
颁发者常用名 (Issuer Common Name)	字符串	SSL证书的颁发者常用名。这通常是证书颁发者的主机和域名，但也可能包含其他信息。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的事件类型的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件类型”(Event Type) 字段中的字节数。
颁发者组织 (Issuer Organization)	字符串	证书颁发者的组织。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的事件类型的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件类型”(Event Type) 字段中的字节数。
颁发者组织单位 (Issuer Organizational Unit)	字符串	证书颁发者的组织单位。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的事件类型的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件类型”(Event Type) 字段中的字节数。
颁发者国家/地区 (Issuer Country)	字符串	证书颁发者所在的国家/地区。
有效开始日期 (Valid Start Date)	uint32	颁发证书时的 Unix 时间戳。
有效结束日期 (Valid End Date)	uint32	证书停止有效的 Unix 时间戳。

网络分析策略名称记录

eStreamer 服务可传输包含网络分析策略名称信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送网络分析策略名称信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 700，表示网络分析策略名称记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															
	Netmap ID																记录类型 (700) (Record Type (700))															
	记录长度 (Record Length)																															
	UUID 字符串块类型 (14) (UUID String Block Type (14))																															
	UUID 字符串块长度 (UUID String Block Length)																															
	网络分析策略 UUID (Network Analysis Policy UUID) 网络分析 UUID (Network Analysis UUID)（续） 网络分析 UUID (Network Analysis UUID)（续） 网络分析 UUID (Network Analysis UUID)（续）																															
网络分析策略名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	网络分析策略名称... (Network Analysis Policy Name...)																															

下表对网络分析策略名称记录中的字段进行了说明。

表 3-67　　网络分析策略名称记录字段

字段	数据类型	说明 (Description)
UUID 字符串数据块类型 (UUID String Data Block Type)	uint32	启动 UUID 字符串数据块。值始终为 14。
UUID 字符串数据块长度 (UUID String Data Block Length)	uint32	UUID 字符串数据块中的字节总数，包括 UUID 字符串数据块类型和长度字段的八个字节，加上随后的数据字节数。

表 3-67 网络分析策略名称记录字段 （续）

字段	数据类型	说明 (Description)
网络分析策略 UUID (Network Analysis Policy UUID)	uint8[16]	网络分析策略的 UUID。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含网络分析策略名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	网络分析策略名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上网络分析策略名称中的字节数。
网络分析策略名称 (Network Analysis Policy Name)	字符串	网络分析策略的名称。

了解发现和连接数据结构

本章提供有关发现和连接事件的 eStreamer 消息中使用的数据结构以及这些事件的元数据的详细信息。发现和连接事件消息使用相同的通用消息格式以及数据块系列；区别在于数据块本身的内容。

发现事件包含两个事件子类别：

- 主机发现事件，识别受管网络上的新主机和更改主机，包括从数据包的内容中检测到的主机上运行的应用，以及主机漏洞。
- 用户事件，报告检测到的新用户及用户活动，如登录。

连接事件报告有关被监控主机与所有其他主机之间的会话流量的信息。连接信息包括事务的第一个和最后一个数据包、源 IP 地址和目标 IP 地址、源端口和目标端口以及发送和接收的数据包数和字节数。如适用，连接事件也报告会话中涉及的客户端应用和 URL。

有关从 eStreamer 服务器请求发现或连接事件的信息，请参阅请求标志，第 2-12 页。

有关 eStreamer 事件数据消息的通用结构的信息，请参阅了解事件数据消息的组织，第 2-17 页。

有关发现和连接事件数据结构的详细信息，请参阅本章中的以下各节：

- 发现和连接事件数据消息，第 4-2 页提供 eStreamer 用于主机发现、用户以及连接消息的结构的高级视图。
- 发现和连接事件记录类型，第 4-2 页对发现和连接事件的记录类型进行了说明。
- 发现事件的元数据，第 4-5 页介绍要将数字和编码数据转换成文本（例如，将事件中的用户 ID 转换成用户名）并可以向其请求情景信息的元数据记录。
- 发现事件报头 5.2+，第 4-38 页对所有发现和连接消息中使用的标准事件报头的结构，以及事件类型和事件子类型字段中可能出现的值进行了说明。事件类型和子类型字段进一步定义消息中包含的数据记录的结构。
- 按事件类型划分的主机发现结构，第 4-42 页对 eStreamer 用于各种主机发现事件类型的数据记录的结构进行了说明。
- 按事件类型划分的用户数据结构，第 4-58 页对 eStreamer 用于各种用户事件类型的数据记录的结构进行了说明。
- 了解发现（系列 1）块，第 4-60 页对用于在发现和连接事件消息中传输复杂记录的数据块结构系列进行了说明。关联事件中也有系列 1 数据块。
- 用户漏洞数据块 5.0+，第 4-159 页对用于传输复杂用户事件记录的其他系列 1 数据块结构进行了说明。

提示 请参阅“数据结构示例”节，第 A-1 页了解说明样本发现事件的示例。

发现和连接事件数据消息

eStreamer 采用相同的消息结构来打包发现和连接事件的数据，该结构包含：

- 选项 netmap ID
- 定义记录类型的记录报头
- 识别和描述事件并明确标识事件类型和子类型的发现事件报头。有关信息，请参阅发现事件报头 5.2+，第 4-38 页。
- 由块报头和数据块组成的数据记录。发现和连接事件数据消息使用系列 1 数据块。有关信息，请参阅主机发现和连接数据块，第 4-60 页或用户漏洞数据块 5.0+，第 4-159 页。

发现和连接事件记录类型

下表列出了主机发现和连接事件的事件记录类型，并提供到每个记录类型的事件消息结构的链接。该列表还包含元数据记录类型。有些记录包含存储特定数据段的数据块。这些数据块分为包含大多数数据类型的系列 1 数据块和专门包含发现数据的系列 2 数据块。该表还指示每个版本的状态（当前版本或旧版本）。当前记录是最新版本。旧记录已被较新的版本替代，但仍可以从 eStreamer 中请求旧记录。

表 4-1 发现和连接事件记录类型

记录类型	包含块类型	系列	说明 (Description)	记录状态	…中描述的数据格式
10	139	1	检测到的新主机	当前	新主机消息与主机上次查看时间消息，第 4-43 页
11	103	1	新 TCP 服务器	当前	服务器消息，第 4-44 页
12	103	1	新 UDP 服务器	当前	服务器消息，第 4-44 页
13	4	1	新网络协议	当前	新网络协议消息，第 4-45 页
14	4	1	新传输协议	当前	新传输协议消息，第 4-45 页
15	122	1	新客户端应用	当前	客户端应用消息，第 4-45 页
16	103	1	TCP 服务器信息更新	当前	服务器消息，第 4-44 页
17	103	1	UDP 服务器信息更新	当前	服务器消息，第 4-44 页
18	53	1	操作系统信息更新	当前	操作系统更新消息，第 4-47 页
19	不适用	不适用	主机超时	当前	IP 地址已重用和主机超时/已删除主机消息，第 4-47 页
20	不适用	不适用	主机 IP 地址已重用	当前	IP 地址已重用和主机超时/已删除主机消息，第 4-47 页
21	不适用	不适用	已删除主机:已达主机限制	当前	IP 地址已重用和主机超时/已删除主机消息，第 4-47 页
22	不适用	不适用	跳数更改	当前	跳数更改消息，第 4-48 页
23	不适用	不适用	TCP 端口已关闭	当前	TCP 和 UDP 端口已关闭/超时消息，第 4-48 页
24	不适用	不适用	UDP 端口已关闭	当前	TCP 和 UDP 端口已关闭/超时消息，第 4-48 页

表 4-1　　发现和连接事件记录类型 （续）

记录类型	包含块类型	系列	说明 (Description)	记录状态	…中描述的数据格式
25	不适用	不适用	TCP 端口超时	当前	TCP 和 UDP 端口已关闭/超时消息，第 4-48 页
26	不适用	不适用	UDP 端口超时	当前	TCP 和 UDP 端口已关闭/超时消息，第 4-48 页
27	不适用	不适用	MAC 信息更改	当前	MAC 地址消息，第 4-49 页
28	不适用	不适用	为主机检测的其他 MAC	当前	MAC 地址消息，第 4-49 页
29	不适用	不适用	主机 IP 地址已更改	当前	IP 地址更改消息，第 4-46 页
31	不适用	不适用	识别为路由器/网桥的主机	当前	识别为路由器/网桥的主机消息，第 4-49 页
34	14	1	VLAN 标记信息更新	当前	VLAN 标签信息更新消息，第 4-50 页
35	122	1	客户端应用超时	当前	客户端应用消息，第 4-45 页
42	35	1	NetBIOS 名称更改	当前	更改 NetBIOS 名称消息，第 4-50 页
44	不适用	不适用	已丢弃主机：已达主机限制	当前	IP 地址已重用和主机超时/已删除主机消息，第 4-47 页
45	37	1	更新横幅	当前	更新横幅消息，第 4-51 页
46	55	1	添加主机属性	当前	属性消息，第 4-54 页
47	55	1	更新主机属性	当前	属性消息，第 4-54 页
48	55	1	删除主机属性	当前	属性消息，第 4-54 页
51	103	1	TCP 服务器置信度更新	传统	服务器消息，第 4-44 页
52	103	1	UDP 服务器置信度更新	传统	服务器消息，第 4-44 页
53	53	1	操作系统置信度更新	传统	操作系统更新消息，第 4-47 页
54	不适用	不适用	指纹元数据	当前	指纹记录，第 4-6 页
55	不适用	不适用	客户端应用元数据	当前	客户端应用记录，第 4-8 页
57	不适用	不适用	漏洞元数据	当前	漏洞记录，第 4-8 页
58	不适用	不适用	临界点元数据	当前	临界点记录，第 4-11 页
59	不适用	不适用	网络协议元数据	当前	网络协议记录，第 4-12 页
60	不适用	不适用	属性元数据	当前	属性记录，第 4-13 页
61	不适用	不适用	扫描类型元数据	当前	扫描类型记录，第 4-13 页
63	不适用	不适用	服务器元数据	当前	服务记录，第 4-14 页
71	144 个	1	连接统计信息	传统	连接统计信息数据块 5.2.x，第 B-175 页
71	152	1	连接统计信息	传统	连接统计信息数据块 5.3，第 B-192 页
71	154 种	1	连接统计信息	传统	连接统计信息数据块 5.3.1，第 B-201 页
71	155	1	连接统计信息	传统	连接统计信息数据块 5.4，第 B-208 页
71	157	1	连接统计信息	传统	连接统计信息数据块 5.4.1，第 B-221 页
71	160	1	连接统计信息	传统	连接统计信息数据块 6.0.x，第 B-236 页

表 4-1 发现和连接事件记录类型 （续）

记录类型	包含块类型	系列	说明 (Description)	记录状态	...中描述的数据格式
71	163	1	连接统计信息	传统模式	连接统计信息数据块 6.2-6.7.x，第 B-272 页
71	173	1	连接统计信息	传统模式	连接统计信息数据块 7.0，第 B-290 页
71	174	1	连接统计信息	当前	连接统计信息数据块 7.1+，第 4-116 页
73	136	1	连接区块	当前	连接区块消息，第 4-52 页
74	不适用	不适用	用户设置操作系统	当前	用户服务器和操作系统消息，第 4-55 页
75	不适用	不适用	用户设置服务器	当前	用户服务器和操作系统消息，第 4-55 页
76	83	1	用户删除协议	当前	用户协议消息，第 4-55 页
77	60	1	用户删除客户端应用	当前	用户客户端应用消息，第 4-56 页
78	78	1	用户删除地址	当前	用户添加和删除主机消息，第 4-53 页
79	77	1	用户删除服务器	当前	用户删除服务器消息，第 4-53 页
80	80	1	用户设置有效漏洞	当前	用于版本 4.6.1+ 的用户设置漏洞消息，第 4-52 页
81	80	1	用户设置无效漏洞	当前	用于版本 4.6.1+ 的用户设置漏洞消息，第 4-52 页
82	81	1	用户设置主机临界点	当前	用户设置主机临界点消息，第 4-53 页
83	55	1	用户设置属性值	当前	属性值消息，第 4-54 页
84	82	1	用户删除属性值	当前	属性值消息，第 4-54 页
85	78	1	用户添加主机	当前	用户添加和删除主机消息，第 4-53 页
86	不适用	不适用	用户添加服务器	当前	用户服务器和操作系统消息，第 4-55 页
87	60	1	用户添加客户端应用	当前	用户客户端应用消息，第 4-56 页
88	83	1	用户添加协议	当前	用户协议消息，第 4-55 页
89	142	1	用户添加扫描结果	当前	添加扫描结果消息，第 4-56 页
90	不适用	不适用	源类型记录	当前	源类型记录，第 4-15 页
91	不适用	不适用	源应用记录	当前	源应用记录，第 4-16 页
92	120	1	已丢弃用户更改事件	当前	用户修改消息，第 4-58 页
93	120	1	已删除用户更改事件	当前	用户修改消息，第 4-58 页
94	120	1	新用户标识事件	当前	用户修改消息，第 4-58 页
95	121	1	用户登录更改事件	当前	用户信息更新消息块，第 4-59 页
96	不适用	不适用	源检测器记录	当前	源检测器记录，第 4-17 页
98	57	2	用户记录	当前	用户记录，第 4-19 页
101	不适用	不适用	新操作系统事件	当前	新操作系统消息，第 4-57 页
102	94	1	身份冲突事件	当前	身份冲突和身份超时系统消息，第 4-57 页
103	94	1	身份超时事件	当前	身份冲突和身份超时系统消息，第 4-57 页
106	不适用	不适用	第三方扫描仪漏洞记录	当前	第三方扫描仪漏洞记录，第 4-17 页
107	122	1	客户端应用更新	当前	客户端应用消息，第 4-45 页
109	不适用	不适用	Web 应用记录	当前	Web 应用记录，第 4-20 页

表 4-1　　发现和连接事件记录类型 （续）

记录类型	包含块类型	系列	说明 (Description)	记录状态	…中描述的数据格式
114	121	1	用户登录失败事件	当前	用户信息更新消息块，第 4-59 页
115	不适用	不适用	安全区名称记录	当前	安全区名称记录，第 3-29 页
116	14	2	接口名称记录	当前	接口名称记录，第 3-30 页
117	14	2	访问控制策略名称元数据	当前	访问控制策略名称记录，第 3-32 页
118	14	2	入侵策略名称记录	当前	入侵策略名称记录，第 4-21 页
119	14	2	访问控制规则 ID 记录	当前	访问控制规则 ID 记录元数据，第 3-33 页
120	不适用	不适用	访问控制规则操作记录	当前	访问控制规则操作记录元数据，第 4-23 页
121	不适用	不适用	URL 类别记录	当前	URL 类别记录元数据，第 4-24 页
122	不适用	不适用	URL 信誉元数据	当前	URL 信誉记录元数据，第 4-24 页
124	21	2	访问控制规则原因元数据	当前	访问控制规则原因元数据，第 4-25 页
145	64	2	访问控制策略元数据	当前	访问控制策略元数据，第 4-27 页
146	64	2	预过滤器策略元数据	当前	预过滤器策略元数据，第 4-28 页
147	21	2	隧道或预过滤器规则元数据	当前	隧道或预过滤器规则元数据，第 4-30 页
160	7	1	主机 IOC 设置消息	当前	主机 IOC 设置消息，第 4-58 页
161	39	2	用于 5.3+ 的 IOC 名称数据块	当前	用于 5.3+ 的 IOC 名称数据块，第 4-35 页
162	148	1	用户主机 IOC 删除	当前	用户 IOC 更改数据块 5.3+，第 4-77 页
163	148	1	用户主机 IOC 启用	当前	用户 IOC 更改数据块 5.3+，第 4-77 页
164	148	1	用户主机 IOC 禁用	当前	用户 IOC 更改数据块 5.3+，第 4-77 页
170	95	1	VPN 用户登录事件	当前	用户信息更新消息块，第 4-59 页
171	95	1	VPN 用户注销事件	当前	用户信息更新消息块，第 4-59 页
280	22	2	安全情报类别元数据	当前	安全情报类别元数据，第 4-31 页
281	不适用	不适用	安全情报源/目标记录	当前	安全情报源/目标记录，第 4-32 页

发现事件的元数据

您可以通过元数据版本号请求元数据。有关与您的 Cisco Secure Firewall 系统的版本对应的元数据版本，请参阅了解元数据，第 2-38 页。有关 eStreamer 如何流传输元数据记录的重要信息，请参阅元数据传输，第 2-38 页。

有关主机发现和用户事件记录的各种元数据记录类型的结构的信息，请参阅：

- 指纹记录，第 4-6 页
- 客户端应用记录，第 4-8 页
- 漏洞记录，第 4-8 页

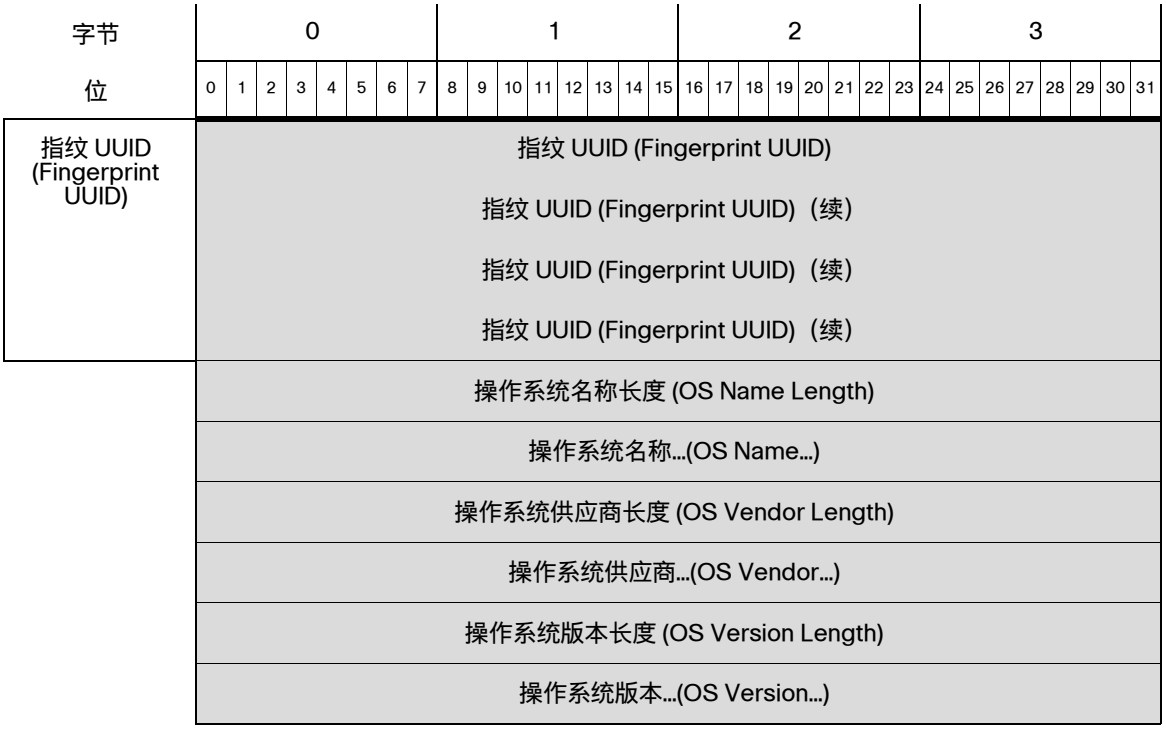
- 临界点记录，第 4-11 页
- 网络协议记录，第 4-12 页
- 属性记录，第 4-13 页
- 扫描类型记录，第 4-13 页
- 服务记录，第 4-14 页
- 源类型记录，第 4-15 页
- 源应用记录，第 4-16 页
- 源检测器记录，第 4-17 页
- 第三方扫描仪漏洞记录，第 4-17 页
- 用户记录，第 4-19 页
- Web 应用记录，第 4-20 页
- 入侵策略名称记录，第 4-21 页
- 访问控制规则操作记录元数据，第 4-23 页
- URL 类别记录元数据，第 4-24 页
- URL 信誉记录元数据，第 4-24 页
- 访问控制规则原因元数据，第 4-25 页
- 安全情报类别元数据，第 4-31 页
- 安全情报源/目标记录，第 4-32 页

有关入侵和关联事件的元数据记录，请参阅入侵事件和元数据记录类型，第 3-1 页。

指纹记录

eStreamer 服务可传输用于指纹记录中的事件的指纹元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送指纹元数据。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 54，表示指纹记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (54) (Record Type (54))															
记录长度 (Record Length)																																



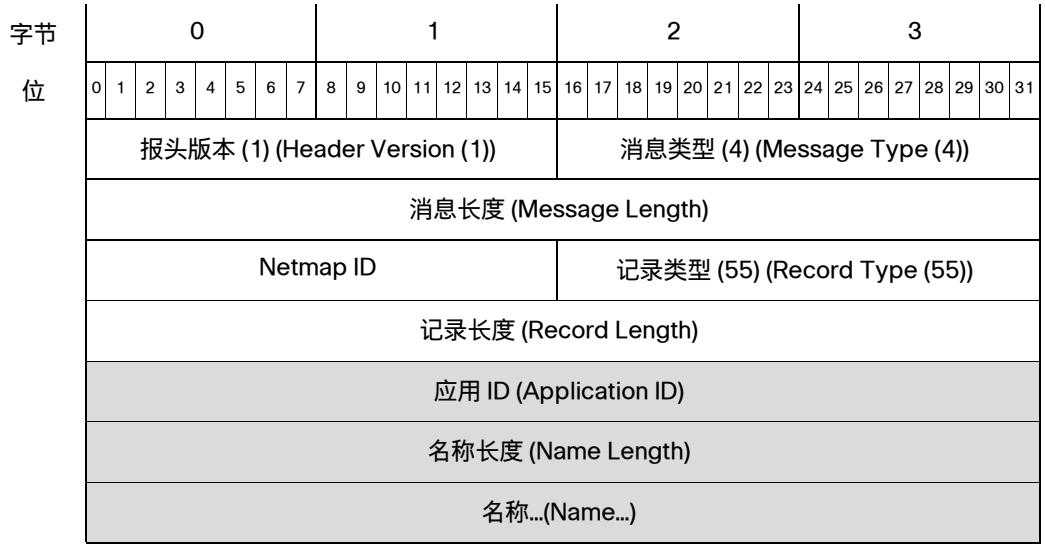
下表对指纹记录中的字段进行了说明。

表 4-2　　指纹记录字段

字段	数据类型	说明 (Description)
指纹 UUID (Fingerprint UUID)	uint8[16]	充当操作系统的唯一标识符的指纹 ID 号码。 此字段是此记录的唯一密钥。
操作系统名称长度 (OS Name Length)	uint32	操作系统名称中包含的字节数。
操作系统名称 (OS Name)	字符串	指纹操作系统的名称。
操作系统供应商长度 (OS Vendor Length)	uint32	操作系统供应商名称中包含的字节数。
操作系统供应商 (OS Vendor)	字符串	指纹操作系统供应商的名称。
操作系统版本长度 (OS Version Length)	uint32	操作系统版本中包含的字节数。
操作系统版本 (OS Version)	字符串	指纹操作系统的版本。

客户端应用记录

eStreamer 服务可传输用于客户端应用记录中的事件的客户端应用元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送客户端应用元数据。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 55，表示客户端应用记录。



下表对客户端应用记录中的字段进行了说明。

表 4-3 客户端应用记录字段

字段	数据类型	说明 (Description)
应用 ID (Application ID)	uint32	客户端应用的应用 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	名称中包含的字节数。
名称 (Name)	字符串	客户端应用名称。

漏洞记录

eStreamer 服务可传输包含漏洞记录中的事件的漏洞信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 57，表示漏洞记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (57) (Record Type (57))															
记录长度 (Record Length)																																
漏洞 ID (Vulnerability ID)																																
影响 (Impact)																																
攻击 (Exploits)									远程 (Remote)								录入日期长度 (Entry Date Length)															
录入日期长度 (Entry Date Length)（续）																	录入日期...(Entry Date...)															
发布日期长度 (Published Date Length)																																
发布日期...(Published Date...)																																
修改日期长度 (Modified Date Length)																																
修改日期...(Modified Date...)																																
标题长度 (Title Length)																																
标题...(Title...)																																
简短说明长度 (Short Description Length)																																
简短说明...(Short Description...)																																
说明长度 (Description Length)																																
说明... (Description...)																																
技术说明长度 (Technical Description Length)																																
技术说明...(Technical Description...)																																
解决方案长度 (Solution Length)																																
解决方案...(Solution...)																																

下表对漏洞记录中的字段进行了说明。

表 4-4 漏洞记录字段

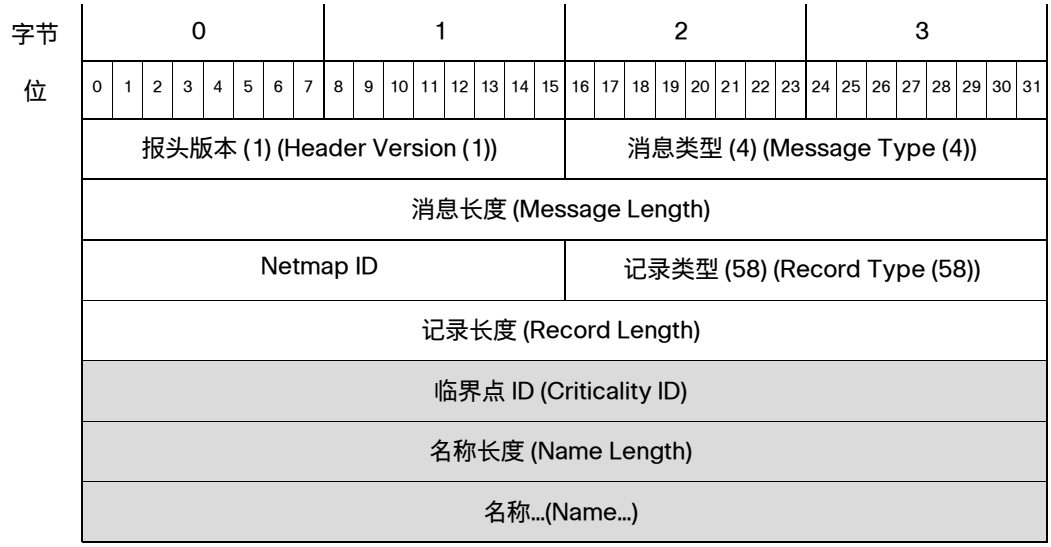
字段	数据类型	说明 (Description)
漏洞 ID (Vulnerability ID)	uint32	漏洞 ID 号码。 此字段是此记录的唯一密钥。
影响 (Impact)	uint32	漏洞影响，与通过入侵数据、主机发现事件和漏洞评估的关联确定的影响级别对应。其值可能为 1 至 10，其中 10 表示其严重程度最高。漏洞的影响级别由 Bugtraq 条目编写者确定。
攻击 (Exploits)	uint8	指示是否存在已知的对漏洞的攻击。可能的值包括: ▪ 0 - 是 ▪ 1 - 否
远程 (Remote)	uint8	指示漏洞是否会通过网络被利用。可能的值包括: ▪ 0 - 是 ▪ 1 - 否 ▪ 空白 - 受远程攻击的可能性未知
录入日期长度 (Entry Date Length)	uint32	录入日期字段的长度。
录入日期 (Entry Date)	字符串	在数据库中输入漏洞时的日期。
发布日期长度 (Published Date Length)	uint32	发布日期字段的长度。
发布日期 (Published Date)	字符串	发布漏洞的日期。
修改日期长度 (Modified Date Length)	uint32	修改日期字段的长度。
修改日期 (Modified Date)	字符串	最近修改漏洞的日期（如果适用）。
标题长度 (Title Length)	uint32	标题字段的长度。
职位	字符串	漏洞的标题。
简短说明长度 (Short Description Length)	uint32	简短说明字段的长度。
简短描述 (Short Description)	字符串	对漏洞的概述。
说明长度 (Description Length)	uint32	说明字段的长度。
说明 (Description)	字符串	对漏洞的一般说明。

表 4-4　　漏洞记录字段 （续）

字段	数据类型	说明 (Description)
技术说明长度 (Technical Description Length)	uint32	技术说明字段的长度。
技术说明 (Technical Description)	字符串	对漏洞的技术说明。
解决方案长度 (Solution Length)	uint32	解决方案字段的长度。
解决方案 (Solution)	字符串	对漏洞的解决方案。

临界点记录

eStreamer 服务可传输包含临界点记录中的事件的主机临界点信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送临界点信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型” (Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 58，表示临界点记录。



下表对临界点记录中的字段进行了说明。

表 4-5 临界点记录字段

字段	数据类型	说明 (Description)
临界点 ID (Criticality ID)	uint32	临界点 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	临界水平中包含的字节数。
名称 (Name)	字符串	临界水平。

网络协议记录

eStreamer 服务可传输包含网络协议记录中的事件的网络协议信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送网络协议信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 59，表示网络协议记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (59) (Record Type (59))															
记录长度 (Record Length)																																
网络协议 ID (Network Protocol ID)																																
名称长度 (Name Length)																																
名称...(Name...)																																

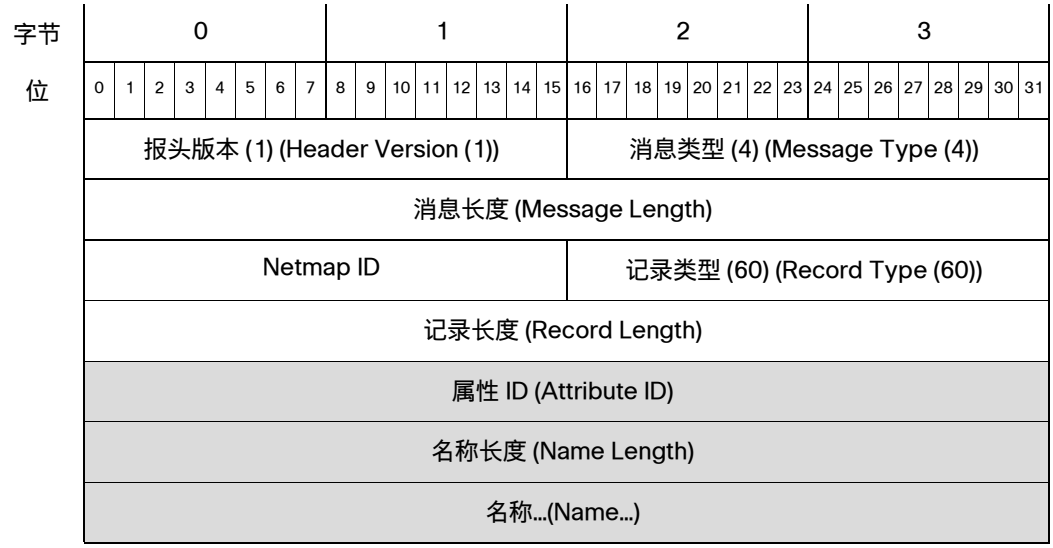
下表对网络协议记录中的字段进行了说明。

表 4-6 网络协议记录字段

字段	数据类型	说明 (Description)
网络协议 ID (Network Protocol ID)	uint32	网络协议 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	网络协议名称中包含的字节数。
名称 (Name)	字符串	网络协议的名称。

属性记录

eStreamer 服务可传输包含属性记录中的事件的属性信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送属性信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 60，表示属性记录。



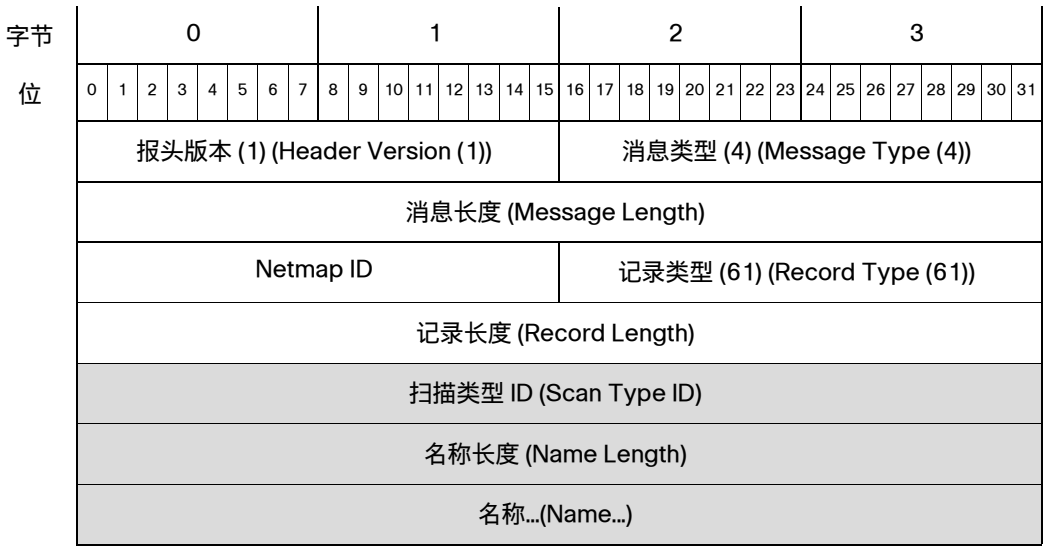
下表对属性记录中的字段进行了说明。

表 4-7　　属性记录字段

字段	数据类型	说明 (Description)
属性 ID (Attribute ID)	uint32	属性 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	属性名称中包含的字节数。
名称 (Name)	字符串	属性的名称。

扫描类型记录

eStreamer 服务可传输包含扫描类型记录中的事件的扫描类型信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送扫描类型信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 61，表示扫描类型记录。



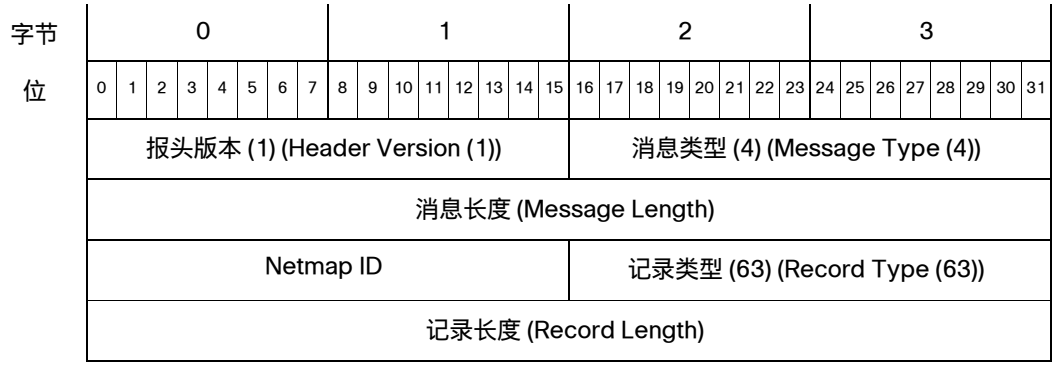
下表对扫描类型记录中的字段进行了说明。

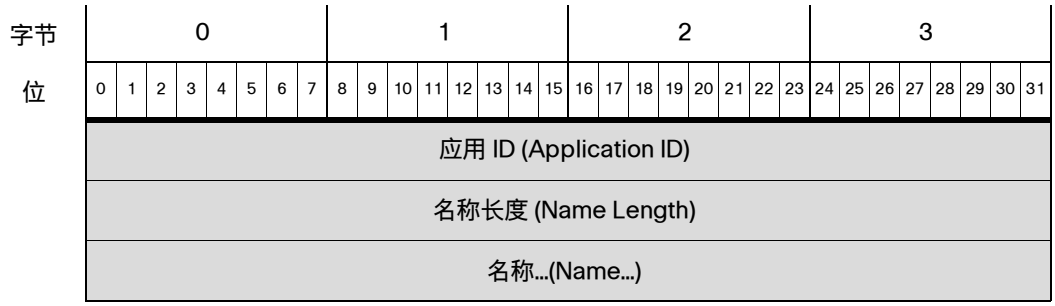
表 4-8 扫描类型记录字段

字段	数据类型	说明 (Description)
扫描类型 ID (Scan Type ID)	uint32	扫描类型 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	扫描类型名称中包含的字节数。
名称 (Name)	字符串	扫描类型的名称。

服务记录

eStreamer 服务可传输包含服务记录中事件的服务信息的元数据，格式如下所示。服务应用协议的应用 ID 提供对元数据的交叉引用。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送服务信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 63，表示服务记录。





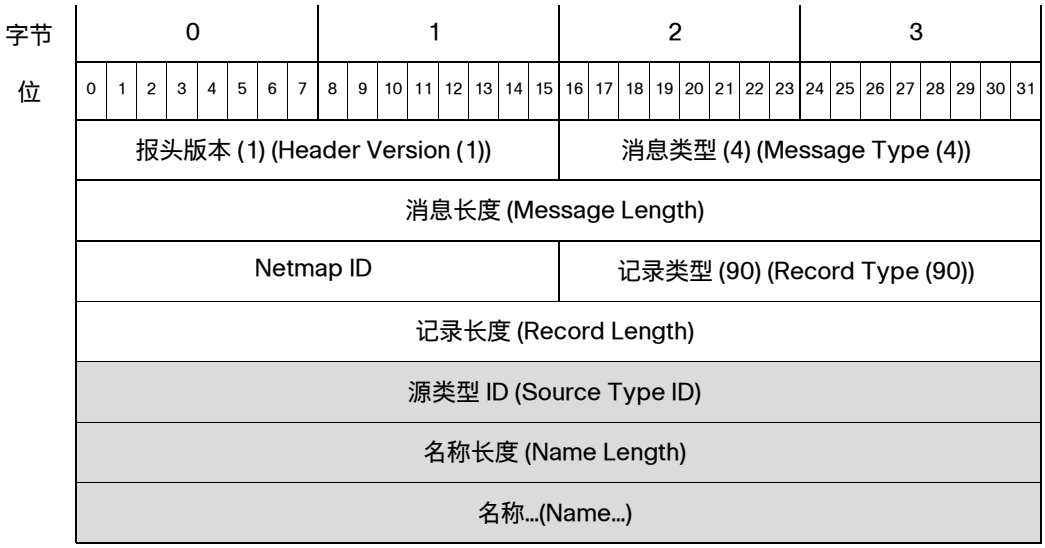
下表介绍服务记录中的字段。

表 4-9　　服务记录字段

字段	数据类型	说明 (Description)
应用 ID (Application ID)	uint32	应用协议的应用 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	服务器名称中包含的字节数。
名称 (Name)	字符串	应用协议的名称。对于应用 ID 65535，名称为 `unknown`。

源类型记录

eStreamer 服务可传输包含源类型记录中的事件的源应用相关信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送源类型信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 `90`，表示源类型记录。



下表对源类型记录中的字段进行了说明。

表 4-10 源类型记录字段

字段	数据类型	说明 (Description)
源类型 ID (Source Type ID)	uint32	源类型的标识号。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	源类型名称中包含的字节数。
名称 (Name)	字符串	源类型的名称。

源应用记录

eStreamer 服务可传输包含源应用记录中的主机发现事件的源应用相关信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送源应用信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型” (Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 91，表示源应用记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (91) (Record Type (91))															
记录长度 (Record Length)																																
源应用 ID (Source Application ID)																																
名称长度 (Name Length)																																
名称...(Name...)																																

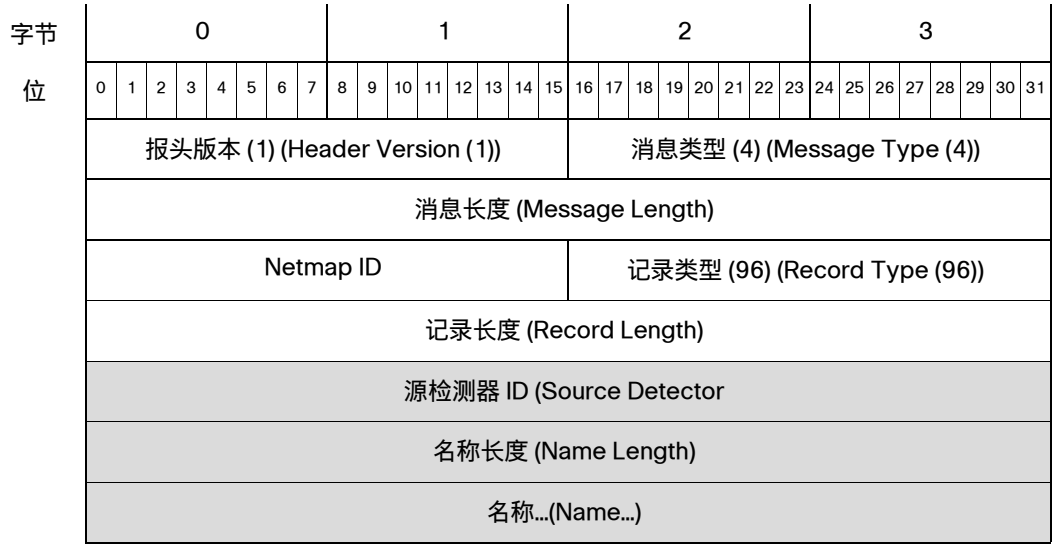
下表对源应用记录中的字段进行了说明。

表 4-11 源应用记录字段

字段	数据类型	说明 (Description)
源应用 ID (Source Application ID)	uint32	源应用的 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	源应用名称中包含的字节数。
名称 (Name)	字符串	源应用的名称。

源检测器记录

eStreamer 服务可传输包含源类型记录中的主机发现事件的源应用相关信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送源类型信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 96，表示源检测器记录。



下表对源检测器记录中的字段进行了说明。

表 4-12　　源检测器记录字段

字段	数据类型	说明 (Description)
源检测器 ID (Source Detector ID)	uint32	源检测器的 ID 字符串。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	源类型名称中包含的字节数。
名称 (Name)	字符串	源检测器的名称。

第三方扫描仪漏洞记录

eStreamer 服务可传输包含第三方扫描仪漏洞记录中事件的第三方漏洞信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 106，表示第三方扫描仪漏洞记录。

下表对漏洞记录中的字段进行了说明。

表 4-13 第三方扫描仪漏洞记录字段

字段	数据类型	说明 (Description)
漏洞 ID (Vulnerability ID)	uint32	第三方漏洞 ID 号码。 此字段与扫描仪类型一起构成此记录的唯一密钥。
扫描仪类型 (Scanner Type)	uint32	第三方扫描仪类型。 此字段与漏洞 ID 一起构成此记录的唯一密钥。
标题长度 (Title Length)	uint32	标题字段的长度。
职位	字符串	漏洞的标题。
说明长度 (Description Length)	uint32	说明字段的长度。
说明 (Description)	字符串	对漏洞的一般说明。

表 4-13　第三方扫描仪漏洞记录字段 （续）

字段	数据类型	说明 (Description)
CVE ID 长度 (CVE ID Length)	uint32	CVE ID 字段的长度。
CVE ID	字符串	漏洞的通用漏洞披露 (CVE) ID 号码。
BugTraq ID 长度 (BugTraq ID Length)	uint32	BugTraq ID 字段的长度。
BugTraq ID	字符串	漏洞的 BugTraq ID 号码。

用户记录

eStreamer 服务可传输包含用户记录中的系统检测到的用户的相关信息的元数据，格式如下所示。（当设置版本 4 元数据和策略事件请求标志（分别为请求消息的“请求标志”(Request Flags) 字段中的位 20 和位 22）时，发送用户信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 98，表示用户记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))														
消息长度 (Message Length)																																
Netmap ID																	记录类型 (98) (Record Type (98))														
记录长度 (Record Length)																																
用户数据块类型 (57) (User Data Block Type (57))																																
用户数据块长度 (User Data Block Length)																																
用户 ID																																
协议 (Protocol)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
用户名...(Username...)																																

下表对用户记录中的字段进行了说明。

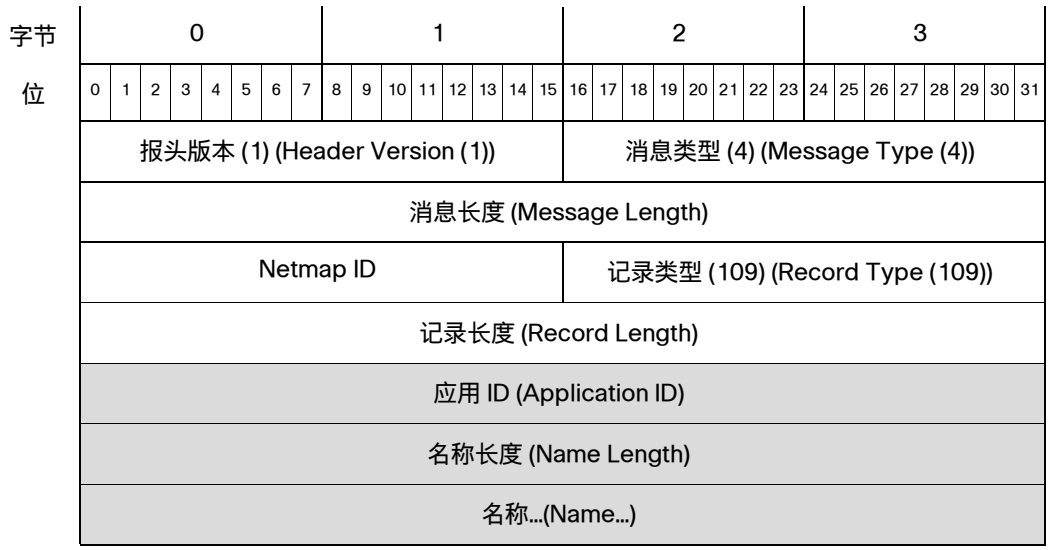
表 4-14 用户记录字段

字段	数据类型	说明 (Description)
用户数据块类型 (User Data Block Type)	uint32	启动用户数据块。值始终为 57。块类型为系列 2 数据块。
用户数据块长度 (User Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的
用户 ID	uint32	用户的唯一标识符。 此字段是此记录的唯一密钥。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值包括: ▪ 165 - FTP ▪ 426 - SIP ▪ 547 - AOL 即时通信工具 ▪ 683 - IMAP ▪ 710 - LDAP ▪ 767 - NTP ▪ 773 - Oracle 数据库 ▪ 788 - POP3 ▪ 1755 - MDNS
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户名”(Username) 字段中的字节数。
用户名 (Username)	字符串	用户的名称

Web 应用记录

系统可检测来自网站的 HTTP 流量的内容（如适用）。主机发现事件的 Web 应用元数据可能包括特定类型的内容（例如，WMV 或 QuickTime）。

eStreamer 服务可传输用于 Web 应用记录中的事件的 Web 应用元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送 Web 应用元数据。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 109，表示 Web 应用记录。



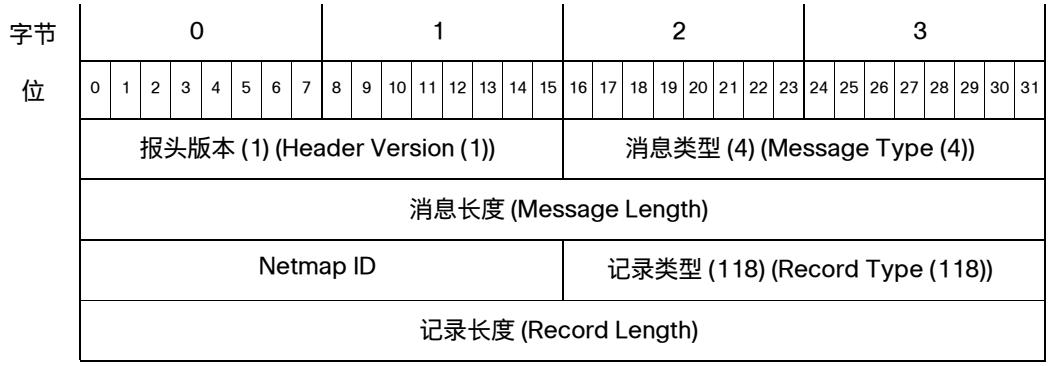
下表对 Web 应用记录中的字段进行了说明。

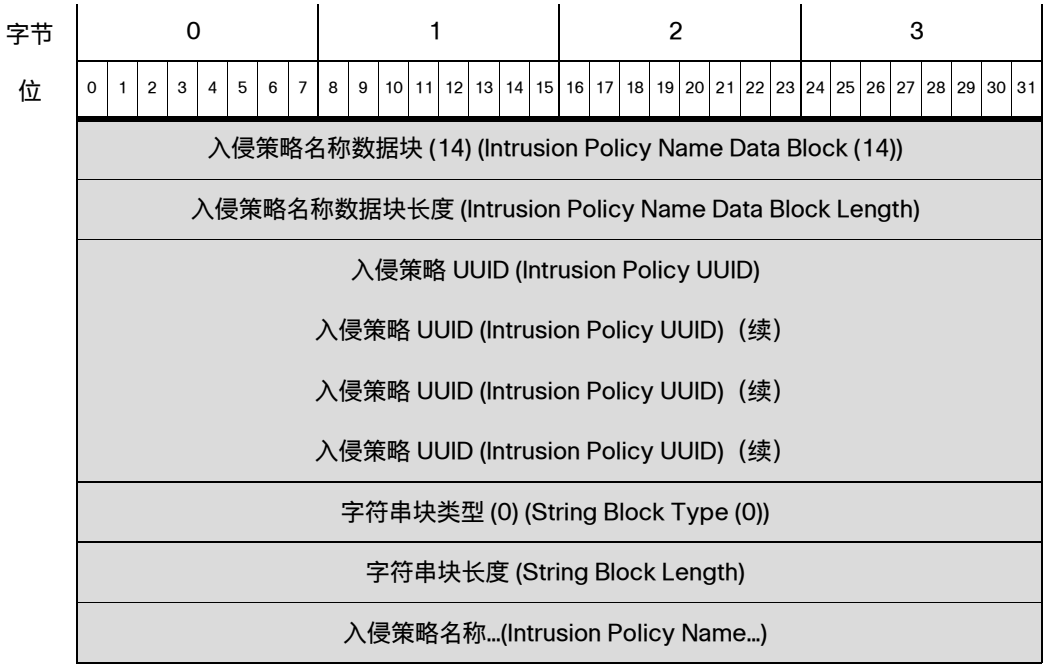
表 4-15　　Web 应用记录字段

字段	数据类型	说明 (Description)
应用 ID (Application ID)	uint32	Web 应用的应用 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	名称中包含的字节数。
名称 (Name)	字符串	Web 应用内容名称。

入侵策略名称记录

eStreamer 服务可传输包含入侵策略名称记录中连接事件的入侵策略名称信息，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的版本 4 元数据位 20）时，发送入侵策略名称信息。请参阅请求标志，第 2-12 页。）请注意，入侵策略名称记录字段（出现在“消息长度”(Message Length) 字段后面）的值为 `118`，表示入侵策略名称记录。它包含一个 UUID 字符串数据块，该数据块的块类型为系列 2 数据块组中的 14。





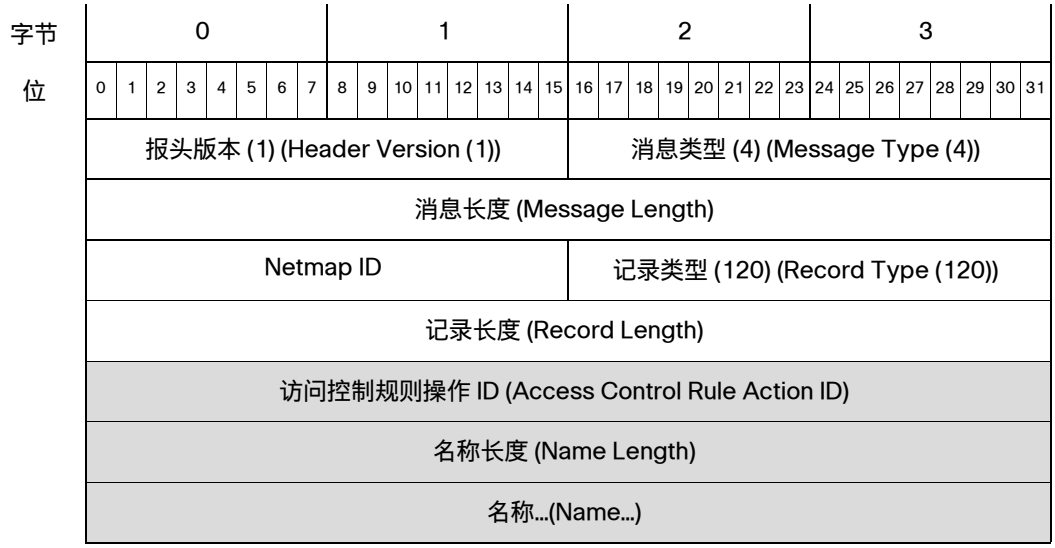
下表对入侵策略名称数据块中的字段进行了说明。

表 4-16 入侵策略名称数据块字段

字段	数据类型	说明 (Description)
入侵策略名称数据块类型 (Intrusion Policy Name Data Block Type)	uint32	启动入侵策略名称数据块。值始终为 14。块类型为系列 2 数据块。
入侵策略名称数据块长度 (Intrusion Policy Name Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的
入侵策略 UUID (Intrusion Policy UUID)	uint8[16]	与连接事件相关的入侵策略的唯一标识符。 此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含入侵策略名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	入侵策略名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。
入侵策略名称 (Intrusion Policy Name)	字符串	入侵策略名称。

访问控制规则操作记录元数据

eStreamer 服务可传输包含与访问控制规则操作记录中已触发的访问控制规则相关的操作的元数据，格式如下所示。（当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送访问控制规则操作信息。请参阅请求标志，第 2-12 页。）请注意，访问控制规则操作记录字段（出现在“消息长度”(Message Length) 字段后面）的值为 120，表示访问控制规则操作记录。



下表对访问控制规则操作记录中的字段进行了说明。

表 4-17　　访问控制规则操作记录字段

字段	数据类型	说明 (Description)
访问控制规则操作 ID (Access Control Rule Action ID)	uint32	访问控制规则操作的 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	名称中包含的字节数。
名称 (Name)	字符串	防火墙规则操作名称。 可能的值包括: ▪ 1 -“待处理” ▪ 2 -“允许” ▪ 3 -“信任” ▪ 4-“阻止” ▪ 5 -“阻止并重置” ▪ 6 -“监控” ▪ 7 -“交互式阻止” ▪ 8 -“交互式阻止并重置” ▪ 14 -“快速路径” ▪ 22 -“找不到域” ▪ 23 -“Sinkhole”

URL 类别记录元数据

eStreamer 服务可传输包含与 URL 类别记录的连接日志中的 URL 相关的类别名称的元数据，格式如下所示。（当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送 URL 类别信息。请参阅请求标志，第 2-12 页。）请注意，记录字段（出现在“消息长度”(Message Length) 字段后面）的值为 121，表示 URL 类别记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (121) (Record Type (121))															
记录长度 (Record Length)																																
URL 类别 ID (URL Category ID)																																
名称长度 (Name Length)																																
名称...(Name...)																																

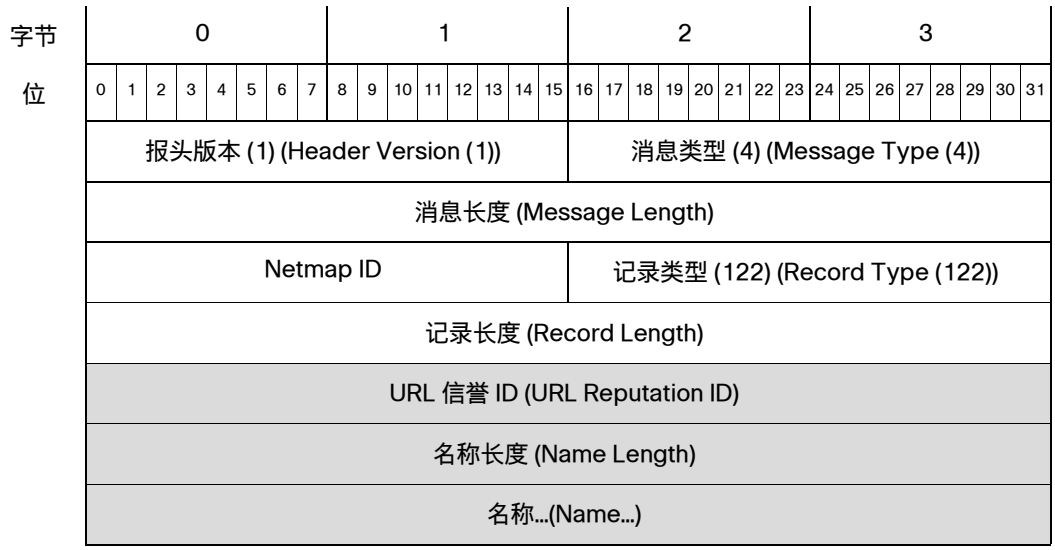
下表对 URL 类别记录中的字段进行了说明。

表 4-18 URL 类别记录字段

字段	数据类型	说明 (Description)
URL 类别 ID (URL Category ID)	uint32	URL 类别的 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	名称中包含的字节数。
名称 (Name)	字符串	URL 类别名称。

URL 信誉记录元数据

eStreamer 服务可传输包含与 URL 信誉记录的连接日志中的 URL 相关的信誉（即风险水平）的元数据，格式如下所示。（当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送 URL 信誉信息。请参阅请求标志，第 2-12 页。）请注意，URL 信誉元数据记录字段（出现在“消息长度”(Message Length) 字段后面）的值为 122，表示 URL 信誉元数据记录。



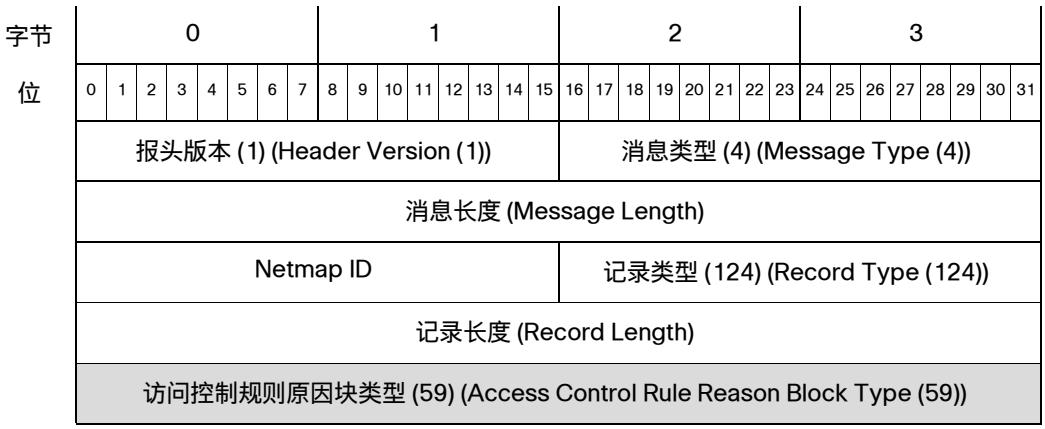
下表对 URL 信誉记录中的字段进行了说明。

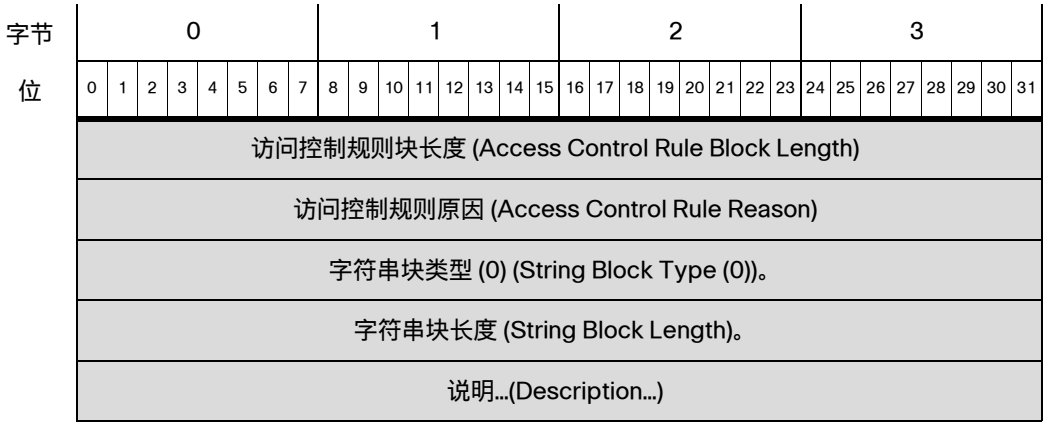
表 4-19　　URL 信誉记录字段

字段	数据类型	说明 (Description)
URL 信誉 ID (URL Reputation ID)	uint32	URL 信誉的 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	名称中包含的字节数。
名称 (Name)	字符串	URL 信誉名称。

访问控制规则原因元数据

eStreamer 服务可传输包含访问控制规则原因记录中访问控制规则触发入侵事件或连接事件的原因相关信息的元数据，格式如下所示。当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送访问控制规则原因元数据。请参阅请求标志，第 2-12 页。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 `124`，表示访问控制规则原因记录。它包含访问控制规则原因块（如访问控制规则原因数据块 6.0+，第 4-203 页中所记录）。访问控制规则原因数据块的块类型为系列 2 中的 59。





下表对访问控制规则 ID 数据块中的字段进行了说明。

表 4-20 访问控制规则原因元数据字段

字段	数据类型	说明 (Description)
访问控制规则原因块类型 (Access Control Rule Reason Block Type)	uint32	启动访问控制规则原因块。值始终为 59。此数据块为系列 2 数据块。
访问控制规则原因块长度 (Access Control Rule	uint32	访问控制规则原因块中的字节总数，包括访问控制规则原因块类型和长度字段的八个字节，加上随后的数据的字节数。
访问控制规则原因 (Access Control Rule Reason)	uint32	访问控制规则记录连接的原因。 此字段是此记录的唯一密钥。 触发事件的规则的原因编号。 规则原因是一个可以在其中设置多个位的二进制位图。规则可能有多种原因。位值如下： ▪ **1** - IP 阻止 ▪ **2** - IP 监控 ▪ **4** - 用户绕行 ▪ **8** - 文件监控 ▪ **16** - 文件阻止 ▪ **32** - 入侵监控 ▪ **64** - 入侵阻止 ▪ **128** - 阻止继续传输文件 ▪ **256** — 允许继续传输文件 ▪ **512** - 文件自定义检测 ▪ **1024** - SSL 阻止 ▪ **2048** - DNS 阻止 ▪ **4096** - DNS 监控 ▪ **8192** - URL 阻止 ▪ **16384** - URL 监控 ▪ **32768** - 内容限制 ▪ **65536** - 智能应用绕行 ▪ **131072** - WSA 威胁

表 4-20　访问控制规则原因元数据字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含与访问控制规则原因相关的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上说明 (Description) 字段中的字节数。
说明 (Description)	字符串	对访问控制规则原因的说明。

访问控制策略元数据

eStreamer服务在访问控制策略元数据记录内传输包含有关触发入侵事件或连接事件的访问控制策略信息的元数据，其格式如下所示。当设置版本 4 元数据标志（请求消息的“请求标志”字段中的位 20）时，发送访问控制规则策略元数据。请参阅请求标志，第 2-12 页。请注意，“记录类型”字段（出现在“消息长度”字段后面）的值为 145，表示访问控制策略元数据记录。它包含访问控制策略元数据块（如访问控制策略元数据块 6.0+，第 4-208 页中所记录）。访问控制策略元数据块的块类型为系列

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															
	Netmap ID																记录类型 (145) (Record Type (161))															
	记录长度 (Record Length)																															
	访问控制策略元数据块类型 (64) (Access Control Policy Metadata Block Type (64))																															
	访问控制策略元数据块长度 (Access Control Policy Metadata Block Length)																															
访问控制策略 UUID	访问控制策略 UUID (Access Control Policy UUID)																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	传感器 ID (Sensor ID)																															
策略名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	策略名称...																															

下表对访问控制策略数据块中的字段进行了说明。

表 4-21 访问控制策略元数据字段

字段	数据类型	说明 (Description)
访问控制策略元数据块类型 (Access Control Policy Metadata Block Type)	uint32	启动访问控制策略元数据块。值始终为 64。此数据块为系列 2 数据块。
访问控制策略元数据块长度 (Access Control Policy Metadata Block Length)	uint32	访问控制策略元数据块中的字节总数，包括访问控制策略元数据块类型和长度字段的八个字节，加上随后的数据的字节数。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	访问控制策略的 UUID。此字段是此记录的唯一密钥。
传感器 ID (Sensor ID)	uint32	与访问控制策略关联的传感器的 ID 号码。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含与访问控制策略关联的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
名称 (Name)	字符串	访问控制策略的名称。

预过滤器策略元数据

eStreamer 服务可传输包含预过滤器策略相关信息的元数据（此策略会触发预过滤器策略元数据记录中的入侵事件或连接事件），格式如下所示当设置版本 4 元数据标志（请求消息的“请求标志”字段中的位 20）时，发送预过滤器策略元数据。请参阅请求标志，第 2-12 页。请注意，“记录类型”字段（出现在“消息长度”字段后面）的值为 146，表示预过滤器策略元数据记录。它包含访问控制策略元数据块（如访问控制策略元数据块 6.0+，第 4-208 页中所记录）。访问控制策略元数据块的块类型为系列

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (146) (Record Type (161))															
记录长度 (Record Length)																																
访问控制策略元数据块类型 (64) (Access Control Policy Metadata Block Type (64))																																
访问控制策略元数据块长度 (Access Control Policy Metadata Block Length)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
访问控制策略 UUID	访问控制策略 UUID (Access Control Policy UUID)																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	传感器 ID (Sensor ID)																															
策略名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	策略名称...																															

下表对预过滤器策略元数据块中的字段进行了说明。

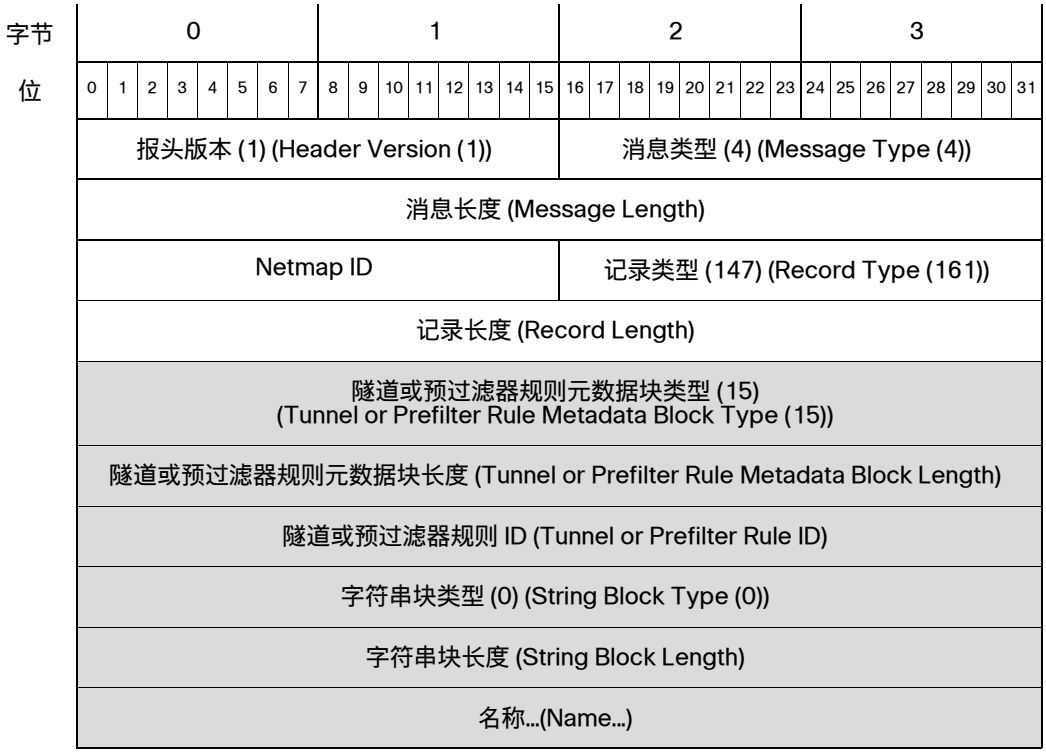
表 4-22　　预过滤器策略元数据字段

字段	数据类型	说明 (Description)
预过滤器策略块类型 (Prefilter Policy Block Type)	uint32	启动预过滤器策略块。值始终为 64。此数据块为系列 2 数据块。
预过滤器策略块长度 (Prefilter Policy Block Length)	uint32	预过滤器策略块中的字节总数，包括预过滤器策略块类型和长度字段的八个字节，加上随后的数据字节数。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	访问控制策略的 UUID。此字段与传感器 ID 一起构成此记录的唯一密钥。
传感器 ID (Sensor ID)	uint32	与访问控制策略关联的传感器的 ID 号码。此字段与访问控制策略 UUID 一起构成此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含与预过滤器策略关联的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
名称 (Name)	字符串	预过滤器策略的名称。

隧道或预过滤器规则元数据

eStreamer 服务可传输包含预过滤器规则原因相关信息的元数据（此策略会触发预过滤器规则原因记录中的入侵事件或连接事件），格式如下所示。当设置版本 4 元数据标志（请求消息的“请求标志”字段中的位 20）时，发送隧道或预过滤器规则原因元数据。请参阅请求标志，第 2-12 页。请注意，“记录类型”字段（出现在“消息长度”字段后面）的值为 147，表示隧道或预过滤器规则原因记录。

由于它们的内容相同，因此它包含访问控制规则原因块（如访问控制规则数据块，第 4-202 页中所记录）。访问控制规则原因数据块的块类型为系列 2 中的 59。



下表对隧道或预过滤器规则元数据块中的字段进行了说明。

表 4-23　　隧道或预过滤器规则原因元数据字段

字段	数据类型	说明 (Description)
隧道或预过滤器规则块类型 (Tunnel or Prefilter Rule Block Type)	uint32	启动访问控制规则块。值始终为 15。请注意，除了访问控制规则，此块还用于隧道和预过滤器规则。
隧道或预过滤器规则块长度 (Tunnel or Prefilter Rule Block Length)	uint32	隧道或预过滤器规则块中的字节总数，包括隧道或预过滤器块类型和长度字段的八个字节，加上随后的数据字节数。
隧道或预过滤器规则 ID (Tunnel or Prefilter Rule ID)	uint32	隧道或预过滤器规则的内部 思科 标识符。

表 4-23　隧道或预过滤器规则原因元数据字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含与隧道或预过滤器规则 UUID 以及隧道或预过滤器规则 ID 关联的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
名称 (Name)	字符串	描述性名称。

安全情报类别元数据

eStreamer 服务可传输包含安全情报类别记录中的安全情报类别相关信息的元数据，格式如下所示。当设置版本 4 元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 20）时，发送安全情报类别元数据。请参阅请求标志，第 2-12 页。请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 280，表示安全情报类别记录。它包含安全情报类别数据块（如安全情报类别数据块 5.1+，第 4-205 页中所记录）。安全情报数据块的块类型为系列 2 中的 22。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (280) (Record Type (280))															
记录长度 (Record Length)																																
安全情报类别块类型 (22) (Security Intelligence Category Block Type (22))																																
安全情报类别块长度 (Security Intelligence Category Block Length)																																
安全情报列表 ID (Security Intelligence List ID)																																
访问控制策略 UUID (Access Control Policy UUID) 访问控制策略 UUID (Access Control Policy UUID)（续） 访问控制策略 UUID (Access Control Policy UUID)（续） 访问控制策略 UUID (Access Control Policy UUID)（续）																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
安全情报列表名称...(Security Intelligence Name...)																																

下表对安全情报类别记录中的字段进行了说明。

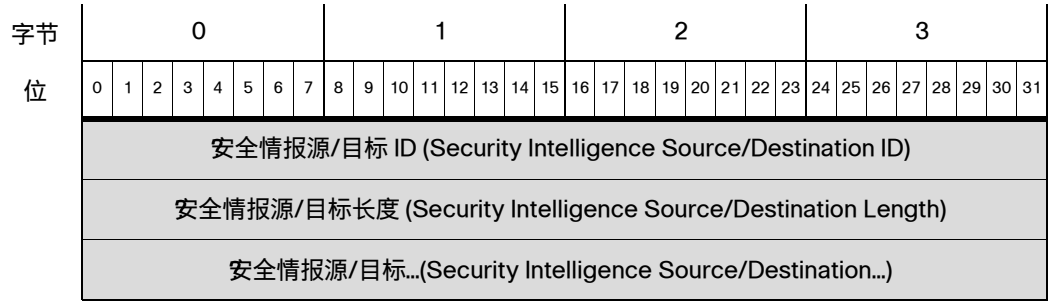
表 4-24 安全情报类别元数据字段

字段	数据类型	说明 (Description)
安全情报类别块类型 (Security Intelligence Category Block Type)	uint32	启动安全情报类别数据块。值始终为 22。此数据块为系列 2 数据块。
安全情报类别块长度 (Security Intelligence Category Block Length)	uint32	安全情报类别块中的字节总数，包括安全情报类别块类型和长度字段的八个字节，加上随后的数据字节数。
安全情报列表 ID (Security Intelligence List ID)	uint32	连接触发的 IP 阻止列表或允许列表的 ID。 此字段与访问控制策略
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	为安全情报配置的访问控制策略的UUID。 此字段与安全情报列表 ID 一起构成此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含与安全情报列表相关的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“安全情报列表名称”(Security Intelligence Name) 字段中的字节数。
安全情报列表名称 (Security Intelligence Name)	字符串	连接触发的 IP 类别阻止列表或允许列表的名称。

安全情报源/目标记录

eStreamer服务可传输包含安全情报源/目标记录中安全情报检测到的 IP 地址是源 IP 地址还是目标 IP 地址这一信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送源/目标 IP 信息。请参阅请求标志，第 2-12 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度” (Message Length) 字段后面）的值为 281，表示安全情报源/目标记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (281) (Record Type (281))															
记录长度 (Record Length)																																



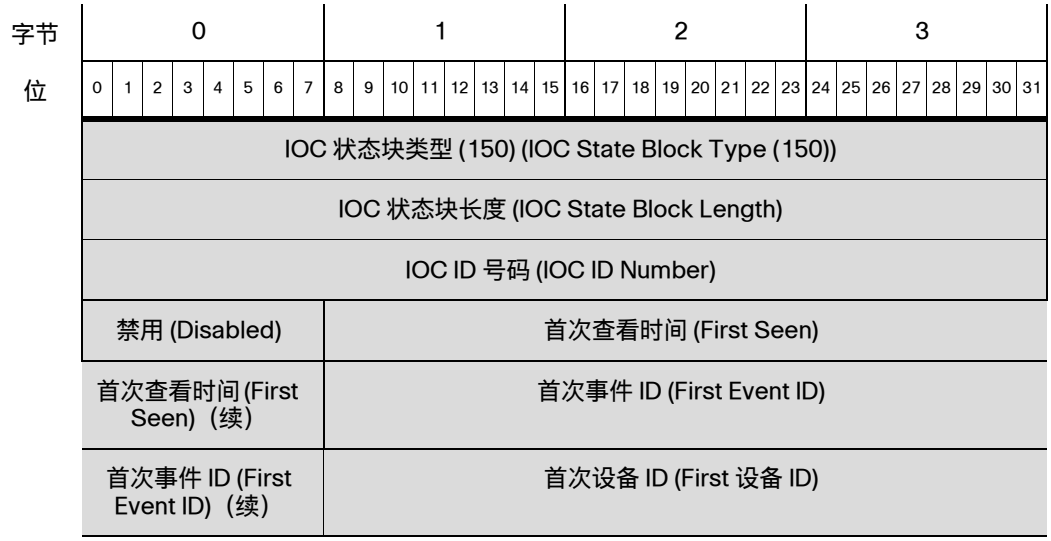
下表对安全情报源/目标记录中的字段进行了说明。

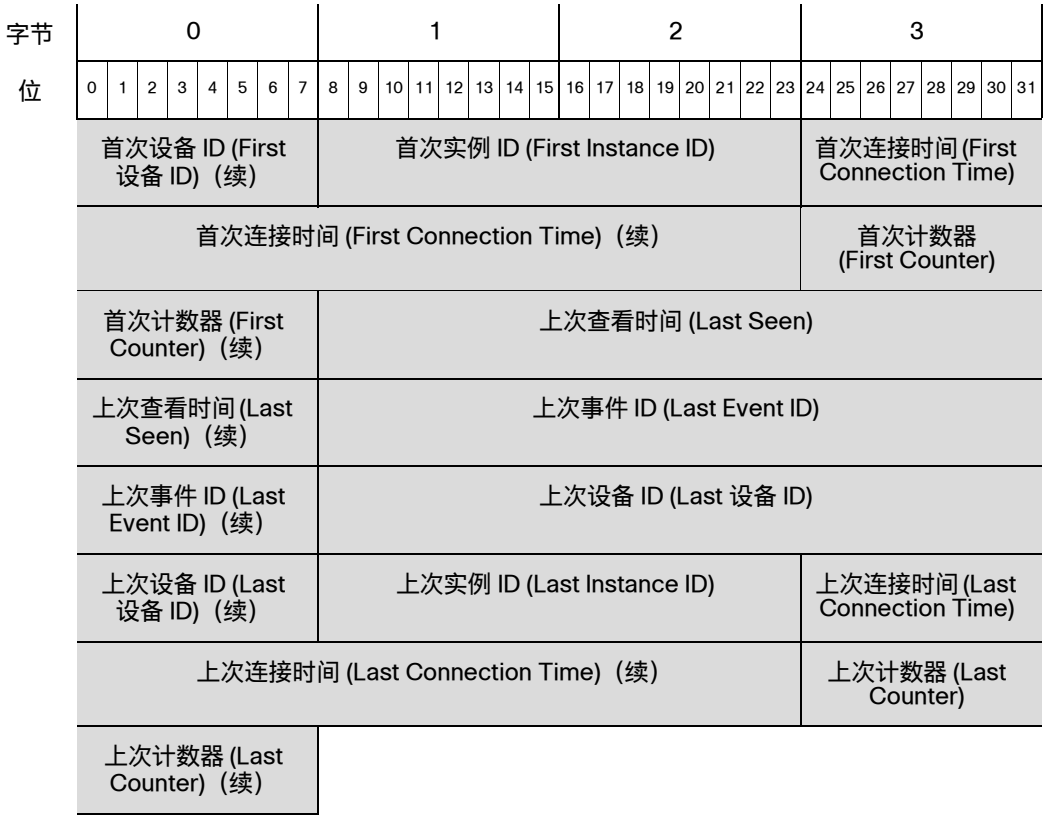
表 4-25　　安全情报源/目标记录字段

字段	数据类型	说明 (Description)
安全情报源/目标 ID (Security Intelligence Source/ Destination ID)	uint32	安全情报源/目标 ID 号码。 此字段是此记录的唯一密钥。
安全情报源/目标长度 (Security Intelligence Source/ Destination Length)	uint32	安全情报源/目标中包含的字节数。
安全情报源/目标 (Security Intelligence Source/ Destination)	字符串	检测到的 IP 地址是源 IP 地址还是目标 IP 地址。

用于 5.3+ 的 IOC 状态数据块

IOC 状态数据块提供有关危害表现 (IOC) 的信息。块类型为系列 1 中的 150。主机跟踪器用该数据块存储有关主机存在的危害的信息。下图显示 IOC 状态数据块的结构:





下表对 IOC 状态数据块的组件进行了说明。

。

表 4-26 IOC 状态数据块字段

字段	数据类型	说明 (Description)
IOC 状态数据块类型 (IOC State Data Block Type)	uint32	启动 IOC 状态数据块。值始终为 150。
IOC 状态数据块长度 (IOC State Data Block Length)	uint32	IOC 状态数据块中的字节总数，包括 IOC 状态数据块类型和长度字段的八个字节，加上随后的数据字节数。
IOC ID 号码 (IOC ID Number)	uint32	威胁的唯一 ID 编号。
禁用 (Disabled)	uint8	指示是否已在主机上禁用该危害: ▪ 0 - 危害未禁用。 ▪ 1 - 危害已禁用。
首次查看时间 (First Seen)	uint32	首次查看到此危害的 Unix 时间戳。
首次事件 ID (First Event ID)	uint32	首次在其上查看到此危害的事件的 ID 号码。

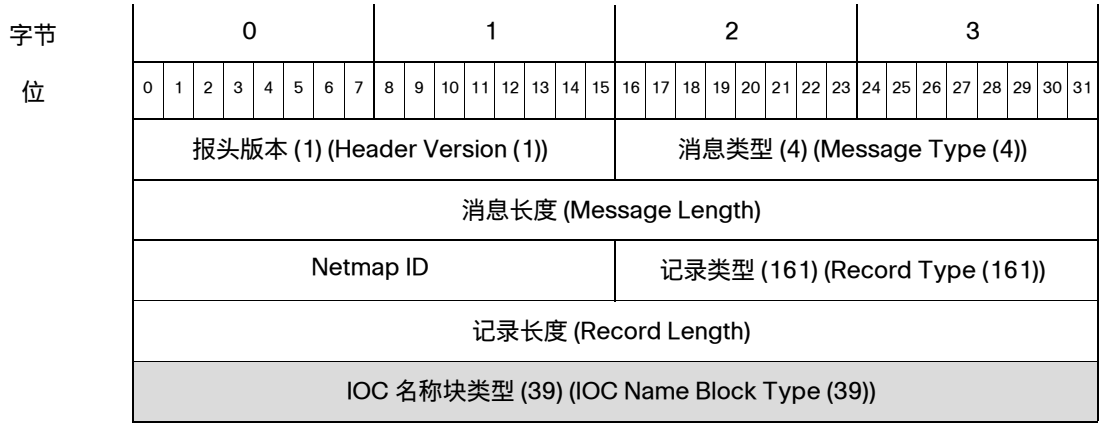
表 4-26　　IOC 状态数据块字段 （续）

字段	数据类型	说明 (Description)
首次设备 ID (First 设备 ID)	uint32	首次检测到 IOC 的传感器的 ID。
首次实例 ID (First Instance ID)	uint16	首次检测到此危害的受管设备上 Snort 实例的数字 ID。
首次连接时间 (First Connection Time)	uint32	首次查看到此危害的连接的 Unix 时间戳。
首次计数器 (First Counter)	uint16	上次在其上查看到此危害的连接的计数器。 用于区分同时出现的多个连接。
上次查看时间 (Last Seen)	uint32	上次查看到此危害的 Unix 时间戳。
上次事件 ID (Last Event ID)	uint32	上次在其上查看到此危害的事件的 ID 号码。
上次设备 ID (Last 设备 ID)	uint32	最近检测到 IOC 的传感器的 ID。
上次实例 ID (Last Instance ID)	uint16	上次检测到此危害的受管设备上 Snort 实例的数字 ID。
上次连接时间 (Last Connection Time)	uint32	上次在其上看到此危害的连接的 Unix 时间戳。
上次计数器 (Last Counter)	uint16	上次在其上查看到此危害的连接的计数器。 用于区分同时出现的多个连接。

用于 5.3+ 的 IOC 名称数据块

此数据块提供危害表现 (IOC) 的类别和事件类型。此数据块的记录类型为系列 2 中的 161，块类型为系列 2 中的 39。它作为任何具有 IOC 信息的事件的元数据显示。这些包括恶意软件事件、文件事件和入侵事件。

下图显示 IOC 名称数据块的结构：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IOC 名称块长度 (IOC Name Block Length)																															
	IOC ID 号码 (IOC ID Number)																															
类别	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	类别...(Category...)																															
事件类型 (Event Type)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件类型...(Event Type...)																															

下表对 IOC 名称数据块中的字段进行了说明。

表 4-27 IOC 名称数据块字段

字段	数据类型	说明 (Description)
IOC 名称数据块类型 (IOC Name Data Block Type)	uint32	启动 IOC 名称数据块。值始终为 39。
IOC 名称数据块长度 (IOC Name Data Block Length)	uint32	IOC 名称数据块中的字节总数，包括 IOC 名称数据块类型和长度字段的八个字节，加上随后的数据字节数。
IOC ID 号码 (IOC ID Number)	uint32	威胁的唯一 ID 编号。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的类别的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“类别”(Category) 字段中的字节数。
类别	字符串	威胁的类别。可能的值包括： ▪ CnC Connected ▪ Exploit Kit ▪ High Impact Attack ▪ Low Impact Attack ▪ Malware Detected ▪ Malware Executed ▪ Dropper Infection ▪ Java Compromise ▪ Word Compromise ▪ Adobe Reader Compromise ▪ Excel Compromise ▪ PowerPoint Compromise ▪ QuickTime Compromise

表 4-27　　IOC 名称数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的事件类型的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件类型”(Event Type) 字段中的字节数。
事件类型 (Event Type)	字符串	威胁的事件类型。可能的值包括： ▪ Adobe Reader launched shell ▪ Dropper Infection Detected by 面向终端的 AMP ▪ Excel Compromise Detected by 面向终端的 AMP ▪ Excel launched shell ▪ Impact 1 Intrusion Event – attempted-admin ▪ Impact 1 Intrusion Event – attempted-user ▪ Impact 1 Intrusion Event – successful-admin ▪ Impact 1 Intrusion Event – successful-user ▪ Impact 1 Intrusion Event – web-application-attack ▪ Impact 2 Intrusion Event – attempted-admin ▪ Impact 2 Intrusion Event – attempted-user ▪ Impact 2 Intrusion Event – successful-admin ▪ Impact 2 Intrusion Event – successful-user ▪ Impact 2 Intrusion Event – web-application-attack ▪ Intrusion Event – exploit-kit ▪ Intrusion Event – malware-backdoor ▪ Intrusion Event – malware-cnc ▪ Java Compromise Detected by 面向终端的 AMP ▪ Java launched shell ▪ PDF Compromise Detected by 面向终端的 AMP ▪ PowerPoint Compromise Detected by 面向终端的 AMP ▪ PowerPoint launched shell ▪ QuickTime Compromise Detected by 面向终端的 AMP ▪ QuickTime launched shell ▪ Security Intelligence Event – CnC ▪ Security Intelligence Event – DNS CnC ▪ Security Intelligence Event – DNS Malware ▪ Security Intelligence Event – DNS Phishing ▪ Security Intelligence Event – Sinkhole CnC ▪ Security Intelligence Event – Sinkhole Malware ▪ Security Intelligence Event – Sinkhole Phishing ▪ Security Intelligence Event – URL CnC ▪ Security Intelligence Event – URL Malware ▪ Security Intelligence Event – URL Phishing ▪ Suspected Botnet Detected by 面向终端的 AMP ▪ Threat Detected by 面向终端的 AMP – Executed ▪ Threat Detected by 面向终端的 AMP – Not Executed ▪ Threat Detected in File Transfer ▪ Word Compromise Detected by 面向终端的 AMP ▪ Word launched shell

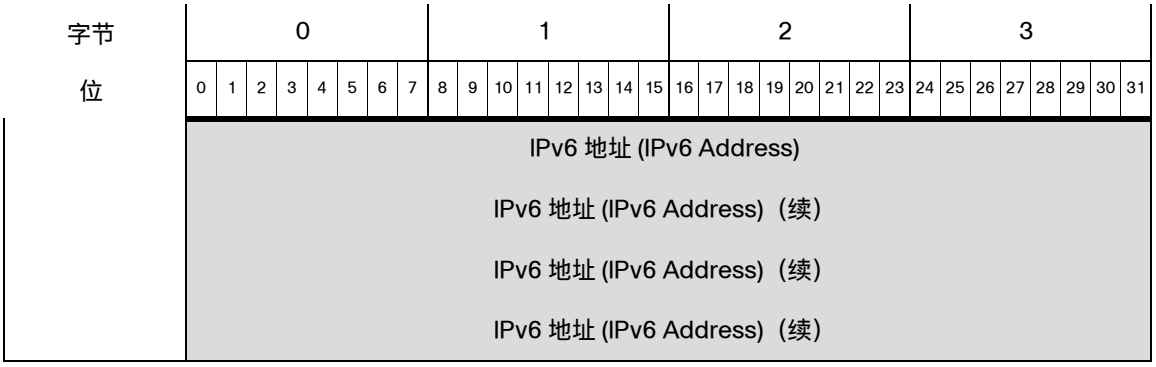
发现事件报头 5.2+

发现和连接事件消息包含发现事件报头。它传送事件的类型和子类型、事件发生的时间、出现该事件的设备以及消息中事件数据的结构。报头后面是实际主机发现、用户或连接事件数据。按事件类型划分的主机发现结构，第 4-42 页中介绍了与不同事件类型/子类型值相关的结构。此报头具有 IPv6 支持，并否决发现事件报头 5.0 - 5.1.1.x，第 B-121 页。

发现事件报头的事件类型和事件子类型字段用于识别传输的事件消息的结构。一旦确定事件数据块的结构，您的程序即可对消息进行适当解析。

下图中的阴影行举例说明了发现事件报头的格式。

	字节	0								1								2								3							
	位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
		消息长度 (Message Length)																															
		Netmap ID																记录类型 (Record Type)															
		记录长度 (Record Length)																															
		eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																															
		留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																															
发现事件报头 (Discovery Event Header)		设备 ID (设备 ID)																															
		旧版 IP 地址 (Legacy IP Address)																															
		MAC 地址																															
		MAC 地址 (MAC Address)（续）																具有 IPv6 (Has IPv6)								留作未来使用 (Reserved for future use)							
		事件秒 (Event Second)																															
		事件微秒 (Event Microsecond)																															
		事件类型 (Event Type)																															
		事件子类型																															
		文件编号 (File Number)（仅限内部使用）																															
		文件位置 (File Position)（仅限内部使用）																															



下表对发现事件报头进行了说明。

表 4-28　　发现事件报头字段

字段	数据类型	说明
设备 ID	uint32	生成发现事件的设备的 ID 号码。您可以通过请求版本 3 和版本 4 元数据获取设备的元数据。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
旧版 IP 地址 (Legacy IP Address)	uint32	保留此字段，但不再填充。IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅IP 地址，第 1-4 页。
MAC 地址 (MAC Address)	uint8[6]	事件所涉及主机的 MAC 地址。
具有 IPv6 (Has IPv6)	uint8	指示主机具有 IPv6 地址的标志。
留作未来使用 (Reserved for future use)	uint8	留作未来使用 (Reserved for future use)
事件秒 (Event Second)	uint32	系统生成事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
事件微秒 (Event Microsecond)	uint32	系统生成事件的微秒（一秒的百万分之一）增量。
事件类型 (Event Type)	uint32	事件类型（新事件为 `1000`，变更事件为 `1001`，用户输入事件为 `1002`，完整主机配置文件为 `1050`）。有关可用事件类型列表，请参阅按事件类型划分的主机发现结构，第 4-42 页。
事件子类型 (Event Subtype)	uint32	事件子类型。有关可用事件子类型列表，请参阅按事件类型划分的主机发现结构，第 4-42 页。
文件编号 (File Number)	byte[4]	串行文件编号。此字段供思科内部使用，可以忽略。
文件位置 (File Position)	byte[4]	事件在串行文件中的位置。此字段供思科内部使用，可以忽略。
IPv6 地址 (IPv6 Address)	uin8[16]	IPv6 地址。若设置了“具有 IPv6”(Has IPv6) 标志，则此字段存在且可使用。

发现与连接事件类型和子类型

“事件类型”(Event Type) 和“事件子类型”(Event Subtype) 字段中的值对主机发现或用户数据消息中包含的事件进行识别和分类。它们也识别消息中的数据的结构。

下表列出了发现事件与连接事件的事件类型和事件子类型。

表 4-29 按类型和子类型划分的发现与连接事件

事件名称	事件类型 (Event Type)	事件子类型
新主机	1000	1
新 TCP 服务器	1000	2
新网络协议	1000	3
新传输协议	1000	4
新 IP 到 IP 流量	1000	5
新 UDP 服务器	1000	6
新客户端应用	1000	7
新操作系统	1000	8
新 IPv6 到 IPv6 流量	1000	9
主机 IP 地址已更改	1001	1
操作系统信息更新	1001	2
主机 IP 地址已重用	1001	3
漏洞更改	1001	4
跳数更改	1001	5
TCP 服务器信息更新	1001	6
主机超时	1001	7
TCP 端口已关闭	1001	8
UDP 端口已关闭	1001	9
UDP 服务器信息更新	1001	10
TCP 端口超时	1001	11
UDP 端口超时	1001	12
MAC 信息更改	1001	13
为主机检测的其他 MAC	1001	14
主机上次查看时间	1001	15
识别为路由器/网桥的主机	1001	16
连接统计信息	1001	17
VLAN 标记信息更新	1001	18
已删除主机:已达主机限制	1001	19
客户端应用超时	1001	20
NetBIOS 名称更改	1001	21

表 4-29　按类型和子类型划分的发现与连接事件 （续）

事件名称	事件类型 (Event Type)	事件子类型
NetBIOS 域更改	1001	22
已丢弃主机：已达主机限制	1001	23
横幅更新	1001	24
TCP 服务器置信度更新	1001	25
UDP 服务器置信度更新	1001	26
身份冲突	1001	29
身份超时	1001	30
辅助主机更新	1001	31
客户端应用更新	1001	32
用户设置有效漏洞（旧版本）	1002	1
用户设置无效漏洞（旧版本）	1002	2
用户删除地址（旧版本）	1002	3
用户删除服务器（旧版本）	1002	4
用户设置主机临界点	1002	5
主机属性添加	1002	6
主机属性更新	1002	7
主机属性删除	1002	8
主机属性设置值（旧版本）	1002	9
主机属性删除值（旧版本）	1002	10
添加扫描结果	1002	11
用户设置漏洞限定条件	1002	12
用户策略控制	1002	13
删除协议	1002	14
删除客户端应用	1002	15
用户设置操作系统	1002	16
用户帐户查看	1002	17
用户帐户更新	1002	18
用户设置服务器	1002	19
用户删除地址（当前版本）	1002	20
用户删除服务器（当前版本）	1002	21
用户设置有效漏洞（当前版本）	1002	22
用户设置无效漏洞（当前版本）	1002	23
用户主机临界点	1002	24
主机属性设置值（当前版本）	1002	25
主机属性删除值（当前版本）	1002	26

表 4-29 按类型和子类型划分的发现与连接事件 （续）

事件名称	事件类型 (Event Type)	事件子类型
用户添加主机	1002	27
用户添加服务器	1002	28
用户添加客户端应用	1002	29
用户添加协议	1002	30
重新加载应用	1002	31
帐户删除	1002	32
连接统计信息	1003	1
连接区块	1003	2
新用户身份	1004	1
用户登录	1004	2
删除用户身份	1004	3
已丢弃用户身份：已达到用户限制	1004	4
用户登录失败	1004	5
VPN 用户登录	1004	8
VPN 用户注销	1004	9
主机 IOC 设置类型	1008	1
完整主机配置文件	1050	不适用

提示 有关用于每个事件类型/子类型的数据结构的信息，请参阅按事件类型划分的主机发现结构，第 4-42 页。

按事件类型划分的主机发现结构

eStreamer 根据发现事件报头中指示的事件类型构建主机发现事件消息。以下子节对每个事件类型的结构进行了概括性说明：

- TCP 和 UDP 端口已关闭/超时消息，第 4-48 页
- MAC 地址消息，第 4-49 页
- 识别为路由器/网桥的主机消息，第 4-49 页
- VLAN 标签信息更新消息，第 4-50 页
- 更改 NetBIOS 名称消息，第 4-50 页
- 更新横幅消息，第 4-51 页
- 策略控制消息，第 4-51 页
- 连接统计信息数据消息，第 4-51 页
- 连接区块消息，第 4-52 页
- 用于版本 4.6.1+ 的用户设置漏洞消息，第 4-52 页
- 用户添加和删除主机消息，第 4-53 页
- 用户删除服务器消息，第 4-53 页
- 用户设置主机临界点消息，第 4-53 页
- 属性消息，第 4-54 页
- 属性值消息，第 4-54 页
- 用户服务器和操作系统消息，第 4-55 页
- 用户协议消息，第 4-55 页
- 用户客户端应用消息，第 4-56 页
- 添加扫描结果消息，第 4-56 页
- 新操作系统消息，第 4-57 页
- 身份冲突和身份超时系统消息，第 4-57 页
- 主机 IOC 设置消息，第 4-58 页

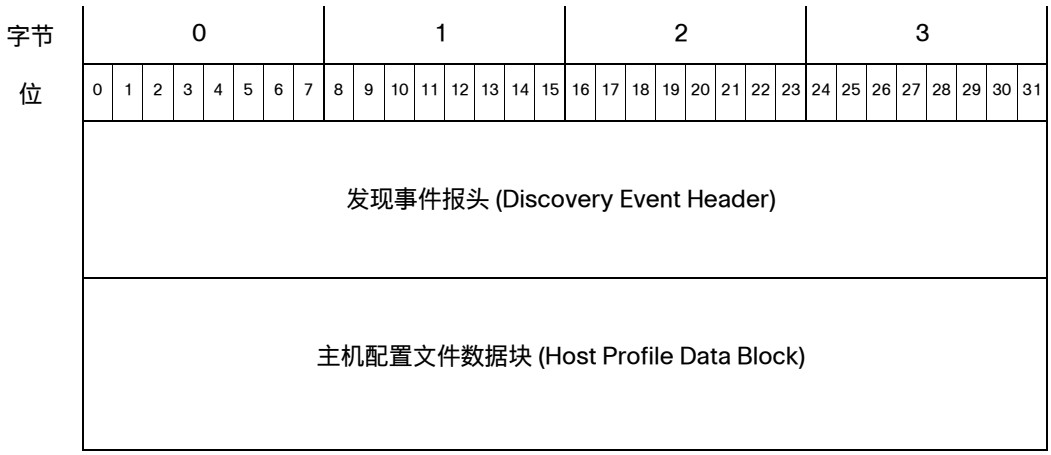
以下章节中的数据块图描绘了主机发现事件消息中返回的不同记录数据块。

新主机消息与主机上次查看时间消息

新主机消息与主机上次查看时间事件消息具有标准发现事件报头和主机配置文件数据块（如用于 5.2+ 的主机配置文件数据块，第 4-164 页中所记录）。主机配置文件数据块的块类型为系列 1 中的 139。

请注意，主机上次查看时间消息仅包含在发现检测策略中设置的更新间隔期间更改的主机上服务器的服务器信息。换句话说，只有自系统上次报告信息起已经更改的服务器才会包含到主机上次查看时间消息中。

注释　主机配置文件数据块因创建该消息的系统版本而异。有关主机配置文件数据块的旧版本的信息，请参阅旧版主机数据结构，第 B-362 页。



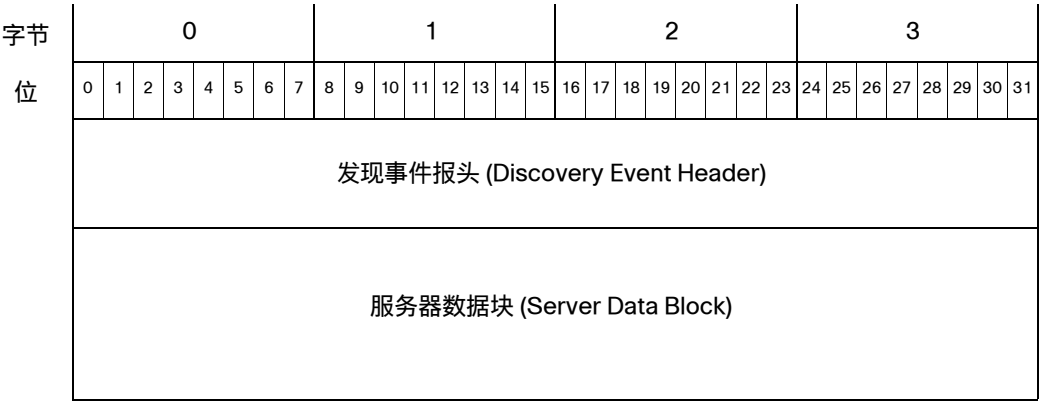
服务器消息

以下 TCP 和 UDP 服务器事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟服务器数据块（如主机服务器数据块 4.10.0+，第 4-139 页中所记录，系列 1 中的块类型 103）：

- 新 TCP 服务器
- 新 UDP 服务器
- TCP 服务器信息更新
- UDP 服务器信息更新
- TCP 服务器置信度更新
- UDP 服务器置信度更新

注释 服务器数据块因创建该消息的系统版本而异。有关服务器数据块的旧版本的信息，请参阅了解旧版数据结构，第 B-1 页。

这些事件都使用以下格式:



新网络协议消息

新网络协议事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟一个用于网络协议的两字节字段（使用下表中描述的协议值）。

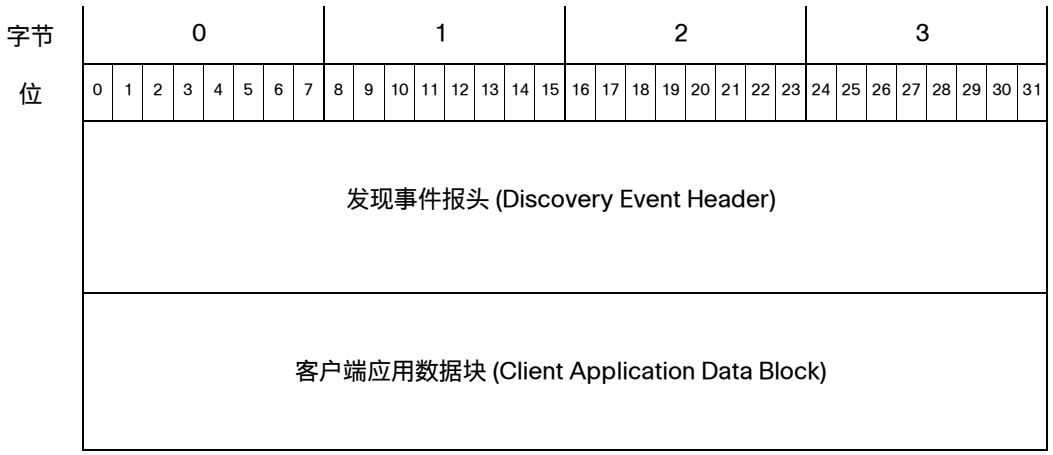
新传输协议消息

新传输协议事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录，系列 1 中的块类型 4），以及一个用于传输协议号的单字节字段（使用下表中描述的值）。

客户端应用消息

新客户端应用、客户端应用更新以及客户端应用超时事件具有相同格式，且都包含一个标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟一个客户端应用数据块（请参阅用于 5.0+ 的主机客户端应用数据块，第 4-157 页，系列 1 中的块类型 122）。发现事件报头具有不同的记录类型、事件类型和事件子类型，这取决于传输的事件。

注释　客户端应用数据块因创建该消息的系统版本而异。有关客户端应用数据块的旧版本的信息，请参阅了解旧版数据结构，第 B-1 页。



IP 地址更改消息

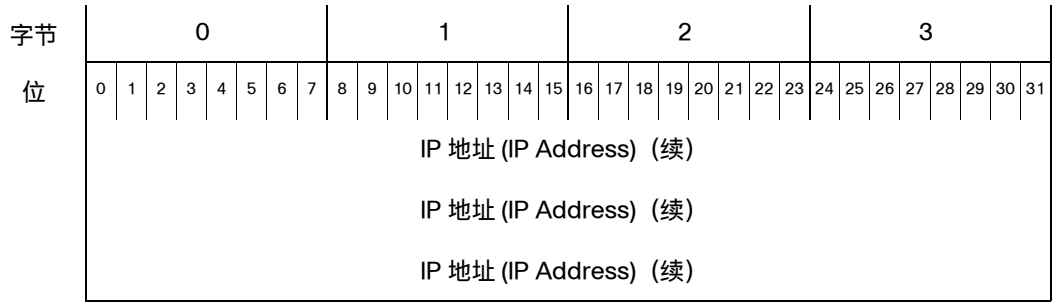
以下主机发现消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录）和两种不同的形式与结构，一种 IP 地址为四个字节，另一种 IP 地址为 16 个字节。

在以下情况下，IP 地址（采用 IP 地址八位组）为四个字节：

- 新 IPv4 到 IPv4 流量
- 主机 IP 地址已更改（当 RNA 事件版本低于 10 时）

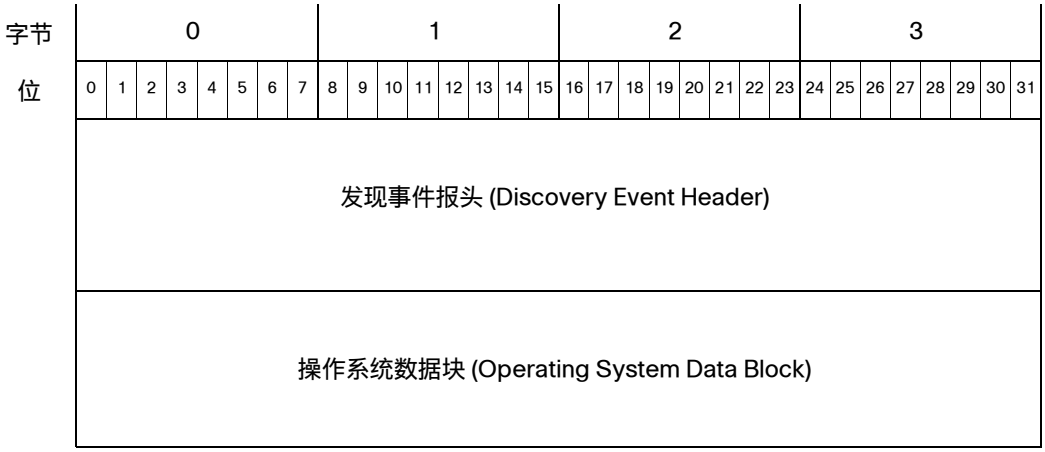
在以下情况下，IP 地址为 16 个字节：

- 新 IPv6 到 IPv6 流量
- 主机 IP 地址已更改（当 RNA 事件版本为 10 时）



操作系统更新消息

操作系统信息更新事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟操作系统数据块（如操作系统数据块 3.5+，第 4-83 页中所记录，系列1 中的块类型 53）。



IP 地址已重用和主机超时/已删除主机消息

以下主机事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），且无其他数据：

- 主机 IP 地址已重用
- 主机超时
- 已删除主机：已达主机限制
- 已丢弃主机：已达主机限制

跳数更改消息

跳数更改事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟一个用于跳数计数的单字节字段。

TCP 和 UDP 端口已关闭/超时消息

TCP 和 UDP 端口已关闭和端口超时事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟一个用于端口号的两字节字段。

MAC 地址消息

MAC 信息更改和检测到主机的其他 MAC 消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），1 个字节用于 TTL 值，6 个字节用于 MAC 地址，1 个字节用于指示通过 ARP/DHCP 流量检测的 MAC 地址是否为实际 MAC 地址。

注释　如果您从运行版本 4.9.x 的系统收到 MAC 地址消息，则必须检查该 MAC 地址数据块的长度并进行相应解码。如果该数据块的长度为8 个字节（加报头共 16 个字节），请参阅MAC 地址消息，第 4-49 页。如果该数据块的长度为 12 个字节（加报头共 20 个字节），请参阅主机 MAC 地址 4.9+，第 4-113 页。

请注意，MAC 地址数据块报头不用于 MAC 信息更改和检测到主机的其他 MAC 消息。

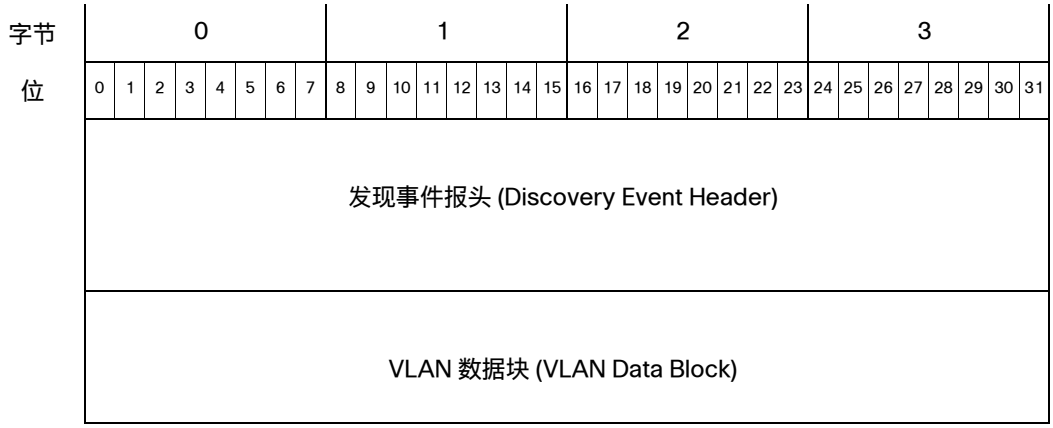
识别为路由器/网桥的主机消息

识别为路由器/网桥的主机事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟用于与主机类型匹配的值的四字节字段：

- 0 - 主机
- 1 - 路由器
- 2 - 网桥

VLAN 标签信息更新消息

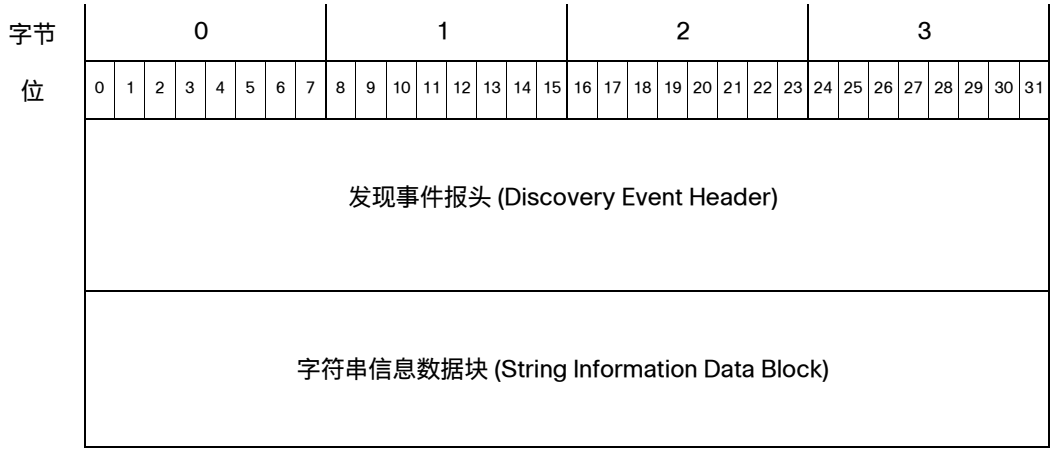
VLAN 标签信息更新事件具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟 VLAN 数据块（如VLAN 数据块，第 4-73 页中所记录）。VLAN 数据块的块类型为系列 1 数据块组中的 14。



更改 NetBIOS 名称消息

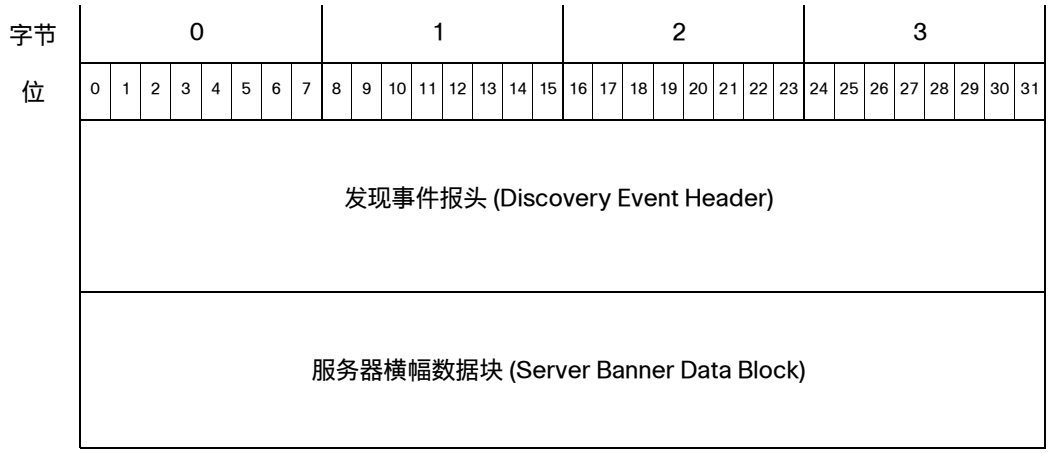
更改 NetBIOS 名称事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟一个字符串信息数据块（如字符串信息数据块，第 4-75 页中所记录）。字符串信息数据块的块类型为系列1 中的 35。

注释　目前，Cisco Secure Firewall 系统不生成更改 NetBIOS 域事件。



更新横幅消息

更新横幅事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟一个服务器横幅数据块（如服务器横幅数据块，第 4-74 页中所记录）。服务器横幅数据块的块类型为系列1 中的 37。



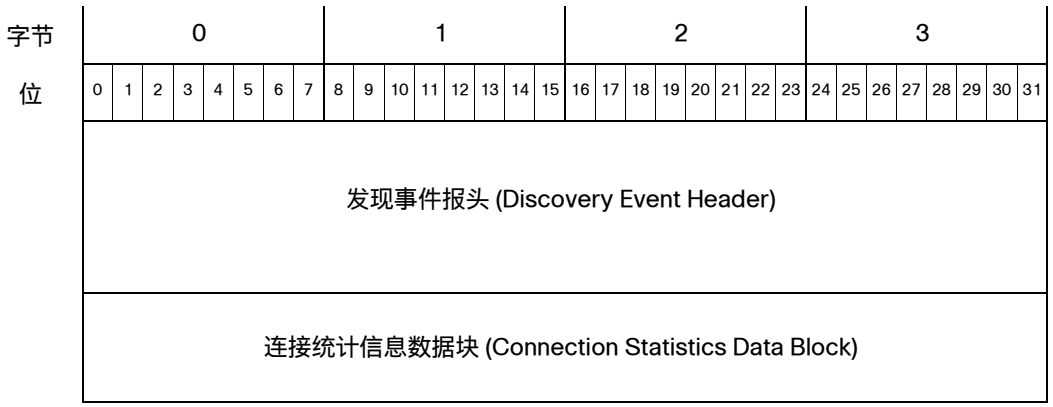
策略控制消息

策略控制消息事件具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟策略控制消息数据块。策略控制消息数据块的格式因系统版本而异。有关当前版本的策略控制消息数据块格式的信息，请参阅策略引擎控制消息数据块，第 4-84 页。

连接统计信息数据消息

连接统计信息事件具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟连接统计信息数据块。连接统计信息数据块的每个版本的文档都包含使用该数据块的系统版本。有关用于版本 6.1+ 的连接统计信息数据块格式的信息，请参阅连接统计信息数据块 7.1+，第 4-116 页。

注释　连接统计信息数据块因创建该消息的系统版本而异。有关旧版本的信息，请参阅了解旧版数据结构，第 B-1 页中的连接统计信息数据块。

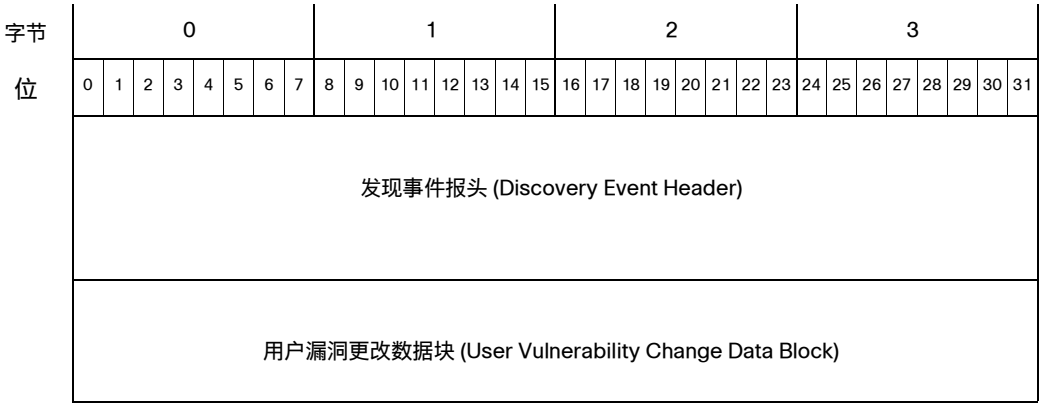


连接区块消息

连接区块事件具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟连接区块数据块。格式因系统版本而异。有关当前版本的连接区块数据块格式的信息，请参阅用于 6.1+ 的连接区块数据块，第 4-98 页。连接区块数据块的块类型为系列 1 中的 136。

用于版本 4.6.1+ 的用户设置漏洞消息

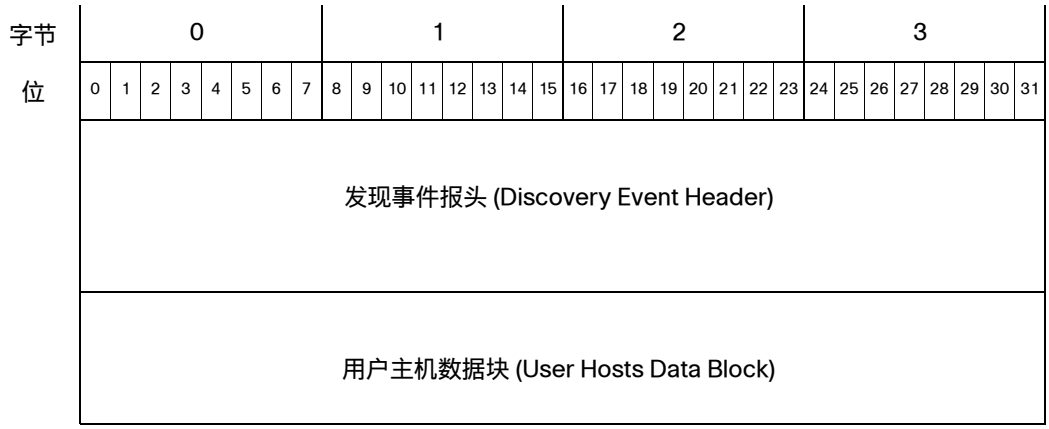
用户设置有效漏洞、用户设置无效漏洞以及用户漏洞限定条件消息使用相同的数据格式：标准发现事件报头（请参阅发现事件报头 5.2+，第 4-38 页），后跟用户漏洞更改数据块（请参阅用户漏洞更改数据块 4.7+，第 4-105 页，系列 1 中的块类型 80）。它们通过记录类型、事件类型和事件子类型进行区分。



用户添加和删除主机消息

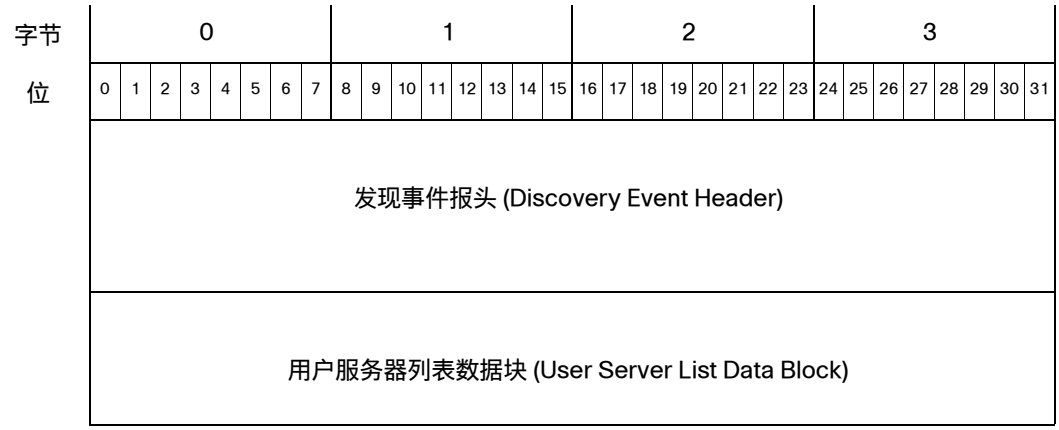
以下主机输入事件消息具有标准发现事件报头（请参阅发现事件报头 5.2+，第 4-38 页），后跟用户主机数据块（请参阅用户主机数据块 4.7+，第 4-103 页，系列 1 中的块类型 78）：

- 用户删除地址
- 用户添加主机



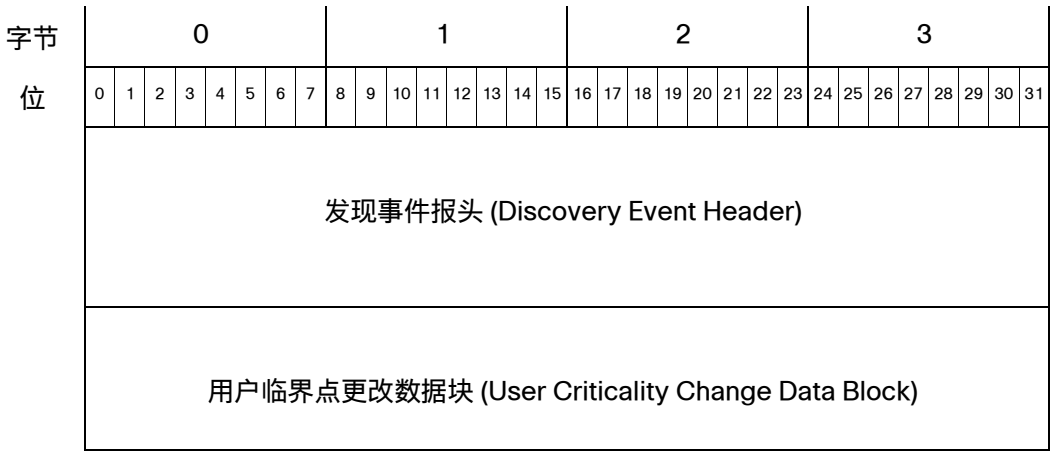
用户删除服务器消息

用户删除服务器消息具有标准发现事件报头（请参阅发现事件报头 5.2+，第 4-38 页），后跟用户服务器列表数据块（请参阅用户服务器列表数据块，第 4-102 页）。用户服务器列表数据块的块类型为系列 1 中的 77。



用户设置主机临界点消息

用户设置主机临界点消息具有标准发现事件报头（请参阅发现事件报头 5.2+，第 4-38 页），后跟用户临界点更改数据块（请参阅用户临界点更改数据块 4.7+，第 4-106 页）。用户临界点更改数据块的块类型为系列 1 中的 81。

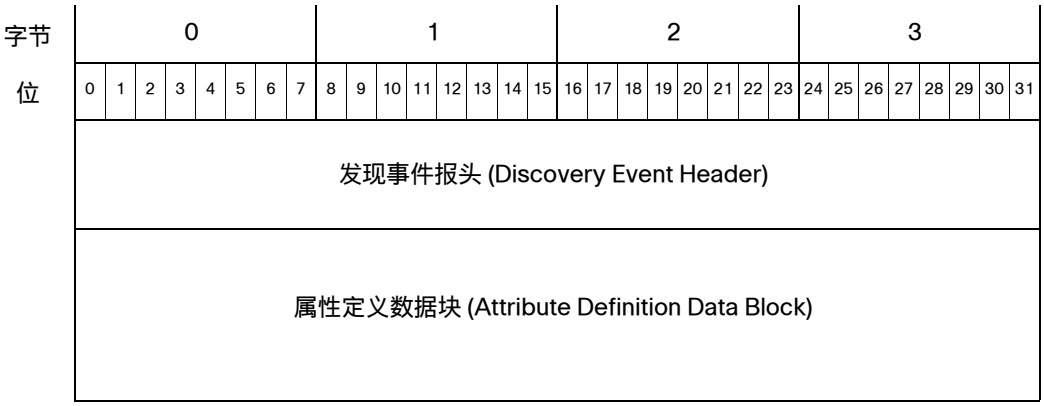


属性消息

以下事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟属性定义数据块（如用于 4.7+ 的属性定义数据块，第 4-85 页中所记录，系列 1 中的块类型 55）：

- 添加主机属性
- 更新主机属性
- 删除主机属性

这些事件都使用以下格式:

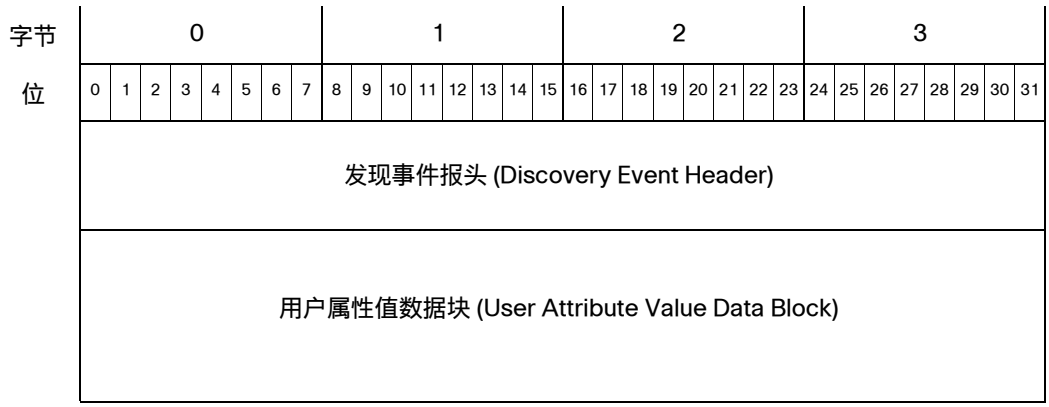


属性值消息

以下事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟用户属性值数据块（如用户属性值数据块 4.7+，第 4-108 页中所记录，系列 1 中的块类型 82）：

- 设置主机属性值
- 删除主机属性值

这些事件都使用以下格式:

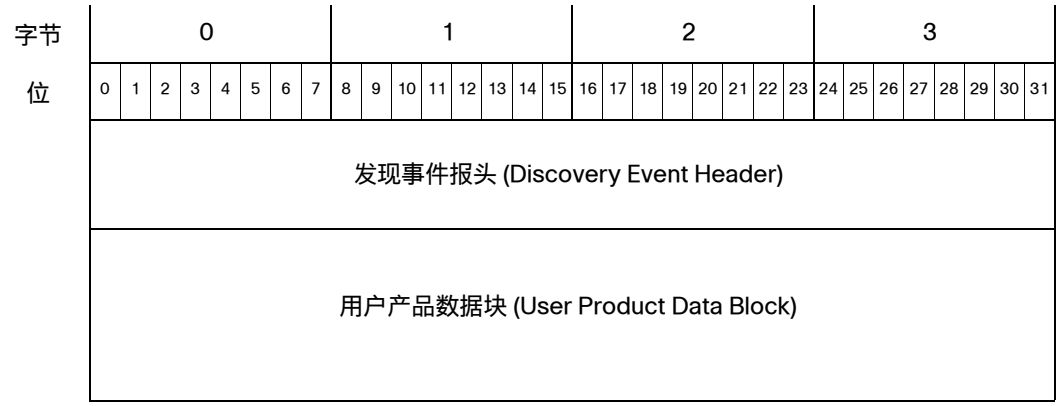


用户服务器和操作系统消息

以下事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），接着是用户产品数据块（如用户产品数据块 5.1+，第 4-173 页中所记录，系列 1 中的块类型 60）：

- 设置操作系统定义
- 设置服务器定义
- 添加服务器

这些事件都使用以下格式:

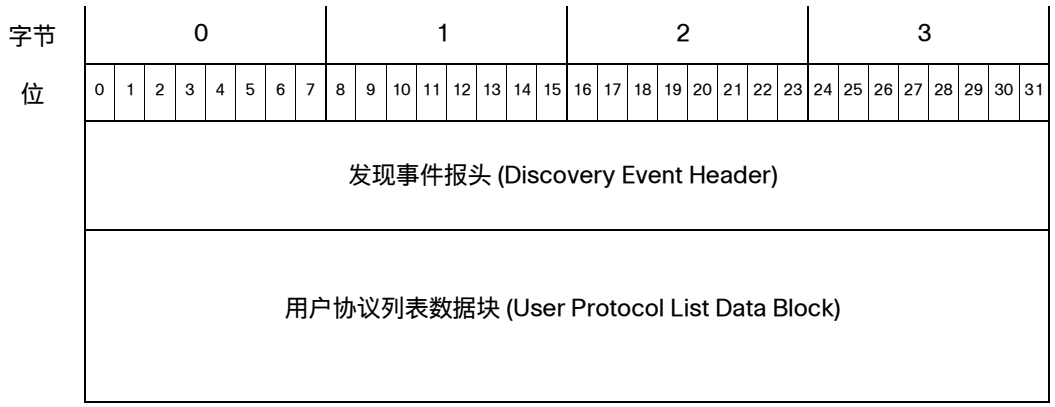


用户协议消息

以下事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟用户协议列表数据块（如用户协议列表数据块 4.7+，第 4-109 页中所记录，系列 1 中的块类型 83）：

- 删除协议
- 添加协议

这些事件都使用以下格式:

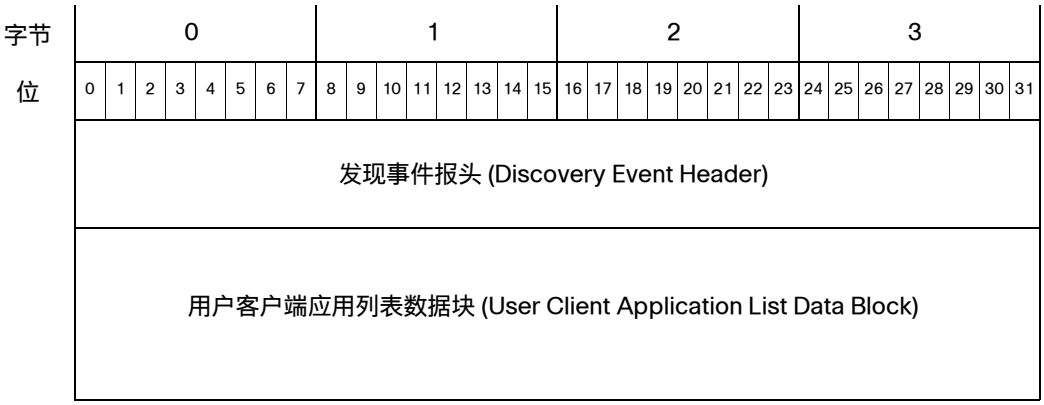


用户客户端应用消息

以下事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟用户客户端应用列表数据块（如用户客户端应用列表数据块，第 4-91 页中所记录，系列 1 中的块类型 60）：

- 删除客户端应用
- 添加客户端应用

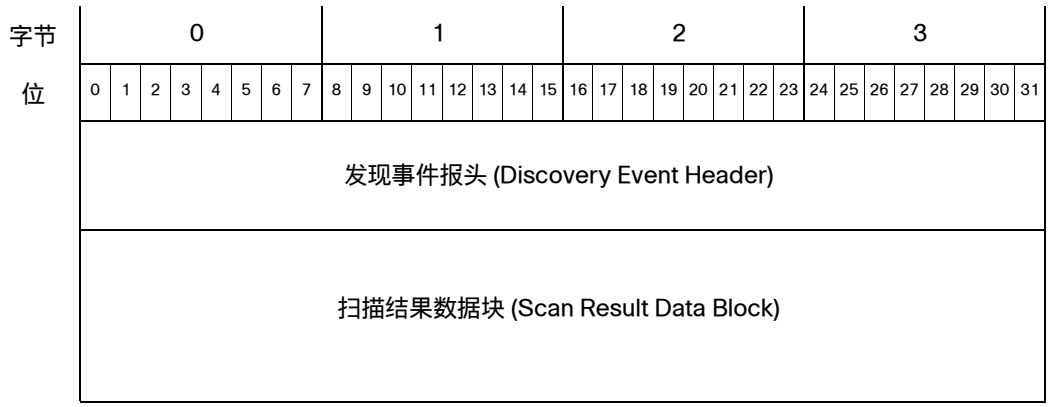
这些事件都使用以下格式:



添加扫描结果消息

添加扫描结果事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟扫描结果数据块（如扫描结果数据块 5.2+，第 4-136 页中所记录）。扫描结果数据块的块类型为系列 1 中的 142。

此事件使用以下格式:



新操作系统消息

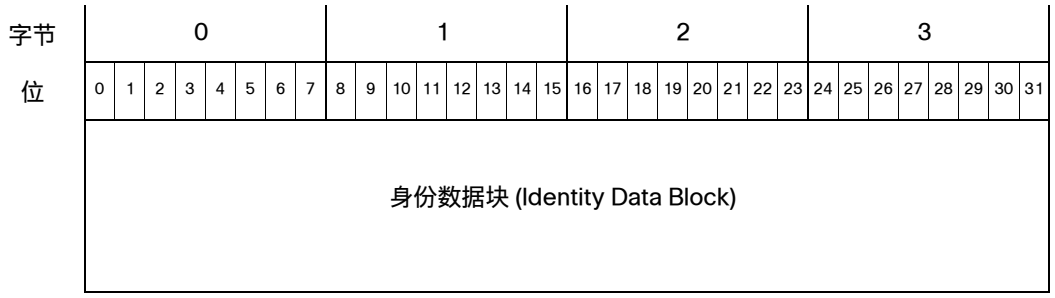
新操作系统事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟操作系统指纹数据块（如操作系统指纹数据块 5.1+，第 4-161 页中所记录）。

此事件使用以下格式:

身份冲突和身份超时系统消息

身份冲突和身份超时事件消息都具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟身份数据块（如身份数据块，第 4-112 页中所记录）。身份数据块的块类型为系列 1 中的 94。当指纹源身份中存在冲突或超时时，系统生成这些消息。

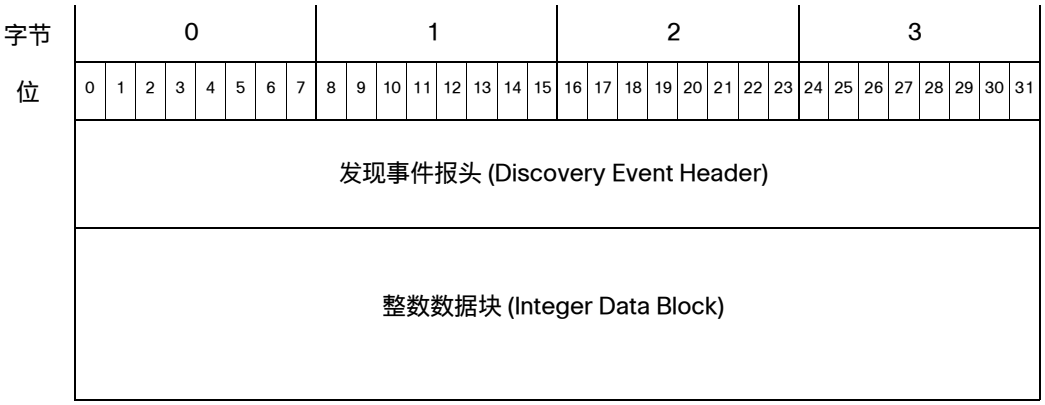
此事件使用以下格式:



主机 IOC 设置消息

主机 IOC 设置消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录），后跟整数数据块（如整数 (INT32) 数据块，第 4-73 页中所记录）。此整数数据块包含主机的 IOC 设置的 ID 号码。

此事件使用以下格式:



按事件类型划分的用户数据结构

eStreamer 根据发现事件报头中指示的事件类型构建用户事件消息。以下子节对每个事件类型的高级结构进行了说明:

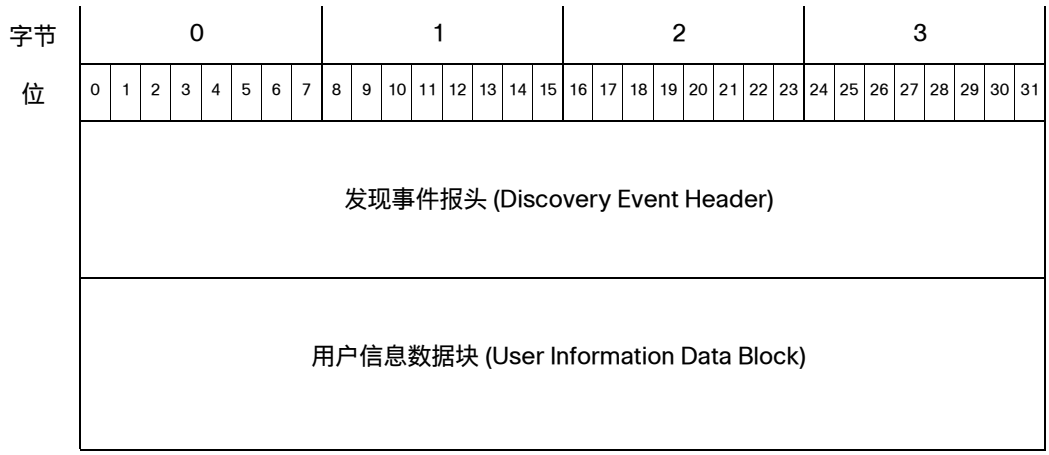
- 用户修改消息，第 4-58 页
- 用户信息更新消息块，第 4-59 页

用户修改消息

当通过系统检测发现以下任何事件时，系统会发送用户修改消息:

- 删除新用户（新用户身份事件 - 事件类型 1004，子类型 1）
- 删除用户（删除用户身份事件 - 事件类型 1004，子类型 3）
- 丢弃用户（已丢弃用户身份：已达用户限制事件 - 事件类型 1004，子类型 4）

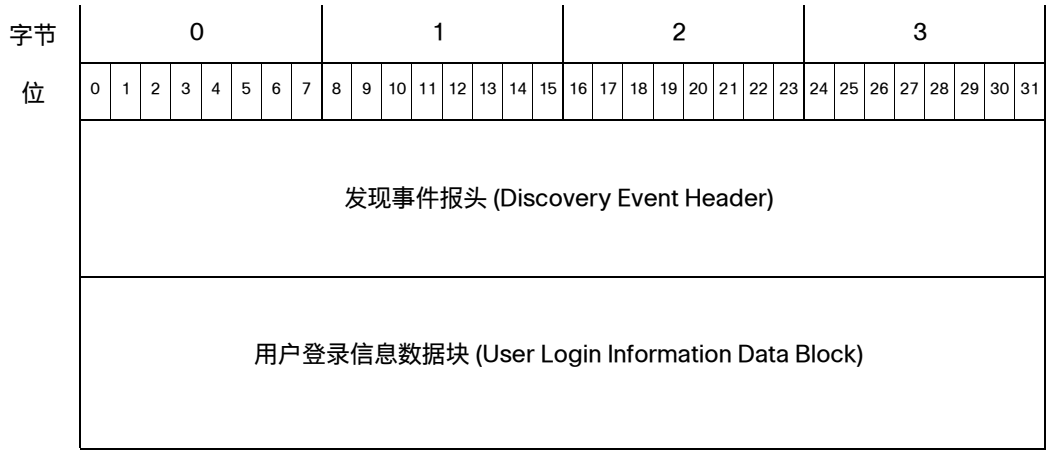
用户修改事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录）和用户信息数据块（如用于 6.0+ 的用户信息数据块，第 4-191 页中所记录）。用户信息数据块的块类型为系列 1 中的 120。



用户信息更新消息块

当系统检测到用户的登录出现变更（用户登录事件 - 事件类型 1004，子类型 2）时，系统会发送用户信息更新消息。当用户登录失败（失败的用户登录事件 - 事件类型 1004，子类型 5）、VPN 用户登录（VPN 用户登录事件 - 事件类型 1004，子类型 8）或 VPN 用户注销（VPN 用户注销事件 - 事件类型 1004，子类型 9）时，也会使用此块。

用户信息更新事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-38 页中所记录）和用户登录信息数据块（如用户登录信息数据块 6.2+，第 4-197 页中所记录）。用户登录信息数据块的块类型为系列 1 中的 121。

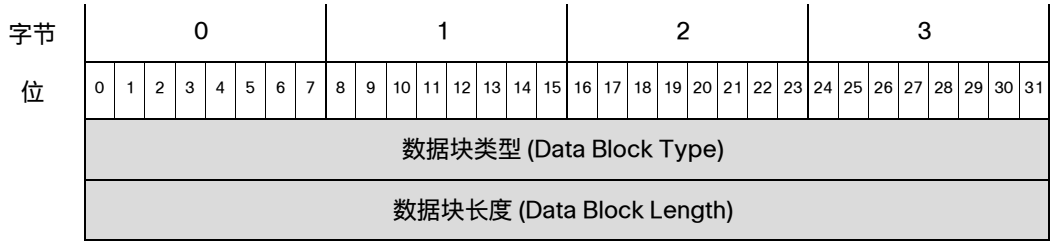


了解发现（系列 1）块

大多数发现和连接事件包含系列 1 数据结构组中的一个或多个数据块。每个系列 1 数据块类型传输一种特定类型的信息。块类型编号出现在数据块中数据前面的数据块报头中。有关块报头格式的信息，请参阅数据块报头，第 2-23 页。

系列 1 数据块报头

与系列 2 块报头一样，系列 1 数据块报头具有两个包含块类型编号和块长度的 32 位整数字段。



注释　数据块长度字段包含整个数据块中的字节数，包括两个数据块报头字段的八个字节。

对于某些系列 1 数据块类型，块报头后面紧跟原始数据。在更复杂的块类型中，报头后面可能是标准固定长度字段或封装其他系列 1 数据块或块列表的系列 1 基元块的报头。

系列 1 基元数据块

系列 1 和系列 2 块都包含一组封装消息中的可变长度块以及可变长度字符串和 BLOB 列表的基元。这些基元块具有上述标准系列 1 块报头。这些基元仅在其他系列 1 数据块中出现。给定的块类型可以包含任何数字。有关基元块的结构的详细信息，请参阅以下内容：

- 字符串数据块，第 4-67 页
- BLOB 数据块，第 4-68 页
- 列表数据块，第 4-69 页
- 通用列表块，第 4-70 页

主机发现和连接数据块

有关主机发现和连接事件中的块类型列表，请参阅表 4-30，第 4-61 页。表 4-86，第 4-180 页对用户事件中的块类型进行了说明。这些都是系列1 数据块。

下表中的每个条目都包含一个到定义数据块的子节的链接。表中指出了每个块类型的状态（当前版本或旧版本）。当前版本数据块是最新版本。旧数据块是用于产品的较旧版本的数据块，但仍然可以向 eStreamer 请求其消息格式。

表 4-30　主机发现和连接数据块类型

类型 (Type)	内容	数据块状态	说明
0	字符串	当前	包含字符串数据。有关详细信息，请参阅字符串数据块，第 4-67 页。
1	子服务器	当前	包含在服务器上检测到的子服务器的相关信息。有关详细信息，请参阅子服务器数据块，第 4-70 页。
4	协议 (Protocol)	当前	包含协议数据。有关详细信息，请参阅协议数据块，第 4-72 页。
7	整数数据	当前	包含整数（数字）数据。有关详细信息，请参阅整数 (INT32) 数据块，第 4-73 页。
10	BLOB	当前	包含一个原始二进制数据块，专门用于横幅。有关详细信息，请参阅BLOB 数据块，第 4-68 页。
11	列表	当前	包含其他数据块列表。有关详细信息，请参阅列表数据块，第 4-69 页。
14	VLAN	当前	包含 VLAN 信息。有关详细信息，请参阅VLAN 数据块，第 4-73 页。
20	入侵影响警报	当前	包含入侵影响警报信息。入侵影响警报事件的报头与其他数据块略有不同。有关详细信息，请参阅入侵影响警报数据 5.3+，第 3-19 页。
31	通用列表	当前	包含通用列表信息，例如用来将块（如客户端应用块）列表封装到主机配置文件块中。有关详细信息，请参阅通用列表块，第 4-70 页。
35	字符串信息	当前	包含字符串信息。例如，在扫描漏洞数据块中使用时，字符串信息数据块包含 CVE 标识号数据。请参阅字符串信息数据块，第 4-75 页。
37	服务器横幅	当前	包含服务器横幅数据。有关详细信息，请参阅服务器横幅数据块，第 4-74 页。
38	属性地址	传统	包含主机属性地址（如较早版本的产品中所记录）。后继块为 146。
39	属性列表项	当前	包含主机属性列表项值。有关详细信息，请参阅属性列表项数据块，第 4-78 页。
42	主机客户端应用	传统	包含用于新客户端应用事件的客户端应用信息（如较早版本的产品中所记录）。
47	完整主机配置文件	传统	包含完整主机配置文件信息（如较早版本的产品中所记录）。
48	属性值	当前	包含属性标识号和主机属性值。有关详细信息，请参阅属性值数据块，第 4-79 页。
51	完整子服务器	当前	包含在服务器上检测到的子服务器的相关信息。在完整服务器信息块和完整主机配置文件中引用。包含每个子服务器的漏洞信息。有关详细信息，请参阅完整子服务器数据块，第 4-81 页。

表 4-30 主机发现和连接数据块类型 （续）

类型 (Type)	内容	数据块状态	说明
53	操作系统	当前	包含用于版本 3.5+ 的操作系统信息。有关详细信息，请参阅操作系统数据块 3.5+，第 4-83 页。
54	策略引擎控制消息	当前	包含有关用户策略控制更改的信息。有关详细信息，请参阅策略引擎控制消息数据块，第 4-84 页。
55	属性定义	当前	包含有关属性定义的信息。有关详细信息，请参阅用于 4.7+ 的属性定义数据块，第 4-85 页。
56	连接统计信息	传统	包含有关 4.7 - 4.9.0 中连接统计信息事件的信息（如较早版本的产品中所记录）。
57	用户协议	当前	包含用户输入的协议信息。有关详细信息，请参阅用户协议数据块，第 4-88 页。
59	用户客户端应用	传统	包含用户输入的客户端应用数据。有关详细信息，请参阅用于 5.0 - 5.1 的用户客户端应用数据块，第 B-124 页。被块 138 替代。
60	用户客户端应用列表	当前	包含用户客户端应用数据块的列表。有关详细信息，请参阅用户客户端应用列表数据块，第 4-91 页。
61	IP 范围规格	传统	包含 IP 地址范围规格。有关详细信息，请参阅用于 5.0 - 5.1.1.x 的 IP 范围规格数据块，第 B-401 页。被块 141 替代。
62	属性规格	当前	包含属性名称和值。有关详细信息，请参阅属性规格数据块，第 4-94 页。
63	MAC 地址规格	当前	包含 MAC 地址范围规格。有关详细信息，请参阅MAC 地址规格数据块，第 4-96 页。
64	IP 地址规格	当前	包含 IP 和 MAC 地址规格块列表。有关详细信息，请参阅地址规格数据块，第 4-97 页。
65	用户产品	传统	包含从第三方应用导入的主机输入数据，包括第三方应用字符串映射。有关详细信息，请参阅用于 5.0.x 的用户产品数据块，第 B-129 页。5.0 中引入的后继块类型 118 的结构与块类型 65 的结构相同。
66	连接区块	传统	包含连接区块信息。有关详细信息，请参阅用于 5.0 - 5.1 的连接区块数据块，第 B-182 页。5.0 中引入的后继块类型 119 的结构与块类型 66 的结构相同。
67	修复列表	当前	包含适用于主机的修复。有关详细信息，请参阅修复列表数据块，第 4-100 页。
71	一般扫描结果	传统	包含 Nmap 扫描的结果（如较早版本的产品中所记录）。
72	扫描结果	传统	包含第三方扫描的结果（如较早版本的产品中所记录）。

表 4-30　主机发现和连接数据块类型 （续）

类型 (Type)	内容	数据块状态	说明
76	用户服务器	当前	包含用户输入事件的服务器信息。有关详细信息，请参阅用户服务器数据块，第 4-101 页。
77	用户服务器列表	当前	包含用户服务器块列表。有关详细信息，请参阅用户服务器列表数据块，第 4-102 页。
78	用户主机	当前	包含用户主机输入事件的主机范围的相关信息。有关详细信息，请参阅用户主机数据块 4.7+，第 4-103 页。
79	用户漏洞	传统	包含一个或多个主机的漏洞相关信息（如较早版本的产品中所记录）。版本 5.0 中引入的后继块的块类型为 124。
80	用户主机漏洞更改	当前	包含停用或激活的漏洞的列表。有关详细信息，请参阅用户漏洞更改数据块 4.7+，第 4-105 页。
81	用户临界点	当前	包含一个或多个主机的临界点更改相关信息。有关详细信息，请参阅用户临界点更改数据块 4.7+，第 4-106 页。
82	用户属性值	当前	包含一个或多个主机的属性值更改。有关详细信息，请参阅用户属性值数据块 4.7+，第 4-108 页。
83	用户协议列表	当前	包含一个或多个主机的协议列表。有关详细信息，请参阅用户协议列表数据块 4.7+，第 4-109 页。
85	漏洞列表	当前	包含适用于主机的漏洞。有关详细信息，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
86	扫描漏洞	传统	包含有关扫描检测到的漏洞的信息（如较早版本的产品中所记录）。
87	操作系统指纹	传统	包含操作系统指纹列表。有关详细信息，请参阅用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-160 页。版本 5.1 中引入的后继块的块类型为 130。
88	服务器信息	传统	包含服务器指纹中使用的服务器信息（如较早版本的产品中所记录）。
89	主服务器	传统	包含主机的服务器信息（如较早版本的产品中所记录）。
90	完整主机服务器	传统	包含主机的服务器信息（如较早版本的产品中所记录）。
91	主机配置文件	传统	包含主机的配置文件信息。有关详细信息，请参阅用于 5.2+ 的主机配置文件数据块，第 4-164 页。版本 5.1 中引入的后继块的块类型为 132。
92	完整主机配置文件	传统	包含完整主机配置文件信息（如较早版本的产品中所记录）。替代数据块 47。
94	身份数据	当前	包含主机的身份数据。有关详细信息，请参阅身份数据块，第 4-112 页。

表 4-30 主机发现和连接数据块类型 （续）

类型 (Type)	内容	数据块状态	说明
95	主机 MAC 地址	当前	包含主机的 MAC 地址信息。有关详细信息，请参阅主机 MAC 地址 4.9+，第 4-113 页。
96	辅助主机更新	当前	包含辅助辅助主机更新，第 4-114 页报告的 MAC 地址信息列表。
97	Web 应用程序	传统	包含 Web 应用数据列表（如较早版本的产品中所记录）。版本 5.0 中引入的后继块的块类型为 123。
98	主服务器	传统	包含主机的服务器信息（如较早版本的产品中所记录）。
99	完整主机服务器	传统	包含主机的服务器信息（如较早版本的产品中所记录）。
100	主机客户端应用	传统	包含用于新客户端应用事件的客户端应用信息（如较早版本的产品中所记录）。5.0中引入的后继块类型 122 的结构与块类型 100 的结构相同。
101	连接统计信息	传统	包含有关 4.9.1+ 中连接统计信息事件的信息（如较早版本的产品中所记录）。
102	扫描结果	传统	包含漏洞的相关信息，且在”添加扫描结果“事件中使用。请参阅扫描结果数据块 5.0 - 5.1.1.x，第 B-126 页。
103	主服务器	当前	包含主机的服务器信息。有关详细信息，请参阅主机服务器数据块 4.10.0+，第 4-139 页。
104	完整主机服务器	当前	包含主机的服务器信息。有关详细信息，请参阅完整主机服务器数据块 4.10.0+，第 4-141 页。
105	服务器信息	传统	包含服务器指纹中使用的服务器信息。有关详细信息，请参阅用于 4.10.x、5.0 - 5.0.2 的服务器信息数据块，第 4-145 页。5.0 中引入的后继块类型 117 的结构与块类型 105 的结构相同。
106	完整服务器信息	当前	包含在主机上检测到的服务器的相关信息。有关详细信息，请参阅完整服务器信息数据块，第 4-147 页。
108	一般扫描结果	当前	包含 Nmap 扫描的结果。有关详细信息，请参阅用于 4.10.0+ 的一般扫描结果数据块，第 4-150 页。
109	扫描漏洞	当前	包含有关第三方扫描检测到的漏洞的信息。请参阅用于 4.10.0+ 的扫描漏洞数据块，第 4-152 页。
111	完整主机配置文件	传统	包含完整主机配置文件信息。有关详细信息，请参阅完整主机配置文件数据块 5.0 - 5.0.2，第 B-363 页。替代数据块 92。
112	完整主机客户端应用	当前	包含用于新客户端应用事件的客户端应用信息，且包含漏洞列表。有关详细信息，请参阅完整主机客户端应用数据块 5.0+，第 4-155 页。

表 4-30　主机发现和连接数据块类型 （续）

类型 (Type)	内容	数据块状态	说明
115	连接统计信息	传统	包含 5.0 - 5.0.2 中连接统计信息事件的信息。有关详细信息，请参阅连接统计信息数据块 5.0 - 5.0.2，第 B-162 页。版本 5.1 中引入的后继块的块类型为 126。
117	服务器信息	当前	包含服务器指纹中使用的服务器信息。有关详细信息，请参阅用于 4.10.x、5.0 - 5.0.2 的服务器信息数据块，第 4-145 页。
118	用户产品	传统	包含从第三方应用导入的主机输入数据，包括第三方应用字符串映射。有关详细信息，请参阅用于 5.0.x 的用户产品数据块，第 B-129 页。先趋块类型 65（在 5.0 中替代）的结构与此块类型的结构相同。版本 5.1 中引入的后继块的块类型为 132。
119	连接区块	传统	包含用于版本 4.10.1 - 5.1 的连接区块信息。有关详细信息，请参阅用于 5.0 - 5.1 的连接区块数据块，第 B-182 页。后继块为 136。
122	主机客户端应用	当前	包含用于版本 5.0+ 的新客户端应用事件的客户端应用信息。有关详细信息，请参阅用于 5.0+ 的主机客户端应用数据块，第 4-157 页。它替代块类型100。
123	Web 应用程序	当前	包含用于版本 5.0+ 的 Web 应用数据。有关详细信息，请参阅用于 5.0+ 的 Web 应用数据块，第 4-115 页。它替代块类型97。
124	用户漏洞	当前	包含一个或多个主机的漏洞相关信息。请参阅用户漏洞数据块 5.0+，第 4-159 页。它替代块类型 79。
125	连接统计信息	传统	包含有关 4.10.2 中连接统计信息事件的信息（如较早版本的产品中所记录）。版本 5.1 中引入的后继块的块类型为 115。
126	连接统计信息	传统	包含 5.1 中连接统计信息事件的信息。有关详细信息，请参阅连接统计信息数据块 5.1，第 B-168 页。它替代块类型 115。此块类型被块类型 137 替代。
130	操作系统指纹	当前	包含操作系统指纹列表。有关详细信息，请参阅操作系统指纹数据块 5.1+，第 4-161 页。它替代块类型87。
131	移动设备信息	当前	包含检测到的移动设备的硬件的相关信息。有关详细信息，请参阅用于 5.1+ 的移动设备 信息数据块，第 4-163 页。
132 个	主机配置文件	传统	包含主机的配置文件信息。有关详细信息，请参阅完整主机配置文件数据块 5.2.x，第 B-381 页。它替代块类型 91。被块 139 替代。

表 4-30 主机发现和连接数据块类型 （续）

类型 (Type)	内容	数据块状态	说明
134	用户产品	当前	包含从第三方应用导入的主机输入数据，包括第三方应用字符串映射。有关详细信息，请参阅用户产品数据块 5.1+，第 4-173 页。这替代先趋块类型 118。
135	完整主机配置文件	传统	包含完整主机配置文件信息。有关详细信息，请参阅完整主机配置文件数据块 5.1.1，第 B-372 页。替代数据块 111。
136	连接区块	当前	包含连接区块信息。有关详细信息，请参阅用于 6.1+ 的连接区块数据块，第 4-98 页。替代块 119。
137	连接统计信息	传统	包含 5.1.1 中连接事件的信息。有关详细信息，请参阅用于 5.0 - 5.1 的连接区块数据块，第 B-182 页。它替代块类型 126。它被块类型 144 替代。
138	用户客户端应用	当前	包含用户输入的客户端应用数据。有关详细信息，请参阅用于 5.1.1+ 的用户客户端应用数据块，第 4-90 页。它替代块类型 。
139	主机配置文件	当前	包含主机的配置文件信息。有关详细信息，请参阅用于 5.2+ 的主机配置文件数据块，第 4-164 页。它替代块类型 132。
140	完整主机配置文件	传统	包含完整主机配置文件信息。有关详细信息，请参阅完整主机配置文件数据块 5.3+，第 5-1 页。替代数据块 135。
141	IP 范围规格	当前	包含 IP 地址范围规格。有关详细信息，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-93 页。它替代块 61。
142	扫描结果	当前	包含漏洞的相关信息，且在添加扫描结果事件中使用。请参阅扫描结果数据块 5.2+，第 4-136 页。它替代块 102。
143	主机 IP	当前	包含主机的 IP 地址和上次查看时间信息。有关详细信息，请参阅主机 IP 地址数据块，第 4-95 页。
144 个	连接统计信息	传统	包含 5.2.x 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 5.2.x，第 B-175 页。它替代块类型 137。
146	属性地址	当前	包含 5.2+ 的主机属性地址。有关详细信息，请参阅属性地址数据块 5.2+，第 4-76 页。它替代块类型 38。
148	用户 IOC 更改	当前	包含有关用户 IOC 更改的信息。有关详细信息，请参阅用户 IOC 更改数据块 5.3+，第 4-77 页。
149	完整主机配置文件	当前	包含完整主机配置文件信息。有关详细信息，请参阅完整主机配置文件数据块 5.3+，第 5-1 页。替代数据块 135。

表 4-30　　主机发现和连接数据块类型 （续）

类型 (Type)	内容	数据块状态	说明
152	连接统计信息	传统	包含 5.3+ 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 5.3，第 B-192 页。它替代块类型 144。
154 种	连接统计信息	传统	包含 5.3 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 5.3.1，第 B-201 页。它替代块类型 152。
155	连接统计信息	传统	包含 5.4 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 5.4，第 B-208 页。它替代块类型 154。
157	连接统计信息	传统	包含 5.4.1 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 5.4.1，第 B-221 页。它替代块类型 155。
160	连接统计信息	传统	包含 5.4.1 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 6.0.x，第 B-236 页。它替代块类型 157。
163	连接统计信息	当前	包含 6.0+ 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 7.1+，第 4-116 页。它替代块类型 160。

字符串数据块

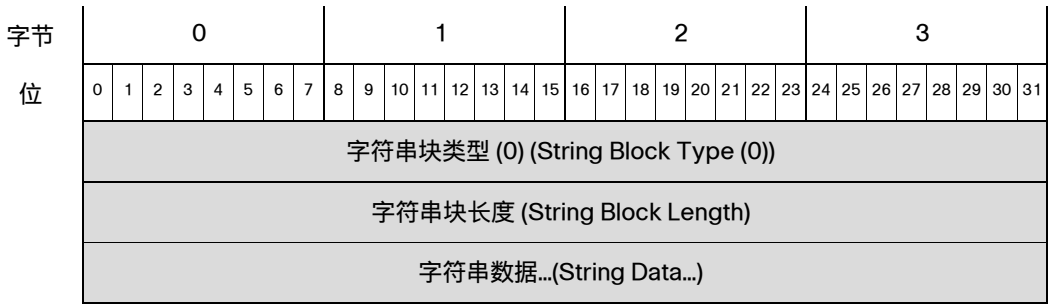
字符串数据块用于发送系列 1 块中的字符串数据。字符串数据块通常出现在其他系列 1 数据块中，用于描述操作系统或服务器名称等。

空字符串数据块（不包含任何字符串数据的字符串数据块）的块长度值为 8，随后是零字节字符串数据。字符串值没有任何内容时返回空字符串数据块，可能出现这种情况的一个例子是，操作系统的供应商未知时操作系统数据块中的操作系统供应商字符字段。

字符串数据块的块类型为系列 1 数据块组中的 0。

注释　此数据块中返回的字符串不总是以空值终止（即不总是以 0 终止）。

下图显示字符串数据块的格式:



下表对字符串数据块的字段进行了说明。

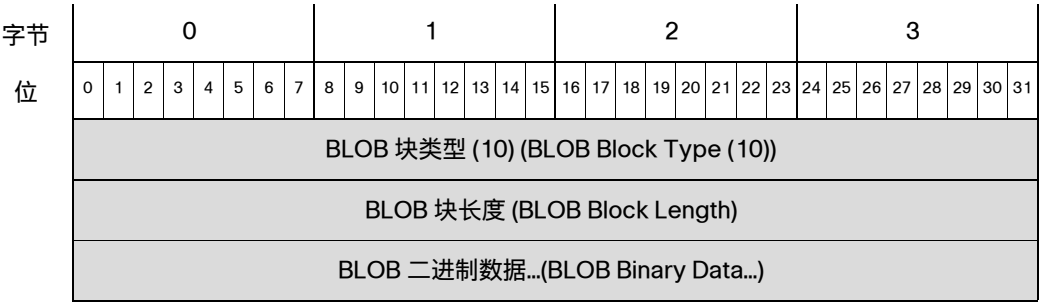
表 4-31 字符串数据块字段

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块报头与字符串数据的总长度。
字符串数据 (String Data)	字符串	包含字符串数据，且可能在字符串结尾包含一个终止字符（空字节）。

BLOB 数据块

BLOB 数据块可用于传输二进制数据。例如，用于承载系统捕获的服务器横幅。BLOB 数据块的块类型为系列 1 数据块组中的 10。

下图显示 BLOB 数据块的格式:



下表对 BLOB 数据块的字段进行了说明。

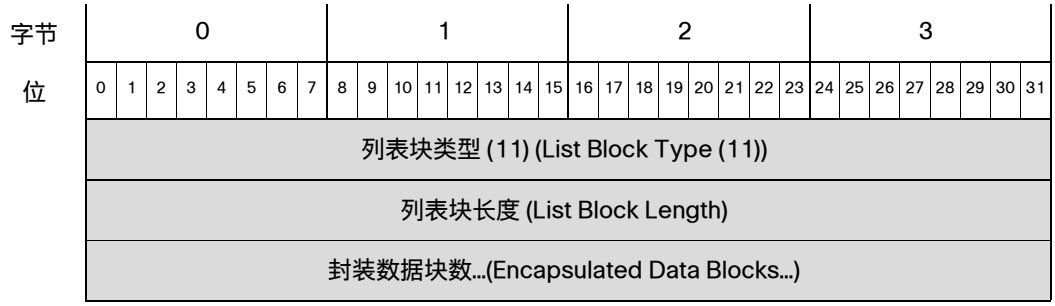
表 4-32　　BLOB 数据块字段

字段	数据类型	说明 (Description)
BLOB 块类型 (BLOB Block Type)	uint32	启动 BLOB 数据块。值始终为 10。
BLOB 块长度 (BLOB Block Length)	uint32	BLOB 数据块中的字节数，包括 BLOB 块类型和长度字段的八个字节，加上随后的二进制数据的长度。
二进制数据 (Binary Data)	变量	包含二进制数据，通常是服务器横幅。

列表数据块

列表数据块用于封装系列 1 数据块列表。例如，如果正在传输 TCP 服务器列表，则包含数据的服务器数据块封装在列表数据块中。列表数据块的块类型为系列 1 数据块组中的 11。

下图显示列表数据块的基本格式:



下表对列表数据块的字段进行了说明。

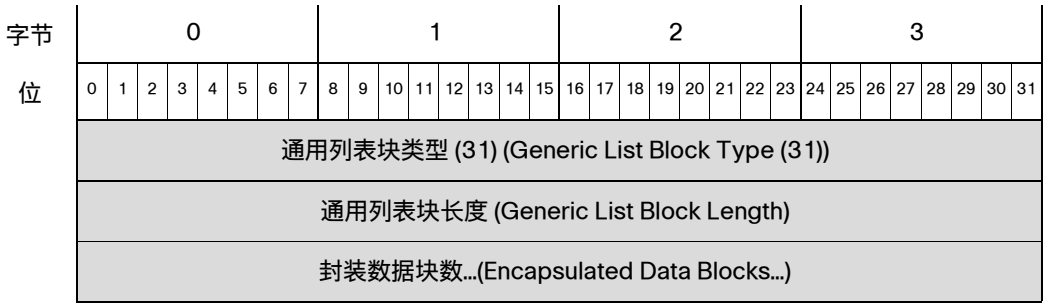
表 4-33　　列表数据块字段

字段	数据类型	说明 (Description)
列表块类型 (List Block Type)	uint32	启动列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表块和封装数据中的字节数。例如，如果列表中包含三个子服务器数据块，则此处的值包含子服务器数据块中的字节数，加上列表块报头的八个字节。
封装数据块数 (Encapsulated Data Blocks)	变量	封装数据块数最多可以是列表块长度中的最大字节数。

通用列表块

通用列表数据块用于封装系列 1 数据块列表。例如，当在主机配置文件数据块中传输客户端应用信息时，客户端应用数据块列表封装在通用列表数据块中。通用列表数据块的块类型为系列 1 数据块组中的 31。

下图显示通用列表数据块的基本结构:



下表对通用列表数据块的字段进行了说明。

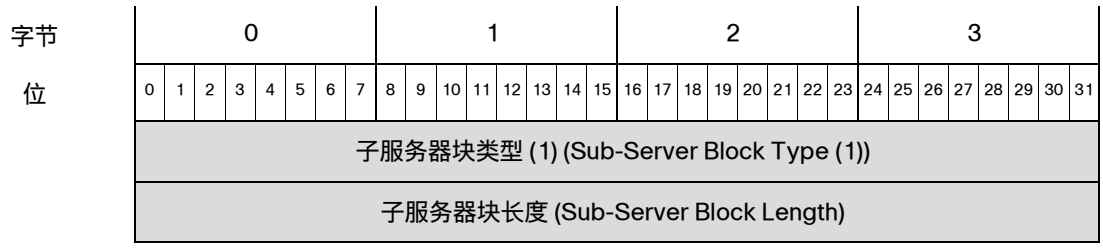
表 4-34 通用列表数据块字段

字段	字节数	说明 (Description)
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
封装数据块数 (Encapsulated Data Blocks)	变量	封装数据块数最多可以是列表块长度中的最大字节数。

子服务器数据块

子服务器数据块传输单个子服务器的相关信息，该服务器是同一主机上的其他服务器调用的服务器且具有相关漏洞。子服务器数据块的块类型为系列 1 数据块组中的 1。

下图显示子服务器数据块的格式:



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
子服务器名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	子服务器名称...(Sub-Server Name...)																															
供应商名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	供应商名称...(Vendor Name...)																															
版本版本	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	版本...(Version...)																															

下表对子服务器数据块的字段进行了说明。

表 4-35　　子服务器数据块字段

字段	数据类型	说明 (Description)
子服务器块类型 (Sub-Server Block Type)	uint32	启动子服务器数据块。值始终为 1。
子服务器块长度 (Sub-Server Block Length)	uint32	子服务器数据块中的字节总数，包括子服务器块类型和长度字段的八个字节，加上随后的数据字节数。
字符串块类型 (String Block Type)	uint32	启动包含子服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	子服务器名称字符串数据块中的字节数，包括字符串块类型和长度字段，加上子服务器名称中的字节数。
子服务器名称 (Sub-Server Name)	字符串	子服务器的名称。
字符串块类型 (String Block Type)	uint32	启动包含子服务器供应商的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	供应商名称字符串数据块中的字节数，包括字符串块类型和长度字段，加上供应商名称中的字节数。
供应商名称 (Vendor Name)	字符串	子服务器供应商名称。
字符串块类型 (String Block Type)	uint32	启动包含子服务器版本的字符串数据块。值始终为 0。

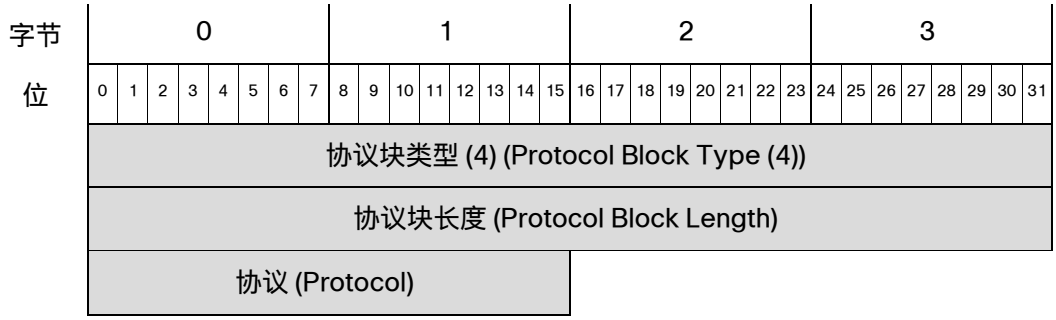
表 4-35 子服务器数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	子服务器版本字符串数据块中的字节数，包括字符串块类型和长度字段，加上版本中的字节数。
版本	字符串	子服务器版本。

协议数据块

协议数据块定义协议。它是非常简单的数据块，只有块类型、块长度和识别协议的 IANA 协议号。协议数据块的块类型为系列 1 数据块组中的 4。

下图显示协议数据块的格式:



下表对协议数据块的字段进行了说明。

表 4-36 协议数据块字段

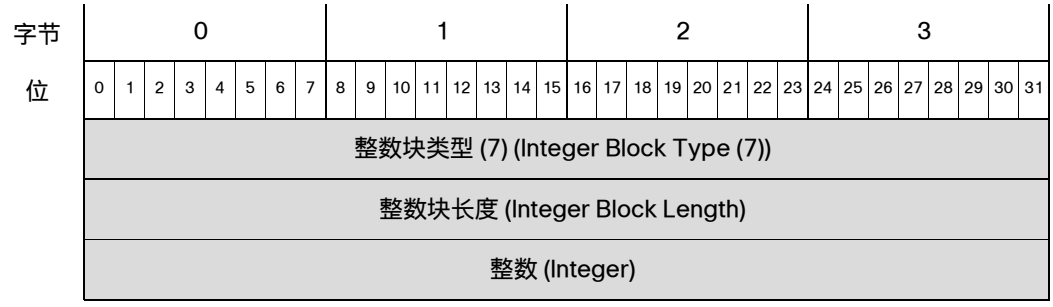
字段	数据类型	说明 (Description)
协议块类型 (Protocol Block Type)	uint32	启动协议数据块。值始终为 4。
协议块长度 (Protocol Block Length)	uint32	协议数据块中的字节数。值始终为 10。
协议 (Protocol)	uint16	IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如: ▪ 6 - TCP ▪ 17 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如: ▪ 2048 - IP

整数 (INT32) 数据块

整数 (INT32) 数据块在列表数据块中使用，用于传输 32 位整数数据。

整数数据块的块类型为系列 1 数据块组中的 7。

下图显示整数数据块的格式:



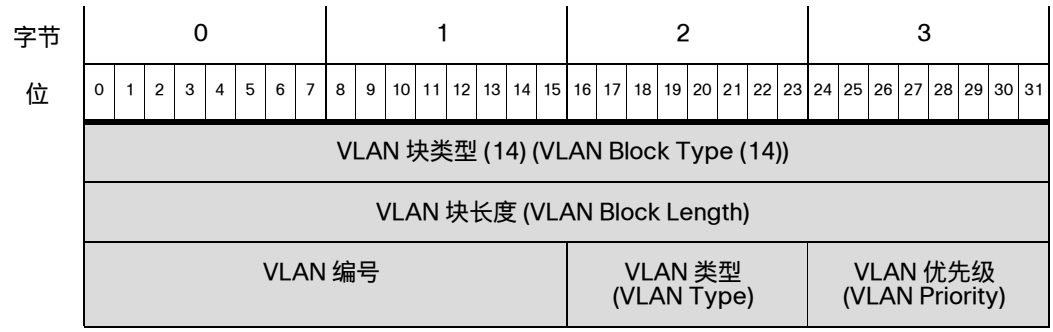
下表对整数数据块的字段进行了说明:

表 4-37　　整数数据块字段

字段	数据类型	说明 (Description)
整数块类型 (Integer Block Type)	uint32	启动整数数据块。值始终为 7。
整数块长度 (Integer Block Length)	uint32	整数数据块中的字节数。值始终为 12。
整数 (Integer)	uint32	包含整数值。

VLAN 数据块

VLAN 数据块包含主机的 VLAN 标签信息。VLAN 数据块的块类型为系列 1 数据块组中的 14。下图显示 VLAN 数据块的格式:



下表对 VLAN 数据块的字段进行了说明。

表 4-38 VLAN 数据块字段

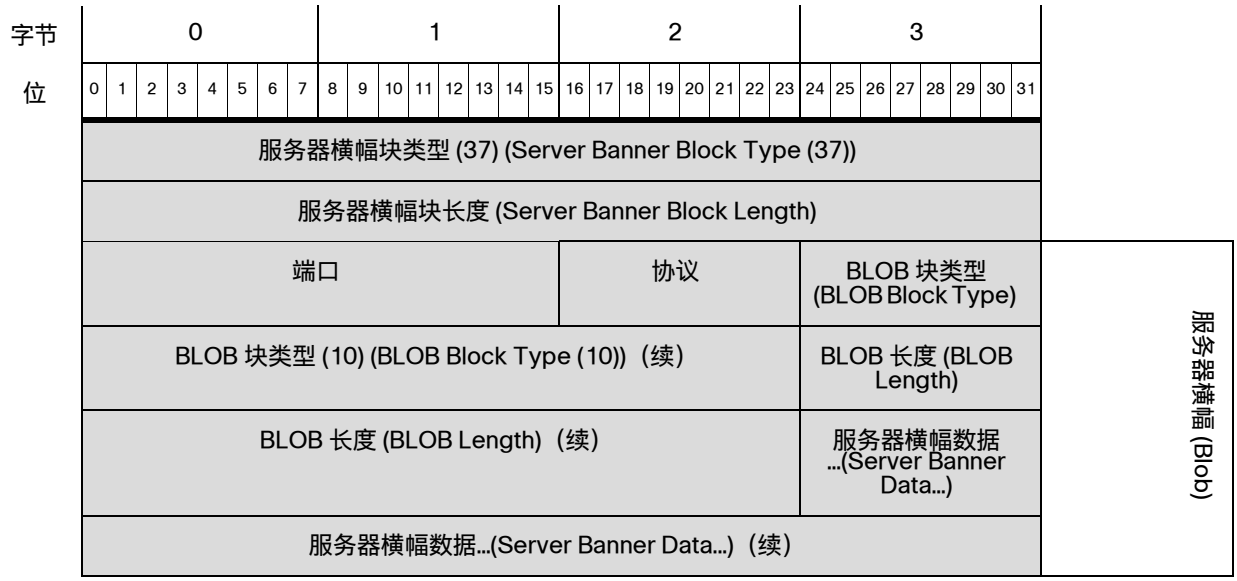
字段	数据类型	说明 (Description)
VLAN 块类型 (VLAN Block Type)	uint32	启动 VLAN 数据块。值始终为 14。
VLAN 块长度 (VLAN Block Length)	uint32	VLAN 数据块中的字节数。值始终为 12。
VLAN ID	uint16	包含表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。 ▪ 0 - 以太网 ▪ 1 - 令牌环
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。

服务器横幅数据块

服务器横幅数据块提供有关主机上运行的服务器的横幅的信息。它包含服务器端口、协议以及横幅数据。服务器横幅数据块的块类型为系列 1 数据块组中的 37。

下图显示服务器横幅数据块的格式。

注释 下图中块类型字段旁边的星号 (*) 表示该消息可能包含零个或多个系列 1 数据块实例。



下表对服务器横幅数据块的字段进行了说明。

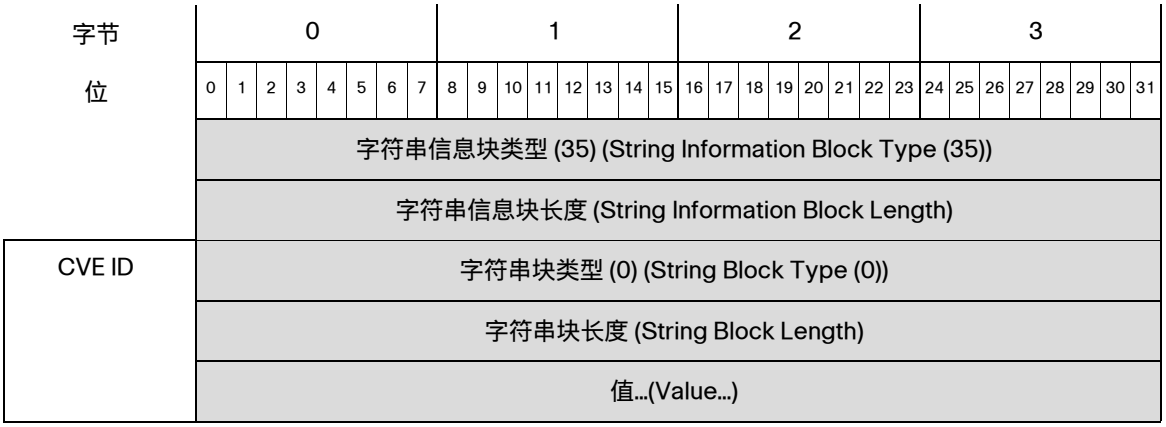
表 4-39　　服务器横幅数据块字段

字段	数据类型	说明 (Description)
服务器横幅块类型 (Server Banner Block Type)	uint32	启动服务器横幅数据块。值始终为 37。
服务器横幅块长度 (Server Banner Block Length)	uint32	服务器横幅数据块中的字节总数，包括服务器横幅块类型和长度字段的八个字节，加上随后的数据字节数。
端口 (Port)	uint16	服务器在其上运行的端口的端口号。
协议 (Protocol)	uint8	服务器的协议号。
BLOB 块类型 (BLOB Block Type)	uint32	启动包含服务器横幅数据的 BLOB 数据块。值始终为 10。
长度 (Length)	uint32	BLOB 数据块中的字节总数（通常是 264 个字节）。
横幅 (Banner)	字节[*n*]	服务器事件中涉及的数据包的前 *n* 个字节，其中 *n* 小于或等于 256。

字符串信息数据块

字符串信息数据块包含字符串数据。例如，字符串信息数据块用于传输扫描漏洞数据块中的通用漏洞披露 (CVE) 标识字符串。字符串信息数据块的块类型为系列 1 数据块组中的 35。

下图显示字符串信息数据块的格式：



下表对字符串信息数据块的字段进行了说明。

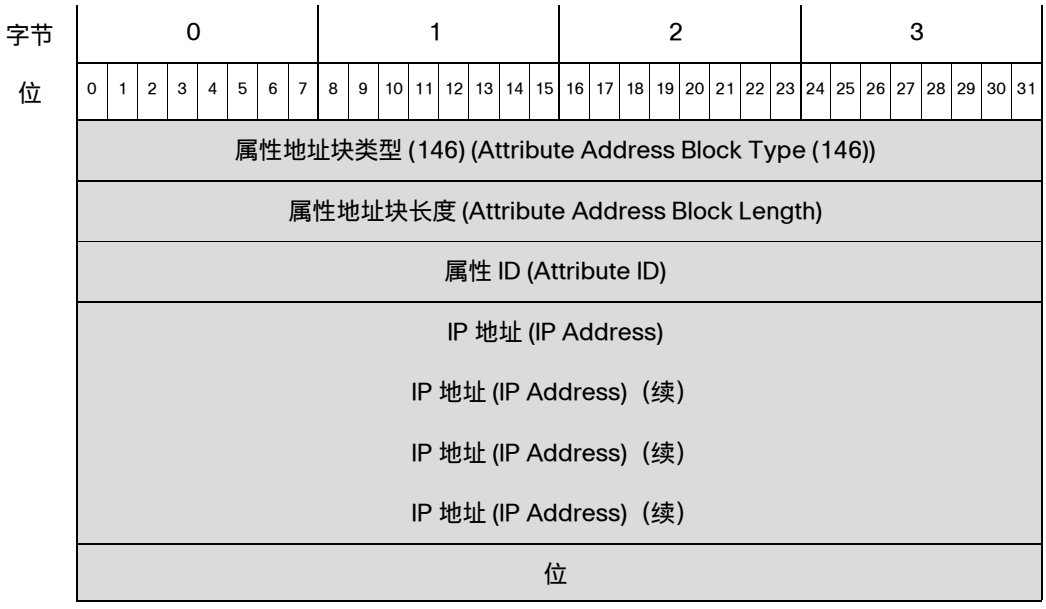
表 4-40 字符串信息数据块字段

字段	数据类型	说明 (Description)
字符串信息块类型 (String Information Block Type)	uint32	启动字符串信息数据块。值始终为 35。
字符串信息块长度 (String Information Block Length)	uint32	字符串信息数据块报头与字符串信息数据的总长度。
字符串块类型 (String Block Type)	uint32	启动该值的字符串数据块。
字符串块长度 (String Block Length)	uint32	用于该值的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上该值中的字节数。
值	字符串	在其中使用字符串信息数据块的漏洞数据块的通用漏洞披露 (CVE) 标识号的值。

属性地址数据块 5.2+

属性地址数据块包含一个属性列表项目，在属性定义数据块中使用。该数据块的块类型为系列 1 数据块组中的 146。

下图显示属性地址数据块的基本结构:



下表对属性地址数据块的字段进行了说明。

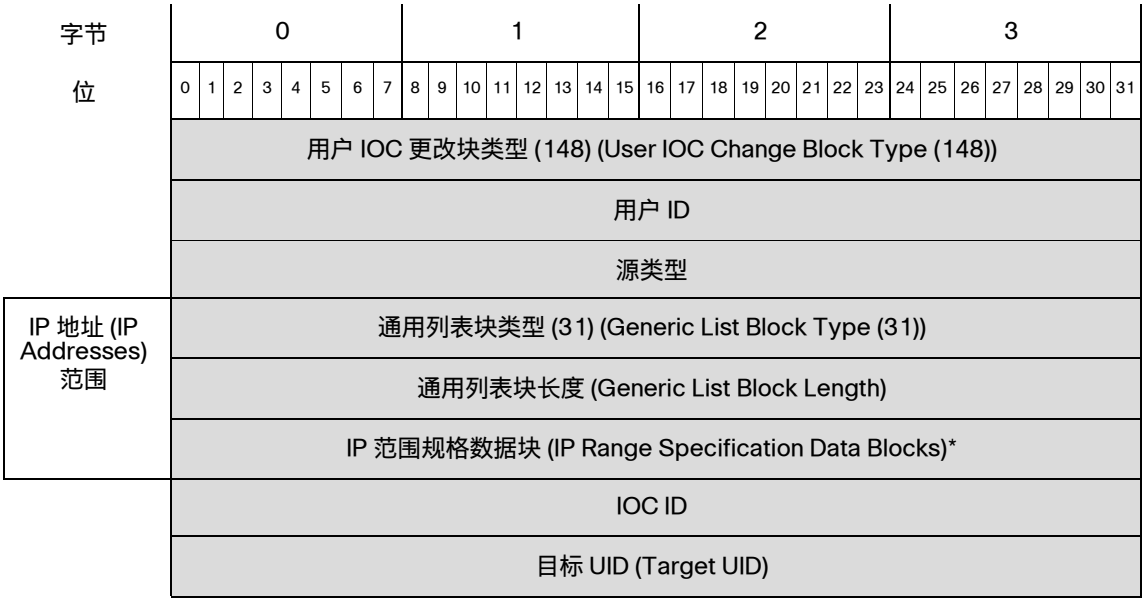
表 4-41　　属性地址数据块 5.2+ 字段

字段	数据类型	说明 (Description)
属性地址块类型 (Attribute Address Block Type)	uint32	启动属性地址数据块。值始终为 146。
属性地址块长度 (Attribute Address Block Length)	uint32	属性地址数据块中的字节数，包括属性地址块类型和长度字段的八个字节，加上随后的属性地址数据的字节数。
属性 ID (Attribute ID)	uint32	受影响属性的标识号（如适用）。
IP 地址 (IP Address)	uint8[16]	主机的 IP 地址（如果地址已自动分配）。此地址可以是 IPv4 或 IPv6。
位	uint32	如果已自动分配 IP 地址，则包含用于计算网络掩码的有效位。

用户 IOC 更改数据块 5.3+

用户 IOC 更改数据块包含有关用户进行的 IOC 更改的信息。它用于用户主机 IOC 删除、用户主机 IOC 启用和用户主机 IOC 禁用记录。该数据块的块类型为系列 1 数据块组中的 148。

下图显示用户 IOC 更改数据块的基本结构：



下表对用户服务器数据块的字段进行了说明。

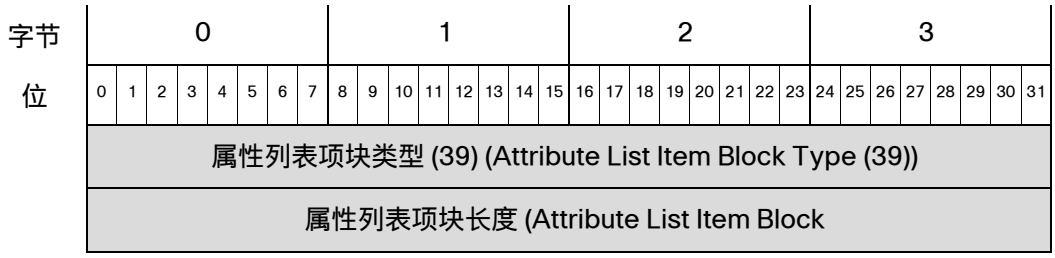
表 4-42 用户 IOC 更改数据块 5.3+ 字段

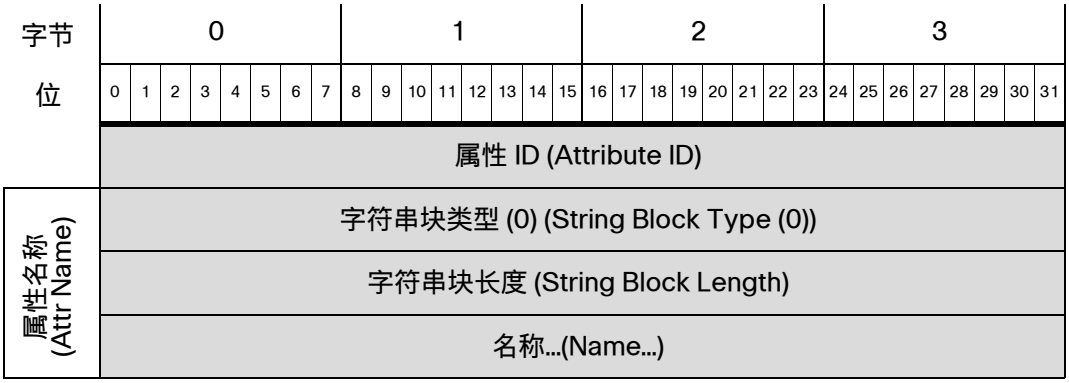
字段	数据类型	说明 (Description)
用户 IOC 更改块类型 (User IOC Change Block Type)	uint32	启动用户 IOC 更改数据块。此值始终为 148。
用户 ID	uint32	进行 IOC 更改的用户的 ID 号码。
源类型	uint32	映射到数据源类型的数字: ▪ 0 如果客户端数据由 RNA 检测到 ▪ 1 如果客户端数据由用户提供 ▪ 2 如果客户端数据由第三方扫描仪检测到 ▪ 3 如果客户端数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
通用列表块类型 (Generic List Block	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-93 页。
IOC ID	uint32	正在更改的 IOC 的 ID 号码。
目标 UID (Target UID)	unit32	未在 eStreamer 输出支持的事件中使用。

属性列表项数据块

属性列表项数据块包含一个属性列表项目，在属性定义数据块中使用。其块类型为系列 1 数据块组中的 39。

下图显示属性列表项数据块的基本结构:





下表对属性列表项数据块的字段进行了说明。

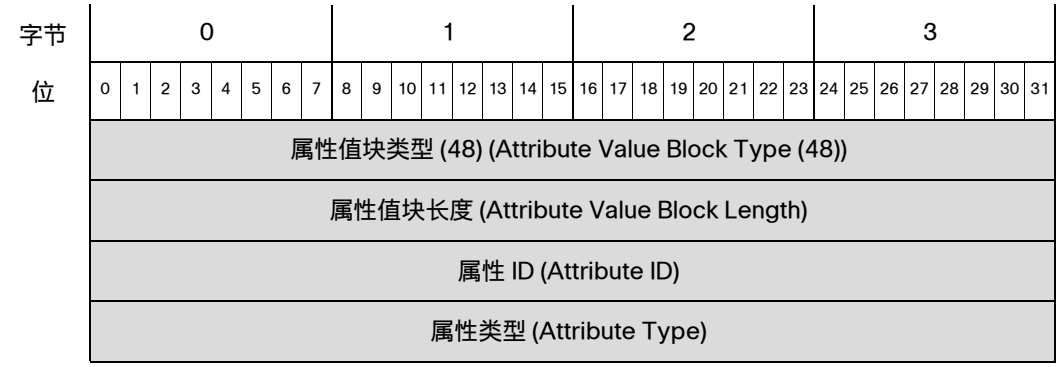
表 4-43　　属性列表项数据块字段

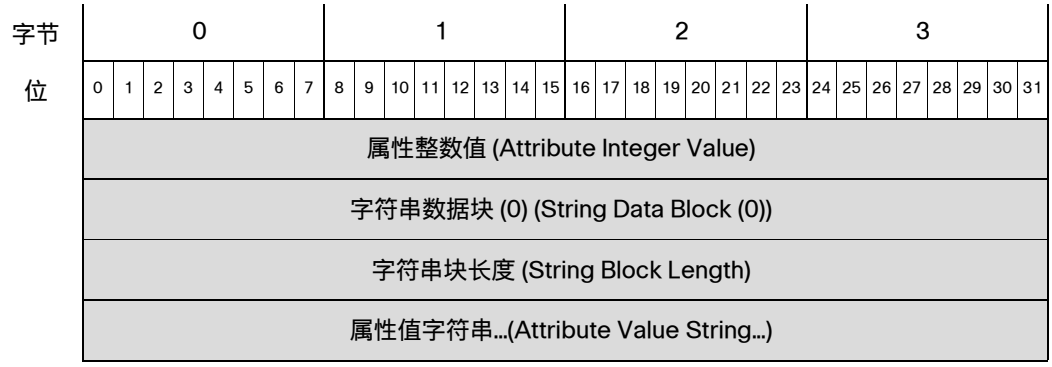
字段	数据类型	说明 (Description)
属性列表项块类型 (Attribute List Item Block	uint32	启动属性列表项数据块。值始终为 39。
属性列表项块长度 (Attribute List Item Block	uint32	属性列表项数据块中的字节数，包括属性列表项块类型和长度字段的八个字节，加上随后的属性列表项数据中的字节数。
属性 ID (Attribute ID)	uint32	受影响属性的标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动属性列表项名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	属性列表项名称字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上属性列表项名称中的字节数。
名称 (Name)	字符串	属性列表项名称。

属性值数据块

属性值数据块传输主机属性的属性标识号和值。完整主机配置文件数据块中的列表包含应用于事件中的主机的每个属性的属性值数据块。属性值数据块的块类型为系列 1 数据块组中的 48。

下图显示属性值数据块的格式:





下表对属性值数据块的组件进行了说明。

表 4-44 属性值数据块字段

字段	数据类型	说明 (Description)
属性值块类型 (Attribute Value Block Type)	uint32	启动属性值数据块。值始终为 48。
属性值块长度 (Attribute Value Block Length)	uint32	属性值数据块中的字节总数，包括属性值块类型和长度字段的八个字节，加上随后的属性块数据的字节数。
属性 ID (Attribute ID)	uint32	属性的标识号。
属性类型 (Attribute Type)	uint32	受影响属性的类型。可能的值包括： ▪ 0 - 值为文本的属性；这使用字符串数据 ▪ 1 - 具有范围值的属性；这使用整数数据 ▪ 2 - 具有可能值列表的属性；这使用整数数据 ▪ 3 - 值为 URL 的属性；这使用字符串数据 ▪ 4 - 值为二进制 BLOB 的属性；这使用字符串数据
属性整数值 (Attribute Integer Value)	uint32	属性的整数值（如适用）。
字符串块类型 (String Block Type)	uint32	启动包含属性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段，加上属性名称中的字节数。
属性值 (Attribute Value)	字符串	属性的值。

完整子服务器数据块

完整子服务器数据块传输与在主机上检测到的服务器关联的子服务器的相关信息，并且包含子服务器的相关信息，如子服务器的供应商和版本以及主上子服务器的任何相关 VDB 和第三方漏洞。子服务器是具有自己的关联漏洞的服务器可加载模块。完整主机服务器数据块包含用于在主机上检测到的每个子服务器的完整子服务器数据块。完整子服务器数据块的块类型为系列 1 数据块组中的 51。

注释　下图中系列 1 数据块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示完整子服务器数据块的格式:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
完整子服务器块类型 (51) (Full Sub-Server Block Type (51))																																
完整子服务器块长度 (Full Sub-Server Block Length)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
子服务器名称字符串...(Sub-Server Name String...)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
子服务器供应商名称字符串...(Sub-Server Vendor Name String...)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
子服务器版本字符串...(Sub-Server Version String...)																																
通用列表块类型 (31) (Generic List Block Type (31))																																
通用列表块长度 (Generic List Block Length)																																
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks)*																																
通用列表块类型 (31) (Generic List Block Type (31))																																
通用列表块长度 (Generic List Block Length)																																
（第三方扫描）主机漏洞数据块 ((Third Party Scan) Host Vulnerability Data Blocks)*																																

下表对完整子服务器数据块的组件进行了说明。

表 4-45　完整子服务器数据块字段

字段	数据类型	说明 (Description)
完整子服务器块类型 (Full Sub-Server Block Type)	uint32	启动完整子服务器数据块。值始终为 51。
完整子服务器块长度 (Full Sub-Server Block Length)	uint32	完整子服务器数据块中的字节总数，包括完整子服务器块类型和长度字段的八个字节，加上随后的完整子服务器数据中的字节数。
字符串块类型 (String Block Type)	uint32	启动包含子服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	子服务器名称字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上子服务器名称中的字节数。
子服务器名称 (Sub-Server Name)	字符串	子服务器名称。
字符串块类型 (String Block Type)	uint32	启动包含子服务器供应商名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	供应商名称字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上子服务器供应商名称中的字节数。
子服务器供应商名称 (Sub-Server Vendor Name)	字符串	子服务器供应商的名称。
字符串块类型 (String Block Type)	uint32	启动包含子服务器版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	子服务器版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上子服务器版本中的字节数。
子服务器版本 (Sub-Server Version)	字符串	子服务器版本。
通用列表块类型 (Generic List Block	uint32	启动由传送 VDB 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装主机漏洞数据块。
VDB 主机漏洞数据块 (VDB Host Vulnerability Data Blocks) *	变量	包含思科识别的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+, 第 4-111 页。
通用列表块类型 (Generic List Block	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。

表 4-45　完整子服务器数据块字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装主机漏洞数据块。
第三方扫描主机漏洞数据块 (Third Party Scan Host Vulnerability Data Blocks) *	变量	包含第三方漏洞扫描仪识别的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。

操作系统数据块 3.5+

用于版本 3.5+ 的操作系统数据块的块类型为系列 1 数据块组中的 53。该块包含指纹通用唯一标识符 (UUID)。下图显示 3.5+ 中操作系统数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	操作系统块类型 (53) (Operating System Block Type (53))																															
	操作系统块长度 (Operating System Block Length)																															
	置信 (Confidence)																															
操作系统指纹 UUID	指纹 UUID (Fingerprint UUID)																															
	指纹 UUID (Fingerprint UUID)（续）																															
	指纹 UUID (Fingerprint UUID)（续）																															
	指纹 UUID (Fingerprint UUID)（续）																															

下表对 v3.5 操作系统数据块的字段进行了说明。

表 4-46　操作系统数据块 3.5+ 字段

字段	数据类型	说明 (Description)
操作系统数据块类型 (Operating System Data Block Type)	uint32	启动操作系统数据块。值始终为 53。
操作系统数据块长度 (Operating System Data Block Length)	uint32	操作系统数据块中的字节数。此值应始终为 28：块类型和长度字段的八个字节，加上置信度值的四个字节以及指纹 UUID 值的十六个字节。

表 4-46 操作系统数据块 3.5+ 字段 （续）

字段	数据类型	说明 (Description)
置信 (Confidence)	uint32	置信度百分比值。
指纹 UUID (Fingerprint UUID)	uint8[16]	采用八位组的指纹识别号，用作操作系统的唯一标识符。在思科数据库中，指纹 UUID 向操作系统映射名称、供应商和版本。

策略引擎控制消息数据块

策略引擎控制消息数据块传输策略类型的控制消息内容。策略引擎控制消息数据块的块类型为系列 1 数据块组中的 54。

下图显示策略引擎控制消息数据块的格式:

<table>
<tr><td>字节</td><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="8">3</td></tr>
<tr><td>位</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>10</td><td>11</td><td>12</td><td>13</td><td>14</td><td>15</td><td>16</td><td>17</td><td>18</td><td>19</td><td>20</td><td>21</td><td>22</td><td>23</td><td>24</td><td>25</td><td>26</td><td>27</td><td>28</td><td>29</td><td>30</td><td>31</td></tr>
<tr><td></td><td colspan="32">策略引擎控制消息块类型 (54) (Policy Engine Control Message Block Type (54))</td></tr>
<tr><td></td><td colspan="32">策略引擎控制消息块长度 (Policy Engine Control Message Block Length)</td></tr>
<tr><td></td><td colspan="32">类型 (Type)</td></tr>
<tr><td rowspan="3">可控性消息 (Message)</td><td colspan="32">字符串块类型 (0) (String Block Type (0))</td></tr>
<tr><td colspan="32">字符串块长度 (String Block Length)</td></tr>
<tr><td colspan="32">控制消息...(Control Message...)</td></tr>
</table>

下表对策略引擎控制消息数据块的组件进行了说明。

表 4-47 策略引擎控制消息数据块字段

字段	数据类型	说明 (Description)
策略引擎控制消息块类型 (Policy Engine Control Message Block Type)	uint32	启动策略引擎控制消息数据块。值始终为 54。
策略引擎控制消息长度 (Policy Engine Control Message Length)	uint32	策略引擎控制消息数据块中的字节总数，包括策略引擎控制块类型和长度字段的八个字节，加上随后的策略引擎控制数据的字节数。
类型 (Type)	uint32	指示事件策略的类型。
字符串块类型 (String Block Type)	uint32	启动包含控制消息的字符串数据块。值始终为 0。

表 4-47　策略引擎控制消息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	控制消息字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上控制消息中的字节数。
控制消息 (Control Message)	uint32	策略引擎发出的控制消息。

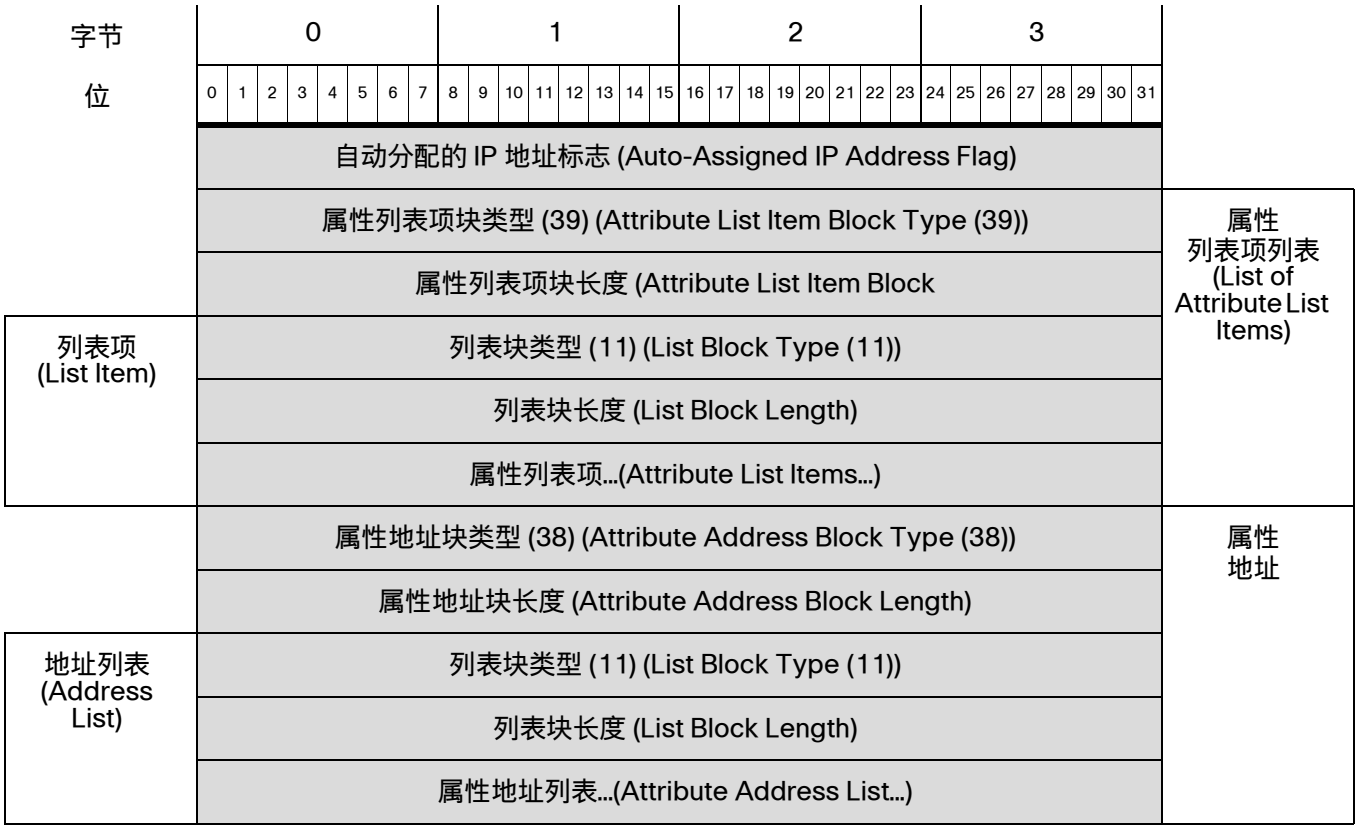
用于 4.7+ 的属性定义数据块

属性定义数据块包含属性创建、更改或删除事件中的属性定义，在主机属性添加事件（事件类型 1002，子类型 6）、主机属性更新事件（事件类型 1002子类型 7）以及主机属性删除事件（事件类型 1002，子类型 8）中使用。其块类型为系列 1 数据块组中的 55。

有关这些事件的详细信息，请参阅属性消息，第 4-54 页。

下图显示属性定义数据块的基本结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	属性定义块类型 (55) (Attribute Definition Block Type (55))																															
	属性定义块长度 (Attribute Definition Block Length)																															
	源 ID (Source ID)																															
	UUID UUID（续） UUID（续） UUID（续）																															
	ID																															
名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名称...(Name...)																															
	属性类型 (Attribute Type)																															
	属性类别 (Attribute Category)																															
	整数范围的起始值 (Starting Value for Integer Range)																															
	整数范围的结束值 (Ending Value for Integer Range)																															



下表对属性定义数据块的字段进行了说明。

表 4-48 属性定义数据块字段

字段	数据类型	说明 (Description)
属性定义块类型 (Attribute Definition Block Type)	uint32	启动属性定义数据块。值始终为 55。
属性定义块长度 (Attribute Definition Block Length)	uint32	属性定义数据块中的字节数，包括属性定义块类型和长度字段的八个字节，加上随后的属性定义数据的字节数。
源 ID (Source ID)	uint32	映射到属性数据源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
UUID	uint8[16]	充当受影响属性的唯一标识符的 ID 号码。
属性 ID (Attribute ID)	uint32	受影响属性的标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动属性定义名称的字符串数据块。值始终为 0。

表 4-48　　属性定义数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	属性定义名称字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上属性定义名称中的字节数。
名称 (Name)	字符串	属性定义名称。
属性类型 (Attribute Type)	uint32	属性的类型。可能的值包括： ▪ 0 - 值为文本的属性；这使用字符串数据 ▪ 1 - 具有范围值的属性；这使用整数数据 ▪ 2 - 具有可能值列表的属性；这使用整数数据 ▪ 3 - 值为 URL 的属性；这使用字符串数据 ▪ 4 - 值为二进制 BLOB 的属性；这使用字符串数据
属性类别 (Attribute Category)	uint32	属性类别。
范围的起始值 (Starting Value for Range)	uint32	定义属性的整数范围中的第一个整数。
范围的结束值 (Ending Value for Range)	uint32	定义属性的整数范围中的最后一个整数。
自动分配的 IP 地址标志 (Auto-Assigned IP Address Flag)	uint32	表示 IP 地址是否是根据属性自动分配的标志。
列表块类型 (List Block Type)	uint32	启动由传送属性列表项的属性列表项数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装属性列表项数据块。 此字段后面是零个或多个属性列表项数据块。
属性列表项块类型 (Attribute List Item Block	uint32	启动第一个属性列表项数据块。此数据块后面可以跟随最大长度为列表块长度字段中定义的限值的其他属性列表项数据块。
属性列表项块长度 (Attribute List Item Block	uint32	属性列表项字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上属性列表项中的字节数。
属性列表项 (Attribute List Item)	变量	属性列表项数据，如属性列表项数据块，第 4-78 页中所记录。
列表块类型 (List Block Type)	uint32	启动由传输带该属性的主机的 IP 地址的属性地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装属性地址数据块。 此字段后面是零个或多个属性地址数据块。

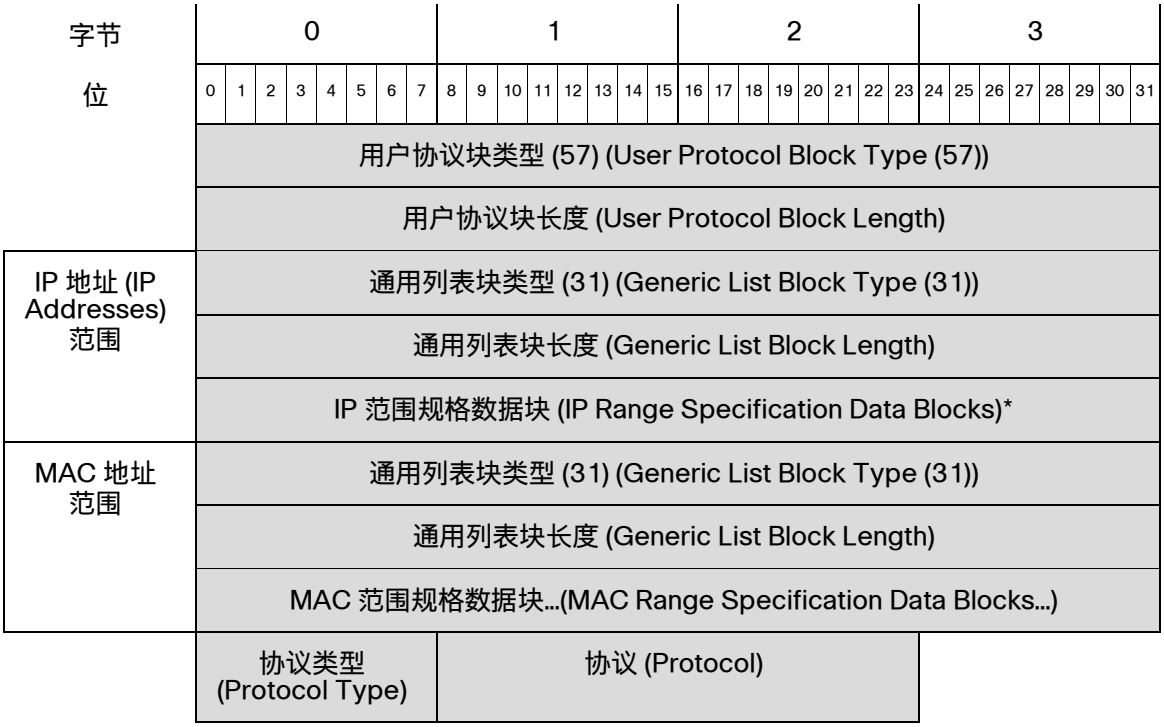
表 4-48 属性定义数据块字段 （续）

字段	数据类型	说明 (Description)
属性地址块类型 (Attribute Address Block Type)	uint32	启动第一个属性地址数据块。此数据块后面可以跟随最大长度为列表块长度字段中定义的限值的其他属性地址数据块。
属性地址块长度 (Attribute Address Block Length)	uint32	属性地址数据块中的字节数，包括块类型和报头字段的八个字节，加上属性地址中的字节数。
属性地址 (Attribute Address)	变量	属性地址数据，如属性地址数据块 5.2+，第 4-76 页中所记录。

用户协议数据块

用户协议数据块用于包含已添加协议、协议类型以及具有该协议的主机的 IP 地址和 MAC 地址范围列表的相关信息。用户协议数据块的块类型为系列 1 数据块组中的 57。

下图显示用户协议数据块的基本结构:



下表对用户协议数据块的字段进行了说明。

表 4-49　用户协议数据块字段

字段	字节数	说明 (Description)
用户协议块类型 (User Protocol Block Type)	uint32	启动用户协议数据块。值始终为 57。
用户协议块长度 (User Protocol Block Length)	uint32	用户协议数据块中的字节总数，包括用户协议块类型和长度字段的八个字节，加上随后的用户协议数据的字节数。
通用列表块类型 (Generic List Block	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-93 页。
通用列表块类型 (Generic List Block	uint32	启动由传送 MAC 地址范围数据的 MAC 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装 MAC 范围规格数据块。
MAC 范围规格数据块 (MAC Range Specification Data Blocks) *	变量	包含用于用户输入的 MAC 地址范围相关信息的 MAC 范围规格数据块。有关此数据块的说明，请参阅MAC 地址规格数据块，第 4-96 页。
协议类型 (Protocol Type)	uint8	指示协议的类型。对于 IP 等网络层协议，协议为 0，对于 TCP 或 UDP 等传输层协议，协议为 1。
协议 (Protocol)	uint16	启动用于数据块中包含的数据的协议。

用于 5.1.1+ 的用户客户端应用数据块

用户客户端应用数据块包含客户端应用数据来源、添加数据的用户的标识号以及 IP 地址范围数据块列表的相关信息。版本 7.2 中添加的负载 ID 指定与记录相关的应用实例。用户客户端应用数据块的块类型为系列 1 数据块组中的 138。它取代块类型 59。

下图显示用户客户端应用数据块的基本结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户客户端应用块类型 (138) (User Client Application Block Type (138))																															
	用户客户端应用块长度 (User Client Application Block Length)																															
IP 范围规范	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IP 范围规格数据块 (IP Range Specification Data Blocks)*																															
	应用协议 ID (Application Protocol ID)																															
	客户端应用 ID (Client Application ID)																															
版本	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	版本...(Version...)																															
	负载类型 (Payload Type)																															
	Web 应用 ID (Web Application ID)																															

下表对用户客户端应用数据块的字段进行了说明。

表 4-50 用户客户端应用数据块字段

字段	字节数	说明 (Description)
用户客户端应用块类型 (User Client Application Block Type)	uint32	启动用户客户端应用数据块。值始终为 138。
用户客户端应用块长度 (User Client Application Block Length)	uint32	用户客户端应用数据块中的字节总数，包括用户客户端应用块类型和长度字段的八个字节，加上随后的用户客户端应用数据的字节数。
通用列表块类型 (Generic List Block	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。

表 4-50　用户客户端应用数据块字段 （续）

字段	字节数	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装
IP 范围规格数据块 (IP Range Specification Datalocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-93 页。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动包含客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用版本字符串数据块中的字节数，包括字符串块类型和长度字段，加上版本中的字节数。
版本	字符串	客户端应用版本。
负载类型 (Payload Type)	uint32	包括此字段以向后兼容。值始终为 0。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。

用户客户端应用列表数据块

用户客户端应用列表数据块包含客户端应用数据来源、添加数据的用户的标识号以及客户端应用块列表的相关信息。用户客户端列表应用数据块的块类型为系列 1 数据块组中的 60。

下图显示用户客户端应用列表数据块的基本结构:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户客户端应用块类型 (60) (User Client Application Block Type (60))																															
	用户客户端应用块长度 (User Client Application Block Length)																															
	源类型 (Source Type)																															
	源 ID (Source ID)																															
用户客户端应用列表代码块	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	用户客户端应用列表数据块...(User Client Application List Data Blocks...)																															

下表对用户客户端应用列表数据块的字段进行了说明。

表 4-51 用户客户端应用列表数据块字段

字段	字节数	说明 (Description)
用户客户端应用列表块类型 (User Client Application List Block Type)	uint32	启动用户客户端应用列表数据块。值始终为60。
用户客户端应用列表块长度 (User Client Application List Block Length)	uint32	用户客户端应用列表数据块中的字节总数，包括用户客户端应用列表块类型和长度字段的八个字节，加上随后的用户客户端应用列表数据的字节数。
源类型 (Source Type)	uint32	映射到数据源类型的数字: ▪ 0 如果客户端数据由 RNA 检测到 ▪ 1 如果客户端数据由用户提供 ▪ 2 如果客户端数据由第三方扫描仪检测到 ▪ 3 如果客户端数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
源 ID (Source ID)	uint32	映射到添加受影响客户端应用的源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
用户客户端应用块 (User Client Application Blocks)	变量	封装用户客户端应用数据块数最多可以是列表块长度中的最大字节数。有关用户客户端应用数据块的详细信息，请参阅用于 5.1.1+ 的用户客户端应用数据块，第 4-90 页。

用于 5.2+ 的 IP 地址范围数据块

用于 5.2+ 的 IP 地址范围数据块传输一系列 IP 地址。IP 地址范围数据块在用户协议、用户客户端应用、地址规格、用户产品、用户服务器、用户主机、用户漏洞、用户临界点以及用户属性值数据块中使。IP 地址范围数据块的块类型为系列 1 数据块组中的 141。

下图显示 IP 地址范围数据块的格式:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IP 地址范围块类型 (141) (IP Address Range Block Type (141))																																
IP 地址范围块长度 (IP Address Range Block Length)																																
IP 地址范围开始 (IP Address Range Start)																																
IP 地址范围开始 (IP Address Range Start)（续）																																
IP 地址范围开始 (IP Address Range Start)（续）																																
IP 地址范围开始 (IP Address Range Start)（续）																																
IP 地址范围结束 (IP Address Range End)																																
IP 地址范围结束 (IP Address Range End)（续）																																
IP 地址范围结束 (IP Address Range End)（续）																																
IP 地址范围结束 (IP Address Range End)（续）																																

下表对 IP 地址范围规格数据块的组件进行了说明。

表 4-52　　IP 地址范围数据块字段

字段	数据类型	说明 (Description)
IP 地址范围块类型 (IP Address Range Block Type)	uint32	启动 IP 地址范围数据块。值始终为 61。
IP 地址范围块长度 (IP Address Range Block Length)	uint32	IP 地址范围数据块中的字节总数，包括 IP 地址范围块类型和长度字段的八个字节，加上随后的 IP 地址范围数据的字节数。
IP 地址范围开始 (IP Address Range Start)	uint8[16]	IP 地址范围的开始 IP 地址。
IP 地址范围结束 (IP Address Range End)	uint8[16]	IP 地址范围的结束 IP 地址。

属性规格数据块

属性规格数据块传输属性名称和值。属性规格数据块的块类型为系列 1 数据块组中的 62。

下图显示属性规格数据块的格式:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	属性规格块类型 (62) (Attribute Specification Block Type (62))																															
属性名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	属性名称...(Attribute Name...)																															
属性值 (Attribute Value)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	属性值...(Attribute Value...)																															

下表对属性规格数据块的组件进行了说明。

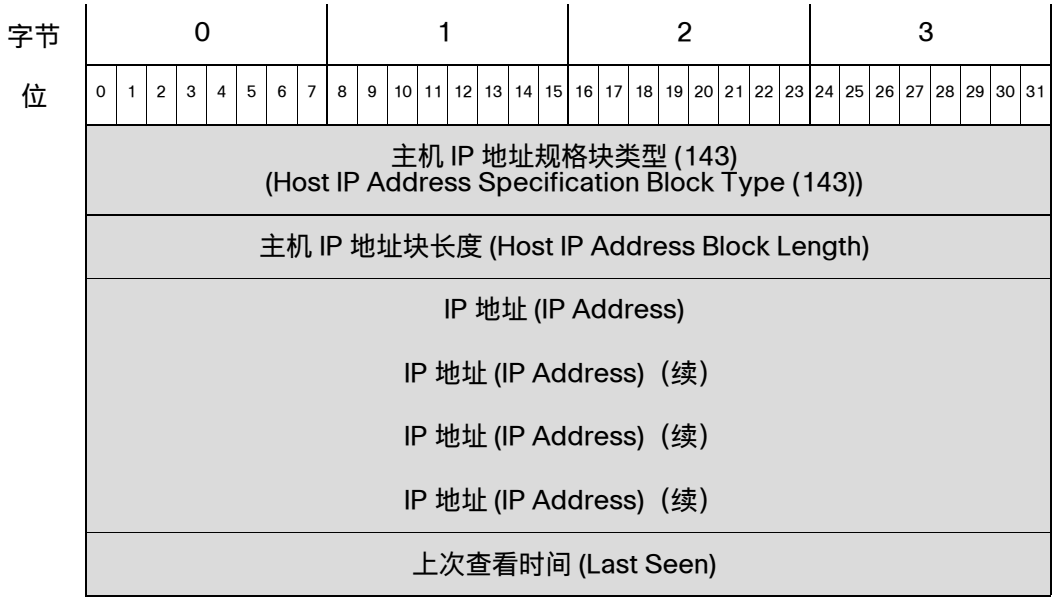
表 4-53 属性规格数据块字段

字段	数据类型	说明 (Description)
属性规格块类型 (Attribute Specification Blockype)	uint32	启动属性规格数据块。值始终为 62。
字符串块类型 (String Block Type)	uint32	启动包含属性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	属性名称字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上属性名称中的字节数。
属性值 (Attribute Value)	uint32	属性的值。
字符串块类型 (String Block Type)	uint32	启动包含属性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	属性名称字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上属性名称中的字节数。
属性名称 (Attribute Name)	uint32	属性的名称。

主机 IP 地址数据块

主机 IP 地址数据块传输单个 IP 地址。该 IP 地址可能是 IPv4 或 IPv6 地址。主机 IP 地址数据块在用户协议、地址规格以及用户主机数据块中使用。主机 IP 数据块的块类型为系列 1 数据块组中的 143。

下图显示主机 IP 地址数据块的格式:



下表对主机 IP 地址数据块的组件进行了说明。

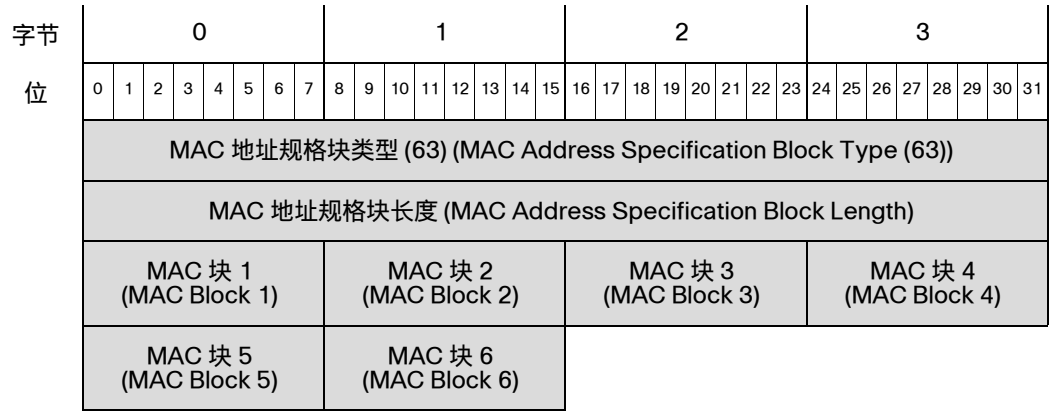
表 4-54　　主机 IP 地址数据块字段

字段	数据类型	说明 (Description)
主机 IP 地址块类型 (Host IP Address Block Type)	uint32	启动主机 IP 地址数据块。值始终为 143。
主机 IP 块长度 (Host IP Block Length)	uint32	主机 IP 地址数据块中的字节总数，包括主机 IP 块类型和长度字段的八个字节，加上随后的主机 IP 地址数据的字节数。
IP 地址 (IP Address)	uint8[16]	IP 地址。可能是 IPv4 或 IPv6。
上次查看时间 (Last Seen)	uint32	表示系统上次检测到 IP 地址的 UNIX 时间戳。

MAC 地址规格数据块

MAC 地址规格数据块传输单个 MAC 地址。MAC 地址规格数据块在用户协议、地址规格以及用户主机数据块中使用。MAC 地址规格数据块的块类型为系列 1 数据块组中的 63。

下图显示 MAC 地址规格数据块的格式:



下表对 MAC 地址规格数据块的组件进行了说明。

表 4-55 MAC 地址规格数据块字段

字段	数据类型	说明 (Description)
MAC 地址规格块类型 (MAC Address Specification Block Type)	uint32	启动 MAC 地址规格数据块。值始终为 63。
MAC 地址规格块长度 (MAC Address Specification Block Length)	uint32	MAC 地址规格数据块中的字节总数，包括 MAC 地址规格块类型和长度字段的八个字节，加上随后的 MAC 地址规格数据的字节数。
MAC 地址块 1 - 6 (MAC Address Blocks 1 - 6)	uint8	按顺序排列的 MAC 地址块。

地址规格数据块

地址规格数据块用于包含 IP 地址范围规格和 MAC 地址规格列表。地址规格数据块的块类型为系列 1 数据块组中的 64。

下图显示地址规格数据块的基本结构:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	地址规格数据块类型 (64) (Address Specification Data Block Type (64))																															
	地址规格块长度 (Address Specification Block Length)																															
IP 地址 (IP Addresses) 范围 代码块	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IP 地址范围规格数据块...(IP Address Range Specification Data Blocks...)																															
MAC Address 代码块	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	MAC 地址规格数据块...(MAC Address Specification Data Blocks...)																															

下表对地址规格数据块的字段进行了说明。

表 4-56　　地址规格数据块字段

字段	字节数	说明 (Description)
地址规格数据块类型 (Address Specification Data Block Type)	uint32	启动地址规格数据块。值始终为 64。
地址规格块长度 (Address Specification Block Length)	uint32	地址规格数据块中的字节总数，包括地址规格块类型和长度字段的八个字节，加上随后的地址规格数据的字节数。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。

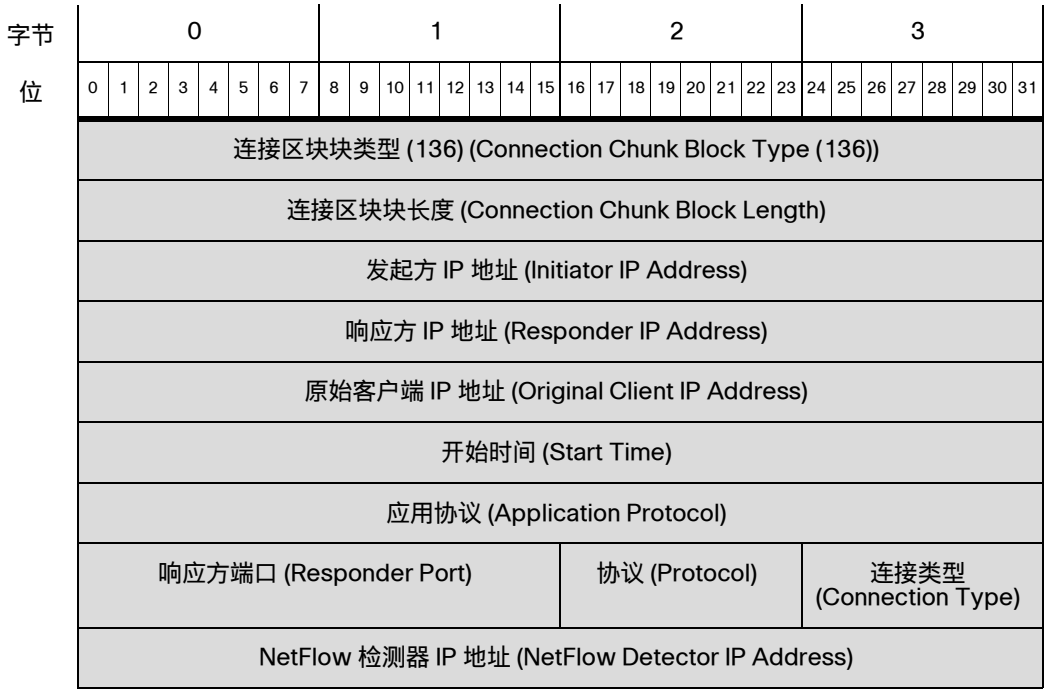
表 4-56 地址规格数据块字段 （续）

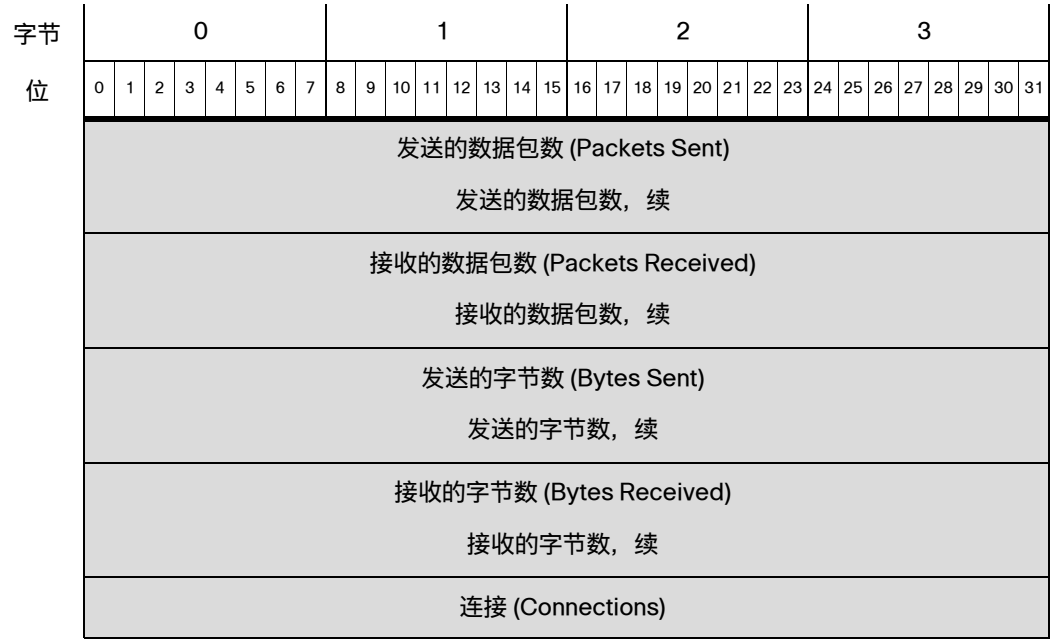
字段	字节数	说明 (Description)
IP 地址范围规格数据块 (IP Address Range Specification Data	变量	封装 IP 地址范围规格数据块数最多可以是列表块长度中的最大字节数。有关详细信息，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-93 页。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
MAC 地址规格数据块 (MAC Address Specification Data Blocks)	变量	封装 MAC 地址规格数据块数最多可以是列表块长度中的最大字节数。有关详细信息，请参阅MAC 地址规格数据块，第 4-96 页。

用于 6.1+ 的连接区块数据块

连接区块数据块传送连接数据。它存储五分钟内汇聚的连接日志数据。6.1+ 版本引入了新字段“原始客户端 IP 地址”。连接区块数据块的块类型为系列 1 数据块组中的 164。它替代块类型 136。

下图显示连接区块数据块的格式:





下表对连接区块数据块的组件进行了说明。

表 4-57　　连接区块数据块字段

字段	数据类型	说明 (Description)
连接区块块类型 (Connection Chunk Block Type)	uint32	启动连接区块数据块。值始终为 164。
连接区块块长度 (Connection Chunk Block Length)	uint32	连接区块数据块中的字节总数，包括连接区块块类型和长度字段的八个字节，加上随后的连接区块数据中的字节数。
发起方 IP 地址 (Initiator IP Address)	uint8(4)	此类型连接的发起方的 IP 地址。与原始客户端 IP 地址和响应方 IP 地址一起使用，以识别相同连接。
响应方 IP 地址 (Responder IP Address)	uint8(4)	此类型连接的响应方的 IP 地址。与发起方 IP 地址和原始客户端 IP 地址一起使用，以识别相同连接。
原始客户端 IP 地址 (Original Client IP Address)	uint8(4)	位于发起请求的代理后面的主机的 IP 地址。与发起方 IP 地址和响应方 IP 地址一起使用，以识别相同连接。
开始时间 (Start Time)	uint32	连接区块的开始时间。
应用协议 (Application Protocol)	uint32	连接中使用的协议的标识号。

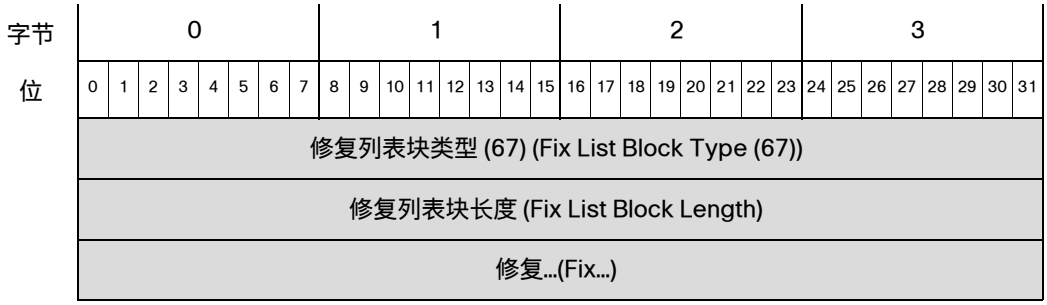
表 4-57 连接区块数据块字段 （续）

字段	数据类型	说明 (Description)
响应方端口 (Responder Port)	uint16	响应者在连接区块中使用的端口。
协议 (Protocol)	uint8	用于包含用户信息的数据包的协议。
连接类型 (Connection Type)	uint8	连接的类型。
NetFlow 检测器 IP 地址 (NetFlow Detector IP Address)	uint8[4]	检测到连接的 NetFlow 设备的 IP 地址，采用 IP 地址八位组。
发送的数据包数 (Packets Sent)	uint64	在连接区块中发送的数据包数。
接收的数据包数 (Packets Received)	uint64	在连接区块中接收的数据包数。
发送的字节数 (Bytes Sent)	uint64	在连接区块中发送的字节数。
接收的字节数 (Bytes Received)	uint64	在连接区块中接收的字节数。
连接	uint32	五分钟内的连接数。

修复列表数据块

修复列表数据块传输应用于主机的修复。用户产品数据块中包含应用于受影响主机的每个修复的修复列表数据块。修复列表数据块的块类型为系列 1 数据块组中的 67。

下图显示修复列表数据块的格式:



下表对修复列表数据块的组件进行了说明。

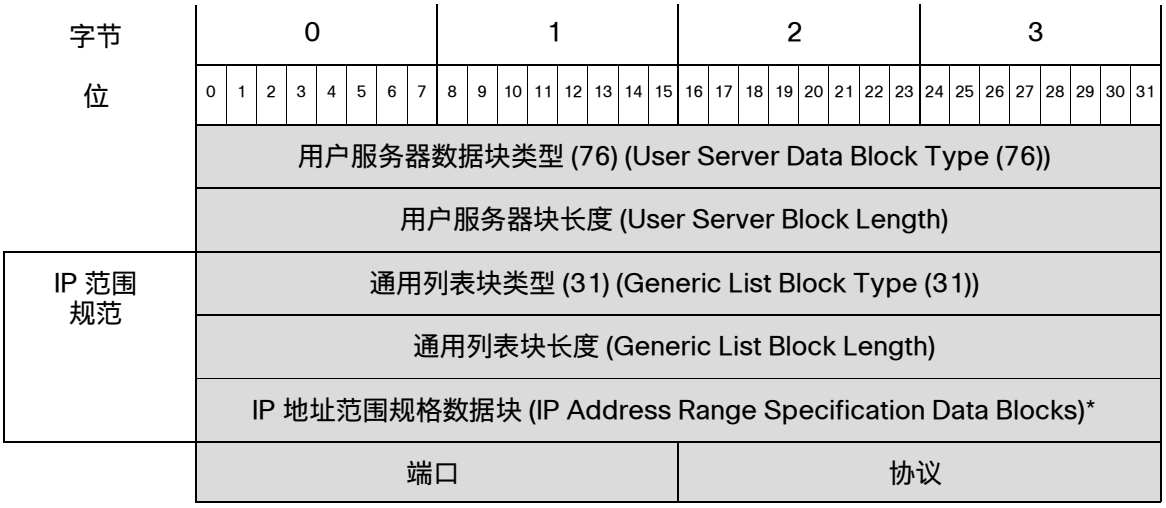
表 4-58　　修复列表数据块字段

字段	数据类型	说明 (Description)
修复列表块类型 (Fix List Block Type)	uint32	启动修复列表数据块。值始终为 67。
修复列表块长度 (Fix List Block Length)	uint32	修复列表数据块中的字节总数，包括修复列表块类型和长度字段的八个字节，加上随后的修复标识数据的字节数。
修复 ID (Fix ID)	uint32	修复的标识号。

用户服务器数据块

用户服务器数据块包含用户输入事件的服务器详细信息。用户服务器数据块的块类型为系列 1 数据块组中的 76。

下图显示用户服务器数据块的基本结构：



下表对用户服务器数据块的字段进行了说明。

表 4-59　　用户服务器数据块字段

字段	字节数	说明 (Description)
用户服务器数据块类型 (User Server Data Block Type)	uint32	启动用户服务器数据块。值始终为 76。
用户服务器块长度 (User Server Block Length)	uint32	用户服务器数据块中的字节总数，包括用户服务器块类型和长度字段的八个字节，加上随后的用户服务器数据的字节数。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。

表 4-59 用户服务器数据块字段 （续）

字段	字节数	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
IP 地址范围规格数据块 (IP Address Range Specification Data	变量	封装 IP 地址范围规格数据块数最多可以是列表块长度中的最大字节数。
端口 (Port)	uint16	服务器使用的端口。
协议 (Protocol)	uint16	IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如: ▪ 6 - TCP ▪ 17 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如: ▪ 2048 - IP

用户服务器列表数据块

用户服务器列表数据块包含用户输入事件的服务器数据块列表。用户服务器列表数据块的块类型为系列 1 数据块组中的 77。下图显示用户服务器列表数据块的基本结构:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户服务器列表数据块类型 (77) (User Server List Data Block Type (77))																															
	用户服务器列表块长度 (User Server List Block Length)																															
	源类型 (Source Type)																															
	源 ID (Source ID)																															
用户 Server 代码块	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	用户服务器数据块 (User Server Data Block)*																															

下表对用户服务器列表数据块的字段进行了说明。

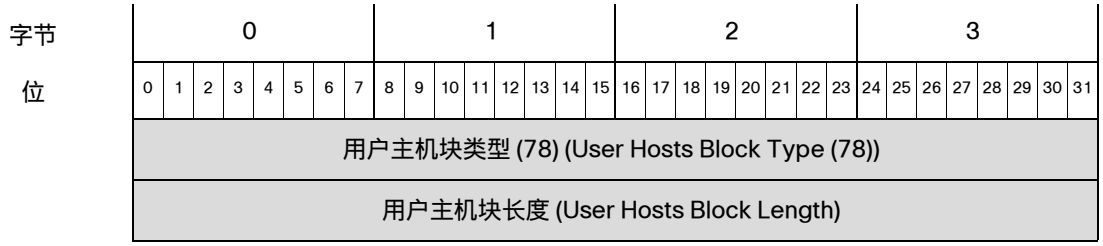
表 4-60　　用户服务器列表数据块字段

字段	字节数	说明 (Description)
用户服务器列表数据块类型 (User Server List Data Block Type)	uint32	启动用户服务器列表数据块。值始终为 77。
用户服务器列表块长度 (User Server List Block Length)	uint32	用户服务器列表数据块中的字节总数，包括用户服务器列表块类型和长度字段的八个字节，加上随后的用户服务器列表数据的字节数。
源类型 (Source Type)	uint32	映射到数据源类型的数字： ▪ 0 如果服务器数据由 RNA 检测到 ▪ 1 如果服务器数据由用户提供 ▪ 2 如果服务器数据由第三方扫描仪检测到 ▪ 3 如果服务器数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
源 ID (Source ID)	uint32	映射到服务器数据源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
用户服务器数据块 (User Server Data Blocks)	变量	封装用户服务器数据块数最多可以是列表块长度中的最大字节数。

用户主机数据块 4.7+

用户主机数据块在用户添加和删除主机消息，第 4-53 页中使用，用于包含用户主机输入事件的主机范围以及用户和源身份的相关信息。用户主机数据块的块类型为系列 1 数据块组中的 78。

下图显示用户主机数据块的基本结构：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IP 范围	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IP 范围规格数据块 (IP Range Specification Data Blocks)*																															
MAC 范围	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	MAC 范围规格数据块...(MAC Range Specification Data Blocks...)																															
	源 ID (Source ID)																															
	源类型 (Source Type)																															

下表对用户主机数据块的字段进行了说明:

表 4-61 用户主机数据块字段

字段	字节数	说明 (Description)
用户主机块类型 (User Hosts Block Type)	uint32	启动用户主机数据块。值始终为 78。
用户主机块长度 (User Hosts Block Length)	uint32	用户主机数据块中的字节总数，包括用户主机块类型和长度字段的八个字节，加上随后的用户主机数据的字节数。
通用列表块类型 (Generic List Block	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-93 页。
通用列表块类型 (Generic List Block	uint32	启动由传送 MAC 地址范围数据的 MAC 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装 MAC 范围规格数据块。

表 4-61　用户主机数据块字段 （续）

字段	字节数	说明 (Description)
MAC 范围规格数据块 (MAC Range Specification Data Blocks) *	变量	包含用于用户输入的 MAC 地址范围相关信息的 MAC 范围规格数据块。有关此数据块的说明，请参阅MAC 地址规格数据块，第 4-96 页。
源 ID (Source ID)	uint32	映射到添加或更新主机数据的源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
源类型 (Source Type)	uint32	映射到数据源类型的数字： ▪ 0 如果主机数据由 RNA 检测到 ▪ 1 如果主机数据由用户提供 ▪ 2 如果主机数据由第三方扫描仪检测到 ▪ 3 如果主机数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供

用户漏洞更改数据块 4.7+

用户漏洞更改数据块包含主机的停用漏洞列表、停用漏洞的用户的标识号、提供漏洞更改的源的相关信息以及临界点值。用户漏洞更改数据块的块类型为系列 1 数据块组中的 80。对之前用户漏洞更改数据块的更改包括新源类型字段以及用通用列表数据块代替列表数据块来存储漏洞停用。此数据块在用户漏洞更改消息中使用，如用于版本 4.6.1+ 的用户设置漏洞消息，第 4-52 页中所记录。

下图显示用户漏洞更改数据块的基本结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户漏洞更改数据块类型 (80) (User Vulnerability Change Data Block Type (80))																															
	用户漏洞更改块长度 (User Vulnerability Change Block Length)																															
	源 ID (Source ID)																															
	源类型 (Source Type)																															
漏洞攻击代码块	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	用户漏洞数据块...(User Vulnerability Data Blocks...)*																															

下表对通用列表数据块的字段进行了说明。

表 4-62　用户漏洞更改数据块字段

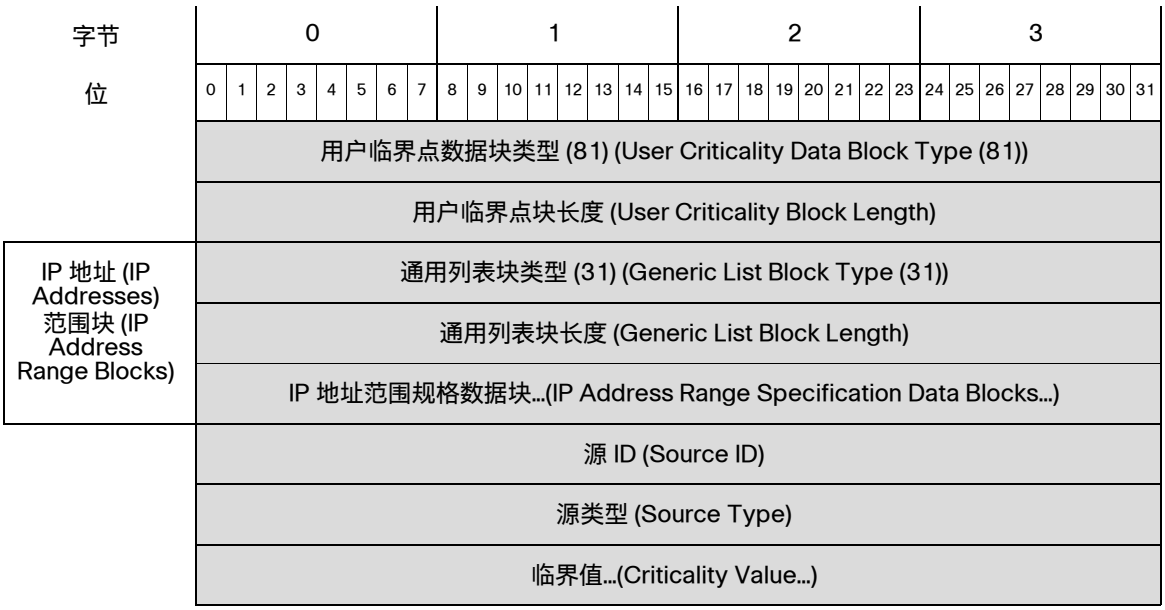
字段	字节数	说明 (Description)
用户漏洞更改数据块类型 (User Vulnerability Change Data Block Type)	uint32	启动用户漏洞更改数据块。值始终为 80。
用户漏洞更改块长度 (User Vulnerability Change Block Length)	uint32	用户漏洞更改数据块中的字节总数，包括主机漏洞块类型和长度字段的八个字节，加上随后的主机漏洞数据的字节数。
源 ID (Source ID)	uint32	映射到更新或添加主机漏洞更改值的源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
源类型 (Source Type)	uint32	映射到数据源类型的数字： ▪ 0 如果主机漏洞数据由 RNA 检测到 ▪ 1 如果主机漏洞数据由用户提供 ▪ 2 如果主机漏洞数据由第三方扫描仪检测到 ▪ 3 如果主机漏洞数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
类型 (Type)	uint32	漏洞的类型。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
用户漏洞数据块 (User Vulnerability Data Blocks)	变量	封装用户漏洞数据块数最多可以是列表块长度中的最大字节数。有关详细信息，请参阅用户漏洞数据块 5.0+，第 4-159 页。

用户临界点更改数据块 4.7+

用户临界点数据块用于包含主机临界点已更改的主机的 IP 地址范围规格列表、更新临界值的用户的标识号、提供临界值的源的相关信息以及临界值。用户临界点数据块的块类型为系列 1 数据块组中的 81。对之前用户临界点数据块的更改包括新源类型字段以及用通用列表数据块代替列表数据块来存储 IP 地址。

用户临界点数据块在用户设置主机临界点消息中使用，如用户设置主机临界点消息，第 4-53 页中所记录。

下图显示用户临界点数据块的基本结构：



下表对用户临界点数据块的字段进行了说明。

表 4-63　　用户临界点数据块字段

字段	字节数	说明 (Description)
用户临界点数据块类型 (User Criticality Data Block Type)	uint32	启动用户临界点数据块。值始终为 81。
用户临界点块长度 (User Criticality Block Length)	uint32	用户临界点数据块中的字节总数，包括用户临界点块类型和长度字段的八个字节，加上随后的用户临界点数据的字节数。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
IP 地址范围规格数据块 (IP Address Range Specification Data	变量	封装 IP 地址范围规格数据块数最多可以是列表块长度中的最大字节数。
源 ID (Source ID)	uint32	映射到更新或添加用户临界值的源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。

表 4-63 用户临界点数据块字段 （续）

字段	字节数	说明 (Description)
源类型 (Source Type)	uint32	映射到数据源类型的数字: ▪ 0 如果用户临界值由 RNA 提供 ▪ 1 如果用户临界值由用户提供 ▪ 2 如果用户临界值由第三方扫描仪提供 ▪ 3 如果用户临界值由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
临界值 (Criticality Value)	uint32	用户临界值。

用户属性值数据块 4.7+

用户属性值数据块包含指示属性值更改的主机的 IP 地址范围列表，连同添加属性值的用户的标识号，提供属性值的源的相关信息，以及包含属性值的 BLOB 数据块。用户属性值数据块的块类型为系列 1 数据块组中的 82。对之前用户属性值数据块的更改包括新源类型字段以及用通用列表数据块代替列表数据块来存储 IP 地址。

下图显示用户属性值数据块的结构:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户属性值数据块类型 (82) (User Attribute Value Data Block Type (82))																															
	用户属性值块长度 (User Attribute Value Block Length)																															
IP 地址 (IP Addresses) 范围块 (IP Address Range Blocks)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IP 地址范围规格数据块...(IP Address Range Specification Data Blocks...)																															
	源 ID (Source ID)																															
	源类型 (Source Type)																															
	属性 ID (Attribute ID)																															
值	BLOB 块类型 (10) (BLOB Block Type (10))																															
	BLOB 块长度 (BLOB Block Length)																															
	值...(Value...)																															

下表对用户属性值数据块的字段进行了说明。

表 4-64　　用户属性值数据块字段

字段	字节数	说明 (Description)
用户属性值数据块类型 (User Attribute Value Data Block Type)	uint32	启动用户属性值数据块。值始终为 82。
用户属性值块长度 (User Attribute Value Block Length)	uint32	属性值数据块中的字节总数，包括用户属性值块类型和长度字段的八个字节，加上随后的用户属性值数据的字节数。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
IP 地址范围规格数据块 (IP Address Range Specification Data	变量	IP 地址范围规格数据块数（每个数据块都有一个开始 IP 地址和结束 IP 地址）最多可以是列表块长度中的最大字节数。
源 ID (Source ID)	uint32	映射到添加或更新属性数据的源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
源类型 (Source Type)	uint32	映射到数据源类型的数字： ▪ 0 如果用户属性值由 RNA 提供 ▪ 1 如果用户属性值由用户提供 ▪ 2 如果用户属性值由第三方扫描仪提供 ▪ 3 如果用户属性值由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
属性 ID (Attribute ID)	uint32	更新的属性的标识号。
BLOB 块类型 (BLOB Block Type)	uint32	启动 BLOB 数据块。值始终为 10。
BLOB 块长度 (BLOB Block Length)	uint32	BLOB 数据块中的字节数，包括 BLOB 块类型和长度字段的八个字节，加上随后的二进制数据的长度。
值	变量	包含用户属性值（二进制格式）。

用户协议列表数据块 4.7+

用户协议列表数据块用于包含协议数据源、添加数据的用户的标识号以及用户协议数据块列表的相关信息。用户协议列表数据块的块类型为系列 1 数据块组中的 83。有关用户协议数据块的详细信息，请参阅用户协议数据块，第 4-88 页。

用户协议列表数据块在用户协议消息中使用，如用户协议消息，第 4-55 页中所记录。

下图显示用户协议列表数据块的基本结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户协议列表块类型 (83) (User Protocol List Block Type (83))																															
	用户协议列表块长度 (User Protocol List Block Length)																															
	源类型 (Source Type)																															
	源 ID (Source ID)																															
用户协议代码块	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	用户协议数据块...(User Protocol Data Blocks...)																															

下表对通用列表数据块的字段进行了说明。

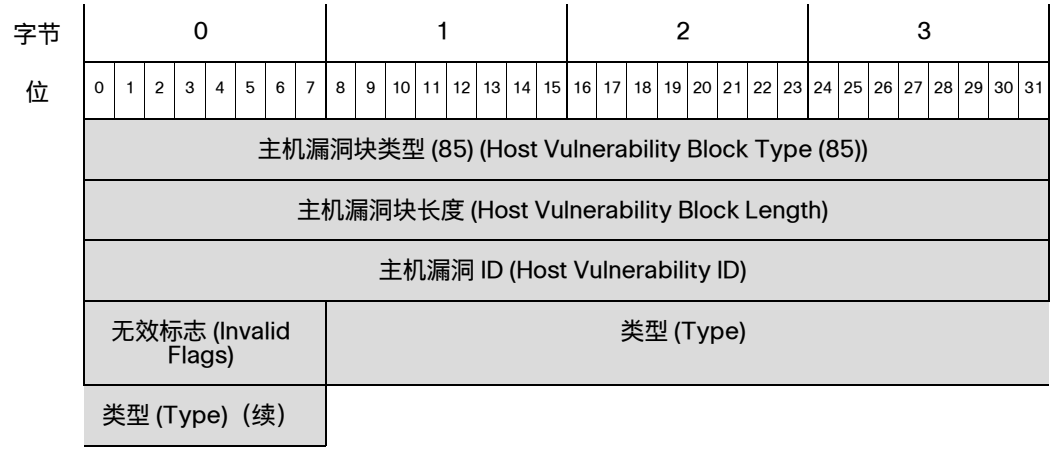
表 4-65 用户协议列表数据块字段

字段	字节数	说明 (Description)
用户协议列表块类型 (User Protocol List Block Type)	uint32	启动用户协议列表数据块。值始终为 `83`。
用户协议列表块长度 (User Protocol List Block Length)	uint32	用户协议列表数据块中的字节总数，包括用户协议列表块类型和长度字段的八个字节，加上随后的用户协议列表数据的字节数。
源类型 (Source Type)	uint32	映射到数据源类型的数字: ▪ `0` 如果协议数据由 RNA 提供 ▪ `1` 如果协议数据由用户提供 ▪ `2` 如果协议数据由第三方扫描仪提供 ▪ `3` 如果协议数据由命令行工具（如 `nmimport.pl`）或主机输入 API 客户端提供
源 ID (Source ID)	uint32	映射到受影响协议源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 `31`。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
用户协议数据块 (User Protocol Data Blocks)	变量	封装用户协议数据块数最多可以是列表块长度中的最大字节数。

主机漏洞数据块 4.9.0+

主机漏洞数据块传输应用于主机的漏洞。每个主机漏洞数据块描述一个事件中一个主机的一个漏洞。主机漏洞数据块在完整主机配置文件、完整主机服务器以及完整子服务器数据块中出现。主机漏洞数据块的块类型为系列 1 数据块组中的 85。

下图显示主机漏洞数据块的格式:



下表对主机漏洞数据块的组件进行了说明。

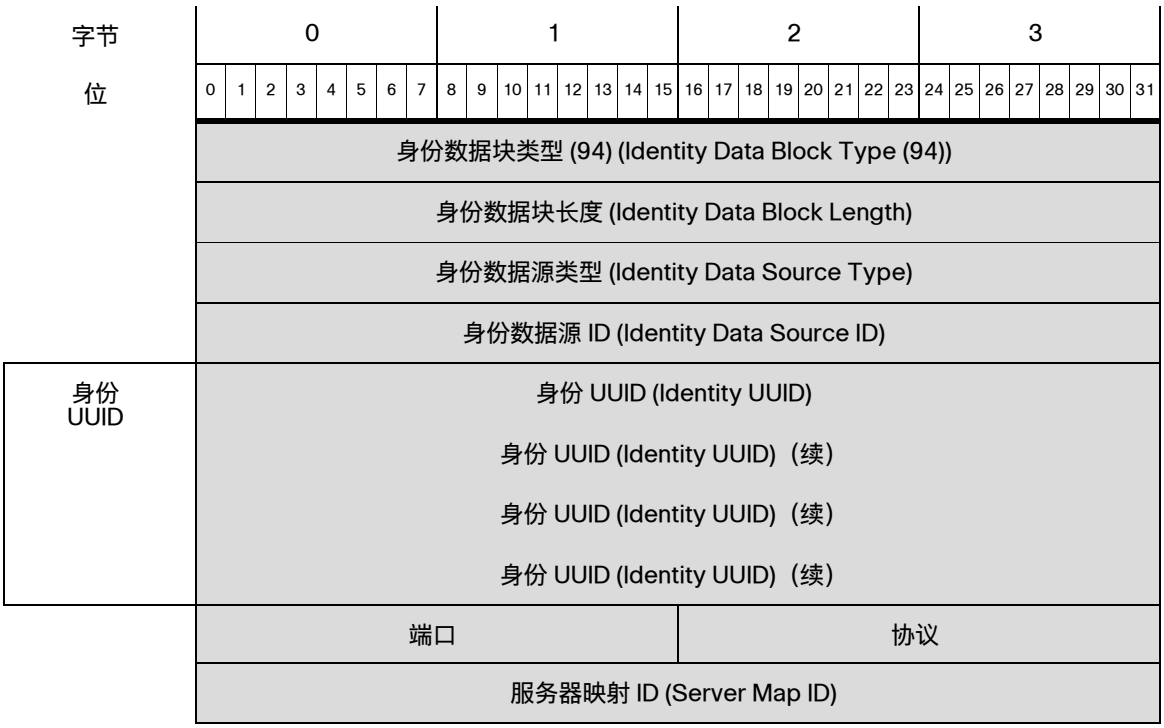
表 4-66　主机漏洞数据块字段

字段	数据类型	说明 (Description)
主机漏洞块类型 (Host Vulnerability Block Type)	uint32	启动主机漏洞数据块。值始终为 85。
主机漏洞块长度 (Host Vulnerability Block Length)	uint32	主机漏洞数据块中的字节总数，包括主机漏洞块类型和长度字段的八个字节，加上随后的主机漏洞数据的字节数。
主机漏洞 ID (Host Vulnerability ID)	uint32	漏洞的标识号。
无效标志 (Invalid Flags)	uint8	指示漏洞对于主机是否有效的一个值。
类型 (Type)	uint32	漏洞的类型。

身份数据块

身份数据块的块类型为系列 1 数据块组中的 94。身份数据块在身份冲突和身份超时消息中使用，表示操作系统或服务器指纹源的身份冲突或超时的时间。数据块描述已被识别为与活动的源身份冲突的报告身份（用户、扫描仪或应用）。有关详细信息，请参阅身份冲突和身份超时系统消息，第 4-57 页。

下图显示用于 4.9+ 的身份数据块的格式：



下表对思科身份数据块的字段进行了说明。

表 4-67　　身份数据块字段

字段	数据类型	说明 (Description)
身份数据块类型 (Identity Data Block Type)	uint32	启动身份数据块。值始终为 `94`。
身份数据块长度 (Identity Data Block Length)	uint32	身份数据块中的字节数。此值应始终为 40：数据块类型和长度字段以及源类型和 ID 字段的十六个字节，指纹 UUID 值的十六个字节，端口的两个字节，协议的两个字节以及 SM ID 的四个字节。
身份数据源类型 (Identity Data Source Type)	uint32	映射到数据源类型的数字： ▪ `0` 如果指纹数据由 RNA 提供 ▪ `1` 如果指纹数据由用户提供 ▪ `2` 如果指纹数据由第三方扫描仪提供 ▪ `3` 如果指纹数据由命令行工具（如 `nmimport.pl`）或主机输入 API 客户端提供

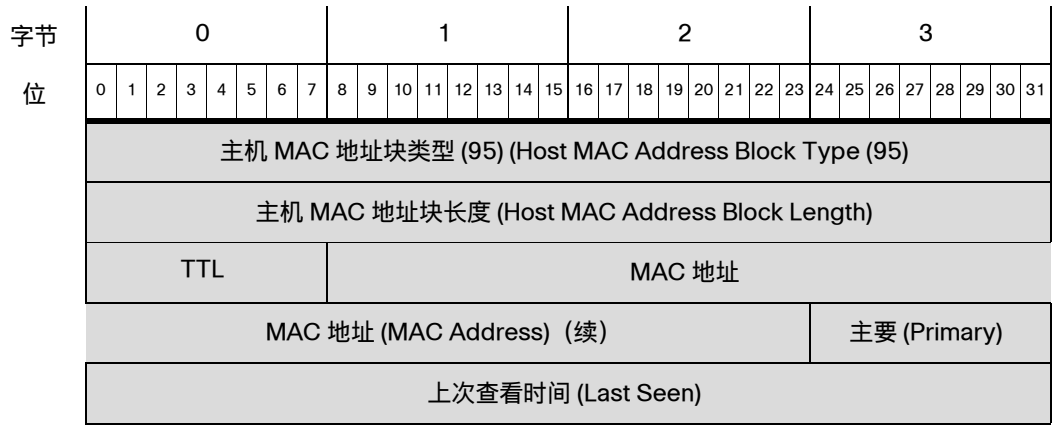
表 4-67　　身份数据块字段 （续）

字段	数据类型	说明 (Description)
身份数据源 ID (Identity Data Source ID)	uint32	映射到指纹数据源的标识号。根据源类型，这可能映射到RNA、用户、扫描仪或第三方应用。
UUID	uint8[16]	如果身份是操作系统身份，则 UUID 是充当指纹唯一标识符的标识号（八位组）。
端口 (Port)	uint16	如果身份是服务器身份，则表示包含服务器数据的数据包使用的端口。
协议 (Protocol)	uint16	如果身份是服务器身份，则表示网络协议的 IANA 号或包含服务器数据的数据包使用的 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如： ▪ 6 - TCP ▪ 7 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如： ▪ 2048 - IP
服务器映射 ID (Server Map ID)	uint32	如果身份是服务器身份，则表示服务器映射 ID，代表服务器 ID、供应商和版本的组合。

主机 MAC 地址 4.9+

主机 MAC 地址数据块的块类型为系列 1 数据块组中的 95。块包括主机数据的生存时间值，以及 MAC 地址、主机的主子网以及主机的上次查看时间值。

下图显示 4.9+ 中的主机 MAC 地址数据块的格式：



下表对主机 MAC 地址数据块的字段进行了说明。

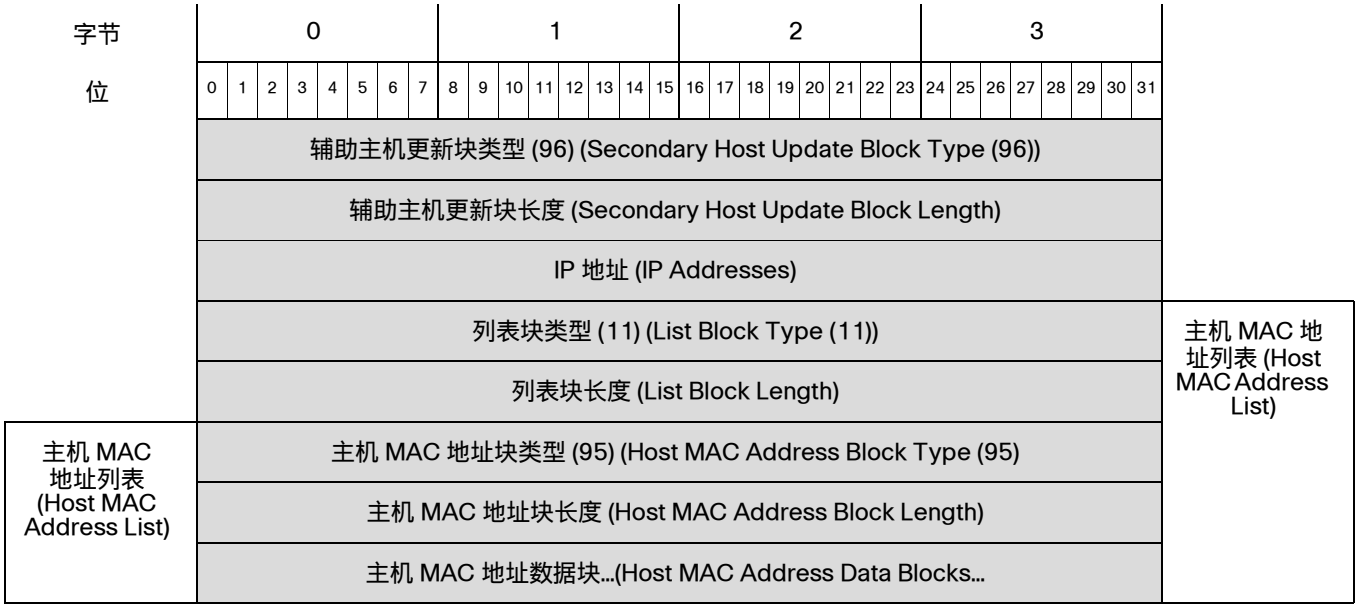
表 4-68 主机 MAC 地址数据块字段

字段	数据类型	说明 (Description)
主机 MAC 地址数据块类型 (Host MAC Address Data Block Type)	uint32	启动主机 MAC 地址数据块。值始终为 95。
主机 MAC 地址数据块长度 (Host MAC Address Data Block Length)	uint32	主机 MAC 地址数据块中的字节数。此值应始终为 20：数据块类型和长度字段的八个字节，TTL 值的一个字节，MAC 地址的 6 个字节，主子网的一个字节以及上次查看时间值的四个字节。
TTL	uint8	表示用于采集主机指纹的数据包中 TTL 值之间的差值。
MAC 地址 (MAC Address)	uint8 [6]	指示主机的 MAC 地址。
主要 (Primary)	uint8	指示主机的主子网。
上次查看时间 (Last Seen)	uint32	指示上次在流量中看到主机的时间。

辅助主机更新

辅助主机更新数据块包含从监控子网的设备而不是主机驻留的设备作为辅助主机更新发送的主机相关信息。它在更改辅助更新事件（事件类型 1001，子类型 31）中使用。辅助主机更新数据块的块类型为系列 1 数据块组中的 96。

下图显示辅助主机更新数据块的格式:



下表对辅助主机更新数据块的字段进行了说明。

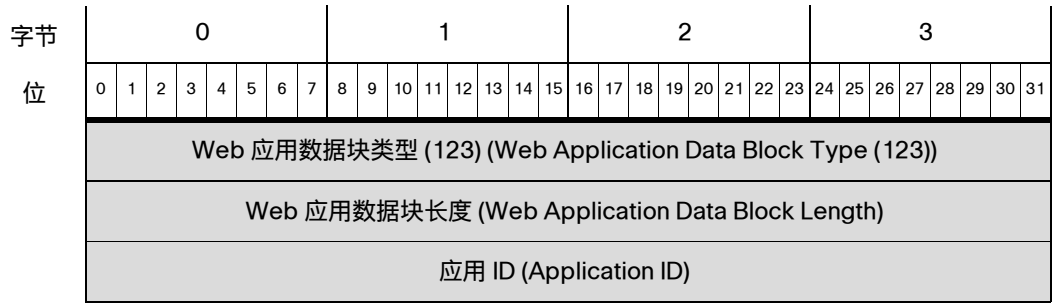
表 4-69　辅助主机更新数据块字段

字段	数据类型	说明 (Description)
辅助主机更新块类型 (Secondary Host Update Block Type)	uint32	启动辅助主机更新数据块。值始终为 96。
辅助主机更新块长度 (Secondary Host Update Block Length)	uint32	辅助主机更新数据块中的字节数，包括辅助主机更新块类型和长度字段的八个字节，加上随后的辅助主机更新数据的字节数。
IP 地址 (IP Address)	uint8[4]	更新中描述的主机的 IP 地址，采用 IP 地址八位组。
列表块类型 (List Block Type)	uint32	启动由传送主机 MAC 地址数据的主机 MAC 地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装主机 MAC 地址数据块。 此字段后面是零个或多个主机 MAC 地址数据块。
主机 MAC 地址块类型 (Host MAC Address Block Type)	uint32	启动描述辅助主机的主机 MAC 地址数据块。值始终为 95。
主机 MAC 地址数据块长度 (Host MAC Address Data Block Length)	uint32	主机 MAC 地址数据块中的字节数。此值应始终为 20：数据块类型和长度字段的八个字节，TTL 值的一个字节，MAC 地址的六个字节，主要子网的一个字节以及上次查看时间值的四个字节。
主机 MAC 地址数据块 (Host MAC Address Data Blocks)	字符串	与更新中的主机的 MAC 地址相关的信息。

用于 5.0+ 的 Web 应用数据块

用于 5.0+ 的 Web 应用数据块的块类型为系列 1 数据块组中的 123。该数据块描述检测到的 HTTP 客户端请求的 Web 应用。

下图显示 5.0+ 中的 Web 应用数据块的格式：



下表对 Web 应用数据块的字段进行了说明。

表 4-70　　Web 应用数据块字段

字段	数据类型	说明 (Description)
Web 应用数据块类型 (Web Application Data Block Type)	uint32	启动 Web 应用数据块。值始终为 123。
Web 应用数据块长度 (Web Application Data Block Length)	uint32	Web 应用数据块中的字节数，包括 Web 应用数据块类型和长度的八个字节，加上随后的应用 ID 字段中的字节数。
应用 ID (Application ID)	uint32	Web 应用的应用 ID。

连接统计信息数据块 7.1+

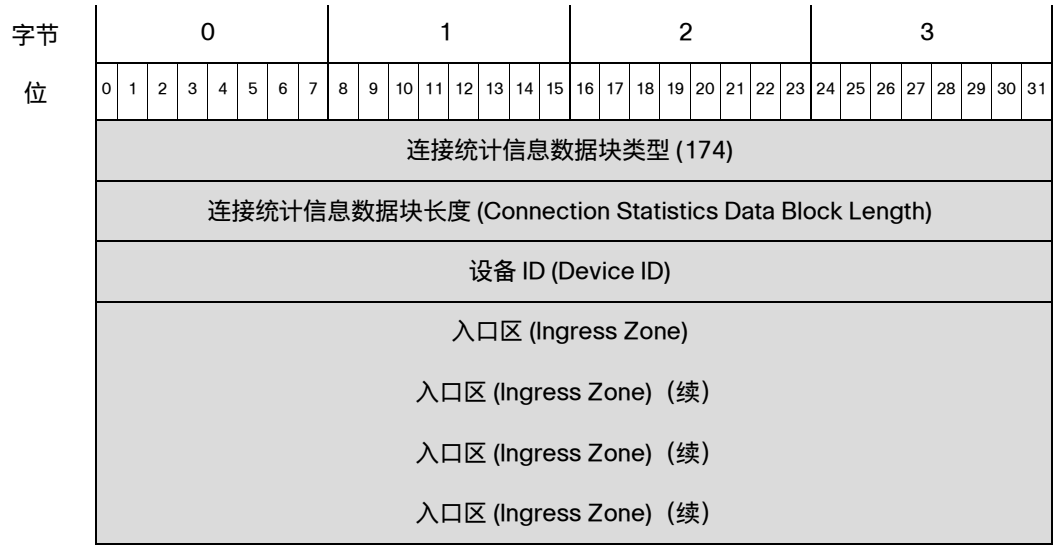
连接统计信息数据块在连接数据消息中使用。已添加 TLS 置信度字段、客户端应用检测器字段和 NAT 字段。用于版本 7.0+ 的连接统计信息数据块的块类型为系列 1 数据块组中的 174。它替代块类型 173，连接统计信息数据块 7.0，第 B-290 页。

您可以通过在事件版本为 16 且事件代码为 71 的请求消息中设置扩展事件标志（“请求标志”(Request Flags) 字段中的位 30）请求连接事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

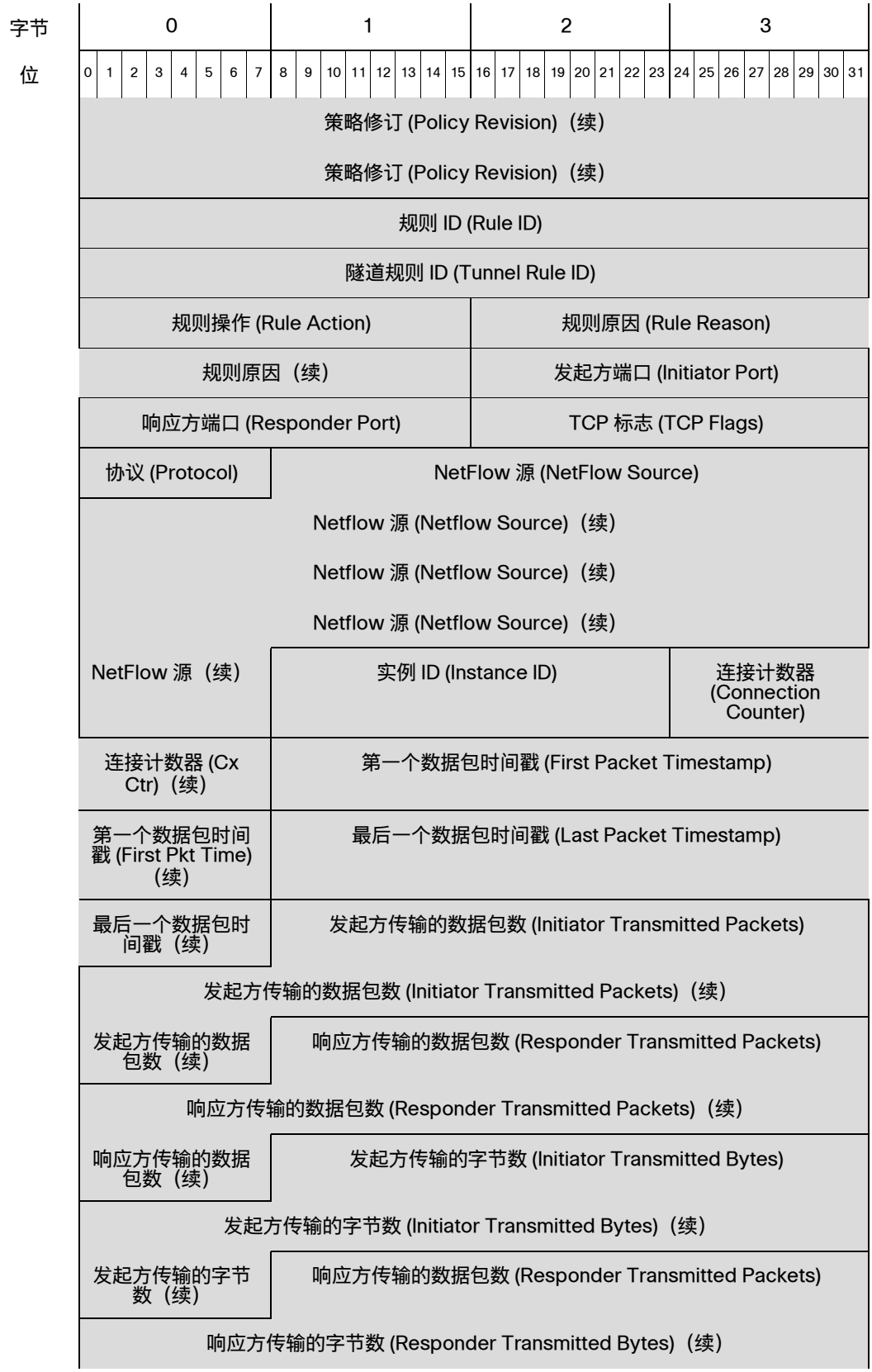
有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

下图显示用于 7.1+ 的连接统计信息数据块的格式：

7

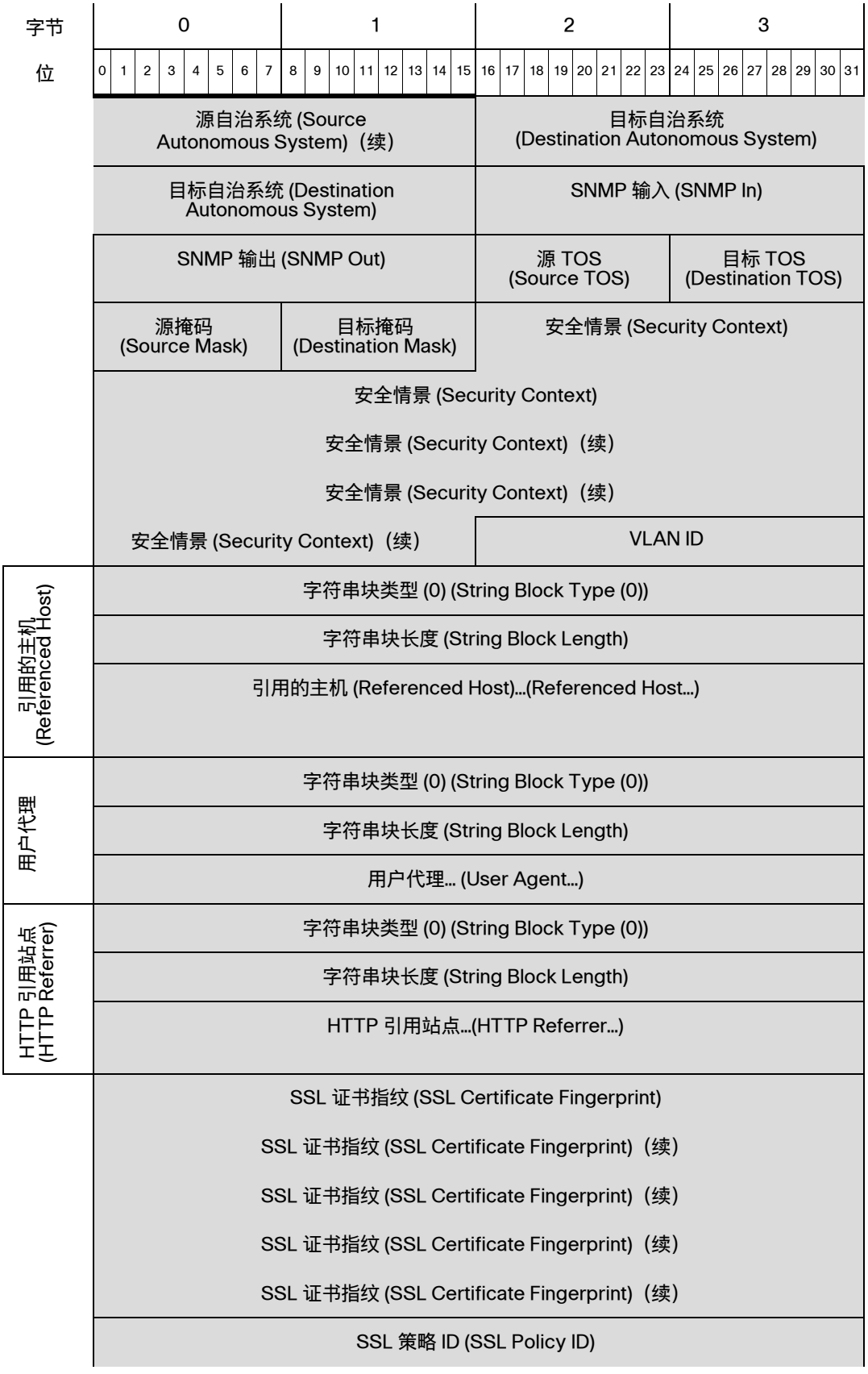


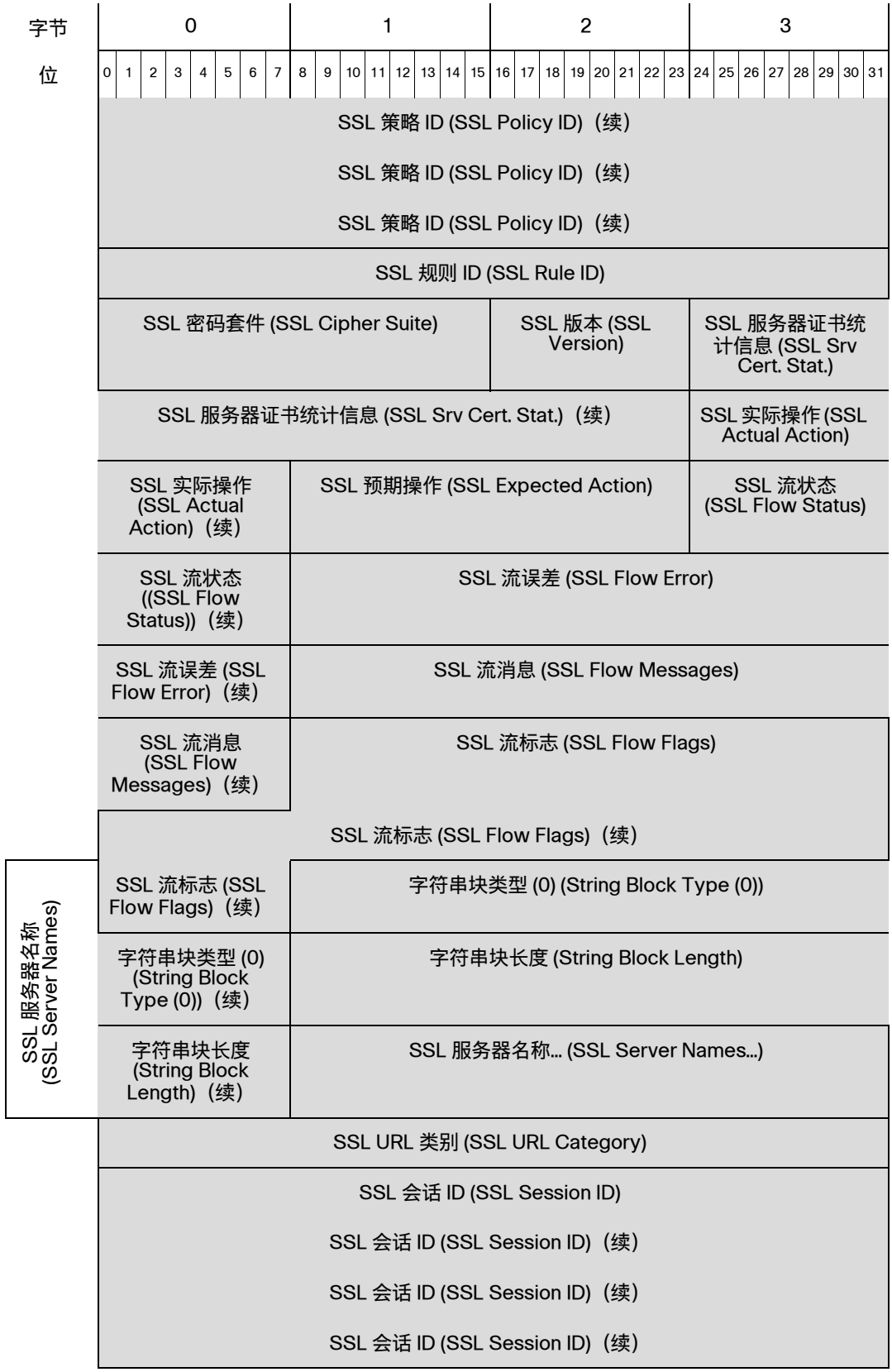
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出口区 (Egress Zone)																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
原始客户端 IP 地址 (Original Client IP Address)																																
原始客户端 IP 地址（续）																																
原始客户端 IP 地址（续）																																
原始客户端 IP 地址（续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision)（续）																																


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
策略修订 (Policy Revision)（续）
策略修订 (Policy Revision)（续）
规则 ID (Rule ID)
隧道规则 ID (Tunnel Rule ID)
规则操作 (Rule Action)
规则原因 (Rule Reason)
规则原因（续）
发起方端口 (Initiator Port)
响应方端口 (Responder Port)
TCP 标志 (TCP Flags)
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
NetFlow 源（续）
实例 ID (Instance ID)
连接计数器 (Connection Counter)
连接计数器 (Cx Ctr)（续）
第一个数据包时间戳 (First Packet Timestamp)
第一个数据包时间戳 (First Pkt Time)（续）
最后一个数据包时间戳 (Last Packet Timestamp)
最后一个数据包时间戳（续）
发起方传输的数据包数 (Initiator Transmitted Packets)
发起方传输的数据包数 (Initiator Transmitted Packets)（续）
发起方传输的数据包数（续）
响应方传输的数据包数 (Responder Transmitted Packets)
响应方传输的数据包数 (Responder Transmitted Packets)（续）
响应方传输的数据包数（续）
发起方传输的字节数 (Initiator Transmitted Bytes)
发起方传输的字节数 (Initiator Transmitted Bytes)（续）
发起方传输的字节数（续）
响应方传输的数据包数 (Responder Transmitted Packets)
响应方传输的字节数 (Responder Transmitted Bytes)（续）

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
响应方传输的字节数（续）	发起方丢弃的数据包数 (Initiator Packets Dropped)																															
发起方丢弃的数据包数 (Initiator Packets Dropped)（续）																																
发起方丢弃的数据包数（续）	响应方丢弃的数据包数 (Responder Packets Dropped) (Responder Packets Dropped)																															
响应方丢弃的数据包数 (Responder Packets Dropped)（续）																																
响应方丢弃的数据包数（续）	发起方丢弃的字节数 (Initiator Bytes Dropped) (Initiator Bytes Dropped)																															
发起方丢弃的字节数 (Initiator Bytes Dropped)（续）																																
发起方丢弃的字节数（续）	响应方丢弃的字节数 (Responder Bytes Dropped) (Responder Bytes Dropped)																															
响应方丢弃的字节数 (Responder Bytes Dropped)（续）																																
响应方丢弃的字节数（续）	QOS 应用的接口 (QOS Applied Interface)																															
QOS 应用的接口（续）																																
QOS 应用的接口（续）																																
QOS 应用的接口（续）																																
QOS 应用的接口（续）	QOS 规则 ID (QOS Rule ID)																															
QOS 规则 ID（续）	用户 ID																															
用户 ID (User ID)（续）	应用协议 ID (Application Protocol ID)																															
应用协议ID（续）	URL 类别 (URL Category)																															
URL 类别 (URL Category)（续）	URL 信誉 (URL Reputation)																															
URL 信誉 (URL Reputation)（续）	客户端应用 ID (Client Application ID)																															
客户端应用 ID (Client App ID)（续）	Web 应用 ID (Web Application ID)																															

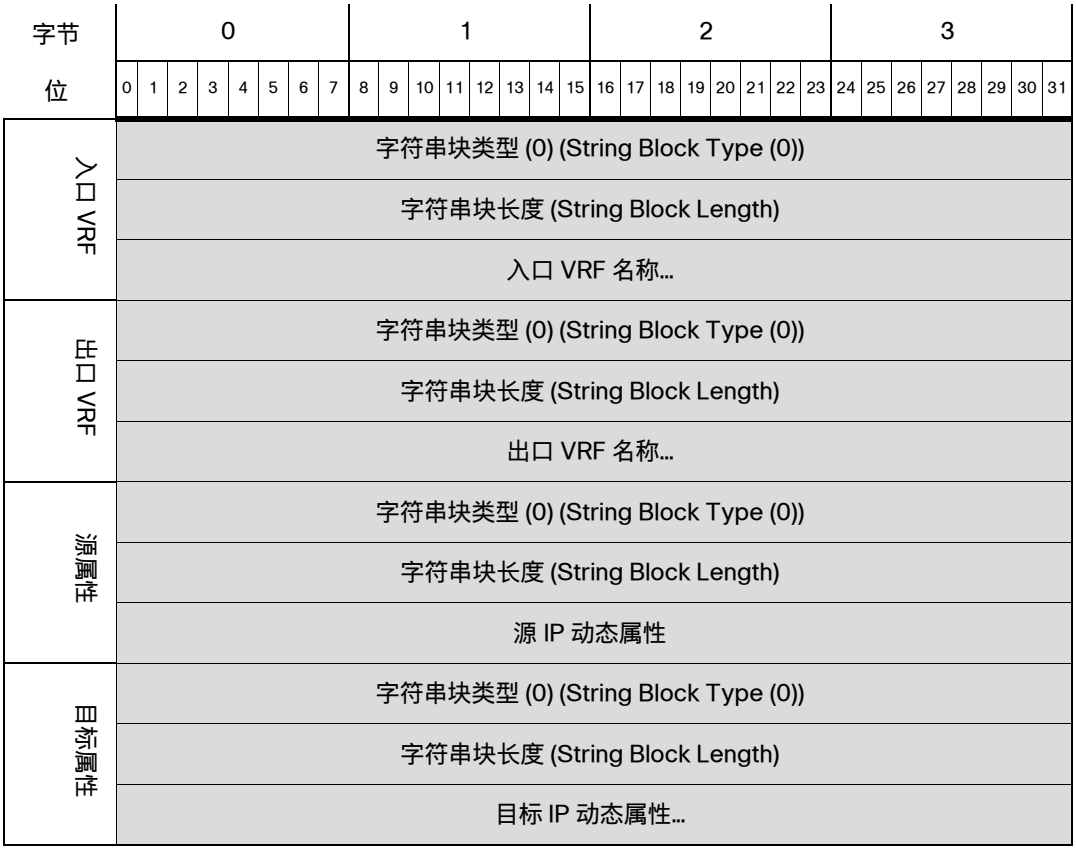
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
客户端 URL	Web 应用ID (Web App. ID) (续)								字符串块类型 (0) (Str. Block Type (0))																							
	字符串块类型 (续)								字符串块长度 (String Block Length)																							
	字符串块长度 (续)								客户端应用URL... (Client App. URL...)																							
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称...(NetBIOS Name...)																															
客户端 应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源/目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																发起方国家/地区 (Initiator Country)															
	响应方国家/地区 (Responder Country)																原始客户端国家/地区 (Original Client Country)															
	IOC 编号 (IOC Number)																源自治系统 (Source Autonomous System)															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
源自治系统 (Source Autonomous System)（续）
目标自治系统 (Destination Autonomous System)
目标自治系统 (Destination Autonomous System)
SNMP 输入 (SNMP In)
SNMP 输出 (SNMP Out)
源 TOS (Source TOS)
目标 TOS (Destination TOS)
源掩码 (Source Mask)
目标掩码 (Destination Mask)
安全情景 (Security Context)
安全情景 (Security Context)
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
VLAN ID
引用的主机 (Referenced Host)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
引用的主机 (Referenced Host)...(Referenced Host...)
用户代理
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
用户代理... (User Agent...)
HTTP 引用站点 (HTTP Referrer)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
HTTP 引用站点...(HTTP Referrer...)
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 策略 ID (SSL Policy ID)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）
SSL 规则 ID (SSL Rule ID)
SSL 密码套件 (SSL Cipher Suite)
SSL 版本 (SSL Version)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)（续）
SSL 实际操作 (SSL Actual Action)
SSL 实际操作 (SSL Actual Action)（续）
SSL 预期操作 (SSL Expected Action)
SSL 流状态 (SSL Flow Status)
SSL 流状态 ((SSL Flow Status))（续）
SSL 流误差 (SSL Flow Error)
SSL 流误差 (SSL Flow Error)（续）
SSL 流消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Messages)（续）
SSL 流标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags)（续）
SSL 流标志 (SSL Flow Flags)（续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
SSL 服务器名称... (SSL Server Names...)
SSL 服务器名称 (SSL Server Names)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID 长度 (SSL Session ID Length)
SSL 票证 ID (SSL Ticket ID)
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID 长度 (SSL Ticket ID Length)
网络分析策略修订 (Network Analysis Policy Revision)
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
终端配置文件 ID (Endpoint Profile ID)
终端配置文件 ID (Endpoint Profile ID)（续）
安全组 ID (Security Group ID)
安全组 ID (Security Group ID)（续）
源安全组标签
源秒组标记类型
目的安全组标签
目标秒组标记类型
位置 IPv6 (Location IPv6)
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
HTTP 响应 (HTTP Response)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
DNS 查询
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
DNS 查询...(DNS Query...)
DNS 记录类型 (DNS Record Type)
DNS 响应类型 (DNS Response Type)
DNS TTL
Sinkhole UUID
Sinkhole UUID（续）
Sinkhole UUID（续）
Sinkhole UUID（续）
安全情报列表 1 (Security Intelligence List 1)
安全情报列表 2 (Security Intelligence List 2)
威胁智能类别
TLSFPProcess
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
TLS FP 进程...
进程置信度
恶意软件置信度
恶意软件索引
客户端检测器
NAT 发起方端口
NAT 响应方端口
NAT 发起方 IP 地址 (NAT Initiator IP Address)
NAT 发起方 IP 地址 (NAT Initiator IP Address)（续）
NAT 发起方 IP 地址 (NAT Initiator IP Address)（续）
NAT 发起方 IP 地址 (NAT Initiator IP Address)（续）
NAT 响应方 IP 地址 (NAT Responder IP Address)
NAT 响应方 IP 地址 (NAT Responder IP Address)（续）
NAT 响应方 IP 地址 (NAT Responder IP Address)（续）
NAT 响应方 IP 地址 (NAT Responder IP Address)（续）



下表对用于 7.1+ 的连接统计信息数据块的字段进行了说明。

表 4-71　　连接统计信息数据块 7.1.+ 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 7.1.+ 的连接统计信息数据块。值始终为 174。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。

表 4-71 连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
原始客户端 IP 地址 (Original Client IP Address)	uint8[16]	位于发起请求的代理后面的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
隧道规则 ID (Tunnel Rule ID)	uint32	触发事件的隧道规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint32	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。

表 4-71　　连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
发起方丢弃的数据包数 (Initiator Packets Dropped)	uint64	由于速率限制而从会话发起方丢弃的数据包的数量。
响应方丢弃的数据包数 (Responder Packets Dropped)	uint64	由于速率限制而从会话响应方丢弃的数据包的数量。
发起方丢弃的字节数 (Initiator Bytes Dropped)	uint64	由于速率限制而从会话发起方丢弃的字节的数量。
响应方丢弃的字节数(Responder Bytes Dropped)	uint64	由于速率限制而从会话响应方丢弃的字节的数量。
QOS 应用的接口	uint8[16]	对于速率受限的连接，是指应用了速率限制的接口的名称。
QOS 规则 ID (QOS Rule ID)	uint32	应用于连接的服务质量规则的内部 ID 号码（如适用）。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。

表 4-71 连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如，`/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。

表 4-71　连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家/地区 (Initiator Country)	uint16	发起主机的国家/地区代码。
响应方国家/地区 (Responder Country)	uint 16	响应主机的国家/地区代码。
原始客户端国家/地区 (Original Client Country)	uint 16	位于发起请求的代理后面的主机的国家/地区的代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“引用的主机”(Referenced Host) 字段中的字节数。
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。

表 4-71 连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户代理”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“HTTP 引用站点”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在HTTP流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 证书的状态。可能的值包括： ▪ 0 - 未检查 - 服务器证书状态未评估。 ▪ 1 - 未知 - 服务器证书状态无法确定。 ▪ 2 - 有效 - 服务器证书有效。 ▪ 4 - 自签 - 服务器证书已自签。 ▪ 16 - 颁发者无效 - 服务器证书的颁发者无效。 ▪ 32 - 签名无效 - 服务器证书的签名无效。 ▪ 64 - 过期 - 服务器证书已过期。 ▪ 128 - 尚未生效 - 服务器证书尚未生效。 ▪ 256 - 撤销 - 服务器证书已被撤销。

表 4-71　连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 4-71 连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 4-71　连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 ▪ 0x00000001 - NSE_MT__HELLO_REQUEST ▪ 0x00000002 - NSE_MT__CLIENT_ALERT ▪ 0x00000004 - NSE_MT__SERVER_ALERT ▪ 0x00000008 - NSE_MT__CLIENT_HELLO ▪ 0x00000010 - NSE_MT__SERVER_HELLO ▪ 0x00000020 - NSE_MT__SERVER_CERTIFICATE ▪ 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE ▪ 0x00000080 - NSE_MT__CERTIFICATE_REQUEST ▪ 0x00000100 - NSE_MT__SERVER_HELLO_DONE ▪ 0x00000200 - NSE_MT__CLIENT_CERTIFICATE ▪ 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE ▪ 0x00000800 - NSE_MT__CERTIFICATE_VERIFY ▪ 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC ▪ 0x00002000 - NSE_MT__CLIENT_FINISHED ▪ 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC ▪ 0x00008000 - NSE_MT__SERVER_FINISHED ▪ 0x00010000 - NSE_MT__NEW_SESSION_TICKET ▪ 0x00020000 - NSE_MT__HANDSHAKE_OTHER ▪ 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT ▪ 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括： ▪ 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 ▪ 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 ▪ 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“SSL 服务器名称”(SSL Server Name) 字段中的字节数。
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时，SSL 握手期间使用的会话 ID 值

表 4-71 连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy Revision)	uint8[16]	与连接事件相关的网络分析策略的修订。
终端配置文件 ID (Endpoint Profile ID)	uint32	ISE 识别的连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	由 ISE 根据策略分配给用户的 ID 号码。
源安全组标签	uint16	连接源的安全组标记。
源安全组标记类型	uint8	如何分配源安全组标记: ▪ 0 — 未知 ▪ 1 — 内联 ▪ 2 — 会话目录 ▪ 3 — 安全组标记交换协议 (SXP)
目的安全组标签	uint16	连接目标的安全组标记。
目标安全组标记类型	uint8	如何分配目标安全组标记: ▪ 0 — 未知 ▪ 1 — 内联 ▪ 2 — 会话目录 ▪ 3 — 安全组标记交换协议 (SXP)
位置 IPv6 (Location IPv6)	uint8[16]	与 ISE 通信的接口的 IP 地址。可以是 IPv4 或 IPv6。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。
字符串块类型 (String Block Type)	uint32	启动 DNS 查询的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 DNS 查询字符串中的字节数。
DNS 查询 (DNS Query)	字符串	发送到 DNS 服务器的查询的内容。
DNS 记录类型 (DNS Record	uint16	DNS 记录类型的数字值。

表 4-71　连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
DNS 响应类型 (DNS Response Type)	uint16	DNS 响应类型的数字值。
DNS TTL	uint32	DNS 响应的生存时间（秒数）
Sinkhole UUID	uin8[16]	与此 sinkhole 对象关联的修订 UUID。
安全情报列表 1 (Security Intelligence List)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能有三个与连接关联的安全情报列表。
安全情报列表 2 (Security Intelligence List)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能有三个与连接关联的安全情报列表。
威胁智能类别	uint32	与事件关联的威胁智能类别。这映射到关联元数据中的威胁智能列表。
字符串块类型 (String Block Type)	uint32	启动包含 TLS 指纹进程的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上 TLS 指纹进程 (TLS Fingerprint Process) 字段中的字节数。
TLS 指纹进程	字符串	从加密可视性引擎识别的指纹的进程名称系列。
TLS FP 进程置信度	uint8	加密可视性引擎（EVE）检测到正确进程的置信度值范围为 0-100%。例如，如果进程名称为 Firefox，并且置信度分数为 80%，则意味着引擎 80% 的置信度表示其检测到的进程是 Firefox。
TLS FP 恶意软件置信度	uint8	加密可视性引擎（EVE）检测到的进程包含恶意软件的置信度值范围为 0-100%。如果恶意软件置信度分数非常高，例如 90%，则 TLS 指纹进程名称字段显示“恶意软件”。
TLS FP 恶意软件索引	uint8	加密可视性引擎 (EVE) 检测到的进程包含恶意软件的概率级别。此字段根据恶意软件置信度分数中的值指示频段（非常高，高，中，低或非常低）。
客户端应用检测器类型	uint8	此字段显示客户端的检测来源。如果应用未加密且未使用正常逻辑检测到，则可以为 0；如果由加密可视性引擎检测到，则为 1。
NAT 发起方端口	uint16	会话发起方使用的端口号。
NAT 响应方端口	uint16	会话响应者使用的端口号。
NAT 发起方 IP	uint8[16]	会话发起方的 NAT 转换 IP 地址。
NAT 响应方 IP	uint8[16]	会话响应方的 NAT 转换 IP 地址。
字符串块类型 (String Block Type)	uint32	启动包含入口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“入口 VRF ”(Ingress VRF) 名称字段中的字节数。
入口 VRF 名称	字符串	用于流量进入网络的虚拟路由器。
字符串块类型 (String Block Type)	uint32	启动包含出口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“出口 VRF ”(Egress VRF) 名称字段中的字节数。

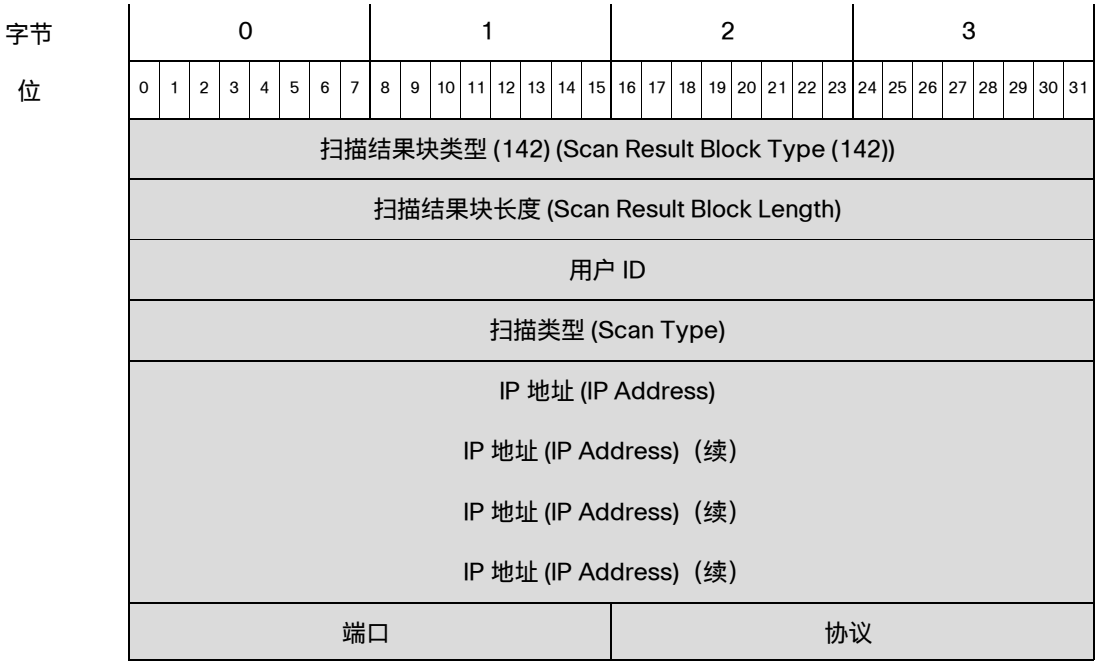
表 4-71 连接统计信息数据块 7.1.+ 字段 （续）

字段	数据类型	说明 (Description)
出口 VRF 名称	字符串	用于流量离开网络的虚拟路由器。
字符串块类型 (String Block Type)	uint32	启动包含源 IP 动态属性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“源 IP 动态属性”(Source IP Dynamic Attribute) 字段中的字节数。
源 IP 动态属性	字符串	与源 IP 地址关联的动态属性。
字符串块类型 (String Block Type)	uint32	启动包含目标 IP 动态属性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“目标 IP 动态属性”(Destination IP Dynamic Attribute) 字段中的字节数。
目标 IP 动态属性	字符串	与目标 IP 地址关联的动态属性。

扫描结果数据块 5.2+

扫描结果数据块对漏洞进行说明，在添加扫描结果事件（事件类型 1002，子类型 11）中使用。扫描结果数据块的块类型为系列 1 数据块组中的 142。它替代块类型 102。版本 5.2 的 IP 地址字段增加到 16 个字节。

下图显示扫描结果数据块的格式:



字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
	标志																列表块类型 (11) (List Block Type (11))																扫描漏洞列表 (Scan Vulnerability List)
	列表块类型 (11) (List Block Type (11))																列表块长度 (List Block Length)																
漏洞列表	列表块长度 (List Block Length)																扫描漏洞块类型 (109) (Scan Vulnerability Block Type (109))																
	扫描漏洞块类型 (109) (Scan Vulnerability Block Type (109))																扫描漏洞块长度 (Scan Vulnerability Block Length)																
	扫描漏洞块长度 (Scan Vulnerability Block Length)																漏洞数据...(Vulnerability Data...)																
	列表块类型 (11) (List Block Type (11))																																一般扫描结果列表 (Generic Scan Results List)
	列表块长度 (List Block Length)																																
Scan Results 列表	一般扫描结果块类型 (108) (Generic Scan Results Block Type (108)																																
	一般扫描结果块长度 (Generic Scan Results Block Length)																																
	一般扫描结果...(Generic Scan Results...)																																
用户产品列表	通用列表块类型 (31) (Generic List Block Type (31))																																
	通用列表块长度 (Generic List Block Length)																																
	用户产品数据块 (User Product Data Blocks)*																																

下表对扫描结果数据块的字段进行了说明。

表 4-72　　扫描结果数据块字段

字段	数据类型	说明 (Description)
扫描结果块类型 (Scan Result Block Type)	uint32	启动扫描结果数据块。值始终为 142。
扫描结果块长度 (Scan Result Block Length)	uint32	扫描漏洞数据块中的字节数，包括扫描漏洞块类型和长度字段的八个字节，加上随后的扫描漏洞数据的字节数。
用户 ID	uint32	包含导入扫描结果或运行产生该扫描结果的扫描的用户的用户标识号。
扫描类型	uint32	表明结果是如何添加到系统中的。
IP 地址 (IP Address)	uint8[16]	受结果中的漏洞影响的主机的 IP 地址，采用 IP 地址八位组。
端口 (Port)	uint16	受结果中的漏洞影响的子服务器使用的端口。

表 4-72 扫描结果数据块字段 （续）

字段	数据类型	说明 (Description)
协议 (Protocol)	uint16	IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如： ▪ 6 - TCP ▪ 17 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如： ▪ 2048 - IP
标志	uint16	保留
列表块类型 (List Block Type)	uint32	启动由传送传输扫描漏洞数据的扫描漏洞数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装扫描漏洞数据块。 此字段后面是零个或多个扫描漏洞数据块。
扫描漏洞块类型 (Scan Vulnerability Block Type)	uint32	启动对扫描期间检测到的漏洞进行说明的扫描漏洞数据块。值始终为 109。
扫描漏洞块长度 (Scan Vulnerability Block Length)	uint32	扫描漏洞数据块中的字节数，包括扫描漏洞块类型和长度字段的八个字节，加上随后的扫描漏洞数据中的字节数。
漏洞数据 (Vulnerability Data)	字符串	每个漏洞的相关信息。
列表块类型 (List Block Type)	uint32	启动由传送传输扫描漏洞数据的扫描漏洞数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装扫描漏洞数据块。 此字段后面是零个或多个扫描漏洞数据块。
一般扫描结果块类型 (Generic Scan Results Block Type)	uint32	启动对扫描期间检测到的服务器和操作系统数据进行说明的一般扫描结果数据块。值始终为 108。
一般扫描结果块长度 (Generic Scan Results Block Length)	uint32	一般扫描结果数据块中的字节数，包括一般扫描结果块类型和长度字段的八个字节，加上随后的扫描结果数据中的字节数。

表 4-72　扫描结果数据块字段 （续）

字段	数据类型	说明 (Description)
一般扫描结果数据 (Generic Scan Results Data)	字符串	每个扫描结果的相关信息。
通用列表块类型 (Generic List Block	uint32	启动由传送第三方应用中的主机输入数据的用户产品数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装用户产品数据块。
用户产品数据块 (User Product Data Blocks) *	变量	包含主机输入数据的用户产品数据块。有关此数据块的说明，请参阅用户产品数据块 5.1+，第 4-173 页。

主机服务器数据块 4.10.0+

主机服务器数据块传输在主机上检测到的服务器的相关信息。它包含每个检测到的服务器的块，且包含服务器运行的 Web 应用的 Web 应用数据块列表。新 TCP 和 UDP 服务器和更改 TCP 和 UDP 服务器的消息中包含主机服务器数据块。有关详细信息，请参阅服务器消息，第 4-44 页。主机服务器数据块的块类型为系列 1 数据块组中的 103。

注释　下图中数据块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示主机服务器数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
服务器块类型 (103) (Server Block Type (103))																																
服务器块长度 (Server Block Length)																																
端口 (Port)																	命中数 (Hits)															
命中数 (Hits)（续）																	上次使用时间 (Last Used)															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
子服务器信息 (Sub-Server Information)	上次使用时间 (Last Used)（续）																通用列表块类型 (31) (Generic List Block Type (31))															
	通用列表块类型 (Generic List Block Type)（续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length)（续）																服务器信息块类型 (117) (Server Information Block Type (117))*															
	置信																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
Web 应用程序 (Web Application)	Web 应用块类型 (123) (Web Application Block Type (123))*																															
	Web 应用块长度 (Web Application Block Length)																															
	Web 应用数据...(Web Application Data...)																															

下表对主机服务器数据块的字段进行了说明。

表 4-73 主机服务器数据块字段

字段	数据类型	说明 (Description)
主机服务器块类型 (Host Server Block Type)	uint32	启动主机服务器数据块。值始终为 `103`。
主机服务器块长度 (Host Server Block Length)	uint32	主机服务器数据块中的字节总数，包括主机服务器块类型和长度字段的八个字节，加上随后的数据的字节数。
端口 (Port)	uint16	服务器在其上运行的端口的端口号。
命中数 (Hits)	uint32	服务器接收的命中数。
上次使用时间 (Last Used)	uint32	表示系统上次检测到使用中的服务器的 UNIX 时间戳。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 `31`。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装子服务器信息数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
服务器信息数据块 (Server Information Data Blocks)*	变量	服务器信息数据块数最多可以是列表块长度中的最大字节数。有关详细信息，请参阅用于 4.10.x、5.0 - 5.0.2 的服务器信息数据块，第 4-145 页。

表 4-73　主机服务器数据块字段 （续）

字段	数据类型	说明 (Description)
置信 (Confidence)	uint32	置信度百分比。
通用列表块类型 (Generic List Block	uint32	启动通用数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用块和封装 Web 应用数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装 Web 应用数据块中的字节数。
Web 应用数据块 (Client Application Data Blocks)*	变量	封装 Web 应用数据块数最多可以是列表块长度中的最大字节数。有关详细信息，请参阅用于 5.0+ 的 Web 应用数据块，第 4-115 页。

完整主机服务器数据块 4.10.0+

完整主机服务器数据块传输服务器相关信息，包括服务器端口、使用频率和最新更新、数据精度的置信度以及与主机的该服务器相关的思科和第三方漏洞。完整主机服务器数据块包含用于服务器上的每个子服务器的完整子服务器信息数据块。每个完整主机配置文件数据块包含用于主机上的每个 TCP 和 UDP 服务器的完整主机服务器数据块。完整主机服务器数据块的块类型为系列 1 数据块组中的 104。

注释　下图中系列 1 数据块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示完整服务器数据块的格式:

::

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	完整服务器块类型 (104) (Full Server Block Type (104))																															
	完整服务器块长度 (Full Server Block Length)																															
	端口 (Port)																命中数 (Hits)															
子服务器 - (Sub-Servers -) 思科	命中数 (Hits) （续）																通用列表块类型 (31) (Generic List Block Type (31))															
	通用列表块类型 (Generic List Block Type) （续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length) （续）																完整服务器信息数据块 (106) (Full Server Information Data Blocks (106))*															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
子服务器 - 用户	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	完整服务器信息数据块类型 (106) (Full Server Information Data Block Type (106))*																															
子服务器 - 扫描器	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	完整服务器信息数据块 (106) (Full Server Information Data Blocks (106))*																															
子服务器 - 应用	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	完整服务器信息数据块 (106) (Full Server Information Data Blocks (106))*																															
	置信																															
Server 横幅	BLOB 块类型 (10) (BLOB Block Type (10))																															
	BLOB 块长度 (BLOB Block Length)																															
	服务器横幅数据...(Server Banner Data...)																															
VDB 漏洞	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(VDB) 主机漏洞数据块 (85) ((VDB) Host Vulnerability Data Blocks (85))*																															
第三方/VDB 漏洞	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方/VDB）主机漏洞数据块 (85) ((Third Party/VDB) Host Vulnerability Data Blocks (85))*																															
第三方主机漏洞	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方）主机漏洞数据块 (85) ((Third Party) Host Vulnerability Data Blocks (85))*																															
Web 应用	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	Web 应用数据 (123) (Web Application Data (123))*																															

下表对完整服务器数据块的组件进行了说明。

表 4-74　　完整服务器数据块 4.10.0+ 字段

字段	数据类型	说明 (Description)
完整服务器块类型 (Full Server Block Type)	uint32	启动完整服务器数据块。值始终为 104。
完整服务器块长度 (Full Server Block Length)	uint32	完整服务器数据块中的字节总数，包括完整服务器块类型和长度字段的八个字节，加上随后的完整服务器数据的字节数。
端口 (Port)	uint16	服务器端口号。
命中数 (Hits)	uint32	服务器接收的命中数。
通用列表块类型 (Generic List Block	uint32	启动由检测到的子服务器数据的数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装子服务器信息数据块。
子服务器信息 - 思科数据块 (Sub-Server Information - 思科 Data Blocks) *	变量	包含思科检测到的主机服务器的子服务器的相关信息的完整主机信息数据块。有关此数据块的说明，请参阅完整服务器信息数据块，第 4-147 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用户添加的子服务器数据的子服务器信息数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装服务器信息数据块。
子服务器信息 - 用户添加数据块 (Sub-Server Information- User Added Data Blocks) *	变量	包含用户添加的主机上的子服务器的相关信息的完整主机信息数据块。有关此数据块的说明，请参阅完整服务器信息数据块，第 4-147 页。
通用列表块类型 (Generic List Block	uint32	启动由传送扫描仪添加的子服务器数据的子服务器信息数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装子服务器信息数据块。
子服务器信息 - 扫描添加数据块 (Sub-Server Information- Scan Added Data Blocks) *	变量	包含扫描仪添加的主机上的子服务器的相关信息的完整主机信息数据块。有关此数据块的说明，请参阅完整服务器信息数据块，第 4-147 页。
通用列表块类型 (Generic List Block	uint32	启动由传送应用添加的子服务器数据的子服务器信息数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装子服务器信息数据块。

表 4-74 完整服务器数据块 4.10.0+ 字段 （续）

字段	数据类型	说明 (Description)
子服务器信息 - 应用添加数据块 (Sub-Server Information - Application Added Data Blocks) *	变量	包含应用添加的主机上的子服务器的相关信息的完整主机信息数据块。有关此数据块的说明，请参阅完整服务器信息数据块，第 4-147 页。
置信 (Confidence)	uint32	思科在正确识别完整服务器数据方面的置信度百分比。
BLOB 块类型 (BLOB Block Type)	uint32	启动包含横幅数据的 BLOB 数据块。值始终为 10。
BLOB 块长度 (BLOB Block Length)	uint32	BLOB 数据块中的字节总数，包括块类型和长度字段的八个字节，加上横幅中的字节数。
服务器横幅数据 (Server Banner Data)	字节[*n*]	服务器事件中涉及的数据包的前 *n* 个字节，其中 *n* 小于或等于 256。
通用列表块类型 (Generic List Block	uint32	启动由传送思科漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装主机漏洞数据块。
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks) *	变量	包含漏洞数据库 (VDB) 中主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
通用列表块类型 (Generic List Block	uint32	启动由主机漏洞数据块组成的通用列表数据块，这些主机漏洞数据块传输源自第三方扫描仪的第三方主机漏洞数据，并且包含已收录到 VDB 的漏洞信。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装主机漏洞数据块。
（第三方/VDB）主机漏洞数据块 ((Third Party/VDB) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪且包含已收录到漏洞数据库 (VDB) 中的主机漏洞相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
通用列表块类型 (Generic List Block	uint32	启动由传输第三方扫描仪生成的第三方主机漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装主机漏洞数据块。
第三方扫描主机漏洞数据块 (Third Party Scan Host Vulnerability Data Blocks) *	变量	包含第三方扫描仪识别但未收录到 VDB 中的漏洞的第三方漏洞数据的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。

表 4-74　　完整服务器数据块 4.10.0+ 字段 （续）

字段	数据类型	说明 (Description)
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装 Web 应用数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
Web 应用数据块 (Client Application Data Blocks)*	变量	封装 Web 应用数据块数最多可以是列表块长度中的最大字节数。

用于 4.10.x、5.0 - 5.0.2 的服务器信息数据块

服务器信息数据块传输服务器的相关信息，包括服务器 ID、服务器供应商和版本以及源信息。在 4.10.x 中，服务器信息数据块的块类型为系列 1 数据块组中的 105，在 5.0 - 5.0.2 中，块类型为系列 1 数据块组中的 117。服务器信息数据块在主机服务器块和完整主机服务器数据块中的列表中传输。有关详细信息，请参阅主机服务器数据块 4.10.0+，第 4-139 页和完整主机服务器数据块 4.10.0+，第 4-141 页。

下图显示服务器信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
服务器信息块类型 (105	117) (Server Information Block Type (105	117))																														
服务器信息块长度 (Server Information Block																																
应用 ID (Application ID)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
服务器供应商名称字符串...(Server Vendor Name String...)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
服务器版本字符串...(Server Version String...)																																
上次使用时间 (Last Used)																																
源类型 (Source Type)																																
源 ID (Source ID)																																
列表块类型 (11) (List Block Type (11))																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	列表块长度 (List Block Length)																															
子服务器 (Sub-Servers)	子服务器块类型 (1) (Sub-Server Block Type (1)) *																															
	子服务器块长度 (Sub-Server Block Length)																															
	子服务器数据...(Sub-Server Data...)																															

下表对服务器信息数据块的组件进行了说明。

表 4-75 服务器信息数据块字段

字段	数据类型	说明 (Description)
服务器信息块类型 (Server Information Blockype)	uint32	启动服务器信息数据块。在 4.10.x 中，块类型为 105，在 5.0+ 中，块类型为 117。
服务器信息块长度 (Server Information Blockength)	uint32	服务器信息数据块中的字节总数，包括服务器信息块类型和长度字段的八个字节，服务器 ID 的四个字节，供应商名称块类型和长度的八个字节，供应商名称的另外四个字节，版本字符串块类型和长度的八个字节，版本字符串的另外四个字节，以及上次使用时间、源类型以及源 ID 字段的各四个字节。
应用 ID (Application ID)	uint32	在检测到的服务器上运行的应用协议的应用 ID。
字符串块类型 (String Block Type)	uint32	启动包含服务器供应商名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	供应商名称字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上服务器供应商名称中的字节数。
服务器供应商名称 (Server Vendor Name)	字符串	服务器供应商的名称。
字符串块类型 (String Block Type)	uint32	启动包含服务器版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	服务器版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上服务器版本中的字节数。
服务器版本 (Server Version)	字符串	服务器版本。
上次使用时间 (Last Time Used)	uint32	指示上次在流量中使用服务器信息的时间。

表 4-75　服务器信息数据块字段 （续）

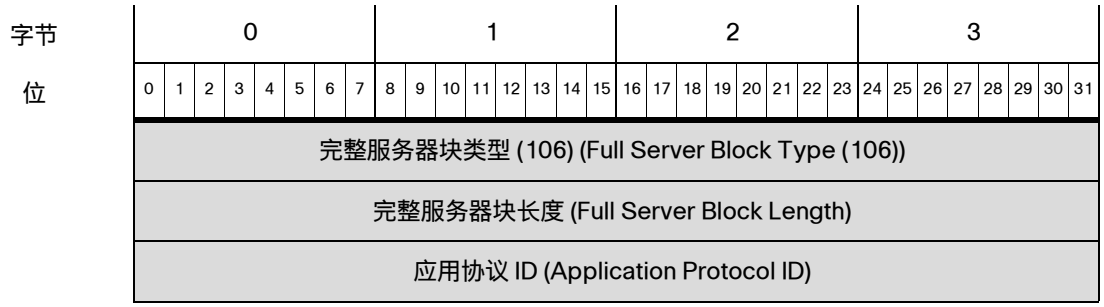
字段	数据类型	说明 (Description)
源类型 (Source Type)	uint32	映射到数据源类型的数字： ▪ 0 如果服务器数据由 RNA 提供 ▪ 1 如果服务器数据由用户提供 ▪ 2 如果服务器数据由第三方扫描仪提供 ▪ 3 如果服务器数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
源 ID (Source ID)	uint32	映射到服务器数据源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
列表块类型 (List Block Type)	uint32	启动子服务器数据块列表。值始终为 11。
列表块长度 (List Block Length)	uint32	列表数据块中的字节数，包括列表块类型和长度字段的八个字节，加上随后的封装子服务器数据块中的字节数。
子服务器块类型 (Sub-Server Block Type)	uint32	启动第一个子服务器数据块。此数据块后面可以跟随最大长度为列表块长度字段中定义的限值的其他子服务器数据块。
子服务器块长度 (Sub-Server Block Length)	uint32	每个子服务器数据块中的字节总数，包括子服务器块类型和长度字段的八个字节，加上随后的数据的字节数。
子服务器数据 (Sub-Server Data)	变量	子服务器数据，如子服务器数据块，第 4-70 页中所记录。

完整服务器信息数据块

完整服务器信息数据块传输在主机上检测到的服务器的相关信息，包括服务器的应用协议、供应商和版本及其关联子服务器的列表。对于每个子服务器，完整子服务器数据块包含其信息（请参阅完整子服务器数据块，第 4-81 页）。完整服务器信息数据块的块类型为系列 1 数据块组中的 106。

注释　下图中系列 1 数据块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示完整服务器信息数据块的格式：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
供应商	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	供应商名称字符串...(Vendor Name String...)																															
版本	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	版本字符串...(Version String...)																															
	上次使用时间 (Last Used)																															
	源类型 (Source Type)																															
	源 ID (Source ID)																															
	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
子服务器 (Sub-Servers)	完整子服务器块类型 (51) (Full Sub-Server Block Type (51)) *																															
	完整子服务器块长度 (Full Sub-Server Block Length)																															
	完整子服务器数据...(Full Sub-Server Data...)																															

下表对完整服务器信息数据块的组件进行了说明。

表 4-76 完整服务器信息数据块字段

字段	数据类型	说明 (Description)
完整服务器信息块类型 (Full Server Information Block Type)	uint32	启动完整服务器信息数据块。值始终为 106。
完整服务器信息块长度 (Full Server Information Block Length)	uint32	完整服务器信息数据块中的字节总数，包括完整服务器块类型和长度字段的八个字节，加上随后的完整服务器数据中的字节数。
应用协议 ID (Application Protocol ID)	uint32	在服务器上运行的应用协议的应用 ID。
字符串块类型 (String Block Type)	uint32	启动包含应用协议供应商名称的字符串数据块。值始终为 0。

表 4-76　完整服务器信息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	供应商名称字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上供应商名称中的字节数。
供应商名称 (Vendor Name)	字符串	服务器供应商的名称。
字符串块类型 (String Block Type)	uint32	启动包含应用协议版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
版本	字符串	服务器的版本。
上次使用时间 (Last Used)	uint32	表示系统上次检测到使用中的服务器的 UNIX 时间戳。
源类型 (Source Type)	uint32	映射到数据源类型的数字： ▪ 0 如果服务器数据由 RNA 提供 ▪ 1 如果服务器数据由用户提供 ▪ 2 如果客户端数据由第三方扫描仪提供 ▪ 3 如果服务器数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
源 ID (Source ID)	uint32	映射到服务器数据源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
列表块类型 (List Block Type)	uint32	启动由传输子服务器数据的完整服务器信息数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整子服务器数据块。 此字段后面是零个或多个完整子服务器数据块。
完整子服务器块类型 (Full Sub-Server Block Type)	uint32	启动第一个完整子服务器数据块。此数据块后面可以跟随最大长度为列表块长度字段中定义的限值的其他完整子服务器数据块。
完整子服务器块长度 (Full Sub-Server Block Length)	uint32	每个完整子服务器数据块中的字节总数，包括完整子服务器块类型和长度字段的八个字节，加上随后的数据的字节数。
完整子服务器数据块 (Full Sub-Server Data Blocks) *	uint32	包含服务器的子服务器的完整子服务器数据块。有关此数据块的说明，请参阅完整子服务器数据块，第 4-81 页。

用于 4.10.0+ 的一般扫描结果数据块

一般扫描结果数据块包含扫描结果，并在扫描结果数据块 5.2+，第 4-136 页中使用。一般扫描结果数据块的块类型为系列 1 数据块组中的 108。

下图显示一般扫描结果数据块的基本结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	一般扫描结果数据块类型 (108) (Generic Scan Results Data Block Type (108))																															
	一般扫描结果块长度 (Generic Scan Results Block Length)																															
	端口																协议															
扫描结果子服务器 (Scan Result Sub-Servers)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	扫描结果子服务器字符串...(Scan Result Sub-Server String...)																															
扫描结果值	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	扫描结果值...(Scan Result Value...)																															
扫描结果子服务器 (Scan Result Sub-Server)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	扫描结果子服务器（未格式化）字符串 ...(Scan Result Sub-Server (unformatted) String...)																															
扫描结果值	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	扫描结果值...(Scan Result Value...)																															

下表对一般扫描结果数据块的字段进行了说明。

表 4-77　　一般扫描结果数据块字段

字段	字节数	说明 (Description)
一般扫描结果数据块类型 (Generic Scan Results Data Block Type)	uint32	启动一般扫描结果数据块。值始终为 108。
一般扫描结果块长度 (Generic Scan Results Block Length)	uint32	一般扫描结果数据块中的字节总数，包括一般扫描结果块类型和长度字段的八个字节，加上随后的扫描结果数据的字节数。
端口 (Port)	uint16	受结果中的漏洞影响的服务器使用的端口。
协议 (Protocol)	uint16	IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如: ▪ 6 - TCP ▪ 17 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如: ▪ 2048 - IP
字符串块类型 (String Block Type)	uint32	启动包含子服务器的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	子服务器字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上子服务器中的字节数。
扫描结果子服务器 (Scan Result Sub-Server)	字符串	子服务器。
字符串块类型 (String Block Type)	uint32	启动包含该值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	值字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上值中的字节数。
扫描结果值 (Scan Result Value)	字符串	扫描结果值。
字符串块类型 (String Block Type)	uint32	启动包含子服务器的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	子服务器字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上子服务器中的字节数。
扫描结果子服务器 (Scan Result Sub-Server)	字符串	子服务器（未格式化）。
字符串块类型 (String Block Type)	uint32	启动包含该值的字符串数据块。值始终为 0。

表 4-77 一般扫描结果数据块字段 （续）

字段	字节数	说明 (Description)
字符串块长度 (String Block Length)	uint32	值字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上值中的字节数。
扫描结果值 (Scan Result Value)	字符串	扫描结果值（未格式化）。

用于 4.10.0+ 的扫描漏洞数据块

扫描漏洞数据块对漏洞进行说明，在扫描结果数据块中使用，扫描结果数据块在添加扫描结果事件（事件类型 1002，子类型 11）中使用。有关详细信息，请参阅扫描结果数据块 5.2+，第 4-136 页和添加扫描结果消息，第 4-56 页。扫描漏洞数据块的块类型为系列 1 数据块组中的 109。

下图显示扫描漏洞数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	扫描漏洞块类型 (109) (Scan Vulnerability Block Type (109))																															
	扫描漏洞块长度 (Scan Vulnerability Block Length)																															
	端口																协议															
ID	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	ID																															
名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	漏洞名称...(Vulnerability Name...)																															
说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明... (Description...)																															
名称清除 (Name Clean)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	漏洞名称清除...(Vulnerability Name Clean...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
说明 (Description) 清洁	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明清除...(Description Clean...)																															
Bugtraq ID	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	整数数据块 (Bugtraq ID)...(Integer Data Blocks (Bugtraq IDs)...)																															
CVE ID	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	CVE ID...																															

下表对扫描漏洞数据块的字段进行了说明。

表 4-78　　扫描漏洞数据块字段

字段	数据类型	说明 (Description)
扫描漏洞块类型 (Scan Vulnerability Block Type)	uint32	启动扫描漏洞数据块。值始终为 `109`。
扫描漏洞块长度 (Scan Vulnerability Block Length)	uint32	扫描漏洞数据块中的字节数，包括扫描漏洞块类型和长度字段的八个字节，加上随后的扫描漏洞数据的字节数。
端口 (Port)	uint16	受漏洞影响的子服务器使用的端口。
协议 (Protocol)	uint16	IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如: ▪ `6` - TCP ▪ `17` - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如: ▪ `2048` - IP
字符串块类型 (String Block Type)	uint32	启动 ID 的字符串数据块。

表 4-78 扫描漏洞数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	用于 ID 的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上 ID 中的字节数。
ID	字符串	检测漏洞的扫描实用程序指定的报告漏洞的 ID。对于 Qualys 扫描检测到的漏洞，此字段表示 Qualys ID。
字符串块类型 (String Block Type)	uint32	启动漏洞名称的字符串数据块。
字符串块长度 (String Block Length)	uint32	漏洞名称字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上漏洞名称中的字节数。
名称 (Name)	字符串	漏洞的名称。
字符串块类型 (String Block Type)	uint32	启动漏洞说明的字符串数据块。
字符串块长度 (String Block Length)	uint32	漏洞说明字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上漏洞说明中的字节数。
说明 (Description)	字符串	对漏洞的说明。
字符串块类型 (String Block Type)	uint32	启动漏洞名称的字符串数据块。
字符串块长度 (String Block Length)	uint32	漏洞名称字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上漏洞名称中的字节数。
名称清除 (Name Clean)	字符串	漏洞的名称（未格式化）。
字符串块类型 (String Block Type)	uint32	启动漏洞说明的字符串数据块。
字符串块长度 (String Block Length)	uint32	漏洞说明字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上漏洞说明中的字节数。
说明清除 (Description Clean)	字符串	对漏洞的说明（未格式化）。
列表块类型 (List Block Type)	uint32	启动 Bugtraq 标识号列表的列表数据块。
列表块长度 (List Block Length)	uint32	Bugtraq 标识号列表的列表数据块中的字节数，包括字符串块类型和长度的八个字节，加上包含 Bugtraq ID 的整数数据块中的字节数。

表 4-78　扫描漏洞数据块字段 （续）

字段	数据类型	说明 (Description)
Bugtraq ID	字符串	包含零个或多个形成 Bugtraq 标识号列表的整数 (INT32) 数据块。有关这些数据块的详细信息，请参阅整数 (INT32) 数据块，第 4-73 页。
列表块类型 (List Block Type)	uint32	启动通用漏洞披露 (CVE) 标识号列表的列表数据块。
列表块长度 (List Block Length)	uint32	CVE 标识号的列表数据块中的字节数，包括字符串块类型和长度的八个字节，加上 CVE 标识号中的字节数。
CVE ID	字符串	包含零个或多个形成 CVE 标识号列表的字符串信息数据块。有关这些数据块的详细信息，请参阅字符串信息数据块，第 4-75 页。

完整主机客户端应用数据块 5.0+

用于版本 5.0+ 的完整主机客户端应用数据块对客户端应用以及附加关联 Web 应用和漏洞列表进行说明。完整主机客户端应用数据块在完整主机配置文件数据块（类型 111）中使用。其块类型为系列 1 数据块组中的 112。

下图显示用于 5.0+ 的完整主机客户端应用数据块的基本结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	完整主机客户端应用块类型 (112) (Full Host Client Application Block Type (112))																															
	完整主机客户端应用块长度 (Full Host Client Application Block																															
	命中数 (Hits)																															
	上次使用时间 (Last Used)																															
	应用 ID (Application ID)																															
版本	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	版本...(Version...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
Web 应用程序 (Web Application)	Web 应用块类型 (123) (Web Application Block Type (123))*																															
	Web 应用块长度 (Web Application Block Length)																															
	Web 应用数据...(Web Application Data...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
漏洞	漏洞块类型 (85) (Vulnerability Block Type (85))*																															
	漏洞块长度 (Vulnerability Block Length)																															
	漏洞数据...(Vulnerability Data...)																															

下表对完整主机客户端应用数据块的字段进行了说明。

表 4-79 完整主机客户端应用数据块 5.0+ 字段

字段	数据类型	说明 (Description)
完整主机客户端应用块类型 (Full Host Client Application Block Type)	uint32	启动完整主机客户端应用数据块。值始终为 112。
完整主机客户端应用块长度 (Full Host Client Application Block Length)	uint32	完整主机客户端应用数据块中的字节数，包括客户端应用块类型和长度的八个字节，加上随后的客户端应用数据中的字节数。
命中数 (Hits)	uint32	系统检测到在使用的客户端应用的次数。
上次使用时间 (Last Used)	uint32	表示系统上次检测到使用中的客户端的 UNIX 时间戳。
应用 ID (Application ID)	uint32	被检测客户端应用的应用 ID（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用名称的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上客户端应用版本中的字节数。
版本	字符串	客户端应用版本。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装 Web 应用数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
Web 应用数据块 (Web Application Data	变量	封装 Web 应用数据块数最多可以是通用列表块长度中的最大字节数。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。

表 4-79　　完整主机客户端应用数据块 5.0+ 字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装漏洞数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装漏洞数据块中的字节数。
漏洞数据块 (Vulnerability Data Blocks)	变量	封装漏洞数据块数最多可以是通用列表块长度中的最大字节数。

用于 5.0+ 的主机客户端应用数据块

用于 5.0+ 的主机客户端应用数据块对客户端应用进行说明，并在新客户端应用事件（事件类型 1000，子类型 7）、客户端应用超时事件（事件类型 1001子类型 20）以及客户端应用更新事件（事件类型 1001，子类型 32）中使用。用于 4.10.2+ 的主机客户端应用数据块的块类型为系列 1 数据块组中的 122。

下图显示用于 5.0+ 的主机客户端应用数据块的基本结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	主机客户端应用块类型 (122) (Host Client Application Block Type (122))																															
	主机客户端应用块长度 (Host Client Application Block Length)																															
	命中数 (Hits)																															
	上次使用时间 (Last Used)																															
	ID																															
	应用协议 ID (Application Protocol ID)																															
版本	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	版本...(Version...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
Web 应用程序 (Web Application)	Web 应用块类型 (123) (Web Application Block Type (123))*																															
	Web 应用块长度 (Web Application Block Length)																															
	Web 应用数据...(Web Application Data...)																															

下表对主机客户端应用数据块的字段进行了说明。

表 4-80 主机客户端应用数据块字段

字段	数据类型	说明 (Description)
客户端应用块类型 (Client Application Block Type)	uint32	启动主机客户端应用数据块。值始终为 122。
客户端应用块长度 (Client Application Block Length)	uint32	客户端应用数据块中的字节数，包括客户端应用块类型和长度的八个字节，加上随后的客户端应用数据中的字节数。
命中数 (Hits)	uint32	系统检测到在使用的客户端应用的次数。
上次使用时间 (Last Used)	uint32	表示系统上次检测到使用中的客户端的 UNIX 时间戳。
ID	uint32	被检测客户端应用的标识号（如适用）。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上客户端应用版本中的字节数。
版本	字符串	客户端应用版本。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装 Web 应用数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
Web 应用数据块 (Web Application Data	变量	封装 Web 应用数据块数最多可以是列表块长度中的最大字节数。请参阅用于 5.0+ 的 Web 应用数据块，第 4-115 页了解有关封装数据块的信息（块类型 123）。

用户漏洞数据块 5.0+

用户漏洞数据块对漏洞进行说明，并在用户漏洞更改数据块中使用。用户漏洞更改数据块在用户设置有效漏洞事件和用户设置无效漏洞事件中使用。用于 5.0+ 的用户漏洞数据块的块类型为系列 1 数据块组中的 124。它替代块类型有关用户漏洞更改数据块的详细信息，请参阅用户漏洞更改数据块 4.7+，第 4-105 页。

下图显示用户漏洞数据块的格式:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户漏洞块类型 (124) (User Vulnerability Block Type (124))																															
	用户漏洞块长度 (User Vulnerability Block Length)																															
IP 范围规格块 (IP Range Spec Blocks)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IP 范围规格数据块...(IP Range Specification Data Blocks...)*																															
	端口																协议															
	漏洞 ID (Vulnerability ID)																															
第三方漏洞 UUID	第三方漏洞 UUID (Third-Party Vulnerability UUID)																															
	UUID（续）																															
	UUID（续）																															
	UUID（续）																															
	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	漏洞字符串...(Vulnerability String...)																															
	客户端应用 ID (Client Application ID)																															
	应用协议 ID (Application Protocol ID)																															
	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	版本字符串...(Version String...)																															

下表对用户漏洞数据块的字段进行了说明。

表 4-81 用户漏洞数据块字段

字段	数据类型	说明 (Description)
用户漏洞块类型 (User Vulnerability Block Type)	uint32	启动用户漏洞数据块。值始终为 124。
用户漏洞块长度 (User Vulnerability Block Length)	uint32	用户漏洞数据块中的字节数，包括用户漏洞块类型和长度字段的八个字节，加上随后的用户漏洞数据的字节数。
通用列表块类型 (Generic List Block	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	用户输入的 IP 地址范围。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-93 页。
端口 (Port)	uint16	受漏洞影响的服务器使用的端口。对于客户端应用漏洞，值为 0。
协议 (Protocol)	uint16	受漏洞影响的服务器使用的协议的 IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如： ▪ 6 - TCP ▪ 17 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如： ▪ 2048 - IP 对于客户端应用漏洞，值为 0。
漏洞 ID (Vulnerability ID)	uint32	思科漏洞 ID。
第三方漏洞 UUID (Third-Party Vulnerability UUID)	uint8 [16]	第三方漏洞的唯一 ID 号码（如果存在）。否则，该值为 0。
字符串块类型 (String Block Type)	uint32	启动漏洞名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	漏洞名称字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上漏洞名称中的字节数。

表 4-81　　用户漏洞数据块字段 （续）

字段	数据类型	说明 (Description)
漏洞名称 (Vulnerability Name)	字符串	漏洞名称。
客户端应用 ID (Client Application ID)	uint32	客户端应用的应用 ID。对于服务器漏洞，值为 0。
应用协议 ID (Application Protocol ID)	uint32	客户端应用使用的应用协议的应用 ID。对于服务器漏洞，值为 0。
字符串块类型 (String Block Type)	uint32	启动版本字符串的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	版本字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上客户端应用版本字符串中的字节数。
版本	字符串	客户端应用版本。对于服务器漏洞，值为 0。

操作系统指纹数据块 5.1+

操作系统指纹数据块的块类型为系列 1 数据块组中的 130。块包括指纹通用唯一标识符 (UUID) 以及指纹类型、指纹源类型和指纹源 ID。

下图显示 5.1+ 中操作系统指纹数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
操作系统指纹 UUID	指纹 UUID (Fingerprint UUID)																															
	指纹 UUID (Fingerprint UUID) （续）																															
	指纹 UUID (Fingerprint UUID) （续）																															
	指纹 UUID (Fingerprint UUID) （续）																															
	指纹类型 (Fingerprint Type)																															
	指纹源类型 (Fingerprint Source Type)																															
	指纹源 ID (Fingerprint Source ID)																															
	上次查看时间 (Last Seen)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
移动设备信息	TTL 差值 (TTL Difference)								通用列表块类型 (31) (Generic List Block Type (31))																							
	通用列表块类型 (Generic List Block Type)（续）								通用列表块长度 (Generic List Block Length)																							
	通用列表块长度 (Generic List Block Length)（续）								移动设备信息数据块 (Mobile 设备 Information Data Blocks)*																							

下表对操作系统指纹数据块的字段进行了说明。

表 4-82 操作系统指纹数据块字段

字段	数据类型	说明 (Description)
操作系统指纹数据块类型 (Operating System Fingerprint Data Block Type)	uint32	启动操作系统数据块。值始终为 130。
操作系统数据块长度 (Operating System Data Block Length)	uint32	操作系统指纹数据块中的字节数，包括操作系统指纹数据块块类型和长度的八个字节，加上随后的操作系统指纹数据中的字节数。
指纹 UUID (Fingerprint UUID)	uint8[16]	采用八位组的指纹识别号，用作操作系统的唯一标识符。指纹 UUID 映射到漏洞数据库 (VDB) 中的操作系统名称、供应商和版本。
指纹类型 (Fingerprint Type)	uint32	表示指纹的类型。
指纹源类型 (Fingerprint Source Type)	uint32	表示提供操作系统指纹的源的类型（即用户或扫描仪）。
指纹源 ID (Fingerprint Source ID)	uint32	映射到提供操作系统指纹的用户的登录名称的标识号。
上次查看时间 (Last Seen)	uint32	表示上次在流量中看到指纹的时间。
TTL 差值 (TTL Difference)	uint8	表示指纹中的 TTL 值与在用于采集主机指纹的数据包中看到的 TTL 值之间的差值。
通用列表块类型 (Generic List Block	uint32	启动通用列表数据块。值始终为 31。

表 4-82　操作系统指纹数据块字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
移动设备信息数据块 (Mobile Device Information Data Blocks)	变量	封装移动设备信息数据块数最多可以是列表块长度中的最大字节数。有关此数据块的说明，请参阅用于 5.1+ 的移动设备 信息数据块，第 4-163 页。

用于 5.1+ 的移动设备 信息数据块

下图显示移动设备信息数据块的格式。该数据块包含上次到检测主机的时间、移动设备信息以及移动设备是否已越狱。移动设备信息数据块的块类型为系列 1 数据块组中的 131。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	移动设备信息块类型 (131) (Mobile Device Information Block Type (131))																															
	移动设备信息块长度 (Mobile Device Information Block Length)																															
移动设备数据	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	移动设备字符串数据...(Mobile Device String Data...)																															
	移动设备上次查看时间 (Mobile 设备 Last Seen)																															
	移动 (Mobile)																															
	Jailbroken																															

下表对 5.1+ 返回的移动设备信息数据块的字段进行了说明。

表 4-83　移动设备信息数据块 5.1+ 字段

字段	数据类型	说明 (Description)
移动设备信息块类型 (131) (Mobile Device Information Block Type (131))	uint32	启动操作系统数据块。值始终为 `131`。
移动设备信息块长度 (Mobile Device Information Block Length)	uint32	移动设备信息数据块中的字节数，包括移动设备信息数据块块类型和长度的八个字节，加上随后的移动设备信息数据中的字节数。

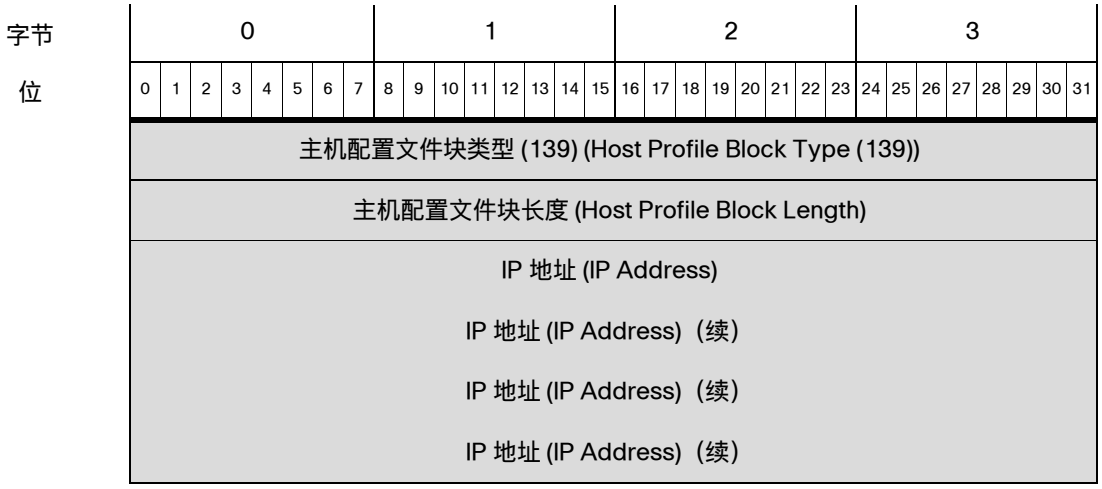
表 4-83 移动设备信息数据块 5.1+ 字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动移动设备字符串的字符串数据块。此值设置为 0 以表示字符串数据。
字符串块长度 (String Block Length)	uint32	移动设备字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上随后的移动设备字符串数据中的字节数。
移动设备字符串数据 (Mobile Device String Data)	变量	包含检测到的主机的移动设备硬件信息。
移动设备上次查看时间 (Mobile 设备 Last Seen)	uint32	包含上次查看移动设备的时间戳。
移动 (Mobile)	uint32	指示主机是否为移动设备的一个真假标志。
Jailbroken	uint32	指示主机是否为已被越狱的移动设备的一个真假标志。

用于 5.2+ 的主机配置文件数据块

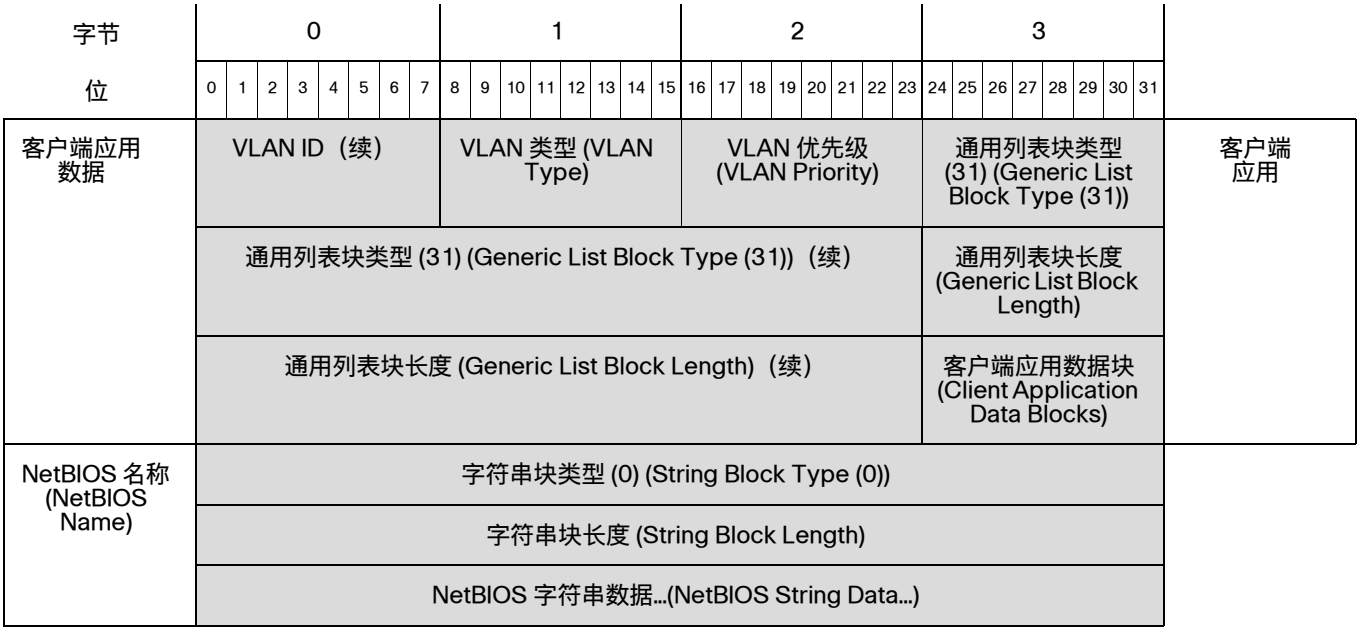
下图显示主机配置文件数据块的格式。该数据块也不包含主机临界值，但包含 VLAN 在线状态指示器。此外，数据块还可以传输主机的 NetBIOS 名称。主机配置文件数据块的块类型为系列 1 数据块组中的 139。数据块现在支持 IPv6 地址，且已添加客户端应用数据块。

注释 下图中块类型字段旁边的星号 (*) 表示该消息可能包含零个或多个系列 1 数据块实例。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
服务器指纹 (Server Fingerprints)	跳数 (Hops)								主要/次要 (Primary/ Secondary)								通用列表块类型 (31) (Generic List Block Type (31))															
	通用列表块类型 (Generic List Block Type) (续)																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length) (续)																服务器指纹数据块 (Server Fingerprint Data Blocks)*															
客户端指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	客户端指纹数据块 (Client Fingerprint Data Blocks)*																															
中小企业指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	SMB 指纹数据块 (SMB Fingerprint Data Blocks)*																															
DHCP 指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	DHCP 指纹数据块 (DHCP Fingerprint Data Blocks)*																															
移动设备指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	移动设备指纹数据块 (Mobile Device Fingerprint Data Blocks)*																															
IPv6 服务器指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	Ipv6 服务器指纹数据块 (Ipv6 Server Fingerprint Data Blocks)*																															
IPv6 客户端指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IPv6 客户端指纹数据块 (Ipv6 Client Fingerprint Data Blocks)*																															
IPv6 DHCP 指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IPv6 DHCP 指纹数据块 (Ipv6 DHCP Fingerprint Data Blocks)*																															

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
用户代理指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																																
	通用列表块长度 (Generic List Block Length)																																
	用户代理指纹数据块 (User Agent Fingerprint Data Blocks)*																																
TCP 服务器块*	列表块类型 (11) (List Block Type (11))																																TCP 服务器
	列表块长度 (List Block Length)																																
	TCP 服务器数据块 (TCP Server Data Blocks)																																
UDP 服务器块*	列表块类型 (11) (List Block Type (11))																																UDP 服务器
	列表块长度 (List Block Length)																																
	UDP 服务器数据块 (UDP Server Data Blocks)																																
网络协议数据块 (Network Protocol Block)*	列表块类型 (11) (List Block Type (11))																																网络协议 (Protocol)
	列表块长度 (List Block Length)																																
	网络协议数据块 (Network Protocol Data Blocks)																																
传输协议数据块 (Transport Protocol Block)*	列表块类型 (11) (List Block Type (11))																																传输协议 (Protocol)
	列表块长度 (List Block Length)																																
	传输协议数据块 (Transport Protocol Data Blocks)																																
MAC 地址块 (MAC Address Block)*	列表块类型 (11) (List Block Type (11))																																MAC 地址
	列表块长度 (List Block Length)																																
	主机 MAC 地址数据块 (Host MAC Address Data Blocks)																																
	主机上次查看时间 (Host Last Seen)																																
	主机类型 (Host Type)																																
	移动 (Mobile)								Jailbroken								VLAN 在线状态 (VLAN Presence)								VLAN ID							



下表对 5.2+ 返回的主机配置文件数据块的字段进行了说明。

表 4-84　　主机配置文件数据块 5.2+ 字段

字段	数据类型	说明 (Description)
主机配置文件块类型 (Host Profile Block Type)	uint32	启动用于 5.2+ 的主机配置文件数据块。值始终为 139。
主机配置文件块长度 (Host Profile Block Length)	uint32	主机配置文件数据块中的字节数，包括主机配置文件块类型和长度字段的八个字节，加上随后的主机配置文件数据中的字节数。
IP 地址 (IP Address)	uint8(16)	主机的 IP 地址。可能是 IPv4 或 IPv6。
跳数 (Hops)	uint8	从主机到设备的跳数。
主/辅助 (Primary/Secondary)	uint8	表示主机是位于检测到其的设备的主网络中还是辅助网络中： ▪ 0 - 主机位于主网络中。 ▪ 1 - 主机位于辅助网络中。
通用列表块类型 (Generic List Block	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 4-84 主机配置文件数据块 5.2+ 字段 （续）

字段	数据类型	说明 (Description)
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 SMB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（SMB指纹）数据块(Operating System Fingerprint (SMB Fingerprint) Data Blocks) *	变量	包含用 SMB 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 4-84　主机配置文件数据块 5.2+ 字段 （续）

字段	数据类型	说明 (Description)
操作系统指纹（DHCP 指纹）数据块 (Operating System Fingerprint (DHCP Fingerprint) Data Blocks) *	变量	包含用 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用移动设备指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（移动）数据块 (Operating System Fingerprint (Mobile) Data Blocks) *	变量	包含用移动设备指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 IPv6 服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（IPv6 服务器）数据块 (Operating System Fingerprint (IPv6 Server) Data Blocks) *	变量	包含用 IPv6 服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 IPv6 客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 4-84 主机配置文件数据块 5.2+ 字段 （续）

字段	数据类型	说明 (Description)
操作系统指纹（IPv6 客户端）数据块 (Operating System Fingerprint (IPv6 Client) Data Blocks) *	变量	包含用 IPv6 客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 IPv6 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（IPv6 DHCP 指纹）数据块 (Operating System Fingerprint (IPv6 DHCP Fingerprint) Data Blocks) *	变量	包含用 IPv6 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用用户代理指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（用户代理指纹）数据块 (Operating System Fingerprint (User Agent Fingerprint) Data Blocks) *	变量	包含用用户代理指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
TCP 服务器数据块 (TCP Server Data Blocks)	变量	描述 TCP 服务器的主机服务器数据块。有关此数据块的说明，请参阅主机服务器数据块 4.10.0+，第 4-139 页。

表 4-84　主机配置文件数据块 5.2+ 字段 （续）

字段	数据类型	说明 (Description)
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
UDP 服务器数据块 (UDP Server Data Blocks)	uint32	描述 UDP 服务器的主机服务器数据块。有关此数据块的说明，请参阅主机服务器数据块 4.10.0+，第 4-139 页。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个协议数据块。
网络协议数据块 (Network Protocol Data Blocks)	uint32	描述网络协议的协议数据块。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个传输协议数据块。
传输协议数据块 (Transport Protocol Data Blocks)	uint32	描述传输协议的协议数据块。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动由 MAC 地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks)	uint32	描述主机 MAC 地址的主机 MAC 地址数据块。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-113 页。
主机上次查看时间 (Host Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。

表 4-84 主机配置文件数据块 5.2+ 字段 （续）

字段	数据类型	说明 (Description)
主机类型 (Host Type)	uint32	表示主机类型。可能会出现以下值: ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥 ▪ 3 - NAT 设备 ▪ 4 - LB（负载均衡器）
移动 (Mobile)	uint8	指示主机是否为移动设备的一个真假标志。
Jailbroken	uint8	指示主机是否同样为已被越狱的移动设备的一个真假标志。
VLAN 在线状态 (VLAN Presence)	uint8	表示是否存在 VLAN: ▪ 0 - 是 ▪ 1 - 否
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
字符串块类型 (String Block Type)	uint32	启动主机客户端应用数据的字符串数据块。值始终为 112。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上主机客户端应用数据中的字节数。
主机客户端应用数据块 (Host Client Application Data Blocks)	变量	客户端应用数据块列表。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-155 页。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。

用户产品数据块 5.1+

用户产品数据块传输从第三方应用导入的主机输入数据，包括第三方应用字符串映射。此数据块在扫描结果数据块 5.2+，第 4-136 页和用户服务器和操作系统消息，第 4-55 页中使用。在版本 4.7 - 4.10.1 中，用户产品数据块的块类型为系列 1 数据块组中的 65；在版本 4.10.2 - 5.0.x 中，块类型为 118；在版本 5.1+ 中，块类型为系列 1 数据块组中的 134。块类型 65 与 118 的结构相同。

注释　下图中数据块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示用户产品数据块的格式:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户产品数据块类型 (134) (User Product Data Block Type (134))																															
	用户产品块长度 (User Product Block Length)																															
	源 ID (Source ID)																															
	源类型 (Source Type)																															
IP 地址 (IP Addresses) 范围	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IP 范围规格数据块 (IP Range Specification Data Blocks)*																															
	端口																协议															
	丢弃用户产品 (Drop User Product)																															
自定义供应商字符串 (Custom Vendor String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	自定义供应商字符串...(Custom Vendor String...)																															
自定义产品字符串 (Custom Product String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	自定义产品字符串...(Custom Product String...)																															
自定义版本字符串 (Custom Version String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	自定义版本字符串...(Custom Version String...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	软件 ID (Software ID)																															
	服务器 ID (Server ID)																															
	供应商 ID (Vendor ID)																															
	产品 ID (Product ID)																															
主版本 (Major Version) 字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	主版本字符串...(Major Version String...)																															
次版本 (Minor Version) 字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	次版本字符串...(Minor Version String...)																															
修订版 (Revision) 字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	修订版字符串...(Revision String...)																															
至主版本字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	至主版本字符串...(To Major Version String...)																															
至次版本字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	至次版本字符串...(To Minor Version String...)																															
至修订版字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	至修订版字符串...(To Revision String...)																															
内部版本字符串 (Build String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	内部版本字符串...(Build String...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
修补版本字符串 (Patch String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	修补版本字符串...(Patch String...)																															
分机 (Extension) 字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	扩展版本字符串...(Extension String...)																															
操作系统 UUID (OS UUID)	操作系统 UUID (Operating System UUID)																															
	操作系统 UUID (Operating System UUID)（续）																															
	操作系统 UUID (Operating System UUID)（续）																															
	操作系统 UUID (Operating System UUID)（续）																															
设备字符串 (Device String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	设备字符串...(Device String...)																															
修复列表 (List of Fixes)	移动 (Mobile)								Jailbroken								通用列表块类型 (31) (Generic List Block Type (31))															
	通用列表块类型 (31) (Generic List Block Type (31))（续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length)（续）																修复列表数据块 (Fix List Data Blocks)*															
	修复列表数据块 (Fix List Data Blocks)*（续）																															

下表对用户产品数据块的组件进行了说明。

表 4-85　　用户产品数据块字段

字段	数据类型	说明 (Description)
用户产品数据块类型 (User Product Data Block Type)	uint32	启动用户产品数据块。在版本 5.1+ 中，此值为 134。
用户产品块长度 (User Product Block Length)	uint32	用户产品数据块中的字节总数，包括用户产品块类型和长度字段的八个字节，加上随后的用户产品数据中的字节数。

表 4-85 用户产品数据块字段 （续）

字段	数据类型	说明 (Description)
源 ID (Source ID)	uint32	映射到导入数据的源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
源类型 (Source Type)	uint32	映射到数据源类型的数字： ▪ 0 如果数据由 RNA 提供 ▪ 1 如果数据由用户提供 ▪ 2 如果数据由第三方扫描仪提供 ▪ 3 如果数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
通用列表块类型 (Generic List Block	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-93 页。
端口 (Port)	uint16	用户指定的端口。
协议 (Protocol)	uint16	IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如： ▪ 6 - TCP ▪ 17 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如： ▪ 2048 - IP
丢弃用户产品 (Drop User Product)	uint32	表示是否已从主机中删除用户操作系统定义： ▪ 0 - 否 ▪ 1 - 是
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义供应商名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	自定义供应商字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上供应商名称中的字节数。
自定义供应商名称 (Custom Vendor Name)	字符串	在用户输入中指定的自定义供应商名称。

表 4-85　　用户产品数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义产品名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	自定义产品字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上产品名称中的字节数。
自定义产品名称 (Custom Product Name)	字符串	在用户输入中指定的自定义产品名称。
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	自定义版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
自定义版本 (Custom Version)	字符串	在用户输入中指定的自定义版本。
软件 ID (Software ID)	uint32	数据库中服务器或操作系统特定修订版的标识符。
服务器 ID (Server ID)	uint32	在用户输入中指定的主机服务器上的应用协议的 Cisco Secure Firewall 系统应用标识符。
供应商 ID (Vendor ID)	uint32	在第三方操作系统映射到 Cisco Secure Firewall 系统 操作系统定义时指定的第三方操作系统的供应商的标识符。
产品 ID (Product ID)	uint32	在第三方操作系统字符串映射到 Cisco Secure Firewall 系统操作系统定义时指定的第三方操作系统字符串的产品标识字符串。
字符串块类型 (String Block Type)	uint32	启动包含用户输入中的第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统定义的主版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	主版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
主版本 (Major Version)	字符串	第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统定义的主版本。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统定义的次版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	次版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
次版本 (Minor Version)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统定义的次版本号。

表 4-85 用户产品数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含用户输入中的第三方操作系统字符串映射到的 Cisco Secure Firewall 系统 操作系统定义的修订号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	修订版字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修订号中的字节数。
修订版 (Revision)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统定义的修订号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco Secure Firewall 系统 操作系统定义的最新主版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至主版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
至主版本 (To Major)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco Secure Firewall 系统 操作系统定义的一系列主版本号中的最新版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco Secure Firewall 系统 操作系统定义的最新次版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至次版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
至次版本 (To Minor)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco Secure Firewall 系统 操作系统定义的一系列次版本号中的最新版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统定义的最新修订号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至修订版字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修订号中的字节数。
至修订版 (To Revision)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统定义的一系列修订号中的最新修订号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统的内部版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	内部版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上内部版本号中的字节数。
内部版本 (Build)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统的内部版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统的修补版本号的字符串数据块。值始终为 0。

表 4-85　用户产品数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	修补版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修补版本号中的字节数。
修补 (Patch)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统的修补版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统的扩展版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	扩展版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上扩展版本号中的字节数。
分机 (Extension)	字符串	用户输入中的第三方操作系统字符串映射到的 Cisco Secure Firewall 系统操作系统的扩展版本号。
UUID	uint8 [x16]	包含操作系统的唯一标识号。
字符串块类型 (String Block Type)	uint32	启动包含用户输入中设备硬件信息的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	内部版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上内部版本号中的字节数。
设备字符串 (Device String)	字符串	移动设备硬件信息。
移动 (Mobile)	uint8	指示操作系统是否在移动设备上运行的一个真假标志。
Jailbroken	uint8	指示移动设备操作系统是否被越狱的一个真假标志。
通用列表块类型 (Generic List Block	uint32	启动由传送有关应用到特定 IP 地址范围中指定主机的修复的用户输入数据的修复列表数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装修复列表数据块。
修复列表数据块 (Fix List Data Blocks) *	变量	包含应用到主机的修复的相关信息的修复列表数据块。有关此数据块的说明，请参阅修复列表数据块，第 4-100 页。

用户数据块

用户数据块在用户事件消息中出现。它们是系列 1 数据块的子集。有关系列 1 数据块的通用格式的信息，请参阅了解发现（系列 1）块，第 4-60 页。

注释 用户数据块报头的数据块长度字段包含该数据块中的字节数，包括两个数据块报头字段的八个字节。

下表列出了可能在用户事件消息中出现的用户数据块。数据块按数据块类型列出。当前版本数据块是最新版本。当前版本的 Cisco Secure Firewall 系统支持旧数据块，但不产生旧数据块。

表 4-86　用户数据块类型

类型 (Type)	内容	数据块类别	说明 (Description)
73	用户登录信息	传统	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用于 5.0 - 5.0.2 的用户登录信息数据块，第 B-135 页。5.0 中引入的后继块类型的结构与块类型 73 的结构相同，但字段中的数据不同。
74	用户帐户更新消息	当前	包含用户帐户信息中的更改。有关详细信息，请参阅用户帐户更新消息数据块，第 4-181 页。
75	用于 4.7 - 4.10.x 的用户信息	传统	包含系统检测到的用户信息中的更改。有关详细信息，请参阅用于 5.x 的用户信息数据块，第 B-150 页。版本 6.0 中引入的后继块的块类型为 158。
120	用于 5.x 的用户信息	当前	包含系统检测到的用户信息中的更改。有关详细信息，请参阅用于 5.x 的用户信息数据块，第 B-150 页。替代块类型 75。它被块类型 158 替代。
121	用户登录信息	传统	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用于 5.0 - 5.0.2 的用户登录信息数据块，第 B-135 页。与块 73 的不同在于“协议”(Protocol) 字段的内容，该字段存储在事件中检测到的应用协议 ID 的版本 5.0+ 应用 ID。版本 5.1 中引入的后继块的块类型为 127。
127	用户登录信息	传统	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用户登录信息数据块 5.1 - 5.4.x，第 B-137 页。它替代块类型 121。版本 6.0 中引入的后继块的块类型为 159。
150	IOC 状态	当前	包含有关危害的信息。有关详细信息，请参阅用于 5.3+ 的 IOC 状态数据块，第 4-33 页。
158	用于 6.0+ 的用户信息	当前	包含系统检测到的用户信息中的更改。有关详细信息，请参阅用于 6.0+ 的用户信息数据块，第 4-191 页。替代块类型 120。
159	用户登录信息	传统	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用户登录信息数据块 6.0.x，第 B-140 页。它替代块类型 127。

表 4-86　用户数据块类型 （续）

类型 (Type)	内容	数据块类别	说明 (Description)
165	用户登录信息	传统模式	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用户登录信息数据块 6.1.x，第 B-147 页。它替代块类型 159。 它被块类型 167 替代。
166	VPN 会话信息	当前	包含系统检测到的有关 VPN 会话的信息。有关详细信息，请参阅用于 6.2+ 的 VPN 会话数据块，第 4-194 页。
167	用户登录信息	当前	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用户登录信息数据块 6.2+，第 4-197 页。它替代块类型 165。

用户帐户更新消息数据块

用户帐户更新消息数据块传输对用户帐户信息的更新相关信息。

用户帐户更新消息数据块的块类型为系列 1 数据块组中的 74。

下图显示用户帐户更新消息数据块的格式:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户帐户更新消息块类型 (74) (User Account Update Message Block Type (74))																															
	用户帐户更新消息块长度 (User Account Update Message Block Length)																															
用户名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名...(User Name...)																															
第一页名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名字...(First Name...)																															
中间首字母缩写	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	中间名首字母缩写...(Middle Initials...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
最后一页名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	姓氏...(Last Name...)																															
全称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	全名...(Full Name...)																															
职位 (Title)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	职位...(Title...)																															
员工身份	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	员工身份...(Staff Identity...)																															
地址 (Address)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	地址...(Address...)																															
城市 (City)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	城市...(City...)																															
省/自治区 (State)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	省/自治区...(State...)																															
国家/地区	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	国家/地区...(Country/Region...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
邮政编码 (Postal Code)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	邮政编码...(Postal Code...)																															
建筑 (Building)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	建筑...(Building...)																															
位置 (Location)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	位置...(Location...)																															
会议室 (Room)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	室...(Room...)																															
公司 (Company)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	公司...(Company...)																															
部门 (Division)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	分部...(Division...)																															
部门 (Dept)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	部门...(Department...)																															
办公室 (Office)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	办公室...(Office...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Mailstop	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	Mailstop...																															
电子邮件 (Email)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件...(Email...)																															
电话	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电话...(Phone...)																															
IP 电话	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	IP 电话...(IP Phone...)																															
用户 1 (User 1)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 1...(User 1...)																															
用户 2	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 2...(User 2...)																															
用户 3	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 3...(User 3...)																															
用户 4	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 4...(User 4...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
邮件别名 1 (Email Alias 1)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	邮件别名 1...(Email Alias 1...)																															
邮件别名 2 (Email Alias 2)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	邮件别名 2...(Email Alias 2...)																															
邮件别名 3 (Email Alias 3)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	邮件别名 3...(Email Alias 3...)																															

下表对用户帐户更新信息数据块的组件进行了说明。

表 4-87　　用户帐户更新消息数据块字段

字段	数据类型	说明 (Description)
用户帐户更新消息块类型 (User Account Update Message Block Type)	uint32	启动用户帐户更新消息数据块。值始终为 74。
用户帐户更新消息块长度 (User Account Update Message Block Length)	uint32	用户帐户更新消息数据块中的字节总数，包括用户帐户更新消息块类型和长度字段的八个字节，加上随后的用户帐户更新消息数据中的字节数。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
字符串块类型 (String Block Type)	uint32	启动包含用户的名字的字符串数据块。值始终为 0。

表 4-87 用户帐户更新消息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	名字字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上名字中的字节数。
名字 (First Name)	字符串	用户的名字。
字符串块类型 (String Block Type)	uint32	启动包含用户的中间名首字母缩写的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	中间名首字母缩写字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上中间名首字母缩写中的字节数。
中间名首字母缩写 (Middle Initials)	字符串	用户的中间名首字母缩写。
字符串块类型 (String Block Type)	uint32	启动包含用户的姓氏的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	姓氏字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上姓氏中的字节数。
姓氏	字符串	用户的姓氏。
字符串块类型 (String Block Type)	uint32	启动包含用户的全名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	全名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上全名中的字节数。
全称 (Full Name)	字符串	用户的全名。
字符串块类型 (String Block Type)	uint32	启动包含用户的职位的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	职位字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上职位中的字节数。
职位	字符串	用户的职位。
字符串块类型 (String Block Type)	uint32	启动包含用户的员工标识的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	员工身份字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上员工身份中的字节数。

表 4-87　用户帐户更新消息数据块字段 （续）

字段	数据类型	说明 (Description)
员工身份 (Staff Identity)	字符串	用户的员工身份。
字符串块类型 (String Block Type)	uint32	启动包含用户的地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上地址中的字节数。
地址	字符串	用户的地址。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的城市的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	城市字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上城市中的字节数。
城市	字符串	用户地址中的城市。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的省/自治区的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	省/自治区字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上省/自治区中的字节数。
省/自治区 (State)	字符串	用户所在的省/自治区。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的国家或地区的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	国家或地区字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上国家或地区中的字节数。
国家或地区 (Country or Region)	字符串	用户地址中的国家或地区。
字符串块类型 (String Block Type)	uint32	启动包含用户地址的邮政编码的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮政编码字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮政编码中的字节数。
邮政编码	字符串	用户地址的邮政编码。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的建筑的字符串数据块。值始终为 0。

表 4-87 用户帐户更新消息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	建筑字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上建筑名称中的字节数。
建筑	字符串	用户地址中的建筑。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的位置的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	位置字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上位置名称中的字节数。
位置 (Location)	字符串	用户地址中的位置。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的室的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	室字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上室中的字节数。
会议室	字符串	用户地址中的室。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的公司的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	公司字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上公司名称中的字节数。
公司	字符串	用户地址中的公司。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的分部的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	分部字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上分部名称中的字节数。
部门	字符串	用户地址中的分部。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的部门的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	部门字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上部门中的字节数。
部门	字符串	用户地址中的部门。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的办公室的字符串数据块。值始终为 0。

表 4-87　　用户帐户更新消息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	办公室字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上办公室中的字节数。
办公室	字符串	用户地址中的办公室。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的 mailstop 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	Mailstop 字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上 mailstop 中的字节数。
Mailstop	字符串	用户地址中的 mailstop。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
字符串块类型 (String Block Type)	uint32	启动包含用户的电话号码的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电话号码字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电话号码中的字节数。
电话	字符串	用户的电话号码。
字符串块类型 (String Block Type)	uint32	启动包含用户的网络电话号码的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	网络电话号码字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上网络电话号码中的字节数。
网络电话 (Internet Phone)	字符串	用户的网络电话号码。
字符串块类型 (String Block Type)	uint32	启动包含用户的替代用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户 1	字符串	用户的替代用户名。

表 4-87 用户帐户更新消息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含用户的替代用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户 2	字符串	用户的替代用户名。
字符串块类型 (String Block Type)	uint32	启动包含用户的替代用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户 3	字符串	用户的替代用户名。
字符串块类型 (String Block Type)	uint32	启动包含用户的替代用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户 4	字符串	用户的替代用户名。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件别名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件别名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件别名中的字节数。
邮件别名 1 (Email alias 1)	字符串	用户的邮件别名。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件别名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件别名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件别名中的字节数。
邮件别名 2 (Email alias 2)	字符串	用户的邮件别名。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件别名的字符串数据块。值始终为 0。

表 4-87　用户帐户更新消息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	邮件别名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件别名中的字节数。
邮件别名 3 (Email alias 3)	字符串	用户的邮件别名。

用于 6.0+ 的用户信息数据块

用户信息数据块在用户修改消息中使用，传送检测到、删除或丢弃的用户的信息。有关详细信息，请参阅用户修改消息，第 4-58 页

在版本 6.0+ 中，用户信息数据块的块类型为系列 1 数据块组中的 158。它具有新终端配置文件、安全情报和 IPv6 字段。

在版本 4.7-4.10.x 中，用户信息数据块的块类型为系列 1 数据块组中的 75，在版本 5.x 中，块类型为系列 1 数据块组中的 120。有关详细信息，请参阅用于 5.x 的用户信息数据块，第 B-150 页。

下图显示用户信息数据块的格式。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户信息块类型 (158) (User Information Block Type (158))																															
	用户信息块长度 (User Information Block Length)																															
	用户 ID																															
用户名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名...(User Name...)																															
	领域 ID (Realm ID)																															
	协议 (Protocol)																															
第一页名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名字...(First Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
最后一页名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	姓氏...(Last Name...)																															
电子邮件 (Email)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件...(Email...)																															
部门	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	部门...(Department...)																															
电话	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电话...(Phone...)																															
	终端配置文件 ID (Endpoint Profile ID)																															
	安全组 ID (Security Group ID)																															
	位置 IPv6 地址 (Location IPv6 Address)																															
	位置 IPv6 地址 (Location IPv6 Address)（续）																															
	位置 IPv6 地址 (Location IPv6 Address)（续）																															
	位置 IPv6 地址 (Location IPv6 Address)（续）																															

下表对用户信息数据块的组件进行了说明。

表 4-88 用户信息数据块字段

字段	数据类型	说明 (Description)
用户信息块类型 (User Information Block Type)	uint32	启动用户信息数据块。值为 158。
用户信息块长度 (User Information Block Length)	uint32	用户信息数据块中的字节总数，包括用户信息块类型和长度字段的八个字节，加上随后的用户信息数据中的字节数。
用户 ID	uint32	用户的标识号。

表 4-88　　用户信息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
领域 ID (Realm ID)	uint32	与身份领域对应的整数 ID。
协议 (Protocol)	uint32	用于包含用户信息的数据包的协议。
字符串块类型 (String Block Type)	uint32	启动包含用户的名字的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名字字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上名字中的字节数。
名字 (First Name)	字符串	用户的名字。
字符串块类型 (String Block Type)	uint32	启动包含用户的姓氏的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户姓氏字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上姓氏中的字节数。
姓氏	字符串	用户的姓氏。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
字符串块类型 (String Block Type)	uint32	启动包含用户所在部门的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	部门字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上部门中的字节数。
部门	字符串	用户所在部门。
字符串块类型 (String Block Type)	uint32	启动包含用户的电话号码的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电话号码字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电话号码中的字节数。
电话	字符串	用户的电话号码。

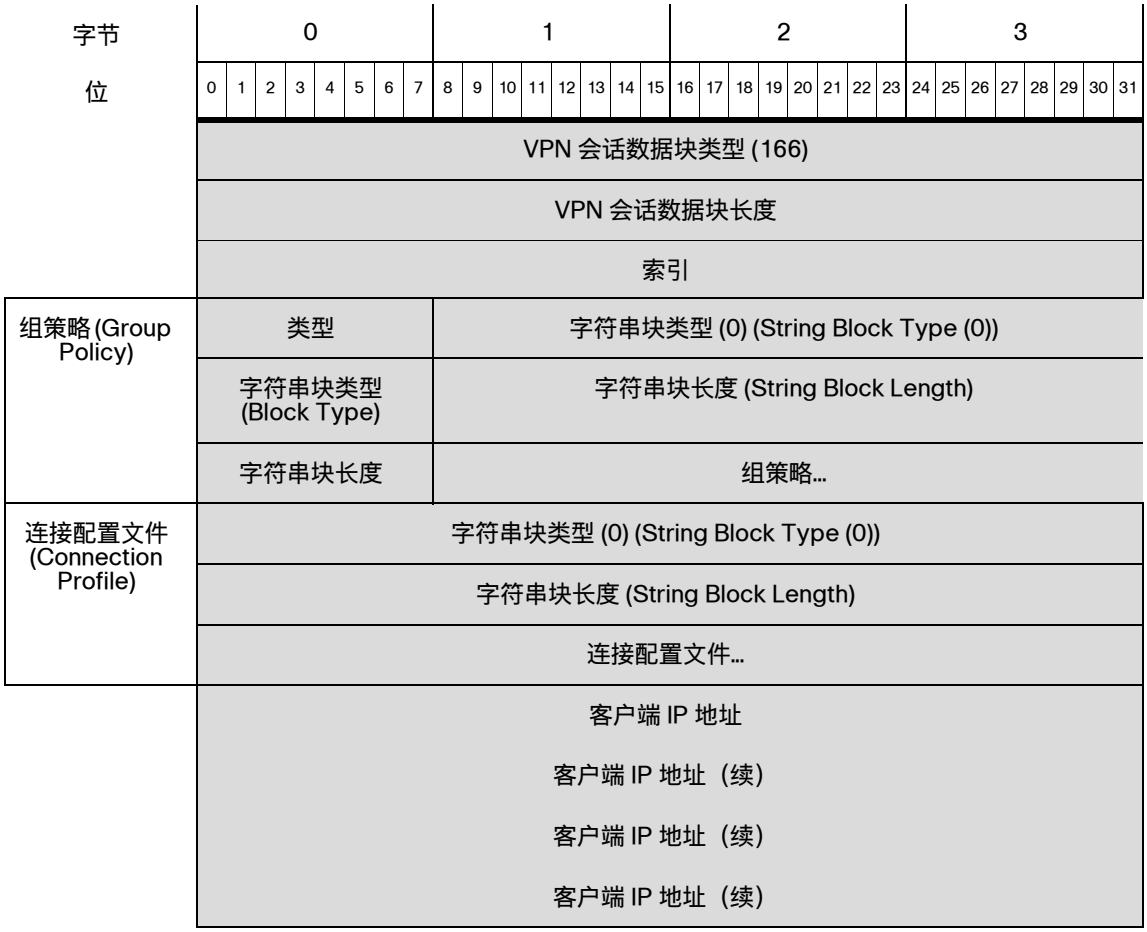
表 4-88 用户信息数据块字段 （续）

字段	数据类型	说明 (Description)
终端配置文件 ID (Endpoint Profile ID)	uint32	连接终端使用的设备类型的 ID 号码。这是每个防御中心特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	网络流量组的 ID 号码。
位置 IPv6 地址 (Location IPv6 Address)	uint16[8]	与 ISE 通信的接口的 IP 地址。可以是IPv4 或 IPv6。

用于 6.2+ 的 VPN 会话数据块

用于 6.2+ 的 VPN 会话数据块的块类型为系列 1 数据块组中的 166。该数据块描述 VPN 会话信息。

下图显示 6.2+ 中的 VPN 会话数据块的格式。



下表对 VPN 会话数据块的字段进行了说明。

表 4-89　　VPN 会话数据块字段

字段	数据类型	说明 (Description)
VPN 会话数据块类型 (VPN Session Data Block Type)	uint32	启动 VPN 会话数据块。值始终为 166。
VPN会话块长度 (VPN Session Block Length)	uint32	VPN 会话数据块中的字节数，包括 VPN 会话数据块类型和长度的八个字节，加上随后的“VPN 会话”数据字段中的字节数。
索引	uint32	由 VPN 设备生成的用于标识会话的编号。
类型	uint8	VPN 会话的类型。可能的值包括: ▪ 0 - 未知 ▪ 1- 思科 IKEv1 客户端 ▪ 2- AnyConnect IKEv1 客户端 ▪ 3 - AnyConnect SSL ▪ 4 - WebVPN 无客户端 ▪ 5 - 站点间 IKEv2 ▪ 6 - 站点间 IKEv2 ▪ 7 - 通用 IKEv2 RA 客户端

表 4-89 VPN 会话数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含 VPN 会话的组策略的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上组策略中的字节数。
组策略	字符串	在建立 VPN 会话时分配给客户端的组策略的名称。
字符串块类型 (String Block Type)	uint32	启动包含 VPN 会话的连接配置文件的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上连接配置文件中的字节数。
连接配置文件	字符串	VPN 会话使用的连接配置文件（隧道组）的名称。
客户端 IP 地址	uint8[16]	VPN 客户端设备的 IP 地址。
客户端国家/地区	uint16	VPN 客户端的国家/地区代码。
字符串块类型 (String Block Type)	uint32	启动包含客户端设备所使用操作系统的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上操作系统名称中的字节数。
客户端操作系统	字符串	客户端设备的操作系统。
字符串块类型 (String Block Type)	uint32	启动包含客户端设备所使用 VPN 应用的字符串数据块。值始终为 0。
字符串块长度	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上 VPN 应用中的字节数。
客户端应用	字符串	客户端设备的 VPN 应用。
连接持续时间	uint32	VPN 会话的持续时间（以秒为单位）。仅指定用于 VPN 注销操作，否则值为 0。
传输的字节数	uint64	VPN 会话期间传输到 VPN 客户端的字节数。仅 指定用于 VPN 注销操作，否则值为 0。
接收的字节数	uint64	VPN 会话期间从 VPN 客户端接收的字节数。仅指定用于 VPN 注销操作，否则值为 0。

用户登录信息数据块 6.2+

用户登录信息数据块在用户信息更新消息中使用，传送检测到的用户的登录信息变更。有关详细信息，请参阅用户信息更新消息块，第 4-59 页。

在版本 6.2+ 中，用户登录信息数据块的块类型为系列 1 数据块组中的 167。它的一些新字段用于支持 VPN。它替代块类型 165。用户登录信息数据块 6.1.x，第 B-143 页有关详细信息，请参阅。

下图显示用户登录信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户登录信息块类型 (167) (User Login Information Block Type (159))																															
	用户登录信息块长度 (User Login Information Block Length)																															
	时间戳 (Timestamp)																															
	IPv4 地址 (IPv4 Addresses)																															
用户名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名...(User Name...)																															
域	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	域...(Domain...)																															
	用户 ID																															
	领域 ID (Realm ID)																															
	终端配置文件 ID (Endpoint Profile ID)																															
	安全组 ID (Security Group ID)																															
	协议 (Protocol)																															
	端口 (Port)																范围开始 (Range Start)															
	开始端口 (Start Port)																结束端口 (End Port)															
电子邮件 (Email)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件...(Email...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPv6 地址 (IPv6 Address)																															
	IPv6 地址 (IPv6 Address)（续）																															
	IPv6 地址 (IPv6 Address)（续）																															
	IPv6 地址 (IPv6 Address)（续）																															
	位置 IPv6 地址 (Location IPv6 Address)																															
	位置 IPv6 地址 (Location IPv6 Address)（续）																															
	位置 IPv6 地址 (Location IPv6 Address)（续）																															
	位置 IPv6 地址 (Location IPv6 Address)（续）																															
报告者 (Reported By)	登录类型 (Login Type)								身份验证类型 (Type)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0))（续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length)（续）																报告者...(Reported By...)															
说明	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明... (Description...)																															
VPN 会话	VPN 会话数据块类型 (166)																															
	VPN 会话数据块长度																															
	VPN 会话...																															

下表对用户登录信息数据块的组件进行了说明。

表 4-90　用户登录信息数据块字段

字段	数据类型	说明 (Description)
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 6.2+ 中，此值为 167。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IPv4 地址 (IPv4 Addresses)	uint32	保留此字段，但不再填充。IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅IP 地址，第 1-4 页。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
字符串块类型 (String Block Type)	uint32	启动包含域的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上域中的字节数。
域	字符串	用户登录的域。
用户 ID	uint32	用户的标识号。
领域 ID (Realm ID)	uint32	与身份领域对应的整数 ID。
终端配置文件 ID (Endpoint Profile ID)	uint32	连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	网络流量组的 ID 号码。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值包括： ▪ 165 - FTP ▪ 426 - SIP ▪ 547 - AOL 即时通信工具 ▪ 683 - IMAP ▪ 710 - LDAP ▪ 767 - NTP ▪ 773 - Oracle 数据库 ▪ 788 - POP3 ▪ 1755 - MDNS

表 4-90 用户登录信息数据块字段 （续）

字段	数据类型	说明 (Description)
端口 (Port)	uint16	在其上检测到用户的端口号。
范围开始 (Range Start)	uint16	TS 代理使用的端口范围内的起始端口。
开始端口 (Start Port)	uint16	TS 代理分配给单个用户的端口范围内的起始端口。
结束端口 (End Port)	uint16	TS 代理分配给单个用户的端口范围内的结束端口。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
IPv6 地址 (IPv6 Address)	uint8[16]	检测到用户登录的主机的 IPv6 地址，采用 IP 地址八位组。
位置 IPv6 地址 (Location IPv6 Address)	uint8[16]	用户最新登录的 IP 地址。可以是 IPv4 或 IPv6 地址。
登录类型 (Login Type)	uint8	检测到的用户登录类型。
身份验证类型 (Authentication Type)	uint8	用户使用的身份验证类型。值可能是: ▪ 0 - 无需授权 ▪ 1 - 被动身份验证、AD 代理或 ISE 会话 ▪ 2 - 强制网络门户身份验证成功 ▪ 3 - 强制网络门户访客身份验证 ▪ 4 - 强制网络门户身份验证失败
字符串块类型 (String Block Type)	uint32	启动包含报告者值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	报告者字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上“报告者”(Reported By) 字段中的字节数。
报告者 (Reported By)	字符串	此活动的报告者，例如 Active Directory 服务器的名称。
字符串块类型 (String Block Type)	uint32	启动包含说明值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	说明字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上“说明”(Description) 字段中的字节数。
说明	字符串	登录或注销活动的说明。
VPN 会话块类型 (VPN Session Block Type)	uint32	启动包含 VPN 会话数据的 VPN 会话数据块。值始终为 166。

表 4-90　用户登录信息数据块字段 （续）

字段	数据类型	说明 (Description)
VPN 会话数据块长度	uint32	VPN 会话数据块中的字节数，包括块类型和长度字段的八个字节，加上 VPN 会话数据块中的字节数。
VPN 会话数据	VPN 会话数据	有关检测到的VPN会话的信息（如果登录与VPN会话关联）。这仅在有 VPN 会话时使用。

发现和连接事件系列 2 数据块

在下表中，“数据块状态”(Data Block Status) 字段指示该块是当前版本（最新版本）还是旧版本（在较旧的版本中使用，但仍可以通过 eStreamer 请求）。

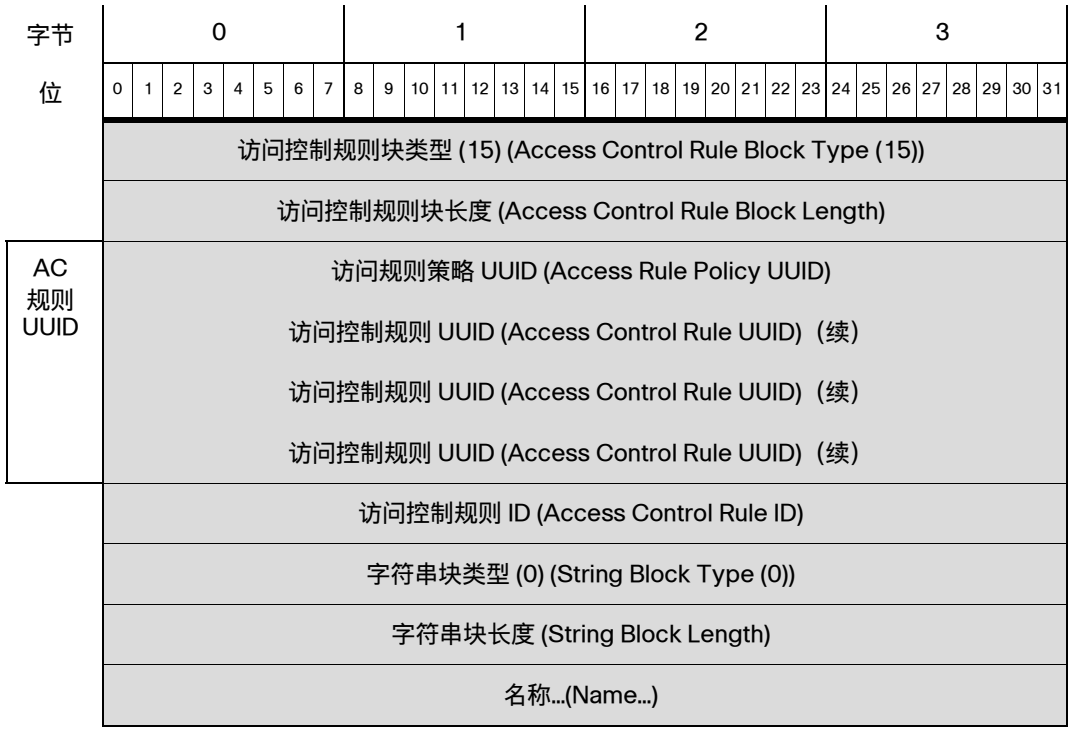
表 4-91　发现和连接事件系列 2 块类型

类型 (Type)	内容	数据块状态	说明 (Description)
15	访问控制规则	当前	访问控制规则元数据消息用其将策略 UUID 和规则 ID 值映射到描述性字符串。请参阅访问控制规则数据块，第 4-202 页。
21	访问控制规则原因	传统	访问控制规则元数据消息用其将访问控制规则原因映射到描述性字符串。请参阅访问控制策略规则原因数据块，第 B-402 页。
22	安全情报类别	当前	用于存储安全情报信息。请参阅安全情报类别数据块 5.1+，第 4-205 页。
57	用户数据	当前	用户记录元数据消息用其提供用户 ID 号码、在其上检测到用户的协议以及用户名。请参阅用户数据块，第 4-206 页。
59	访问控制规则原因	当前	访问控制规则元数据消息用其将访问控制规则原因映射到描述性字符串。请参阅访问控制规则原因数据块 6.0+，第 4-203 页。

访问控制规则数据块

eStreamer 服务使用访问控制规则元数据消息中的访问控制规则数据块将策略 UUID 和规则 ID 组合映射到描述性字符串。访问控制规则数据块的块类型为系列 2 数据块组中的 15。

下图显示访问控制规则数据块的结构:



下表对访问控制规则数据块中的字段进行了说明。

表 4-92 访问控制规则数据块字段

字段	数据类型	说明 (Description)
访问控制规则块类型 (Access Control Rule Block Type)	uint32	启动访问控制规则块。值始终为 15。
访问控制规则块长度 (Access Control Rule Block Length)	uint32	访问控制规则块中的字节总数，包括访问控制规则块类型和长度字段的八个字节，加上随后的数据的字节数。
访问控制规则 UUID (Access Control Rule UUID)	uint8[16]	访问控制规则的唯一标识符。此字段与访问控制规则 ID 一起构成此记录的唯一密钥。
访问控制规则 ID (Access Control Rule ID)	uint32	访问控制规则的内部思科标识符。 此字段与访问控制规则 UUID 一起构成此记录的唯一密钥。

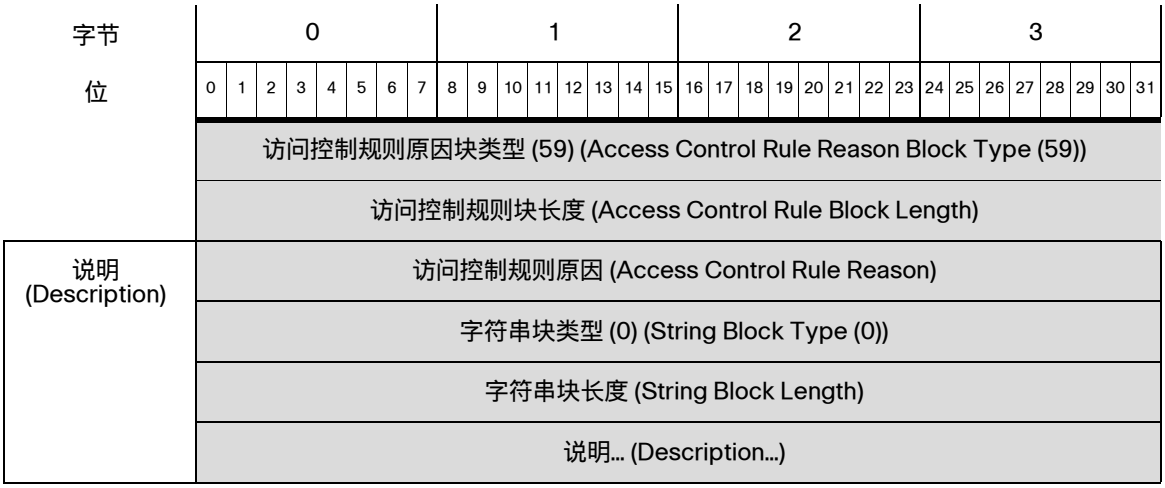
表 4-92　访问控制规则数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含与访问控制策略规则 UUID 和访问控制规则 ID 相关的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
名称 (Name)	字符串	描述性名称。

访问控制规则原因数据块 6.0+

eStreamer 服务使用访问控制规则原因元数据消息中的访问控制规则原因数据块将访问控制原因映射到描述性字符串。访问控制规则原因数据块的块类型为系列 2 数据块组中的 59。它替代了块类型 21。

下图显示访问控制规则原因数据块的结构：



下表对访问控制规则原因数据块中的字段进行了说明。

表 4-93　访问控制规则原因数据块字段

字段	数据类型	说明 (Description)
访问控制规则原因块类型 (Access Control Rule Reason Block Type)	uint32	启动访问控制规则原因块。值始终为 59。
访问控制规则原因块长度 (Access Control Rule	uint32	访问控制规则原因块中的字节总数，包括访问控制规则原因块类型和长度字段的八个字节，加上随后的数据的字节数。

表 4-93 访问控制规则原因数据块字段 （续）

字段	数据类型	说明 (Description)
访问控制规则原因 (Access Control Rule Reason)	uint32	访问控制规则记录连接的原因。 此字段是此记录的唯一密钥。触发事件的规则的原因编号。 规则原因是一个可以在其中设置多个位的二进制位图。规则可能有多种原因。位值如下： ▪ **1** - IP 阻止 ▪ **2** - IP 监控 ▪ **4** - 用户绕行 ▪ **8** - 文件监控 ▪ **16** - 文件阻止 ▪ **32** - 入侵监控 ▪ **64** - 入侵阻止 ▪ **128** - 阻止继续传输文件 ▪ **256** - 允许继续传输文件 ▪ **512** - 文件自定义检测 ▪ **1024** - SSL 阻止 ▪ **2048** - DNS 阻止 ▪ **4096** - DNS 监控 ▪ **8192** - URL 阻止 ▪ **16384** - URL 监控 ▪ **32768** - 内容限制 ▪ **65536** - 智能应用绕行 ▪ **131072** - WSA 威胁
字符串块类型 (String Block Type)	uint32	启动包含与访问控制规则原因相关的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上说明 (Description) 字段中的字节数。
说明 (Description)	字符串	对访问控制规则原因的说明。

安全情报类别数据块 5.1+

eStreamer 服务使用访问控制规则元数据消息中的安全情报类别数据块流传输安全情报信息。安全情报类别数据块的块类型为系列 2 数据块组中的 22。

下图显示安全情报类别数据块的结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	安全情报类别块类型 (22) (Security Intelligence Category Block Type (22))																															
	安全情报类别块长度 (Security Intelligence Category Block Length)																															
	安全情报列表 ID (Security Intelligence List ID)																															
访问控制策略 UUID	访问控制策略 UUID (Access Control Policy UUID)																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
规则名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	安全情报列表名称...(Security Intelligence Name...)																															

下表对安全情报类别数据块中的字段进行了说明：

表 4-94　　安全情报类别数据块字段

字段	数据类型	说明 (Description)
安全情报类别块类型 (Security Intelligence Category Block Type)	uint32	启动安全情报类别数据块。值始终为 22。
安全情报类别块长度 (Security Intelligence Category Block Length)	uint32	安全情报类别块中的字节总数，包括安全情报类别块类型和长度字段的八个字节，加上随后的数据字节数。
安全情报列表 ID (Security Intelligence List ID)	uint32	连接触发的 IP 阻止列表或允许列表的 ID。 此字段与访问控制策略

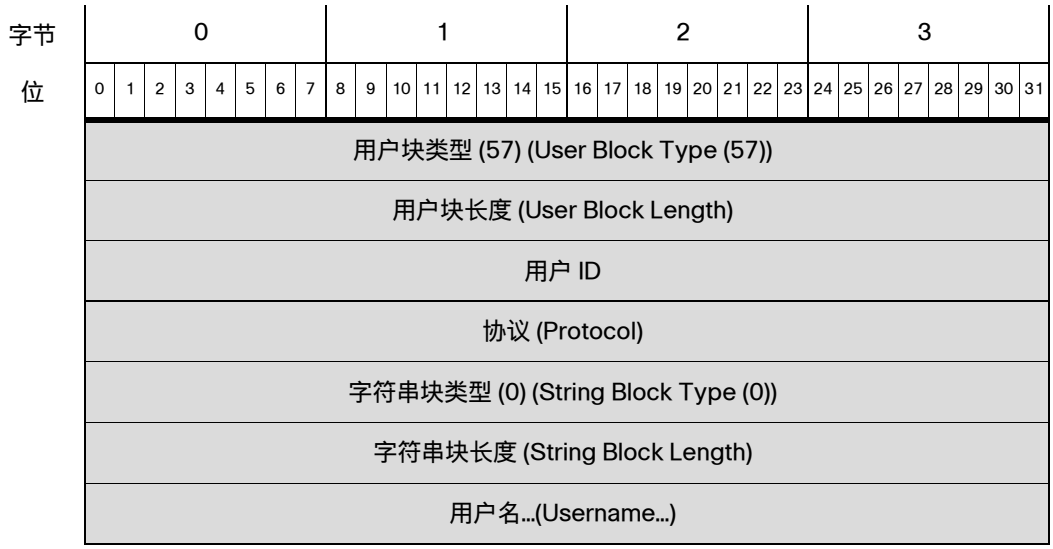
表 4-94 安全情报类别数据块字段 （续）

字段	数据类型	说明 (Description)
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	为安全情报配置的访问控制策略的 UUID。 此字段与安全情报列表 ID 一起构成此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含与安全情报列表相关的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“安全情报列表名称”(Security Intelligence Name) 字段中的字节数。
安全情报列表名称 (Security Intelligence Name)	字符串	连接触发的安全情报类别 IP 阻止列表或允许列表的名称。

用户数据块

eStreamer服务使用用户记录元数据消息中的用户数据块提供用户 ID 号码、在其上检测到用户的协议以及用户名。用户数据块的块类型为系列 2 数据块组中的 57。

下图显示用户数据块的结构:



下表对用户数据块中的字段进行了说明。

表 4-95　用户数据块字段

字段	数据类型	说明 (Description)
用户块类型(User Block Type)	uint32	启动用户块。值始终为 57。
用户块长度(User Block Length)	uint32	用户块中的字节总数，包括用户块类型和长度字段的八个字节，加上随后的数据字节数。
用户 ID	uint32	用户的唯一标识符。 此字段是此记录的唯一密钥。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值包括: ▪ 165 - FTP ▪ 426 - SIP ▪ 547 - AOL 即时通信工具 ▪ 683 - IMAP ▪ 710 - LDAP ▪ 767 - NTP ▪ 773 - Oracle 数据库 ▪ 788 - POP3 ▪ 1755 - MDNS
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户名”(Username) 字段中的字节数。
用户名 (Username)	字符串	用户的名称

访问控制策略元数据块 6.0+

eStreamer 服务使用访问控制策略元数据消息中的访问控制策略元数据块来提供访问控制策略信息。访问控制策略元数据块的块类型为系列 2 数据块组中的 64。

下图显示访问控制策略元数据块的结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	访问控制策略元数据块类型 (64) (Access Control Policy Metadata Block Type (64))																															
	访问控制策略元数据块长度 (Access Control Policy Metadata Block Length)																															
访问控制策略 UUID	访问控制策略 UUID (Access Control Policy UUID)																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	传感器 ID (Sensor ID)																															
策略名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	策略名称...																															

下表对访问控制策略元数据块中的字段进行了说明。

表 4-96 访问控制策略元数据块字段

字段	数据类型	说明 (Description)
访问控制策略元数据块类型 (Access Control Policy Metadata Block Type)	uint32	启动访问控制策略元数据块。值始终为 64。
访问控制策略元数据块长度 (Access Control Policy Metadata Block Length)	uint32	访问控制策略元数据块中的字节总数，包括访问控制策略元数据块类型和长度字段的八个字节，加上随后的数据的字节数。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	访问控制策略的 UUID。此字段是此记录的唯一密钥。
传感器 ID (Sensor ID)	uint32	与访问控制策略关联的传感器的 ID 号码

表 4-96　访问控制策略元数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含与访问控制策略关联的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
名称 (Name)	字符串	访问控制策略的名称。

了解主机数据结构

本章介绍传送描述单个主机的一组数据的完整主机配置文件数据块的格式。eStreamer 根据对主机数据的请求生成并发送这些数据块。有关客户端请求程序、消息结构以及交付方法的信息，请参阅主机数据和多主机数据消息格式，第 2-28 页。

eStreamer 使用系列 1 数据块结构打包这些完整主机配置文件数据块。有关系列 1 数据块的一般结构，请参阅系列 1 数据块报头，第 4-60 页。完整主机配置文件数据块包含许多封装数据块，了解发现和连接数据结构，第 4-1 页中定义这些数据块的子节中有对这些数据块的单独说明。

有关当前和旧版完整主机配置文件数据块的详细信息，请参阅以下各节：

- 完整主机配置文件数据块 5.3+，第 5-1 页介绍当前完整主机配置文件数据块结构。
- 完整主机配置文件数据块 5.0 - 5.0.2，第 B-363 页介绍用于版本 5.0 - 5.0.2 的旧版完整主机配置文件数据块结构。

完整主机配置文件数据块 5.3+

用于版本 5.3+ 的完整主机配置文件数据块包含一整套主机说明数据。其格式如下图中所示，并在下表中进行说明。请注意，除列表数据块之外，该图未显示封装数据块的字段。这些封装数据块在了解发现和连接数据结构，第 4-1 页中单独进行说明。完整主机配置文件数据块的块类型值为 149。它替代了之前的版本，之前版本的块类型为 140。

注释 下图中块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示用于 5.3+ 的完整主机配置文件数据块的格式:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	完整主机配置文件数据块 (149) (Full Host Profile Data Block (149))																															
	数据块长度 (Data Block Length)																															
	主机 ID 主机 ID (Host ID)（续） 主机 ID (Host ID)（续） 主机 ID (Host ID)（续）																															
IP 地址 (IP Address)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	IP 地址数据块 (143) (IP Address Data Blocks (143))*																															
	跳数 (Hops)								通用列表块类型 (31) (Generic List Block Type (31))																							
	通用列表块类型 (Generic List Block Type)（续）								通用列表块长度 (Generic List Block Length)																							
源自操作系统的指纹 (OS Derived Fingerprints)	通用列表块长度 (Generic List Block Length)（续）								操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																							
	操作系统指纹块类型 (130) (OS Fingerprint Block Type (130))*（续）								操作系统指纹块长度 (Operating System Fingerprint Block Length)																							
	操作系统指纹块长度 (OS Fingerprint Block Length)（续）								源自操作系统的指纹数据... (Operating System Derived Fingerprint Data...)																							
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
服务器指纹 (Server Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统服务器指纹数据... (Operating System Server Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	通用列表块长度 (Generic List Block Length)																															
客户端指纹	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统客户端指纹数据... (Operating System Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 1 (VDB Native Fingerprints 1)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 2 (VDB Native Fingerprints 2)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
用户指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户指纹数据... (Operating System User Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
扫描指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统扫描指纹数据... (Operating System Scan Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
应用指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统应用指纹数据... (Operating System Application Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
冲突指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统冲突指纹数据... (Operating System Conflict Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
移动 (Mobile) 指纹 (Mobile Device Fingerprint)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统移动指纹数据... (Operating System Mobile Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
IPv6 服务器指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 IPv6 服务器指纹数据... (Operating System IPv6 Server Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
Ipv6 客户端指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 Ipv6 客户端指纹数据... (Operating System Ipv6 Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Ipv6 DHCP 指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 IPv6 DHCP 指纹数据... (Operating System IPv6 DHCP Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
用户代理指纹 (User Agent Fingerprint)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户代理指纹数据... (Operating System User Agent Fingerprint Data...)																															
(TCP) 完整服务器数据	列表块类型 (11)... (List Block Type (11))...																															
	列表块长度... (List Block Length)...																															
	(TCP) 完整服务器数据块 (104) ((TCP) Full Server Data Blocks (104))*																															
(UDP) 完整服务器数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	(UDP) 完整服务器数据块 (104) ((UDP) Full Server Data Blocks (104))*																															
网络协议数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（网络）协议数据块 (4) ((Network) Protocol Data Blocks (4))*																															
传输协议数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（传输）协议数据块 (4) ((Transport) Protocol Data Blocks (4))*																															
MAC 地址数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	主机 MAC 地址数据块 (95) (Host MAC Address Data Blocks (95))*																															
	上次查看时间 (Last Seen)																															
	主机类型 (Host Type)																															
	业务临界点 (Business Criticality)								VLAN ID																							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	VLAN 类型 (VLAN Type)								VLAN 优先级 (VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))															
主机客户端数据	通用列表块类型 (Generic List Block Type)（续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length)（续）																完整主机客户端应用数据块 (112) (Full Host Client Application Data Blocks (112))*															
NetBIOS 名称 (NetBIOS Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
名称 (Name)	NetBIOS 名称字符串... (NetBIOS Name String...)																															
说明 (Description) 数据	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	注释字符串... (Notes String....)																															
(VDB) 主机漏洞 ((VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(VDB) 主机漏洞数据块 (85) ((VDB) Host Vulnerability Data Blocks (85))*																															
（第三方/VDB）主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方/VDB）主机漏洞数据块 (85) ((Third Party/VDB) Host Vulnerability Data Blocks (85))*																															
第三方扫描主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方扫描）具有原始漏洞 ID 的主机漏洞数据块 (85) ((Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85))*																															
属性值数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	属性值数据块 (Attribute Value Data Blocks) *																															
	移动 (Mobile)								Jailbroken								通用列表块类型 (31) (Generic List Block Type (31))															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IOC 状态 (IOC State)	通用列表块类型 (Generic List Block Type)（续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length)（续）																IOC 状态数据块 (150) (IOC State Data Blocks (150))*															

下表描述的是用于 5.3+ 记录的完整主机配置文件的组件。

表 5-1　　完整主机配置文件记录 5.3+ 字段

字段	数据类型	说明 (Description)
主机 ID	uint8[16]	主机的唯一 ID 号码。这是一个 UUID。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务数据的 IP 地址数据块组成的列表数据块。值始终为 `11`。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装 IP 地址数据块的长度。
IP 地址 (IP Address)	变量	主机的 IP 地址以及上次看到每个 IP 地址的时间。有关此数据块的说明，请参阅主机 IP 地址数据块，第 4-95 页。
跳数 (Hops)	uint8	从主机到设备的网络跳数。
通用列表块类型 (Generic List Block	uint32	启动由传送源自主机的现有指纹的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 `31`。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
源自操作系统的指纹数据块 (Operating System Derived Fingerprint Data Blocks) *	变量	包含源自主机的现有指纹的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 `31`。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 5-1　完整主机配置文件记录 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用思科 VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 1) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks) *	变量	包含用思科漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用思科 VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。

表 5-1　完整主机配置文件记录 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 2) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks) *	变量	包含用思科漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用户添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（用户指纹）数据块 (Operating System Fingerprint (User Fingerprint) Data Blocks) *	变量	包含用户添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送漏洞扫描仪添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（扫描指纹）数据块 (Operating System Fingerprint (Scan Fingerprint) Data Blocks) *	变量	包含漏洞扫描仪添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。

表 5-1　完整主机配置文件记录 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
通用列表块类型 (Generic List Block	uint32	启动由传送应用添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（应用指纹）数据块 (Operating System Fingerprint (Application Fingerprint) Data Blocks) *	变量	包含应用添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送通过指纹冲突解决选择的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（冲突指纹）数据块 (Operating System Fingerprint (Conflict Fingerprint) Data Blocks) *	变量	包含通过指纹冲突解决选择的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送移动设备指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（移动）数据块 (Operating System Fingerprint (Mobile) Data Blocks) *	变量	包含移动设备主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。

表 5-1　完整主机配置文件记录 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
通用列表块类型 (Generic List Block	uint32	启动由传送用 IPv6 服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（IPv6 服务器指纹）数据块 (Operating System Fingerprint (IPv6 Server Fingerprint) Data Blocks) *	变量	包含用 IPv6 服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 IPv6 客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（IPv6 客户端指纹）数据块 (Operating System Fingerprint (IPv6 Client Fingerprint) Data Blocks) *	变量	包含用 IPv6 客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 IPv6 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 5-1　完整主机配置文件记录 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
操作系统指纹 (IPv6 DHCP) 数据块 (Operating System Fingerprint (IPv6 DHCP) Data Blocks) *	变量	包含用 IPv6 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用用户代理指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（用户代理）数据块 (Operating System Fingerprint (User Agent) Data Blocks) *	变量	包含用用户代理指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
列表块类型 (List Block Type)	uint32	启动由传送TCP服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(TCP) 完整服务器数据块 ((TCP) Full Server Data Blocks) *	变量	传输主机上的 TCP有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-141 页。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(UDP) 完整服务器数据块 ((UDP) Full Server Data Blocks) *	变量	传输主机上的 UDP 子服务器相关数据的完整主机数据块列表。有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-141 页。

表 5-1　完整主机配置文件记录 5.3+ 字段（续）

字段	数据类型	说明 (Description)
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（网络）协议数据块 ((Network) Protocol Data Blocks) *	变量	传输主机上的网络协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（传输）协议数据块 ((Transport) Protocol Data Blocks) *	变量	传送主机上的传输协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动包含主机 MAC 地址数据块的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装主机 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks) *	变量	主机 MAC 地址数据块列表。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-113 页。
上次查看时间 (Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。值包括： ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥 ▪ 3 - NAT（网络地址转换设备） ▪ 4 - LB（负载均衡器）

表 5-1　完整主机配置文件记录 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
业务临界点 (Business Criticality)	uint16	表示主机到业务的临界点。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block	uint32	启动由传送客户端应用数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
完整主机客户端应用数据块 (Full Host Client Application Data Blocks) *	变量	客户端应用数据块列表。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-155 页。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动主机注释的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	注释字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上注释字符串中的字节数。
说明 (Description)	字符串	包含主机的主机属性注释的内容。
通用列表块类型 (Generic List Block	uint32	启动由传送 VDB 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。

表 5-1　完整主机配置文件记录 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks) *	变量	在思科漏洞数据库 (VDB) 中识别的漏洞的主机漏洞数据块列表。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
通用列表块类型 (Generic List Block	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方/VDB）主机漏洞数据块 ((Third Party/VDB) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪且包含已收录到思科漏洞数据库 (VDB) 中的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
通用列表块类型 (Generic List Block	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方扫描）主机漏洞数据块 ((Third Party Scan) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪的主机漏洞数据块。请注意，这些数据块的主机漏洞 ID 为第三方扫描仪 ID，而不是思科检测到的 ID。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
列表块类型 (List Block Type)	uint32	启动由传送属性数据的属性值数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表数据块中的字节数，包括列表报头以及所有封装数据块。

表 5-1　完整主机配置文件记录 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
属性值数据块 (Attribute Value Data Blocks) *	变量	属性值数据块列表。有关此列表中的数据块的说明，请参阅属性值数据块，第 4-79 页。
移动 (Mobile)	uint8	指示操作系统是否在移动设备上运行的一个真假标志。
Jailbroken	uint8	指示移动设备操作系统是否被越狱的一个真假标志。
通用列表块类型 (Generic List Block	uint32	表示由 IOC 状态数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表标头以及所有封装 IOC 状态数据块。
IOC 状态数据块 (IOC State Data Blocks) *	变量	包含主机存在的威胁的相关信息的 IOC 状态数据块。有关此数据块的说明，请参阅用于 5.3+ 的 IOC 状态数据块，第 4-33 页。

配置eStreamer

创建一个客户端应用之后，您可以将其连接至 eStreamer 服务器，启动 eStreamer 服务，开始交换数据。

注释 *eStreamer 服务器*是运行 eStreamer 服务的 管理中心 或受管设备（版本 4.9 或更高版本）。

请执行以下任务以管理 eStreamer 和客户端交互：

1. 在 eStreamer 服务器上启用 eStreamer。

   有关允许访问 eStreamer 服务器、添加客户端以及生成身份验证凭证以建立已验证连接的信息，请参阅在 eStreamer 服务器上配置 eStreamer，第 6-1 页。

2. 如需要，请手动运行 eStreamer 服务 (eStreamer)。您可以停止、启动以及查看服务的状态，并使用命令行选项调试客户端-服务器的通信。

   有关详细信息，请参阅管理 eStreamer 服务，第 6-4 页。

3. 或者，要使用 eStreamer 标准客户端对连接或数据流进行故障排除，请在准备用于运行客户端的计算机上设置标准客户端。

   请参阅配置 eStreamer 标准客户端，第 6-5 页。

在 eStreamer 服务器上配置 eStreamer

许可证： 任意

在您想要用作 eStreamer 服务器的管理中心或受管设备可以开始将事件流传输到客户端应用之前，您必须配置用于向客户端发送事件的 eStreamer 服务器，提供关于客户端的信息，并生成一套要在建立通信时使用的身份验证凭证。您可以从管理中心或受管设备用户界面执行所有这些任务。

有关详细信息，请参阅以下各节：

- 配置 eStreamer 事件类型，第 6-2 页
- 为 eStreamer 客户端添加身份验证，第 6-3 页

配置 eStreamer 事件类型

许可证：任意

您可以控制 eStreamer 服务器能够向客户端应用传输其所请求的事件的类型。

受管设备或管理中心上的可用事件类型包括：

- 入侵事件
- 入侵事件数据包数据
- 入侵事件额外数据

管理中心上的可用事件类型包括：

- 发现事件（这也会启用连接事件）
- 关联并允许列表事件
- 影响标志警报 (Impact flag alerts)
- 用户活动事件
- 恶意事件
- 文件事件

请注意，堆叠 3D9900 对中的主设备和辅助设备像独立受管设备一样向管理中心报告入侵事件。如果在 3D9900 堆栈中的主设备上配置与 eStreamer 客户端通信，则也需要在辅助设备上配置该客户端；客户端配置不会复制。同样，如果要删除该客户端，请将主设备和辅助设备上的该客户端都删除。如果以堆栈配置为管理 3D9900 的管理中心配置 eStreamer 客户端，请注意，管理中心会报告从两个受管设备收到的所有事件，即使两个设备报告的是同一事件。

如果以高可用性配置在管理中心上配置 eStreamer 客户端，客户端配置将不从主管理中心复制至辅助管理中心。

要配置 eStreamer 捕获的事件类型，请执行以下操作：

访问权限：管理员

步骤 1 选择**系统 (System) > 集成 (Integration) > eStreamer**。

步骤 2 单击 **eStreamer**。

系统将显示 eStreamer 页面和 **eStreamer 事件配置 (eStreamer Event Configuration)** 菜单。

步骤 3 选中想要 eStreamer 捕获并转发至请求客户端的事件类型旁的复选框。请注意，如果现在不选中该复选框，则其对应的数据不会被捕获。取消选中复选框不会删除已捕获的数据。

在管理中心或受管设备上，可选择以下任何或全部事件：

- **入侵事件 (Intrusion Events)**，以传输受管设备生成的入侵事件。
- **入侵事件数据包数据 (Intrusion Event Packet Data)**，以传输与入侵事件关联的数据包。
- **入侵事件额外数据 (Intrusion Event Extra Data)**，以传输与入侵事件关联的额外数据，如与通过 HTTP 代理或负载均衡器连接至 Web 服务器的客户端的源 IP 地址关联的 URI。

在管理中心上，还可选择以下任何或全部事件：

- **发现事件 (Discovery Events)**，以传输主机发现事件。
- **关联事件 (Correlation Events)**，以传输关联并允许列表事件。
- **Impact Flag Alerts**，以传输管理中心生成的影响警报。
- **用户活动事件 (User Activity Events)**，以传输用户事件。
- **入侵事件额外数据 (Intrusion Event Extra Data)**，以传输入侵事件的额外数据，如与通过 HTTP 代理或负载均衡器连接至 Web 服务器的客户端的源 IP 地址关联的 URI。

注释　请注意，这可以控制 eStreamer 服务器可传输的事件。您的客户端应用还必须明确请求您希望其接收的事件类型。有关详细信息，请参阅请求标志，第 2-12 页。

步骤 4　点击**保存**。

系统会保存您的设置，并且在收到请求时，会将您选择的事件转发至 eStreamer 客户端。

为 eStreamer 客户端添加身份验证

许可证：任意

只有先将客户端添加至 eStreamer 服务器的对等数据库，eStreamer 才能向客户端发送事件。还必须将 eStreamer 服务器生成的身份验证证书复制至客户端。

要添加 eStreamer 客户端，请执行以下操作：

访问权限：管理员

步骤 1　选择**系统 (System) > 集成 (Integration) > eStreamer**。

系统将显示 **eStreamer** 页面。

步骤 2　点击**创建客户端 (Create Client)**。

系统将显示“创建客户端”(Create Client) 页面。

步骤 3　在**主机名 (Hostname)** 字段中，输入运行 eStreamer 客户端的主机的主机名称或 IP 地址。

注释　如果使用主机名，则主机输入服务器**必须**能够将主机解析为 IP 地址。如果尚未配置 DNS 解析，应先配置解析或使用 IP 地址。

步骤 4　如果要对证书文件进行加密，请在**密码 (Password)** 字段中输入密码。

步骤 5　点击**保存 (Save)**。

eStreamer 服务器允许客户端计算机访问管理中心上的 8302 端口，并创建在客户端-服务器身份验证过程中使用的身份验证证书。系统再次显示“eStreamer 客户端”(eStreamer Client) 页面，新的客户端将在**eStreamer 客户端 (eStreamer Client)** 下列出。

步骤 6　点击证书文件旁边的下载图标 ( )。

步骤 7　将证书文件保存至客户端计算机用于 SSL 身份验证的目录。

客户端现在可以连接到管理中心。

提示　要撤消客户端的访问权限，请点击想要移除的主机旁的删除图标 ( )。请注意，无需重启管理中心上的主机输入服务；访问权限将立即撤消。

管理 eStreamer 服务

许可证： 任意

您可以从用户界面管理 eStreamer 服务。您也可以使用命令行启动和停止服务。以下部分介绍 eStreamer 命令行选项：

- 启动和停止 eStreamer 服务，第 6-4 页介绍如何启动和停止 eStreamer 服务。
- eStreamer 服务选项，第 6-4 页介绍可用于 eStreamer 服务的命令行选项及其使用方法。

启动和停止 eStreamer 服务

许可证： 任意

您可以用 `manage_estreamer.pl` 脚本管理 eStreamer 服务，通过该脚本，您可以启动、停止、重新加载以及重新启动服务。

提示 您也可以在 eStreamer 初始化脚本中添加命令行选项。有关详细信息，请参阅eStreamer 服务选项，第 6-4 页。

下表介绍您可以在管理中心或受管设备上使用的 `manage_estreamer.pl` 脚本中的选项。

表 6-1 eStreamer 管理选项

选项	说明	选择选项编号....
enable	启动服务。	3
disable	停止服务。	2
restart	重新启动服务。	4
status	表示服务是否正在运行。	1

eStreamer 服务选项

许可证： 任意

eStreamer 提供许多允许您对服务进行故障排除的服务选项。您可以使用下表中描述的 eStreamer 服务选项。

表 6-2 eStreamer 服务选项

选项	说明
`--debug`	运行 eStreamer，并进行调试级日志记录。系统将错误保存到系统日志中并在屏幕上显示错误（与 `--nodaemon` 一起使用时）。

表 6-2　　eStreamer 服务选项

选项	说明
`--nodaemon`	将 eStreamer 作为前台进程运行。系统在屏幕上显示错误。
`--nohostcheck`	运行 eStreamer，并禁用主机名检查。即，当客户端主机名与客户端证书 subjectAltName:dNSName 条目中包含的主机名不匹配时，仍允许访问。`nohostcheck` 选项在网络 DNS 和/或 NAT 配置阻止主机名成功检查时有用。请注意，系统会执行所有其他安全检查。 ⚠ **小心**　启用此选项会对您系统的安全性造成不良影响。

通过首先停止 eStreamer 服务，然后用您想要的选项运行该服务，最后重新启动该服务来使用以上选项。例如，您可以按照在调试模式下运行 eStreamer 服务，第 6-5 页中提供的说明调试 eStreamer 功能。

在调试模式下运行 eStreamer 服务

许可证：任意

您可以在调试模式下运行 eStreamer 服务，以查看该服务在您的终端屏幕上生成的所有状态消息。使用以下程序进行调试。

要在调试模式下运行 eStreamer 服务，请执行以下操作：

访问权限：管理员

步骤 1　用 SSH 登录到管理中心或受控设备。

步骤 2　使用 `manage_estreamer.pl`，并选择选项 `2` 来停止 eStreamer 服务。

步骤 3　使用 `./usr/local/sf/bin/sfestreamer --nodaemon --debug` 在调试模式下重新启动 eStreamer 服务。

系统在终端屏幕上显示该服务的状态消息。

步骤 4　调试完成后，通过使用 `manage_estreamer.pl` 和选择选项 `4` 在正常模式下重新启动该服务。

配置 eStreamer 标准客户端

配备 eStreamer SDK 的*标准客户端*是一组示例客户端脚本和 Perl 模块，以及 Python 脚本，用于说明如何使用 eStreamer API。您可以运行它们以熟悉 eStreamer 输出，或者使用它们调试您的定制客户端的安装问题。

有关设置标准客户端的详细信息，请参阅以下各节：

- 设置eStreamer 标准客户端，第 6-6 页
- 运行 eStreamer Perl 标准客户端，第 6-11 页
- 运行 eStreamer Python 标准客户端，第 6-12 页

设置eStreamer 标准客户端

要使用eStreamer 标准客户端，必须先配置示例脚本，使其适合您的环境和要求。

有关详细信息，请参阅以下各节:

下载eStreamer 标准客户端

您可以从思科支持网站下载包含eStreamer 标准客户端文件的 `eStreamerSDK.zip` 软件包。`eStreamerSDK.zip` 软件包包含以下文件:

- `SF_CUSTOM_ALERT.MIB`

  `snmp.pm` 文件用此 MIB 文件为 SNMP 设置陷阱。
- `SFRecords.pm`

  此 Perl 模块包含发现消息记录块的定义。
- `SFStreamer.pm`

  此 Perl 模块包含 Perl 客户端调用的函数。
- `SFPkcs12.pm`

  此 Perl 模块解析客户端证书并允许客户端连接到 eStreamer 服务器。
- `SFRNABlocks.pm`

  此 Perl 模块包含发现数据块的定义。
- `ssl_test.pl`

  您可以使用此 Perl 脚本测试 SSL 连接上的入侵事件请求。
- `OutputPlugins/csv.pm`

  此 Perl 模块以逗号分隔值 (CSV) 格式打印入侵事件。
- `OutputPlugins/print.pm`

  此 Perl 模块以用户可读的格式打印事件。
- `OutputPlugins/snmp.pm`

  此 Perl 模块将事件发送到指定的 SNMP 服务器。
- `OutputPlugins/pcap.pm`

  此 Perl 模块将数据包捕获存储为 pcap 文件。
- `python_client/estreamer_client.py`

  您可以使用此 Python 脚本测试 SSL 连接上的入侵事件请求。
- `python_client/estreamer_connection.py`

  此 Python 脚本会连接到 eStreamer 服务器。它对于 `estreamer_client.py` 是必需的。

配置用于 eStreamer 标准客户端的通信

标准客户端使用安全套接字层 (SSL) 进行数据通信。您必须在打算用作客户端的计算机上安装 OpenSSL，并根据环境对其进行适当配置。

注释　对于 Linux 操作系统上的初始安装，必须将 `libssl-dev` 组件作为此下载的一部分进行安装。

要在您的客户端上设置 SSL，请执行以下操作：

步骤 1　请从 http://openssl.org/source/ 下载 OpenSSL。

步骤 2　将源解压到 `/usr/local/src`。

步骤 3　通过运行配置脚本来配置源。

步骤 4　制作并安装编译源。

创建用于标准客户端的证书

许可证：任意

在使用标准客户端之前，您需要在管理中心或受管设备上为您想要其运行客户端的计算机创建一个证书。然后将该证书文件下载到客户端计算机上，并用它创建证书 (`server.crt`) 和 RSA 密钥文件 (`server.key`)。

要创建标准客户端的证书，请执行以下操作：

访问权限：管理员

步骤 1　选择**系统 (System) > 集成 (Integration) > eStreamer**。

系统将显示 eStreamer 页面。

步骤 2　点击**创建客户端 (Create Client)**。

系统将显示“创建客户端”(Create Client) 页面。

步骤 3　在**主机名 (Hostname)** 字段中，输入运行 eStreamer 客户端的主机的主机名称或 IP 地址。

注释　如果使用主机名，则主机输入服务器**必须**能够将主机解析为 IP 地址。如果尚未配置 DNS 解析，应先配置解析或使用 IP 地址。

步骤 4　如果要对证书文件进行加密，请在**密码 (Password)** 字段中输入密码。

步骤 5　单击**保存**。

eStreamer 服务器允许客户端计算机访问管理中心上的 8302 端口，并创建在客户端-服务器身份验证过程中使用的身份验证证书。系统再次显示“ eStreamer 客户端”(eStreamer Client) 页面，新的客户端将在“**eStreamer 客户端”(eStreamer Client)** 下列出。

步骤 6　点击证书文件旁边的下载图标 ( )。

步骤 7　将证书文件保存至客户端计算机用于 SSL 身份验证的目录。

客户端现在可以连接到管理中心。

提示 要撤消客户端的访问权限，请点击想要移除的主机旁的删除图标 ( )。请注意，无需重启管理中心上的主机输入服务；访问权限将立即撤消。

加载用于 Python 标准客户端的通用前提条件

在运行 eStreamer Python 参考客户端之前，您必须？？？

加载用于 Perl 标准客户端的通用前提条件

在运行 eStreamer Perl 标准客户端之前，必须在客户端计算机上安装 `IO::Socket::SSL` Perl 模块。您可以手动安装该模块或用 `cpan` 进行安装。

注释 如果客户端计算机上没有安装 `Net::SSLeay` 模块，请也安装该模块。与 OpenSSL 进行通信需要使用 `Net::SSLeay`。

您也需要安装并配置 OpenSSL，以支持与 eStreamer 服务器的 SSL 连接。有关详细信息，请参阅配置用于 eStreamer 标准客户端的通信，第 6-7 页。

加载用于 Perl SNMP 标准客户端的前提条件

在运行 Perl 标准客户端的 eStreamer SNMP 模块之前，必须先在客户端计算机上安装客户端操作系统可用的最新 `net-snmp` Perl 模块。

下载并解压缩标准客户端

您可以从思科支持网站下载包含eStreamer 标准客户端的 `EventStreamerSDK.zip` 文件。

将压缩文件解压到运行 Linux 操作系统的计算机（打算用于运行客户端的计算机）上。

了解 Perl 测试脚本请求的数据

默认情况下，当您使用标准客户端中的 `ssl_test -o` 设置时，您请求下表中所示的数据。

表 6-3 输出插件进行的默认请求

此语法...	调用插件...	并发送...	以请求以下数据...
`./ssl_test.pl` *`eStreamerServerName`* `-h HostIPAddresses`	不适用	主机请求，消息类型 5，将位 11 设置为 `1`	主机数据（请参阅主机数据和多主机数据消息格式，第 2-28 页）
`./ssl_test.pl` *`eStreamerServerName`* `-d "Global \ domain \ subdomain"`	不适用	指定域或子域的事件流请求。	流传输指定域的事件信息（请参阅域流传输请求消息格式，第 2-32 页）

表 6-3　　输出插件进行的默认请求 （续）

此语法...	调用插件...	并发送...	以请求以下数据...
`./ssl_test.pl` *eStreamerServerName* `-o print -f` *TextFile*	OutputPlugins/print.pm	事件流请求，消息类型 2，将位 2 和 20-24 设置为 1	事件数据（请参阅事件流请求消息格式，第 2-11 页、关联策略记录，第 3-26 页、关联规则记录，第 3-27 页、发现事件的元数据，第 4-5 页、按事件类型划分的主机发现结构，第 4-42 页和按事件类型划分的用户数据结构，第 4-58 页） eStreamer 传输类型 1 入侵事件，因为已在事件流请求上设置位 2。
`./ssl_test.pl` *eStreamerServerName* `-o pcap -f` *TargetPCAPFile*	OutputPlugins/pcap.pm	事件流请求，消息类型 2，将位 0 和 23 设置为 1	数据包数据（请参阅事件数据消息格式，第 2-16 页和数据包记录 4.8.0.2+，第 3-5 页） eStreamer 仅传输数据包数据，因为已在事件流请求上设置位 0。
`./ssl_test.pl` *eStreamerServerName* `-o csv -f` *CSVFile*	OutputPlugins/csv.pm	事件流请求，消息类型 2，将位 2 和 23 设置为 1	入侵事件数据（请参阅事件数据消息格式，第 2-16 页和入侵事件记录 7.1+，第 3-7 页） eStreamer 传输类型 1 入侵事件，因为已在事件流请求上设置位 2。
`./ssl_test.pl` *eStreamerServerName* `-o snmp -f` *SNMPServer*	OutputPlugins/snmp.pm	事件流请求，消息类型 2，将位 2、20 和 23 设置为 1	入侵事件数据（请参阅事件数据消息格式，第 2-16 页和入侵事件记录 7.1+，第 3-7 页） eStreamer 传输类型 1 入侵事件，因为已在事件流请求上设置位 2。
`./ssl_test.pl` *eStreamerServerName* `-o syslog`	OutputPlugins/syslog.pm	事件流请求，消息类型 2，将位 2、20 和 23 设置为 1	入侵事件数据（请参阅事件数据消息格式，第 2-16 页和入侵事件记录 7.1+，第 3-7 页） eStreamer 传输类型 1 入侵事件，因为已在事件流请求上设置位 2。
`./ssl_test.pl` *eStreamerServerName* `json=<filename>`	不适用	事件流请求，消息类型 2，将位 23 设置为 1，并将所有其他位设置为 0。发送名为 <filename> 的 JSON 文件	提供的 JSON 格式的入侵、连接和文件事件数据。

修改 Perl 测试脚本请求的数据类型

`SFStreamer.pm` Perl 模块可定义多个您可以在示例脚本中用于请求数据的请求标志变量。下表指出在事件流请求消息中设置每个请求标志需要调用什么请求标志变量。如果您想用其中一个输出模块请求不同的数据，您可以编辑该模块中的 `$FLAG` 设置。

有关请求标志及其请求的数据以及与每个标志相对应的产品版本的详细信息，请参阅请求标志，第 2-12 页。

表 6-4 示例脚本中使用的请求标志变量

变量	设置请求标志...	以请求以下数据...
$FLAG_PKTS	0	数据包数据
$FLAG_METADATA	1	版本 1 元数据
$FLAG_IDS	2	类型 1 入侵事件
$FLAG_RNA	3	版本 1 发现事件
$FLAG_POLICY_EVENTS	4	版本 1 关联事件
$FLAG_IMPACT_ALERTS	5	入侵影响警报
$FLAG_IDS_IMPACT_FLAG	6	类型 7 入侵事件
$FLAG_RNA_EVENTS_2	7	版本 2 发现事件
$FLAG_RNA_FLOW	8	版本 1 连接数据
$FLAG_POLICY_EVENTS_2	9	版本 2 关联事件
$FLAG_RNA_EVENTS_3	10	版本 3 发现事件
$FLAG_HOST_ONLY	11	与 $FLAG_HOST_SINGLE（用于一个主机）或 $FLAG_HOST_MULTI（用于多个主机）一起发送时，只有主机数据，无事件数据
$FLAG_RNA_FLOW_3	12	版本 3 连接数据
$FLAG_POLICY_EVENTS_3	13	版本 3 关联事件
$FLAG_METADATA_2	14	版本 2 元数据
$FLAG_METADATA_3	15	版本 3 元数据
$FLAG_RNA_EVENTS_4	17	版本 4 发现事件
$FLAG_RNA_FLOW_4	18	版本 4 连接数据
$FLAG_POLICY_EVENTS_4	19	版本 4 关联事件
$FLAG_METADATA_4	20	版本 4 元数据
$FLAG_RUA	21	用户活动事件
$FLAG_POLICY_EVENTS_5	22	版本 5 关联事件
$FLAGS_SEND_ARCHIVE_TIMESTAMP	23	包含将事件存档供 eStreamer 服务器处理时应用的时间戳的扩展事件报头
$FLAG_RNA_EVENTS_5	24	版本 5 发现事件
$FLAG_RNA_EVENTS_6	25	版本 6 发现事件
$FLAG_RNA_FLOW_5	26	版本 5 连接数据
$FLAG_EXTRA_DATA	27	入侵事件额外数据记录
$FLAG_RNA_EVENTS_7	28	版本 7 发现事件
$FLAG_POLICY_EVENTS_6	29	版本 6 关联事件
$FLAG_DETAIL_REQUEST	30	向 eStreamer 发出的扩展请求

小心 在所有事件类型中，在版本 5.x 之前，标准客户端都将 detection engine ID 字段标记为 sensor ID。

运行 eStreamer Perl 标准客户端

eStreamer Perl 标准客户端脚本设计用于配备 Linux 内核的 64 位操作系统，但是，只要客户端计算机满足设置eStreamer 标准客户端，第 6-6 页中规定的前提条件，该标准客户端应该可以在任何基于 POSIX 的 64 位操作系统上使用。

有关详细信息，请参阅以下各节：

用主机请求测试经由 SSL 的客户端连接

您可以使用 `ssl_test.pl` 脚本测试 eStreamer 服务器与 eStreamer 客户端之间的连接。`ssl_test.pl` 脚本可处理任何记录类型并将其打印到 STDOUT 或您指定的输出插件。当您使用不具有输出选项的 `-h` 选项时，它会将指定主机的主机数据流传输到您的终端。

注释　如果不将数据包数据定向到输出插件，则无法使用此脚本来流传输数据包数据，因为将原始数据包数据打印到 STDOUT 会干扰您的终端。

通过以下语法用 `ssl_test.pl` 脚本将主机数据发送到标准输出：

```
./ssl_test.pl eStreamerServerIPAddress -h HostIPAddresses
```

例如，通过与 IP 地址为 10.10.0.4 的 eStreamer 服务器的连接测试 10.0.0.0/8 子网中主机的主机数据接收情况：

```
./ssl_test.pl 10.10.0.4 -h 10.0.0.0/8
```

用标准客户端捕获 PCAP

您可以用标准客户端捕获 PCAP 文件中流传输的数据包数据，以查看客户端接收的数据的结构。请注意，使用 `-o pcap` 输出选项时，必须使用 `-f` 来指定目标文件。

通过以下语法用 `ssl_test.pl` 脚本捕获 PCAP 文件中流传输的数据包：

```
./ssl_test.pl eStreamerServerIPAddress -o pcap -f ResultingPCAPFile
```

例如，用 IP 地址为 10.10.0.4 的 eStreamer 服务器流传输的事件创建名为 `test.pcap` 的 PCAP 文件：

```
./ssl_test.pl 10.10.0.4 -o pcap -f test.pcap
```

用标准客户端捕获 CSV 记录

您也可以用标准客户端捕获CSV文件中流传输的入侵事件数据，以查看客户端接收的数据的结构。

使用以下语法运行 `streamer_csv.pl` 脚本：

```
./ssl_test.pl eStreamerServerIPAddress -o csv -f ResultingCSVFile
```

例如，用 IP 地址为 10.10.0.4 的 eStreamer 服务器流传输的事件创建名为 `test.csv` 的 CSV 文件：

```
./ssl_test.pl 10.10.0.4 -o csv -f test.csv
```

用标准客户端将记录发送到 SNMP 服务器

您也可以使用标准客户端将入侵事件数据流传输到 SNMP 服务器。使用 `-f` 选项指示应接收事件的 SNMP 陷阱服务器的名称。请注意，此输出方法需要路径中有一个名为 `snmptrapd` 的二进制文件，因此只能用于 UNIX 类系统。

使用以下语法将入侵事件发送到 SNMP 服务器:

```
./ssl_test.pl eStreamerServerIPAddress -o snmp -f SNMPServerName
```

例如，用 IP 地址为 10.10.0.4 的 eStreamer 服务器流传输的事件将事件发送到 IP 地址为 10.10.0.3 的 SNMP 服务器:

```
./ssl_test.pl 10.10.0.4 -o snmp -f 10.10.0.3
```

用标准客户端将事件记录到系统日志中

您也可以使用标准客户端将入侵事件流传输到客户端上的本地系统日志服务器。

使用以下语法将事件发送到系统日志:

```
./ssl_test.pl eStreamerServerIPAddress -o syslog
```

例如，记录 IP 地址为 10.10.0.4 的 eStreamer 服务器流传输的事件:

```
./ssl_test.pl 10.10.0.4 -o syslog
```

连接到 IPv6 地址

您可以使用标准客户端通过主管理接口连接到具有 IPv6 地址的管理中心。必须在客户端计算机上安装 Socket6 和 IO::Socket::INET6 Perl 模块，并使用 `-ipv6` 选项或其简称 `-i`。

通过以下语法用 ssl_test.pl 脚本指定 IPv6 地址:

```
./ssl_test.pl -ipv6 eStreamerServerIPAddress
```

或

```
./ssl_test.pl -i eStreamerServerIPAddress
```

例如，要连接到 IPv6 地址为 `2001:470:e09c:20:7c1e:5248:1bf7:2ea0` 的管理中心，请使用以下命令:

```
./ssl_test.pl -ipv6 2001:470:e09c:20:7c1e:5248:1bf7:2ea0
```

运行 eStreamer Python 标准客户端

eStreamer Python 标准客户端脚本演示了一种从 Cisco Secure Firewall 系统 管理中心 eStreamer 服务获取事件数据的更简单的新机制。事件信息不会以二进制数据形式返回，而是以 JSON 或 CSV 等格式的完全限定文本形式返回。

此 API 仅支持请求三种事件类型的信息：连接事件、入侵事件和文件事件。对于所有其他事件，您必须使用单独的客户端和《eStreamer 集成指南》中介绍的常规方法。

Python 代码提供了一个使用新机制的简单客户端示例。Perl 示例客户端代码也已修改为可选择性地使用此新机制（使用 `json=<filename>` 命令行参数），但 Python 示例更容易理解，因为它仅支持新机制。

示例用法：

```
./estreamer_client.py --server 192.168.1.1 --configfile json_request.json --pkcs12_file
192.168.1.2_8.pkcs12 --start all
```

表 6-5　　Python 脚本参数

此参数...	以下...
-h, --help	是否显示了此帮助消息并退出。
--server SERVER	指定 eStreamer 服务器的 IP 地址。此 IP 地址必须可从运行客户端的计算机进行访问。
--port PORT	指定 eStreamer 服务器的端口。默认值为 8302
--configfile CONFIGFILE	提供 JSON 格式的配置文件。有关详细信息，请参阅JSON 文件的格式，第 2-5 页。
--pkcs12_file PKCS12_FILE	向 eStreamer 服务器提供用于身份验证的 Pkcs12 文件。
--pkcs12_password PKCS12_PASSWORD	如有必要，提供 Pkcs12 密码。
--debug	启用调试模式。
--start {now,all,bookmark}	流媒体事件的开始时间
--outfile OUTFILE	用于存储事件的输出文件。默认值为打印到标准输出

数据结构示例

本附录包含选定的入侵事件、关联事件和发现事件的数据结构示例。每个示例均以二进制格式显示，以清楚地展示每一个位是如何设置的。

有关详细信息，请参阅以下各节：

入侵事件数据结构示例

本节包含可能由 eStreamer 传输的入侵事件的数据结构示例。提供以下示例：

管理中心 5.4+ 的入侵事件示例

下图显示了一个事件记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	0	1	1	0
3	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
5	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0
11	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	1	0	1	1	1	0	0	1	1	1	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1
15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1	1	1	0	1	1	1	0	1	1	1	0	0
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1	1	0	0	0	1	0	0	0	0	1	0	1
20	1	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	0	0	0	1	1	1	1	1	1	0	0	1	0	0	0	0
21	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
24	1	0	1	0	1	0	0	0	0	0	0	1	1	0	0	1	1	1	0	1	0	0	1	1	0	1	1	1	1	1	1	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	0	0
	1	0	1	0	0	1	0	0	1	0	0	0	0	1	0	1	1	1	0	1	0	0	0	0	0	1	1	1	0	0	0	1
	1	0	0	0	1	1	1	1	0	0	0	0	1	1	1	0	1	0	0	0	1	0	0	1	1	0	1	0	0	0	1	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	1	1	1
27	0	1	1	1	0	1	1	1	0	0	1	1	0	1	0	1	1	0	0	1	0	1	1	0	1	0	1	0	0	1	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
30	1	1	0	0	0	0	0	1	0	1	0	0	0	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	1	0
	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	0	0
	1	0	1	0	0	1	0	1	1	1	1	1	0	1	1	0	1	0	1	1	0	0	1	1	0	0	0	0	1	0	0	1
	0	1	0	0	0	0	0	1	1	0	0	1	0	1	1	1	1	0	0	1	1	1	1	1	0	0	0	1	0	1	0	0
31	0	1	1	0	1	0	0	1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	1	0	1	0
	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	1	0	1	0	0	0	1	0	1	0	0	1	0	0	0	0	1	0	1	0	0	1	1	0	0	1	1	0	1
	1	0	1	0	1	0	1	1	0	0	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1	1	0	0
32	0	1	1	0	1	0	0	1	0	0	0	1	0	1	0	1	1	0	1	0	1	0	0	1	0	0	0	1	1	0	1	0
	1	1	1	1	1	1	1	0	0	0	1	1	1	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	1	0	1	0	0	0	1	0	1	0	0	1	0	0	0	0	1	0	1	0	0	1	1	0	0	1	1	0	1
	1	0	1	0	1	0	1	1	0	0	0	1	0	1	0	0	1	1	0	0	1	1	1	1	1	0	0	1	1	1	0	0
33	0	0	1	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	0	1	1	0	0	0	0
	1	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1
	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	0	0	0	1	1	0	1	0	0	1	0	0	1	1
34	0	0	1	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	0	1	1	0	0	0	0
	1	1	1	1	1	1	1	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1
	1	0	1	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	1

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	1	0	0	1	1	1	1	1	0	1	1	1	1	1	1	0	0	1	0	0	0	1	1	0	1	0	0	1	0	0	1	1
35	0	1	0	1	0	0	1	1	1	0	1	1	0	1	0	0	0	0	1	0	1	1	1	1	0	0	1	0	1	1	1	1
36	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	1	0	0	0	0	1	1	0
37	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
38	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
41	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0																

在上一个示例中，出现以下事件信息：

编号	说明
1	此行的前两个字节表示标准报头值 `1`。接下来的两个字节表示该消息为数据消息（也就是消息类型 4）。
2	此行表示后面的消息长度为 `294` 个字节。
3	这里的第一位是一个标志，表示该报头是一个含有存档时间戳的扩展报头。接下来的 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。该行的其余部分表示记录类型值 `400`，说明这是入侵事件记录。
4	此行表示后面的事件记录长度为 `278` 个字节。

编号	说明
5	此行是保存事件的时间戳。在本例中，事件保存时间为 2014 年 7 月 2 日，星期三，16:11:27。
6	此行留作未来使用，用 0 填充。
7	此行表示块类型为 45，这是版本 5.4+ 的入侵事件记录的块类型。
8	此行表示数据块长度为 278 个字节。
9	此行表示事件是从编号为 5 的传感器收集的。
10	此行表示事件标识号为 65580。
11	此行表示事件发生于 1404317489 秒。
12	此行表示事件发生于 46542 微秒。
13	此行表示规则 ID 号码为 4。
14	此行表示事件是由 ID 号码为 119 的生成器（也就是规则引擎）检测到的。
15	此行表示规则版本号为 1。
16	此行表示分类标识号为 1。
17	此行表示优先级标识号为 3。
18	此行表示源 IP 地址为 10.5.61.220。请注意，此字段可包含 IPv4 或 IPv6 地址。
19	此行表示目标 IP 地址为 10.5.56.133。请注意，此字段可包含 IPv4 或 IPv6 地址。
20	此行的前两个字节表示源端口号为 33018，接下来的两个字节表示目标端口号为 8080。
21	此行的第一个字节表示 TCP (6) 是事件中使用的协议。第二个字节为影响标志，由于第二位为 1，表示此事件为红色（易受攻击）事件；表示源主机或目标主机位于受系统监控的网络中，源主机或目标主机存在于网络映射中，并且在此事件中，?»机或目标主机在端口上运行服务器；因为第二和第三个标志均为 1，因此这是一个可能易受攻击的橙色事件。此行的第三个字节表示影响，该字节值为 2，表示事件为可能易受攻击的橙色事件。最后一个字节表示事件未被阻止。
22	此行包含 MPLS 标签（若有）。
23	此行的前两个字节表示 VLAN ID 为 0。最后两个字节保留，并设置为 0。
24	此行包含入侵策略的唯一 ID 号码。
25	此行包含用户的内部标识号。因为没有适用的用户，因此该行全部为 0。
26	此行包含 Web 应用的内部标识号，即 847。
27	此行包含客户端应用的内部标识号，即 2000000676。
28	此行包含应用协议的内部标识号，即 676。
29	此行包含访问控制规则的唯一标识符，即 1。
30	此行包含访问控制策略的唯一标识符。
31	此行包含入口接口的唯一标识符。
32	此行包含出口接口的唯一标识符。因为此事件已被阻止。
33	此行包含入口安全区的唯一标识符。
34	此行包含出口安全区的唯一标识符。
35	此行包含与入侵事件关联的连接事件的 Unix 时间戳。
36	此行的前两个字节表示生成连接事件的受管设备上的 Snort 示例的数字 ID。其余两个字节表示用于区别在同一秒内发生的连接事件的值。

编号	说明
37	此行的前两个字节表示源主机的国家/地区代码。其余两个字节表示目标主机的国家/地区代码。
38	此行的前两个字节包含与此事件关联的威胁的 ID 号码。其余两个字节包含流量通过的安全情景（虚拟防火墙）的 ID 号码的开头。
39	此行包含流量通过的安全情景（虚拟防火墙）的 ID 号码的其余部分。
40	此行的前两个字节包含流量通过的安全情景（虚拟防火墙）的最后两个字节。接下来的两个字节包含 SSL 服务器证书的 SHA1 散列的开头（若使用 SSL）。
41	此行包含 SSL 服务器证书的 SHA1 散列的其余部分（若使用 SSL）。
42	此行的前两个字节包含 SSL 服务器证书的 SHA1 散列的最后两个字节。接下来的两个字节包含实际采取的 SSL 操作。由于此连接未使用 SSL，所以其值为 0•
43	此行的前两个字节包含 SSL 流状态。由于此连接未使用 SSL，所以其值为 0。接下来的两个字节包含与此事件关联的网络分析策略的 UUID 的前两个字节。
44	此行包含与此事件关联的网络分析策略的 UUID 的其余部分。

入侵影响警报示例

下图显示了一个入侵影响警报记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	1	0	1	0	0	0
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
9	0	1	0	0	0	0	0	1	1	0	0	1	1	0	1	1	0	1	1	0	1	1	1	1	0	0	1	0	1	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
11	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	1	1	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0
15	0	1	0	1	0	1	1	0	0	1	1	1	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1	0
	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	0
	0	1	1	0	1	1	0	0	0	1	1	0	0	1	0	1																

在上一个实例中，出现以下信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（消息类型 4）。
2	此行表示后面的消息长度为 58 个字节。
3	这里的第一位是一个标志，表示该报头不是一个含有存档时间戳的扩展报头。接下来的 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。该行的其余部分表示记录类型值 9，说明这是入侵影响警报记录。
4	此行表示后面的数据长度为 50 个字节。
5	此行包含值 20，表示后面跟着一个入侵影响警报数据块。
6	此行表示影响警报块的长度（包括影响警报块报头）为 50 个字节。
7	此行表示事件标识号为 201256。
8	此行表示事件是从编号为 2 的设备收集的。
9	此行表示事件发生于 1087223700 秒。
10	此行表示与事件相关联的影响级别是 1（红色，易受攻击）。
11	此行表示与违规事件关联的 IP 地址为 172.16.1.22。
12	此行表示不存在与违规关联的目标 IP 地址（值设置为 0）。
13	此行表示后面跟着一个字符串块，包含字符串块长度和文本字符串（在本例中，该文本字符串包含影响名称）。有关字符串块的详细信息，请参阅字符串数据块，第 3-59 页。
14	此行表示字符串块的总长度（包括字符串块指示符和长度）为 18 个字节。其中，影响描述占 10 个字节，字符串报头占 8 个字节。
15	此行表示影响的描述为“Vulnerable”（易受攻击）。

数据包记录示例

下图显示了一个数据包记录示例:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	1	1	0	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	1	0	1
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	0	1	1	0	1	1	0	0	1	1	0
7	0	0	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	0	1	0
8	0	0	1	1	1	1	1	1	0	0	0	0	0	1	0	0	0	1	1	1	1	1	1	1	0	1	1	1	0	1	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	1	0	0	1	1	1	0	1
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	1	1	0	0	1
12	0	0	1	1	0	0	0	0	0	1	1	1	1	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0
	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	0	0	0	0	0

在上一个示例中，出现以下数据包信息:

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（消息类型 4）。
2	此行表示后面的消息长度为 989 个字节。
3	这里的第一位是一个标志，表示该报头不是一个含有存档时间戳的扩展报头。接下来的 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。该行的其余部分表示记录类型值 2，说明这是数据包记录。
4	此行表示后面的数据包记录长度为 981 个字节。
5	此行表示事件是从编号为 3 的设备收集的。
6	此行表示事件标识号为 195430。
7	此行表示事件发生于 10572378 秒。
8	此行表示数据包采集于 10572380 秒。
9	此行表示数据包采集于 254365 微秒。

编号	说明
10	此行表示链路类型为 1（以太网层）。
11	此行表示后面的数据包数据长度为 953 个字节。
12	此行及后面一行显示实际负载数据。请注意，实际数据为 953 个字节，此示例中将其截断，以便展示。

分类记录示例

下图显示了一个分类记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	1	0	1	0	0	0	1	1	1	0	0	1	0
	0	1	1	0	1	1	1	1	0	1	1	0	1	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0
	0	0	1	0	1	1	0	1	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	0
	0	1	1	0	1	0	0	1	0	1	1	1	0	1	1	0	0	1	1	0	1	0	0	1	0	1	1	1	0	1	0	0
7	0	1	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	1	0	1	0	0	0	0	0	1
	0	0	1	0	0	0	0	0	0	1	0	0	1	1	1	0	0	1	1	0	0	1	0	1	0	1	1	1	0	1	0	0
	0	1	1	1	0	1	1	1	0	1	1	0	1	1	1	1	0	1	1	1	0	0	1	0	0	1	1	0	1	0	1	1
	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	0	0	1	1	1	0	0	1	0	0	1	1	0	1	1	1	1
	0	1	1	0	1	0	1	0	0	1	1	0	0	0	0	1	0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0
	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	1	0	1	1	1	0	0	1	1	0	0	1	0	0	0	0	0
	0	1	0	0	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	1	0	1	0	0	0	1	1	0	0	1	0	1
	0	1	1	0	0	0	1	1	0	1	1	1	0	1	0	0	0	1	1	0	0	1	0	1	0	1	1	0	0	1	0	0
8	1	0	0	1	1	1	0	1	1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	1	0	1	0	0	0
	1	1	0	0	1	0	1	1	1	0	1	0	0	0	1	0	0	0	0	1	0	0	0	1	1	1	0	1	1	0	0	1
	1	0	0	0	1	0	0	1	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	1	0	1	0	1	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	1
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

在上一个示例中，出现以下事件信息：

编号	说明
1	此行的前两个字节表示标准报头值 `1`。接下来的两个字节表示该消息为数据消息（消息类型 4）。
2	此行表示后面的消息长度为 `92` 个字节。
3	这里的第一位是一个标志，表示该报头不是一个含有存档时间戳的扩展报头。接下来的 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。该行的其余部分表示记录类型值 `67`，说明这是分类记录。
4	此行表示后面的分类记录长度为 `84` 个字节。
5	此行表示分类 ID 为 `35`。
6	此行的前两个字节表示其后的分类名称长度为 `15` 个字节。接下来的两个字节开始显示分类名称自身，（在本例中为“trojan-activity”（特洛伊木马事件）。
7	此行的第一个字节是第 6 行描述的分类名称的继续。此行中接下来的两个字节表示其后的分类描述长度为 `29` 个字节。其余字节开始分类描述（在本例中为 `A Network Trojan was Detected`（检测到网络特洛伊木马））。
8	此行表示充当分类的唯一标识符的分类 ID 号码。
9	此行表示充当分类修订的唯一标识符的分类修订版本 ID 号码（空值，因为该分类没有修订）。

优先级记录示例

以下示例显示了一个优先级记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	1	0	0	0	0	1	1	0	1	0	0	1
	0	1	1	0	0	1	1	1	0	1	1	0	1	0	0	0																

在上一个示例中，出现以下事件信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（消息类型 4）。
2	此行表示后面的消息长度为 16 个字节。
3	此行表示记录类型值 4，说明这是优先级记录。
4	此行表示后面的优先级记录长度为 8 个字节。
5	此行表示优先级 ID 为 1。
6	此行的前两个字节表示优先级名称中包含四个字节。接下来的两个字节以及后面一行的两个字节显示优先级名称自身（“高”）。

规则消息记录示例

以下示例显示了一个规则记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	1	0	1	0	0	1	0	1
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	1	0	1	1	0	1	0	0	1	0	1
9	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	1	0	0	1	1	1	0	0	1	1	1	0	0	1	0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1
	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	1
	1	0	0	0	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	0	0	1	1	1	1	0	0	0	1	1
10	0	1	1	0	1	1	0	1	1	1	0	1	0	0	1	0	1	0	1	1	0	1	1	0	0	0	1	1	0	1	1	1
	0	0	1	0	1	0	1	0	1	0	1	0	0	1	0	1	0	0	1	0	0	1	1	0	0	0	0	1	1	1	1	1
	0	0	0	1	0	0	0	1	1	1	1	0	0	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	1	0	0	1
	1	0	0	0	0	1	0	0	1	0	0	0	1	1	1	1	0	1	1	0	1	0	0	1	1	1	1	0	0	0	1	1
11	0	1	1	0	1	1	0	1	1	1	0	1	0	0	1	0	0	1	0	0	0	0	0	1	0	1	0	1	0	0	0	0
	0	1	0	1	0	0	0	0	0	0	1	0	1	1	0	1	0	1	0	0	0	1	0	0	0	1	0	0	0	1	0	1
	0	1	0	1	0	1	0	0	0	1	0	0	0	1	0	1	0	1	0	0	0	0	1	1	0	1	0	1	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	0	0	0	1	0	0	0	1	0	0	1	1	1	0	0	1	0	1	0	0	1	1
	0	0	1	0	0	0	0	0	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	1	1	1	0	0	0	1
	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	1	0	1	1	1	0	0	1	1	0	1	1	1	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	1	1	1	1	0	1	1	1	0	0	1	0
	0	0	1	0	0	0	0	0	0	1	1	1	0	0	0	0	0	1	1	0	1	1	1	1	0	1	1	1	0	1	0	0
	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	1	1	0	1	0	0	0	1	1	0	1	0	0	1
	0	1	1	0	0	0	0	0	1	0	1	1	0	1	1	0	0	0	0	1	0	0	0	0	0	1	1	0	1	1	0	1
	0	1	1	0	0	0	0	1	0	1	1	0	1	1	0	0	0	1	1	1	0	1	1	1	0	1	1	0	0	0	0	1
	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	1	0	0	1	0	0	0	0	0	0	1	0	1	0	0	1	1
	0	1	1	0	0	0	0	1	0	1	1	0	0	1	1	0	0	1	1	0	0	1	0	1	0	1	0	0	0	1	1	1
	0	1	1	1	0	1	0	1	0	1	1	0	0	0	0	1	0	1	1	1	0	0	1	0	0	1	1	0	0	1	0	0
	0	0	1	0	0	0	0	0	0	1	1	1	0	1	0	0	0	1	1	0	0	1	1	1	0	0	1	0	0	0	0	0
	0	1	1	0	0	1	0	0	0	1	1	0	1	1	1	1	0	1	1	0	1	1	0	1	0	1	1	0	0	0	0	1
	0	1	1	0	1	0	0	1	0	1	1	0	1	1	1	0	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1
	0	0	1	1	0	1	1	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0	0	1	1	0	0	0	1	1
	0	1	1	0	1	1	1	0																								

在上一个示例中，出现以下事件信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（也就是消息类型 4）。
2	此行表示后面的消息长度为 129 个字节。
3	这里的第一位是一个标志，表示该报头不是一个含有存档时间戳的扩展报头。接下来的 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。该行的其余部分表示记录类型值 66，说明这是规则消息记录。
4	此行表示后面的规则消息记录长度为 121 个字节。
5	此行表示生成器标识号为 1，表示规则引擎。
6	此行表示规则标识号为 28069。
7	此行表示规则版本号为 1。
8	此行表示向 Cisco Secure Firewall 系统呈现的规则标识号为 28069。
9	此行的前两个字节表示规则文本名称中包含 71 个字节。接下来的两个字节开始显示规则的唯一标识符号码。
10	此行的前两个字节完成规则的唯一标识符号码。接下来的两个字节开始显示规则修订版的唯一标识符号码。
11	此行的前两个字节完成规则修订版的唯一标识符号码。接下来的两个字节开始显示规则消息自身的文本。传输的规则消息的完整文本为：APP-DETECT DNS request for potential malware SafeGuard to domain 360.cn（潜在恶意软件 SafeGuard 向域 360.cn 发出的 APP-DETECT DNS 请求）。

6.1.x 的连接统计数据块示例

下图显示了一个连接统计记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	1	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	1	1	1	1	0	0
5	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0	0	0	1	1	0	1	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	0	1	1
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
15	1	1	0	1	0	0	0	1	1	0	0	0	0	1	0	0	1	1	1	1	1	0	1	1	0	1	0	1	0	1	1	1
16	0	0	0	0	1	0	0	0	1	0	1	1	1	0	1	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1	1
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
21	0	1	0	1	1	0	0	1	1	1	1	0	0	1	0	0	0	1	0	1	0	0	0	0	0	1	0	1	1	1	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	0	1	1	0	0	0	1	0	1	1	0	1	1	1	1	1	0	0	0	1	1	1	0	1	1	1	0	1
	1	1	1	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	1	1	1	1	0
22	0	1	1	0	0	0	0	0	1	1	0	1	0	1	0	1	0	0	0	0	1	1	0	0	1	0	0	0	0	0	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0
	1	1	0	1	0	1	1	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0
23	0	1	0	1	1	0	0	1	1	0	0	1	0	0	0	1	0	0	1	0	0	1	1	0	1	1	0	1	1	1	1	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	0	1	1	0	0	0	1	0	1	1	0	1	1	1	1	1	0	0	0	1	1	1	0	1	1	1	1	1
	1	1	1	1	0	1	1	1	0	0	1	1	0	0	0	1	1	0	1	0	1	0	0	0	0	1	0	1	1	1	1	0
24	0	1	1	0	0	0	0	0	1	0	0	0	1	1	0	1	0	1	1	0	1	1	0	0	1	1	1	1	0	1	0	0
	0	1	0	0	0	1	0	0	1	0	0	1	0	0	1	1	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	0	1	1	0	0	0	0	1	0	0	0	0	1	1	1	0	0	0	0	1	0	0	1	1	0	1	1	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	1	1	0	1	0	1	1	0	1	0	1	0	0	0	1	1	1	1	1	0	0	0	0	0	0	0	0	0	1	0	0	0
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	1	0	1	0	1	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	1	0	1
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	1	0	0	1	0	0	0	0	0	1	1	0	0	0	0	1	0	0	1	0	1	0	1	1	1	1	1	0	1	0	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	0	1	0	1	1	1	1	1	1	0	1	0	0	1	1	1	0	0	0	0	1	1	1	0	0	1	1	1	0	1
29	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	1	1
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
32	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	0	1	0	1	0	1	1	0	0	0	0	1	0	1	0
33	0	0	0	0	0	0	0	1	1	0	1	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
34	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
35	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	0	1	1	1	0	0
36	0	1	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0
37	0	0	1	1	0	0	1	1	0	1	0	1	0	1	1	1	1	1	1	1	1	0	1	1	1	0	0	0	1	1	1	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
38	0	0	1	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
39	0	0	0	0	1	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
40	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0
41	1	1	0	0	1	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
42	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
43	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
44	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
45	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
46	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
47	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
48个	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0
49	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
50	0	1	1	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
51	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
52	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1
53	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
54	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
55	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
56	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
57	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
58	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
59	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
60	0	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
61	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
62	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
63	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
64	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
65	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
66	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
67	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
68	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
69	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0
70	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
71	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
72	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
73	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
74	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
75	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
76	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
77	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
78	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
79	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
80	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
81	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
82	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
83	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
84	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
85	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
86	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
87	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
88	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
89	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
90	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
91	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
92	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
93	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
94	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
95	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
96	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	1	0	0	1	1	1	0	0	1	1	1	1	0	0	0	1	1	0	0	1	0	1	1	0	1	1	1	0	0	0	0
	0	1	1	1	1	0	0	0	0	1	0	0	0	0	1	0	0	0	0	1	0	0	0	1	1	1	1	0	0	1	1	0
	1	0	1	0	1	0	0	1	1	0	0	1	1	0	1	1	1	1	0	0	1	1	0	1	1	0	1	1	0	0	0	1
97	1	0	0	1	1	1	0	0	1	0	1	1	0	1	0	1	0	1	0	1	0	0	1	1	1	1	1	1	1	1	0	1
98	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
99	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
100	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
101	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
102	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
103	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0
104	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
105	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
106	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
107	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0								

在上一个示例中，出现以下事件信息:

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（也就是消息类型 4）。
2	此行表示后面的消息长度为 716 个字节。
3	这里的第一位是一个标志，表示该报头是一个含有存档时间戳的扩展报头。接下来的 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。该行的其余部分表示记录类型值 71，说明这是连接统计记录。
4	此行表示后面的事件记录长度为 700 个字节。
5	此行是保存事件的时间戳。在本例中，其保存时间为 2016 年 10 月 10 日（星期一）08:48:52（上午）。
6	此行留作未来使用，用 0 填充。
7	此行提供生成发现事件的设备的 ID 号码。设备 ID 为 1•
8	此行用作旧版 (IPv4) IP 地址。此行的值全部为 0，因为尚未填充，而 IPv4 地址存储在 IPv6 字段中。
9	此行包含事件所涉及主机的 MAC 地址。MAC 地址为 00:00:00:00:00:00。
10	此行的前 16 位包含 MAC 地址的其余部分。接下来的 8 位是一个标志，用于指示主机是否具有 IPv6 地址。最后 8 位为空，保留以供将来使用。
11	此行包含事件发生时的 Unix 时间戳。
12	此行包含事件微秒。在本例中，此值为 0。
13	此行包含事件类型。此处的类型为 1003。
14	此行包含事件子类型。在本例中，事件子类型为 1，与事件类型 1003一致，这意味着它是连接统计事件。
15	此行用于文件编号。仅供内部使用。
16	此行用于文件位置。仅供内部使用。
17	此行包含 IPv6 地址。若设置了 Has IPv6 标志，则此字段存在且可使用。在本例中，它包含 IPv6 地址 0:3eb:0:1:d184:fb57:8ba:c00。
18	此行包含块类型。值为 163，表示连接统计数据块类型。
19	此行包含数据块的长度，表示它包含 644 字节的数据。
20	此行提供生成发现事件的设备的 ID 号码。设备 ID 为 1•
21	这包含入口安全区域。此区域为 59e4505c-4493-11e6-a62d-f1dff731a85。
22	这包含出口安全区域。区域为 60d50c80-4493-11e6-9843-84d8d6a3e008。
23	这包含入口接口。此接口为 599126de-4493-11e6-a62d-f1dff731a85e。
24	这包含出口接口。此接口为 608d6cf4-4493-11e6-9843-84d8d6a3e008。
25	此行包含发起连接事件中描述的会话的主机的 IP 地址。此 IP 地址为 172.16.3.5。
26	此行包含对发起主机作出响应的主机的 IP 地址。此 IP 地址为 72.48.149.244。
27	位于发起请求的代理后面的主机的 IP 地址。此地址在本例中为空。
28	此行包含与触发的关联事件相关的规则版本号。此版本号为 00000000-0000-0000-0000-000057e9c39d。
29	这包含触发事件的规则的内部标识符。此规则为 268439603。

编号	说明
30	此行包含触发事件的隧道规则的内部标识符。由于此事件并非由隧道规则触发，因此该值为 0。
31	此行的前两个字节包含规则指定的操作。在本例中，此值为 4，表示该操作为阻止。最后两个字节包含规则原因，在本例中为 64，表示入侵阻止。
32	前两个字节包含规则原因的其余部分。后两个字节包含发起方主机使用的端口 43786。
33	此行的前两个字节包含响应方端口 443。其余两个字节包含 TCP 标志。
34	此行的第一个字节包含协议 6，这表示此事件通过 TCP 发生。其余 24 位包含 Netflow 源 IP 地址的第一部分，即 00000000-0000-0000-0000-000000000000
35	此行的第一个字节包含 Netflow 源的最后 8 位。接下来的两个字节包含生成事件的 Snort 实例的标识符 7。剩余字节包含连接计数器。
36	此行的第一个字节包含连接计数器的剩余部分。最后 24 位包含会话中交换的第一个数据包的 Unix 时间戳开头。此时间戳为 1476103731，表示时间为 2016 年 10 月 10 日星期一上午 8:48:51。
37	第一个字节包含第一个数据包时间戳的其余部分。剩余的三个字节包含会话中要交换的最后一个数据包的时间戳，此时间戳给出的时间为 2016 年 10 月 10 日星期一上午 8:48:51，表示会话持续时间不到一秒。
38	此行的第一个字节包含最后一个数据包时间戳的最后 8 位。剩余的 24 位包含发起主机传输的数据包数量，本例中为 13。
39	此行中的第一个字节是发起方传输的数据包的其余部分。接下来的 24 位包含响应方传输的数据包数量 0。
40	此行中的第一个字节是响应方传输的数据包的其余部分。接下来的 24 位包含发起方传输的字节数 1743。
41	第一个字节是发起方传输字节的末尾，其余 24 位是响应方传输字节 0 的开头。
42	第一个字节是响应方传输字节的末尾，其余 24 位是发起方丢弃的数据包 0 的开头。
43	第一个字节是发起方丢弃的数据包的末尾，其余 24 位是响应方丢弃的数据包 0 的开头。
44	第一个字节是响应方丢弃的数据包的末尾，其余 24 位是发起方丢弃的字节 0 的开头。
45	第一个字节是发起方丢弃的字节的末尾，其余 24 位是响应方丢弃的字节 0 的开头。
46	第一个字节是响应方丢弃的字节的末尾，其余 24 位是应用了速率限制的接口名称 00000000-0000-0000-0000-000000000000 的开头。
47	此行的第一个字节是 QOS 应用接口的其余部分。其余部分是应用于连接的 QOS 规则；因为没有应用于此接口的 QoS 规则，所以 ID 为 0。
48	此行的第一个字节是 QoS 规则 ID 的其余部分。其余部分为登录生成流量的主机的最后一个用户的 ID 编号 16466。
49	此行的第一个字节是用户 ID 的其余部分。其余部分是连接中使用的应用协议的 ID 1122，此值表示连接是 HTTPS 连接。
50	此行的第一个字节是应用协议 ID 的其余部分。其余部分为 URL 类别。
51	此行的第一个字节是 URL 类别的其余部分。其余部分为 URL 信誉，即 0，表示“未知风险”。
52	此行的第一个字节是 URL 信誉的其余部分。其余部分为客户端应用 ID，即 1296，表示“SSL客户端”。

编号	说明
53	此行的第一个字节是客户端应用 ID 的其余部分。其余部分为 Web 应用 ID，即 0，表示“未知”。
54	此行的第一个字节是 Web 应用 ID 的其余部分。此行的其余部分是块类型 0 的开头，表示字符串块类型的开头。
55	此行的第一个字节是字符串块类型的其余部分。其余部分为块长度，表明客户端应用 URL 包含 8 个字节（包括报头和长度），这意味着客户端应用 URL 中没有数据。
56	此行的第一个字节是字符串块长度的其余部分。由于客户端应用 URL 中没有数据，因此，此行的其余部分为块类型 0 的开头，表示 NetBIOS 名称字符串块类型的开头。
57	此行的第一个字节是字符串块类型的其余部分。其余部分为块长度，表明 NetBIOS 名称包含 8 个字节（包括报头和长度），这意味着 NetBIOS 名称中没有数据。
58	此行的第一个字节是字符串块长度的其余部分。由于 NetBIOS 名称中没有数据，因此，此行的其余部分为块类型0的开头，表示客户端应用版本的字符串块类型的开头。
59	此行的第一个字节是字符串块类型的其余部分。其余部分为块长度，表明客户端应用版本包含 8 个字节（包括信头和长度），这意味着客户端应用版本中没有数据。
60	此行包含客户端应用版本块长度的剩余字节。最后三个字节是与连接事件关联的第一个监控规则的 ID 268439553。
61	此行包含第一个监控规则的 ID 的最后一个字节。其余三个字节是第二个监控规则的 ID，即 0。
62	此行包含第二个监控规则的 ID 的最后一个字节。其余三个字节是第三个监控规则的 ID，即 0。
63	此行包含第三个监控规则的 ID 的最后一个字节。其余三个字节是第四个监控规则的 ID，即 0。
64	此行包含第四个监控规则的 ID 的最后一个字节。其余三个字节是第五个监控规则的 ID，即 0。
65	此行包含第六个监控规则的 ID 的最后一个字节。其余三个字节是第七个监控规则的0。
66	此行包含第七个监控规则的 ID 的最后一个字节。其余三个字节是第八个监控规则的 ID，即 0。
67	此行包含第八个监控规则的 ID 的最后一个字节。此行中的第二个字节指明源或目标 IP 地址是否与 IP 阻止列表匹配。此行中的第三个字节是与 IP 阻止列表匹配的 IP 层。最后一个字节为文件事件计数 0 的开头。
68	此行的第一个字节是剩余文件事件计数。接下来的两个字节包含入侵事件计数。最后一个字节包含发起方所在国家/地区，在本例中为 0，表示“未知”。
69	此行的第一个字节是发起方所在国家/地区的第二个字节。接下来的两个字节是响应方所在国家/地区 840。最后一个字节是原始客户端所在国家/地区的开头，在本例中为 0，表示“未知”。
70	此行的第一个字节是原始客户端所在国家/地区的结尾。接下来的两个字节是 IOC 编号 0。最后一个字节是源自治系统的第一个字节，即 0。
71	此行的前三个字节是源自治系统。最后一个字节是目标自治系统的第一个字节，即 0。
72	此行的前三个字节是目标自治系统。最后一个字节是输入接口的 SNMP 索引，即 0。
73	此行的第一个字节是输入接口的 SNMP 索引。接下来的两个字节是输出接口的 SNMP 索引，即 0。此行中的最后一个字节是传入接口的服务类型设置 0。

编号	说明
74	此行的第一个字节是传出接口的服务类型设置 0。第二个字节是源掩码 0。第三个字节是目标掩码 0。最后一个字节是流量通过的安全背景的 ID 号码的开头。在本例中，安全背景为 00000000-0000-0000-0000-000000000000。
75	此行的前三个字节是安全背景的其余部分。最后一个字节是 VLAN ID，即 0。
76	第一个字节是 VLAN ID。最后三个字节以 0 值作为一个字符串块的开头。此字符串块包含引用的主机的名称。
77	第一个字节是字符串块类型的其余部分。最后三个字节提供字符串块的总长度，包括块类型和长度，此总长度为 8 个字节，这意味着字符串块中没有数据，因为没有引用的主机。
78	第一个字节是字符串块长度的其余部分。最后三个字节以 0 值作为一个字符串块的开头。此字符串块包含用户代理。
79	第一个字节是字符串块类型的其余部分。最后三个字节提供字符串块的总长度，包括块类型和长度，此总长度为 8 个字节，这意味着字符串块中没有数据，因为没有用户代理。
80	第一个字节是字符串块长度的其余部分。最后三个字节以 0 值作为一个字符串块的开头。此字符串块包含 HTTP 引用站点。
81	第一个字节是字符串块类型的其余部分。最后三个字节提供字符串块的总长度，包括块类型和长度，此总长度为 8 个字节，这意味着字符串块中没有数据，因为没有 HTTP 引用站点。
82	此行的第一个字节包含字符串块长度的最后部分。最后三个字节包含 SSL 证书指纹，即 0000000000000000000。
83	此行的第一个字节包含 SSL 证书指纹 ID 的最后部分。此行的其余部分包含 SSL 策略 ID，即 00000000-0000-0000-0000-000000000000。
84	此行的第一个字节是 SSL 策略 ID 的结尾。其余三个字节是 SSL 规则 ID，即 0。
85	此行的第一个字节是 SSL 规则 ID 的其余部分。接下来的两个字节是 SSL 密码套件，即 0，表示 TLS_NULL_WITH_NUL_NULL。最后一个字节是 SSL 版本，即 0。
86	此行包含 SSL 服务器证书状态，即 0，表示未检查。
87	此行的前两个字节是 SSL 实际操作，即 0，表示未知。接下来的两个字节是 SSL 预期操作，即 0，表示未知。
88	此行的前两个字节是 SSL 流状态，即 0，表示未知。接下来的两个字节是 SSL 流错误，即 0，表示未知。
89	此行的前两个字节是SSL流错误的其余部分。接下来的两个字节是为 0 的SSL流消息。
90	此行的前两个字节是 SSL 流消息。接下来的两个字节是 SSL 流标志，即 0。
91	此行的前两个字节是 SSL 流标志的其余部分。接下来的两个字节是 SSL 服务器名称的类型为 0 的字符串块开头。
92	此行的前两个字节 结束字符串块类型，接下来的两个字节包含字符串块长度。块长度为 8，这包括块类型和长度，表示字符串块不包含数据。
93	前两个字节包含字符串块长度的其余部分。接下来的两个字节包含 SSL URL 类别，即 0，表示未知。
94	此行的前两个字节包含 SSL URL 类别的其余部分。接下来的两个字节是 SSL 会话 ID 00000000000000000000000000000000 的开头。
95	此行的第一个字节包含 SSL 会话 ID 的结尾。下一个字节包含 SSL 会话 ID 0 的长度。接下来的两个字节是 SSL 票证00000000000000000000 的开头。

编号	说明
96	此行的第两个字节包含 SSL 票证 ID 的结尾。第三个字节包含为 0 的 SSL 票证 ID 长度。最后一个字节为网络分析策略修订（即 4e78cb70-7842-11e6-a99b-cdb19cb553fd）的开头。
97	此行的前三个字节包含网络分析策略修订的结尾。最后一个字节为终端配置文件 ID 0 的开头。
98	此行的前三个字节是终端配置文件 ID。其余字节是安全组 ID 0 的开头。
99	此行的前三个字节是安全组 ID。其余字节为位置 IPv6（即与 ISE 进行的接口通信的 IP 地址，该地址为空）的开头。
100	此行的前三个字节结束位置 IPv6。其余字节为 HTTP 响应（即 0，表示没有 HTTP 响应）的开头。
101	此行的前三个字节结束 HTTP 响应。其余字节为字符串块（类型为 0，表示 DNS 查询）的开头。
102	前三个字节完成字符串块类型。其余字节包含字符串块长度，此长度为 8 个字节，包括块类型和长度，这意味着 DNS 查询中没有数据。
103	前三个字节结束字符串块长度。此行中的其余字节为 DNS 记录类型（即 71）的开头。
104	此行中的第一个字节结束 DNS 记录类型。接下来的两个字节是 DNS 响应类型，即 0。最后一个字节为 DNS TTL 的开头。
105	此行的前三个字节是 DNS TTL。最后一个字节是 Sinkhole UUID（即 00000000-0000-0000-0000-000000000000）的开头。
106	此行的前三个字节为 Sinkhole UUID 的结尾。最后一个字节为第一个安全情报列表（即 0）的开头。
107	此行中的前三个字节为第一个安全情报列表的结尾。最后一个字节为第二个安全情报列表（即 0）的开头。

版本 5.1+ 用户事件示例

下图显示了一个用户事件记录示例：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	1	0	0	1
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	1	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1	0	0	1
5	0	1	0	1	0	0	1	1	0	0	1	1	0	0	0	0	0	1	1	1	1	1	0	0	0	0	1	0	1	0	0	1
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0
11	0	1	0	1	0	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	1	1
12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	0	0	1	1	0	0	1	0	0	1	1	1	1
13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	0	1	1	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0
15	0	1	1	1	0	0	1	1	1	1	1	1	0	0	0	1	1	1	1	0	1	1	1	1	0	1	0	1	0	0	1	0
16	0	0	0	1	0	0	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1
19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	1
20	0	1	0	1	0	0	1	0	1	1	1	0	1	1	1	1	1	1	1	1	0	0	0	1	0	1	1	1	0	0	1	1
21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
24	0	0	1	0	0	0	0	0	0	0	1	1	0	0	1	1	0	0	1	1	0	0	0	0	0	0	1	1	0	0	0	1
	0	1	0	0	0	0	0	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0
	0	0	1	1	0	1	0	0	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1	0	0	0	1
	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	0	1
25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	1
26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	0	1	0	1	0
27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
29	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	0	0	0	0	1	0	1	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	1	1	0	1	1	1	1	0	0	0
30	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
31	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
	0	0	0	0	0	0	0	0																								

在上一个实例中，出现以下信息：

编号	说明
1	此行的前两个字节表示标准报头值 1。接下来的两个字节表示该消息为数据消息（也就是消息类型 4）。
2	此行表示后面的消息长度为 153 个字节。
3	这里的第一位是一个标志，表示该报头是一个含有存档时间戳的扩展报头。接下来的 15 位是一个可选字段，包含在其上检测到事件的域的 Netmap ID。该行的其余部分表示记录类型值95，说明这是用户信息更新消息块。
4	此行表示后面的数据长度为 137 个字节。
5	此行包含存档时间戳。因为设置了位 23，所以包含该时间戳。该时间戳为Unix 时间戳，存储为自 1/1/1970 起经过的秒数。此时间戳为 1,391,789,354，表示 2014 年 2 月 3 日，星期一，19:43:49。
6	此行全部为 0，留作未来使用。
7	此行表示检测引擎 ID 为 3。
8	此行用作旧版 (IPv4) IP 地址。此行的值全部为 0，因为尚未填充，而 IPv4 地址存储在 IPv6 字段中。
9	此行包含与事件关联的 MAC 地址。因为没有 MAC 地址，此行的值全部为 0。
10	此行的前半部分为 MAC 地址的剩余部分，全部为 0。接下来的一个字节表示存在 IPv6 地址。此行的最后一个字节留作未来使用，全部为 0。
11	此行包含系统生成事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
12	此行包含系统生成事件的微秒（一秒的一百万分之一）增量。
13	此行包含事件类型。事件类型值为 1004，表示用户修改消息。
14	此行包含事件子类型。事件子类型值为 2，表示用户登录消息。
15	此行包含串行文件编号。此字段供内部使用，可以忽略。
16	此行包含串行文件中的事件位置。此字段供内部使用，可以忽略。
17	此行包含 IPv6 地址。若设置了 Has IPv6 标志，则此字段存在且可使用。但是在本例中，它包含 IPv4 地址 10.4.15.120。
18	此行可启动用户登录信息数据块，以块类型 127 表示。
19	此行表示后面的块长度为 81 个字节。
20	此行表示用户登录时间戳为 1,391,456,7，说明其生成时间为 2014 年 10 月 3 日，星期一，19:43:47 GMT（格林威治标准时间）。

编号	说明
21	此行用作旧版 (IPv4) IP 地址。此行的值全部为 0，因为尚未填充，而 IPv4 地址存储在 IPv6 字段中。
22	此行表示后面跟着一个字符串块，包含字符串块长度和文本字符串（在本例中，该文本字符串包含用户名称）。有关字符串块的详细信息，请参阅字符串数据块，第 3-59 页。
23	此行表示字符串块中数据的长度为 16 个字节。
24	此行表示用户的名称为“301@10.4.11.175”。
25	此行表示用户的 ID 号码。
26	此行表示在连接（登录信息源自此连接）中使用的应用协议的应用 ID。
27	此行表示后面跟着一个字符串块，包含字符串块长度和文本字符串（在本例中，该文本字符串包含电子邮件地址）。有关字符串块的详细信息，请参阅字符串数据块，第 3-59 页。
28	此行表示字符串块中数据的长度为 0 个字节。这是因为没有电子邮件地址与此用户关联。
29	此行包含检测到用户登录的主机的 IP 地址。
30	第一个字节包含登录类型。此行的其余部分表示后面跟着一个字符串块，包含字符串块长度和文本字符串（在本例中，该文本字符串包含报告登录的 Active Directory 的名称）。有关字符串块的详细信息，请参阅字符串数据块，第 3-59 页。
31	此行的第一个字节完成字符串数据块的启动。此行的其余部分表示字符串块中数据的长度为 0 个字节。这是因为没有 Active Directory 服务器与此登录关联。

发现数据结构示例

本节包含可能由 eStreamer 传输的发现事件的数据结构示例。提供以下示例：

新网络协议消息示例

下图说明 3.0+ 的新网络协议消息的示例:

字节	0	1	2	3	
位	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31	
报头版本	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 0 0 1 0 0	以事件消息 (4) 开始标准消息报头
消息长度 (49B)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 1 1 0 0 0 1	
新网络协议消息 (13)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 1 1 0 1	
消息长度 (41B)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 1 1 0 1 0 0 0	
检测引擎	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0	
IP (192.168.1.10)	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 1 0 1 0	
MAC 地址（无）	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	
	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	保留的字节 (0)
Unix 秒 (1047242787)	0 0 1 1 1 1 1 0	0 1 1 0 1 0 1 1	1 0 1 0 1 0 0 0	0 0 1 0 0 0 1 1	
Unix 微秒 (973208)	0 0 0 0 0 0 0 0	0 0 0 0 1 1 1 0	1 1 0 1 1 0 0 1	1 0 0 1 1 0 0 0	
保留的字节 (0)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 1	1 1 1 0 1 0 0 0	事件类型 1000—新
事件子类型 4 - 新传输协议	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 1 0 0	
文件编号	0 1 0 0 0 0 0 0	0 1 0 0 0 1 1 1	1 0 0 0 1 0 0 1	1 1 0 1 0 0 0 1	
文件位置	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	1 1 0 0 0 0 0 0	结束标准消息报头
协议 (6—TCP)	0 0 0 0 0 1 1 0				

新 TCP 服务器消息示例

下图说明 3.0 的新 TCP 服务器消息的示例：

字节	0	1	2	3	
位	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31	
报头版本	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 0 0 1 0 0	以事件消息 (4) 开始标准消息报头
消息长度 (256B)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0	
新 TCP 服务消息 (11)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 1 0 1 1	
消息长度 (248B)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	1 1 1 1 1 0 0 0	
检测引擎	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0	
IP (192.168.1.10)	1 1 0 0 0 0 0 0	1 0 1 0 1 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 1 0 1 0	
MAC 地址（无）	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	
	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	保留的字节 (0)
Unix 秒 (1047242787)	0 0 1 1 1 1 1 0	0 1 1 0 1 0 1 1	1 0 1 0 1 0 0 0	0 0 1 0 0 0 1 1	
Unix 微秒 (973208)	0 0 0 0 0 0 0 0	0 0 0 0 1 1 1 0	1 1 0 1 1 0 0 1	1 0 0 1 1 0 0 0	
保留的字节 (0)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 1 1 1	1 1 1 0 1 0 0 0	事件类型 1000—新
事件子类型 2 - 新主机	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 1 0	
文件编号	0 1 0 0 0 0 0 0	0 1 0 0 0 1 1 1	1 0 0 0 1 0 0 1	1 1 0 1 0 0 0 1	
文件位置	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	1 1 0 0 0 0 0 0	结束标准消息报头
服务器块报头 (12)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 1 1 0 0	开始服务器数据块
服务器长度 (208B)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	1 1 0 1 0 0 0 0	
服务器端口 (80)	0 0 0 0 0 0 0 0	0 1 0 1 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	命中数 (Hits)
命中数 (1)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 1	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	字符串块报头
字符串块报头 (0)	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0 0	字符串块长度
字符串块长度 (13B)	0 0 0 0 0 0 0 0	0 0 0 0 1 1 0 1	0 1 1 0 1 0 0 0	0 1 1 1 0 1 0 0	

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
服务器名称 (https)	0	1	1	1	0	1	0	0	0	1	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块长度
字符串块长度 (15B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	1	0	1	0	0	0	0	0	1	
服务器供应商 (Apache + 空字节)	0	1	1	1	0	0	0	0	0	1	1	0	0	0	0	1	0	1	1	0	0	0	1	1	0	1	1	0	1	0	0	0	
	0	1	1	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块长度
字符串长度 (8 - 无产品)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块长度
字符串块长度 (22B)	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	0	1	1	0	0	0	1	0	0	1	0	1	1	1	0	
版本 - 1.3.26 (Unix)	0	0	1	1	0	0	1	1	0	0	1	0	1	1	1	0	0	0	1	1	0	0	1	0	0	0	1	1	0	1	1	0	
	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	0	0	1	0	1	0	1	0	1	0	1	1	0	1	1	1	0	
	0	1	1	0	1	0	0	1	0	1	1	1	1	0	0	0	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	
列表块报头 (11)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	0	1	开始子服务器列表
列表块大小 (94B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	1	0	
子服务器报头 (1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	开始子服务器块
子服务器长度 (46B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	1	0	
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
字符串长度 (16B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0		
子服务器名称 - mod_ssl	0	1	1	0	1	1	0	1	0	1	1	0	1	1	1	1	0	1	1	0	0	1	0	0	0	1	0	1	1	1	1	1		
	0	1	1	1	0	0	1	1	0	1	1	1	0	0	1	1	0	1	1	0	1	1	0	0	0	0	0	0	0	0	0	0		
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0		
字符串块长度 (8B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	(无子类型供应商)	

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
字符串块长度 (14B)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	1	1	0	
子服务器版本 - 2.8.9 + 空字符	0	0	1	1	0	0	1	0	0	0	1	0	1	1	1	0	0	0	1	1	1	0	0	0	0	0	1	0	1	1	1	0	结束子服务器块
	0	0	1	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	开始子服务器块
子服务器报头 (1)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	子服务器长度
子服务器长度 (48B)	0	0	0	0	0	0	0	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块大小
字符串块大小 (16B)	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	1	0	0	1	1	1	1	0	1	1	1	0	0	0	0	
子服务器名称 - OpenSSL	0	1	1	0	0	1	0	1	0	1	1	0	1	1	1	0	0	1	0	1	0	0	1	1	0	1	0	1	0	0	1	1	
	0	1	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串数据长度
字符串长度 (8 - 无供应商)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块报头
字符串块报头 (0)	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	字符串块长度
字符串块长度 (16B)	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	1	1	0	0	0	0	0	0	1	0	1	1	1	0	
子服务器版本 - 0.9.6.d + 空字节	0	0	1	1	1	0	0	1	0	0	1	0	1	1	1	0	0	0	1	1	0	1	1	0	0	0	1	0	1	1	1	0	结束子服务器块
	0	1	1	0	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	置信度 %
置信度 % (100)	0	0	0	0	0	0	0	0	0	1	1	0	0	1	0	0	0	0	1	1	1	1	1	0	0	1	1	0	1	0	1	1	上次使用时间
首次使用时间 (1047242787)	1	0	1	0	1	0	0	0	0	0	1	0	0	0	1	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Blob 数据块
Blob 数据块 (10)	0	0	0	0	0	0	0	0	0	0	0	0	1	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	Blob 数据长度
Blob 数据长度 (22B)	0	0	0	0	0	0	0	0	0	0	0	1	0	1	1	0	0	1	0	0	1	0	0	0	0	1	0	1	0	1	0	0	

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
服务器横幅（HTTP/1.1414 请求）- 服务器横幅缩短以便用于示例，通常为 256B。	0	1	0	1	0	1	0	0	0	1	0	1	0	0	0	0	0	0	1	0	1	1	1	1	0	0	1	1	0	0	0	1	
	0	0	1	0	1	1	1	0	0	0	1	1	0	0	0	1	0	0	1	0	0	0	0	0	0	0	0	1	1	0	1	0	0
	0	0	1	1	0	0	0	1	0	0	1	1	0	1	0	0	0	0	1	0	0	0	0	0	0	0	1	0	1	0	0	1	0
	0	1	1	0	0	1	0	1	0	1	1	1	0	0	0	1	0	1	1	1	0	1	0	1	0	1	1	0	0	1	0	1	结束服务器数据块

了解旧版数据结构

本附录包含之前版本的 Cisco Secure Firewall 系统产品中受 eStreamer 支持的数据结构的相关信息。

如果您的客户端使用事件流请求并对比特位进行设置，以请求采用较旧版本格式的数据，您可以使用此附录中的信息识别您收到的数据消息的数据结。

请注意，在版本 5.0 之前的版本中，ID 分配给单独的检测引擎。对于版本 5.0，ID 分配给设备。根据版本，数据结构可反映这一点。

注释 此附录仅描述 Cisco Secure Firewall 系统版本 4.9 及更高版本的数据结构。如果您需要有关较早数据结构版本的结构的文件，请联系思科客户支持。

有关详细信息，请参阅以下各节：

旧版入侵数据结构

入侵事件 (IPv4) 记录 5.0.x - 5.1

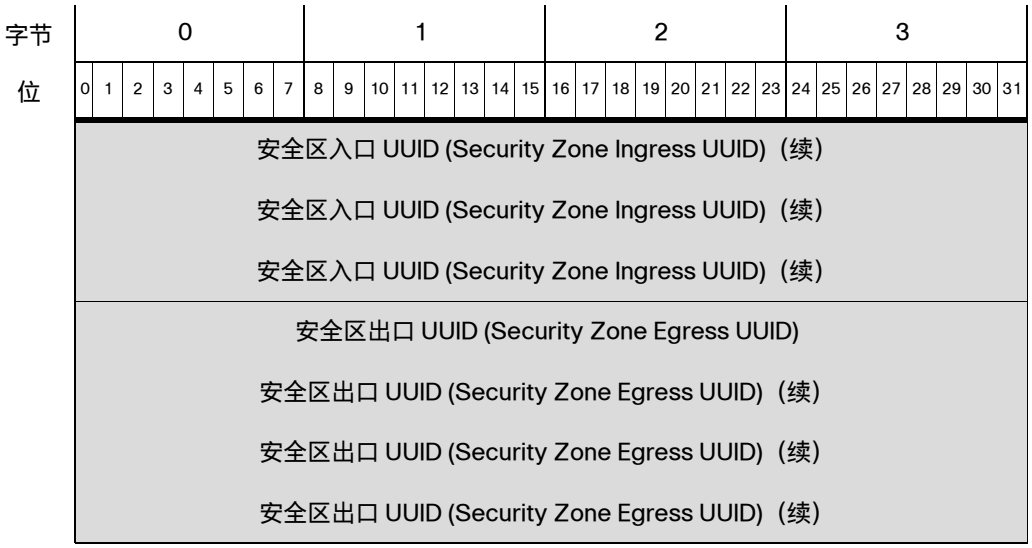
下图中的阴影部分表示入侵事件 (IPv4) 记录中的字段。记录类型为 207。

通过在请求消息中设置入侵事件标志或扩展请求标志可请求入侵事件记录。请参阅请求标志，第 2-12 页和提交扩展请求，第 2-4 页。

对于版本 5.0.x - 5.1 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (207)（Record Type (207))															
记录长度 (Record Length)																																
er 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
设备 ID (设备 ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID（签名 ID）(Rule ID (Signature																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																
源 IPv4 地址																																
目的 IPv4 地址																																
源端口 (Source Port)																	目标端口 (Destination Port)															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IP 协议 ID (IP Protocol ID)								影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
	MPLS 标签 (MPLS Label)																															
	VLAN ID																Pad															
	策略 UUID (Policy UUID)																															
	策略 UUID (Policy UUID)（续）																															
	策略 UUID (Policy UUID)（续）																															
	策略 UUID (Policy UUID)（续）																															
	用户 ID																															
	Web 应用 ID (Web Application ID)																															
	客户端应用 ID (Client Application ID)																															
	应用协议 ID (Application Protocol ID)																															
	访问控制规则 ID (Access Control Rule ID)																															
	访问控制策略 UUID (Access Control Policy UUID)																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	接口入口 UUID (Interface Ingress UUID)																															
	接口入口 UUID (Interface Ingress UUID)（续）																															
	接口入口 UUID (Interface Ingress UUID)（续）																															
	接口入口 UUID (Interface Ingress UUID)（续）																															
	接口出口 UUID (Interface Egress UUID)																															
	接口出口 UUID (Interface Egress UUID)（续）																															
	接口出口 UUID (Interface Egress UUID)（续）																															
	接口出口 UUID (Interface Egress UUID)（续）																															
	安全区入口 UUID (Security Zone Ingress UUID)																															



20下21表22对每个入侵事件记录数据字段进行了说明。

表 B-1　　入侵事件 (IPv4) 记录字段

字段	数据类型	说明
设备 ID	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒（一秒的百万分之一）增量。
规则 ID（签名 ID）(Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Cisco Secure Firewall 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IPv4 地址	uint8[4]	事件中使用的源 IPv4 地址，采用地址八位组。
目的 IPv4 地址	uint8[4]	事件中使用的目标 IPv4 地址，采用地址八位组。
源端口 (Source Port)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号。
目标端口 (Destination Port)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号。

表 B-1　　入侵事件 (IPv4) 记录字段 （续）

字段	数据类型	说明
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如: ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。 以下影响级别值映射到“防御中心”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1: ▪ （0，未知）： 00X00000 ▪ 红色（1，易受攻击）： XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX ▪ 橙色（2，可能易受攻击）： 00X00111 ▪ 黄色（3，当前不易受攻击）： 00X00011 ▪ 蓝色（4，未知目标）： 00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下: ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 -（未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 ▪ 0 - 未被阻止 ▪ 1 - 已阻止 ▪ 2 - 将被阻止（但配置不允许）

表 B-1　　入侵事件 (IPv4) 记录字段 （续）

字段	数据类型	说明
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID	uint32	用户的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。

入侵事件 (IPv6) 记录 5.0.x - 5.1

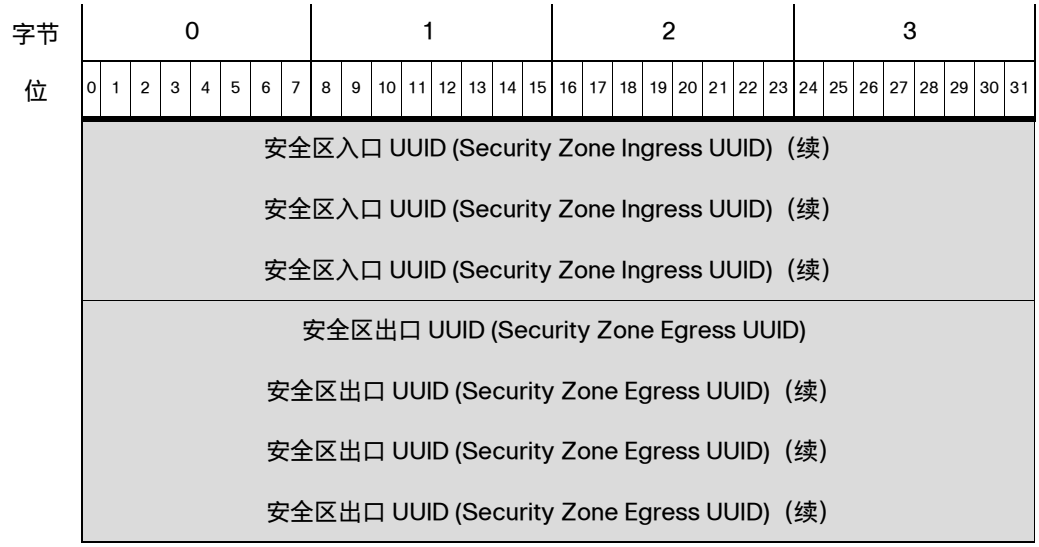
下图中的阴影部分表示入侵事件 (IPv6) 记录中的字段。记录类型为 208。

通过在请求消息中设置入侵事件标志或扩展请求标志可请求入侵事件记录。请参阅请求标志，第 2-12 页和提交扩展请求，第 2-4 页。

对于版本 5.0.x - 5.1 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (208)（Record Type (208))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
设备 ID (设备 ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID（签名 ID）(Rule ID (Signature																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																
源 IPv6 地址 (Source IPv6 Address) 源 IPv6 地址 (Source IPv6 Address)（续） 源 IPv6 地址 (Source IPv6 Address)（续） 源 IPv6 地址 (Source IPv6 Address)（续）																																
目的 IPv6 地址 (Destination IPv6 Address) 目标 IPv6 地址 (Destination IPv6 Address)（续） 目标 IPv6 地址 (Destination IPv6 Address)（续） 目标 IPv6 地址 (Destination IPv6 Address)（续）																																
源端口/ICMP 类型 (Source Port/ICMP Type)																	目标端口/ICMP 代码 (Destination Port/ICMP Code)															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID)																																
策略 UUID (Policy UUID)（续）																																
策略 UUID (Policy UUID)（续）																																
策略 UUID (Policy UUID)（续）																																
用户 ID																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																



下表对每个入侵事件记录数据字段进行了说明。

表 B-2　　入侵事件 (IPv6) 记录字段

字段	数据类型	说明
设备 ID	unit32	包含检测设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒（一秒的百万分之一）增量。
规则 ID（签名 ID）(Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Cisco Secure Firewall 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IPv6 地址 (Source IPv6 Address)	uint8[16]	事件中使用的源 IPv6 地址，采用地址八位组。

表 B-2　　入侵事件 (IPv6) 记录字段 （续）

字段	数据类型	说明
目的 IPv6 地址	uint8[16]	事件中使用的目标 IPv6 地址，采用地址八位组。
源端口/ICMP 类型 (Source Port/ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号。如果协议类型为 ICMP，则这表示 ICMP 类型。
目标端口 /ICMP 代码 (Destination Port/ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号。如果协议类型为 ICMP，则这表示 ICMP 代码。
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如: ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。 以下影响级别值映射到“防御中心”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1: ▪ （0，未知）：00X00000 ▪ 红色（1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX ▪ 橙色（2，可能易受攻击）：00X00111 ▪ 黄色（3，当前不易受攻击）：00X00011 ▪ 蓝色（4，未知目标）：00X00001

表 B-2　　入侵事件 (IPv6) 记录字段 （续）

字段	数据类型	说明
影响 (Impact)	uint8	事件的影响标志值。其值如下： ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 -（未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 ▪ 0 - 未被阻止 ▪ 1 - 已阻止 ▪ 2 - 将被阻止（但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。（仅适用于 4.9+ 事件。）
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。（仅适用于 4.9+ 事件。）
Pad	uint16	已保留供将来使用。
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID	uint32	用户的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。

表 B-2　　入侵事件 (IPv6) 记录字段 （续）

字段	数据类型	说明
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。

入侵事件记录 5.2.x

下图中的阴影部分表示入侵事件记录中的字段。在系列 2 数据块组中，记录类型为 400，块类型为 34。

你可以通过扩展请求，仅从 eStreamer 请求 5.2.x 入侵事件，为此，您需要在流请求消息中请求事件类型代码 12 和版本代码 5（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

对于版本 5.2.x 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。连接秒、连接实例以及连接计数器在一起构成与入侵事件相关的连接事件的唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
块类型 (34) (Block Type (34))																																
块长度 (Block Length)																																
设备 ID (设备 ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
规则 ID（签名 ID）(Rule ID (Signature																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																
来源 IP 地址 来源 IP 地址，续 来源 IP 地址，续 源 IP 地址 (Source IP Address)（续）																																
目标 IP 地址 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址，续 目标 IP 地址 (Destination IP Address)（续）																																
源端口或 ICMP 类型 (Source Port or ICMP Type)																	目标端口或 ICMP 代码 (Destination Port or ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID) 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续）																																
用户 ID																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
连接时间戳 (Connection Timestamp)																																
连接实例 ID (Connection Instance ID)																	连接计数器 (Connection Counter)															
源国家/地区 (Source Country)																	目标国家/地区 (Destination Country)															

下表对每个入侵事件记录数据字段进行了说明。

表 B-3　　入侵事件记录 5.2.x 字段

字段	数据类型	说明 (Description)
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 34。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (设备 ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒（一秒的百万分之一）增量。
规则 ID（签名 ID）(Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Cisco Secure Firewall 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如： ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP

表 B-3　　入侵事件记录 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到“防御中心”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1: ▪ （0，未知）：00X00000 ▪ 红色（1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）：00X0011X ▪ 黄色（3，当前不易受攻击）：00X0001X ▪ 蓝色（4，未知目标）：00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下: ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 - （未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 ▪ 0 - 未被阻止 ▪ 1 - 已阻止 ▪ 2 - 将被阻止（但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。

表 B-3　　入侵事件记录 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID	uint32	用户的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。

入侵事件记录 5.3

下图中的阴影部分表示入侵事件记录中的字段。在系列 2 数据块组中，记录类型为 400，块类型为 41。

您可以通过扩展请求，仅从 eStreamer 请求 5.3 入侵事件，要提交扩展请求，您需要在流请求消息中请求事件类型代码 12 和版本代码 6（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

对于版本 5.3 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。连接秒、连接实例以及连接计数器在一起构成与入侵事件相关的连接事件的唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
块类型 (41) (Block Type (41))																																
块长度 (Block Length)																																
设备 ID (设备 ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID（签名 ID）(Rule ID (Signature																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
来源 IP 地址 来源 IP 地址，续 来源 IP 地址，续 源 IP 地址 (Source IP Address)（续）																																
目标 IP 地址 目标 IP 地址，续 目标 IP 地址，续 目标 IP 地址 (Destination IP Address)（续）																																
源端口或 ICMP 类型 (Source Port or ICMP Type)																	目标端口或 ICMP 代码 (Destination Port or ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID) 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续）																																
用户 ID																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID) 访问控制策略 UUID (Access Control Policy UUID)（续） 访问控制策略 UUID (Access Control Policy UUID)（续） 访问控制策略 UUID (Access Control Policy UUID)（续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
连接时间戳 (Connection Timestamp)																																
连接实例 ID (Connection Instance ID)																	连接计数器 (Connection Counter)														
源国家/地区 (Source Country)																	目标国家/地区 (Destination Country)														
IOC 编号 (IOC Number)																																

下表对每个入侵事件记录数据字段进行了说明。

表 B-4 入侵事件记录 5.3 字段

字段	数据类型	说明 (Description)
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 34。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据的字节数。

表 B-4　　入侵事件记录 5.3 字段 （续）

字段	数据类型	说明 (Description)
设备 ID (设备 ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒（一秒的百万分之一）增量。
规则 ID（签名 ID）(Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Cisco Secure Firewall 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如: ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP

表 B-4 入侵事件记录 5.3 字段 （续）

字段	数据类型	说明 (Description)
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到“防御中心”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1: ▪ （0，未知）： 00X00000 ▪ 红色（1，易受攻击）： XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）： 00X0011X ▪ 黄色（3，当前不易受攻击）： 00X0001X ▪ 蓝色（4，未知目标）： 00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下: ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 -（未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 ▪ 0 - 未被阻止 ▪ 1 - 已阻止 ▪ 2 - 将被阻止（但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。

表 B-4　　入侵事件记录 5.3 字段 （续）

字段	数据类型	说明 (Description)
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID	uint32	用户的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。

表 B-4　　入侵事件记录 5.3 字段 （续）

字段	数据类型	说明 (Description)
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。

入侵事件记录 5.1.1.x

下图中的阴影部分表示入侵事件记录中的字段。记录类型为 400，块类型为 25。

您可以通过扩展请求，仅从 eStreamer 请求 5.1.1.x 入侵事件，为此，您需要在流请求消息中请求事件类型代码 12 和版本代码 4（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

对于版本 5.1.1.x 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。连接秒、连接实例以及连接计数器在一起构成与入侵事件相关的连接事件的唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
块类型 (25) (Block Type (25))																																
块长度 (Block Length)																																
设备 ID (设备 ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
规则 ID（签名 ID）(Rule ID (Signature
生成器 ID (Generator ID)
规则修订 (Rule Revision)
分类 ID (Classification ID)
优先级 ID (Priority ID)
来源 IP 地址
来源 IP 地址，续
来源 IP 地址，续
源 IP 地址 (Source IP Address)（续）
目标 IP 地址
目标 IP 地址 (Destination IP Address)（续）
目标 IP 地址，续
目标 IP 地址 (Destination IP Address)（续）
源端口/ICMP 类型 (Source Port/ICMP Type)
目标端口/ICMP 代码 (Destination Port/ICMP Code)
IP 协议 ID (IP Protocol ID)
影响标志 (Impact Flags)
影响 (Impact)
已阻止 (Blocked)
MPLS 标签 (MPLS Label)
VLAN ID
Pad
策略 UUID (Policy UUID)
策略 UUID (Policy UUID)（续）
策略 UUID (Policy UUID)（续）
策略 UUID (Policy UUID)（续）
用户 ID
Web 应用 ID (Web Application ID)
客户端应用 ID (Client Application ID)
应用协议 ID (Application Protocol ID)

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
连接时间戳 (Connection Timestamp)																																
连接实例 ID (Connection Instance ID)																	连接计数器 (Connection Counter)															

下表对每个入侵事件记录数据字段进行了说明。

表 B-5　　入侵事件记录 5.1.1 字段

字段	数据类型	说明 (Description)
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 25。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (设备 ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒（一秒的百万分之一）增量。
规则 ID（签名 ID）(Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Cisco Secure Firewall 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口/ICMP 类型 (Source Port/ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口/ICMP 代码 (Destination Port/ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如: ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP

表 B-5 入侵事件记录 5.1.1 字段 （续）

字段	数据类型	说明 (Description)
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。 以下影响级别值映射到“防御中心”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1: ▪ （0，未知）： 00X00000 ▪ 红色（1，易受攻击）： XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX ▪ 橙色（2，可能易受攻击）： 00X00111 ▪ 黄色（3，当前不易受攻击）： 00X00011 ▪ 蓝色（4，未知目标）： 00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下: ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 - （未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 ▪ 0 - 未被阻止 ▪ 1 - 已阻止 ▪ 2 - 将被阻止（但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。

表 B-5　　入侵事件记录 5.1.1 字段 （续）

字段	数据类型	说明 (Description)
用户 ID	uint32	用户的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。

入侵事件记录 5.3.1

下图中的阴影部分表示入侵事件记录中的字段。在系列 2 数据块组中，记录类型为 400，块类型为 42。

你可以通过扩展请求，仅从 eStreamer 请求 5.3.1 入侵事件，为此，您需要在流请求消息中请求事件类型代码 12 和版本代码 7（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

对于版本 5.3.1 入侵事件，事件 ID、受管设备 ID 以及事件秒构成唯一标识符。连接秒、连接实例以及连接计数器在一起构成与入侵事件相关的连接事件的唯一标识符。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
块类型 (42) (Block Type (42))																																
块长度 (Block Length)																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID（签名 ID）(Rule ID (Signature																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																
源 IP 地址 (Source IP Address) 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
目标 IP 地址 (Destination IP Address)																																
目标 IP 地址 (Destination IP Address)（续）																																
目标 IP 地址，续																																
目标 IP 地址 (Destination IP Address)（续）																																
源端口或 ICMP 类型 (Source Port or ICMP Type)																	目标端口或 ICMP 代码 (Destination Port or ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID)																																
策略 UUID (Policy UUID)（续）																																
策略 UUID (Policy UUID)（续）																																
策略 UUID (Policy UUID)（续）																																
用户 ID																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID)																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
访问控制策略 UUID (Access Control Policy UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
接口出口 UUID (Interface Egress UUID)
接口出口 UUID (Interface Egress UUID)（续）
接口出口 UUID (Interface Egress UUID)（续）
接口出口 UUID (Interface Egress UUID)（续）
安全区入口 UUID (Security Zone Ingress UUID)
安全区入口 UUID (Security Zone Ingress UUID)（续）
安全区入口 UUID (Security Zone Ingress UUID)（续）
安全区入口 UUID (Security Zone Ingress UUID)（续）
安全区出口 UUID (Security Zone Egress UUID)
安全区出口 UUID (Security Zone Egress UUID)（续）
安全区出口 UUID (Security Zone Egress UUID)（续）
安全区出口 UUID (Security Zone Egress UUID)（续）
连接时间戳 (Connection Timestamp)
连接实例 ID (Connection Instance ID)
连接计数器 (Connection Counter)
源国家/地区 (Source Country)
目标国家/地区 (Destination Country)
IOC 编号 (IOC Number)
安全情景 (Security Context)
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）

下表对每个入侵事件记录数据字段进行了说明。

表 B-6　　入侵事件记录 5.3.1 字段

字段	数据类型	说明 (Description)
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 42。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒（一秒的百万分之一）增量。
规则 ID（签名 ID）(Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Cisco Secure Firewall 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如： ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP

表 B-6 入侵事件记录 5.3.1 字段 （续）

字段	数据类型	说明 (Description)
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到“防御中心”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1: ▪ （0，未知）：00X00000 ▪ 红色（1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）：00X0011X ▪ 黄色（3，当前不易受攻击）：00X0001X ▪ 蓝色（4，未知目标）：00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下: ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 -（未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 ▪ 0 - 未被阻止 ▪ 1 - 已阻止 ▪ 2 - 将被阻止（但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。

表 B-6　　入侵事件记录 5.3.1 字段 （续）

字段	数据类型	说明 (Description)
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID	uint32	用户的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。

表 B-6 入侵事件记录 5.3.1 字段 （续）

字段	数据类型	说明 (Description)
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

入侵事件记录 5.4.x

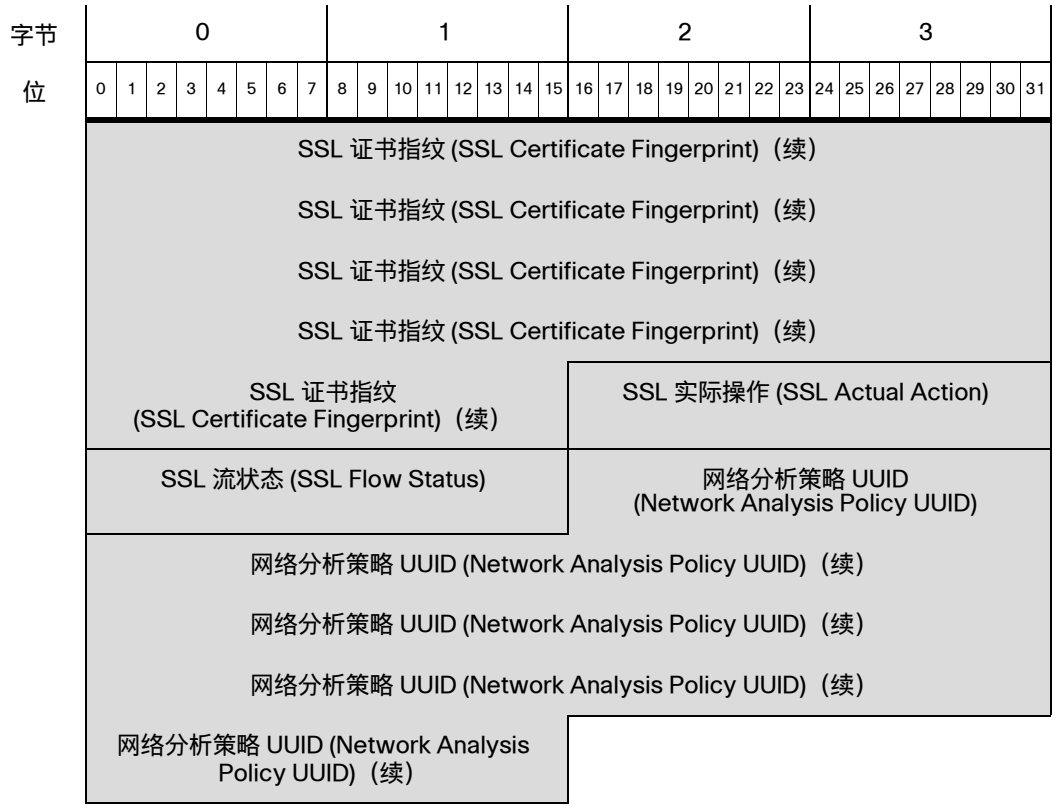
下图中的阴影部分表示入侵事件记录中的字段。在系列 2 数据块组中，记录类型为 400，块类型为 45。它替代了块类型 42，然后被块类型 60 替代。已添加用于 SSL 支持和网络分析策略的字段。

你可以通过扩展请求，仅从 eStreamer 请求 5.4.x 入侵事件，为此，您需要在流请求消息中请求事件类型代码 12 和版本代码 8（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
块类型 (45) (Block Type (45))																																
块长度 (Block Length)																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID（签名 ID）(Rule ID (Signature																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
优先级 ID (Priority ID)																																
源 IP 地址 (Source IP Address) 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续）																																
目标 IP 地址 (Destination IP Address) 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址，续 目标 IP 地址 (Destination IP Address)（续）																																
源端口或 ICMP 类型 (Source Port or ICMP Type)																	目标端口或 ICMP 代码 (Destination Port or ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID) 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续）																																
用户 ID																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID) 访问控制策略 UUID (Access Control Policy UUID)（续） 访问控制策略 UUID (Access Control Policy UUID)（续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
访问控制策略 UUID (Access Control Policy UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
连接时间戳 (Connection Timestamp)																																
连接实例 ID (Connection Instance ID)																	连接计数器 (Connection Counter)															
源国家/地区 (Source Country)																	目标国家/地区 (Destination Country)															
IOC 编号 (IOC Number)																	安全情景 (Security Context)															
安全情景 (Security Context)（续）																																
安全情景 (Security Context)（续）																																
安全情景 (Security Context)（续）																																
安全情景 (Security Context)（续）																	SSL 证书指纹 (SSL Certificate Fingerprint)															



下表对每个入侵事件记录数据字段进行了说明。

表 B-7　　入侵事件记录 5.4.x 字段

字段	数据类型	说明 (Description)
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 45。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒（一秒的百万分之一）增量。
规则 ID（签名 ID）(Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Cisco Secure Firewall 系统预处理器的标识号。

表 B-7 入侵事件记录 5.4.x 字段 （续）

字段	数据类型	说明 (Description)
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由
IP 协议号 (IP Protocol Number)	uint8	IANA 指定的协议号。例如: ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP

表 B-7　　入侵事件记录 5.4.x 字段 （续）

字段	数据类型	说明 (Description)
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到“防御中心”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1: ▪ 灰色（0，未知）：00X00000 ▪ 红色（1，易受攻击）：XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）：00X0011X ▪ 黄色（3，当前不易受攻击）：00X0001X ▪ 蓝色（4，未知目标）：00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下: ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 - 灰色（未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 ▪ 0 - 未被阻止 ▪ 1 - 已阻止 ▪ 2 - 将被阻止（但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。

表 B-7 入侵事件记录 5.4.x 字段 （续）

字段	数据类型	说明 (Description)
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID	uint32	用户的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
入口安全区 UUID (Ingress Security Zone UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
出口安全区 UUID (Egress Security Zone UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。

表 B-7　　入侵事件记录 5.4.x 字段 （续）

字段	数据类型	说明 (Description)
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8[16]	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-7 入侵事件记录 5.4.x 字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
网络分析策略 UUID (Network Analysis Policy UUID)	uint8[16]	创建入侵事件的网络分析策略的 UUID。

入侵事件记录 6.x

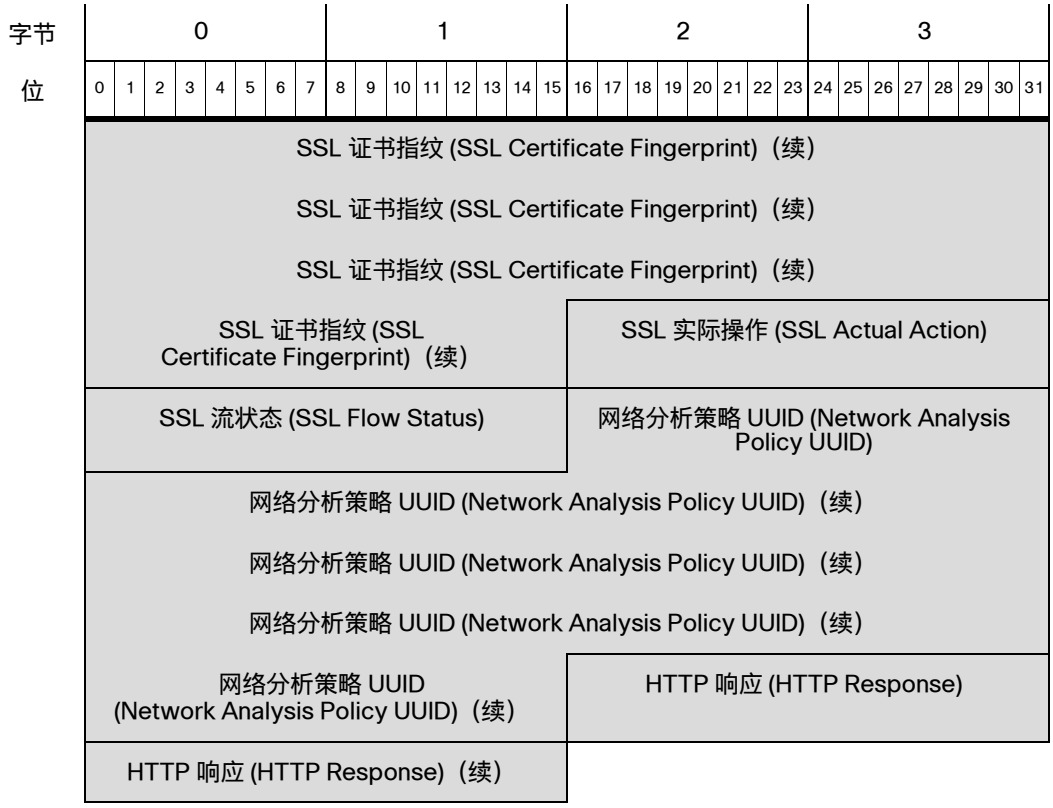
下图中的阴影部分表示入侵事件记录中的字段。此数据块的记录类型为系列 2 数据块组中的 400，块类型为系列 2 数据块组中的 60。它取代了块类型 45，并在 7.0 中被块类型 81 取代。已添加 HTTP 响应字段。

您可以通过扩展请求，仅从 eStreamer 请求 6.x 入侵事件，要提交扩展请求，您需要在流请求消息中请求事件类型代码 12 和版本代码 9（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))														
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))														
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
块类型 (60) (Block Type (60))																																
块长度 (Block Length)																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID（签名 ID）(Rule ID (Signature																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
源 IP 地址 (Source IP Address) 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续）																																
目标 IP 地址 (Destination IP Address) 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址，续 目标 IP 地址 (Destination IP Address)（续）																																
源端口或 ICMP 类型 (Source Port or ICMP Type)																	目标端口或 ICMP 代码 (Destination Port or ICMP Code)														
IP 协议 ID (IP Protocol ID)									影响标志 (Impact Flags)								影响 (Impact)								已阻止 (Blocked)							
MPLS 标签 (MPLS Label)																																
VLAN ID																	Pad															
策略 UUID (Policy UUID) 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续） 策略 UUID (Policy UUID)（续）																																
用户 ID																																
Web 应用 ID (Web Application ID)																																
客户端应用 ID (Client Application ID)																																
应用协议 ID (Application Protocol ID)																																
访问控制规则 ID (Access Control Rule ID)																																
访问控制策略 UUID (Access Control Policy UUID) 访问控制策略 UUID (Access Control Policy UUID)（续） 访问控制策略 UUID (Access Control Policy UUID)（续） 访问控制策略 UUID (Access Control Policy UUID)（续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
接口入口 UUID (Interface Ingress UUID)																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口入口 UUID (Interface Ingress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
接口出口 UUID (Interface Egress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区入口 UUID (Security Zone Ingress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
安全区出口 UUID (Security Zone Egress UUID)（续）																																
连接时间戳 (Connection Timestamp)																																
连接实例 ID (Connection Instance ID)																	连接计数器 (Connection Counter)														
源国家/地区 (Source Country)																	目标国家/地区 (Destination Country)														
IOC 编号 (IOC Number)																	安全情景 (Security Context)														
安全情景 (Security Context)（续）																																
安全情景 (Security Context)（续）																																
安全情景 (Security Context)（续）																																
安全情景 (Security Context)（续）																	SSL 证书指纹 (SSL Certificate Fingerprint)														
SSL 证书指纹 (SSL Certificate Fingerprint)（续）																																



下表对每个入侵事件记录数据字段进行了说明。

表 B-8 入侵事件记录 6.x 字段

字段	数据类型	说明 (Description)
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 60。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒（一秒的百万分之一）增量。
规则 ID（签名 ID）(Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Cisco Secure Firewall 系统预处理器的标识号。

表 B-8　　入侵事件记录 6.x 字段 （续）

字段	数据类型	说明 (Description)
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由
IP 协议 ID (IP Protocol ID)	uint8	IANA 指定的协议号。例如: ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP

表 B-8　　入侵事件记录 6.x 字段 （续）

字段	数据类型	说明 (Description)
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到管理中心上的特定优先级中。x 表示值可以为 0 或 1: ▪ 灰色（0，未知）： 00X00000 ▪ 红色（1，易受攻击）： XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）： 00X0011X ▪ 黄色（3，当前不易受攻击）： 00X0001X ▪ 蓝色（4，未知目标）： 00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下: ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 - 灰色（未知影响）
已阻止 (Blocked)	uint8	表示事件是否已被阻止的值。 ▪ 0 - 未被阻止 ▪ 1 - 已阻止 ▪ 2 - 将被阻止（但配置不允许）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。

表 B-8　　入侵事件记录 6.x 字段 （续）

字段	数据类型	说明 (Description)
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID	uint32	用户的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
接口入口 UUID (Interface Ingress UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
接口出口 UUID (Interface Egress UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
安全区入口 UUID (Security Zone Ingress UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。
安全区出口 UUID (Security Zone Egress UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。

表 B-8 入侵事件记录 6.x 字段 （续）

字段	数据类型	说明 (Description)
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8[16]	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-8　　入侵事件记录 6.x 字段 （续）

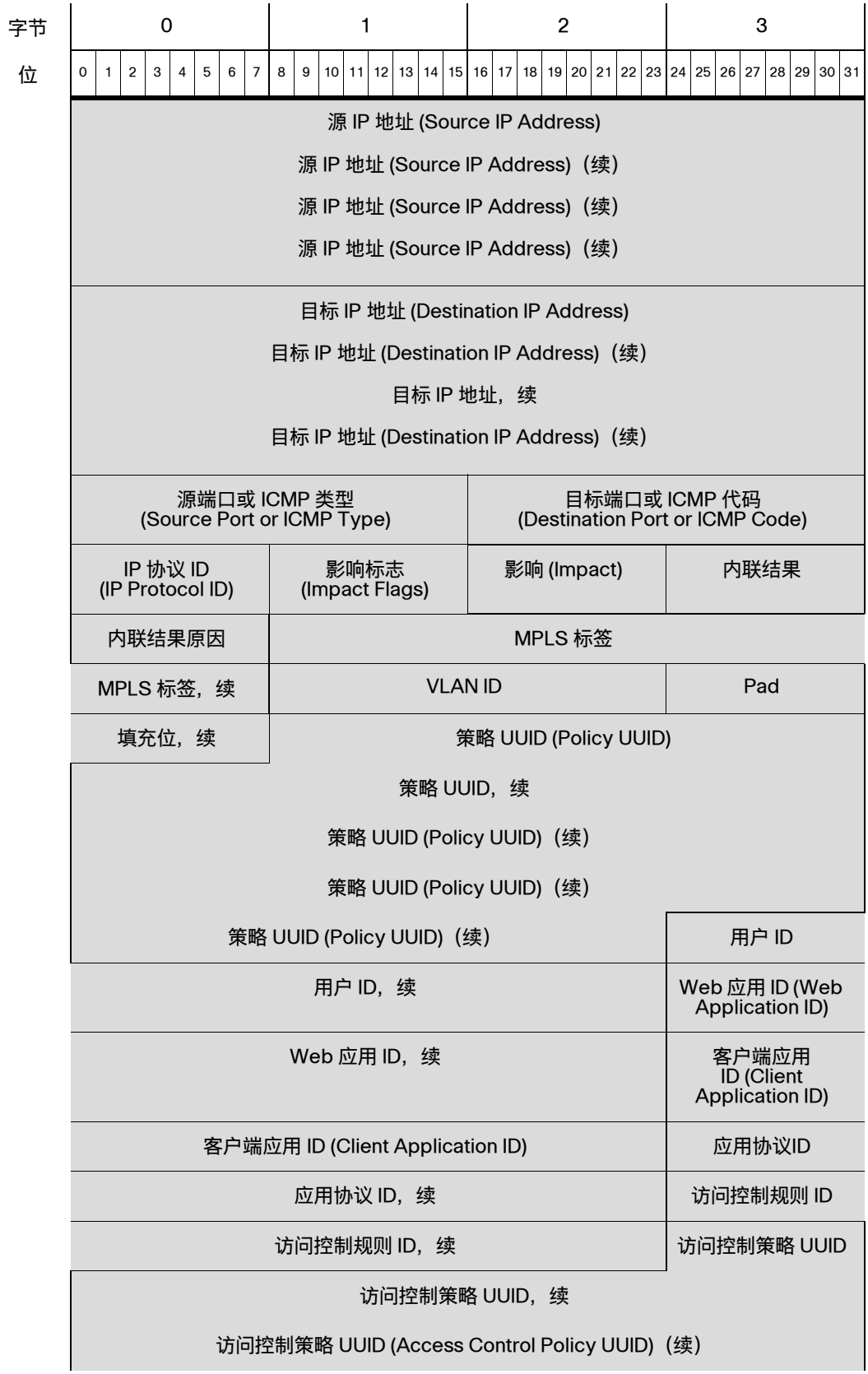
字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
网络分析策略 UUID (Network Analysis Policy UUID)	uint8[16]	创建入侵事件的网络分析策略的 UUID。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。

入侵事件记录 7.0

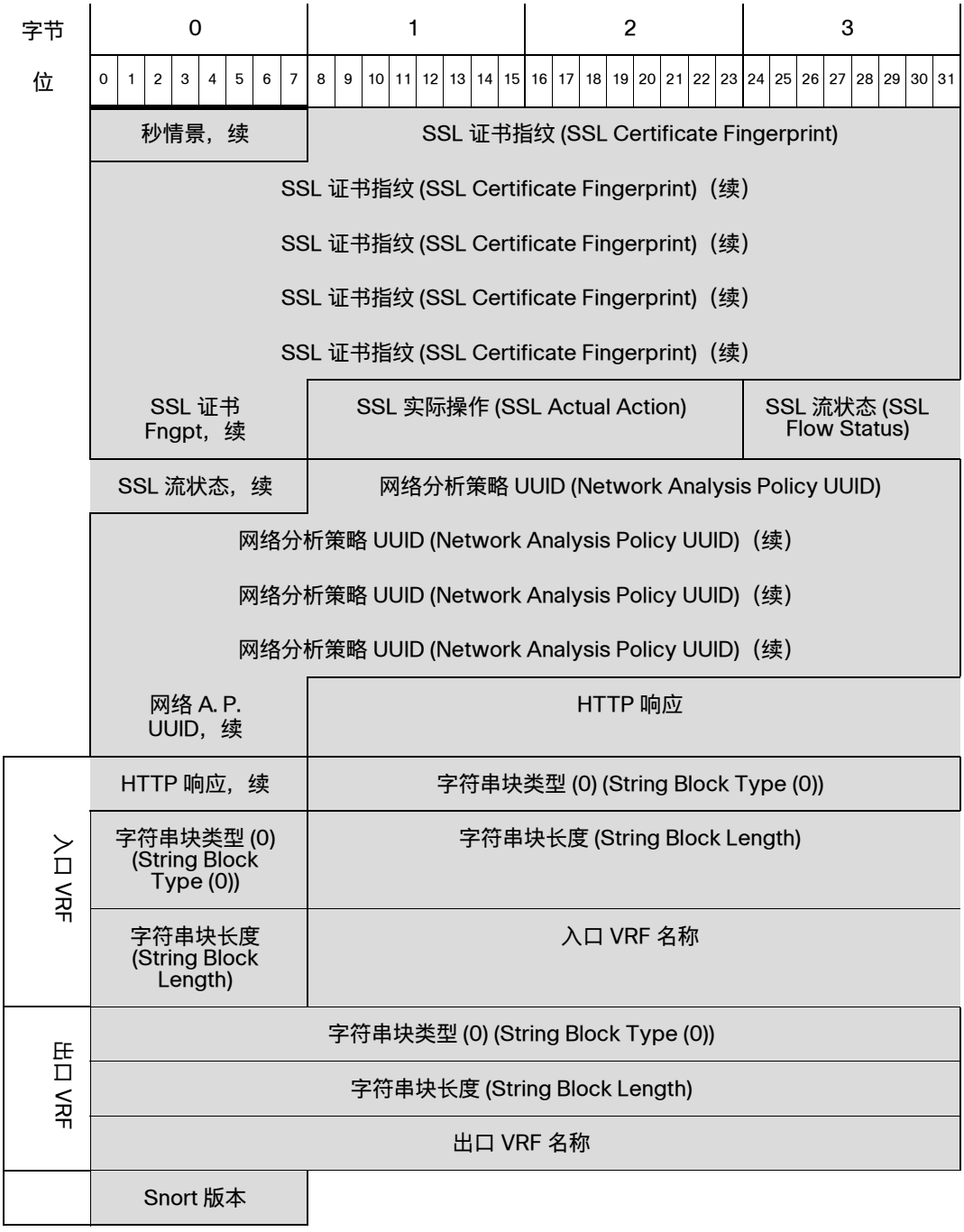
下图中的阴影部分表示入侵事件记录中的字段。此数据块的记录类型为系列 2 数据块组中的 400，块类型为系列 2 数据块组中的 81。它替代了块类型 60，然后被块类型 85 替代。已添加“内联结果原因”(Inline Result Reason)、“入口和出口虚拟路由转发”(Ingress and Egress Virtual Route Forwarding) 以及“Snort 版本”(Snort Version) 字段。“已阻止”(Blocked) 字段已重命名为“内联结果”(Inline Result)。

您可以通过扩展请求，仅从 eStreamer 请求 7.0 入侵事件，要提交扩展请求，您需要在流请求消息中请求事件类型代码 12 和版本代码 10（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (400) (Record Type (400))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
块类型 (81)																																
块长度 (Block Length)																																
设备 ID (Device ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
事件微秒 (Event Microsecond)																																
规则 ID（签名 ID）(Rule ID (Signature																																
生成器 ID (Generator ID)																																
规则修订 (Rule Revision)																																
分类 ID (Classification ID)																																
优先级 ID (Priority ID)																																


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address)（续）
源 IP 地址 (Source IP Address)（续）
源 IP 地址 (Source IP Address)（续）
目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address)（续）
目标 IP 地址，续
目标 IP 地址 (Destination IP Address)（续）
源端口或 ICMP 类型 (Source Port or ICMP Type)
目标端口或 ICMP 代码 (Destination Port or ICMP Code)
IP 协议 ID (IP Protocol ID)
影响标志 (Impact Flags)
影响 (Impact)
内联结果
内联结果原因
MPLS 标签
MPLS 标签，续
VLAN ID
Pad
填充位，续
策略 UUID (Policy UUID)
策略 UUID，续
策略 UUID (Policy UUID)（续）
策略 UUID (Policy UUID)（续）
策略 UUID (Policy UUID)（续）
用户 ID
用户 ID，续
Web 应用 ID (Web Application ID)
Web 应用 ID，续
客户端应用 ID (Client Application ID)
客户端应用 ID (Client Application ID)
应用协议ID
应用协议 ID，续
访问控制规则 ID
访问控制规则 ID，续
访问控制策略 UUID
访问控制策略 UUID，续
访问控制策略 UUID (Access Control Policy UUID)（续）


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID (Access Control Policy UUID)（续）
接口入口 UUID
接口入口 UUID，续
接口入口 UUID (Interface Ingress UUID)（续）
接口入口 UUID (Interface Ingress UUID)（续）
接口入口 UUID (Interface Ingress UUID)（续）
接口出口 UUID
接口出口 UUID，续
接口出口 UUID (Interface Egress UUID)（续）
接口出口 UUID (Interface Egress UUID)（续）
接口出口 UUID (Interface Egress UUID)（续）
秒区域入口UUID
安全区入口 UUID，续
安全区入口 UUID (Security Zone Ingress UUID)（续）
安全区入口 UUID (Security Zone Ingress UUID)（续）
安全区入口 UUID (Security Zone Ingress UUID)（续）
秒区域出口UUID
安全区出口 UUID，续
安全区出口 UUID (Security Zone Egress UUID)（续）
安全区出口 UUID (Security Zone Egress UUID)（续）
安全区出口 UUID (Security Zone Egress UUID)（续）
连接时间戳
连接时间戳，续
连接实例ID
连接实例 ID
连接计数器 (Connection Counter)
源国家/地区 (Source Country)
源国家/地区 (Source Country)
目标国家/地区 (Destination Country)
IOC 编号 (IOC Number)
IOC 编号 (IOC Number)
安全情景 (Security Context)
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）



下表对每个入侵事件记录数据字段进行了说明。

表 B-9 入侵事件记录 7.0 字段

字段	数据类型	说明 (Description)
块类型 (Block Type)	unint32	启动入侵事件数据块。值始终为 81。
块长度 (Block Length)	unint32	入侵事件数据块中的字节总数，包括入侵事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	unit32	包含检测受管设备的标识号。您可以通过请求版本 3 或 4 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件检测的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
事件微秒 (Event Microsecond)	uint32	事件检测的时间戳微秒（一秒的百万分之一）增量。
规则 ID（签名 ID）(Rule ID (Signature	uint32	与事件对应的规则标识号。
生成器 ID (Generator ID)	uint32	生成事件的 Cisco Secure Firewall 系统预处理器的标识号。
规则修订 (Rule Revision)	uint32	规则版本号。
分类 ID (Classification ID)	uint32	事件分类消息的标识号。
优先级 ID (Priority ID)	uint32	与事件相关的优先级的标识号。
源 IP 地址 (Source IP Address)	uint8[16]	事件中使用的源 IPv4 或 IPv6 地址。
目标	uint8[16]	事件中使用的目标 IPv4 或 IPv6 地址。
源端口或 ICMP 类型 (Source Port or ICMP Type)	uint16	如果事件协议类型是 TCP 或 UDP，则为源端口号，或者如果事件是由 ICMP 流量引起的，则为 ICMP 类型。
目标端口或 ICMP 代码 (Destination Port or ICMP Code)	uint16	如果事件协议类型是 TCP 或 UDP，则为目标端口号，或者如果事件是由
IP 协议 ID (IP Protocol ID)	uint8	IANA 指定的协议号。例如: ▪ 0 - IP ▪ 1 - ICMP ▪ 6 - TCP ▪ 17 - UDP

表 B-9　　入侵事件记录 7.0 字段 （续）

字段	数据类型	说明 (Description)
影响标志 (Impact Flags)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到管理中心上的特定优先级中。x 表示值可以为 0 或 1: ▪ 灰色（0，未知）： 00X00000 ▪ 红色（1，易受攻击）： XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）： 00X0011X ▪ 黄色（3，当前不易受攻击）： 00X0001X ▪ 蓝色（4，未知目标）： 00X00001
影响 (Impact)	uint8	事件的影响标志值。其值如下: ▪ 1 - 红色（易受攻击） ▪ 2 - 橙色（可能易受攻击） ▪ 3 - 黄色（目前不易受攻击） ▪ 4 - 蓝色（未知目标） ▪ 5 - 灰色（未知影响）
内联结果	uint8	表示内联结果的值。 ▪ 0 — 通过 ▪ 1 — 已丢弃 ▪ 2 — 将被丢弃（但配置不允许） ▪ 3— 已部分丢弃

表 B-9 入侵事件记录 7.0 字段 （续）

字段	数据类型	说明 (Description)
内联结果原因	uint8	指示内联结果原因的值。 ▪ 1— 被动或分流模式下的接口 ▪ 2— “检测”检测模式下的入侵策略 ▪ 3— “检测”检测模式下的网络分析策略 ▪ 4— 连接超时 ▪ 5— 连接已关闭（内部使用） ▪ 6— 连接已关闭（内部使用） ▪ 7— 连接已关闭（内部使用）
MPLS 标签 (MPLS Label)	uint32	MPLS 标签。
VLAN ID	uint16	表示数据包起源的 VLAN 的 ID。
Pad	uint16	已保留供将来使用。
策略 UUID (Policy UUID)	uint8[16]	充当入侵策略的唯一标识符的策略 ID 号码。
用户 ID	uint32	用户的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
访问控制规则 ID (Access Control Rule ID)	uint32	充当访问控制规则的唯一标识符的规则 ID 号码。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	充当访问控制策略的唯一标识符的策略 ID 号码。
接口入口 UUID (Interface Ingress UUID)	uint8[16]	充当入口接口的唯一标识符的接口 ID 号码。
接口出口 UUID (Interface Egress UUID)	uint8[16]	充当出口接口的唯一标识符的接口 ID 号码。
安全区入口 UUID (Security Zone Ingress UUID)	uint8[16]	充当入口安全区的唯一标识符的区域 ID 号码。

表 B-9　　入侵事件记录 7.0 字段 （续）

字段	数据类型	说明 (Description)
安全区出口 UUID (Security Zone Egress UUID)	uint8[16]	充当出口安全区的唯一标识符的区域 ID 号码。
连接时间戳 (Connection Timestamp)	uint32	与入侵事件关联的连接事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
连接实例 ID (Connection Instance ID)	uint16	生成连接事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8[16]	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-9 入侵事件记录 7.0 字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
网络分析策略 UUID (Network Analysis Policy UUID)	uint8[16]	创建入侵事件的网络分析策略的 UUID。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。

表 B-9　　入侵事件记录 7.0 字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含入口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“入口 VRF ”(Ingress VRF) 名称字段中的字节数。
入口 VRF 名称	字符串	用于流量进入网络的虚拟路由器。
字符串块类型 (String Block Type)	uint32	启动包含出口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“出口 VRF ”(Egress VRF) 名称字段中的字节数。
出口 VRF 名称	字符串	用于流量离开网络的虚拟路由器。
Snort 版本	uint8	Snort 版本号。

入侵影响警报数据

入侵影响警报事件包含影响事件的相关信息。当将入侵事件与系统网络映射数据进行比较且影响已确定时，系统传输入侵影响警报数据。该记录使用记录类型为 9 的标准记录报头，后面跟着数据块类型为系列 1 数据块组中的 20 的入侵影响警报数据块。（影响警报数据块是系列 1 类型的数据块。有关系列 1 数据块的详细信息，请参阅了解发现（系列 1）块，第 4-60 页。）

您可以通过在请求消息的标志字段中设置位 5 来请求 eStreamer 只传输入侵影响事件。有关请求消息的详细信息，请参阅事件流请求消息格式，第 2-11 页。这些警报的版本 1 只处理 IPv4。5.3 中引入的版本 2 除了处理 IPv4 之外，还处理 IPv6 事件。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (9) (Record Type (9))															
记录长度 (Record Length)																																
入侵影响警报块类型 (20)（Intrusion Impact Alert Block Type (20))																																
入侵影响警报块长度 (Intrusion Impact Alert Block Length)																																
事件 ID (Event ID)																																
设备 ID (设备 ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	事件秒 (Event Second)																															
	影响 (Impact)																															
	源																															
	目标																															
影响 (Impact) 说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明... (Description...)																															

下表对影响事件中的每个数据字段进行了说明。

表 B-10 影响事件数据字段

字段	数据类型	说明 (Description)
入侵影响警报块类型 (Intrusion Impact Alert Block Type)	uint32	表示后面是入侵影响警报数据块。此字段的值始终为 20。请参阅入侵事件和元数据记录类型，第 3-1 页。
入侵影响警报块长度 (Intrusion Impact Alert Block Length)	uint32	表示入侵影响警报数据块的长度，包括后面的所有数据以及入侵影响警报块类型和长度的 8 个字节。
事件 ID (Event ID)	uint32	表示事件标识号。
设备 ID	uint32	表示受管设备标识号。
事件秒 (Event Second)	uint32	表示检测到事件的秒数（从 1970/01/01 起）。

表 B-10　影响事件数据字段 （续）

字段	数据类型	说明 (Description)
影响 (Impact)	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到“防御中心”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1: ▪ （0，未知）： 00X00000 ▪ 红色（1，易受攻击）： XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）： 00X0011X ▪ 黄色（3，当前不易受攻击）： 00X0001X ▪ 蓝色（4，未知目标）： 00X00001
源 IP 地址 (Source IP Address)	uint8[4]	与影响事件相关的主机的 IP 地址，采用 IP 地址八位组。
目标 IP 地址:	uint8[4]	与影响事件相关的目标 IP 地址的 IP 地址（如适用），采用 IP 地址八位组。如果无目标 IP 地址，则此值为 0。
字符串块类型 (String Block Type)	uint32	启动包含影响名称的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-67 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数。这包括字符串块类型的四个字节，字符串块长度的四个字节以及说明中的字节数。
说明 (Description)	字符串	影响事件的说明。

入侵事件额外数据记录

eStreamer 服务可传输与入侵事件额外数据记录中的入侵事件相关的事件额外数据。记录类型始终为 110。

此记录在版本 7.1 中已弃用。虽然仍然可以请求，但不会生成任何记录。

事件额外数据出现在封装事件额外数据数据块中，该数据块的数据块类型值始终为 4。（事件额外数据数据块是系列 2 数据块。有关系列 2 数据块的详细信息，请参阅了解系列 2 数据块，第 3-55 页。）

支持的额外数据类型包括 IPv6 源地址和目标地址，以及通过 HTTP 代理或负载均衡器与网络服务器连接的客户端的源 IP 地址（v4 或 v6）。下图显示入侵事件额外数据记录的格式。

如果在请求消息的“请求标志”(Request Flags) 字段中设置位 27，您将收到每个入侵事件的事件额外数据。如果设置位 20，您也会收到入侵事件额外数据元数据，第 B-67 页中描述的事件额外数据元数据。如果启用位 23，eStreamer 将包含扩展事件报头。有关设置请求标志的信息，请参阅请求标志，第 2-12 页。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (110)（Record Type (110))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
事件额外数据数据块类型 (4) (Event Extra Data Data Block Type (4))																																
事件额外数据数据块长度 (Event Extra Data Data Block Length)																																
设备 ID (设备 ID)																																
事件 ID (Event ID)																																
事件秒 (Event Second)																																
类型 (Type)																																
BLOB 块类型 (1) (BLOB Block Type (1))																																
BLOB 长度 (BLOB Length)																																
事件额外数据 (Event Extra Data)																																

请注意，事件额外数据块结构包含一个 BLOB 块类型，该块类型是 Cisco Secure Firewall 系统版本 4.10 中引入的几种可变长度数据结构之一。

下表对入侵事件额外数据记录中的字段进行了说明。

表 B-11　　入侵事件额外数据数据块字段

字段	数据类型	说明 (Description)
事件额外数据数据块类型 (Event Extra Data Data Block Type)	uint32	启动事件额外数据数据块。值始终为 4。块类型为系列 2 数据块；有关详细信息，请参阅了解系列 2 数据块，第 3-55 页。
事件额外数据数据块长度 (Event Extra Data Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的
设备 ID	uint32	受管设备标识号。
事件 ID (Event ID)	uint32	事件标识号。
事件秒 (Event Second)	uint32	事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
类型 (Type)	uint32	额外数据类型的标识符；例如： ▪ 2 - XFF 客户端 (IPv6) ▪ 9 - HTTP URI
BLOB 块类型 (BLOB Block Type)	uint32	启动包含额外数据的 BLOB 数据块。值始终为 1。块类型为系列 2 数据块。
长度 (Length)	uint32	BLOB 数据块中的字节总数。
额外数据 (Extra Data)	变量	额外数据的内容。数据类型在“类型”(Type) 字段中指示。

入侵事件额外数据元数据

eStreamer 服务可传输与入侵事件额外数据元数据记录中的入侵事件额外数据记录相关的事件额外数据元数据。记录类型始终为 111。

此记录在版本 7.1 中已弃用。虽然仍然可以请求，但不会生成任何记录。

事件额外数据元数据出现在封装事件额外数据元数据数据块中，该数据块的数据块类型值始终为 5。事件额外数据数据块是系列 2 数据块。

如果在请求消息的“请求标志”(Request Flags) 字段中设置位 20，您将收到事件额外数据元数据。如果想收到入侵事件和事件额外数据元数据，还必须设置位 2。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (111) (Record Type (111))															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
事件额外数据元数据数据块类型 (5) (Event Extra Data Metadata Data Block Type (5))																																
数据块长度 (Data Block Length)																																
类型 (Type)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
名称...(Name...)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
编码 (Encoding)																																

请注意，块结构包含封装字符串块类型，该块类型是 Cisco Secure Firewall 系统 版本 4.10 中引入的几种系列 2 可变长度数据结构之一。

下表对事件额外数据元数据记录中的字段进行了说明。

表 B-12　事件额外数据元数据数据块字段

字段	数据类型	说明 (Description)
事件额外数据元数据数据块类型 (Event Extra Data Metadata Data Block Type)	uint32	启动事件额外数据元数据数据块。值始终为 5。块类型为系列 2 数据块。
事件额外数据元数据数据块长度 (Event Extra Data Metadata Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的
类型 (Type)	uint32	额外数据的类型。与关联事件额外数据记录中的类型字段匹配。 此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。块类型为系列 2 数据块。
字符串块长度 (String Block Length)	uint32	客户端应用版本字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上版本字符串中的字节数。
名称 (Name)	字符串	事件额外数据类型的名称，例如 XFF 客户端 (IPv6) 和 HTTP URI。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。块类型为系列 2 数据块。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 URL 字符串中的字节数。
编码 (Encoding)	字符串	用于事件额外数据的编码，如 IPv4、IPv6 或字符串。

旧版恶意软件事件数据结构

恶意软件事件数据块 5.1

eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 16。您可以通过在事件版本为 1 且事件代码为 101 的请求消息中设置恶意软件事件标志（请求标志字段中的位 30）将该事件作为恶意软件事件记录的一部进行请求。

下图显示恶意软件事件数据块的结构:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	恶意软件事件块类型 (16)（Malware Event Block Type (16)）																															
	恶意软件事件块长度 (Malware Event Block Length)																															
	代理 UUID (Agent UUID) 代理 UUID (Agent UUID)（续） 代理 UUID (Agent UUID)（续） 代理 UUID (Agent UUID)（续）																															
	云 UUID (Cloud UUID) 云 UUID (Cloud UUID)（续） 云 UUID (Cloud UUID)（续） 云 UUID (Cloud UUID)（续）																															
	时间戳 (Timestamp)																															
	事件类型 ID (Event Type ID)																															
	事件子类型 ID (Event Subtype ID)								主机 IP 地址 (Host IP Address)																							
检测名称 (Detection Name)	主机 IP 地址 (Host IP Address)（续）								检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0))（续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length)（续）																检测名称... (Detection Name...)															
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户... (User...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列... (File SHA Hash...)																															
	文件大小 (File Size)																															
	面向终端的 AMP 文件类型 (File								文件时间戳 (File Timestamp)																							
父文件名称 (Name)	文件时间戳 (File Timestamp)（续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0))（续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)（续）								父文件名... (Parent File Name...)																							
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列... (Parent File SHA Hash...)																															
事件说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件说明... (Event Description...)																															

下表对恶意软件事件数据块中的字段进行了说明。

表 B-13 恶意软件事件数据块字段

字段	数据类型	说明 (Description)
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 16。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的恶意软件感知网络的内部唯一 ID。
时间戳 (Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint8	导致恶意软件检测的操作的内部 ID。
主机 IP 地址 (Host IP Address)	uint32	与恶意软件事件相关的主机 IP 地址。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“检测名称”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户”(User) 字段中的字节数。
用户	字符串	安装思科代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件名”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。

表 B-13　恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件路径”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件 SHA 散列”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 哈希值。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小（字节）。
面向终端的 AMP 文件类型 (File	uint8	被检测或隔离文件的文件类型。
文件时间戳 (File Timestamp)	uint32	被检测或隔离的文件的创建时间戳。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件名”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件 SHA 散列”(Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件说明”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。

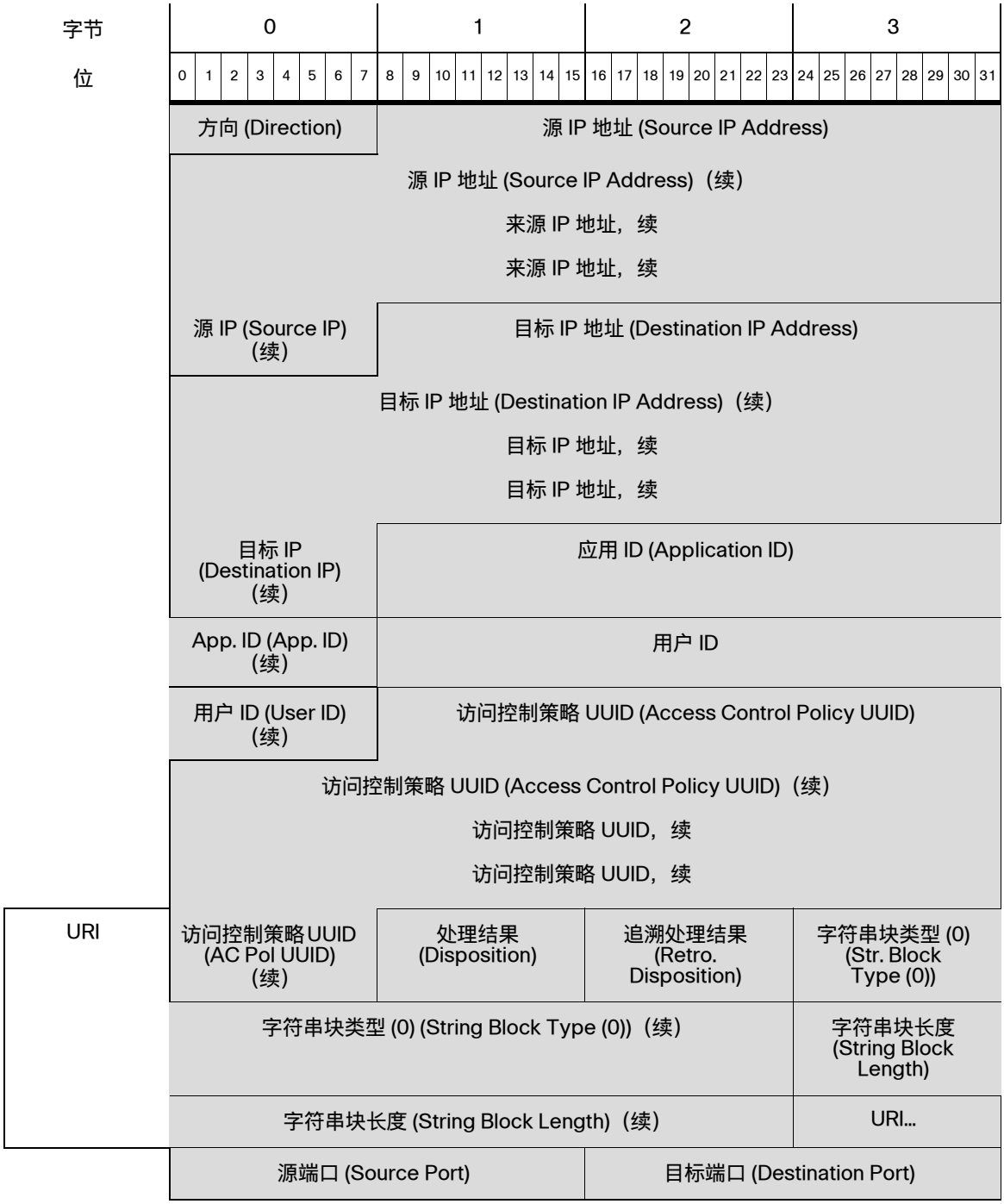
恶意软件事件数据块 5.1.1.x

eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 24。您可以通过在事件版本为 2 且事件代码为 101 的请求消息中设置恶意软件事件标志（请求标志字段中的位 30）将该事件作为恶意软件事件记录的一部进行请求。

下图显示恶意软件事件数据块的结构:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	恶意软件事件块类型 (24) (Malware Event Block Type (24))																															
	恶意软件事件块长度 (Malware Event Block Length)																															
	代理 UUID (Agent UUID) 代理 UUID (Agent UUID)（续） 代理 UUID (Agent UUID)（续） 代理 UUID (Agent UUID)（续）																															
	云 UUID (Cloud UUID) 云 UUID (Cloud UUID)（续） 云 UUID (Cloud UUID)（续） 云 UUID (Cloud UUID)（续）																															
	恶意软件事件时间戳 (Malware Event Timestamp)																															
	事件类型 ID (Event Type ID)																															
	事件子类型 ID (Event Subtype ID)								主机 IP 地址 (Host IP Address)																							
检测名称 (Detection Name)	主机 IP 地址 (Host IP Address)（续）								检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))														
	字符串块类型 (0) (String Block Type (0))（续）																字符串块长度 (String Block Length)														
	字符串块长度 (String Block Length)（续）																检测名称... (Detection Name...)														
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户... (User...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列... (File SHA Hash...)																															
	文件大小 (File Size)																															
	面向终端的 AMP 文件类型 (File								文件时间戳 (File Timestamp)																							
父文件名称 (Name)	文件时间戳 (File Timestamp)（续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0))（续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)（续）								父文件名... (Parent File Name...)																							
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列... (Parent File SHA Hash...)																															
事件说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件说明... (Event Description...)																															
	设备 ID (设备 ID)																															
	连接实例 (Connection Instance)																连接计数器 (Connection Counter)															
	连接事件时间戳 (Connection Event Timestamp)																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
方向 (Direction)
源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address)（续）
来源 IP 地址，续
来源 IP 地址，续
源 IP (Source IP)（续）
目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address)（续）
目标 IP 地址，续
目标 IP 地址，续
目标 IP (Destination IP)（续）
应用 ID (Application ID)
App. ID (App. ID)（续）
用户 ID
用户 ID (User ID)（续）
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID，续
访问控制策略 UUID，续
URI
访问控制策略 UUID (AC Pol UUID)（续）
处理结果 (Disposition)
追溯处理结果 (Retro. Disposition)
字符串块类型 (0) (Str. Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
URI...
源端口 (Source Port)
目标端口 (Destination Port)

下表对恶意软件事件数据块中的字段进行了说明。

表 B-14　　用于 5.1.1.x 的恶意软件事件数据块字段

字段	数据类型	说明 (Description)
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 24。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的恶意软件感知网络的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint8	导致恶意软件检测的操作的内部 ID。
主机 IP 地址 (Host IP Address)	uint32	与恶意软件事件相关的主机 IP 地址。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“检测名称”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户”(User) 字段中的字节数。
用户	字符串	安装思科代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件名”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。

表 B-14 用于 5.1.1.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件路径”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件 SHA 散列”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小（字节）。
面向终端的 AMP 文件类型 (File	uint8	被检测或隔离文件的文件类型。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件名”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件 SHA 散列”(Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件说明”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID	uint32	生成事件的设备的 ID。

表 B-14　　用于 5.1.1.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值: ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN - 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN - 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE - 文件包含恶意软件。 ▪ 4 - CACHE_MISS - 软件无法向思科云发送请求以了解处置情况。 ▪ 5 - NO_CLOUD_RESP - 思科云服务未响应此请求。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与“处置情况”(Disposition) 字段包含的值相同。可能值与“处置情况”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。

表 B-14 用于 5.1.1.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。

恶意软件事件数据块 5.2.x

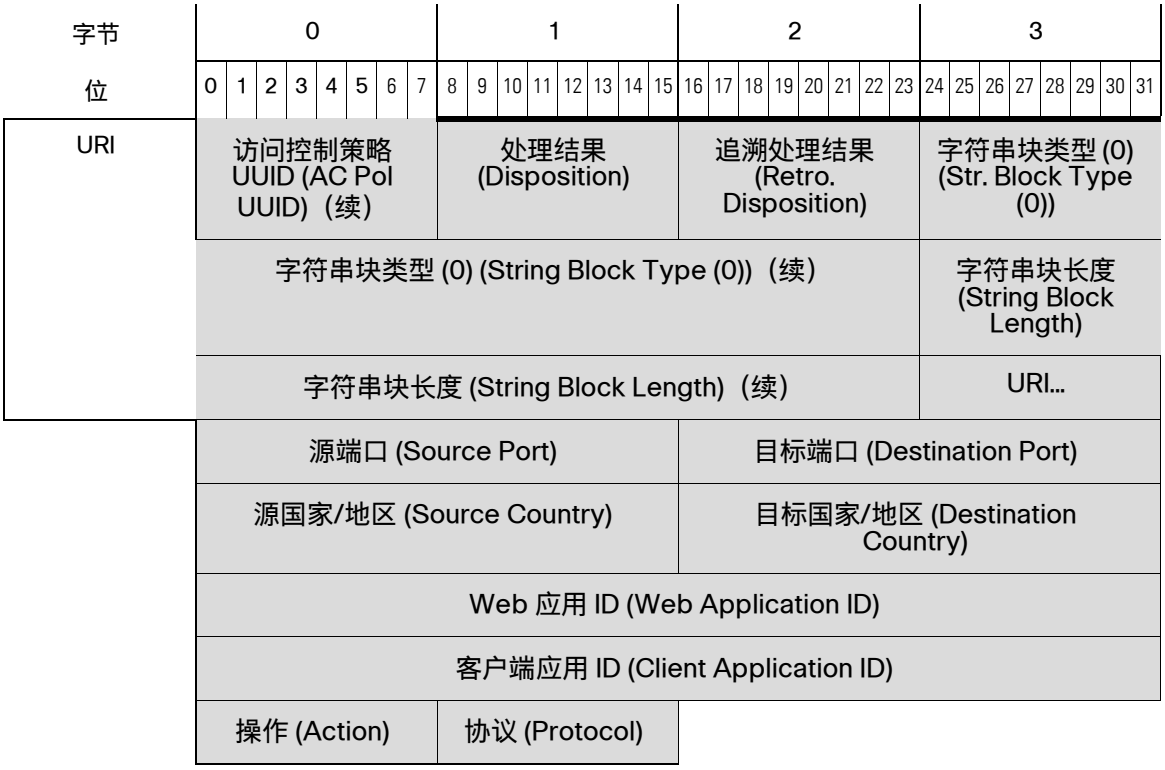
eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 33。您可以通过在事件版本为 3 且事件代码为 101 的请求消息中设置恶意软件事件标志（请求标志字段中的位 30）将该事件作为恶意软件事件记录的一部进行请求。

下图显示恶意软件事件数据块的结构:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
恶意软件事件块类型 (33) (Malware Event Block Type (33))																																
恶意软件事件块长度 (Malware Event Block Length)																																
代理 UUID (Agent UUID)																																
代理 UUID (Agent UUID)（续）																																
代理 UUID (Agent UUID)（续）																																
代理 UUID (Agent UUID)（续）																																
云 UUID (Cloud UUID)																																
云 UUID (Cloud UUID)（续）																																
云 UUID (Cloud UUID)（续）																																
云 UUID (Cloud UUID)（续）																																
恶意软件事件时间戳 (Malware Event Timestamp)																																
事件类型 ID (Event Type ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
检测名称 (Detection Name)	事件子类型 ID (Event Subtype ID)								检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0))（续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length)（续）																检测名称... (Detection Name...)															
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户... (User...)																															
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列... (File SHA Hash...)																															
	文件大小 (File Size)																															
	面向终端的 AMP 文件类型 (File																															
	文件时间戳 (File Timestamp)																															
父文件名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件名... (Parent File Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列... (Parent File SHA Hash...)																															
事件说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件说明... (Event Description...)																															
	设备 ID (设备 ID)																															
	连接实例 (Connection Instance)																连接计数器 (Connection Counter)															
	连接事件时间戳 (Connection Event Timestamp)																															
	方向 (Direction)								源 IP 地址 (Source IP Address)																							
	源 IP 地址 (Source IP Address)（续）																															
	来源 IP 地址，续																															
	来源 IP 地址，续																															
	源 IP (Source IP)（续）								目标 IP 地址 (Destination IP Address)																							
	目标 IP 地址 (Destination IP Address)（续）																															
	目标 IP 地址，续																															
	目标 IP 地址，续																															
	目标 IP (Destination IP)（续）								应用 ID (Application ID)																							
	App. ID (App. ID)（续）								用户 ID																							
	用户 ID (User ID)（续）								访问控制策略 UUID (Access Control Policy UUID)																							
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID，续																															
	访问控制策略 UUID，续																															



下表对恶意软件事件数据块中的字段进行了说明。

表 B-15　　用于 5.2.x 的恶意软件事件数据块字段

字段	数据类型	说明 (Description)
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 33。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的恶意软件感知网络的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint8	导致恶意软件检测的操作的内部 ID。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。

表 B-15　用于 5.2.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“检测名称”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户”(User) 字段中的字节数。
用户	字符串	安装思科代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件名”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件路径”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件 SHA 散列”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小（字节）。
面向终端的 AMP 文件类型 (File	uint8	被检测或隔离文件的文件类型。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件名”(Parent File Name) 字段中的字节数。

表 B-15　　用于 5.2.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件 SHA 散列”(Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件说明”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值: ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。

表 B-15 用于 5.2.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN - 文件是安全的，不包含恶意软件。 ▪ 2 - NEUTRAL - 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE - 文件包含恶意软件。 ▪ 4 - CACHE_MISS - 软件无法向思科云发送请求以了解处置情况，或思科云服务未响应此请求。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与“处置情况”(Disposition) 字段包含的值相同。可能值与“处置情况”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度(String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
客户端应用ID(Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值: ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。

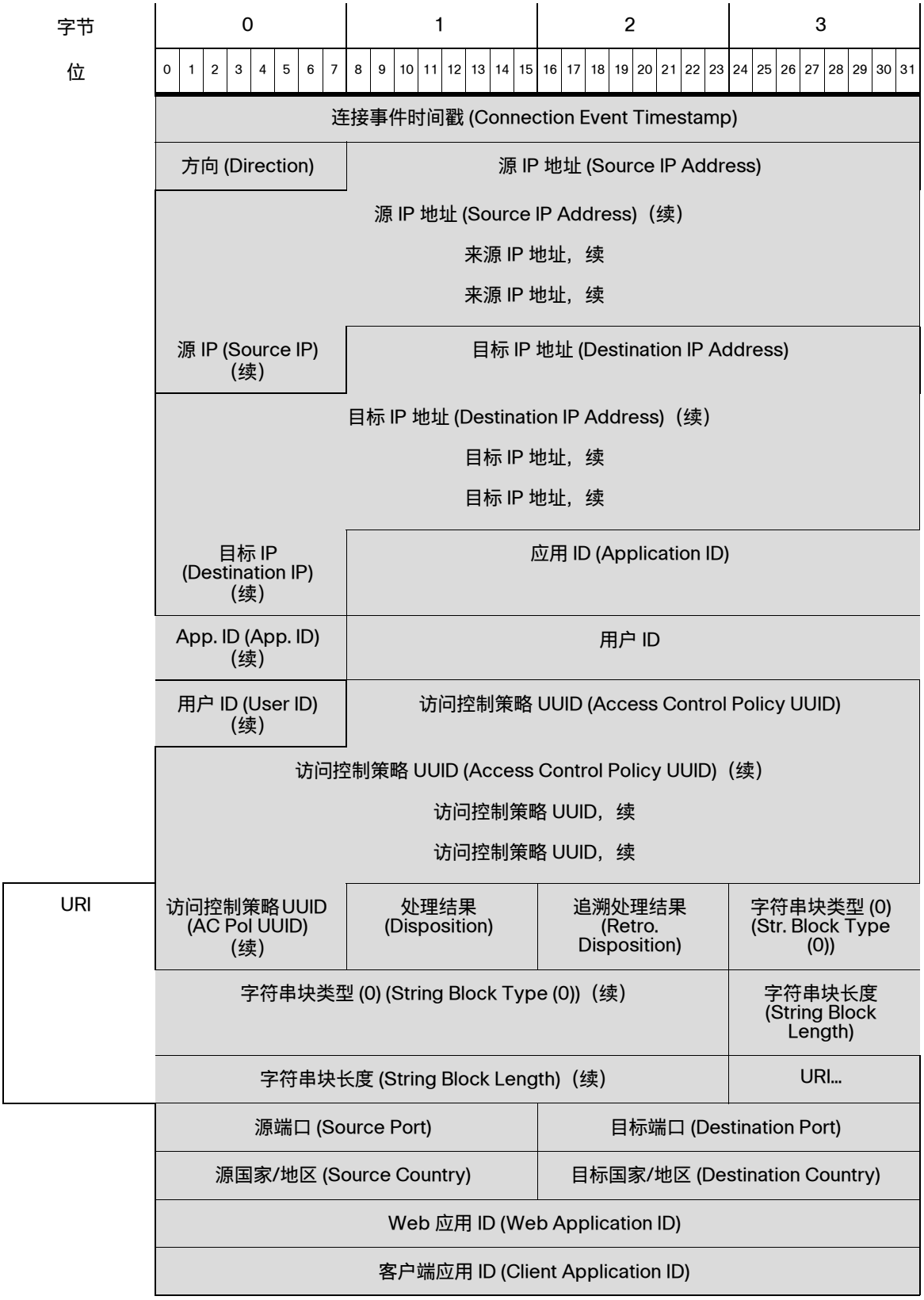
恶意软件事件数据块 5.3

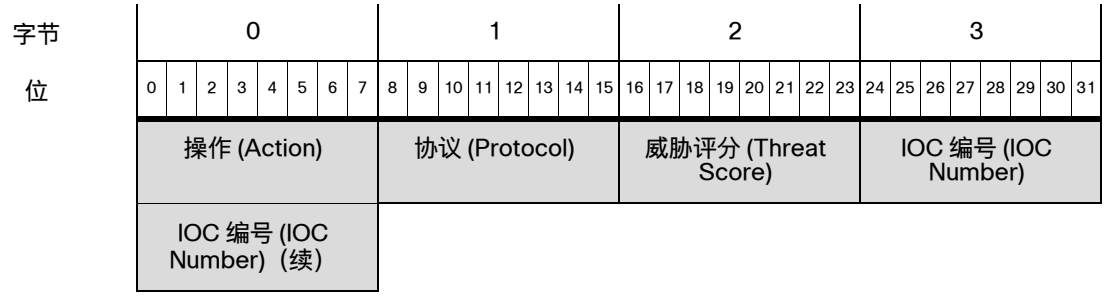
eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 35。您可以通过在事件版本为 4 且事件代码为 101 的请求消息中设置恶意软件事件标志（请求标志字段中的位 30）将该事件作为恶意软件事件记录的一部进行请求。

下图显示恶意软件事件数据块的结构：

字节	0				1			
位	0 1 2 3 4 5 6 7				8 9 10 11 12 13 14 15			
	恶意软件事件块类型 (35) (Malware Event Block Type (35))							
	恶意软件事件块长度 (Malware Event Block Length)							
	代理 UUID (Agent UUID)							
	代理 UUID (Agent UUID)（续）							
	代理 UUID (Agent UUID)（续）							
	代理 UUID (Agent UUID)（续）							
	云 UUID (Cloud UUID)							
	云 UUID (Cloud UUID)（续）							
	云 UUID (Cloud UUID)（续）							
	云 UUID (Cloud UUID)（续）							
	恶意软件事件时间戳 (Malware Event Timestamp)							
	事件类型 ID (Event Type ID)							
	事件子类型 ID (Event Subtype ID)							
检测名称 (Detection Name)	检测器 ID (Detector ID)				字符串块类型 (0) (String Block Type (0))			
	字符串块类型 (0) (String Block Type (0))（续）				字符串块长度 (String Block Length)			
	字符串块长度 (String Block Length)（续）				检测名称... (Detection Name...)			

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户... (User...)																															
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列... (File SHA Hash...)																															
	文件大小 (File Size)																															
	面向终端的 AMP 文件类型 (File																															
	文件时间戳 (File Timestamp)																															
父文件名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件名... (Parent File Name...)																															
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列... (Parent File SHA Hash...)																															
事件说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件说明... (Event Description...)																															
	设备 ID (设备 ID)																															
	连接实例 (Connection Instance)																连接计数器 (Connection Counter)															


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
连接事件时间戳 (Connection Event Timestamp)
方向 (Direction)
源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address)（续）
来源 IP 地址，续
来源 IP 地址，续
源 IP (Source IP)（续）
目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address)（续）
目标 IP 地址，续
目标 IP 地址，续
目标 IP (Destination IP)（续）
应用 ID (Application ID)
App. ID (App. ID)（续）
用户 ID
用户 ID (User ID)（续）
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID，续
访问控制策略 UUID，续
URI
访问控制策略 UUID (AC Pol UUID)（续）
处理结果 (Disposition)
追溯处理结果 (Retro. Disposition)
字符串块类型 (0) (Str. Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
URI...
源端口 (Source Port)
目标端口 (Destination Port)
源国家/地区 (Source Country)
目标国家/地区 (Destination Country)
Web 应用 ID (Web Application ID)
客户端应用 ID (Client Application ID)



下表对恶意软件事件数据块中的字段进行了说明。

表 B-16 用于 5.3 的恶意软件事件数据块字段

字段	数据类型	说明 (Description)
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 35。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的恶意软件感知网络的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint32	导致恶意软件检测的操作的内部 ID。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“检测名称”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户”(User) 字段中的字节数。
用户	字符串	安装思科代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。

表 B-16　用于 5.3 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件名”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件路径”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件 SHA 散列”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小（字节）。
面向终端的 AMP 文件类型 (File	uint8	被检测或隔离文件的文件类型。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-40 页。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件名”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件 SHA 散列”(Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。

表 B-16 用于 5.3 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件说明”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值: ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE 文件包含恶意软件。 ▪ 4 - UNAVAILABLE 软件无法向 云发送请求以了解设备情况，或 云服务设备响应此请求。 ▪ 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与“处置情况”(Disposition) 字段包含的值相同。可能值与“处置情况”(Disposition) 字段包含的值相同。

表 B-16　　用于 5.3 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值: ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。

恶意软件事件数据块 5.3.1

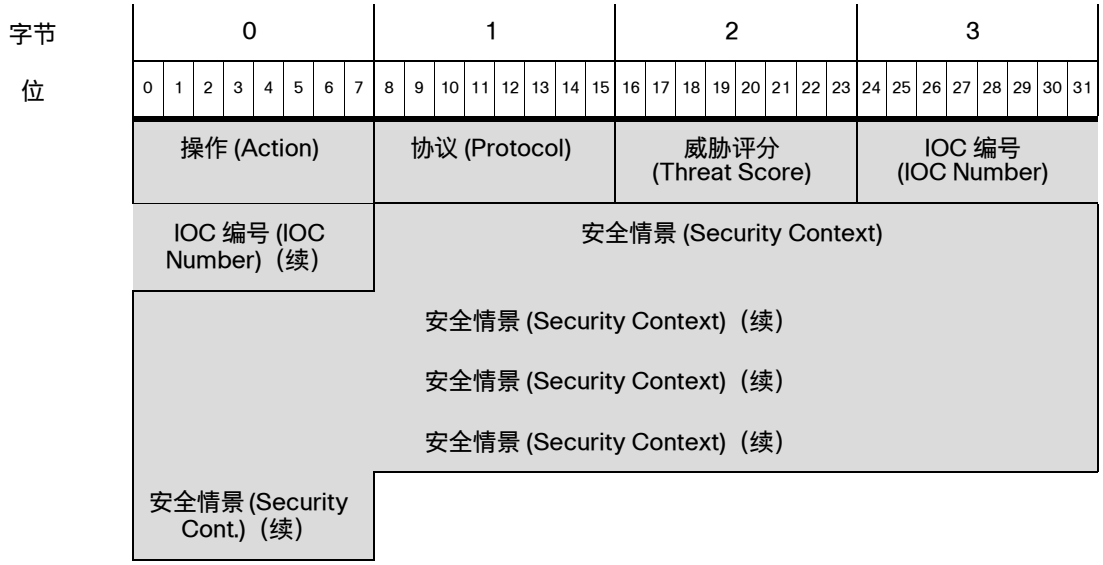
eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 44。它替代了块 35。您可以通过在事件版本为 5 且事件代码为 101 的请求消息中设置恶意软件事件标志（请求标志字段中的位 30）将该事件作为恶意软件事件记录的一部分进行请求。

下图显示恶意软件事件数据块的结构:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	恶意软件事件块类型 (44) (Malware Event Block Type (44))																															
	恶意软件事件块长度 (Malware Event Block Length)																															
	代理 UUID (Agent UUID) 代理 UUID (Agent UUID)（续） 代理 UUID (Agent UUID)（续） 代理 UUID (Agent UUID)（续）																															
	云 UUID (Cloud UUID) 云 UUID (Cloud UUID)（续） 云 UUID (Cloud UUID)（续） 云 UUID (Cloud UUID)（续）																															
	恶意软件事件时间戳 (Malware Event Timestamp)																															
	事件类型 ID (Event Type ID)																															
	事件子类型 ID (Event Subtype ID)																															
检测名称 (Detection Name)	检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0))（续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)（续）								检测名称... (Detection Name...)																							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户... (User...)																															
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列... (File SHA Hash...)																															
	文件大小 (File Size)																															
	面向终端的 AMP 文件类型 (File																															
	文件时间戳 (File Timestamp)																															
父文件名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件名... (Parent File Name...)																															
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列... (Parent File SHA Hash...)																															
事件说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件说明... (Event Description...)																															
	设备 ID (Device ID)																															
	连接实例 (Connection Instance)																连接计数器 (Connection Counter)															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	连接事件时间戳 (Connection Event Timestamp)																															
	方向 (Direction)								源 IP 地址 (Source IP Address)																							
	源 IP 地址 (Source IP Address)（续）																															
	来源 IP 地址，续																															
	来源 IP 地址，续																															
	源 IP (Source IP)（续）								目标 IP 地址 (Destination IP Address)																							
	目标 IP 地址 (Destination IP Address)（续）																															
	目标 IP 地址，续																															
	目标 IP 地址，续																															
	目标 IP (Destination IP)（续）								应用 ID (Application ID)																							
	App. ID (App. ID)（续）								用户 ID																							
	用户 ID (User ID)（续）								访问控制策略 UUID (Access Control Policy UUID)																							
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID，续																															
	访问控制策略 UUID，续																															
URI	访问控制策略 UUID (AC Pol UUID)（续）								处理结果 (Disposition)								追溯处理结果 (Retro. Disposition)								字符串块类型 (0) (Str. Block Type (0))							
	字符串块类型 (0) (String Block Type (0))（续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length)（续）																								URI...							
	源端口 (Source Port)																目标端口 (Destination Port)															
	源国家/地区 (Source Country)																目标国家/地区 (Destination Country)															
	Web 应用 ID (Web Application ID)																															
	客户端应用 ID (Client Application ID)																															



下表对恶意软件事件数据块中的字段进行了说明。

表 B-17　　用于 5.3.1 的恶意软件事件数据块字段

字段	数据类型	说明 (Description)
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 44。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的 思科高级恶意软件防护云的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint32	导致恶意软件检测的操作的内部 ID。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“检测名称”(Detection Name) 字段中的字节数。

表 B-17 用于 5.3.1 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户”(User) 字段中的字节数。
用户	字符串	安装思科代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件名”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件路径”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件 SHA 散列”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小（字节）。
面向终端的 AMP 文件类型 (File	uint8	被检测或隔离文件的文件类型。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-40 页。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件名”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件SHA散列的字符串数据块。值始终为0。

表 B-17　　用于 5.3.1 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件 SHA 散列”(Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件说明”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值: ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。

表 B-17 用于 5.3.1 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE 文件包含恶意软件。 ▪ 4 - UNAVAILABLE 软件无法向 云发送请求以了解情况，或 云服务响应此请求。 ▪ 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与“处置情况”(Disposition) 字段包含的值相同。可能值与“处置情况”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值: ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表

表 B-17　　用于 5.3.1 的恶意软件事件数据块字段 （续）

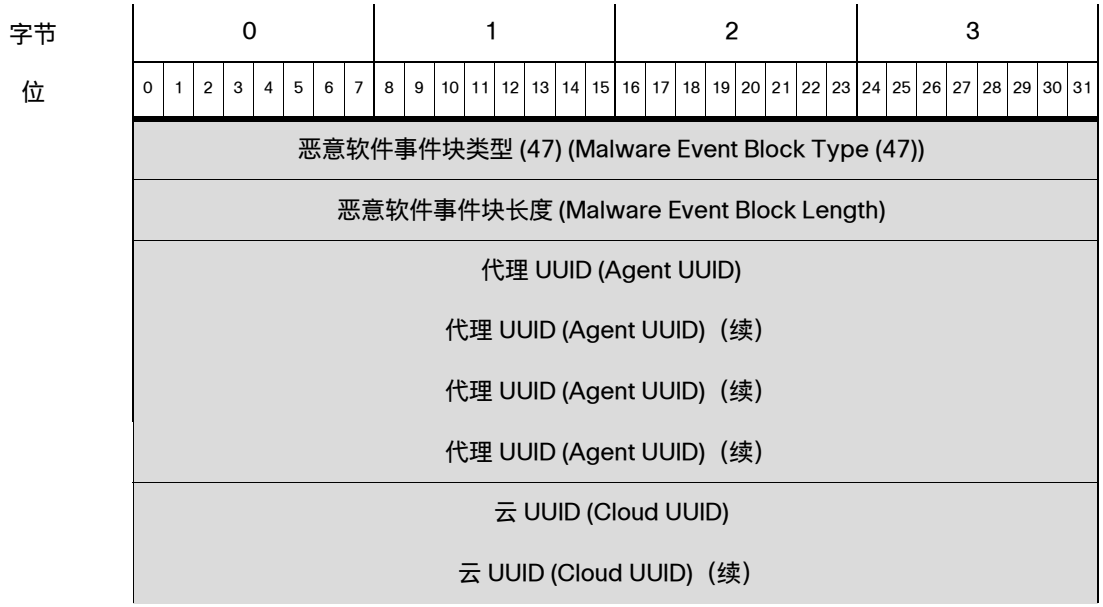
字段	数据类型	说明 (Description)
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

恶意软件事件数据块 5.4.x

eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 47。它替代了块 44，然后被块替代。已添加用于 SSL 和文件存档支持的字段。

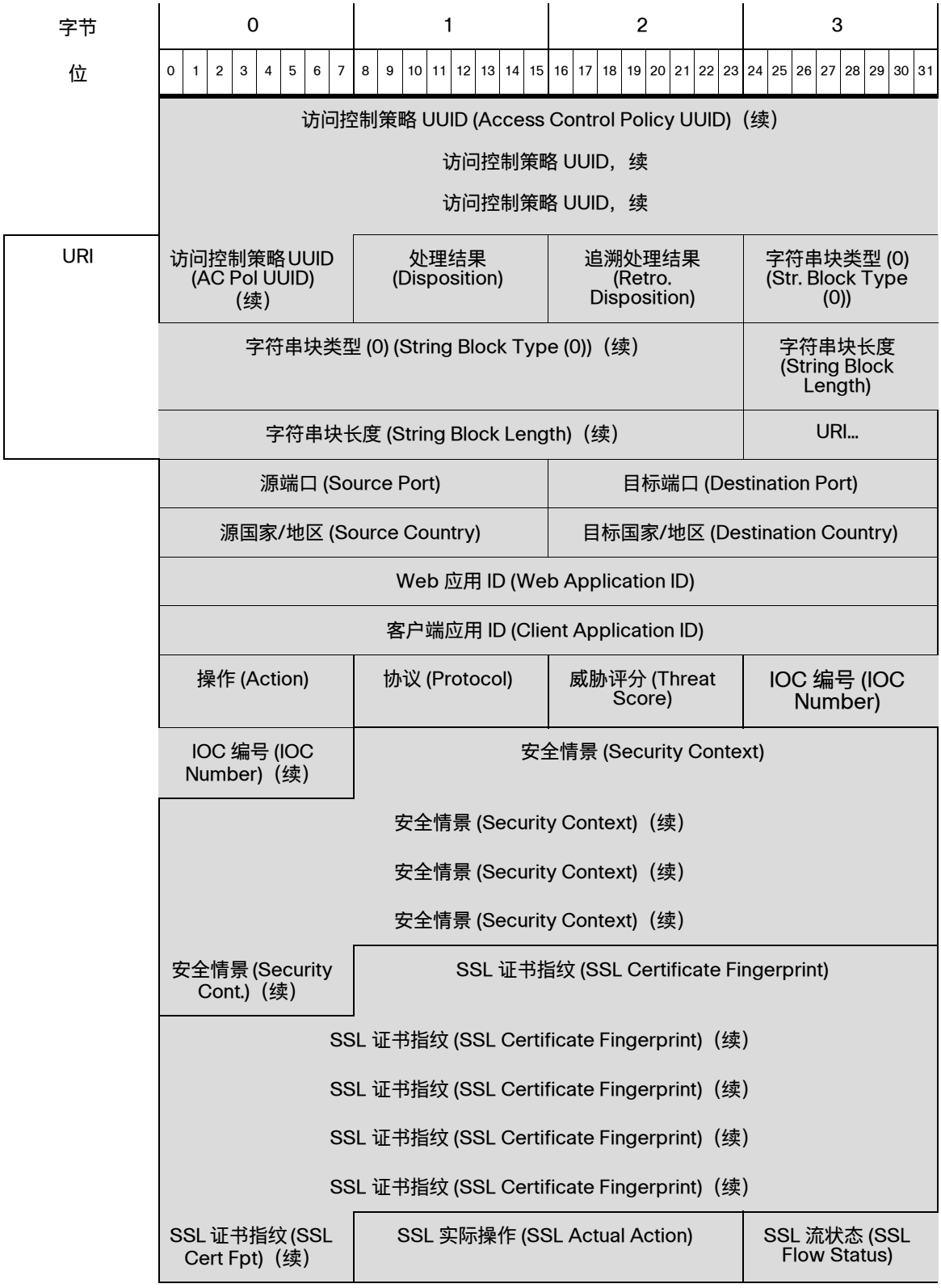
您可以通过在事件版本为 6 且事件代码为 101 的请求消息中设置恶意软件事件标志（请求标志字段中的位 30）将该事件作为恶意软件事件记录的一部进行请求。

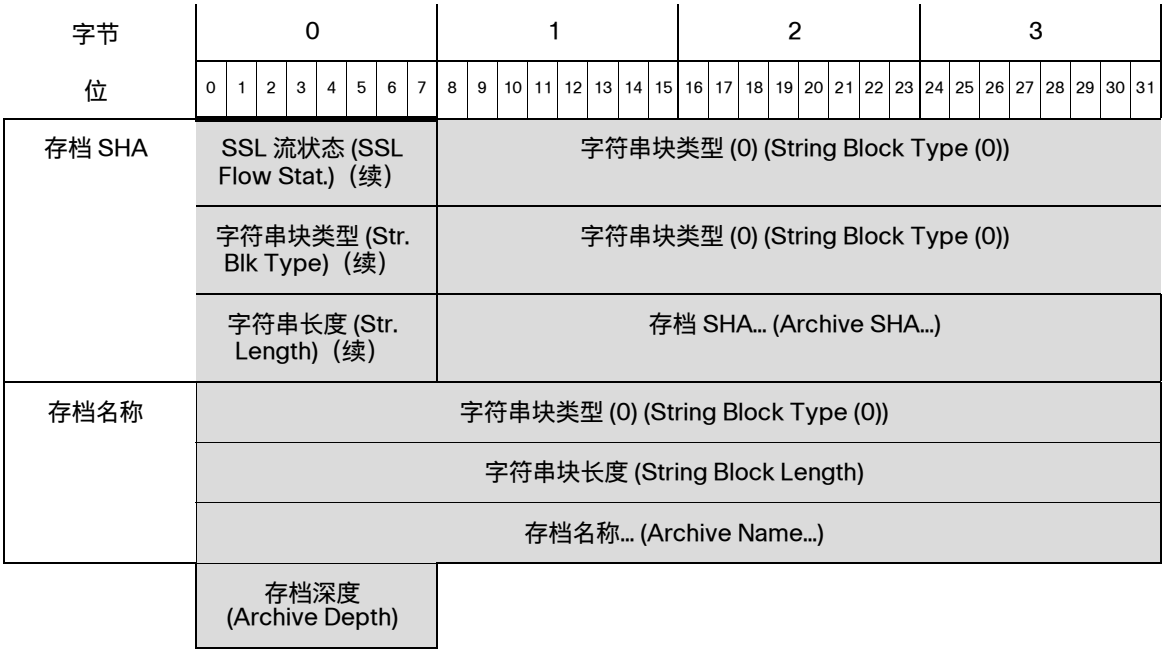
下图显示恶意软件事件数据块的结构:



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	云 UUID (Cloud UUID)（续）																															
	云 UUID (Cloud UUID)（续）																															
	恶意软件事件时间戳 (Malware Event Timestamp)																															
	事件类型 ID (Event Type ID)																															
	事件子类型 ID (Event Subtype ID)																															
检测名称 (Detection Name)	检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0))（续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)（续）								检测名称... (Detection Name...)																							
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户... (User...)																															
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列... (File SHA Hash...)																															
	文件大小 (File Size)																															
	面向终端的 AMP 文件类型 (File																															
	文件时间戳 (File Timestamp)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
父文件名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件名... (Parent File Name...)																															
父文件 SHA 散列	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件 SHA 散列... (Parent File SHA Hash...)																															
事件说明 (Description)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件说明... (Event Description...)																															
	设备 ID (Device ID)																															
	连接实例 (Connection Instance)																连接计数器 (Connection Counter)															
	连接事件时间戳 (Connection Event Timestamp)																															
	方向 (Direction)								源 IP 地址 (Source IP Address)																							
	源 IP 地址 (Source IP Address)（续）																															
	来源 IP 地址，续																															
	来源 IP 地址，续																															
	源 IP (Source IP)（续）								目标 IP 地址 (Destination IP Address)																							
	目标 IP 地址 (Destination IP Address)（续）																															
	目标 IP 地址，续																															
	目标 IP 地址，续																															
	目标 IP (Destination IP)（续）								应用 ID (Application ID)																							
	App. ID (App. ID)（续）								用户 ID																							
	用户 ID (User ID)（续）								访问控制策略 UUID (Access Control Policy UUID)																							


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID，续
访问控制策略 UUID，续
URI
访问控制策略 UUID (AC Pol UUID)（续）
处理结果 (Disposition)
追溯处理结果 (Retro. Disposition)
字符串块类型 (0) (Str. Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
URI...
源端口 (Source Port)
目标端口 (Destination Port)
源国家/地区 (Source Country)
目标国家/地区 (Destination Country)
Web 应用 ID (Web Application ID)
客户端应用 ID (Client Application ID)
操作 (Action)
协议 (Protocol)
威胁评分 (Threat Score)
IOC 编号 (IOC Number)
IOC 编号 (IOC Number)（续）
安全情景 (Security Context)
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Cont.)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Cert Fpt)（续）
SSL 实际操作 (SSL Actual Action)
SSL 流状态 (SSL Flow Status)



下表对恶意软件事件数据块中的字段进行了说明。

表 B-18　　用于 5.4.x 的恶意软件事件数据块字段

字段	数据类型	说明 (Description)
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 47。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的AMP代理的内部唯一ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的 思科高级恶意软件防护云的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint32	导致恶意软件检测的操作的内部 ID。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。

表 B-18 用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“检测名称”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户”(User) 字段中的字节数。
用户	字符串	安装思科代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件名”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件路径”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件 SHA 散列”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小（字节）。
面向终端的 AMP 文件类型 (File	uint8	被检测或隔离文件的文件类型。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-40 页。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件名”(Parent File Name) 字段中的字节数。

表 B-18　用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件 SHA 散列”(Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件说明”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值: ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。

表 B-18 用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE 文件包含恶意软件。 ▪ 4 - UNAVAILABLE 软件无法向 云发送请求以了解情况，或 云服务响应此请求。 ▪ 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与“处置情况”(Disposition) 字段包含的值相同。可能值与“处置情况”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。

表 B-18　用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值: ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表 ▪ 6 - 云查找超时 ▪ 7 - 自定义检测 ▪ 8 - 自定义检测阻止 ▪ 9 - 存档阻止（超出深度） ▪ 10 - 存档阻止（已加密） ▪ 11 - 存档阻止（检查失败）
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-18 用于 5.4.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
字符串块类型 (String Block Type)	uint32	启动包含存档 SHA 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档 SHA 字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。

表 B-18　　用于 5.4.x 的恶意软件事件数据块字段 （续）

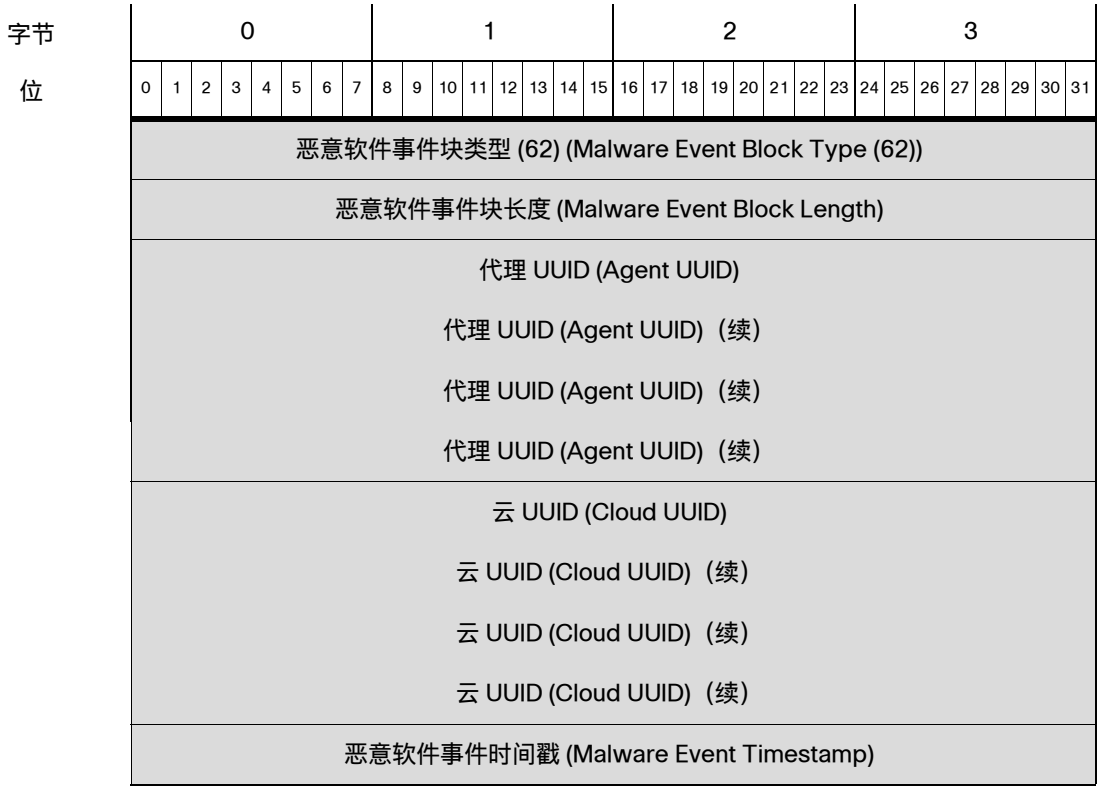
字段	数据类型	说明 (Description)
存档 SHA (Archive SHA)	字符串	包含该文件的父存档的 SHA1 散列。
字符串块类型 (String Block Type)	uint32	启动包含“存档名称”(Archive Name) 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上入侵策略名称中的字节数。
存档名称 (Archive Name)	字符串	父存档的名称。
存档深度 (Archive Depth)	uint8	嵌套文件的层数。例如，如果文本文件位于压缩存档中，则此值为 1。

恶意软件事件数据块 6.x

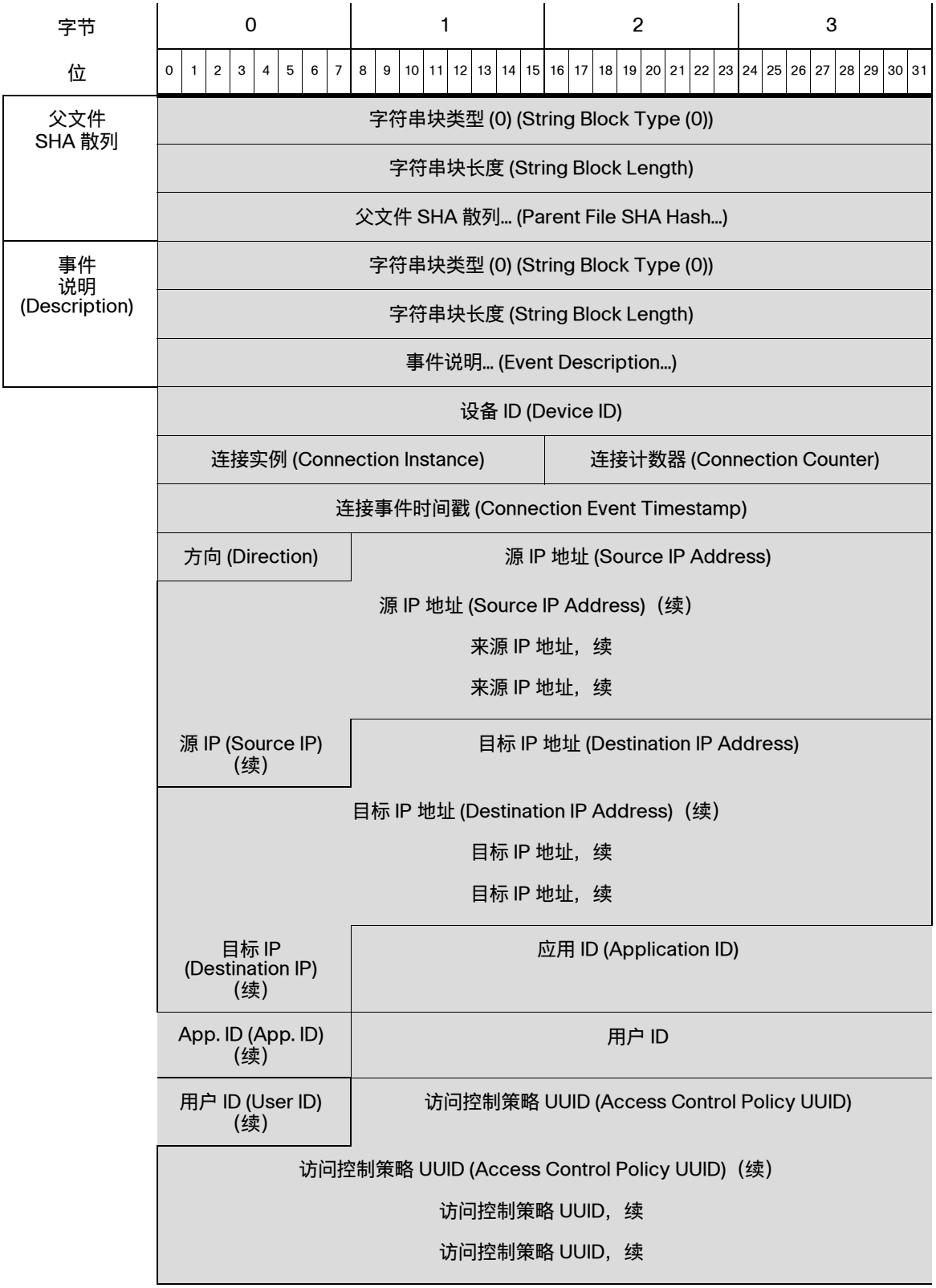
eStreamer 服务使用恶意软件事件数据块存储有关恶意软件事件的信息。这些事件包含关于在云内检测到或被隔离的恶意软件、检测方法以及受恶意软件影响的主机和用户的信息。恶意软件事件数据块的块类型为系列 2 数据块组中的 62。它替代了块 47。已添加 HTTP 响应字段。它被块 80 替代。

您可以通过在事件版本为 7 且事件代码为 101 的请求消息中设置恶意软件事件标志（“请求标志”(Request Flags) 字段中的位 30），将该事件作为恶意软事件记录的一部分进行请求。

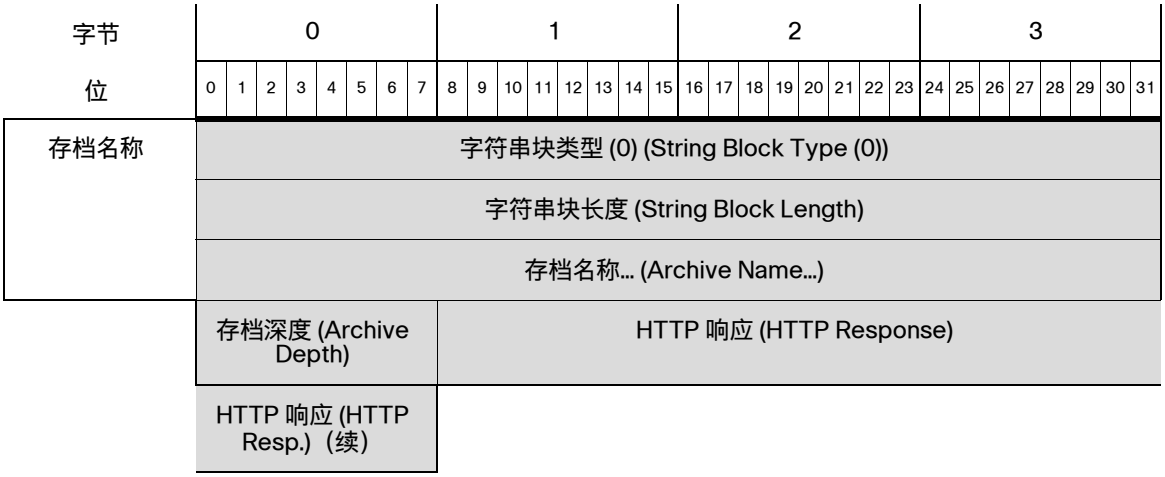
下图显示恶意软件事件数据块的结构。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	事件类型 ID (Event Type ID)																															
	事件子类型 ID (Event Subtype ID)																															
检测名称 (Detection Name)	检测器 ID (Detector ID)								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0))（续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)（续）								检测名称... (Detection Name...)																							
用户	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户... (User...)																															
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名... (File Name...)																															
文件路径	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件路径... (File Path...)																															
文件 SHA 哈希	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件 SHA 散列... (File SHA Hash...)																															
	文件大小 (File Size)																															
	面向终端的 AMP 文件类型 (File																															
	文件时间戳 (File Timestamp)																															
父文件名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	父文件名... (Parent File Name...)																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
父文件 SHA 散列
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
父文件 SHA 散列... (Parent File SHA Hash...)
事件说明 (Description)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
事件说明... (Event Description...)
设备 ID (Device ID)
连接实例 (Connection Instance)
连接计数器 (Connection Counter)
连接事件时间戳 (Connection Event Timestamp)
方向 (Direction)
源 IP 地址 (Source IP Address)
源 IP 地址 (Source IP Address)（续）
来源 IP 地址，续
来源 IP 地址，续
源 IP (Source IP) (续)
目标 IP 地址 (Destination IP Address)
目标 IP 地址 (Destination IP Address)（续）
目标 IP 地址，续
目标 IP 地址，续
目标 IP (Destination IP) (续)
应用 ID (Application ID)
App. ID (App. ID) (续)
用户 ID
用户 ID (User ID) (续)
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID，续
访问控制策略 UUID，续

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
URI	访问控制策略 UUID (AC Pol UUID) (续)								处理结果 (Disposition)								追溯处理结果 (Retro. Disposition)								字符串块类型 (0) (Str. Block Type (0))							
	字符串块类型 (0) (String Block Type (0)) (续)																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length) (续)																								URI...							
	源端口 (Source Port)																目标端口 (Destination Port)															
	源国家/地区 (Source Country)																目标国家/地区 (Destination Country)															
	Web 应用 ID (Web Application ID)																															
	客户端应用 ID (Client Application ID)																															
	操作 (Action)								协议 (Protocol)								威胁评分 (Threat Score)								IOC 编号 (IOC Number)							
	IOC 编号 (IOC Number) (续)								安全情景 (Security Context)																							
	安全情景 (Security Context) (续)																															
	安全情景 (Security Context) (续)																															
	安全情景 (Security Context) (续)																															
	安全情景 (Security Cont.) (续)								SSL 证书指纹 (SSL Certificate Fingerprint)																							
	SSL 证书指纹 (SSL Certificate Fingerprint) (续)																															
	SSL 证书指纹 (SSL Certificate Fingerprint) (续)																															
	SSL 证书指纹 (SSL Certificate Fingerprint) (续)																															
	SSL 证书指纹 (SSL Certificate Fingerprint) (续)																															
	SSL 证书指纹 (SSL Cert Fpt) (续)								SSL 实际操作 (SSL Actual Action)																SSL 流状态 (SSL Flow Status)							
存档 SHA	SSL 流状态 (SSL Flow Stat.) (续)								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (Str. Blk Type) (续)								字符串块类型 (0) (String Block Type (0))																							
	字符串长度 (Str. Length) (续)								存档 SHA... (Archive SHA...)																							



下表对恶意软件事件数据块中的字段进行了说明。

表 B-19　　用于 6.x 的恶意软件事件数据块字段

字段	数据类型	说明 (Description)
恶意软件事件块类型 (Malware Event Block Type)	uint32	启动恶意软件事件数据块。值始终为 62。
恶意软件事件块长度 (Malware Event Block Length)	uint32	恶意软件事件数据块中的字节总数，包括恶意软件事件块类型和长度字段的八个字节，加上随后的数据字节数。
代理 UUID (Agent UUID)	uint8[16]	报告恶意软件事件的面向终端的 AMP 代理的内部唯一 ID。
云 UUID (Cloud UUID)	uint8[16]	发生恶意软件事件的 AMP 云的内部唯一 ID。
恶意软件事件时间戳 (Malware Event Timestamp)	uint32	恶意软件事件生成时间戳。
事件类型 ID (Event Type ID)	uint32	恶意软件事件类型的内部 ID。
事件子类型 ID (Event Subtype ID)	uint32	导致恶意软件检测的操作的内部 ID。
检测器 ID (Detector ID)	uint8	检测到恶意软件的检测技术的内部 ID。
字符串块类型 (String Block Type)	uint32	启动包含检测名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	检测名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“检测名称”(Detection Name) 字段中的字节数。
检测名称 (Detection Name)	字符串	检测到或被隔离的恶意软件的名称。

表 B-19 用于 6.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户”(User) 字段中的字节数。
用户	字符串	安装思科代理并发生恶意软件事件的计算机的用户。请注意，这些用户未绑定到用户发现。
字符串块类型 (String Block Type)	uint32	启动包含文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件名”(File Name) 字段中的字节数。
文件名 (File Name)	字符串	被检测或隔离的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含文件路径的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件路径字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件路径”(File Path) 字段中的字节数。
文件路径 (File Path)	字符串	被检测或隔离的文件的文件路径，不包括文件名。
字符串块类型 (String Block Type)	uint32	启动包含文件 SHA 散列的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“文件 SHA 散列”(File SHA Hash) 字段中的字节数。
文件 SHA 散列 (File SHA Hash)	字符串	被检测或隔离的文件 SHA-256 散列值的呈现字符串。
文件大小 (File Size)	uint32	被检测或隔离的文件的大小（字节）。
面向终端的 AMP 文件类型 (File	uint32	被检测或隔离文件的文件类型。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-40 页。
文件时间戳 (File Timestamp)	uint32	创建被检测或隔离的文件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
字符串块类型 (String Block Type)	uint32	启动包含父文件名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	父文件名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件名”(Parent File Name) 字段中的字节数。
父文件名 (Parent File Name)	字符串	检测期间访问被检测或隔离文件的文件的名称。
字符串块类型 (String Block Type)	uint32	启动包含父文件 SHA 散列的字符串数据块。值始终为 0。

表 B-19　用于 6.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	父文件 SHA 散列字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“父文件 SHA 散列”(Parent File SHA Hash) 字段中的字节数。
父文件 SHA 散列 (Parent File SHA Hash)	字符串	检测期间访问被检测或隔离文件的父文件的 SHA-256 哈希值。
字符串块类型 (String Block Type)	uint32	启动包含事件说明的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	事件说明字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“事件说明”(Event Description) 字段中的字节数。
活动说明 (Event Description)	字符串	与事件类型相关的其他事件信息。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或 IDS
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接事件时间戳 (Connection Event Timestamp)	uint32	连接事件的时间戳。
方向 (Direction)	uint8	表示文件是否已上传或下载。可能会有以下值: ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的标识号。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	作为触发事件的访问控制策略的唯一标识符的标别号。

表 B-19 用于 6.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE 文件包含恶意软件。 ▪ 4 - UNAVAILABLE 软件无法向 AMP 云发送请求以了解处置情况，或 AMP 云服务未响应此请求。 ▪ 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
追溯处置情况 (Retrospective Disposition)	uint8	处置情况更新后的处置情况。如果处置情况未更新，则此字段包含的值与“处置情况”(Disposition) 字段包含的值相同。可能值与“处置情况”(Disposition) 字段包含的值相同。
字符串块类型 (String Block Type)	uint32	启动包含 URI 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	URI 数据块中的字节数，包括块类型和报头字段的八个字节，加上 URI 字段中的字节数。
URI	字符串	连接的 URI。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint 16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。

表 B-19　　用于 6.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值: ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表 ▪ 6 - 云查找超时 ▪ 7 - 自定义检测 ▪ 8 - 自定义检测阻止 ▪ 9 - 存档阻止（超出深度） ▪ 10 - 存档阻止（已加密） ▪ 11 - 存档阻止（检查失败）
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
IOC 编号 (IOC Number)	uint16	与此事件相关的威胁的 ID 号码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-19 用于 6.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
字符串块类型 (String Block Type)	uint32	启动包含存档 SHA 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档 SHA 字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。

表 B-19　用于 6.x 的恶意软件事件数据块字段 （续）

字段	数据类型	说明 (Description)
存档 SHA (Archive SHA)	字符串	包含该文件的父存档的 SHA1 散列。
字符串块类型 (String Block Type)	uint32	启动包含“存档名称”(Archive Name) 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上入侵策略名称中的字节数。
存档名称 (Archive Name)	字符串	父存档的名称。
存档深度 (Archive Depth)	uint8	嵌套文件的层数。例如，如果文本文件位于压缩存档中，则此值为 1。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。

旧版发现数据结构

旧版发现事件报头

发现事件报头 5.0 - 5.1.1.x

发现和连接事件消息包含发现事件报头。它传送事件的类型和子类型、事件发生的时间、出现该事件的设备以及消息中事件数据的结构。报头后面是实际主机发现、用户或连接事件数据。按事件类型划分的主机发现结构，第 4-42 页中介绍了与不同事件类型/子类型值相关的结构。

发现事件报头的事件类型和事件子类型字段用于识别传输的事件消息的结构。一旦确定事件数据块的结构，您的程序即可对消息进行适当解析。

下图中的阴影行举例说明了发现事件报头的格式。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	报头版本 (1) (Header Version (1))																消息类型 (4) (Message Type (4))															
	消息长度 (Message Length)																															

	Netmap ID	记录类型 (Record Type)
	记录长度 (Record Length)	
	eStreamer 服务器时间戳 (eStreamer Server Timestamp) （在事件中，只有当位 23 已设置时）	
	留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）	
发现事件报头 (Discovery Event Header)	设备 ID (设备 ID)	
	IP 地址 (IP Addresses)	
	MAC 地址	
	MAC 地址 (MAC Address)（续）	留作未来使用 (Reserved for future use)
	事件秒 (Event Second)	
	事件微秒 (Event Microsecond)	
	保留（内部） (Reserved (Internal))	事件类型 (Event Type)
	事件子类型	
	文件编号 (File Number)（仅限内部使用）	
	文件位置 (File Position)（仅限内部使用）	

下表对发现事件报头进行了说明。

表 B-20　　发现事件报头字段

字段	数据类型	说明
设备 ID	uint32	生成发现事件的设备的 ID 号码。您可以通过请求版本 3 和版本 4 元数据获取设备的元数据。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
IP 地址 (IP Address)	uint32	事件所涉及主机的 IP 地址。
MAC 地址 (MAC Address)	uint8[6]	事件所涉及主机的 MAC 地址。
留作未来使用 (Reserved for future use)	byte[2]	值设置为 0 的两个字节的填充。
事件秒 (Event Second)	uint32	系统生成事件的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
事件微秒 (Event Microsecond)	uint32	系统生成事件的微秒（一秒的百万分之一）增量。

表 B-20　　发现事件报头字段 （续）

字段	数据类型	说明
保留（内部）(Reserved (Internal))	字节	源自思科的内部数据，可忽略。
事件类型 (Event Type)	uint32	事件类型 (Event Type)（新事件为 1000，变更事件为 1001，用户输入事件为 1002，完整主机配置文件为 1050）。有关可用事件类型列表，请参阅按事件类型划分的主机发现结构，第 4-42 页。
事件子类型 (Event Subtype)	uint32	事件子类型。有关可用事件子类型列表，请参阅按事件类型划分的主机发现结构，第 4-42 页。
文件编号 (File Number)	byte[4]	串行文件编号。此字段供思科内部使用，可以忽略。
文件位置 (File Position)	byte[4]	事件在串行文件中的位置。此字段供思科内部使用，可以忽略。

旧版服务器数据块

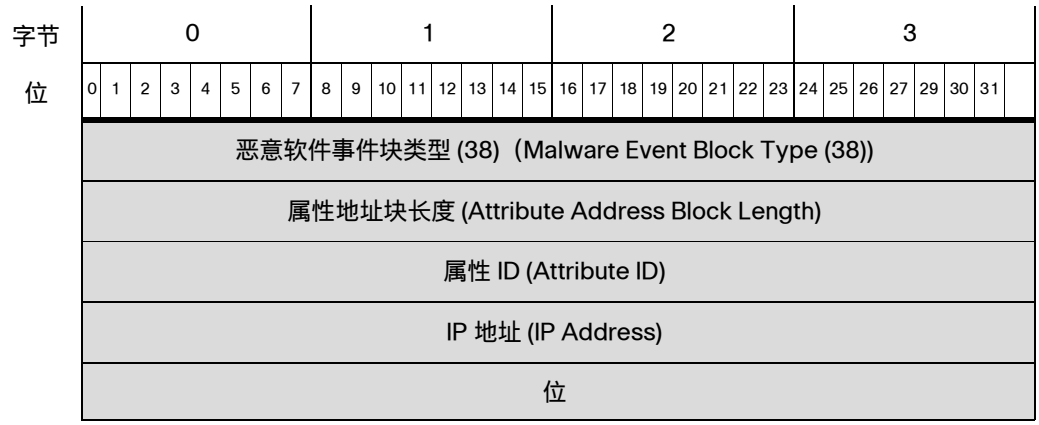
有关详细信息，请参阅以下各节：

- 用于 5.0 - 5.1.1.x 的属性地址数据块，第 B-123 页

用于 5.0 - 5.1.1.x 的属性地址数据块

属性地址数据块包含一个属性列表项目，在属性定义数据块中使用。它的块类型为 38。

下图显示属性地址数据块的基本结构：



下表对属性地址数据块的字段进行了说明。

表 B-21 属性地址数据块字段

字段	数据类型	说明 (Description)
属性地址块类型 (Attribute Address Block Type)	uint32	启动属性地址数据块。值始终为 38。
属性地址块长度 (Attribute Address Block Length)	uint32	属性地址数据块中的字节数，包括属性地址块类型和长度字段的八个字节，加上随后的属性地址数据的字节数。
属性 ID (Attribute ID)	uint32	受影响属性的标识号（如适用）。
IP 地址 (IP Address)	uint8[4]	主机的 IP 地址（如果地址已自动分配），采用 IP 地址八位组。
位	uint32	如果已自动分配 IP 地址，则包含用于计算网络掩码的有效位。

旧版客户端应用数据块

有关详细信息，请参阅以下各节：

- 用于 5.0 - 5.1 的用户客户端应用数据块，第 B-124 页

用于 5.0 - 5.1 的用户客户端应用数据块

用户客户端应用数据块包含客户端应用数据来源、添加数据的用户的标识号以及 IP 地址范围数据块列表的相关信息。用户客户端应用数据块的块类型为 59。

下图显示用户客户端应用数据块的基本结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户客户端应用块类型 (59)（User Client Application Block Type (59)）																															
	用户客户端应用块长度 (User Client Application Block Length)																															
IP 地址 (IP Addresses) 范围	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IP 范围规格数据块 (IP Range Specification Data Blocks)*																															
	应用协议 ID (Application Protocol ID)																															
	客户端应用 ID (Client Application ID)																															

版本	字符串块类型 (0) (String Block Type (0))
	字符串块长度 (String Block Length)
	版本...(Version...)

下表对用户客户端应用数据块的字段进行了说明。

表 B-22　　用户客户端应用数据块字段

字段	字节数	说明 (Description)
用户客户端应用块类型 (User Client Application Block Type)	uint32	启动用户客户端应用数据块。此值始终为。
用户客户端应用块长度 (User Client Application Block Length)	uint32	用户客户端应用数据块中的字节总数，包括用户客户端应用块类型和长度字段的八个字节，加上随后的用户客户端应用数据的字节数。
通用列表块类型 (Generic List Block	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅表 4-59用户服务器数据块字段，第 4-101 页。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号（如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动包含客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用版本字符串数据块中的字节数，包括字符串块类型和长度字段，加上版本中的字节数。
版本	字符串	客户端应用版本。

旧版扫描结果数据块

有关详细信息，请参阅以下各节：

- 扫描结果数据块 5.0 - 5.1.1.x，第 B-126 页
- 用于 5.0.x 的用户产品数据块，第 B-129 页
- 用于 5.x 的用户信息数据块，第 B-150 页

扫描结果数据块 5.0 - 5.1.1.x

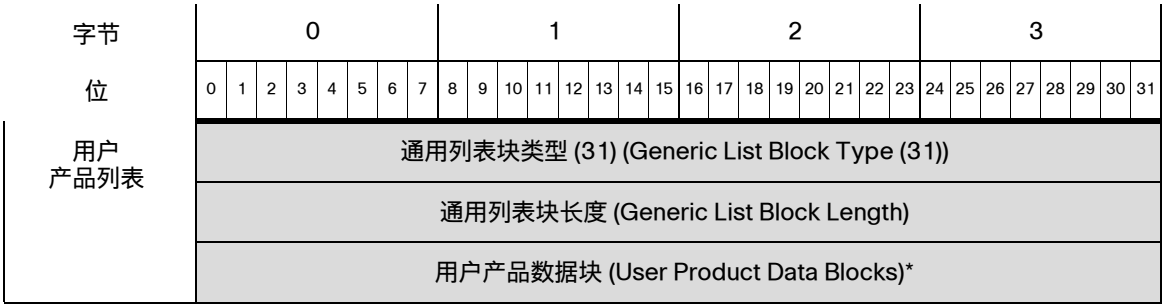
扫描结果数据块对漏洞进行说明，在添加扫描结果事件（事件类型 1002，子类型 11）中使用。扫描结果数据块的块类型为 102。

下图显示扫描结果数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	扫描结果块类型 (102)（Scan Result Block Type (102)）																															
	扫描结果块长度 (Scan Result Block Length)																															
	用户 ID																															
	扫描类型 (Scan Type)																															
	IP 地址																															
	端口																协议															
	标志																列表块类型 (11) (List Block Type (11))															
	列表块类型 (11) (List Block Type (11))																列表块长度 (List Block Length)															
漏洞列表	列表块长度 (List Block Length)																扫描漏洞块类型 (109) (Scan Vulnerability Block Type (109))															
	扫描漏洞块类型 (109) (Scan Vulnerability Block Type (109))																扫描漏洞块长度 (Scan Vulnerability Block Length)															
	扫描漏洞块长度 (Scan Vulnerability Block Length)																漏洞数据...(Vulnerability Data...)															
	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
Scan Results 列表	一般扫描结果块类型 (108) (Generic Scan Results Block Type (108)																															
	一般扫描结果块长度 (Generic Scan Results Block Length)																															
	一般扫描结果...(Generic Scan Results...)																															

扫描漏洞列表 (Scan Vulnerability List)

一般扫描结果列表 (Generic Scan Results List)



下表对扫描结果数据块的字段进行了说明。

表 B-23　　扫描结果数据块字段

字段	数据类型	说明 (Description)
扫描结果块类型 (Scan Result Block Type)	uint32	启动扫描结果数据块。值始终为 102。
扫描结果块长度 (Scan Result Block Length)	uint32	扫描漏洞数据块中的字节数，包括扫描漏洞块类型和长度字段的八个字节，加上随后的扫描漏洞数据的字节数。
用户 ID	uint32	包含导入扫描结果或运行产生该扫描结果的扫描的用户的用户标识号。
扫描类型	uint32	表明结果是如何添加到系统中的。
IP 地址 (IP Address)	uint32	受结果中的漏洞影响的主机的 IP 地址，采用 IP 地址八位组。
端口 (Port)	uint16	受结果中的漏洞影响的子服务器使用的端口。
协议 (Protocol)	uint16	IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP
标志	uint16	保留
列表块类型 (List Block Type)	uint32	启动由传送传输扫描漏洞数据的扫描漏洞数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装扫描漏洞数据块。 此字段后面是零个或多个扫描漏洞数据块。
扫描漏洞块类型 (Scan Vulnerability Block Type)	uint32	启动对扫描期间检测到的漏洞进行说明的扫描漏洞数据块。值始终为 109。

表 B-23 扫描结果数据块字段 （续）

字段	数据类型	说明 (Description)
扫描漏洞块长度 (Scan Vulnerability Block Length)	uint32	扫描漏洞数据块中的字节数，包括扫描漏洞块类型和长度字段的八个字节，加上随后的扫描漏洞数据中的字节数。
漏洞数据 (Vulnerability Data)	字符串	每个漏洞的相关信息。
列表块类型 (List Block Type)	uint32	启动由传送传输扫描漏洞数据的扫描漏洞数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装扫描漏洞数据块。 此字段后面是零个或多个扫描漏洞数据块。
一般扫描结果块类型 (Generic Scan Results Block Type)	uint32	启动对扫描期间检测到的服务器和操作系统数据进行说明的一般扫描结果数据块。值始终为 108。
一般扫描结果块长度 (Generic Scan Results Block Length)	uint32	一般扫描结果数据块中的字节数，包括一般扫描结果块类型和长度字段的八个字节，加上随后的扫描结果数据中的字节数。
一般扫描结果数据 (Generic Scan Results Data)	字符串	每个扫描结果的相关信息。
通用列表块类型 (Generic List Block	uint32	启动由传送第三方应用中的主机输入数据的用户产品数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装用户产品数据块。
用户产品数据块 (User Product Data Blocks) *	变量	包含主机输入数据的用户产品数据块。有关此数据块的说明，请参阅用户产品数据块 5.1+，第 4-173 页。

用于 5.0.x 的用户产品数据块

用户产品数据块传输从第三方应用导入的主机输入数据，包括第三方应用字符串映射。此数据块在连接统计信息数据块 6.0.x，第 B-236 页和用户服务器和操作系统消息，第 4-55 页中使用。在版本 4.10.x 中，用户产品数据块的块类型为 65，在版本 5.0 - 5.0.x 中，其块类型为 118。这两种块类型的结构相同。

注释　下图中数据块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示用户产品数据块的格式:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户产品数据块类型 (65	118) (User Product Data Block Type (65	118))																													
	用户产品块长度 (User Product Block Length)																															
	源 ID (Source ID)																															
	源类型 (Source Type)																															
IP 地址 (IP Addresses) 范围	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IP 范围规格数据块 (IP Range Specification Data Blocks)*																															
	端口																协议															
	丢弃用户产品 (Drop User Product)																															
自定义供应商字符串 (Custom Vendor String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	自定义供应商字符串...(Custom Vendor String...)																															
自定义产品字符串 (Custom Product String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	自定义产品字符串...(Custom Product String...)																															
自定义版本字符串 (Custom Version String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	自定义版本字符串...(Custom Version String...)																															
	软件 ID (Software ID)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	服务器 ID (Server ID)																															
	供应商 ID (Vendor ID)																															
	产品 ID (Product ID)																															
主版本 (Major Version) 字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	主版本字符串...(Major Version String...)																															
次版本 (Minor Version) 字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	次版本字符串...(Minor Version String...)																															
修订版 (Revision) 字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	修订版字符串...(Revision String...)																															
至主版本字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	至主版本字符串...(To Major Version String...)																															
至次版本字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	至次版本字符串...(To Minor Version String...)																															
至修订版字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	至修订版字符串...(To Revision String...)																															
内部版本字符串 (Build String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	内部版本字符串...(Build String...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
修补版本字符串 (Patch String)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	修补版本字符串...(Patch String...)																															
分机 (Extension) 字符串	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	扩展版本字符串...(Extension String...)																															
操作系统 UUID (OS UUID)	操作系统 UUID (Operating System UUID)																															
	操作系统 UUID (Operating System UUID)（续）																															
	操作系统 UUID (Operating System UUID)（续）																															
	操作系统 UUID (Operating System UUID)（续）																															
修复列表 (List of Fixes)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	修复列表数据块 (Fix List Data Blocks)*																															

下表对用户产品数据块的组件进行了说明。

表 B-24　　用于 4.10.x、5.0-5.0.x 的用户产品数据块字段

字段	数据类型	说明 (Description)
用户产品数据块类型 (User Product Data Block Type)	uint32	启动用户产品数据块。在版本 4.10.x 中，此值为 65，在版本 5.0 - 5.0.x 中，此值为 118。
用户产品块长度 (User Product Block Length)	uint32	用户产品数据块中的字节总数，包括用户产品块类型和长度字段的八个字节，加上随后的用户产品数据中的字节数。
源 ID (Source ID)	uint32	导入数据的源的标识号。
源类型 (Source Type)	uint32	提供数据的源的源类型。
通用列表块类型 (Generic List Block	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。

表 B-24 用于 4.10.x、5.0-5.0.x 的用户产品数据块字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-93 页。
端口 (Port)	uint16	用户指定的端口。
协议 (Protocol)	uint16	用户指定的 IANA 协议号。例如： ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP
丢弃用户产品 (Drop User Product)	uint32	表示是否已从主机中删除用户操作系统定义： ▪ 0 - 否 ▪ 1 - 是
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义供应商名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	自定义供应商字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上供应商名称中的字节数。
自定义供应商名称 (Custom Vendor Name)	字符串	在用户输入中指定的自定义供应商名称。
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义产品名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	自定义产品字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上产品名称中的字节数。
自定义产品名称 (Custom Product Name)	字符串	在用户输入中指定的自定义产品名称。
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	自定义版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。

表 B-24　用于 4.10.x、5.0-5.0.x 的用户产品数据块字段 （续）

字段	数据类型	说明 (Description)
自定义版本 (Custom Version)	字符串	在用户输入中指定的自定义版本。
软件 ID (Software ID)	uint32	思科数据库中服务器或操作系统特定修订版的标识符。
服务器 ID (Server ID)	uint32	在用户输入中指定的主机服务器上的应用协议的 思科应用标识符。
供应商 ID (Vendor ID)	uint32	在第三方操作系统映射到思科 3D 操作系统定义时指定的第三方操作系统的供应商的标识符。
产品 ID (Product ID)	uint32	在第三方操作系统字符串映射到思科 3D 操作系统定义时指定的第三方操作系统字符串的产品标识字符串。
字符串块类型 (String Block Type)	uint32	启动包含用户输入中的第三方操作系统字符串映射到的思科 3D 操作系统定义的主版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	主版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
主版本 (Major Version)	字符串	第三方操作系统字符串映射到的思科 3D 操作系统定义的主版本。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的思科 3D 操作系统定义的次版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	次版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
次版本 (Minor Version)	字符串	用户输入中的第三方操作系统字符串映射到的思科 3D 操作系统定义的次版本号。
字符串块类型 (String Block Type)	uint32	启动包含用户输入中的第三方操作系统字符串映射到的思科操作系统定义的修订号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	修订版字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修订号中的字节数。
修订版 (Revision)	字符串	用户输入中的第三方操作系统字符串映射到的思科 3D 操作系统定义的修订号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的思科 3D 操作系统定义的最新主版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至主版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
至主版本 (To Major)	字符串	用户输入中的第三方操作系统字符串映射到的思科 3D 操作系统定义的一系列主版本号中的最新版本号。

表 B-24 用于 4.10.x、5.0-5.0.x 的用户产品数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的思科 3D 操作系统定义的最新次版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至次版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
至次版本 (To Minor)	字符串	用户输入中的第三方操作系统字符串映射到的思科 3D 操作系统定义的一系列次版本号中的最新版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的思科 3D 操作系统定义的最新修订号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至修订版字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修订号中的字节数。
至修订版 (To Revision)	字符串	用户输入中的第三方操作系统字符串映射到的思科 3D 操作系统定义的一系列修订号中的最新修订号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的思科 3D 操作系统的内部版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	内部版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上内部版本号中的字节数。
内部版本 (Build)	字符串	用户输入中的第三方操作系统字符串映射到的思科 3D 操作系统的内部版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的思科 3D 操作系统的修补版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	修补版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修补版本号中的字节数。
修补 (Patch)	字符串	用户输入中的第三方操作系统字符串映射到的思科 3D 操作系统的修补版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的思科 3D 操作系统的扩展版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	扩展版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上扩展版本号中的字节数。
分机 (Extension)	字符串	用户输入中的第三方操作系统字符串映射到的思科 3D 操作系统的扩展版本号。
UUID	uint8 [x16]	包含操作系统的唯一标识号。

表 B-24　用于 4.10.x、5.0-5.0.x 的用户产品数据块字段 （续）

字段	数据类型	说明 (Description)
通用列表块类型 (Generic List Block	uint32	启动由传送有关应用到特定 IP 地址范围中指定主机的修复的用户输入数据的修复列表数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装修复列表数据块。
修复列表数据块 (Fix List Data Blocks) *	变量	包含应用到主机的修复的相关信息的修复列表数据块。有关此数据块的说明，请参阅修复列表数据块，第 4-100 页。

旧版用户登录数据块

有关详细信息，请参阅以下各节：

用于 5.0 - 5.0.2 的用户登录信息数据块

用户登录信息数据块在用户信息更新消息中使用，传送检测到的用户的登录信息变更。有关详细信息，请参阅用户信息更新消息块，第 4-59 页。

在版本 5.0 - 5.0.2 中，用户登录信息数据块的块类型为 121。

下图显示用户登录信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户登录信息块类型 (121) (User Login Information Block Type (121))																															
	用户登录信息块长度 (User Login Information Block Length)																															
	时间戳 (Timestamp)																															
	IP 地址 (IP Addresses)																															
用户名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名...(User Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户 ID																															
	应用 ID (Application ID)																															
电子邮件 (Email)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件...(Email...)																															

下表对用户登录信息数据块的组件进行了说明。

表 B-25 用户登录信息数据块字段 5.0 - 5.0.2

字段	数据类型	说明 (Description)
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 5.0 - 5.0.2 中，此值为 121。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IP 地址 (IP Address)	uint8[4]	检测到用户登录的主机的 IP 地址，采用 IP 地址八位组。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
用户 ID	uint32	用户的标识号。
应用 ID (Application ID)	uint32	派生登录信息的连接中使用的应用协议的应用 ID。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。

表 B-25　　用户登录信息数据块字段 5.0 - 5.0.2 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。

用户登录信息数据块 5.1 - 5.4.x

用户登录信息数据块在用户信息更新消息中使用，传送检测到的用户的登录信息变更。有关详细信息，请参阅用户帐户更新消息数据块，第 4-181 页。

在版本 4.7-4.10.x 中，用户登录信息数据块的块类型为 73，在版本 5.0 - 5.0.2 中，块类型为系列 1 数据块组中的 121，在版本 5.1-5.4.x 中，块类型为系列 1 数据块组中的 127。

下图显示用户登录信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户登录信息块类型 (127)(User Login Information Block Type (127))																															
	用户登录信息块长度 (User Login Information Block Length)																															
	时间戳 (Timestamp)																															
	IPv4 地址 (IPv4 Addresses)																															
用户名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名...(User Name...)																															
	用户 ID																															
	应用 ID (Application ID)																															
电子邮件 (Email)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件...(Email...)																															
	IPv6 地址 (IPv6 Address) IPv6 地址 (IPv6 Address)（续） IPv6 地址 (IPv6 Address)（续） IPv6 地址 (IPv6 Address)（续）																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报告者 (Reported By)	登录类型 (Login Type)								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0)) （续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)								报告者...(Reported By...)																							

下表对用户登录信息数据块的组件进行了说明。

表 B-26　　用户登录信息数据块字段

字段	数据类型	说明 (Description)
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 5.1+ 中，此值为 127。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IPv4 地址 (IPv4 Addresses)	uint32	保留此字段，但不再填充。IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅IP 地址，第 1-4 页。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
用户 ID	uint32	用户的标识号。
应用 ID (Application ID)	uint32	派生登录信息的连接中使用的应用协议的应用 ID。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
IPv6 地址 (IPv6 Address)	uint8[16]	检测到用户登录的主机的 IPv6 地址，采用 IP 地址八位组。
登录类型 (Login Type)	uint8	检测到的用户登录类型。
字符串块类型 (String Block Type)	uint32	启动包含报告者值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	报告者字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上“报告者”(Reported By) 字段中的字节数。
报告者 (Reported By)	字符串	报告登录的 Active Directory 服务器的名称。

用户登录信息数据块 6.0.x

用户登录信息数据块在用户信息更新消息中使用，传送检测到的用户的登录信息变更。有关详细信息，请参阅用户帐户更新消息数据块，第 4-181 页。

在版本 6.0.x 中，用户登录信息数据块的块类型为 159。它具有新 ISE 集成终端配置文件、安全情报字段。

在版本 4.7-4.10.x 中，用户登录信息数据块的块类型为 73。在版本 5.0 - 5.0.2 中，块类型为系列 1 数据块组中的 121。在版本 5.1+ 中，块类型为系列 1 数块组中的 127。有关详细信息，请参阅用户登录信息数据块 5.1 - 5.4.x，第 B-137 页。

下图显示用户登录信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户登录信息块类型 (159) (User Login Information Block Type (159))																															
	用户登录信息块长度 (User Login Information Block Length)																															
	时间戳 (Timestamp)																															
	IPv4 地址 (IPv4 Addresses)																															
用户名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名...(User Name...)																															
域	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	域...(Domain...)																															
	用户 ID																															
	领域 ID (Realm ID)																															
	终端配置文件 ID (Endpoint Profile ID)																															
	安全组 ID (Security Group ID)																															
	协议 (Protocol)																															
电子邮件 (Email)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件...(Email...)																															
	IPv6 地址 (IPv6 Address)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPv6 地址 (IPv6 Address)（续）																															
	IPv6 地址 (IPv6 Address)（续）																															
	IPv6 地址 (IPv6 Address)（续）																															
	位置 IPv6 地址 (Location IPv6 Address)																															
	位置 IPv6 地址 (Location IPv6 Address)（续）																															
	位置 IPv6 地址 (Location IPv6 Address)（续）																															
	位置 IPv6 地址 (Location IPv6 Address)（续）																															
报告者 (Reported By)	登录类型 (Login Type)								身份验证类型 (Type)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0))（续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length)（续）																报告者...(Reported By...)															

下表对用户登录信息数据块的组件进行了说明。

表 B-27　　用户登录信息数据块字段

字段	数据类型	说明 (Description)
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 6.0.x 中，此值为 159。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IPv4 地址 (IPv4 Addresses)	uint32	保留此字段，但不再填充。IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅IP 地址，第 1-4 页。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。

表 B-27 用户登录信息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含域的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上域中的字节数。
域	字符串	用户登录的域。
用户 ID	uint32	用户的标识号。
领域 ID (Realm ID)	uint32	与身份领域对应的整数 ID。
终端配置文件 ID (Endpoint Profile ID)	uint32	连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	网络流量组的 ID 号码。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值包括: ▪ 165 - FTP ▪ 426 - SIP ▪ 547 - AOL 即时通信工具 ▪ 683 - IMAP ▪ 710 - LDAP ▪ 767 - NTP ▪ 773 - Oracle 数据库 ▪ 788 - POP3 ▪ 1755 - MDNS
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
IPv6 地址 (IPv6 Address)	uint8[16]	检测到用户登录的主机的 IPv6 地址，采用 IP 地址八位组。
位置 IPv6 地址 (Location IPv6 Address)	uint8[16]	用户最新登录的 IP 地址。可以是 IPv4 或 IPv6 地址。
登录类型 (Login Type)	uint8	检测到的用户登录类型。

表 B-27　　用户登录信息数据块字段 （续）

字段	数据类型	说明 (Description)
身份验证类型 (Authentication Type)	uint8	用户使用的身份验证类型。值可能是： ▪ 0 - 无需授权 ▪ 1 - 被动身份验证、AD 代理或 ISE 会话 ▪ 2 - 强制网络门户身份验证成功 ▪ 3 - 强制网络门户访客身份验证 ▪ 4 - 强制网络门户身份验证失败
字符串块类型 (String Block Type)	uint32	启动包含报告者值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	报告者字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上“报告者”(Reported By) 字段中的字节数。
报告者 (Reported By)	字符串	报告登录的 Active Directory 服务器的名称。

用户登录信息数据块 6.1.x

在版本 6.1+ 中，用户登录信息数据块的块类型为系列 1 数据块组中的 165。它具有新的端口和隧道字段。它替代块类型 159。有关详细信息，请参阅用户登录信息数据块 6.0.x，第 B-140 页。它被块类型 167 替代。

下图显示用户登录信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户登录信息块类型 (165) (User Login Information Block Type (159))																															
	用户登录信息块长度 (User Login Information Block Length)																															
	时间戳 (Timestamp)																															
	IPv4 地址 (IPv4 Addresses)																															
用户名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名...(User Name...)																															
域	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	域...(Domain...)																															
	用户 ID																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	领域 ID (Realm ID)																															
	终端配置文件 ID (Endpoint Profile ID)																															
	安全组 ID (Security Group ID)																															
	协议 (Protocol)																															
	端口 (Port)																范围开始 (Range Start)															
	开始端口 (Start Port)																结束端口 (End Port)															
电子邮件 (Email)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件...(Email...)																															
	IPv6 地址 (IPv6 Address) IPv6 地址 (IPv6 Address)（续） IPv6 地址 (IPv6 Address)（续） IPv6 地址 (IPv6 Address)（续）																															
	位置 IPv6 地址 (Location IPv6 Address) 位置 IPv6 地址 (Location IPv6 Address)（续） 位置 IPv6 地址 (Location IPv6 Address)（续） 位置 IPv6 地址 (Location IPv6 Address)（续）																															
报告者 (Reported By)	登录类型 (Login Type)								身份验证类型 (Type)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0))（续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length)（续）																报告者...(Reported By...)															

下表对用户登录信息数据块的组件进行了说明。

表 B-28　用户登录信息数据块字段

字段	数据类型	说明 (Description)
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 6.1+ 中，此值为 165。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IPv4 地址 (IPv4 Addresses)	uint32	保留此字段，但不再填充。IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅IP 地址，第 1-4 页。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
字符串块类型 (String Block Type)	uint32	启动包含域的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上域中的字节数。
域	字符串	用户登录的域。
用户 ID	uint32	用户的标识号。
领域 ID (Realm ID)	uint32	与身份领域对应的整数 ID。
终端配置文件 ID (Endpoint Profile ID)	uint32	连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	网络流量组的 ID 号码。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值包括： ▪ 165 - FTP ▪ 426 - SIP ▪ 547 - AOL 即时通信工具 ▪ 683 - IMAP ▪ 710 - LDAP ▪ 767 - NTP ▪ 773 - Oracle 数据库 ▪ 788 - POP3 ▪ 1755 - MDNS

表 B-28 用户登录信息数据块字段 （续）

字段	数据类型	说明 (Description)
端口 (Port)	uint16	在其上检测到用户的端口号。
范围开始 (Range Start)	uint16	TS 代理使用的端口范围内的起始端口。
开始端口 (Start Port)	uint16	TS 代理分配给单个用户的端口范围内的起始端口。
结束端口 (End Port)	uint16	TS 代理分配给单个用户的端口范围内的结束端口。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
IPv6 地址 (IPv6 Address)	uint8[16]	检测到用户登录的主机的 IPv6 地址，采用 IP 地址八位组。
位置 IPv6 地址 (Location IPv6 Address)	uint8[16]	用户最新登录的 IP 地址。可以是 IPv4 或 IPv6 地址。
登录类型 (Login Type)	uint8	检测到的用户登录类型。
身份验证类型 (Authentication Type)	uint8	用户使用的身份验证类型。值可能是: ▪ 0 - 无需授权 ▪ 1 - 被动身份验证、AD 代理或 ISE 会话 ▪ 2 - 强制网络门户身份验证成功 ▪ 3 - 强制网络门户访客身份验证 ▪ 4 - 强制网络门户身份验证失败
字符串块类型 (String Block Type)	uint32	启动包含报告者值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	报告者字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上“报告者”(Reported By) 字段中的字节数。
报告者 (Reported By)	字符串	报告登录的 Active Directory 服务器的名称。

用户登录信息数据块 6.1.x

用户登录信息数据块在用户信息更新消息中使用，传送检测到的用户的登录信息变更。有关详细信息，请参阅用户信息更新消息块，第 4-59 页。

在版本 6.1x 中，用户登录信息数据块的块类型为系列 1 数据块组中的 165。它具有新的端口和隧道字段。它替代块类型 159。它被块类型 167 替代。用户登录信息数据块 6.0.x，第 B-140 页有关详细信息，请参阅。

下图显示用户登录信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户登录信息块类型 (User Login Information Block Type) (165))																															
	用户登录信息块长度 (User Login Information Block Length)																															
	时间戳 (Timestamp)																															
	IPv4 地址 (IPv4 Addresses)																															
用户 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名...(User Name...)																															
域	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	域...(Domain...)																															
	用户 ID																															
	领域 ID (Realm ID)																															
	终端配置文件 ID (Endpoint Profile ID)																															
	安全组 ID (Security Group ID)																															
	协议 (Protocol)																															
	端口 (Port)																范围开始 (Range Start)															
	开始端口 (Start Port)																结束端口 (End Port)															
电子邮件 (Email)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件...(Email...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPv6 地址 (IPv6 Address) IPv6 地址 (IPv6 Address)（续） IPv6 地址 (IPv6 Address)（续） IPv6 地址 (IPv6 Address)（续）																															
	位置 IPv6 地址 (Location IPv6 Address) 位置 IPv6 地址 (Location IPv6 Address)（续） 位置 IPv6 地址 (Location IPv6 Address)（续） 位置 IPv6 地址 (Location IPv6 Address)（续）																															
报告者 (Reported By)	登录类型 (Login Type)								身份验证类型 (Type)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0))（续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length)（续）																报告者...(Reported By...)															
域	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明... (Description...)																															

下表对用户登录信息数据块的组件进行了说明。

表 B-29 用户登录信息数据块字段

字段	数据类型	说明 (Description)
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 6.2+ 中，此值为 165。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IPv4 地址 (IPv4 Addresses)	uint32	保留此字段，但不再填充。IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅IP 地址，第 1-4 页。

表 B-29　　用户登录信息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
字符串块类型 (String Block Type)	uint32	启动包含域的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上域中的字节数。
域	字符串	用户登录的域。
用户 ID	uint32	用户的标识号。
领域 ID (Realm ID)	uint32	与身份领域对应的整数 ID。
终端配置文件 ID (Endpoint Profile ID)	uint32	连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	网络流量组的 ID 号码。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值包括: ▪ 165 - FTP ▪ 426 - SIP ▪ 547 - AOL 即时通信工具 ▪ 683 - IMAP ▪ 710 - LDAP ▪ 767 - NTP ▪ 773 - Oracle 数据库 ▪ 788 - POP3 ▪ 1755 - MDNS
端口 (Port)	uint16	在其上检测到用户的端口号。
范围开始 (Range Start)	uint16	TS 代理使用的端口范围内的起始端口。
开始端口 (Start Port)	uint16	TS 代理分配给单个用户的端口范围内的起始端口。
结束端口 (End Port)	uint16	TS 代理分配给单个用户的端口范围内的结束端口。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。

表 B-29 用户登录信息数据块字段 （续）

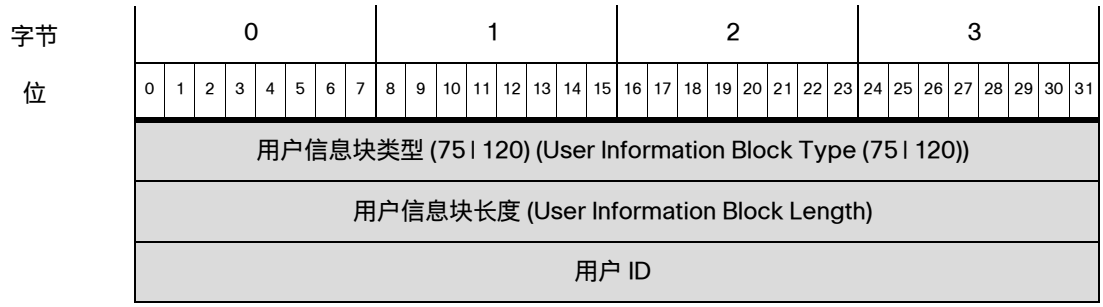
字段	数据类型	说明 (Description)
电子邮件 (Email)	字符串	用户的邮件地址。
IPv6 地址 (IPv6 Address)	uint8[16]	检测到用户登录的主机的 IPv6 地址，采用 IP 地址八位组。
位置 IPv6 地址 (Location IPv6 Address)	uint8[16]	用户最新登录的 IP 地址。可以是 IPv4 或 IPv6 地址。
登录类型 (Login Type)	uint8	检测到的用户登录类型。
身份验证类型 (Authentication Type)	uint8	用户使用的身份验证类型。值可能是: ▪ 0 - 无需授权 ▪ 1 - 被动身份验证、AD 代理或 ISE 会话 ▪ 2 - 强制网络门户身份验证成功 ▪ 3 - 强制网络门户访客身份验证 ▪ 4 - 强制网络门户身份验证失败
字符串块类型 (String Block Type)	uint32	启动包含报告者值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	报告者字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上“报告者”(Reported By) 字段中的字节数。
报告者 (Reported By)	字符串	报告登录的 Active Directory 服务器的名称。

用于 5.x 的用户信息数据块

用户信息数据块在用户修改消息中使用，传送检测到、删除或丢弃的用户的信息。有关详细信息，请参阅用户修改消息，第 4-58 页

在版本 4.7-4.10.x 中，用户信息数据块的块类型为系列 1 数据块组中的 75，在版本 5.x 中，块类型为系列 1 数据块组中的 120。块类型 75 与块类型 120 的结构相同。

下图显示用户信息数据块的格式:



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
用户 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名...(User Name...)																															
	协议 (Protocol)																															
第一页 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名字...(First Name...)																															
最后一页 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	姓氏...(Last Name...)																															
电子邮件 (Email)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件...(Email...)																															
部门	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	部门...(Department...)																															
电话	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电话...(Phone...)																															

下表对用户信息数据块的组件进行了说明。

表 B-30 用户信息数据块字段

字段	数据类型	说明 (Description)
用户信息块类型 (User Information Block Type)	uint32	启动用户信息数据块。在版本 4.7 - 4.10.x 中，此值为 75，在版本 5.0+ 中，此值为 120 。
用户信息块长度 (User Information Block Length)	uint32	用户信息数据块中的字节总数，包括用户信息块类型和长度字段的八个字节，加上随后的用户信息数据中的字节数。
用户 ID	uint32	用户的标识号。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
协议 (Protocol)	uint32	用于包含用户信息的数据包的协议。
字符串块类型 (String Block Type)	uint32	启动包含用户的名字的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名字字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上名字中的字节数。
名字 (First Name)	字符串	用户的名字。
字符串块类型 (String Block Type)	uint32	启动包含用户的姓氏的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户姓氏字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上姓氏中的字节数。
姓氏	字符串	用户的姓氏。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
字符串块类型 (String Block Type)	uint32	启动包含用户所在部门的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	部门字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上部门中的字节数。
部门	字符串	用户所在部门。

表 B-30　　用户信息数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含用户的电话号码的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电话号码字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电话号码中的字节数。
电话	字符串	用户的电话号码。

旧版主机配置文件数据块

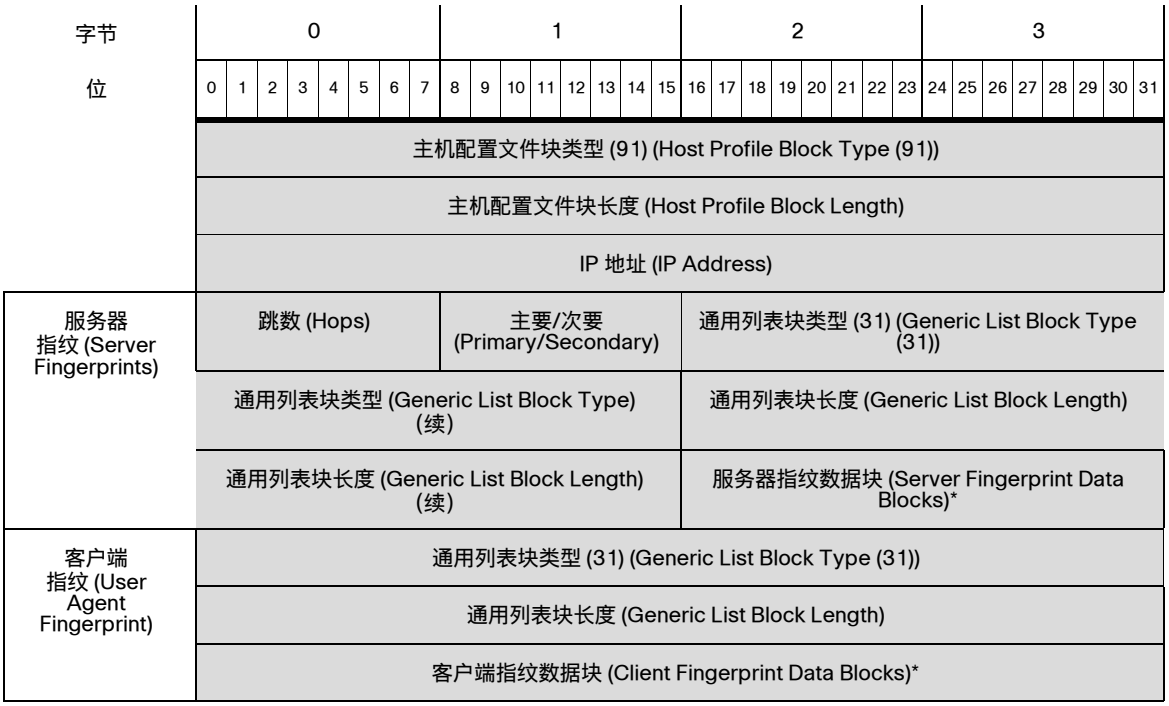
有关详细信息，请参阅以下各节：

- 用于 5.0 - 5.0.2 的主机配置文件数据块，第 B-153 页

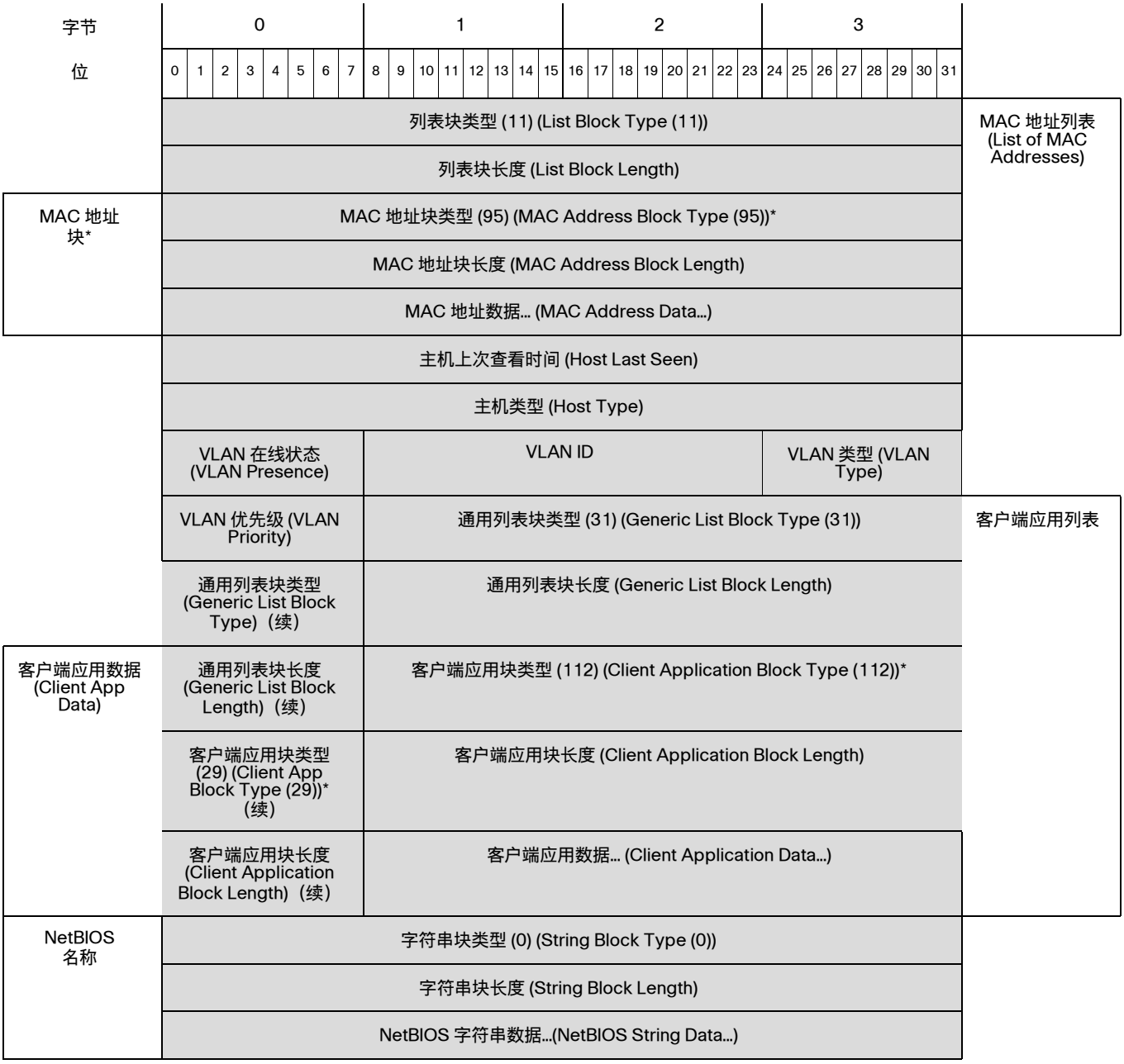
用于 5.0 - 5.0.2 的主机配置文件数据块

下图显示版本 5.0 至 5.0.2 中主机配置文件数据块的格式。主机配置文件数据块也不包含主机临界值，但包含 VLAN 在线状态指示器。此外，主机配置文件数据块可以传输主机的 NetBIOS 名称。此主机配置文件数据块的块类型为 91。

注释　下图中块类型字段旁边的星号 (*) 表示该消息可能包含零个或多个系列 1 数据块实例。



字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
中小企业指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																																
	通用列表块长度 (Generic List Block Length)																																
	SMB 指纹数据块 (SMB Fingerprint Data Blocks)*																																
DHCP 指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																																
	通用列表块长度 (Generic List Block Length)																																
	DHCP 指纹数据块 (DHCP Fingerprint Data Blocks)*																																
	列表块类型 (11) (List Block Type (11))																																TCP 服务器列表 (List of TCP Servers)
	列表块长度 (List Block Length)																																
TCP 服务器块*	服务器块类型 (36) (Server Block Type (36))																																
	服务器块长度 (Server Block																																
	TCP 服务器数据... (TCP Server Data...)																																
	列表块类型 (11) (List Block Type (11))																																UDP 服务器列表 (List of UDP Servers)
	列表块长度 (List Block Length)																																
UDP 服务器块*	服务器块类型 (36) (Server Block Type (36))*																																
	服务器块长度 (Server Block																																
	UDP 服务器数据... (UDP Server Data...)																																
	列表块类型 (11) (List Block Type (11))																																网络协议列表 (List of Network Protocols)
	列表块长度 (List Block Length)																																
网络协议块*	协议块类型 (4) (Protocol Block Type (4))*																																
	协议块长度 (Protocol Block Length)																																
	网络协议数据... (Network Protocol Data...)																																
	列表块类型 (11) (List Block Type (11))																																传输协议列表 (List of Transport Protocols)
	列表块长度 (List Block Length)																																
传输协议块*	协议块类型 (4) (Protocol Block Type (4))*																																
	协议块长度 (Protocol Block Length)																																
	传输协议数据... (Transport Protocol Data...)																																



下表对由版本 4.9 返回到版本 5.0.2 的主机配置文件数据块的字段进行了说明。

表 B-31 用于 5.0 - 5.0.2 的主机配置文件数据块字段

字段	数据类型	说明 (Description)
主机配置文件块类型 (Host Profile Block Type)	uint32	启动用于 4.9 至 5.0.2 的主机配置文件数据块。此数据块的块类型为 91。
主机配置文件块长度 (Host Profile Block Length)	uint32	主机配置文件数据块中的字节数，包括主机配置文件块类型和长度字段的八个字节，加上随后的主机配置文件数据中的字节数。
IP 地址 (IP Address)	uint8[4]	配置文件中描述的主机的 IP 地址，采用 IP 地址八位组。
跳数 (Hops)	uint8	从主机到设备的跳数。
主/辅助 (Primary/ Secondary)	uint8	表示主机是位于检测到其的设备的主网络中还是辅助网络中： ▪ 0 - 主机位于主网络中。 ▪ 1 - 主机位于辅助网络中。
通用列表块类型 (Generic List Block	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-160 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-160 页。

表 B-31　用于 5.0 - 5.0.2 的主机配置文件数据块字段 （续）

字段	数据类型	说明 (Description)
通用列表块类型 (Generic List Block	uint32	启动由传送用 SMB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（SMB指纹）数据块(Operating System Fingerprint (SMB Fingerprint) Data Blocks) *	变量	包含用 SMB 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-160 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（DHCP 指纹）数据块 (Operating System Fingerprint (DHCP Fingerprint) Data Blocks) *	变量	包含用 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-160 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
服务器块类型 (Server Block Type)	uint32	启动服务器数据块。值始终为 89。
服务器块长度 (Server Block	uint32	服务器数据块中的字节数，包括服务器块类型和长度字段的八个字节，加上随后的 TCP 服务器数据的字节数。
TCP 服务器数据 (TCP Server Data)	变量	描述 TCP 服务器的数据字段（按照产品早期版本的记录）。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。

表 B-31 用于 5.0 - 5.0.2 的主机配置文件数据块字段 （续）

字段	数据类型	说明 (Description)
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
服务器块类型 (Server Block Type)	uint32	启动描述 UDP 服务器的服务器数据块。值始终为 89。
服务器块长度 (Server Block	uint32	服务器数据块中的字节数，包括服务器块类型和长度字段的八个字节，加上随后的 UDP 服务器数据的字节数。
UDP 服务器数据 (UDP Server Data)	变量	描述 UDP 服务器的数据字段（按照产品早期版本的记录）。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个协议数据块。
协议块类型 (Protocol Block Type)	uint32	启动描述网络协议的协议数据块。值始终为 4。
协议块长度 (Protocol Block Length)	uint32	协议数据块中的字节数，包括协议块类型和长度字段的八个字节，加上随后的协议数据中的字节数。
网络协议数据 (Network Protocol Data)	uint16	包含网络协议号的数据字段，如协议数据块，第 4-72 页中所记录。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个传输协议数据块。
协议块类型 (Protocol Block Type)	uint32	启动描述传输协议的协议数据块。值始终为 4。
协议块长度 (Protocol Block Length)	uint32	协议数据块中的字节数，包括协议块类型和长度的八个字节，加上随后的协议数据中的字节数。
传输协议数据 (Transport Protocol Data)	变量	包含传输协议号的数据字段，如协议数据块，第 4-72 页中所记录。
列表块类型 (List Block Type)	uint32	启动由 MAC 地址数据块组成的列表数据块。值始终为 11。

表 B-31　用于 5.0 - 5.0.2 的主机配置文件数据块字段 （续）

字段	数据类型	说明 (Description)
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装 MAC 地址数据块。
主机 MAC 地址块类型 (Host MAC Address Block Type)	uint32	启动主机 MAC 地址数据块。值始终为 95。
主机 MAC 地址块长度 (Host MAC Address Block Length)	uint32	主机 MAC 地址数据块中的字节数，包括主机 MAC 地址块类型和长度字段的八个字节，加上随后的主机 MAC 地址数据中的字节数。
主机 MAC 地址数据 (Host MAC Address Data)	变量	主机 MAC 地址 4.9+，第 4-113 页中描述的主机 MAC 地址数据字段。
主机上次查看时间 (Host Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。可能会出现以下值： ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥 ▪ 3 - NAT 设备 ▪ 4 - LB（负载均衡器）
VLAN 在线状态 (VLAN Presence)	uint8	表示是否存在 VLAN： ▪ 0 - 是 ▪ 1 - 否
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block	uint32	启动由传送客户端应用数据的客户端应用数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
客户端应用块类型 (Client Application Block Type)	uint32	启动客户端应用块。值始终为 5。

表 B-31 用于 5.0 - 5.0.2 的主机配置文件数据块字段 （续）

字段	数据类型	说明 (Description)
客户端应用块长度 (Client Application Block Length)	uint32	客户端应用块中的字节数，包括客户端应用块类型和长度字段的八个字节，加上随后的客户端应用数据中的字节数。
客户端应用数据 (Client Application Data...)	变量	描述客户端应用的客户端应用数据字段，如用于 5.0+ 的主机客户端应用数据块，第 4-157 页中所记录。
字符串块类型 (String Block Type)	uint32	启动 NetBIOS 名称的字符串数据块。此值设置为 0 以表示字符串数据。
字符串块长度 (String Block Length)	uint32	表示 NetBIOS 名称字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称的字节数。
NetBIOS 字符串数据 (NetBIOS String Data)	变量	包含主机配置文件中描述的主机的 NetBIOS 名称。

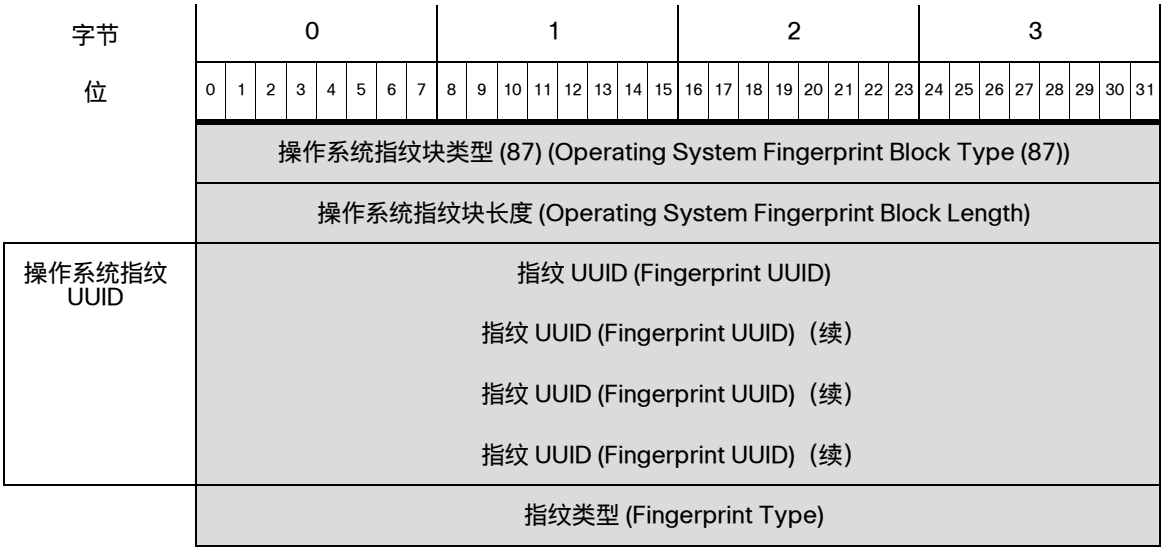
旧版操作系统指纹数据块

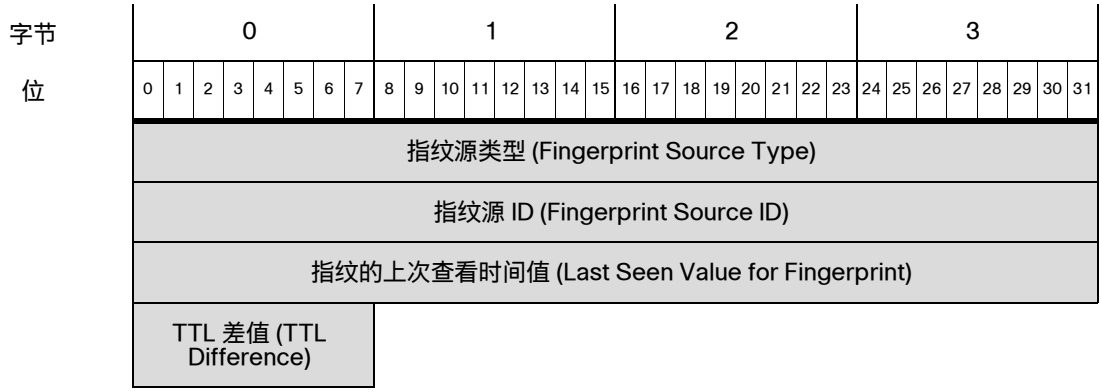
有关详细信息，请参阅以下各节：

- 用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-160 页

用于 5.0 - 5.0.2 的操作系统指纹数据块

操作系统指纹数据块的块类型为 87。块包括指纹通用唯一标识符 (UUID) 以及指纹类型、指纹源类型和指纹源 ID。下图显示用于版本 5.0 至版本 5.0.2 的操作系统指纹数据块的格式。





下表对操作系统指纹数据块的字段进行了说明。

表 B-32　　操作系统指纹数据块字段

字段	数据类型	说明 (Description)
操作系统指纹数据块类型 (Operating System Fingerprint Data Block Type)	uint32	启动操作系统数据块。值始终为 87。
操作系统数据块长度 (Operating System Data Block Length)	uint32	操作系统指纹数据块中的字节数。此值应始终为 41：数据块类型和长度字段的八个字节，指纹 UUID 值的十六个字节，指纹类型的四个字节，指纹源类型的四个字节，指纹源 ID 的四个字节，上次查看时间值的四个字节以及 TTL 差值的一个字节。
指纹 UUID (Fingerprint UUID)	uint8[16]	采用八位组的指纹识别号，用作操作系统的唯一标识符。指纹 UUID 映射到漏洞数据库 (VDB) 中的操作系统名称、供应商和版本。
指纹类型 (Fingerprint Type)	uint32	表示指纹的类型。
指纹源类型 (Fingerprint Source Type)	uint32	表示提供操作系统指纹的源的类型（即用户或扫描仪）。
指纹源 ID (Fingerprint Source ID)	uint32	表示提供操作系统指纹的源的 ID。
上次查看时间 (Last Seen)	uint32	表示上次在流量中看到指纹的时间。
TTL 差值 (TTL Difference)	uint8	表示指纹中的 TTL 值与在用于采集主机指纹的数据包中看到的 TTL 值之间的差值。

旧版连接数据结构

有关详细信息，请参阅以下各节：

连接统计信息数据块 5.0 - 5.0.2

连接统计信息数据块在连接数据消息中使用。用于版本 5.0 - 5.0.2 的连接统计信息数据块的块类型为 115。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

下图显示用于 5.0 - 5.0.2 的连接统计信息数据块的格式：

::

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (115) (Connection Data Block Type (115))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (设备 ID)																																
入口区 (Ingress Zone) 入口区 (Ingress Zone)（续） 入口区 (Ingress Zone)（续） 入口区 (Ingress Zone)（续）																																
出口区 (Egress Zone)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																																
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)														


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
TCP 标志 (TCP Flags)
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
第一个数据包时间 (First Pkt Time)
第一个数据包时间戳 (First Packet Timestamp)（续）
最后一个数据包时间 (Last Pkt Time)
最后一个数据包时间戳 (Last Packet Timestamp)（续）
发送的数据包数 (Packets Sent)
发送的数据包数 (Packets Sent)（续）
发送的数据包数 (Packets Sent)（续）
接收的数据包数 (Packets Rcvd)
接收的数据包数 (Packets Received)（续）
接收的数据包数 (Packets Received)（续）
发送的字节数 (Bytes Sent)
发送的字节数 (Bytes Sent)（续）
接收的数据包数 (Packets Received)（续）
接收的字节数 (Bytes Rcvd)
接收的字节数 (Bytes Received)（续）
接收的字节数 (Bytes Received)（续）
用户 ID
用户 ID (User ID)（续）
应用协议 ID (Application Protocol ID)
应用协议 ID (Application Protocol ID)（续）
URL 类别 (URL Category)
URL 类别 (URL Category)（续）
URL 信誉 (URL Reputation)
URL 信誉 (URL Reputation)（续）
客户端应用 ID (Client App ID)
客户端应用 ID (Client Application ID)（续）
Web 应用 ID (Web App ID)

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	Web 应用 ID (Web Application ID)（续）																								字符串块类型 (0) (String Block Type (0))							
客户端应用 URL (Client App URL)	字符串块类型 (String Block Type)（续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length)（续）																								客户端应用 URL... (Client Application URL...)							
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称.... (NetBIOS Name....)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本...(Client Application Version...)																															

下表对用于 5.0 - 5.0.2 的连接统计信息数据块的字段进行了说明。

表 B-33　　连接统计信息数据块 5.0 - 5.0.2 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.0 至 5.0.2 的连接统计信息数据块。值始终为 115。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。

表 B-33 连接统计信息数据块 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明 (Description)
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint32	在用户界面中选择的针对该规则的操作（允许、阻止等）。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发送的数据包数 (Packets Sent)	uint64	发起主机传输的数据包数。
接收的数据包数 (Packets Received)	uint64	响应主机传输的数据包数。

表 B-33　　连接统计信息数据块 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明 (Description)
发送的字节数 (Bytes Sent)	uint64	发起主机传输的字节数。
接收的字节数 (Bytes Received)	uint64	响应主机传输的字节数。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如/files/index.html）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。

表 B-33 连接统计信息数据块 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。

连接统计信息数据块 5.1

连接统计信息数据块在连接数据消息中使用。5.0.2 到 5.1 的连接数据块变更包括添加了具有 5.1 中引入的配置参数的新字段（规则操作原因、监控器规则、安全情报源/目标、安全情报层）。用于版本 5.1 的连接统计信息数据块的块类型为 126。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

下图显示用于 5.1 的连接统计信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (126) (Connection Data Block Type (126))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (设备 ID)																																
入口区 (Ingress Zone)																																
入口区 (Ingress Zone)（续）																																
入口区 (Ingress Zone)（续）																																
入口区 (Ingress Zone)（续）																																
出口区 (Egress Zone)																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	入口接口 (Ingress Interface)（续）																															
	出口接口 (Egress Interface)																															
	出口接口 (Egress Interface)（续）																															
	出口接口 (Egress Interface)（续）																															
	出口接口 (Egress Interface)（续）																															
	发起方 IP 地址 (Initiator IP Address)																															
	发起方 IP 地址 (Initiator IP Address)（续）																															
	发起方 IP 地址 (Initiator IP Address)（续）																															
	发起方 IP 地址 (Initiator IP Address)（续）																															
	响应方 IP 地址 (Responder IP Address)																															
	响应方 IP 地址 (Responder IP Address)（续）																															
	响应方 IP 地址 (Responder IP Address)（续）																															
	响应方 IP 地址 (Responder IP Address)（续）																															
	策略修订 (Policy Revision)																															
	策略修订 (Policy Revision)（续）																															
	策略修订 (Policy Revision)（续）																															
	策略修订 (Policy Revision)（续）																															
	规则 ID (Rule ID)																															
	规则操作 (Rule Action)																规则原因 (Rule Reason)															
	发起方端口 (Initiator Port)																响应方端口 (Responder Port)															
	TCP 标志 (TCP Flags)																协议 (Protocol)								NetFlow 源 (NetFlow Source)							
	Netflow 源 (Netflow Source)（续）																															
	Netflow 源 (Netflow Source)（续）																															
	Netflow 源 (Netflow Source)（续）																															
	Netflow 源 (Netflow Source)（续）																								第一个数据包时间 (First Pkt Time)							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
第一个数据包时间戳 (First Packet Timestamp)（续）																									最后一个数据包时间 (Last Pkt Time)							
最后一个数据包时间戳 (Last Packet Timestamp)（续）																									发起方传输的数据包数 (Initiator Transmitted Packets)							
发起方传输的数据包数 (Initiator Transmitted Packets)（续）																																
发起方传输的数据包数 (Initiator Transmitted Packets)（续）																									响应方传输的数据包数 (Responder Transmitted Packets)							
响应方传输的数据包数 (Responder Transmitted Packets)（续）																																
响应方传输的数据包数 (Responder Transmitted Packets)（续）																									发起方传输的字节数 (Initiator Transmitted Bytes)							
发起方传输的字节数 (Initiator Transmitted Bytes)（续）																																
发起方传输的字节数 (Initiator Transmitted Bytes)（续）																									响应方传输的字节数 (Responder Transmitted Bytes)							
响应方传输的字节数 (Responder Transmitted Bytes)（续）																																
响应方传输的字节数 (Responder Transmitted Bytes)（续）																									用户 ID							
用户 ID (User ID)（续）																									应用协议 ID (Application Protocol ID)							
应用协议 ID (Application Protocol ID)（续）																									URL 类别 (URL Category)							
URL 类别 (URL Category)（续）																									URL 信誉 (URL Reputation)							
URL 信誉 (URL Reputation)（续）																									客户端应用 ID (Client App ID)							
客户端应用 ID (Client Application ID)（续）																									Web 应用 ID (Web App ID)							
Web 应用 ID (Web Application ID)（续）																									字符串块类型 (0) (String Block Type (0))							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
客户端应用 URL (Client App URL)	字符串块类型 (String Block Type)（续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length)（续）																								客户端应用 URL... (Client Application URL...)							
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称.... (NetBIOS Name....)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源/目标 (Sec. Int. Src/Dst)								安全接口代表层 (Sec. Int. Rep Layer)																								

下表对用于 5.1 的连接统计信息数据块的字段进行了说明。

表 B-34 连接统计信息数据块 5.1 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.1 的连接统计信息数据块。值始终为 126。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。

表 B-34　　连接统计信息数据块 5.1 字段 （续）

字段	数据类型	说明 (Description)
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的UNIX时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如 `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。

表 B-34 连接统计信息数据块 5.1 字段 （续）

字段	数据类型	说明 (Description)
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。

连接统计信息数据块 5.2.x

连接统计信息数据块在连接数据消息中使用。版本 5.1.1 到版本 5.2 的连接数据块变更包括添加了用于支持地理位置的新字段。用于版本 5.2.x 的连接统计信息数据块的块类型为系列 1 数据块组中的 144。它否决了块类型 137，连接统计信息数据块 5.1.1.x，第 B-186 页。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

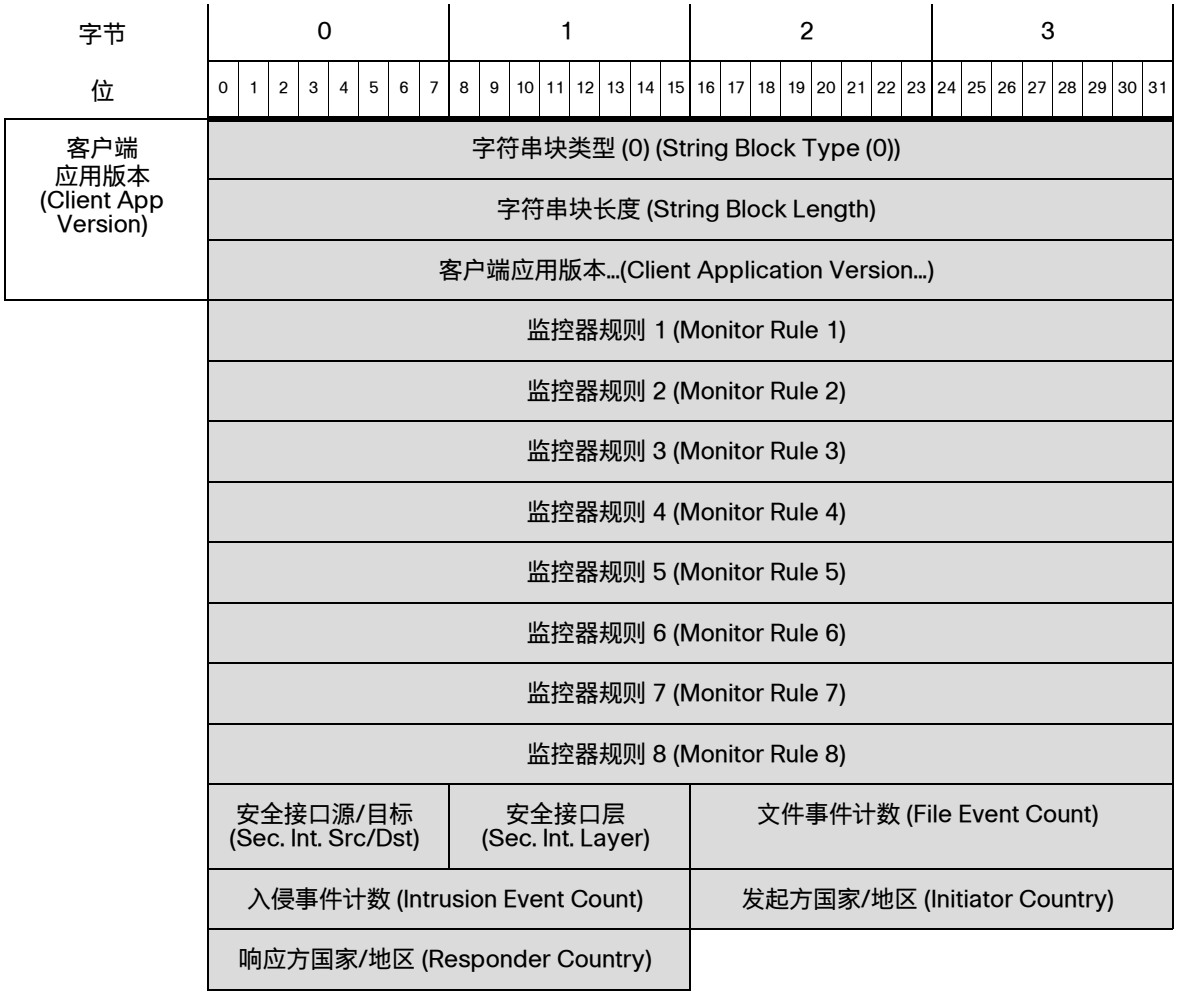
下图显示用于 5.2.x 的连接统计信息数据块的格式：

::

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (144) (Connection Data Block Type (144))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (设备 ID)																																
入口区 (Ingress Zone)																																
入口区 (Ingress Zone)（续）																																
入口区 (Ingress Zone)（续）																																
入口区 (Ingress Zone)（续）																																
出口区 (Egress Zone)																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)														
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)														
TCP 标志 (TCP Flags)																	协议 (Protocol)								NetFlow 源 (NetFlow Source)							
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																									实例 ID (Instance ID)							
实例 ID (Instance ID)（续）									连接计数器 (Connection Counter)																	第一个数据包时间 (First Pkt Time)							
第一个数据包时间戳 (First Packet Timestamp)（续）																																
最后一个数据包时间戳 (Last Packet Timestamp)（续）																																
发起方传输的数据包数 (Initiator Transmitted Packets)（续）																																

	字节	0								1								2								3							
	位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		发起方传输的数据包数 (Initiator Transmitted Packets)（续）																								响应方传输的数据包数 (Resp. Tx Packets)							
		响应方传输的数据包数 (Responder Transmitted Packets)（续）																															
		响应方传输的数据包数 (Responder Transmitted Packets)（续）																								发起方传输的字节数 (Initiator Tx Bytes)							
		发起方传输的字节数 (Initiator Transmitted Bytes)（续）																															
		发起方传输的字节数 (Initiator Transmitted Bytes)（续）																								响应方传输的字节数 (Resp. Tx Bytes)							
		响应方传输的字节数 (Responder Transmitted Bytes)（续）																															
		响应方传输的字节数 (Responder Transmitted Bytes)（续）																								用户 ID							
		用户 ID (User ID)（续）																								应用协议ID							
		应用协议 ID (Application Protocol ID)（续）																								URL 类别 (URL Category)							
		URL 类别 (URL Category)（续）																								URL 信誉 (URL Reputation)							
		URL 信誉 (URL Reputation)（续）																								客户端应用 ID (Client App ID)							
		客户端应用 ID (Client Application ID)（续）																								Web 应用 ID (Web App ID)							
	客户端 URL	Web 应用 ID (Web Application ID)（续）																								字符串块类型 (0) (Str. Block Type (0))							
		字符串块类型 (String Block Type)（续）																								字符串块长度 (String Block Length)							
		字符串块长度 (String Block Length)（续）																								客户端应用URL... (Client App. URL...)							
	NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
		字符串块长度 (String Block Length)																															
		NetBIOS 名称...(NetBIOS Name...)																															



下表对用于 5.2.x 的连接统计信息数据块的字段进行了说明:

表 B-35 连接统计信息数据块 5.2.x 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.2.x 的连接统计信息数据块。值始终为 144。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。

表 B-35　　连接统计信息数据块 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的UNIX时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。

表 B-35 连接统计信息数据块 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如 `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。

表 B-35　　连接统计信息数据块 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家/地区 (Initiator Country)	uint16	发起主机的国家/地区代码。
响应方国家/地区 (Responder Country)	uint16	响应主机的国家/地区代码。

用于 5.0 - 5.1 的连接区块数据块

连接区块数据块传送 NetFlow 设备检测到的连接数据。在 4.10.1 之前的版本中，连接区块数据块的块类型为 66。在版本 5.0 - 5.1 中，其块类型为 119。

下图显示连接区块数据块的格式:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接区块块类型 (66	119) (Connection Chunk Block Type (66	119))																														
连接区块块长度 (Connection Chunk Block Length)																																
发起方 IP 地址 (Initiator IP Address)																																
响应方 IP 地址 (Responder IP Address)																																
开始时间 (Start Time)																																
应用 ID (Application ID)																																
响应方端口 (Responder Port)																	协议 (Protocol)								连接类型 (Connection Type)							
NetFlow 检测器 IP 地址 (NetFlow Detector IP Address)																																
发送的数据包数 (Packets Sent)																																
接收的数据包数 (Packets Received)																																
发送的字节数 (Bytes Sent)																																
接收的字节数 (Bytes Received)																																
连接 (Connections)																																

下表对连接区块数据块的组件进行了说明:

表 B-36 连接区块数据块字段

字段	数据类型	说明 (Description)
连接区块块类型 (Connection Chunk Block Type)	uint32	启动连接区块数据块。在 4.10.1 之前的版本中，此值为 66，在版本 5.0 中，此值为 119。
连接区块块长度 (Connection Chunk Block Length)	uint32	连接区块数据块中的字节总数，包括连接区块块类型和长度字段的八个字节，加上随后的连接区块数据中的字节数。

表 B-36　　连接区块数据块字段 （续）

字段	数据类型	说明 (Description)
发起方 IP 地址 (Initiator IP Address)	uint8[4]	发起连接的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[4]	响应连接的主机的 IP 地址，采用 IP 地址八位组。
开始时间 (Start Time)	uint32	连接区块的开始时间。
应用 ID (Application ID)	uint32	连接中使用的应用协议的应用标识号。
响应方端口 (Responder Port)	uint16	响应者在连接区块中使用的端口。
协议 (Protocol)	uint8	用于包含用户信息的数据包的协议。
连接类型 (Connection Type)	uint8	连接的类型。
源设备 IP 地址 (Source 设备 IP Address)	uint8[4]	检测到连接的 NetFlow 设备的 IP 地址，采用 IP 地址八位组。
发送的数据包数 (Packets Sent)	uint32	在连接区块中发送的数据包数。
接收的数据包数 (Packets Received)	uint32	在连接区块中接收的数据包数。
发送的字节数 (Bytes Sent)	uint32	在连接区块中发送的字节数。
接收的字节数 (Bytes Received)	uint32	在连接区块中接收的字节数。
连接	uint32	在连接区块中进行的会话数。

用于 5.1.1-6.0.x 的连接区块数据块

连接区块数据块传送连接数据。它存储五分钟内汇聚的连接日志数据。连接区块数据块的块类型为系列 1 数据块组中的 136。它替代块类型 119。

下图显示连接区块数据块的格式:

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接区块块类型 (136) (Connection Chunk Block Type (136))																																
连接区块块长度 (Connection Chunk Block Length)																																
发起方 IP 地址 (Initiator IP Address)																																
响应方 IP 地址 (Responder IP Address)																																
开始时间 (Start Time)																																
应用协议 (Application Protocol)																																
响应方端口 (Responder Port)																	协议 (Protocol)								连接类型 (Connection Type)							
NetFlow 检测器 IP 地址 (NetFlow Detector IP Address)																																
发送的数据包数 (Packets Sent) 发送的数据包数，续																																
接收的数据包数 (Packets Received) 接收的数据包数，续																																
发送的字节数 (Bytes Sent) 发送的字节数，续																																
接收的字节数 (Bytes Received) 接收的字节数，续																																
连接 (Connections)																																

下表对连接区块数据块的组件进行了说明。

表 B-37　　连接区块数据块字段

字段	数据类型	说明 (Description)
连接区块块类型 (Connection Chunk Block Type)	uint32	启动连接区块数据块。值始终为 136。
连接区块块长度 (Connection Chunk Block Length)	uint32	连接区块数据块中的字节总数，包括连接区块块类型和长度字段的八个字节，加上随后的连接区块数据中的字节数。
发起方 IP 地址 (Initiator IP Address)	uint8(4)	此类型连接的发起方的 IP 地址。与响应方 IP 地址一起使用，以识别相同连接。
响应方 IP 地址 (Responder IP Address)	uint8(4)	此类型连接的响应方的 IP 地址。与发起方 IP 地址一起使用，以识别相同连接。
开始时间 (Start Time)	uint32	连接区块的开始时间。
应用协议 (Application Protocol)	uint32	连接中使用的协议的标识号。
响应方端口 (Responder Port)	uint16	响应者在连接区块中使用的端口。
协议 (Protocol)	uint8	用于包含用户信息的数据包的协议。
连接类型 (Connection Type)	uint8	连接的类型。
NetFlow 检测器 IP 地址 (NetFlow Detector IP Address)	uint8[4]	检测到连接的 NetFlow 设备的 IP 地址，采用 IP 地址八位组。
发送的数据包数 (Packets Sent)	uint64	在连接区块中发送的数据包数。
接收的数据包数 (Packets Received)	uint64	在连接区块中接收的数据包数。
发送的字节数 (Bytes Sent)	uint64	在连接区块中发送的字节数。
接收的字节数 (Bytes Received)	uint64	在连接区块中接收的字节数。
连接	uint32	五分钟内的连接数。

连接统计信息数据块 5.1.1.x

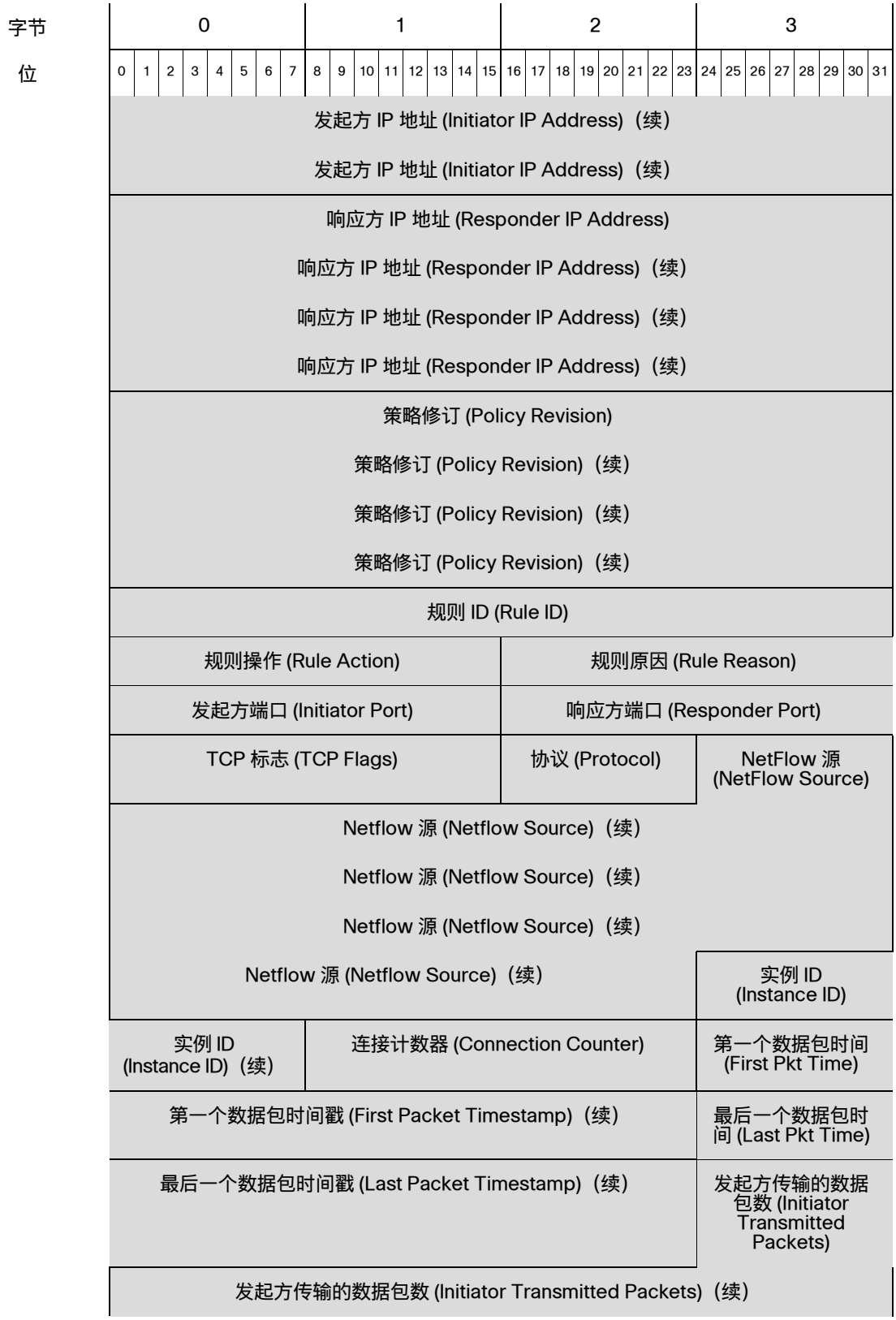
连接统计信息数据块在连接数据消息中使用。版本 5.1 到版本 5.1.1 的连接数据块变更包括添加了用于识别相关入侵事件的新字段。用于版本 5.1.1.x 的连接统计信息数据块的块类型为 137。它否决了块类型 126，连接统计信息数据块 5.1，第 B-168 页。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

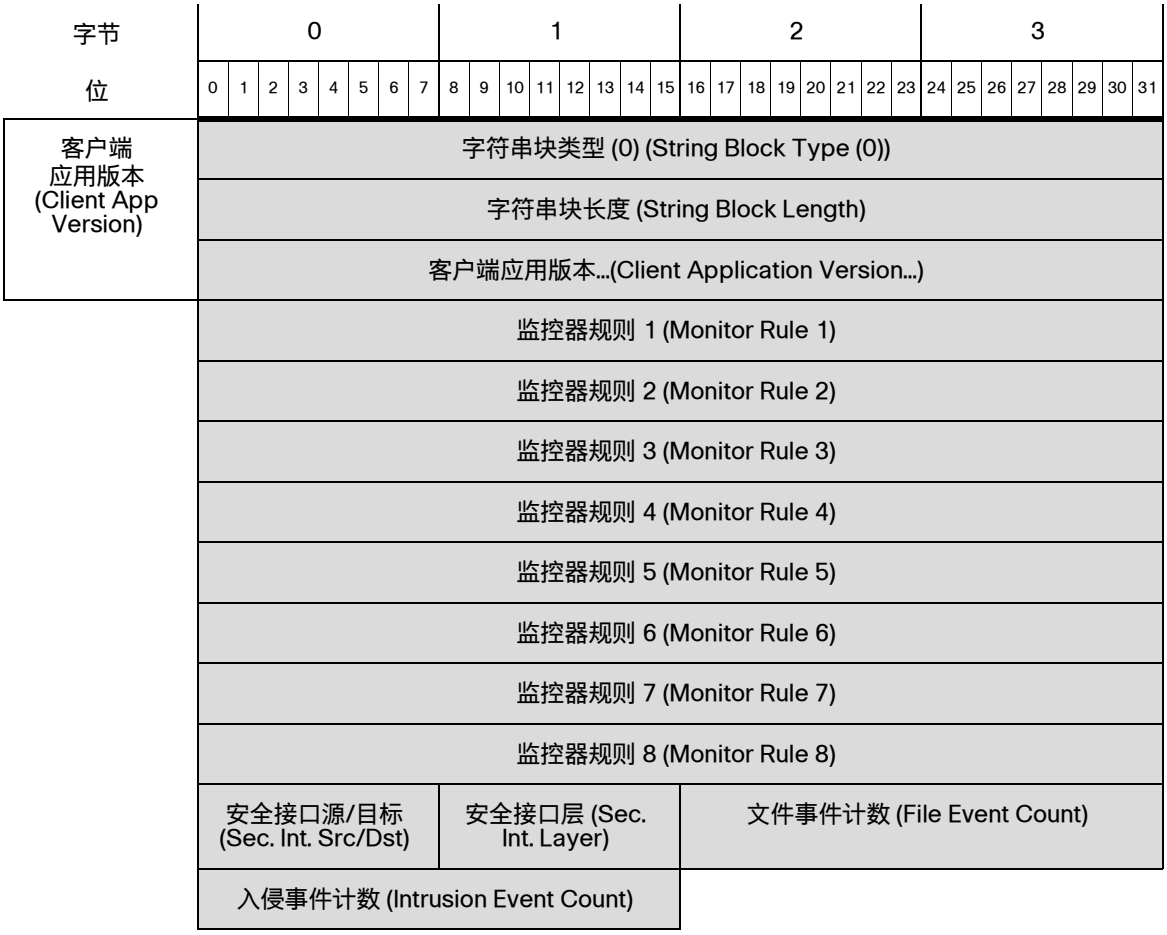
下图显示用于 5.1.1 的连接统计信息数据块的格式：

::

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (137) (Connection Data Block Type (137))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (设备 ID)																																
入口区 (Ingress Zone)																																
入口区 (Ingress Zone)（续）																																
入口区 (Ingress Zone)（续）																																
入口区 (Ingress Zone)（续）																																
出口区 (Egress Zone)																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
发起方 IP 地址 (Initiator IP Address)（续）
发起方 IP 地址 (Initiator IP Address)（续）
响应方 IP 地址 (Responder IP Address)
响应方 IP 地址 (Responder IP Address)（续）
响应方 IP 地址 (Responder IP Address)（续）
响应方 IP 地址 (Responder IP Address)（续）
策略修订 (Policy Revision)
策略修订 (Policy Revision)（续）
策略修订 (Policy Revision)（续）
策略修订 (Policy Revision)（续）
规则 ID (Rule ID)
规则操作 (Rule Action)
规则原因 (Rule Reason)
发起方端口 (Initiator Port)
响应方端口 (Responder Port)
TCP 标志 (TCP Flags)
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
实例 ID (Instance ID)
实例 ID (Instance ID)（续）
连接计数器 (Connection Counter)
第一个数据包时间 (First Pkt Time)
第一个数据包时间戳 (First Packet Timestamp)（续）
最后一个数据包时间 (Last Pkt Time)
最后一个数据包时间戳 (Last Packet Timestamp)（续）
发起方传输的数据包数 (Initiator Transmitted Packets)
发起方传输的数据包数 (Initiator Transmitted Packets)（续）

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	发起方传输的数据包数 (Initiator Transmitted Packets)（续）																								响应方传输的数据包数 (Resp. Tx Packets)							
	响应方传输的数据包数 (Responder Transmitted Packets)（续）																															
	响应方传输的数据包数 (Responder Transmitted Packets)（续）																								发起方传输的字节数 (Initiator Tx Bytes)							
	发起方传输的字节数 (Initiator Transmitted Bytes)（续）																															
	发起方传输的字节数 (Initiator Transmitted Bytes)（续）																								响应方传输的字节数 (Resp. Tx Bytes)							
	响应方传输的字节数 (Responder Transmitted Bytes)（续）																															
	响应方传输的字节数 (Responder Transmitted Bytes)（续）																								用户 ID							
	用户 ID (User ID)（续）																								应用协议ID							
	应用协议 ID (Application Protocol ID)（续）																								URL 类别 (URL Category)							
	URL 类别 (URL Category)（续）																								URL 信誉 (URL Reputation)							
	URL 信誉 (URL Reputation)（续）																								客户端应用 ID (Client App ID)							
	客户端应用 ID (Client Application ID)（续）																								Web 应用 ID (Web App ID)							
客户端 URL	Web 应用 ID (Web Application ID)（续）																								字符串块类型 (0) (Str. Block Type (0))							
	字符串块类型 (String Block Type)（续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length)（续）																								客户端应用URL... (Client App. URL...)							
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称...(NetBIOS Name...)																															



下表对用于 5.1.1.x 的连接统计信息数据块的字段进行了说明。

表 B-38　　连接统计信息数据块 5.1.1.x 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.1.1.x 的连接统计信息数据块。值始终为 137。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。

表 B-38 连接统计信息数据块 5.1.1.x 字段 （续）

字段	数据类型	说明 (Description)
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。

表 B-38　　连接统计信息数据块 5.1.1.x 字段 （续）

字段	数据类型	说明 (Description)
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如 /files/index.html）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。

表 B-38 连接统计信息数据块 5.1.1.x 字段 （续）

字段	数据类型	说明 (Description)
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。

连接统计信息数据块 5.3

连接统计信息数据块在连接数据消息中使用。版本 5.2.x 到版本 5.3 的连接数据块变更包括添加了用于 NetFlow 信息的新字段。用于版本 5.3 的连接统计信息数据块的块类型为系列 1 数据块组中的 152。它否决了块类型 144，连接统计信息数据块 5.2.x，第 B-175 页。

您可以通过在事件版本为 10 且事件代码为 71 的请求消息中设置扩展事件标志（请求标志字段中的位 30）请求扩展事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

下图显示用于 5.3+ 的连接统计信息数据块的格式：

::

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (152) (Connection Data Block Type (152))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (设备 ID)																																
入口区 (Ingress Zone)																																
入口区 (Ingress Zone)（续）																																
入口区 (Ingress Zone)（续）																																
入口区 (Ingress Zone)（续）																																
出口区 (Egress Zone)																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address)（续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)															
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)															
TCP 标志 (TCP Flags)																	协议 (Protocol)								NetFlow 源 (NetFlow Source)							
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																									实例 ID (Instance ID)							
实例 ID (Instance ID)（续）									连接计数器 (Connection Counter)																第一个数据包时间 (First Pkt Time)							
第一个数据包时间戳 (First Packet Timestamp)（续）																									最后一个数据包时间 (Last Pkt Time)							
最后一个数据包时间戳 (Last Packet Timestamp)（续）																									发起方传输的数据包数 (Initiator Transmitted Packets)							
发起方传输的数据包数 (Initiator Transmitted Packets)（续）																																
发起方传输的数据包数 (Initiator Transmitted Packets)（续）																									响应方传输的数据包数 (Resp. Tx Packets)							
响应方传输的数据包数 (Responder Transmitted Packets)（续）																																
响应方传输的数据包数 (Responder Transmitted Packets)（续）																									发起方传输的字节数 (Initiator Tx Bytes)							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	发起方传输的字节数 (Initiator Transmitted Bytes)（续）																															
	发起方传输的字节数 (Initiator Transmitted Bytes)（续）																								响应方传输的字节数 (Resp. Tx Bytes)							
	响应方传输的字节数 (Responder Transmitted Bytes)（续）																															
	响应方传输的字节数 (Responder Transmitted Bytes)（续）																								用户 ID							
	用户 ID (User ID)（续）																								应用协议ID							
	应用协议 ID (Application Protocol ID)（续）																								URL 类别 (URL Category)							
	URL 类别 (URL Category)（续）																								URL 信誉 (URL Reputation)							
	URL 信誉 (URL Reputation)（续）																								客户端应用 ID (Client App ID)							
	客户端应用 ID (Client Application ID)（续）																								Web 应用 ID (Web App ID)							
客户端 URL	Web 应用 ID (Web Application ID)（续）																								字符串块类型 (0) (Str. Block Type (0))							
	字符串块类型 (String Block Type)（续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length)（续）																								客户端应用URL... (Client App. URL...)							
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称...(NetBIOS Name...)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
监控器规则 4 (Monitor Rule 4)																																
监控器规则 5 (Monitor Rule 5)																																
监控器规则 6 (Monitor Rule 6)																																
监控器规则 7 (Monitor Rule 7)																																
监控器规则 8 (Monitor Rule 8)																																
安全接口源/目标 (Sec. Int. Src/Dst)									安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
入侵事件计数 (Intrusion Event Count)																	发起方国家/地区 (Initiator Country)															
响应方国家/地区 (Responder Country)																	IOC 编号 (IOC Number)															
源自治系统 (Source Autonomous System)																																
目标自治系统 (Destination Autonomous System)																																
SNMP 输入 (SNMP In)																	SNMP 输出 (SNMP Out)															
源 TOS (Source TOS)									目标 TOS (Destination TOS)								源掩码 (Source Mask)								目标掩码 (Destination Mask)							

下表对用于 5.3 的连接统计信息数据块的字段进行了说明。

表 B-39 连接统计信息数据块 5.3+ 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.3 的连接统计信息数据块。值始终为 152。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。

表 B-39　　连接统计信息数据块 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。

表 B-39 连接统计信息数据块 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如 `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。

表 B-39　　连接统计信息数据块 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。

表 B-39 连接统计信息数据块 5.3+ 字段 （续）

字段	数据类型	说明 (Description)
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家/地区 (Initiator Country)	uint16	发起主机的国家/地区代码。
响应方国家/地区 (Responder Country)	uint 16	响应主机的国家/地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。

连接统计信息数据块 5.3.1

连接统计信息数据块在连接数据消息中使用。从版本 5.3 到版本 5.3.1 对连接数据块进行的唯一变更是添加了安全情景字段。用于版本 5.3.1 的连接统计信息数据块的块类型为系列 1 数据块组中的 154。它否决了块类型 152，连接统计信息数据块 5.3，第 B-192 页。

您可以通过在事件版本为 11 且事件代码为 71 的请求消息中设置扩展事件标志（请求标志字段中的位 30）请求扩展事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

下图显示用于 5.3.1 的连接统计信息数据块的格式：

::

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接数据块类型 (154) (Connection Data Block Type (154))																																
连接数据块长度 (Connection Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone) 入口区 (Ingress Zone)（续） 入口区 (Ingress Zone)（续） 入口区 (Ingress Zone)（续）																																
出口区 (Egress Zone) 出口区 (Egress Zone)（续） 出口区 (Egress Zone)（续） 出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface) 入口接口 (Ingress Interface)（续） 入口接口 (Ingress Interface)（续） 入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface) 出口接口 (Egress Interface)（续） 出口接口 (Egress Interface)（续） 出口接口 (Egress Interface)（续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)														
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)														
TCP 标志 (TCP Flags)																	协议 (Protocol)								NetFlow 源 (NetFlow Source)						
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																									实例 ID (Instance ID)							
实例 ID (Instance ID)（续）									连接计数器 (Connection Counter)																				第一个数据包时间 (First Pkt Time)							
第一个数据包时间戳 (First Packet Timestamp)（续）																									最后一个数据包时间 (Last Pkt Time)							
最后一个数据包时间戳 (Last Packet Timestamp)（续）																									发起方传输的数据包数 (Initiator Transmitted Packets)							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	发起方传输的数据包数 (Initiator Transmitted Packets)（续）																															
	发起方传输的数据包数 (Initiator Transmitted Packets)（续）																								响应方传输的数据包数 (Resp. Tx Packets)							
	响应方传输的数据包数 (Responder Transmitted Packets)（续）																															
	响应方传输的数据包数 (Responder Transmitted Packets)（续）																								发起方传输的字节数 (Initiator Tx Bytes)							
	发起方传输的字节数 (Initiator Transmitted Bytes)（续）																															
	发起方传输的字节数 (Initiator Transmitted Bytes)（续）																								响应方传输的字节数 (Resp. Tx Bytes)							
	响应方传输的字节数 (Responder Transmitted Bytes)（续）																															
	响应方传输的字节数 (Responder Transmitted Bytes)（续）																								用户 ID							
	用户 ID (User ID)（续）																								应用协议ID							
	应用协议 ID (Application Protocol ID)（续）																								URL 类别 (URL Category)							
	URL 类别 (URL Category)（续）																								URL 信誉 (URL Reputation)							
	URL 信誉 (URL Reputation)（续）																								客户端应用 ID (Client App ID)							
	客户端应用 ID (Client Application ID)（续）																								Web 应用 ID (Web App ID)							
客户端 URL	Web 应用 ID (Web Application ID)（续）																								字符串块类型 (0) (Str. Block Type (0))							
	字符串块类型 (String Block Type)（续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length)（续）																								客户端应用URL... (Client App. URL...)							
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称...(NetBIOS Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源/目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																发起方国家/地区 (Initiator Country)															
	响应方国家/地区 (Responder Country)																IOC 编号 (IOC Number)															
	源自治系统 (Source Autonomous System)																															
	目标自治系统 (Destination Autonomous System)																															
	SNMP 输入 (SNMP In)																SNMP 输出 (SNMP Out)															
	源 TOS (Source TOS)								目标 TOS (Destination TOS)								源掩码 (Source Mask)								目标掩码 (Destination Mask)							
	安全情景 (Security Context) 安全情景 (Security Context)（续） 安全情景 (Security Context)（续） 安全情景 (Security Context)（续）																															

下表对用于 5.3.1 的连接统计信息数据块的字段进行了说明。

表 B-40　　连接统计信息数据块 5.3.1 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.3.1+ 的连接统计信息数据块。值始终为 154。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。

表 B-40 连接统计信息数据块 5.3.1 字段 （续）

字段	数据类型	说明 (Description)
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如 /files/index.html）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。

表 B-40　　连接统计信息数据块 5.3.1 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本(Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件计数(Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家/地区 (Initiator Country)	uint16	发起主机的国家/地区代码。
响应方国家/地区 (Responder Country)	uint 16	响应主机的国家/地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。

表 B-40　　连接统计信息数据块 5.3.1 字段 （续）

字段	数据类型	说明 (Description)
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

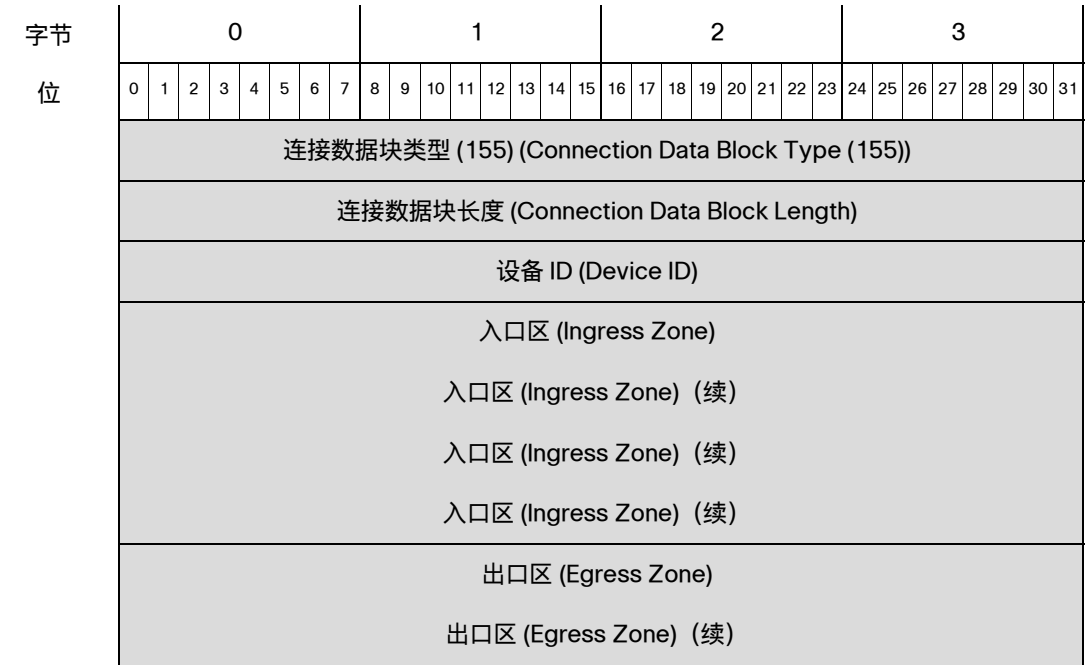
连接统计信息数据块 5.4

连接统计信息数据块在连接数据消息中使用。用于 5.4 的连接统计信息数据块中添加了多个新字段，添加新字段是为了支持 SSL 连接、HTTP 重定向以及网络分析策略。用于版本 5.4 的连接统计信息数据块的块类型为系列 1 数据块组中的 155。它不支持块类型 154，连接统计信息数据块 5.3.1，第 B-201 页。

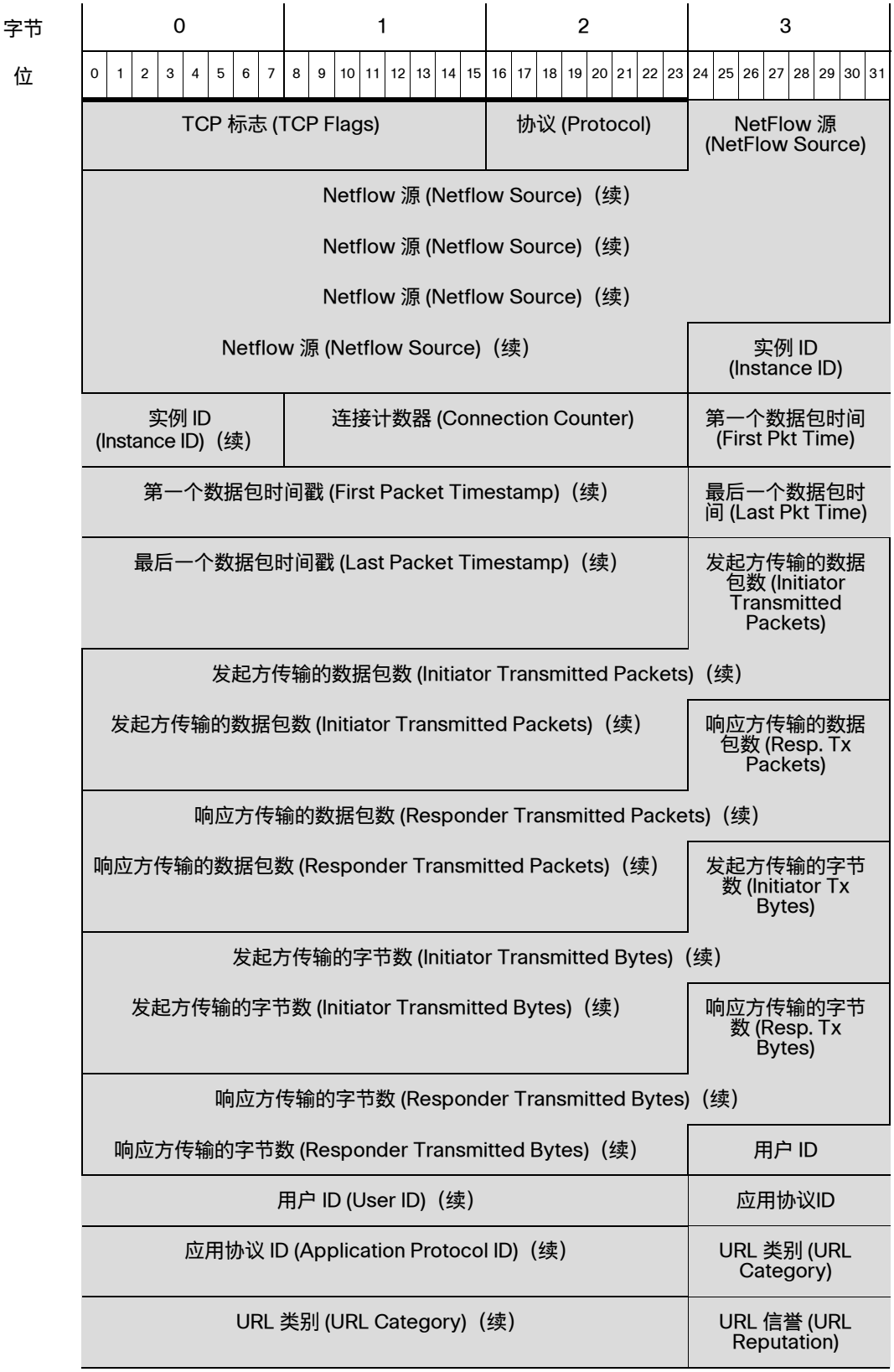
您可以通过在事件版本为 12 且事件代码为 71 的请求消息中设置扩展事件标志（请求标志字段中的位 30）请求扩展事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

下图显示用于 5.4 的连接统计信息数据块的格式：



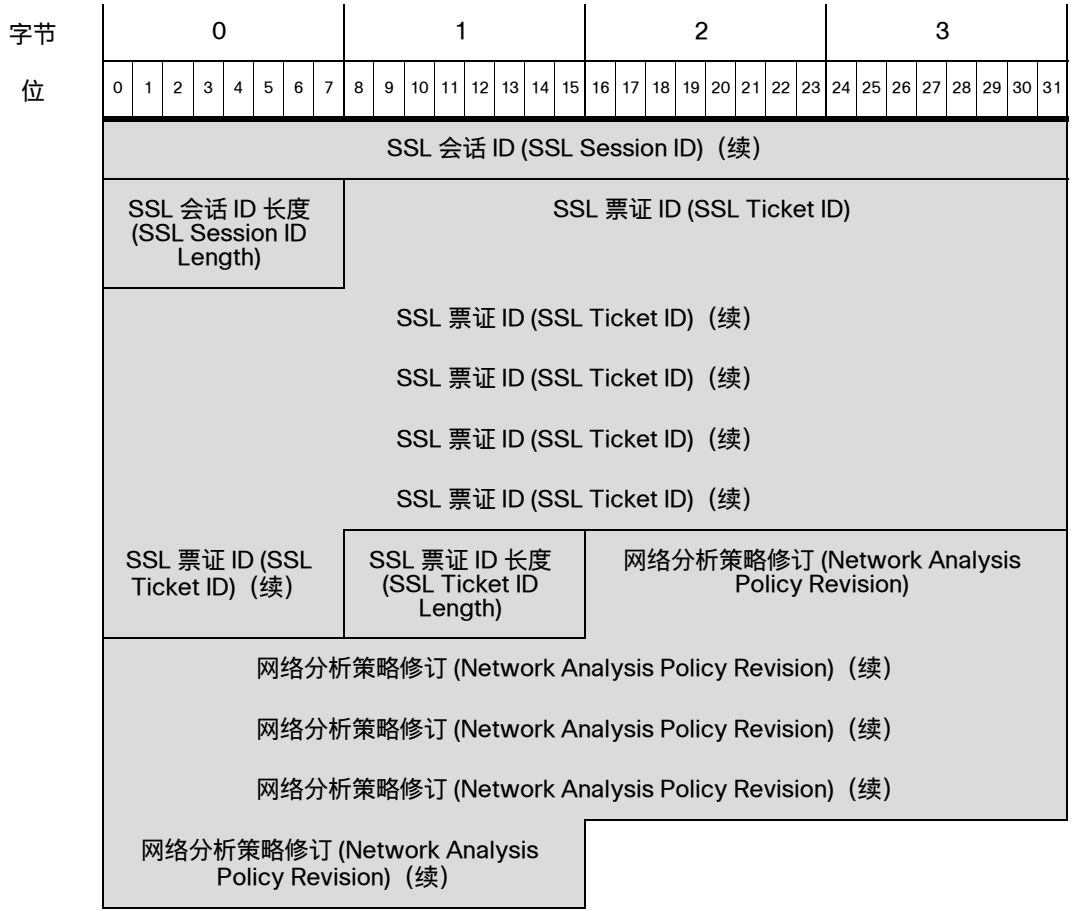
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)															
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)															


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
TCP 标志 (TCP Flags)
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
实例 ID (Instance ID)
实例 ID (Instance ID)（续）
连接计数器 (Connection Counter)
第一个数据包时间 (First Pkt Time)
第一个数据包时间戳 (First Packet Timestamp)（续）
最后一个数据包时间 (Last Pkt Time)
最后一个数据包时间戳 (Last Packet Timestamp)（续）
发起方传输的数据包数 (Initiator Transmitted Packets)
发起方传输的数据包数 (Initiator Transmitted Packets)（续）
发起方传输的数据包数 (Initiator Transmitted Packets)（续）
响应方传输的数据包数 (Resp. Tx Packets)
响应方传输的数据包数 (Responder Transmitted Packets)（续）
响应方传输的数据包数 (Responder Transmitted Packets)（续）
发起方传输的字节数 (Initiator Tx Bytes)
发起方传输的字节数 (Initiator Transmitted Bytes)（续）
发起方传输的字节数 (Initiator Transmitted Bytes)（续）
响应方传输的字节数 (Resp. Tx Bytes)
响应方传输的字节数 (Responder Transmitted Bytes)（续）
响应方传输的字节数 (Responder Transmitted Bytes)（续）
用户 ID
用户 ID (User ID)（续）
应用协议ID
应用协议 ID (Application Protocol ID)（续）
URL 类别 (URL Category)
URL 类别 (URL Category)（续）
URL 信誉 (URL Reputation)

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	URL 信誉 (URL Reputation)（续）																								客户端应用 ID (Client App ID)							
	客户端应用 ID (Client Application ID)（续）																								Web 应用 ID (Web App ID)							
客户端 URL	Web 应用 ID (Web Application ID)（续）																								字符串块类型 (0) (Str. Block Type (0))							
	字符串块类型 (String Block Type)（续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length)（续）																								客户端应用URL... (Client App. URL...)							
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称...(NetBIOS Name...)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源/目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																发起方国家/地区 (Initiator Country)															
	响应方国家/地区 (Responder Country)																IOC 编号 (IOC Number)															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	源自治系统 (Source Autonomous System)																															
	目标自治系统 (Destination Autonomous System)																															
	SNMP 输入 (SNMP In)																SNMP 输出 (SNMP Out)															
	源 TOS (Source TOS)								目标 TOS (Destination TOS)								源掩码 (Source Mask)								目标掩码 (Destination Mask)							
	安全情景 (Security Context)																															
	安全情景 (Security Context)（续）																															
	安全情景 (Security Context)（续）																															
	安全情景 (Security Context)（续）																															
引用的主机 (Referenced Host)	VLAN ID																字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0))（续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length)（续）																引用的主机 (Referenced Host)...(Referenced Host...)															
用户代理	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户代理... (User Agent...)																															
HTTP 引用站点 (HTTP Referrer)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	HTTP 引用站点...(HTTP Referrer...)																															
	SSL 证书指纹 (SSL Certificate Fingerprint)																															
	SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															
	SSL 策略 ID (SSL Policy ID)																															
	SSL 策略 ID (SSL Policy ID)（续）																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）
SSL 规则 ID (SSL Rule ID)
SSL 密码套件 (SSL Cipher Suite)
SSL 版本 (SSL Version)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)（续）
SSL 实际操作 (SSL Actual Action)
SSL 预期操作 (SSL Expected Action)
SSL 预期操作 (SSL Expected Action)（续）
SSL 流状态 (SSL Flow Status)
SSL 流误差 (SSL Flow Error)
SSL 流误差 (SSL Flow Error)（续）
SSL 流消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Messages)（续）
SSL 流标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags)（续）
SSL 流标志 (SSL Flow Flags)（续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
SSL 服务器名称... (SSL Server Names...)
SSL 服务器名称 (SSL Server Names)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）



下表对用于 5.4+ 的连接统计信息数据块的字段进行了说明。

表 B-41 连接统计信息数据块 5.4+ 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.4+ 的连接统计信息数据块。值始终为 155。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。

表 B-41　　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。

表 B-41 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如/files/index.html）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本(Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。

表 B-41　　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家/地区 (Initiator Country)	uint16	发起主机的国家/地区代码。
响应方国家/地区 (Responder Country)	uint 16	响应主机的国家/地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“引用的主机”(Referenced Host) 字段中的字节数。
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户代理”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。

表 B-41 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“HTTP 引用站点”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在HTTP流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。
SSL 服务器证书状态 (SSL Server Certificate Status)	uint16	SSL 证书的状态。可能的值包括: ▪ 0 - 未检查 - 服务器证书状态未评估。 ▪ 1 - 未知 - 服务器证书状态无法确定。 ▪ 2 - 有效 - 服务器证书有效。 ▪ 4 - 自签 - 服务器证书已自签。 ▪ 16 - 颁发者无效 - 服务器证书的颁发者无效。 ▪ 32 - 签名无效 - 服务器证书的签名无效。 ▪ 64 - 过期 - 服务器证书已过期。 ▪ 128 - 尚未生效 - 服务器证书尚未生效。 ▪ 256 - 撤销 - 服务器证书已被撤销。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-41　　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 11 -‘待处理通用名称分类查找’ ▪ 11 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 B-41 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 ▪ 0x00000001 - NSE_MT__HELLO_REQUEST ▪ 0x00000002 - NSE_MT__CLIENT_ALERT ▪ 0x00000004 - NSE_MT__SERVER_ALERT ▪ 0x00000008 - NSE_MT__CLIENT_HELLO ▪ 0x00000010 - NSE_MT__SERVER_HELLO ▪ 0x00000020 - NSE_MT__SERVER_CERTIFICATE ▪ 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE ▪ 0x00000080 - NSE_MT__CERTIFICATE_REQUEST ▪ 0x00000100 - NSE_MT__SERVER_HELLO_DONE ▪ 0x00000200 - NSE_MT__CLIENT_CERTIFICATE ▪ 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE ▪ 0x00000800 - NSE_MT__CERTIFICATE_VERIFY ▪ 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC ▪ 0x00002000 - NSE_MT__CLIENT_FINISHED ▪ 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC ▪ 0x00008000 - NSE_MT__SERVER_FINISHED ▪ 0x00010000 - NSE_MT__NEW_SESSION_TICKET ▪ 0x00020000 - NSE_MT__HANDSHAKE_OTHER ▪ 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT ▪ 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括： ▪ 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 ▪ 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 ▪ 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“SSL 服务器名称”(SSL Server Name) 字段中的字节数。
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时，SSL 握手期间使用的会话 ID 值
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。

表 B-41　　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy Revision)	uint8[16]	与连接事件相关的网络分析策略的修订。

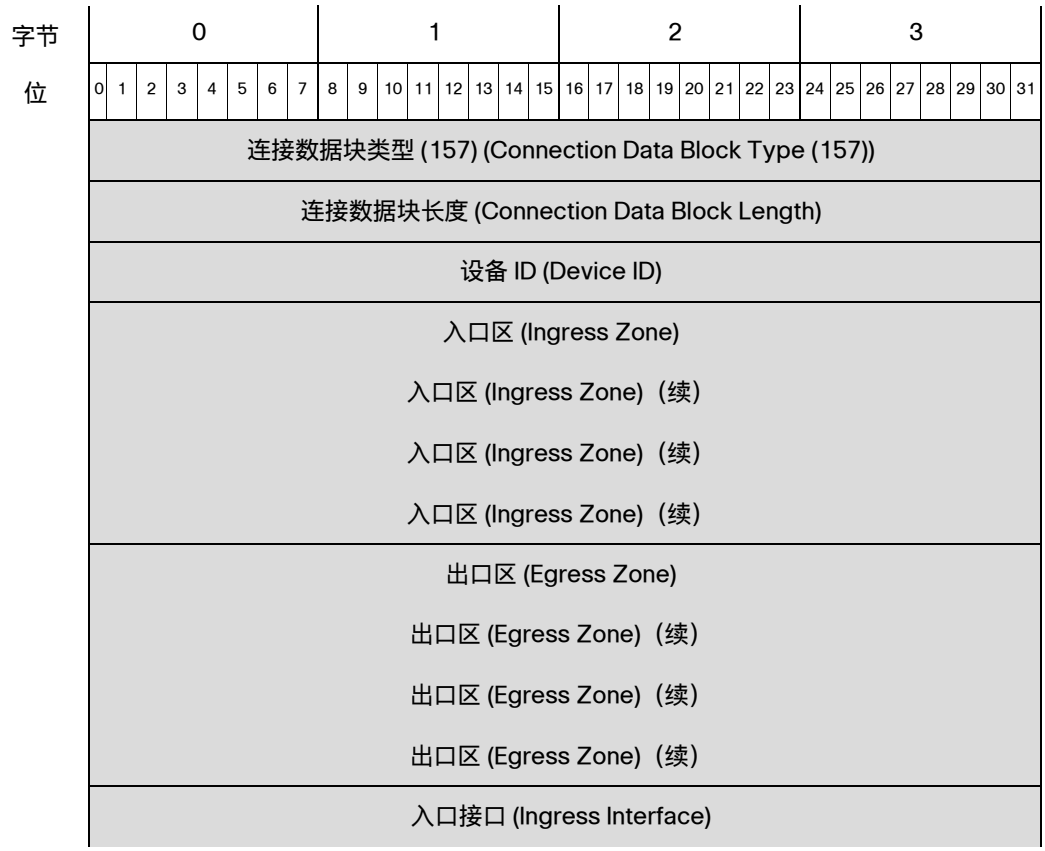
连接统计信息数据块 5.4.1

连接统计信息数据块在连接数据消息中使用。用于 5.4 的连接统计信息数据块中添加了多个新字段，添加新字段是为了支持 SSL 连接、HTTP 重定向以及网络分析策略。用于版本 5.4+ 的连接统计信息数据块的块类型为系列 1 数据块组中的 157。它否决了块类型 155，连接统计信息数据块 5.3.1，第 B-201 页。

您可以通过在事件版本为 12 且事件代码为 71 的请求消息中设置扩展事件标志（请求标志字段中的位 30）请求扩展事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

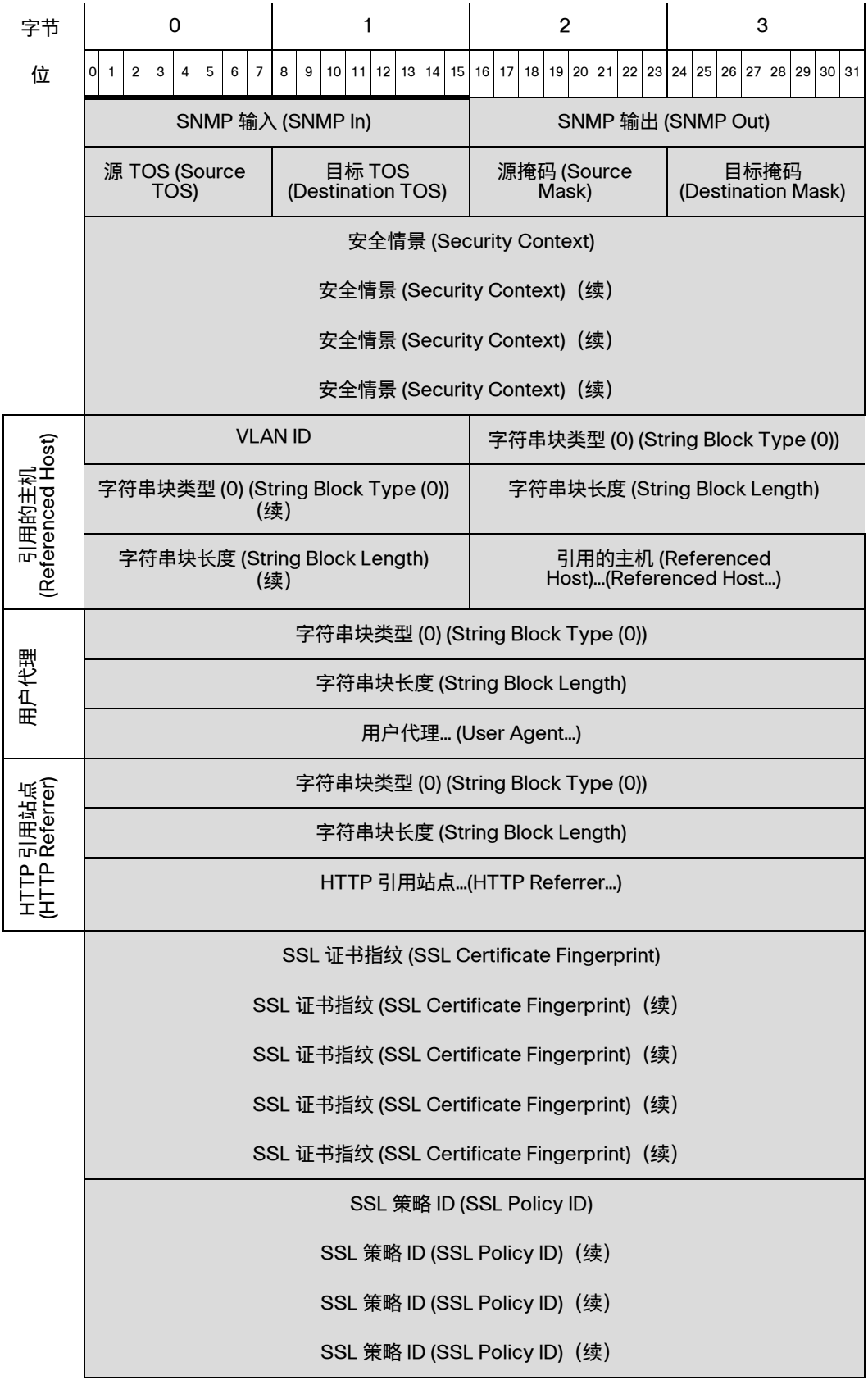
下图显示用于 5.4+ 的连接统计信息数据块的格式：

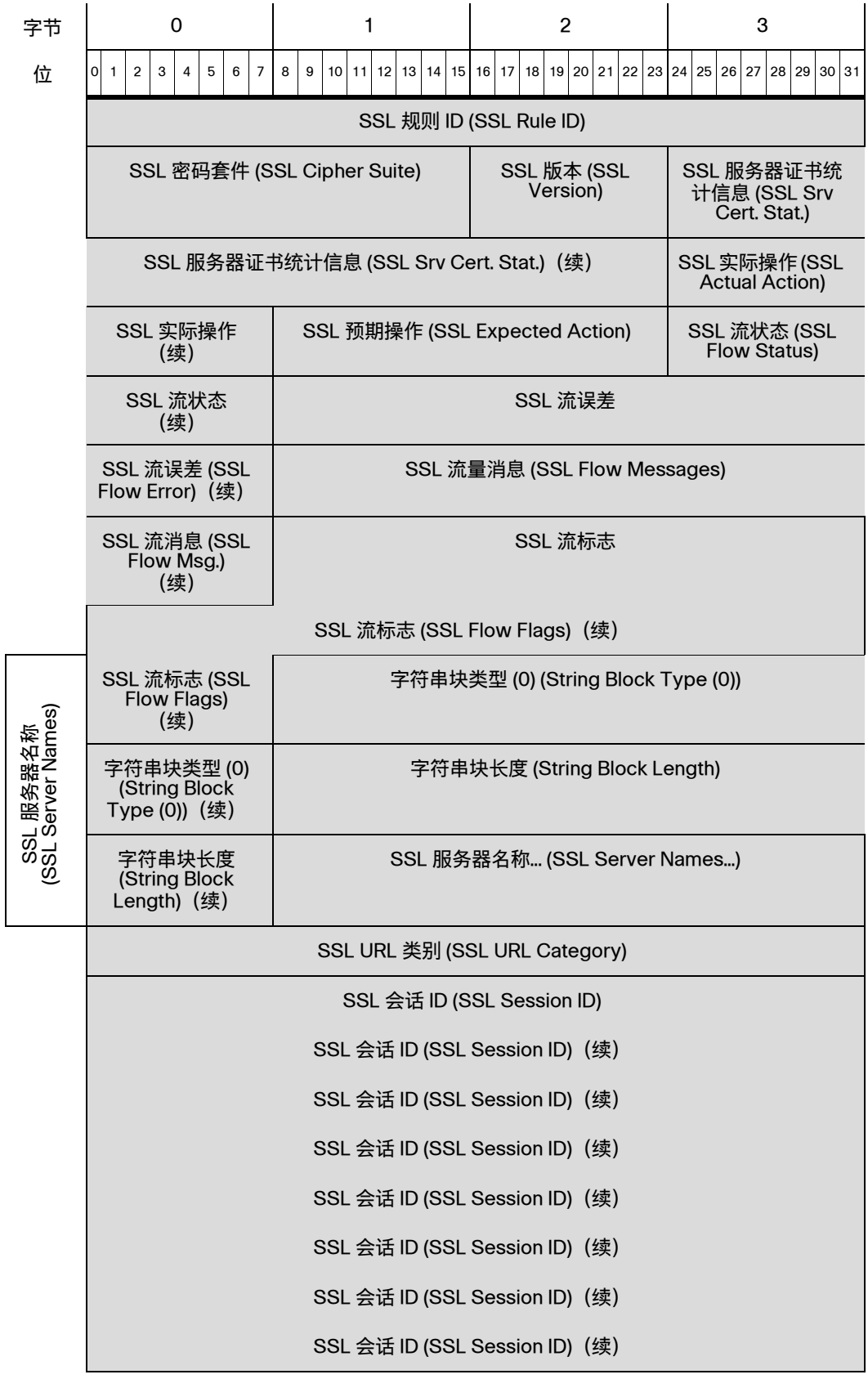


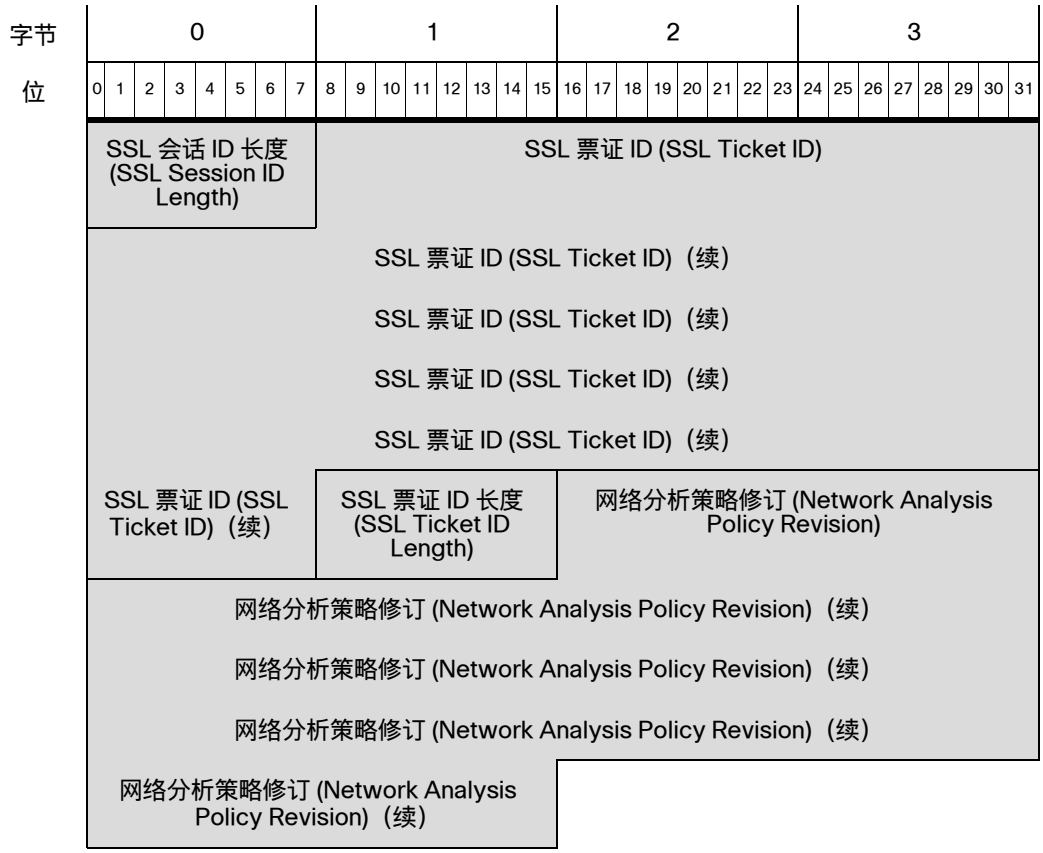
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)														
发起方端口 (Initiator Port)																	响应方端口 (Responder Port)														
TCP 标志 (TCP Flags)																	协议 (Protocol)								NetFlow 源 (NetFlow Source)						
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																									实例 ID (Instance ID)							
实例 ID (Instance ID)（续）									连接计数器 (Connection Counter)																				第一个数据包时间 (First Pkt Time)							
第一个数据包时间戳 (First Packet Timestamp)（续）																																
最后一个数据包时间 (Last Pkt Time)																																
最后一个数据包时间戳 (Last Packet Timestamp)（续）																																
发起方传输的数据包数 (Initiator Transmitted Packets)																																
发起方传输的数据包数 (Initiator Transmitted Packets)（续）																																
响应方传输的数据包数 (Resp. Tx Packets)																																
响应方传输的数据包数 (Responder Transmitted Packets)（续）																																
响应方传输的数据包数 (Responder Transmitted Packets)（续）																																
发起方传输的字节数 (Initiator Tx Bytes)																																
发起方传输的字节数 (Initiator Transmitted Bytes)（续）																																
发起方传输的字节数 (Initiator Transmitted Bytes)（续）																																
响应方传输的字节数 (Resp. Tx Bytes)																																
响应方传输的字节数 (Responder Transmitted Bytes)（续）																																
响应方传输的字节数 (Responder Transmitted Bytes)（续）																																
用户 ID																																
用户 ID (User ID)（续）																																
应用协议ID																																
应用协议 ID (Application Protocol ID)（续）																																
URL 类别 (URL Category)																																
URL 类别 (URL Category)（续）																																
URL 信誉 (URL Reputation)																																
URL 信誉 (URL Reputation)（续）																																
客户端应用 ID (Client App ID)																																
客户端应用 ID (Client Application ID)（续）																																
Web 应用 ID (Web App ID)																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
客户端 URL	Web 应用 ID (Web Application ID)（续）																								字符串块类型 (0) (Str. Block Type (0))							
	字符串块类型 (String Block Type)（续）																								字符串块长度 (String Block Length)							
	字符串块长度 (String Block Length)（续）																								客户端应用URL... (Client App. URL...)							
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称...(NetBIOS Name...)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源/目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																发起方国家/地区 (Initiator Country)															
	响应方国家/地区 (Responder Country)																IOC 编号 (IOC Number)															
	源自治系统 (Source Autonomous System)																															
	目标自治系统 (Destination Autonomous System)																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SNMP 输入 (SNMP In)
SNMP 输出 (SNMP Out)
源 TOS (Source TOS)
目标 TOS (Destination TOS)
源掩码 (Source Mask)
目标掩码 (Destination Mask)
安全情景 (Security Context)
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
引用的主机 (Referenced Host)
VLAN ID
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
引用的主机 (Referenced Host)...(Referenced Host...)
用户代理
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
用户代理... (User Agent...)
HTTP 引用站点 (HTTP Referrer)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
HTTP 引用站点...(HTTP Referrer...)
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 策略 ID (SSL Policy ID)
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 规则 ID (SSL Rule ID)
SSL 密码套件 (SSL Cipher Suite)
SSL 版本 (SSL Version)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)（续）
SSL 实际操作 (SSL Actual Action)
SSL 实际操作 (续)
SSL 预期操作 (SSL Expected Action)
SSL 流状态 (SSL Flow Status)
SSL 流状态 (续)
SSL 流误差
SSL 流误差 (SSL Flow Error)（续）
SSL 流量消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Msg.) (续)
SSL 流标志
SSL 流标志 (SSL Flow Flags)（续）
SSL 服务器名称 (SSL Server Names)
SSL 流标志 (SSL Flow Flags) (续)
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
SSL 服务器名称... (SSL Server Names...)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）



下表对用于 5.4+ 的连接统计信息数据块的字段进行了说明。

表 B-42　　连接统计信息数据块 5.4+ 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 5.4+ 的连接统计信息数据块。值始终为 157。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。

表 B-42 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint16	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。

表 B-42　　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如 `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。

表 B-42 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。

表 B-42　　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家/地区 (Initiator Country)	uint16	发起主机的国家/地区代码。
响应方国家/地区 (Responder Country)	uint 16	响应主机的国家/地区代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“引用的主机”(Referenced Host) 字段中的字节数。

表 B-42 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户代理”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“HTTP 引用站点”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在 HTTP 流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 证书的状态。可能的值包括: ▪ 0 - 未检查 - 服务器证书状态未评估。 ▪ 1 - 未知 - 服务器证书状态无法确定。 ▪ 2 - 有效 - 服务器证书有效。 ▪ 4 - 自签 - 服务器证书已自签。 ▪ 16 - 颁发者无效 - 服务器证书的颁发者无效。 ▪ 32 - 签名无效 - 服务器证书的签名无效。 ▪ 64 - 过期 - 服务器证书已过期。 ▪ 128 - 尚未生效 - 服务器证书尚未生效。 ▪ 256 - 撤销 - 服务器证书已被撤销。

表 B-42　　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-42 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 B-42　　连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 ▪ 0x00000001 - NSE_MT__HELLO_REQUEST ▪ 0x00000002 - NSE_MT__CLIENT_ALERT ▪ 0x00000004 - NSE_MT__SERVER_ALERT ▪ 0x00000008 - NSE_MT__CLIENT_HELLO ▪ 0x00000010 - NSE_MT__SERVER_HELLO ▪ 0x00000020 - NSE_MT__SERVER_CERTIFICATE ▪ 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE ▪ 0x00000080 - NSE_MT__CERTIFICATE_REQUEST ▪ 0x00000100 - NSE_MT__SERVER_HELLO_DONE ▪ 0x00000200 - NSE_MT__CLIENT_CERTIFICATE ▪ 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE ▪ 0x00000800 - NSE_MT__CERTIFICATE_VERIFY ▪ 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC ▪ 0x00002000 - NSE_MT__CLIENT_FINISHED ▪ 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC ▪ 0x00008000 - NSE_MT__SERVER_FINISHED ▪ 0x00010000 - NSE_MT__NEW_SESSION_TICKET ▪ 0x00020000 - NSE_MT__HANDSHAKE_OTHER ▪ 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT ▪ 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括： ▪ 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 ▪ 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 ▪ 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“SSL 服务器名称”(SSL Server Name) 字段中的字节数。

表 B-42 连接统计信息数据块 5.4+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时，SSL 握手期间使用的会话 ID 值
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy Revision)	uint8[16]	与连接事件相关的网络分析策略的修订。

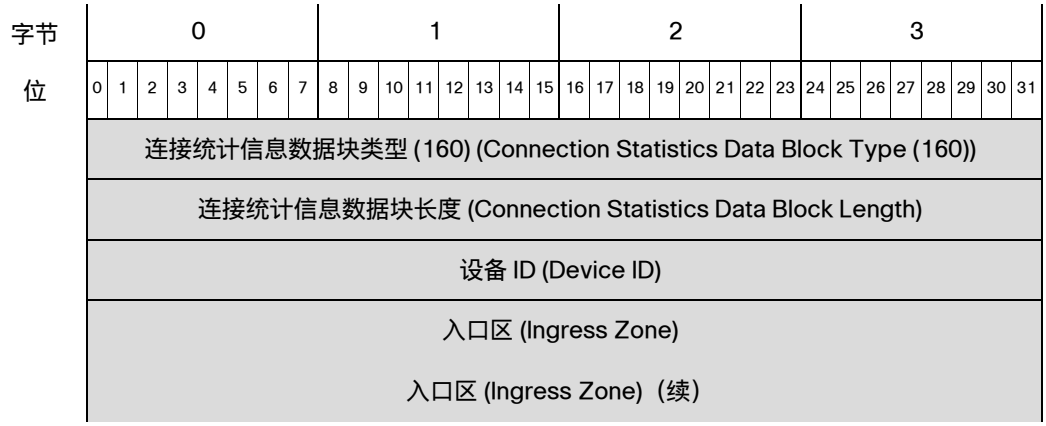
连接统计信息数据块 6.0.x

连接统计信息数据块在连接数据消息中使用。用于 6.0 的连接统计信息数据块中添加了多个新字段。添加新字段是为了支持 ISE 集成和多个网络映射。用于版本 6.0.x 的连接统计信息数据块的块类型为系列 1 数据块组中的 160。它替代块类型 157，连接统计信息数据块 5.4.1，第 B-221 页。添加新字段是为了支持 DNS 查询和安全情报。

您可以通过在事件版本为 13 且事件代码为 71 的请求消息中设置扩展事件标志（“请求标志”(Request Flags) 字段中的位 30）请求连接事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

下图显示用于 6.0.x 的连接统计信息数据块的格式:

7

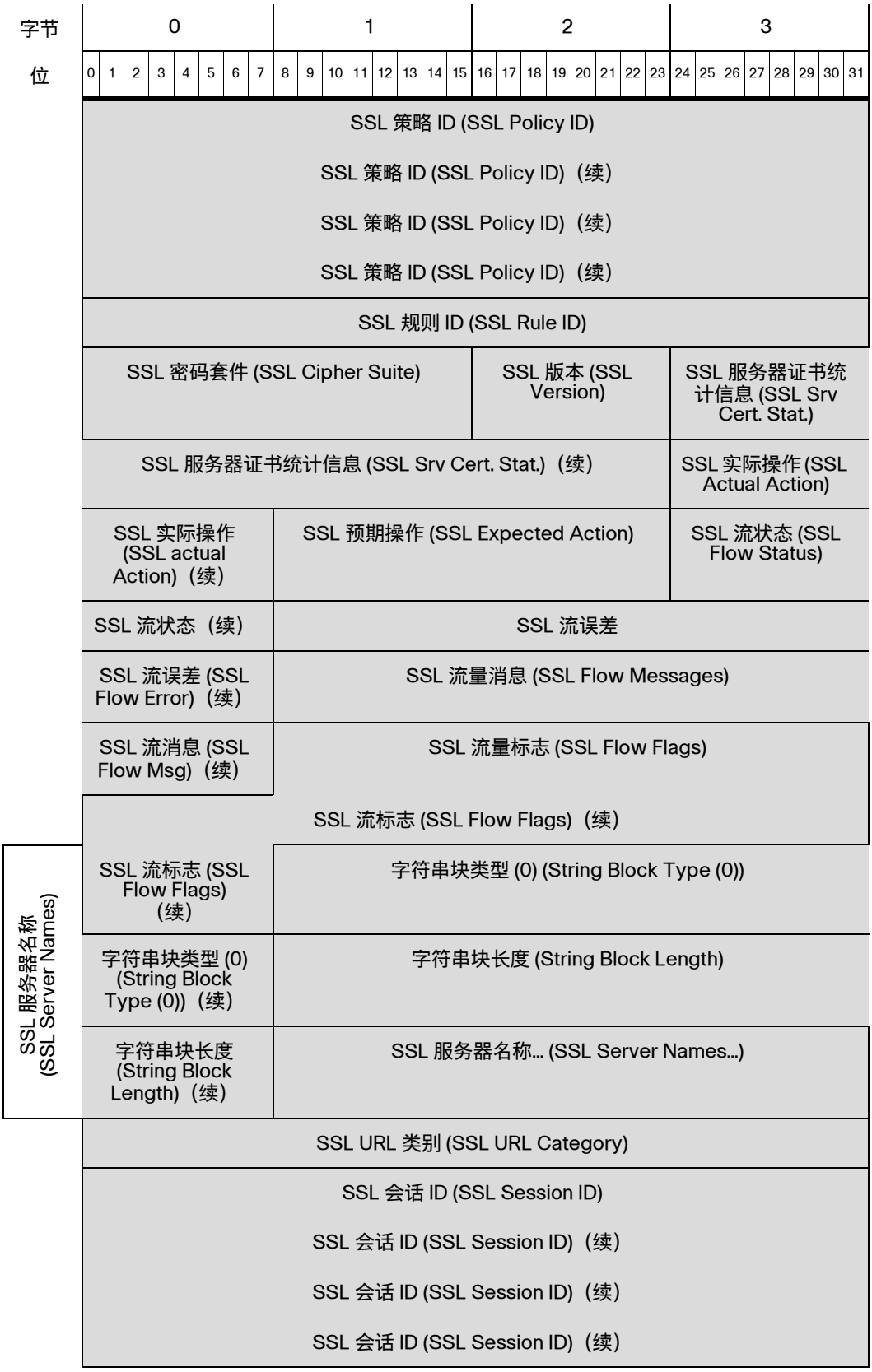


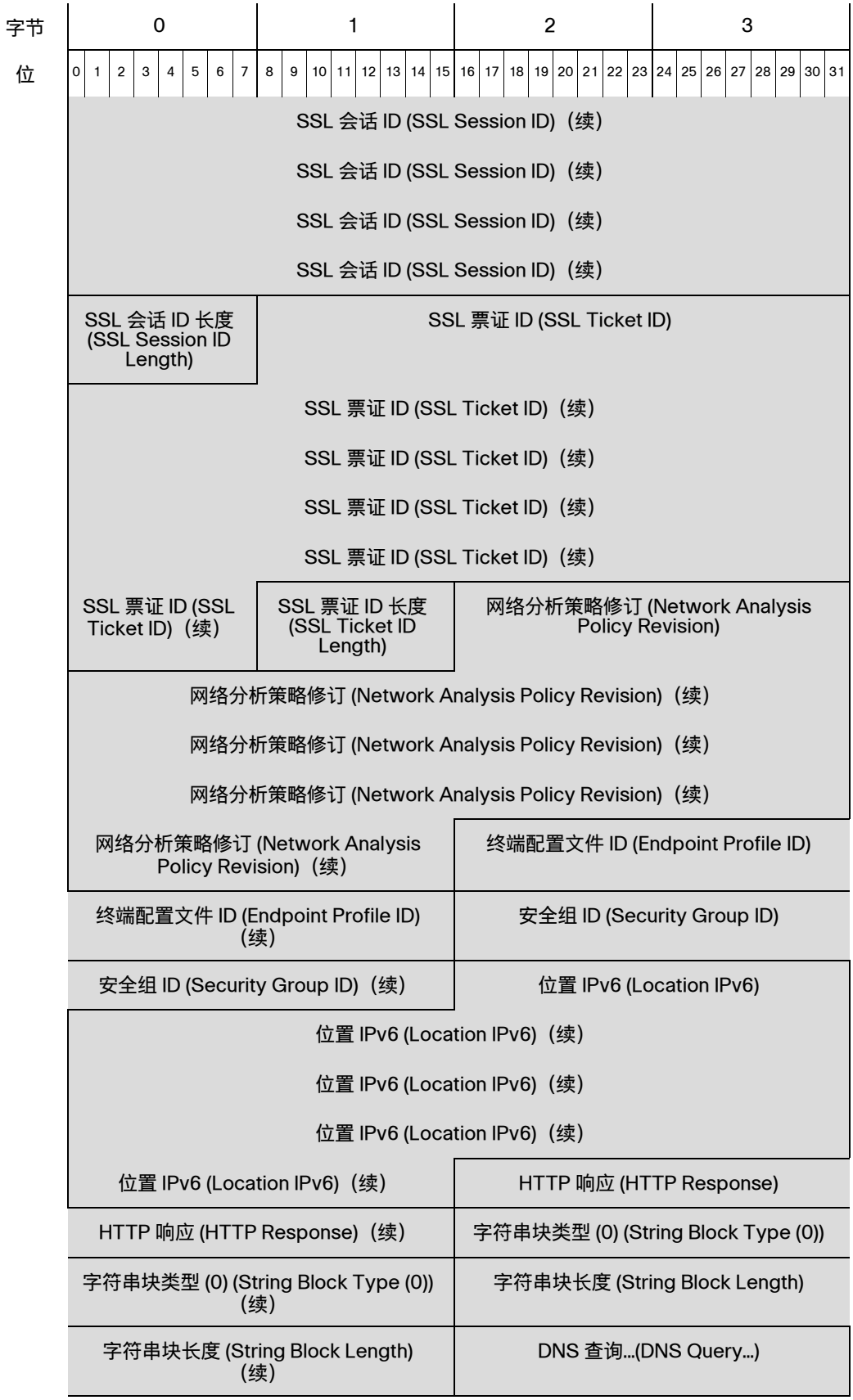
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入口区 (Ingress Zone)（续）																																
入口区 (Ingress Zone)（续）																																
出口区 (Egress Zone)																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																

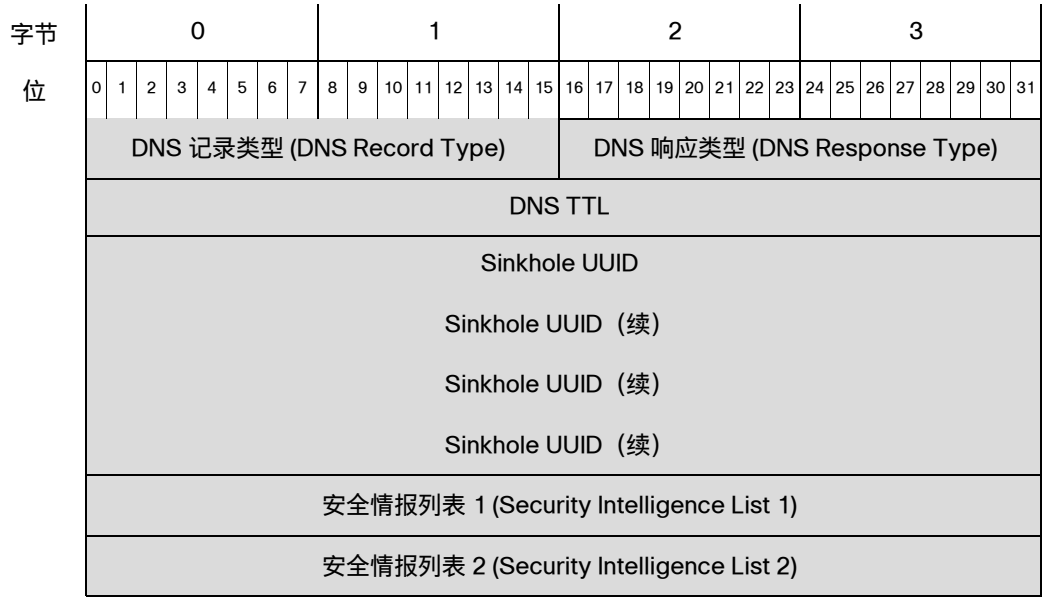
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
规则 ID (Rule ID)																																
规则操作 (Rule Action)																	规则原因 (Rule Reason)														
规则原因（续）																	发起方端口 (Initiator Port)														
响应方端口 (Responder Port)																	TCP 标志 (TCP Flags)														
协议 (Protocol)									NetFlow 源 (NetFlow Source)																							
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																																
Netflow 源 (Netflow Source)（续）																																
NetFlow 源（续）									实例 ID (Instance ID)																连接计数器 (Connection Counter)							
连接计数器（续）									第一个数据包时间戳 (First Packet Timestamp)																							
第一个数据包时间戳 (First Pkt Time)（续）									最后一个数据包时间戳 (Last Packet Timestamp)																							
最后一个数据包时间戳（续）									发起方传输的数据包数 (Initiator Transmitted Packets)																							
发起方传输的数据包数 (Initiator Transmitted Packets)（续）																																
发起方传输的数据包数（续）									响应方传输的数据包数 (Responder Transmitted Packets)																							
响应方传输的数据包数 (Responder Transmitted Packets)（续）																																
响应方传输的数据包数（续）									发起方传输的字节数 (Initiator Transmitted Bytes)																							
发起方传输的字节数 (Initiator Transmitted Bytes)（续）																																
发起方传输的字节数（续）									响应方传输的字节数 (Responder Transmitted Bytes)																							
响应方传输的字节数 (Responder Transmitted Bytes)（续）																																
响应方传输的字节数（续）									用户 ID																							
用户 ID (User ID)（续）									应用协议 ID (Application Protocol ID)																							
应用协议 ID（续）									URL 类别 (URL Category)																							


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
URL 类别 (URL Category)（续）
URL 信誉 (URL Reputation)
URL 信誉 (URL Reputation)（续）
客户端应用 ID (Client Application ID)
客户端应用 ID (Client App ID)（续）
Web 应用 ID (Web Application ID)
客户端 URL
Web 应用 ID（续）
字符串块类型 (0) (Str. Block Type (0))
字符串块类型（续）
字符串块长度 (String Block Length)
字符串块长度（续）
客户端应用URL... (Client App. URL...)
NetBIOS 名称 (Name)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
NetBIOS 名称...(NetBIOS Name...)
客户端应用版本 (Client App Version)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
客户端应用版本...(Client Application Version...)
监控器规则 1 (Monitor Rule 1)
监控器规则 2 (Monitor Rule 2)
监控器规则 3 (Monitor Rule 3)
监控器规则 4 (Monitor Rule 4)
监控器规则 5 (Monitor Rule 5)
监控器规则 6 (Monitor Rule 6)
监控器规则 7 (Monitor Rule 7)
监控器规则 8 (Monitor Rule 8)
安全接口源/目标 (Sec. Int. Src/Dst)
安全接口层 (Sec. Int. Layer)
文件事件计数 (File Event Count)

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	入侵事件计数 (Intrusion Event Count)																发起方国家/地区 (Initiator Country)															
	响应方国家/地区 (Responder Country)																IOC 编号 (IOC Number)															
	源自治系统 (Source Autonomous System)																															
	目标自治系统 (Destination Autonomous System)																															
	SNMP 输入 (SNMP In)																SNMP 输出 (SNMP Out)															
	源 TOS (Source TOS)								目标 TOS (Destination TOS)								源掩码 (Source Mask)								目标掩码 (Destination Mask)							
	安全情景 (Security Context) 安全情景 (Security Context)（续） 安全情景 (Security Context)（续） 安全情景 (Security Context)（续）																															
引用的主机 (Referenced Host)	VLAN ID																字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0))（续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length)（续）																引用的主机 (Referenced Host)...(Referenced Host...)															
用户代理	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户代理... (User Agent...)																															
HTTP 引用站点 (HTTP Referrer)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	HTTP 引用站点...(HTTP Referrer...)																															
	SSL 证书指纹 (SSL Certificate Fingerprint) SSL 证书指纹 (SSL Certificate Fingerprint)（续） SSL 证书指纹 (SSL Certificate Fingerprint)（续） SSL 证书指纹 (SSL Certificate Fingerprint)（续） SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 策略 ID (SSL Policy ID)
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）
SSL 规则 ID (SSL Rule ID)
SSL 密码套件 (SSL Cipher Suite)
SSL 版本 (SSL Version)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)（续）
SSL 实际操作 (SSL Actual Action)
SSL 实际操作 (SSL actual Action)（续）
SSL 预期操作 (SSL Expected Action)
SSL 流状态 (SSL Flow Status)
SSL 流状态（续）
SSL 流误差
SSL 流误差 (SSL Flow Error)（续）
SSL 流量消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Msg)（续）
SSL 流量标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags)（续）
SSL 流标志 (SSL Flow Flags)（续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
SSL 服务器名称... (SSL Server Names...)
SSL 服务器名称 (SSL Server Names)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID 长度 (SSL Session ID Length)
SSL 票证 ID (SSL Ticket ID)
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID 长度 (SSL Ticket ID Length)
网络分析策略修订 (Network Analysis Policy Revision)
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
终端配置文件 ID (Endpoint Profile ID)
终端配置文件 ID (Endpoint Profile ID)（续）
安全组 ID (Security Group ID)
安全组 ID (Security Group ID)（续）
位置 IPv6 (Location IPv6)
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
HTTP 响应 (HTTP Response)
HTTP 响应 (HTTP Response)（续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
DNS 查询...(DNS Query...)



下表对用于 6.0.x 的连接统计信息数据块的字段进行了说明。

表 B-43　　连接统计信息数据块 6.0.x 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 6.0+ 的连接统计信息数据块。值始终为 160。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。

表 B-43 连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明 (Description)
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint32	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。

表 B-43　　连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明 (Description)
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如 `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。

表 B-43 连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家/地区 (Initiator Country)	uint16	发起主机的国家/地区代码。
响应方国家/地区 (Responder Country)	uint 16	响应主机的国家/地区代码。

表 B-43　　连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明 (Description)
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“引用的主机”(Referenced Host) 字段中的字节数。
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户代理”(User Agent) 字段中的字节数。

表 B-43 连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明 (Description)
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“HTTP 引用站点”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在 HTTP 流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 证书的状态。可能的值包括： ▪ 0 - 未检查 - 服务器证书状态未评估。 ▪ 1 - 未知 - 服务器证书状态无法确定。 ▪ 2 - 有效 - 服务器证书有效。 ▪ 4 - 自签 - 服务器证书已自签。 ▪ 16 - 颁发者无效 - 服务器证书的颁发者无效。 ▪ 32 - 签名无效 - 服务器证书的签名无效。 ▪ 64 - 过期 - 服务器证书已过期。 ▪ 128 - 尚未生效 - 服务器证书尚未生效。 ▪ 256 - 撤销 - 服务器证书已被撤销。

表 B-43　　连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明 (Description)
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-43 连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 B-43　　连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明 (Description)
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 ▪ 0x00000001 - NSE_MT__HELLO_REQUEST ▪ 0x00000002 - NSE_MT__CLIENT_ALERT ▪ 0x00000004 - NSE_MT__SERVER_ALERT ▪ 0x00000008 - NSE_MT__CLIENT_HELLO ▪ 0x00000010 - NSE_MT__SERVER_HELLO ▪ 0x00000020 - NSE_MT__SERVER_CERTIFICATE ▪ 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE ▪ 0x00000080 - NSE_MT__CERTIFICATE_REQUEST ▪ 0x00000100 - NSE_MT__SERVER_HELLO_DONE ▪ 0x00000200 - NSE_MT__CLIENT_CERTIFICATE ▪ 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE ▪ 0x00000800 - NSE_MT__CERTIFICATE_VERIFY ▪ 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC ▪ 0x00002000 - NSE_MT__CLIENT_FINISHED ▪ 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC ▪ 0x00008000 - NSE_MT__SERVER_FINISHED ▪ 0x00010000 - NSE_MT__NEW_SESSION_TICKET ▪ 0x00020000 - NSE_MT__HANDSHAKE_OTHER ▪ 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT ▪ 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括： ▪ 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 ▪ 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 ▪ 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“SSL 服务器名称”(SSL Server Name) 字段中的字节数。
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。

表 B-43 连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明 (Description)
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时，SSL 握手期间使用的会话 ID 值
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy Revision)	uint8[16]	与连接事件相关的网络分析策略的修订。
终端配置文件 ID (Endpoint Profile ID)	uint32	ISE 识别的连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	由 ISE 根据策略分配给用户的 ID 号码。
位置 IPv6 (Location IPv6)	uint8[16]	与 ISE 通信的接口的 IP 地址。可以是 IPv4 或 IPv6。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。
字符串块类型 (String Block Type)	uint32	启动 DNS 查询的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 DNS 查询字符串中的字节数。
DNS 查询 (DNS Query)	字符串	发送到 DNS 服务器的查询的内容。
DNS 记录类型 (DNS Record	uint16	DNS 记录类型的数字值。

表 B-43　　连接统计信息数据块 6.0.x 字段 （续）

字段	数据类型	说明 (Description)
DNS 响应类型 (DNS Response Type)	uint16	0 - NoError - 无错误 1 - FormErr - 格式错误 2 - ServFail - 服务器故障 3 - NXDomain - 域不存在 4 - NotImp - 未执行 5 - Refused - 查询被拒绝 6 - YXDomain - 名称在不应该存在的时候存在 7 - YXRRSet - RR 设置在不应该存在的时候存在 8 - NXRRSet - 应该存在的 RR 设置不存在 9 - NotAuth - 未授权 10 - NotZone - 区域中不包含名称 16 - BADSIG - TSIG 签名故障 17 - BADKEY - 密钥未识别 18 - BADTIME - 签名超出时间窗口 19 - BADMODE - 坏 TKEY 模式 20 - BADNAME - 密钥名称重复 21 - BADALG - 不支持算法 22 - BADTRUNC - 截断错误 3841 - NXDOMAIN - 防火墙的 NXDOMAIN 响应 3842 - SINKHOLE - 从防火墙发出黑洞 (Sinkhole) 响应
DNS TTL	uint32	DNS 响应的生存时间（秒数）
Sinkhole UUID	uin8[16]	与此 sinkhole 对象关联的修订 UUID。
安全情报列表 1 (Security Intelligence List 1)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能存在两个与连接关联的安全情报列表。
安全情报列表 2 (Security Intelligence List 2)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能存在两个与连接关联的安全情报列表。

连接统计信息数据块 6.1.x

连接统计信息数据块在连接数据消息中使用。用于 6.1.x 的连接统计信息数据块中添加了多个新字段。添加新字段是为了支持 ISE 集成和多个网络映射。用于版本 6.1+ 的连接统计信息数据块的块类型为系列 1 数据块组中的 163。它替代块类型 160，连接统计信息数据块 6.0.x，第 B-236 页。添加新字段是为了支持 DNS 查询和安全情报。它被块类型 168 替代，连接统计信息数据块 7.1+，第 4-116 页，

您可以通过在事件版本为 13 且事件代码为 71 的请求消息中设置扩展事件标志（“请求标志”(Request Flags) 字段中的位 30）请求连接事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

下图显示用于 6.1+ 的连接统计信息数据块的格式：

7

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接统计信息数据块类型 (163) (Connection Statistics Data Block Type (160))																																
连接统计信息数据块长度 (Connection Statistics Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone) 入口区 (Ingress Zone)（续） 入口区 (Ingress Zone)（续） 入口区 (Ingress Zone)（续）																																
出口区 (Egress Zone) 出口区 (Egress Zone)（续） 出口区 (Egress Zone)（续） 出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface) 入口接口 (Ingress Interface)（续） 入口接口 (Ingress Interface)（续） 入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface) 出口接口 (Egress Interface)（续） 出口接口 (Egress Interface)（续）																																

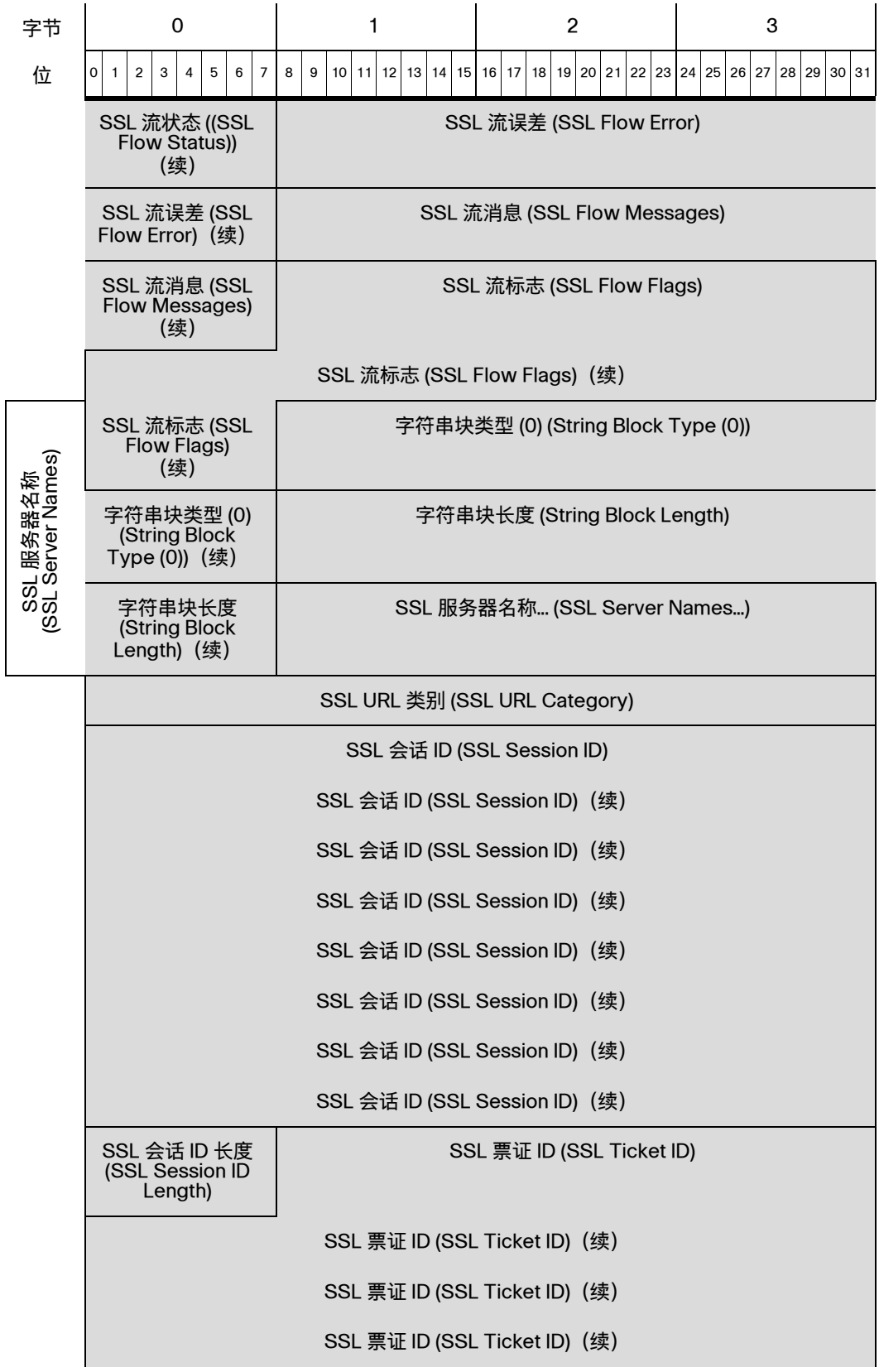

字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
出口接口 (Egress Interface)（续）
发起方 IP 地址 (Initiator IP Address)
发起方 IP 地址 (Initiator IP Address)（续）
发起方 IP 地址 (Initiator IP Address)（续）
发起方 IP 地址 (Initiator IP Address)（续）
响应方 IP 地址 (Responder IP Address)
响应方 IP 地址 (Responder IP Address)（续）
响应方 IP 地址 (Responder IP Address)（续）
响应方 IP 地址 (Responder IP Address)（续）
原始客户端 IP 地址 (Original Client IP Address)
原始客户端 IP 地址（续）
原始客户端 IP 地址（续）
原始客户端 IP 地址（续）
策略修订 (Policy Revision)
策略修订 (Policy Revision)（续）
策略修订 (Policy Revision)（续）
策略修订 (Policy Revision)（续）
规则 ID (Rule ID)
隧道规则 ID (Tunnel Rule ID)
规则操作 (Rule Action)
规则原因 (Rule Reason)
规则原因（续）
发起方端口 (Initiator Port)
响应方端口 (Responder Port)
TCP 标志 (TCP Flags)
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）

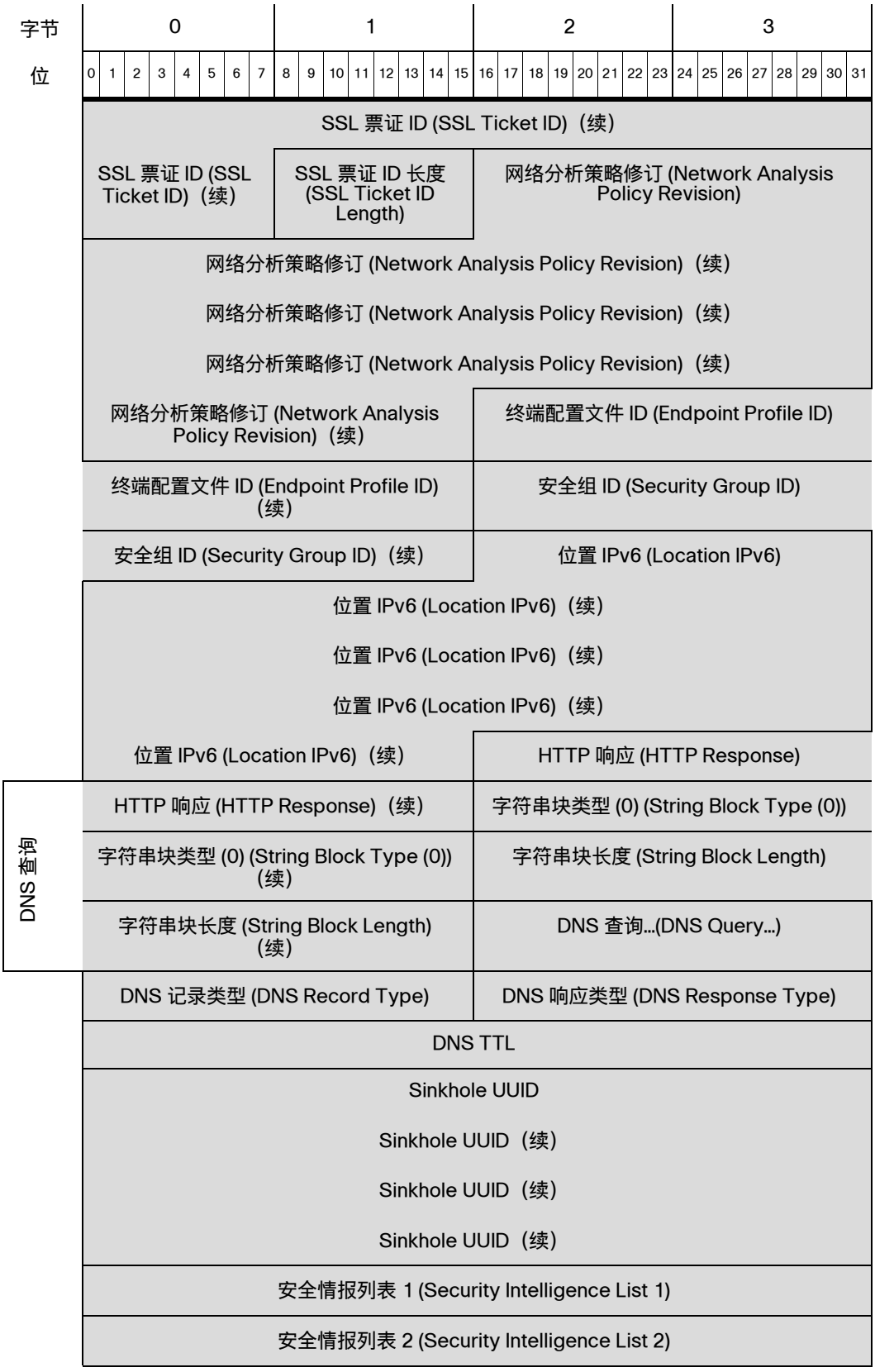
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetFlow 源（续）									实例 ID (Instance ID)																连接计数器 (Connection Counter)							
连接计数器 (Cx Ctr)（续）									第一个数据包时间戳 (First Packet Timestamp)																							
第一个数据包时间戳 (First Pkt Time)（续）									最后一个数据包时间戳 (Last Packet Timestamp)																							
最后一个数据包时间戳（续）									发起方传输的数据包数 (Initiator Transmitted Packets)																							
发起方传输的数据包数 (Initiator Transmitted Packets)（续）																																
发起方传输的数据包数（续）									响应方传输的数据包数 (Responder Transmitted Packets)																							
响应方传输的数据包数 (Responder Transmitted Packets)（续）																																
响应方传输的数据包数（续）									发起方传输的字节数 (Initiator Transmitted Bytes)																							
发起方传输的字节数 (Initiator Transmitted Bytes)（续）																																
发起方传输的字节数（续）									响应方传输的数据包数 (Responder Transmitted Packets)																							
响应方传输的字节数 (Responder Transmitted Bytes)（续）																																
响应方传输的字节数（续）									发起方丢弃的数据包数 (Initiator Packets Dropped)																							
发起方丢弃的数据包数 (Initiator Packets Dropped)（续）																																
发起方丢弃的数据包数（续）									响应方丢弃的数据包数 (Responder Packets Dropped) (Responder Packets Dropped)																							
响应方丢弃的数据包数 (Responder Packets Dropped)（续）																																
响应方丢弃的数据包数（续）									发起方丢弃的字节数 (Initiator Bytes Dropped) (Initiator Bytes Dropped)																							
发起方丢弃的字节数 (Initiator Bytes Dropped)（续）																																
发起方丢弃的字节数（续）									响应方丢弃的字节数 (Responder Bytes Dropped) (Responder Bytes Dropped)																							
响应方丢弃的字节数 (Responder Bytes Dropped)（续）																																
响应方丢弃的字节数（续）									QOS 应用的接口 (QOS Applied Interface)																							


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
QOS 应用的接口（续）
QOS 应用的接口（续）
QOS 应用的接口（续）
QOS 应用的接口 (续)
QOS 规则 ID (QOS Rule ID)
QOS 规则 ID (续)
用户 ID
用户 ID (User ID) (续)
应用协议 ID (Application Protocol ID)
应用协议ID (续)
URL 类别 (URL Category)
URL 类别 (URL Category)（续）
URL 信誉 (URL Reputation)
URL 信誉 (URL Reputation) (续)
客户端应用 ID (Client Application ID)
客户端应用 ID (Client App ID) (续)
Web 应用 ID (Web Application ID)
客户端 URL
Web 应用ID (Web App. ID) (续)
字符串块类型 (0) (Str. Block Type (0))
字符串块类型 (续)
字符串块长度 (String Block Length)
字符串块长度 (续)
客户端应用URL... (Client App. URL...)
NetBIOS 名称 (Name)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
NetBIOS 名称...(NetBIOS Name...)
客户端应用版本 (Client App Version)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
客户端应用版本...(Client Application Version...)

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
监控器规则 1 (Monitor Rule 1)																																
监控器规则 2 (Monitor Rule 2)																																
监控器规则 3 (Monitor Rule 3)																																
监控器规则 4 (Monitor Rule 4)																																
监控器规则 5 (Monitor Rule 5)																																
监控器规则 6 (Monitor Rule 6)																																
监控器规则 7 (Monitor Rule 7)																																
监控器规则 8 (Monitor Rule 8)																																
安全接口源/目标 (Sec. Int. Src/Dst)									安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
入侵事件计数 (Intrusion Event Count)																	发起方国家/地区 (Initiator Country)														
响应方国家/地区 (Responder Country)																	原始客户端国家/地区 (Original Client Country)														
IOC 编号 (IOC Number)																	源自治系统 (Source Autonomous System)														
源自治系统 (Source Autonomous System)（续）																	目标自治系统 (Destination Autonomous System)														
目标自治系统 (Destination Autonomous System)																	SNMP 输入 (SNMP In)														
SNMP 输出 (SNMP Out)																	源 TOS (Source TOS)								目标 TOS (Destination TOS)						
源掩码 (Source Mask)									目标掩码 (Destination Mask)								安全情景 (Security Context)														
安全情景 (Security Context)																																
安全情景 (Security Context)（续）																																
安全情景 (Security Context)（续）																																
安全情景 (Security Context)（续）																									VLAN ID							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
引用的主机 (Referenced Host)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	引用的主机 (Referenced Host)...(Referenced Host...)																															
用户代理	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户代理... (User Agent...)																															
HTTP 引用站点 (HTTP Referrer)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	HTTP 引用站点...(HTTP Referrer...)																															
	SSL 证书指纹 (SSL Certificate Fingerprint)																															
	SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															
	SSL 策略 ID (SSL Policy ID)																															
	SSL 策略 ID (SSL Policy ID)（续）																															
	SSL 策略 ID (SSL Policy ID)（续）																															
	SSL 策略 ID (SSL Policy ID)（续）																															
	SSL 规则 ID (SSL Rule ID)																															
	SSL 密码套件 (SSL Cipher Suite)																SSL 版本 (SSL Version)								SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)							
	SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)（续）																								SSL 实际操作 (SSL Actual Action)							
	SSL 实际操作 (SSL Actual Action)（续）								SSL 预期操作 (SSL Expected Action)																SSL 流状态 (SSL Flow Status)							


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 流状态 ((SSL Flow Status)) (续)
SSL 流误差 (SSL Flow Error)
SSL 流误差 (SSL Flow Error) (续)
SSL 流消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Messages) (续)
SSL 流标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags) (续)
SSL 服务器名称 (SSL Server Names)
SSL 流标志 (SSL Flow Flags) (续)
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) (续)
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) (续)
SSL 服务器名称... (SSL Server Names...)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID 长度 (SSL Session ID Length)
SSL 票证 ID (SSL Ticket ID)
SSL 票证 ID (SSL Ticket ID) (续)
SSL 票证 ID (SSL Ticket ID) (续)
SSL 票证 ID (SSL Ticket ID) (续)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID 长度 (SSL Ticket ID Length)
网络分析策略修订 (Network Analysis Policy Revision)
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
终端配置文件 ID (Endpoint Profile ID)
终端配置文件 ID (Endpoint Profile ID)（续）
安全组 ID (Security Group ID)
安全组 ID (Security Group ID)（续）
位置 IPv6 (Location IPv6)
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
HTTP 响应 (HTTP Response)
DNS 查询
HTTP 响应 (HTTP Response)（续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
DNS 查询...(DNS Query...)
DNS 记录类型 (DNS Record Type)
DNS 响应类型 (DNS Response Type)
DNS TTL
Sinkhole UUID
Sinkhole UUID（续）
Sinkhole UUID（续）
Sinkhole UUID（续）
安全情报列表 1 (Security Intelligence List 1)
安全情报列表 2 (Security Intelligence List 2)

下表对用于 6.1.x 的连接统计信息数据块的字段进行了说明。

表 B-44 连接统计信息数据块 6.1+ 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 6.1.x 的连接统计信息数据块。值始终为 163。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
原始客户端 IP 地址 (Original Client IP Address)	uint8[16]	位于发起请求的代理后面的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
隧道规则 ID (Tunnel Rule ID)	uint32	触发事件的隧道规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint32	规则触发事件的原因。

表 B-44　　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明 (Description)
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
发起方丢弃的数据包数 (Initiator Packets Dropped)	uint64	由于速率限制而从会话发起方丢弃的数据包的数量。

表 B-44 连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明 (Description)
响应方丢弃的数据包数 (Responder Packets Dropped)	uint64	由于速率限制而从会话响应方丢弃的数据包的数量。
发起方丢弃的字节数 (Initiator Bytes Dropped)	uint64	由于速率限制而从会话发起方丢弃的字节的数量。
响应方丢弃的字节数 (Responder Bytes Dropped)	uint64	由于速率限制而从会话响应方丢弃的字节的数量。
QOS 应用的接口	uint8[16]	对于速率受限的连接，是指应用了速率限制的接口的名称。
QOS 规则 ID (QOS Rule ID)	uint32	应用于连接的服务质量规则的内部 ID 号码（如适用）。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如 `/files/index.html`）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。

表 B-44　　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。

表 B-44 连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明 (Description)
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家/地区 (Initiator Country)	uint16	发起主机的国家/地区代码。
响应方国家/地区 (Responder Country)	uint 16	响应主机的国家/地区代码。
原始客户端国家/地区 (Original Client Country)	uint 16	位于发起请求的代理后面的主机的国家/地区的代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。

表 B-44　　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“引用的主机”(Referenced Host) 字段中的字节数。
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户代理”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“HTTP 引用站点”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在 HTTP 流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。

表 B-44 连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 证书的状态。可能的值包括: ▪ 0 - 未检查 - 服务器证书状态未评估。 ▪ 1 - 未知 - 服务器证书状态无法确定。 ▪ 2 - 有效 - 服务器证书有效。 ▪ 4 - 自签 - 服务器证书已自签。 ▪ 16 - 颁发者无效 - 服务器证书的颁发者无效。 ▪ 32 - 签名无效 - 服务器证书的签名无效。 ▪ 64 - 过期 - 服务器证书已过期。 ▪ 128 - 尚未生效 - 服务器证书尚未生效。 ▪ 256 - 撤销 - 服务器证书已被撤销。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-44　　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 B-44 连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明 (Description)
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 ▪ 0x00000001 - NSE_MT__HELLO_REQUEST ▪ 0x00000002 - NSE_MT__CLIENT_ALERT ▪ 0x00000004 - NSE_MT__SERVER_ALERT ▪ 0x00000008 - NSE_MT__CLIENT_HELLO ▪ 0x00000010 - NSE_MT__SERVER_HELLO ▪ 0x00000020 - NSE_MT__SERVER_CERTIFICATE ▪ 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE ▪ 0x00000080 - NSE_MT__CERTIFICATE_REQUEST ▪ 0x00000100 - NSE_MT__SERVER_HELLO_DONE ▪ 0x00000200 - NSE_MT__CLIENT_CERTIFICATE ▪ 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE ▪ 0x00000800 - NSE_MT__CERTIFICATE_VERIFY ▪ 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC ▪ 0x00002000 - NSE_MT__CLIENT_FINISHED ▪ 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC ▪ 0x00008000 - NSE_MT__SERVER_FINISHED ▪ 0x00010000 - NSE_MT__NEW_SESSION_TICKET ▪ 0x00020000 - NSE_MT__HANDSHAKE_OTHER ▪ 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT ▪ 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括: ▪ 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 ▪ 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 ▪ 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“SSL 服务器名称”(SSL Server Name) 字段中的字节数。
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。

表 B-44　　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明 (Description)
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时，SSL 握手期间使用的会话 ID 值
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy Revision)	uint8[16]	与连接事件相关的网络分析策略的修订。
终端配置文件 ID (Endpoint Profile ID)	uint32	ISE 识别的连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	由 ISE 根据策略分配给用户的 ID 号码。
位置 IPv6 (Location IPv6)	uint8[16]	与 ISE 通信的接口的 IP 地址。可以是 IPv4 或 IPv6。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。
字符串块类型 (String Block Type)	uint32	启动 DNS 查询的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 DNS 查询字符串中的字节数。
DNS 查询 (DNS Query)	字符串	发送到 DNS 服务器的查询的内容。
DNS 记录类型 (DNS Record	uint16	DNS 记录类型的数字值。
DNS 响应类型 (DNS Response Type)	uint16	DNS 响应类型的数字值。
DNS TTL	uint32	DNS 响应的生存时间（秒数）

表 B-44　　连接统计信息数据块 6.1+ 字段 （续）

字段	数据类型	说明 (Description)
Sinkhole UUID	uin8[16]	与此 sinkhole 对象关联的修订 UUID。
安全情报列表 1 (Security Intelligence List 1)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能存在两个与连接关联的安全情报列表。
安全情报列表 2 (Security Intelligence List 2)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能存在两个与连接关联的安全情报列表。

连接统计信息数据块 6.2-6.7.x

连接统计信息数据块在连接数据消息中使用。用于 6.2-6.7.x 的连接统计信息数据块中添加了第三个安全情报字段。用于版本 6.2-6.7.x 的连接统计信息数据块的块类型为系列 1 数据块组中的 168。它替代块类型 163，连接统计信息数据块 6.1.x，第 B-254 页。它被块类型 173 替代。

您可以通过在事件版本为 15 且事件代码为 71 的请求消息中设置扩展事件标志（“请求标志”(Request Flags) 字段中的位 30）请求连接事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

下图显示用于 6.2-6.7.x 的连接统计信息数据块的格式:

7

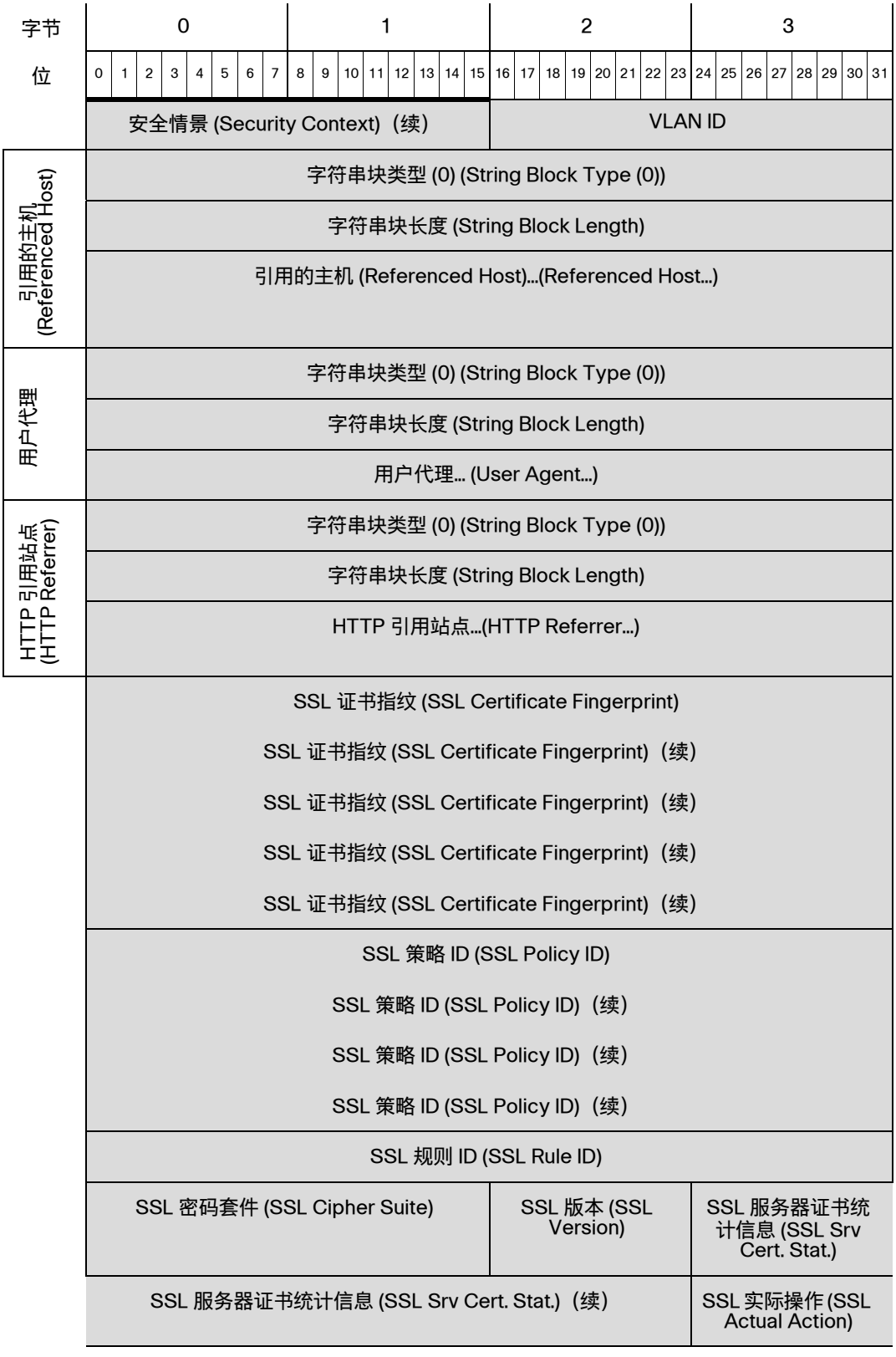
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接统计信息数据块类型 (168) (Connection Statistics Data Block Type (168))																																
连接统计信息数据块长度 (Connection Statistics Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone)																																
入口区 (Ingress Zone) （续）																																
入口区 (Ingress Zone) （续）																																
入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone)																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																
出口区 (Egress Zone) （续）																																

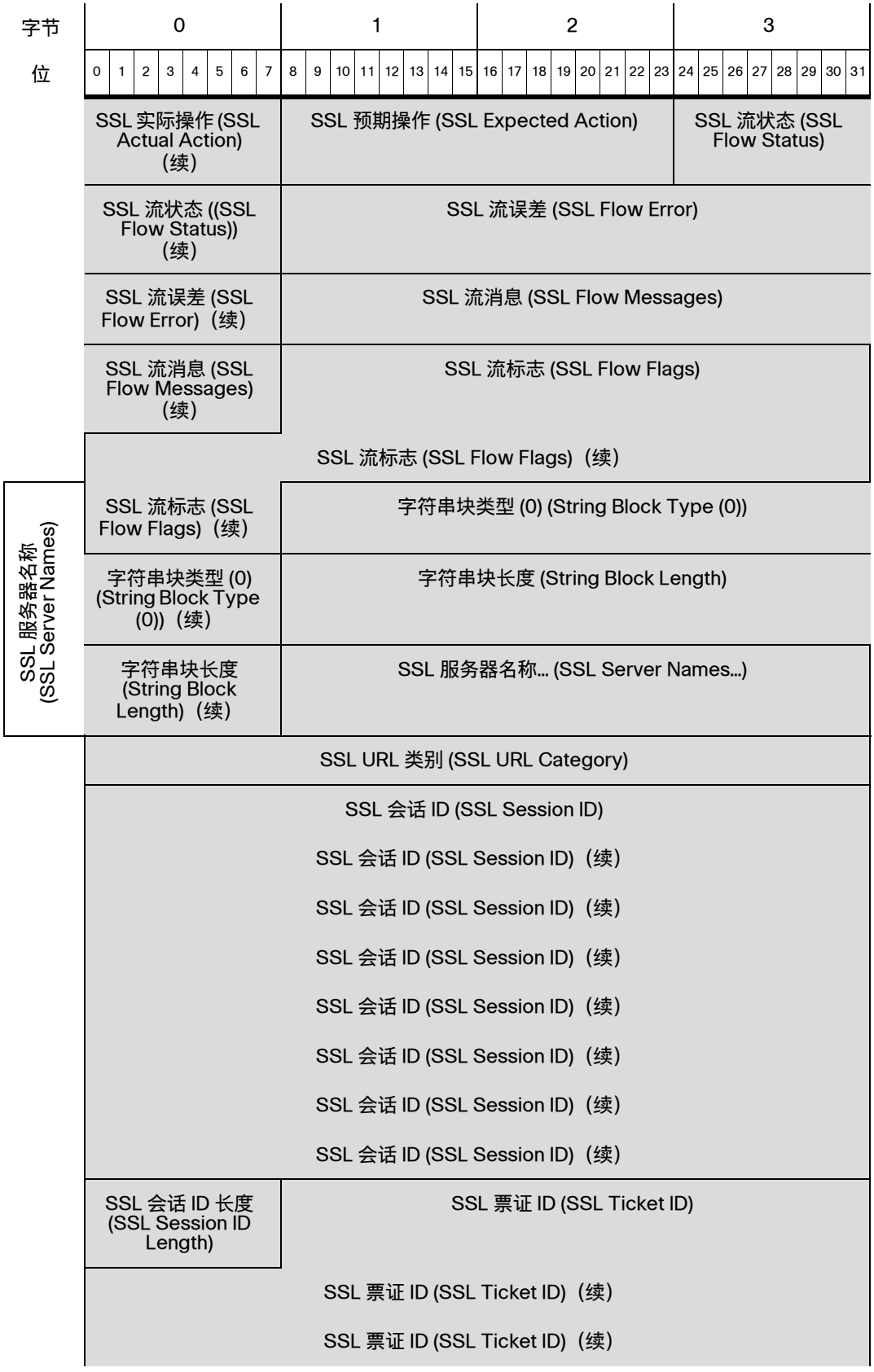
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
原始客户端 IP 地址 (Original Client IP Address)																																
原始客户端 IP 地址（续）																																
原始客户端 IP 地址（续）																																
原始客户端 IP 地址（续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																
规则 ID (Rule ID)																																
隧道规则 ID (Tunnel Rule ID)																																

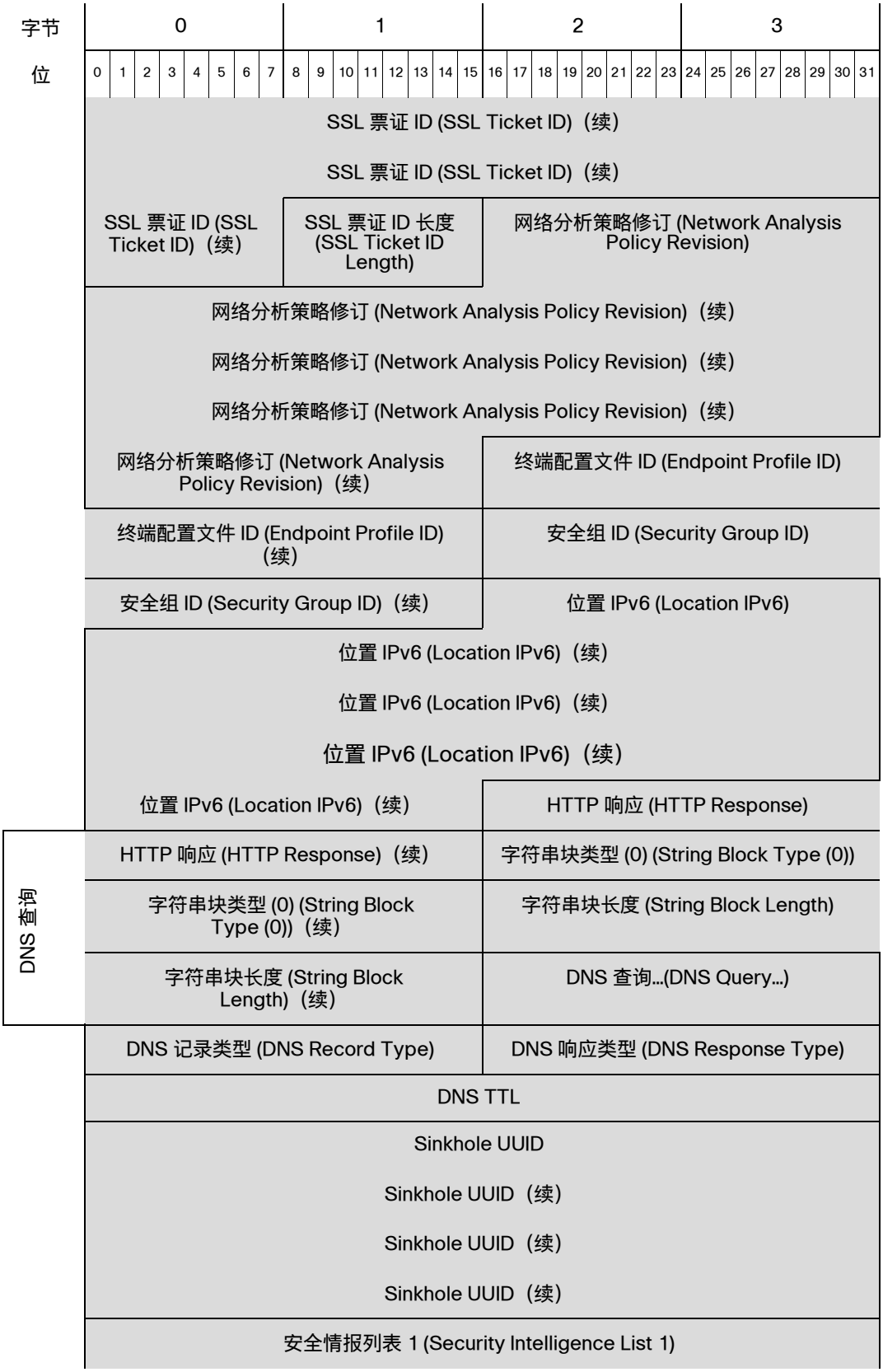
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	规则操作 (Rule Action)																规则原因 (Rule Reason)															
	规则原因（续）																发起方端口 (Initiator Port)															
	响应方端口 (Responder Port)																TCP 标志 (TCP Flags)															
	协议 (Protocol)								NetFlow 源 (NetFlow Source)																							
	Netflow 源 (Netflow Source)（续）																															
	Netflow 源 (Netflow Source)（续）																															
	Netflow 源 (Netflow Source)（续）																															
	NetFlow 源（续）								实例 ID (Instance ID)																连接计数器 (Connection Counter)							
	连接计数器 (Cx Ctr)（续）								第一个数据包时间戳 (First Packet Timestamp)																							
	第一个数据包时间戳 (First Pkt Time)（续）								最后一个数据包时间戳 (Last Packet Timestamp)																							
	最后一个数据包时间戳（续）								发起方传输的数据包数 (Initiator Transmitted Packets)																							
	发起方传输的数据包数 (Initiator Transmitted Packets)（续）																															
	发起方传输的数据包数（续）								响应方传输的数据包数 (Responder Transmitted Packets)																							
	响应方传输的数据包数 (Responder Transmitted Packets)（续）																															
	响应方传输的数据包数（续）								发起方传输的字节数 (Initiator Transmitted Bytes)																							
	发起方传输的字节数 (Initiator Transmitted Bytes)（续）																															
	发起方传输的字节数（续）								响应方传输的数据包数 (Responder Transmitted Packets)																							
	响应方传输的字节数 (Responder Transmitted Bytes)（续）																															
	响应方传输的字节数（续）								发起方丢弃的数据包数 (Initiator Packets Dropped)																							
	发起方丢弃的数据包数 (Initiator Packets Dropped)（续）																															
	发起方丢弃的数据包数（续）								响应方丢弃的数据包数 (Responder Packets Dropped) (Responder Packets Dropped)																							
	响应方丢弃的数据包数 (Responder Packets Dropped)（续）																															

	字节	0								1								2								3							
	位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		响应方丢弃的数据包数（续）								发起方丢弃的字节数 (Initiator Bytes Dropped) (Initiator Bytes Dropped)																							
		发起方丢弃的字节数 (Initiator Bytes Dropped)（续）																															
		发起方丢弃的字节数（续）								响应方丢弃的字节数 (Responder Bytes Dropped) (Responder Bytes Dropped)																							
		响应方丢弃的字节数 (Responder Bytes Dropped)（续）																															
		响应方丢弃的字节数（续）								QOS 应用的接口 (QOS Applied Interface)																							
		QOS 应用的接口（续）																															
		QOS 应用的接口（续）																															
		QOS 应用的接口（续）																															
		QOS 应用的接口（续）								QOS 规则 ID (QOS Rule ID)																							
		QOS 规则 ID（续）								用户 ID																							
		用户 ID (User ID)（续）								应用协议 ID (Application Protocol ID)																							
		应用协议ID（续）								URL 类别 (URL Category)																							
		URL 类别 (URL Category)（续）								URL 信誉 (URL Reputation)																							
		URL 信誉 (URL Reputation)（续）								客户端应用 ID (Client Application ID)																							
		客户端应用 ID (Client App ID)（续）								Web 应用 ID (Web Application ID)																							
客户端 URL		Web 应用ID (Web App. ID)（续）								字符串块类型 (0) (Str. Block Type (0))																							
客户端 URL		字符串块类型（续）								字符串块长度 (String Block Length)																							
客户端 URL		字符串块长度（续）								客户端应用URL... (Client App. URL...)																							
NetBIOS 名称 (Name)		字符串块类型 (0) (String Block Type (0))																															
NetBIOS 名称 (Name)		字符串块长度 (String Block Length)																															
NetBIOS 名称 (Name)		NetBIOS 名称...(NetBIOS Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源/目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																发起方国家/地区 (Initiator Country)															
	响应方国家/地区 (Responder Country)																原始客户端国家/地区 (Original Client Country)															
	IOC 编号 (IOC Number)																源自治系统 (Source Autonomous System)															
	源自治系统 (Source Autonomous System)（续）																目标自治系统 (Destination Autonomous System)															
	目标自治系统 (Destination Autonomous System)																SNMP 输入 (SNMP In)															
	SNMP 输出 (SNMP Out)																源 TOS (Source TOS)								目标 TOS (Destination TOS)							
	源掩码 (Source Mask)								目标掩码 (Destination Mask)								安全情景 (Security Context)															
	安全情景 (Security Context)																															
	安全情景 (Security Context)（续）																															
	安全情景 (Security Context)（续）																															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
安全情景 (Security Context)（续）
VLAN ID
引用的主机 (Referenced Host)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
引用的主机 (Referenced Host)...(Referenced Host...)
用户代理
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
用户代理... (User Agent...)
HTTP 引用站点 (HTTP Referrer)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
HTTP 引用站点...(HTTP Referrer...)
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 策略 ID (SSL Policy ID)
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）
SSL 规则 ID (SSL Rule ID)
SSL 密码套件 (SSL Cipher Suite)
SSL 版本 (SSL Version)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)（续）
SSL 实际操作 (SSL Actual Action)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 实际操作 (SSL Actual Action) (续)
SSL 预期操作 (SSL Expected Action)
SSL 流状态 (SSL Flow Status)
SSL 流状态 ((SSL Flow Status)) (续)
SSL 流误差 (SSL Flow Error)
SSL 流误差 (SSL Flow Error) (续)
SSL 流消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Messages) (续)
SSL 流标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags) (续)
SSL 服务器名称 (SSL Server Names)
SSL 流标志 (SSL Flow Flags) (续)
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) (续)
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) (续)
SSL 服务器名称... (SSL Server Names...)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID (SSL Session ID) (续)
SSL 会话 ID 长度 (SSL Session ID Length)
SSL 票证 ID (SSL Ticket ID)
SSL 票证 ID (SSL Ticket ID) (续)
SSL 票证 ID (SSL Ticket ID) (续)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID 长度 (SSL Ticket ID Length)
网络分析策略修订 (Network Analysis Policy Revision)
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
终端配置文件 ID (Endpoint Profile ID)
终端配置文件 ID (Endpoint Profile ID)（续）
安全组 ID (Security Group ID)
安全组 ID (Security Group ID)（续）
位置 IPv6 (Location IPv6)
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
HTTP 响应 (HTTP Response)
DNS 查询
HTTP 响应 (HTTP Response)（续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
DNS 查询...(DNS Query...)
DNS 记录类型 (DNS Record Type)
DNS 响应类型 (DNS Response Type)
DNS TTL
Sinkhole UUID
Sinkhole UUID（续）
Sinkhole UUID（续）
Sinkhole UUID（续）
安全情报列表 1 (Security Intelligence List 1)

下表对用于 6.2-6.7.x 的连接统计信息数据块的字段进行了说明。

表 B-45 连接统计信息数据块 6.2-6.7.x 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 6.2-6.7.x. 的连接统计信息数据块值始终为 168。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
原始客户端 IP 地址 (Original Client IP Address)	uint8[16]	位于发起请求的代理后面的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。

表 B-45　　连接统计信息数据块 6.2-6.7.x 字段 （续）

字段	数据类型	说明 (Description)
隧道规则 ID (Tunnel Rule ID)	uint32	触发事件的隧道规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint32	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。

表 B-45 连接统计信息数据块 6.2-6.7.x 字段 （续）

字段	数据类型	说明 (Description)
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
发起方丢弃的数据包数 (Initiator Packets Dropped)	uint64	由于速率限制而从会话发起方丢弃的数据包的数量。
响应方丢弃的数据包数 (Responder Packets Dropped)	uint64	由于速率限制而从会话响应方丢弃的数据包的数量。
发起方丢弃的字节数 (Initiator Bytes Dropped)	uint64	由于速率限制而从会话发起方丢弃的字节的数量。
响应方丢弃的字节数 (Responder Bytes Dropped)	uint64	由于速率限制而从会话响应方丢弃的字节的数量。
QOS 应用的接口	uint8[16]	对于速率受限的连接，是指应用了速率限制的接口的名称。
QOS 规则 ID (QOS Rule ID)	uint32	应用于连接的服务质量规则的内部 ID 号码（如适用）。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用 ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。

表 B-45　　连接统计信息数据块 6.2-6.7.x 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的URL（如适用）（例如/files/index.html）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。

表 B-45 连接统计信息数据块 6.2-6.7.x 字段 （续）

字段	数据类型	说明 (Description)
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家/地区 (Initiator Country)	uint16	发起主机的国家/地区代码。
响应方国家/地区 (Responder Country)	uint 16	响应主机的国家/地区代码。
原始客户端国家/地区 (Original Client Country)	uint 16	位于发起请求的代理后面的主机的国家/地区的代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。

表 B-45　　连接统计信息数据块 6.2-6.7.x 字段 （续）

字段	数据类型	说明 (Description)
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“引用的主机”(Referenced Host) 字段中的字节数。
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户代理”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“HTTP 引用站点”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在 HTTP 流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。

表 B-45 连接统计信息数据块 6.2-6.7.x 字段 （续）

字段	数据类型	说明 (Description)
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 证书的状态。可能的值包括: ▪ 0 - 未检查 - 服务器证书状态未评估。 ▪ 1 - 未知 - 服务器证书状态无法确定。 ▪ 2 - 有效 - 服务器证书有效。 ▪ 4 - 自签 - 服务器证书已自签。 ▪ 16 - 颁发者无效 - 服务器证书的颁发者无效。 ▪ 32 - 签名无效 - 服务器证书的签名无效。 ▪ 64 - 过期 - 服务器证书已过期。 ▪ 128 - 尚未生效 - 服务器证书尚未生效。 ▪ 256 - 撤销 - 服务器证书已被撤销。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-45　　连接统计信息数据块 6.2-6.7.x 字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 B-45 连接统计信息数据块 6.2-6.7.x 字段 （续）

字段	数据类型	说明 (Description)
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 ▪ 0x00000001 - NSE_MT__HELLO_REQUEST ▪ 0x00000002 - NSE_MT__CLIENT_ALERT ▪ 0x00000004 - NSE_MT__SERVER_ALERT ▪ 0x00000008 - NSE_MT__CLIENT_HELLO ▪ 0x00000010 - NSE_MT__SERVER_HELLO ▪ 0x00000020 - NSE_MT__SERVER_CERTIFICATE ▪ 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE ▪ 0x00000080 - NSE_MT__CERTIFICATE_REQUEST ▪ 0x00000100 - NSE_MT__SERVER_HELLO_DONE ▪ 0x00000200 - NSE_MT__CLIENT_CERTIFICATE ▪ 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE ▪ 0x00000800 - NSE_MT__CERTIFICATE_VERIFY ▪ 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC ▪ 0x00002000 - NSE_MT__CLIENT_FINISHED ▪ 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC ▪ 0x00008000 - NSE_MT__SERVER_FINISHED ▪ 0x00010000 - NSE_MT__NEW_SESSION_TICKET ▪ 0x00020000 - NSE_MT__HANDSHAKE_OTHER ▪ 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT ▪ 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括: ▪ 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 ▪ 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 ▪ 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“SSL 服务器名称”(SSL Server Name) 字段中的字节数。
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。

表 B-45　　连接统计信息数据块 6.2-6.7.x 字段 （续）

字段	数据类型	说明 (Description)
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时，SSL 握手期间使用的会话 ID 值
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy Revision)	uint8[16]	与连接事件相关的网络分析策略的修订。
终端配置文件 ID (Endpoint Profile ID)	uint32	ISE 识别的连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	由 ISE 根据策略分配给用户的 ID 号码。
位置 IPv6 (Location IPv6)	uint8[16]	与 ISE 通信的接口的 IP 地址。可以是 IPv4 或 IPv6。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。
字符串块类型 (String Block Type)	uint32	启动 DNS 查询的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 DNS 查询字符串中的字节数。
DNS 查询 (DNS Query)	字符串	发送到 DNS 服务器的查询的内容。
DNS 记录类型 (DNS Record	uint16	DNS 记录类型的数字值。
DNS 响应类型 (DNS Response Type)	uint16	DNS 响应类型的数字值。
DNS TTL	uint32	DNS 响应的生存时间（秒数）

表 B-45　　连接统计信息数据块 6.2-6.7.x 字段 （续）

字段	数据类型	说明 (Description)
Sinkhole UUID	uin8[16]	与此 sinkhole 对象关联的修订 UUID。
安全情报列表 1 (Security Intelligence List 1)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能有三个与连接关联的安全情报列表。
安全情报列表 2 (Security Intelligence List 2)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能有三个与连接关联的安全情报列表。
安全情报列表 3 (Security Intelligence List 3)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能有三个与连接关联的安全情报列表。

连接统计信息数据块 7.0

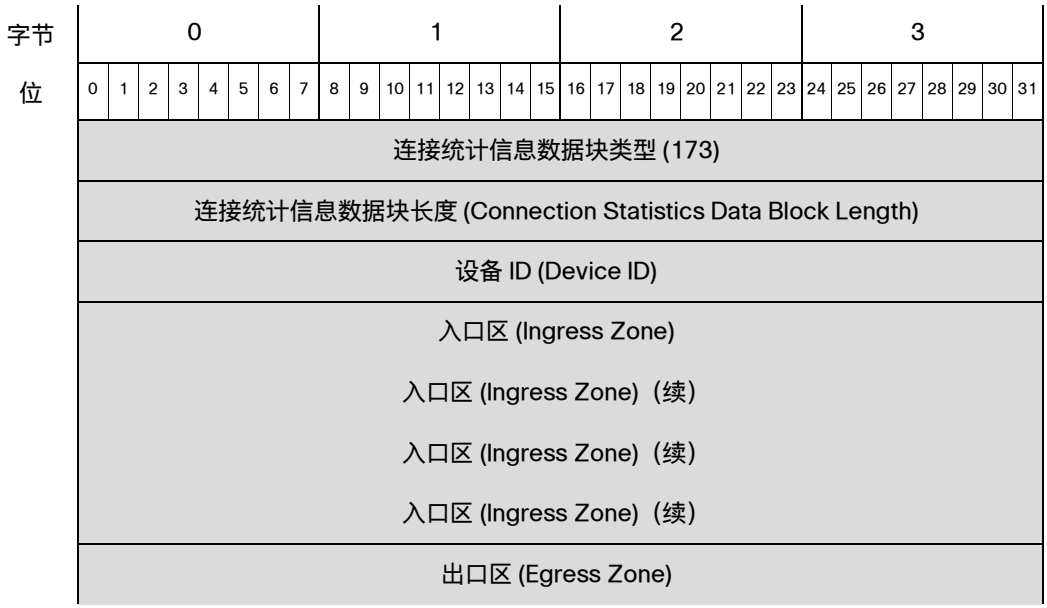
连接统计信息数据块在连接数据消息中使用。“安全组标记”(Security Group Tag)、“虚拟路由和转发”(virtual routing and forwarding) 以及“动态属性”(dynamic attribute) 字段已添加到“7.0+ 的连接统计信息据块”中。用于版本 7.0+ 的连接统计信息数据块的块类型为系列 1 数据块组中的 173。它替代块类型 168，连接统计信息数据块 6.2-6.7.x，第 B-272 页。它被块类型 174 替代

您可以通过在事件版本为 16 且事件代码为 71 的请求消息中设置扩展事件标志（“请求标志”(Request Flags) 字段中的位 30）请求连接事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-51 页。

下图显示用于 7.0 的连接统计信息数据块的格式:

7



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
出口区 (Egress Zone)（续）																																
入口接口 (Ingress Interface)																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
入口接口 (Ingress Interface)（续）																																
出口接口 (Egress Interface)																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
出口接口 (Egress Interface)（续）																																
发起方 IP 地址 (Initiator IP Address)																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
发起方 IP 地址 (Initiator IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
响应方 IP 地址 (Responder IP Address)（续）																																
原始客户端 IP 地址 (Original Client IP Address)																																
原始客户端 IP 地址（续）																																
原始客户端 IP 地址（续）																																
原始客户端 IP 地址（续）																																
策略修订 (Policy Revision)																																
策略修订 (Policy Revision)（续）																																
策略修订 (Policy Revision)（续）																																


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
策略修订 (Policy Revision)（续）
规则 ID (Rule ID)
隧道规则 ID (Tunnel Rule ID)
规则操作 (Rule Action)
规则原因 (Rule Reason)
规则原因（续）
发起方端口 (Initiator Port)
响应方端口 (Responder Port)
TCP 标志 (TCP Flags)
协议 (Protocol)
NetFlow 源 (NetFlow Source)
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
Netflow 源 (Netflow Source)（续）
NetFlow 源（续）
实例 ID (Instance ID)
连接计数器 (Connection Counter)
连接计数器 (Cx Ctr)（续）
第一个数据包时间戳 (First Packet Timestamp)
第一个数据包时间戳 (First Pkt Time)（续）
最后一个数据包时间戳 (Last Packet Timestamp)
最后一个数据包时间戳（续）
发起方传输的数据包数 (Initiator Transmitted Packets)
发起方传输的数据包数 (Initiator Transmitted Packets)（续）
发起方传输的数据包数（续）
响应方传输的数据包数 (Responder Transmitted Packets)
响应方传输的数据包数 (Responder Transmitted Packets)（续）
响应方传输的数据包数（续）
发起方传输的字节数 (Initiator Transmitted Bytes)
发起方传输的字节数 (Initiator Transmitted Bytes)（续）
发起方传输的字节数（续）
响应方传输的数据包数 (Responder Transmitted Packets)
响应方传输的字节数 (Responder Transmitted Bytes)（续）
响应方传输的字节数（续）
发起方丢弃的数据包数 (Initiator Packets Dropped)

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	发起方丢弃的数据包数 (Initiator Packets Dropped)（续）																															
	发起方丢弃的数据包数（续）								响应方丢弃的数据包数 (Responder Packets Dropped) (Responder Packets Dropped)																							
	响应方丢弃的数据包数 (Responder Packets Dropped)（续）																															
	响应方丢弃的数据包数（续）								发起方丢弃的字节数 (Initiator Bytes Dropped) (Initiator Bytes Dropped)																							
	发起方丢弃的字节数 (Initiator Bytes Dropped)（续）																															
	发起方丢弃的字节数（续）								响应方丢弃的字节数 (Responder Bytes Dropped) (Responder Bytes Dropped)																							
	响应方丢弃的字节数 (Responder Bytes Dropped)（续）																															
	响应方丢弃的字节数（续）								QOS 应用的接口 (QOS Applied Interface)																							
	QOS 应用的接口（续）																															
	QOS 应用的接口（续）																															
	QOS 应用的接口（续）																															
	QOS 应用的接口（续）								QOS 规则 ID (QOS Rule ID)																							
	QOS 规则 ID（续）								用户 ID																							
	用户 ID (User ID)（续）								应用协议 ID (Application Protocol ID)																							
	应用协议ID（续）								URL 类别 (URL Category)																							
	URL 类别 (URL Category)（续）								URL 信誉 (URL Reputation)																							
	URL 信誉 (URL Reputation)（续）								客户端应用 ID (Client Application ID)																							
	客户端应用 ID (Client App ID)（续）								Web 应用 ID (Web Application ID)																							
客户端URL	Web 应用ID (Web App. ID)（续）								字符串块类型 (0) (Str. Block Type (0))																							
	字符串块类型（续）								字符串块长度 (String Block Length)																							
	字符串块长度（续）								客户端应用URL... (Client App. URL...)																							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称...(NetBIOS Name...)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源/目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															
	入侵事件计数 (Intrusion Event Count)																发起方国家/地区 (Initiator Country)															
	响应方国家/地区 (Responder Country)																原始客户端国家/地区 (Original Client Country)															
	IOC 编号 (IOC Number)																源自治系统 (Source Autonomous System)															
	源自治系统 (Source Autonomous System) (续)																目标自治系统 (Destination Autonomous System)															
	目标自治系统 (Destination Autonomous System)																SNMP 输入 (SNMP In)															


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SNMP 输出 (SNMP Out)
源 TOS (Source TOS)
目标 TOS (Destination TOS)
源掩码 (Source Mask)
目标掩码 (Destination Mask)
安全情景 (Security Context)
安全情景 (Security Context)
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
VLAN ID
引用的主机 (Referenced Host)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
引用的主机 (Referenced Host)...(Referenced Host...)
用户代理
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
用户代理... (User Agent...)
HTTP 引用站点 (HTTP Referrer)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
HTTP 引用站点...(HTTP Referrer...)
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 策略 ID (SSL Policy ID)
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）
SSL 策略 ID (SSL Policy ID)（续）

字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 规则 ID (SSL Rule ID)
SSL 密码套件 (SSL Cipher Suite)
SSL 版本 (SSL Version)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)
SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)（续）
SSL 实际操作 (SSL Actual Action)
SSL 实际操作 (SSL Actual Action)（续）
SSL 预期操作 (SSL Expected Action)
SSL 流状态 (SSL Flow Status)
SSL 流状态 ((SSL Flow Status))（续）
SSL 流误差 (SSL Flow Error)
SSL 流误差 (SSL Flow Error)（续）
SSL 流消息 (SSL Flow Messages)
SSL 流消息 (SSL Flow Messages)（续）
SSL 流标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags)（续）
SSL 服务器名称 (SSL Server Names)
SSL 流标志 (SSL Flow Flags)（续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
SSL 服务器名称... (SSL Server Names...)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID (SSL Session ID)（续）


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 会话 ID (SSL Session ID)（续）
SSL 会话 ID 长度 (SSL Session ID Length)
SSL 票证 ID (SSL Ticket ID)
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID (SSL Ticket ID)（续）
SSL 票证 ID 长度 (SSL Ticket ID Length)
网络分析策略修订 (Network Analysis Policy Revision)
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
网络分析策略修订 (Network Analysis Policy Revision)（续）
终端配置文件 ID (Endpoint Profile ID)
终端配置文件 ID (Endpoint Profile ID)（续）
安全组 ID (Security Group ID)
安全组 ID (Security Group ID)（续）
源安全组标签
源秒组标记类型
目的安全组标签
目标秒组标记类型
位置 IPv6 (Location IPv6)
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
位置 IPv6 (Location IPv6)（续）
HTTP 响应 (HTTP Response)
DNS 查询
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
DNS 查询...(DNS Query...)
DNS 记录类型 (DNS Record Type)
DNS 响应类型 (DNS Response Type)

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	DNS TTL																															
	Sinkhole UUID Sinkhole UUID（续） Sinkhole UUID（续） Sinkhole UUID（续）																															
	安全情报列表 1 (Security Intelligence List 1)																															
	安全情报列表 2 (Security Intelligence List 2)																															
	威胁智能类别																															
入口 VRF	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	入口 VRF 名称...																															
出口 VRF	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	出口 VRF 名称...																															
源属性	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	源 IP 动态属性																															
目标属性	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	目标 IP 动态属性...																															

下表对用于 7.0 的连接统计信息数据块的字段进行了说明。

表 B-46　　连接统计信息数据块 7.0 字段

字段	数据类型	说明 (Description)
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 7.0.+ 的连接统计信息数据块。值始终为 173。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
原始客户端 IP 地址 (Original Client IP Address)	uint8[16]	位于发起请求的代理后面的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号（如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符（如适用）。
隧道规则 ID (Tunnel Rule ID)	uint32	触发事件的隧道规则的内部标识符（如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作（允许、阻止等）。
规则原因 (Rule Reason)	uint32	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。

表 B-46 连接统计信息数据块 7.0 字段 （续）

字段	数据类型	说明 (Description)
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。
发起方丢弃的数据包数 (Initiator Packets Dropped)	uint64	由于速率限制而从会话发起方丢弃的数据包的数量。
响应方丢弃的数据包数 (Responder Packets Dropped)	uint64	由于速率限制而从会话响应方丢弃的数据包的数量。
发起方丢弃的字节数 (Initiator Bytes Dropped)	uint64	由于速率限制而从会话发起方丢弃的字节的数量。
响应方丢弃的字节数 (Responder Bytes Dropped)	uint64	由于速率限制而从会话响应方丢弃的字节的数量。
QOS 应用的接口	uint8[16]	对于速率受限的连接，是指应用了速率限制的接口的名称。

表 B-46　　连接统计信息数据块 7.0 字段 （续）

字段	数据类型	说明 (Description)
QOS 规则 ID (QOS Rule ID)	uint32	应用于连接的服务质量规则的内部 ID 号码（如适用）。
用户 ID	uint32	最后登录到生成流量的主机的用户的内部标识号。
应用协议 ID (Application Protocol ID)	uint32	应用协议的应用 ID。
URL 类别 (URL Category)	uint32	URL 类别的内部标别号。
URL 信誉 (URL Reputation)	uint32	URL 信誉的内部标识号。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号（如适用）。
Web 应用ID (Web Application ID)	uint32	被检测 Web 应用的内部标识号（如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用 URL 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用 URL 字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上客户端应用 URL 字符串中的字节数。
客户端应用 URL (Client Application URL)	字符串	客户端应用访问的 URL（如适用）（例如/files/index.html）。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上版本中的字节数。
客户端应用版本 (Client Application Version)	字符串	客户端应用版本。
监控器规则 1 (Monitor Rule 1)	uint32	与连接事件关联的第一个监控器规则的 ID。
监控器规则 2 (Monitor Rule 2)	uint32	与连接事件关联的第二个监控器规则的 ID。

表 B-46 连接统计信息数据块 7.0 字段 （续）

字段	数据类型	说明 (Description)
监控器规则 3 (Monitor Rule 3)	uint32	与连接事件关联的第三个监控器规则的 ID。
监控器规则 4 (Monitor Rule 4)	uint32	与连接事件关联的第四个监控器规则的 ID。
监控器规则 5 (Monitor Rule 5)	uint32	与连接事件关联的第五个监控器规则的 ID。
监控器规则 6 (Monitor Rule 6)	uint32	与连接事件关联的第六个监控器规则的 ID。
监控器规则 7 (Monitor Rule 7)	uint32	与连接事件关联的第七个监控器规则的 ID。
监控器规则 8 (Monitor Rule 8)	uint32	与连接事件关联的第八个监控器规则的 ID。
安全情报源/目标 (Security Intelligence Source/ Destination)	uint8	源或目标 IP 地址与 IP 阻止列表是否匹配。
安全情报层 (Security Intelligence Layer)	uint8	与 IP 阻止列表匹配的 IP 层。
文件事件计数 (File Event Count)	uint16	用于区别同一秒发生的文件事件的值。
入侵事件计数 (Intrusion Event Count)	uint16	用于区别同一秒发生的入侵事件的值。
发起方国家/地区 (Initiator Country)	uint16	发起主机的国家/地区代码。
响应方国家/地区 (Responder Country)	uint 16	响应主机的国家/地区代码。
原始客户端国家/地区 (Original Client Country)	uint 16	位于发起请求的代理后面的主机的国家/地区的代码。
IOC 编号 (IOC Number)	uint16	与此事件相关的危害的 ID 号码。
源自治系统 (Source Autonomous System)	uint32	作为源或对等体的源自治系统的编号。
目标自治系统 (Destination Autonomous System)	uint32	作为源或对等体的目标自治系统的编号。
SNMP 输入 (SNMP Input)	uint16	输入接口的 SNMP 索引。

表 B-46　连接统计信息数据块 7.0 字段 （续）

字段	数据类型	说明 (Description)
SNMP 输出 (SNMP Output)	uint16	输出接口的 SNMP 索引。
源 TOS (Source TOS)	uint8	传入接口的服务字节设置类型。
目标 TOS (Destination TOS)	uint8	传出接口的服务字节设置类型。
源掩码 (Source Mask)	uint8	源地址前缀掩码。
目标掩码 (Destination Mask)	uint8	目标地址前缀掩码。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
字符串块类型 (String Block Type)	uint32	启动包含引用的主机的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“引用的主机”(Referenced Host) 字段中的字节数。
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“用户代理”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“HTTP 引用站点”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在 HTTP 流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。

表 B-46 连接统计信息数据块 7.0 字段 （续）

字段	数据类型	说明 (Description)
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 证书的状态。可能的值包括： ▪ 0 - 未检查 - 服务器证书状态未评估。 ▪ 1 - 未知 - 服务器证书状态无法确定。 ▪ 2 - 有效 - 服务器证书有效。 ▪ 4 - 自签 - 服务器证书已自签。 ▪ 16 - 颁发者无效 - 服务器证书的颁发者无效。 ▪ 32 - 签名无效 - 服务器证书的签名无效。 ▪ 64 - 过期 - 服务器证书已过期。 ▪ 128 - 尚未生效 - 服务器证书尚未生效。 ▪ 256 - 撤销 - 服务器证书已被撤销。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括： ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-46　　连接统计信息数据块 7.0 字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
SSL 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 B-46 连接统计信息数据块 7.0 字段 （续）

字段	数据类型	说明 (Description)
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 ▪ 0x00000001 - NSE_MT__HELLO_REQUEST ▪ 0x00000002 - NSE_MT__CLIENT_ALERT ▪ 0x00000004 - NSE_MT__SERVER_ALERT ▪ 0x00000008 - NSE_MT__CLIENT_HELLO ▪ 0x00000010 - NSE_MT__SERVER_HELLO ▪ 0x00000020 - NSE_MT__SERVER_CERTIFICATE ▪ 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE ▪ 0x00000080 - NSE_MT__CERTIFICATE_REQUEST ▪ 0x00000100 - NSE_MT__SERVER_HELLO_DONE ▪ 0x00000200 - NSE_MT__CLIENT_CERTIFICATE ▪ 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE ▪ 0x00000800 - NSE_MT__CERTIFICATE_VERIFY ▪ 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC ▪ 0x00002000 - NSE_MT__CLIENT_FINISHED ▪ 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC ▪ 0x00008000 - NSE_MT__SERVER_FINISHED ▪ 0x00010000 - NSE_MT__NEW_SESSION_TICKET ▪ 0x00020000 - NSE_MT__HANDSHAKE_OTHER ▪ 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT ▪ 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括： ▪ 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 ▪ 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 ▪ 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“SSL 服务器名称”(SSL Server Name) 字段中的字节数。
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时，SSL 握手期间使用的会话 ID 值

表 B-46　　连接统计信息数据块 7.0 字段 （续）

字段	数据类型	说明 (Description)
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy Revision)	uint8[16]	与连接事件相关的网络分析策略的修订。
终端配置文件 ID (Endpoint Profile ID)	uint32	ISE 识别的连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	由 ISE 根据策略分配给用户的 ID 号码。
源安全组标签	uint16	连接源的安全组标记。
源安全组标记类型	uint8	如何分配源安全组标记: ▪ 0 — 未知 ▪ 1 — 内联 ▪ 2 — 会话目录 ▪ 3 — 安全组标记交换协议 (SXP)
目的安全组标签	uint16	连接目标的安全组标记。
目标安全组标记类型	uint8	如何分配目标安全组标记: ▪ 0 — 未知 ▪ 1 — 内联 ▪ 2 — 会话目录 ▪ 3 — 安全组标记交换协议 (SXP)
位置 IPv6 (Location IPv6)	uint8[16]	与 ISE 通信的接口的 IP 地址。可以是 IPv4 或 IPv6。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。
字符串块类型 (String Block Type)	uint32	启动 DNS 查询的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 DNS 查询字符串中的字节数。
DNS 查询 (DNS Query)	字符串	发送到 DNS 服务器的查询的内容。
DNS 记录类型 (DNS Record	uint16	DNS 记录类型的数字值。

表 B-46 连接统计信息数据块 7.0 字段 （续）

字段	数据类型	说明 (Description)
DNS 响应类型 (DNS Response Type)	uint16	DNS 响应类型的数字值。
DNS TTL	uint32	DNS 响应的生存时间（秒数）
Sinkhole UUID	uin8[16]	与此 sinkhole 对象关联的修订 UUID。
安全情报列表 1 (Security Intelligence List 1)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能有三个与连接关联的安全情报列表。
安全情报列表 2 (Security Intelligence List 2)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能有三个与连接关联的安全情报列表。
威胁智能类别	uint32	与事件关联的威胁智能类别。这映射到关联元数据中的威胁智能列表。
字符串块类型 (String Block Type)	uint32	启动包含入口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“入口 VRF ”(Ingress VRF) 名称字段中的字节数。
入口 VRF 名称	字符串	用于流量进入网络的虚拟路由器。
字符串块类型 (String Block Type)	uint32	启动包含出口 VRF 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“出口 VRF ”(Egress VRF) 名称字段中的字节数。
出口 VRF 名称	字符串	用于流量离开网络的虚拟路由器。
字符串块类型 (String Block Type)	uint32	启动包含源 IP 动态属性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“源 IP 动态属性”(Source IP Dynamic Attribute) 字段中的字节数。
源 IP 动态属性	字符串	与源 IP 地址关联的动态属性。
字符串块类型 (String Block Type)	uint32	启动包含目标 IP 动态属性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“目标 IP 动态属性”(Destination IP Dynamic Attribute) 字段中的字节数。
目标 IP 动态属性	字符串	与目标 IP 地址关联的动态属性。

旧版文件事件数据结构

以下主题介绍其他旧版文件事件数据结构：

用于 5.1.1.x 的文件事件

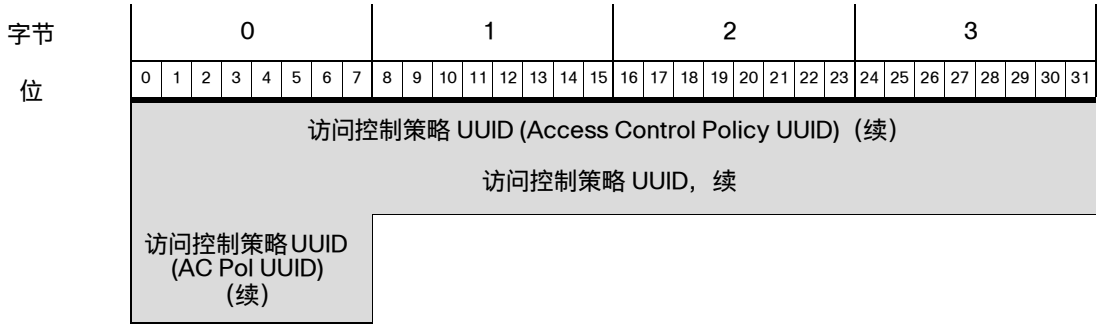
该文件事件包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 23。

下图显示文件事件数据块的结构：

字节	0				1			
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
	文件事件块类型 (23) (File Event Block Type (23))															
	文件事件块长度 (File Event Block Length)															
	设备 ID (设备 ID)															
	连接实例 (Connection Instance)															
	连接时间戳 (Connection Timestamp)															
	文件事件时间戳 (File Event Timestamp)															
	源 IP 地址 (Source IP Address)															
	源 IP 地址 (Source IP Address)（续）															
	源 IP 地址 (Source IP Address)（续）															
	源 IP 地址 (Source IP Address)（续）															
	目标 IP 地址 (Destination IP Address)															
	目标 IP 地址 (Destination IP Address)（续）															
	目标 IP 地址 (Destination IP Address)（续）															
	目标 IP 地址 (Destination IP Address)（续）															
	处理结果 (Disposition)								操作 (Action)							

字节	2				3			
位	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	连接计数器 (Connection Counter)															
	SHA 散列 (SHA Hash)															

字节	0	1	2	3
位	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）		文件类型 ID (File Type ID)	
文件名	文件类型 ID (File Type ID)（续）		字符串块类型 (0) (String Block Type (0))	
	字符串块类型 (0) (String Block Type (0))（续）		字符串块长度 (String Block Length)	
	字符串块长度 (String Block Length)（续）		文件名... (File Name...)	
	文件大小 (File Size)			
	文件大小，续			
	方向 (Direction)	应用 ID (Application ID)		
	应用 ID (App ID)（续）	用户 ID		
URI	用户 ID (User ID)（续）	字符串块类型 (0) (String Block Type (0))		
	字符串块类型 (0) (String Block Type (0))（续）	字符串块长度 (String Block Length)		
	字符串块长度 (String Block Length)（续）	URI...		
签名	字符串块类型 (0) (String Block Type (0))			
	字符串块长度 (String Block Length)			
	签名... (Signature...)			
	源端口 (Source Port)		目标端口 (Destination Port)	
	协议 (Protocol)	访问控制策略 UUID (Access Control Policy UUID)		
	访问控制策略 UUID (Access Control Policy UUID)（续）			



下表对文件事件数据块中的字段进行了说明:

表 B-47　　文件事件数据块字段

字段	数据类型	说明 (Description)
文件事件块类型 (File Event Block	uint32	启动文件事件数据块。值始终为 23。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN - 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN - 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE - 文件包含恶意软件。 ▪ 4 - CACHE_MISS - 软件无法向思科云发送请求以了解处置情况。 ▪ 5 - NO_CLOUD_RESP - 思科云服务未响应此请求。

表 B-47 文件事件数据块字段 （续）

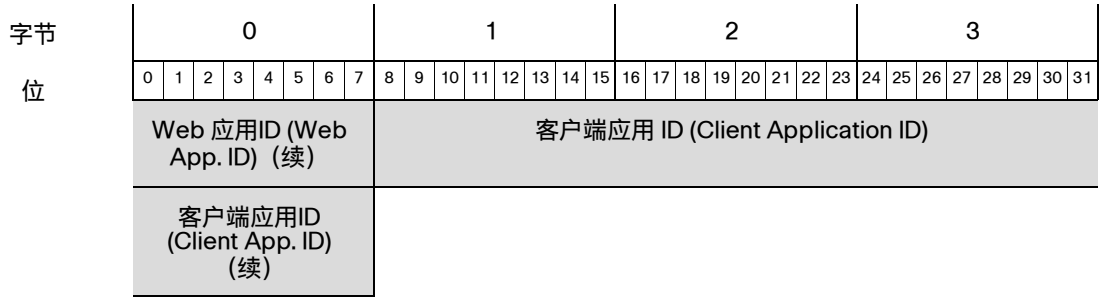
字段	数据类型	说明 (Description)
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小（字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值： ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。
签名	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。

用于 5.2 的文件事件

该文件事件包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 32。它替代了块类型 23。已添加新字段以跟踪源和目标国家/地区以及客户端和 web 应用实例。

下图显示文件事件数据块的结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	SHA 散列 (SHA Hash)（续）																文件类型 ID (File Type ID)																
文件名	文件类型 ID (File Type ID)（续）																字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0))（续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length)（续）																文件名... (File Name...)															
	文件大小 (File Size) 文件大小，续																															
	方向 (Direction)								应用 ID (Application ID)																							
	应用 ID (App ID)（续）								用户 ID																							
URI	用户 ID (User ID)（续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0))（续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)（续）								URI...																							
签名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	签名... (Signature...)																															
	源端口 (Source Port)																目标端口 (Destination Port)															
	协议 (Protocol)								访问控制策略 UUID (Access Control Policy UUID)																							
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (AC Pol UUID)（续）								源国家/地区 (Source Country)																目标国家/地区							
	目标国家/地区 (Dst. Country)（续）								Web 应用 ID (Web Application ID)																							



下表对文件事件数据块中的字段进行了说明:

表 B-48　　文件事件数据块字段

字段	数据类型	说明 (Description)
文件事件块类型 (File Event Block	uint32	启动文件事件数据块。值始终为 23。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN - 文件是安全的，不包含恶意软件。 ▪ 2 - NEUTRAL - 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE - 文件包含恶意软件。 ▪ 4 - CACHE_MISS - 软件无法向思科云发送请求以了解处置情况，或思科云服务未响应此请求。

表 B-48 文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小（字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值： ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。
签名	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如： ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。

表 B-48　　文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。

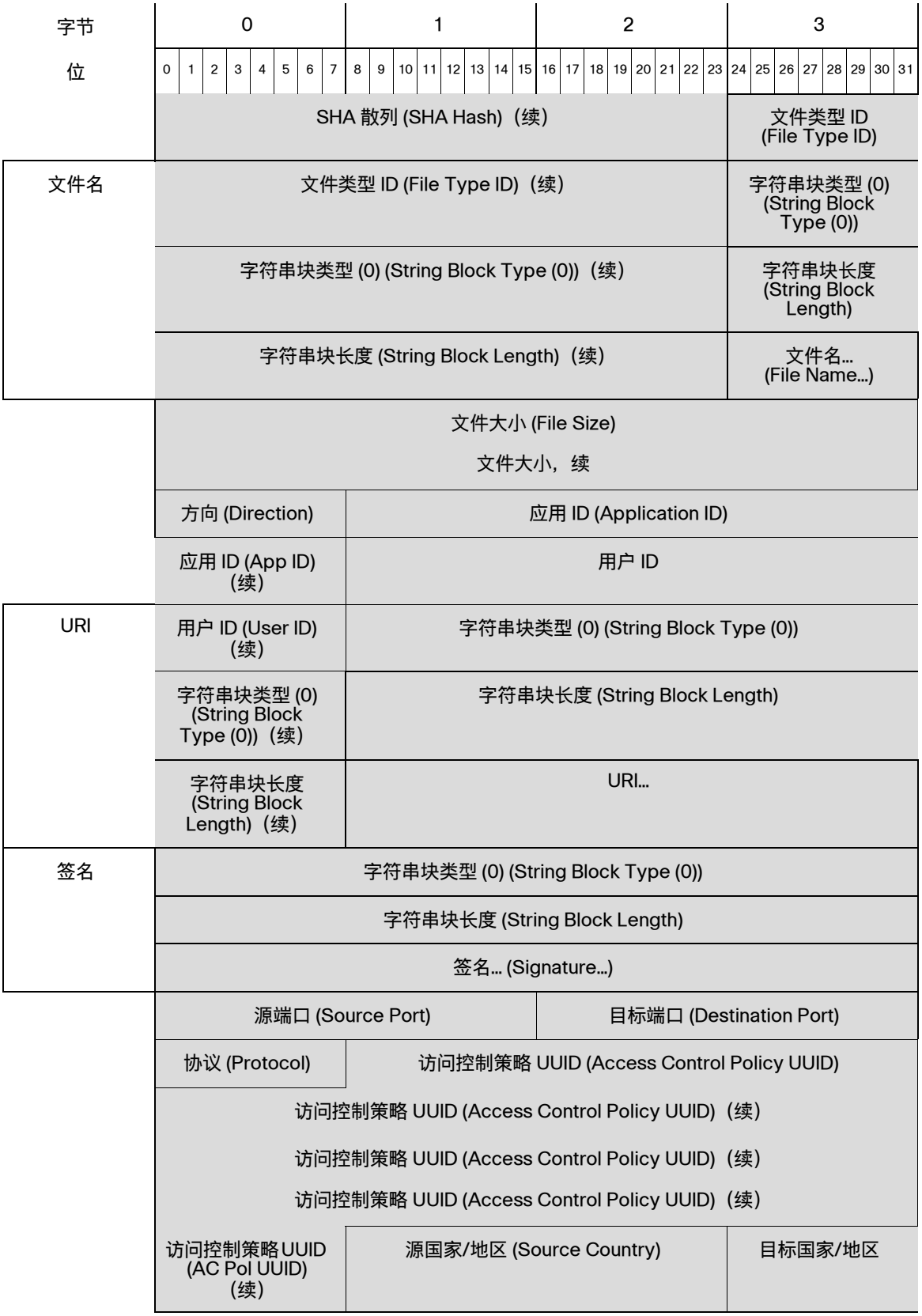
用于 5.3 的文件事件

该文件事件包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 38。它替代了块类型 32。已添加新字段以跟踪动态文件分析和文件存储。

您可以通过在事件版本为 3 且事件代码为 111 的请求消息中设置文件事件标志（请求标志字段中的位 30）请求文件事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

下图显示文件事件数据块的结构。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件事件块类型 (38) (File Event Block Type (38))																																
文件事件块长度 (File Event Block Length)																																
设备 ID (设备 ID)																																
连接实例 (Connection Instance)																	连接计数器 (Connection Counter)														
连接时间戳 (Connection Timestamp)																																
文件事件时间戳 (File Event Timestamp)																																
源 IP 地址 (Source IP Address) 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续）																																
目标 IP 地址 (Destination IP Address) 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址 (Destination IP Address)（续）																																
处理结果 (Disposition)									SPERO 处置情况 (SPERO Disposition)								文件存储状态 (File Storage Status)								文件分析状态 (File Analysis Status)							
存档文件状态 (Archive File Status)									威胁评分 (Threat Score)								操作 (Action)								SHA 散列 (SHA Hash)							
SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续）																																


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SHA 散列 (SHA Hash)（续）
文件类型 ID (File Type ID)
文件名
文件类型 ID (File Type ID)（续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
文件名... (File Name...)
文件大小 (File Size)
文件大小，续
方向 (Direction)
应用 ID (Application ID)
应用 ID (App ID)（续）
用户 ID
URI
用户 ID (User ID)（续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0))（续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length)（续）
URI...
签名
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
签名... (Signature...)
源端口 (Source Port)
目标端口 (Destination Port)
协议 (Protocol)
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略UUID (AC Pol UUID)（续）
源国家/地区 (Source Country)
目标国家/地区

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
目标国家/地区 (Dst. Country) (续)									Web 应用 ID (Web Application ID)																							
Web 应用ID (Web App. ID) (续)									客户端应用 ID (Client Application ID)																							
客户端应用ID (Client App. ID) (续)																																

下表对文件事件数据块中的字段进行了说明。

表 B-49 文件事件数据块字段

字段	数据类型	说明 (Description)
文件事件块类型 (File Event Block	uint32	启动文件事件数据块。值始终为 23。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE 文件包含恶意软件。 ▪ 4 - UNAVAILABLE 软件无法向 云发送请求以了解设备情况，或 云服务设备响应此请求。 ▪ 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
SPERO 处置情况 (SPERO Disposition)	uint8	表示文件分析中是否使用了 SPERO 签名。如果值为 1、2 或 3，则表示使用了 SPERO 分析。如果是任何其他值，则表示未使用 SPERO 分析。

表 B-49　　文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
文件存储状态 (File Storage Status)	uint8	文件的存储状态。可能的值如下： ▪ 1 - 文件已存储 ▪ 2 - 文件已存储 ▪ 3 - 无法存储文件 ▪ 4 - 无法存储文件 ▪ 5 - 无法存储文件 ▪ 6 - 无法存储文件 ▪ 7 - 无法存储文件 ▪ 8 - 文件太大 ▪ 9 - 文件太小 ▪ 10 - 无法存储文件 ▪ 11 - 文件未存储，无法获取处置情况
文件分析状态 (File Analysis Status)	uint8	是否已发送该文件进行动态分析。可能的值如下： ▪ 0 - 未发送文件进行分析 ▪ 1 - 已发送进行分析 ▪ 2 - 已发送进行分析 ▪ 4 - 已发送进行分析 ▪ 5 - 发送失败 ▪ 6 - 发送失败 ▪ 7 - 发送失败 ▪ 8 - 发送失败 ▪ 9 - 文件太小 ▪ 10 - 文件太大 ▪ 11 - 已发送进行分析 ▪ 12 - 分析完成 ▪ 13 - 故障（网络问题） ▪ 14 - 故障（速率限制） ▪ 15 - 故障（文件太大） ▪ 16 - 故障（文件读取错误） ▪ 17 - 故障（内部库错误） ▪ 19 - 文件未发送，无法获取处置情况 ▪ 20 - 故障（无法运行文件） ▪ 21 - 故障（分析超时） ▪ 22 - 已发送进行分析 ▪ 23 - 文件不受支持

表 B-49 文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
存档文件状态 (Archive File Status)	uint8	值始终为 0。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值: ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-40 页。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小（字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值: ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。
签名	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。

表 B-49　　文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。

用于 5.3.1 的文件事件

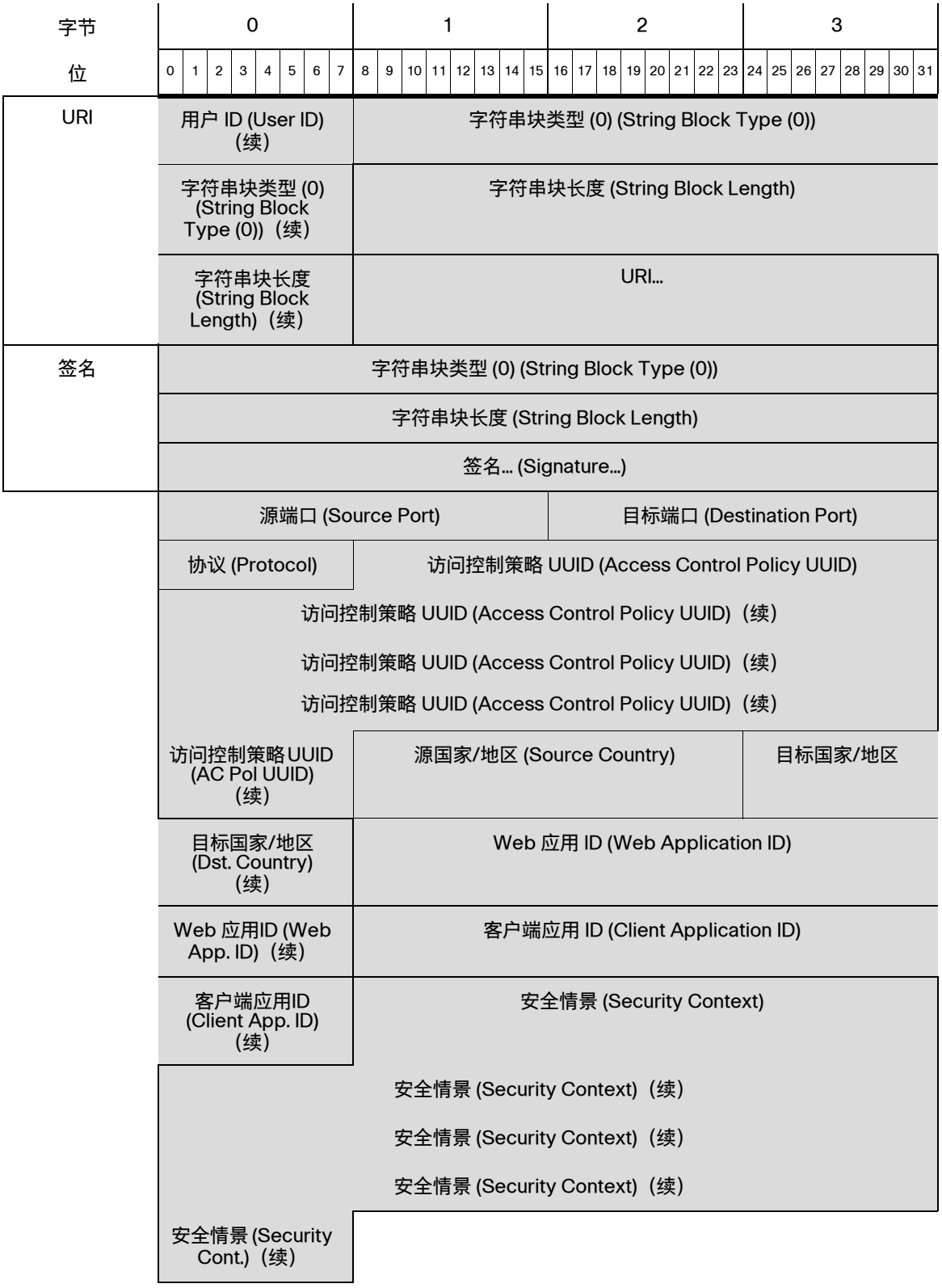
该文件事件包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 43。它替代了块类型 38。已添加安全情景字段。

您可以通过在事件版本为 4 且事件代码为 111 的请求消息中设置文件事件标志（请求标志字段中的位 30）请求文件事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

下图显示文件事件数据块的结构。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件事件块类型 (43) (File Event Block Type (43))																																
文件事件块长度 (File Event Block Length)																																
设备 ID (Device ID)																																
连接实例 (Connection Instance)																	连接计数器 (Connection Counter)														
连接时间戳 (Connection Timestamp)																																
文件事件时间戳 (File Event Timestamp)																																
源 IP 地址 (Source IP Address) 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续）																																

字节	0	1	2	3
位	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
	目标 IP 地址 (Destination IP Address)			
	目标 IP 地址 (Destination IP Address)（续）			
	目标 IP 地址 (Destination IP Address)（续）			
	目标 IP 地址 (Destination IP Address)（续）			
	处理结果 (Disposition)	SPERO 处置情况 (SPERO Disposition)	文件存储状态 (File Storage Status)	文件分析状态 (File Analysis Status)
	存档文件状态 (Archive File Status)	威胁评分 (Threat Score)	操作 (Action)	SHA 散列 (SHA Hash)
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			文件类型 ID (File Type ID)
文件名	文件类型 ID (File Type ID)（续）			字符串块类型 (0) (String Block Type (0))
	字符串块类型 (0) (String Block Type (0))（续）			字符串块长度 (String Block Length)
	字符串块长度 (String Block Length)（续）			文件名... (File Name...)
	文件大小 (File Size)			
	文件大小，续			
	方向 (Direction)	应用 ID (Application ID)		
	应用 ID (App ID)（续）	用户 ID		



下表对文件事件数据块中的字段进行了说明。

表 B-50 文件事件数据块字段

字段	数据类型	说明 (Description)
文件事件块类型 (File Event Block	uint32	启动文件事件数据块。值始终为 43。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE 文件包含恶意软件。 ▪ 4 - UNAVAILABLE 软件无法向 云发送请求以了解 （续）情况，或 云服务 （续）响应此请求。 ▪ 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
SPERO 处置情况 (SPERO Disposition)	uint8	表示文件分析中是否使用了 SPERO 签名。如果值为 1、2 或 3，则表示使用了 SPERO 分析。如果是任何其他值，则表示未使用 SPERO 分析。
文件存储状态 (File Storage Status)	uint8	文件的存储状态。可能的值如下: ▪ 1 - 文件已存储 ▪ 2 - 文件已存储 ▪ 3 - 无法存储文件 ▪ 4 - 无法存储文件 ▪ 5 - 无法存储文件 ▪ 6 - 无法存储文件 ▪ 7 - 无法存储文件 ▪ 8 - 文件太大 ▪ 9 - 文件太小 ▪ 10 - 无法存储文件 ▪ 11 - 文件未存储，无法获取处置情况

表 B-50　　文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
文件分析状态 (File Analysis Status)	uint8	是否已发送该文件进行动态分析。可能的值如下： ▪ 0 - 未发送文件进行分析 ▪ 1 - 已发送进行分析 ▪ 2 - 已发送进行分析 ▪ 4 - 已发送进行分析 ▪ 5 - 发送失败 ▪ 6 - 发送失败 ▪ 7 - 发送失败 ▪ 8 - 发送失败 ▪ 9 - 文件太小 ▪ 10 - 文件太大 ▪ 11 - 已发送进行分析 ▪ 12 - 分析完成 ▪ 13 - 故障（网络问题） ▪ 14 - 故障（速率限制） ▪ 15 - 故障（文件太大） ▪ 16 - 故障（文件读取错误） ▪ 17 - 故障（内部库错误） ▪ 19 - 文件未发送，无法获取处置情况 ▪ 20 - 故障（无法运行文件） ▪ 21 - 故障（分析超时） ▪ 22 - 已发送进行分析 ▪ 23 - 文件不受支持 ▪ 23 - 文件传输文件容量已处理 - 由于无法将文件提交到沙盒进行分析而导致文件容量已处理（存储到传感器上） ▪ 25 - 文件传输服务器限制超出容量已处理 - 服务器上的速率限制导致文件容量已处理 ▪ 26 - 通信故障 - 云连接故障导致文件容量已处理 ▪ 27 - 未发送 - 因配置原因导致文件未发送 ▪ 28 - 预分类不匹配 - 未发送文件进行动态分析，因为预分类在文件中未找到任何嵌入式或可疑对象 ▪ 29 - 传输已发送沙盒私有云 - 已将文件发送到私有云进行动态分析 ▪ 30 - 传输未发送沙盒私有云 - 未将文件发送到私有云进行分析
存档文件状态 (Archive File Status)	uint8	值始终为 0。
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。

表 B-50 文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-40 页。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小（字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值: ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。
签名	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。

用于 5.4 的文件事件

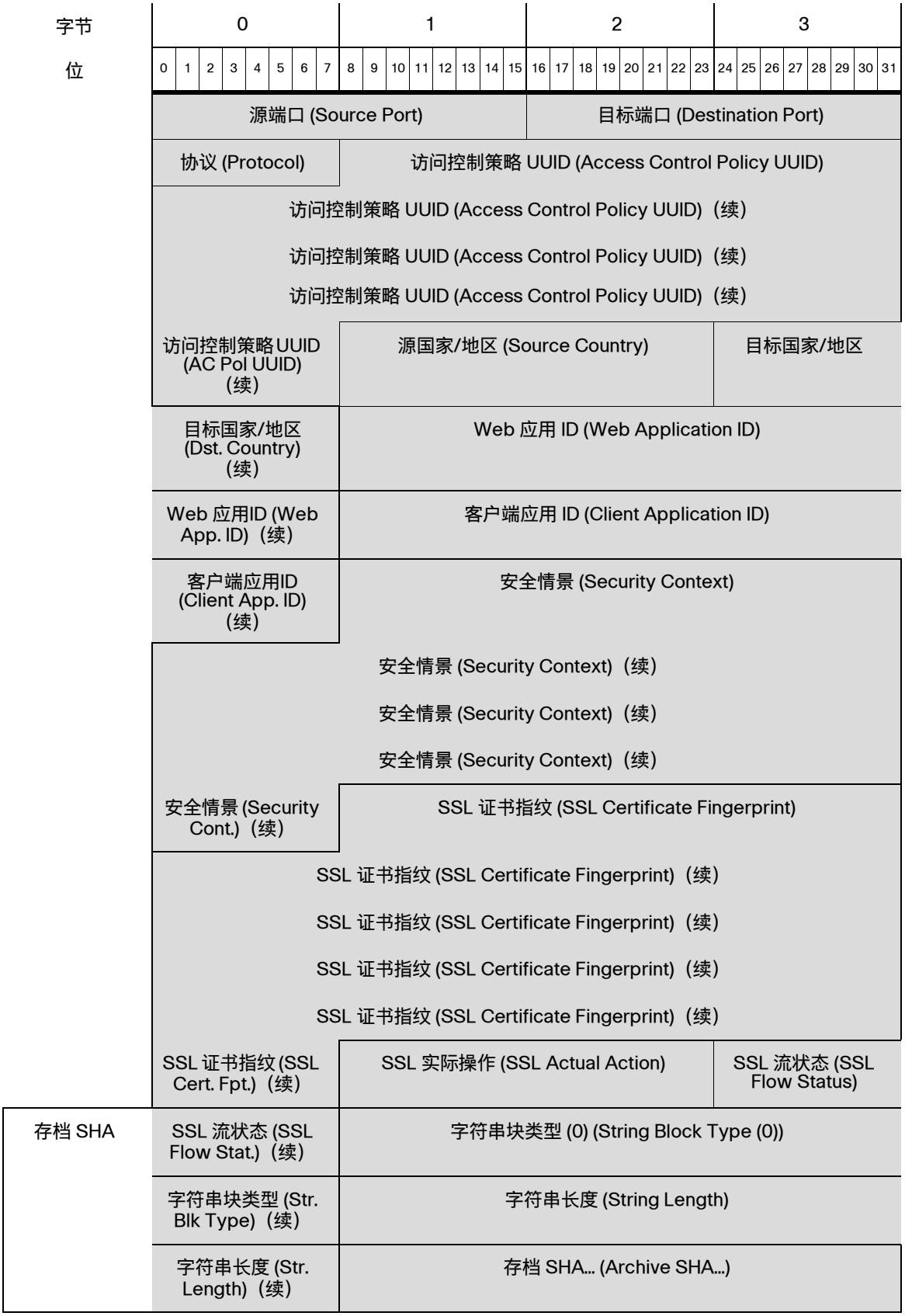
该文件事件包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 46。它替代了块类型 43。已添加用于 SSL 和文件存档支持的字段。

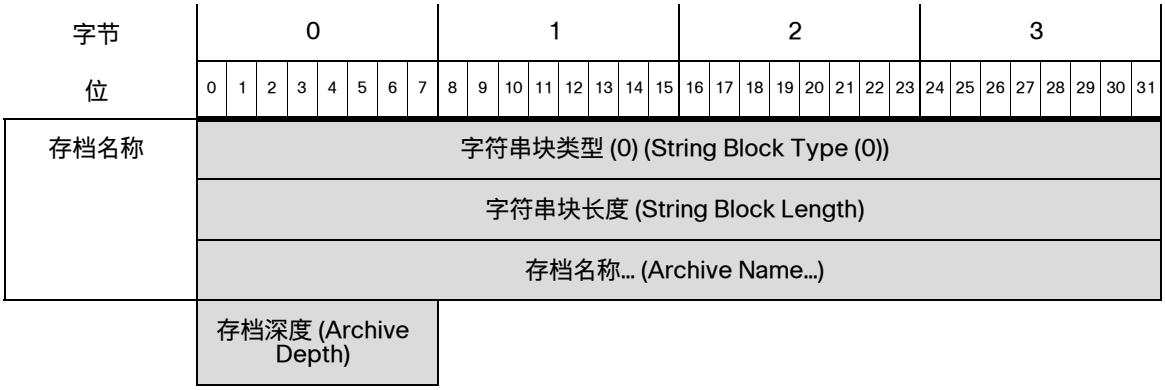
您可以通过在事件版本为 5 且事件代码为 111 的请求消息中设置文件事件标志（“请求标志”(Request Flags) 字段中的位 30）请求文件事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

下图显示文件事件数据块的结构。

字节	0				1			
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件事件块类型 (46) (File Event Block Type (46))																																
文件事件块长度 (File Event Block Length)																																
设备 ID (Device ID)																																
连接实例 (Connection Instance)																	连接计数器 (Connection Counter)														
连接时间戳 (Connection Timestamp)																																
文件事件时间戳 (File Event Timestamp)																																
源 IP 地址 (Source IP Address) 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续）																																
目标 IP 地址 (Destination IP Address) 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址 (Destination IP Address)（续）																																
处理结果 (Disposition)									SPERO 处置情况 (SPERO Disposition)								文件存储状态 (File Storage Status)								文件分析状态 (File Analysis Status)							
存档文件状态 (Archive File Status)									威胁评分 (Threat Score)								操作 (Action)								SHA 散列 (SHA Hash)							

字节	0	1	2	3
位	0 1 2 3 4 5 6 7	8 9 10 11 12 13 14 15	16 17 18 19 20 21 22 23	24 25 26 27 28 29 30 31
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			
	SHA 散列 (SHA Hash)（续）			文件类型 ID (File Type ID)
文件名	文件类型 ID (File Type ID)（续）			字符串块类型 (0) (String Block Type (0))
	字符串块类型 (0) (String Block Type (0))（续）			字符串块长度 (String Block Length)
	字符串块长度 (String Block Length)（续）			文件名… (File Name…)
	文件大小 (File Size)			
	文件大小，续			
	方向 (Direction)	应用 ID (Application ID)		
	应用 ID (App ID)（续）	用户 ID		
URI	用户 ID (User ID)（续）	字符串块类型 (0) (String Block Type (0))		
	字符串块类型 (0) (String Block Type (0))（续）	字符串块长度 (String Block Length)		
	字符串块长度 (String Block Length)（续）	URI…		
签名	字符串块类型 (0) (String Block Type (0))			
	字符串块长度 (String Block Length)			
	签名… (Signature…)			


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
源端口 (Source Port)
目标端口 (Destination Port)
协议 (Protocol)
访问控制策略 UUID (Access Control Policy UUID)
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略 UUID (Access Control Policy UUID)（续）
访问控制策略UUID (AC Pol UUID)（续）
源国家/地区 (Source Country)
目标国家/地区
目标国家/地区 (Dst. Country)（续）
Web 应用 ID (Web Application ID)
Web 应用ID (Web App. ID)（续）
客户端应用 ID (Client Application ID)
客户端应用ID (Client App. ID)（续）
安全情景 (Security Context)
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Context)（续）
安全情景 (Security Cont.)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Certificate Fingerprint)（续）
SSL 证书指纹 (SSL Cert. Fpt.)（续）
SSL 实际操作 (SSL Actual Action)
SSL 流状态 (SSL Flow Status)
存档 SHA
SSL 流状态 (SSL Flow Stat.)（续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (Str. Blk Type)（续）
字符串长度 (String Length)
字符串长度 (Str. Length)（续）
存档 SHA... (Archive SHA...)



下表对文件事件数据块中的字段进行了说明。

表 B-51 用于 5.4.x 的文件事件数据块字段

字段	数据类型	说明 (Description)
文件事件块类型 (File Event Block	uint32	启动文件事件数据块。值始终为 46。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括: ▪ 1 - CLEAN 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE 文件包含恶意软件。 ▪ 4 - UNAVAILABLE 软件无法向 云发送请求以了解 （续）情况，或 云服务 （续）响应此请求。 ▪ 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
SPERO 处置情况 (SPERO Disposition)	uint8	表示文件分析中是否使用了 SPERO 签名。如果值为 1、2 或 3，则表示使用了 SPERO 分析。如果是任何其他值，则表示未使用 SPERO 分析。

表 B-51　　用于 5.4.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
文件存储状态 (File Storage Status)	uint8	文件的存储状态。可能的值如下： ▪ 1 - 文件已存储 ▪ 2 - 文件已存储 ▪ 3 - 无法存储文件 ▪ 4 - 无法存储文件 ▪ 5 - 无法存储文件 ▪ 6 - 无法存储文件 ▪ 7 - 无法存储文件 ▪ 8 - 文件太大 ▪ 9 - 文件太小 ▪ 10 - 无法存储文件 ▪ 11 - 文件未存储，无法获取处置情况
文件分析状态 (File Analysis Status)	uint8	是否已发送该文件进行动态分析。可能的值如下： ▪ 0 - 未发送文件进行分析 ▪ 1 - 已发送进行分析 ▪ 2 - 已发送进行分析 ▪ 4 - 已发送进行分析 ▪ 5 - 发送失败 ▪ 6 - 发送失败 ▪ 7 - 发送失败 ▪ 8 - 发送失败 ▪ 9 - 文件太小 ▪ 10 - 文件太大 ▪ 11 - 已发送进行分析 ▪ 12 - 分析完成 ▪ 13 - 故障（网络问题） ▪ 14 - 故障（速率限制） ▪ 15 - 故障（文件太大） ▪ 16 - 故障（文件读取错误） ▪ 17 - 故障（内部库错误） ▪ 19 - 文件未发送，无法获取处置情况 ▪ 20 - 故障（无法运行文件） ▪ 21 - 故障（分析超时） ▪ 22 - 已发送进行分析 ▪ 23 - 文件不受支持

表 B-51 用于 5.4.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
存档文件状态 (Archive File Status)	uint8	正在被检测的存档的状态。可能会有以下值： ▪ 0 - 不适用 - 文件没有被作为存档进行检测 ▪ 1 - 待处理 - 正在检测存档 ▪ 2 - 提取 - 已成功检测，且无任何问题 ▪ 3 - 失败 - 检测失败，系统资源不足 ▪ 4 - 超出深度 - 成功，但存档超出了嵌套的检测深度 ▪ 5 - 加密 - 部分成功，存档已加密或包含加密的存档 ▪ 6 - 无法检出 - 部分成功，文件可能已变形或损坏
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值： ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表 ▪ 6 - 云查找超时 ▪ 7 - 自定义检测 ▪ 8 - 自定义检测阻止 ▪ 9 - 存档阻止（超出深度） ▪ 10 - 存档阻止（已加密） ▪ 11 - 存档阻止（检查失败）
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-40 页。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小（字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值： ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。

表 B-51　　用于 5.4.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
签名	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-51 用于 5.4.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
字符串块类型 (String Block Type)	uint32	启动包含存档 SHA 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档 SHA 字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。
存档 SHA (Archive SHA)	字符串	包含该文件的父存档的 SHA1 散列。

表 B-51　　用于 5.4.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含“存档名称”(Archive Name) 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上入侵策略名称中的字节数。
存档名称 (Archive Name)	字符串	父存档的名称。
存档深度 (Archive Depth)	uint8	嵌套文件的层数。例如，如果文本文件位于压缩存档中，则此值为 1。

6.x 的文件事件

文件事件数据块包含通过网络发送的文件的相关信息。这包括连接信息，文件是否是恶意软件以及用于识别文件的特定信息。文件事件的块类型为系列 2 数据块组中的 56。它替代了块类型 46，然后被块类型 79 替代。已添加 ISE 集成、文件分析、本地恶意软件分析以及容量处理状态等字段。

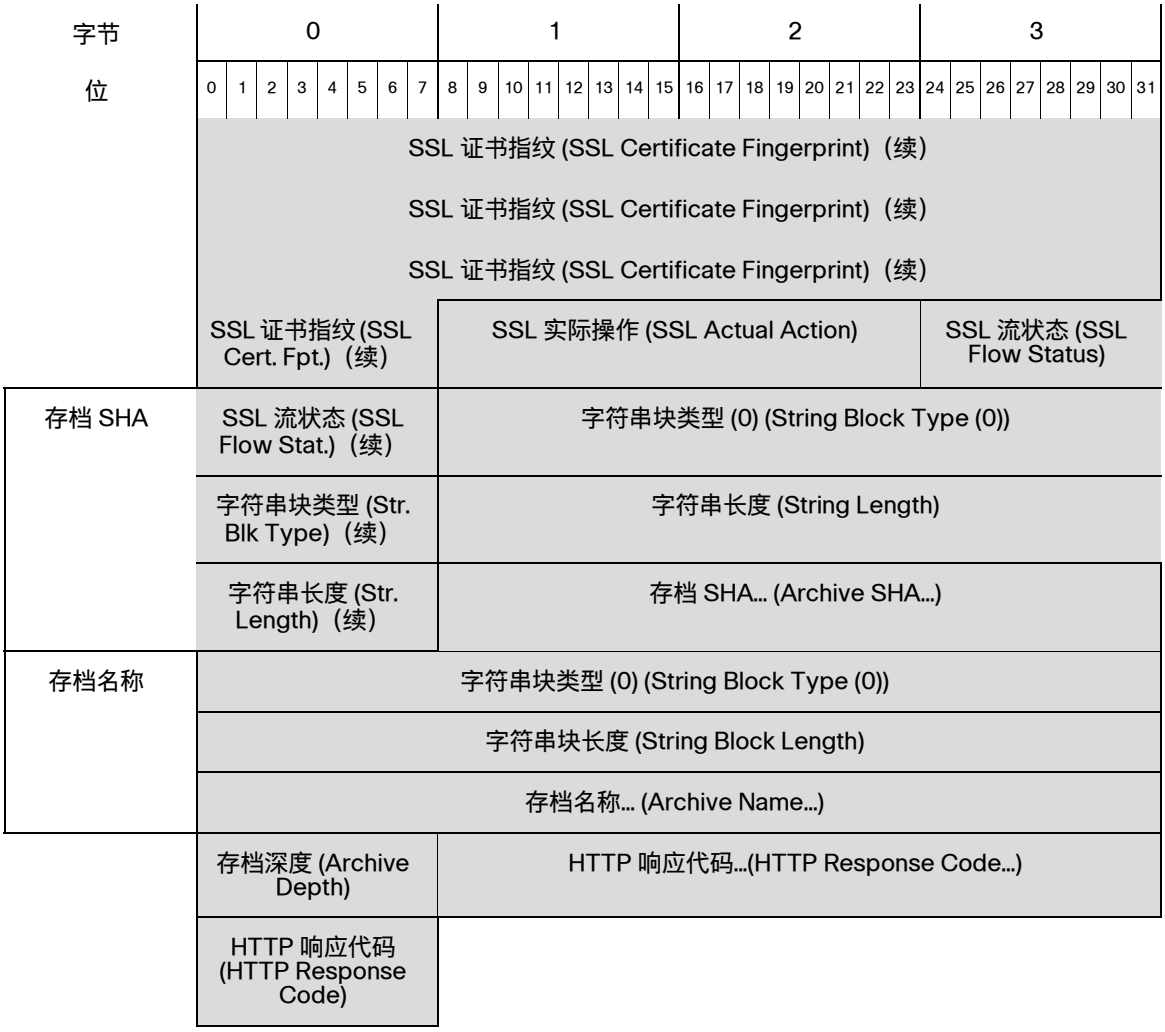
您可以通过在事件版本为 5 且事件代码为 111 的请求消息中设置文件事件标志（“请求标志”(Request Flags) 字段中的位 30）请求文件事件记录。请参阅请求标志，第 2-12 页。如果您启用位 23，则记录中会包含扩展事件报头。

下图显示文件事件数据块的结构。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
文件事件块类型 (56) (File Event Block Type (56))																																
文件事件块长度 (File Event Block Length)																																
设备 ID (Device ID)																																
连接实例 (Connection Instance)																	连接计数器 (Connection Counter)														
连接时间戳 (Connection Timestamp)																																
文件事件时间戳 (File Event Timestamp)																																
源 IP 地址 (Source IP Address) 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续） 源 IP 地址 (Source IP Address)（续）																																

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	目标 IP 地址 (Destination IP Address) 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址 (Destination IP Address)（续） 目标 IP 地址 (Destination IP Address)（续）																															
	处理结果 (Disposition)								SPERO 处置情况 (SPERO Disposition)								文件存储状态 (File Storage Status)								文件分析状态 (File Analysis Status)							
	本地恶意软件分析统计信息 (Local Malware Analysis Stat.)								存档文件状态 (Archive File Status)								威胁评分 (Threat Score)								操作 (Action)							
	SHA 散列 (SHA Hash) SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续） SHA 散列 (SHA Hash)（续）																															
	文件类型 ID (File Type ID)																															
文件名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	文件名... (File Name...)																															
	文件大小 (File Size) 文件大小，续																															
	方向 (Direction)								应用 ID (Application ID)																							
	应用 ID (App ID)（续）								用户 ID																							

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
URI	用户 ID (User ID)（续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (0) (String Block Type (0))（续）								字符串块长度 (String Block Length)																							
	字符串块长度 (String Block Length)（续）								URI...																							
签名	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	签名... (Signature...)																															
	源端口 (Source Port)																目标端口 (Destination Port)															
	协议 (Protocol)								访问控制策略 UUID (Access Control Policy UUID)																							
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略 UUID (Access Control Policy UUID)（续）																															
	访问控制策略UUID (AC Pol UUID)（续）								源国家/地区 (Source Country)																目标国家/地区							
	目标国家/地区 (Dst. Country)（续）								Web 应用 ID (Web Application ID)																							
	Web 应用ID (Web App. ID)（续）								客户端应用 ID (Client Application ID)																							
	客户端应用ID (Client App. ID)（续）								安全情景 (Security Context)																							
	安全情景 (Security Context)（续）																															
	安全情景 (Security Context)（续）																															
	安全情景 (Security Context)（续）																															
	安全情景 (Security Cont.)（续）								SSL 证书指纹 (SSL Certificate Fingerprint)																							
	SSL 证书指纹 (SSL Certificate Fingerprint)（续）																															



下表对文件事件数据块中的字段进行了说明。

表 B-52 用于 6.x 的文件事件数据块字段

字段	数据类型	说明 (Description)
文件事件块类型 (File Event Block	uint32	启动文件事件数据块。值始终为 56。
文件事件块长度 (File Event Block Length)	uint32	文件事件块中的字节总数，包括文件事件块类型和长度字段的八个字节，加上随后的数据的字节数。
设备 ID (Device ID)	uint32	生成事件的设备的 ID。
连接实例 (Connection Instance)	uint16	生成事件的设备上的 Snort 实例。用于将该事件与连接或入侵事件相关联。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
连接时间戳 (Connection Timestamp)	uint32	相关连接事件的

表 B-52　　用于 6.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
文件事件时间戳 (File Event Timestamp)	uint32	识别文件类型以及生成文件事件时的
源 IP 地址 (Source IP Address)	uint8[16]	连接源的 IPv4 或 IPv6 地址。
目标	uint8[16]	连接目标的 IPv4 或 IPv6 地址。
处理结果 (Disposition)	uint8	文件的恶意软件状态。可能的值包括： ▪ 1 - CLEAN 文件是安全的，不包含恶意软件。 ▪ 2 - UNKNOWN 不确定文件是否包含恶意软件。 ▪ 3 - MALWARE 文件包含恶意软件。 ▪ 4 - UNAVAILABLE 软件无法向 AMP 云发送请求以了解处置情况，或 AMP 云服务未响应此请求。 ▪ 5 - CUSTOM SIGNATURE 文件与用户定义的散列匹配，并且以用户指定的方式进行处理。
SPERO 处置情况 (SPERO Disposition)	uint8	表示文件分析中是否使用了 SPERO 签名。如果值为 1、2 或 3，则表示使用了 SPERO 分析。如果是任何其他值，则表示未使用 SPERO 分析。
文件存储状态 (File Storage Status)	uint8	文件的存储状态。可能的值如下： ▪ 1 - 文件已存储 ▪ 2 - 文件已存储 ▪ 3 - 无法存储文件 ▪ 4 - 无法存储文件 ▪ 5 - 无法存储文件 ▪ 6 - 无法存储文件 ▪ 7 - 无法存储文件 ▪ 8 - 文件太大 ▪ 9 - 文件太小 ▪ 10 - 无法存储文件 ▪ 11 - 文件未存储，无法获取处置情况

表 B-52 用于 6.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
文件分析状态 (File Analysis Status)	uint8	是否已发送该文件进行动态分析。可能的值如下: ▪ 0 - 未发送文件进行分析 ▪ 1 - 已发送进行分析 ▪ 2 - 已发送进行分析 ▪ 4 - 已发送进行分析 ▪ 5 - 发送失败 ▪ 6 - 发送失败 ▪ 7 - 发送失败 ▪ 8 - 发送失败 ▪ 9 - 文件太小 ▪ 10 - 文件太大 ▪ 11 - 已发送进行分析 ▪ 12 - 分析完成 ▪ 13 - 故障（网络问题） ▪ 14 - 故障（速率限制） ▪ 15 - 故障（文件太大） ▪ 16 - 故障（文件读取错误） ▪ 17 - 故障（内部库错误） ▪ 19 - 文件未发送，无法获取处置情况 ▪ 20 - 故障（无法运行文件） ▪ 21 - 故障（分析超时） ▪ 22 - 已发送进行分析 ▪ 23 - 文件传输文件容量已处理 - 由于无法将文件提交到沙盒进行分析而导致文件容量已处理（存储到传感器上） ▪ 25 - 文件传输服务器限制超出容量已处理 - 服务器上的速率限制导致文件容量已处理 ▪ 26 - 通信故障 - 云连接故障导致文件容量已处理 ▪ 27 - 未发送 - 因配置原因导致文件未发送 ▪ 28 - 预分类不匹配 - 未发送文件进行动态分析，因为预分类在文件中未找到任何嵌入式或可疑对象 ▪ 29 - 传输已发送沙盒私有云 - 已将文件发送到私有云进行动态分析 ▪ 30 - 传输未发送沙盒私有云 - 未将文件发送到私有云进行分析
本地恶意软件分析状态 (Local Malware Analysis Status)	uint8	文件的恶意软件分析状态。可能的值包括: ▪ 0 - 文件未分析 ▪ 1 - 分析完成 ▪ 2 - 分析失败 ▪ 3 - 手动分析请求

表 B-52　用于 6.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
存档文件状态 (Archive File Status)	uint8	正在被检测的存档的状态。可能会有以下值: ▪ 0 - 不适用 - 文件没有被作为存档进行检测 ▪ 1 - 待处理 - 正在检测存档 ▪ 2 - 提取 - 已成功检测，且无任何问题 ▪ 3 - 失败 - 检测失败，系统资源不足 ▪ 4 - 超出深度 - 成功，但存档超出了嵌套的检测深度 ▪ 5 - 加密 - 部分成功，存档已加密或包含加密的存档 ▪ 6 - 无法检出 - 部分成功，文件可能已变形或损坏
威胁评分 (Threat Score)	uint8	0 到 100 之间的数值，基于在动态分析期间观察到的潜在恶意行为而打出。
操作 (Action)	uint8	根据文件类型对文件执行的操作。可能会有以下值: ▪ 1 - 检测 ▪ 2 - 阻止 ▪ 3 - 恶意软件云查找 ▪ 4 - 恶意软件阻止 ▪ 5 - 恶意软件允许列表 ▪ 6 - 云查找超时 ▪ 7 - 自定义检测 ▪ 8 - 自定义检测阻止 ▪ 9 - 存档阻止（超出深度） ▪ 10 - 存档阻止（已加密） ▪ 11 - 存档阻止（检查失败）
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
文件类型 ID (File Type ID)	uint32	映射至文件类型的 ID 编号。此字段的含义在随此事件提供的元数据中传输。有关详细信息，请参阅面向终端的 AMP 文件类型元数据，第 3-40 页。
文件名 (File Name)	字符串	文件的名称。
文件大小 (File Size)	uint64	文件的大小（字节数）。
方向 (Direction)	uint8	指示是否已上传或下载此文件的值。可能会有以下值: ▪ 1 - 下载 ▪ 2 - 上传 目前该值取决于协议（例如，如果连接是 HTTP，则其值为 Download）。
应用 ID (Application ID)	uint32	通过文件传送映射至应用的 ID 编号。
用户 ID	uint32	系统识别的登录目标主机的用户的 ID 号码。
URI	字符串	连接的统一资源标识符 (URI)。

表 B-52 用于 6.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
签名	字符串	字符串格式的文件的 SHA-256 散列。
源端口 (Source Port)	uint16	连接源的端口号。
目标端口 (Destination Port)	uint16	连接的目标的端口号。
协议 (Protocol)	uint8	用户指定的 IANA 协议号。例如: ▪ 1 - ICMP ▪ 4 - IP ▪ 6 - TCP ▪ 17 - UDP 目前仅限 TCP。
访问控制策略 UUID (Access Control Policy UUID)	uint8[16]	触发事件的访问控制策略的唯一标识符。
源国家/地区 (Source Country)	uint16	源主机的国家/地区代码。
目标国家/地区 (Destination Country)	uint16	目标主机的国家/地区代码。
Web 应用 ID (Web Application ID)	uint32	Web 应用（如适用）的内部标别号。
客户端应用 ID (Client Application ID)	uint32	客户端应用（如适用）的内部标别号。
安全情景 (Security Context)	uint8(16)	流量通过的安全情景（虚拟防火墙）的 ID 号码。请注意，系统仅对多情景模式下的 ASA FirePOWER 设备填充此字段。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘请勿解密’ ▪ 2 -‘阻止’ ▪ 3 -‘阻止并重置’ ▪ 4 -‘解密（已知密钥）’ ▪ 5 -‘解密（更换秘钥）’ ▪ 6 -‘解密（放弃）’

表 B-52　　用于 6.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
SSL 流状态 (SSL Flow Status)	uint16	SSL 流的状态。这些值说明所执行的操作或所显示的错误消息背后的原因。可能的值包括: ▪ 0 -‘未知’ ▪ 1 -‘不匹配’ ▪ 2 -‘成功’ ▪ 3 -‘非缓存会话’ ▪ 4 -‘未知密码套件’ ▪ 5 -‘不受支持的密码套件’ ▪ 6 -‘不受支持的 SSL 版本’ ▪ 7 -‘使用的 SSL 压缩’ ▪ 8 -‘在被动模式中无法解密的会话’ ▪ 9 -‘握手错误’ ▪ 10 -‘解密错误’ ▪ 11 -‘待处理服务器名称分类查找’ ▪ 12 -‘待处理通用名称分类查找’ ▪ 13 -‘内部错误’ ▪ 14 -‘网络参数不可用’ ▪ 15 -‘服务器证书处理无效’ ▪ 16 -‘服务器证书指纹不可用’ ▪ 17 -‘无法缓存持有者 DN’ ▪ 18 -‘无法缓存颁发者 DN’ ▪ 19 -‘未知 SSL 版本’ ▪ 20 -‘外部证书列表不可用’ ▪ 21 -‘外部证书指纹不可用’ ▪ 22 -‘内部证书列表无效’ ▪ 23 -‘内部证书列表不可用’ ▪ 24 -‘内部证书不可用’ ▪ 25 -‘内部证书指纹不可用’ ▪ 26 -‘服务器证书验证不可用’ ▪ 27 -‘服务器证书验证失败’ ▪ 28 -‘操作无效’
字符串块类型 (String Block Type)	uint32	启动包含存档 SHA 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档 SHA 字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。
存档 SHA (Archive SHA)	字符串	包含该文件的父存档的 SHA1 散列。

表 B-52　　用于 6.x 的文件事件数据块字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动包含“存档名称”(Archive Name) 的字符串数据块。值始终为 `0`。
字符串块长度 (String Block Length)	uint32	存档名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上入侵策略名称中的字节数。
存档名称 (Archive Name)	字符串	父存档的名称。
存档深度 (Archive Depth)	uint8	嵌套文件的层数。例如，如果文本文件位于压缩存档中，则此值为 `1`。
HTTP 响应代码 (HTTP Response	uint32	HTTP 响应代码 (HTTP Response

用于 5.1.1-5.2.x 的文件事件 SHA 散列

eStreamer 服务使用文件事件 SHA 散列数据块以包含文件的 SHA 散列到其文件名的映射的元数据。块类型为系列 2 数据块列表中的 26。如果已在扩展请求中请求文件日志事件（事件代码为 111）且已设置位 20 或已请求元数据（事件版本为 4，事件代码为 21），则可以请求它。

下图显示文件事件散列数据块的结构：

下表对文件事件 SHA 散列数据块中的字段进行了说明。

表 B-53　　文件事件 SHA 散列 5.1.1 - 5.2.x 数据块字段

字段	数据类型	说明 (Description)
文件事件 SHA 散列块类型 (File Event SHA Hash Block Type)	uint32	启动文件事件 SHA 散列块。值始终为 26。
文件事件 SHA 散列块长度 (File Event SHA Hash Block Length)	uint32	文件事件 SHA 散列块中的字节总数，包括文件事件 SHA 散列块类型和长度字段的八个字节，加上随后的数据的字节数。
SHA 散列 (SHA Hash)	uint8[32]	二进制格式的文件的 SHA-256 散列。
字符串块类型 (String Block Type)	uint32	启动包含与文件相关的描述性名称的字符串数据块。值始终为0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上“名称”(Name) 字段中的字节数。
文件名或处置情况 (File Name or Disposition)	字符串	文件的描述性名称或处置情况。如果文件是安全的，则值为 Clean。如果文件的处置情况未知，则值为 Neutral。如果文件包含恶意软件，则提供文件名。

旧版关联事件数据结构

以下主题介绍其他旧版关联（合规性）数据结构:

- 用于 5.0 - 5.0.2 的关联事件，第 B-348 页
- 用于 5.1-5.3.x 的关联事件，第 B-355 页

用于 5.0 - 5.0.2 的关联事件

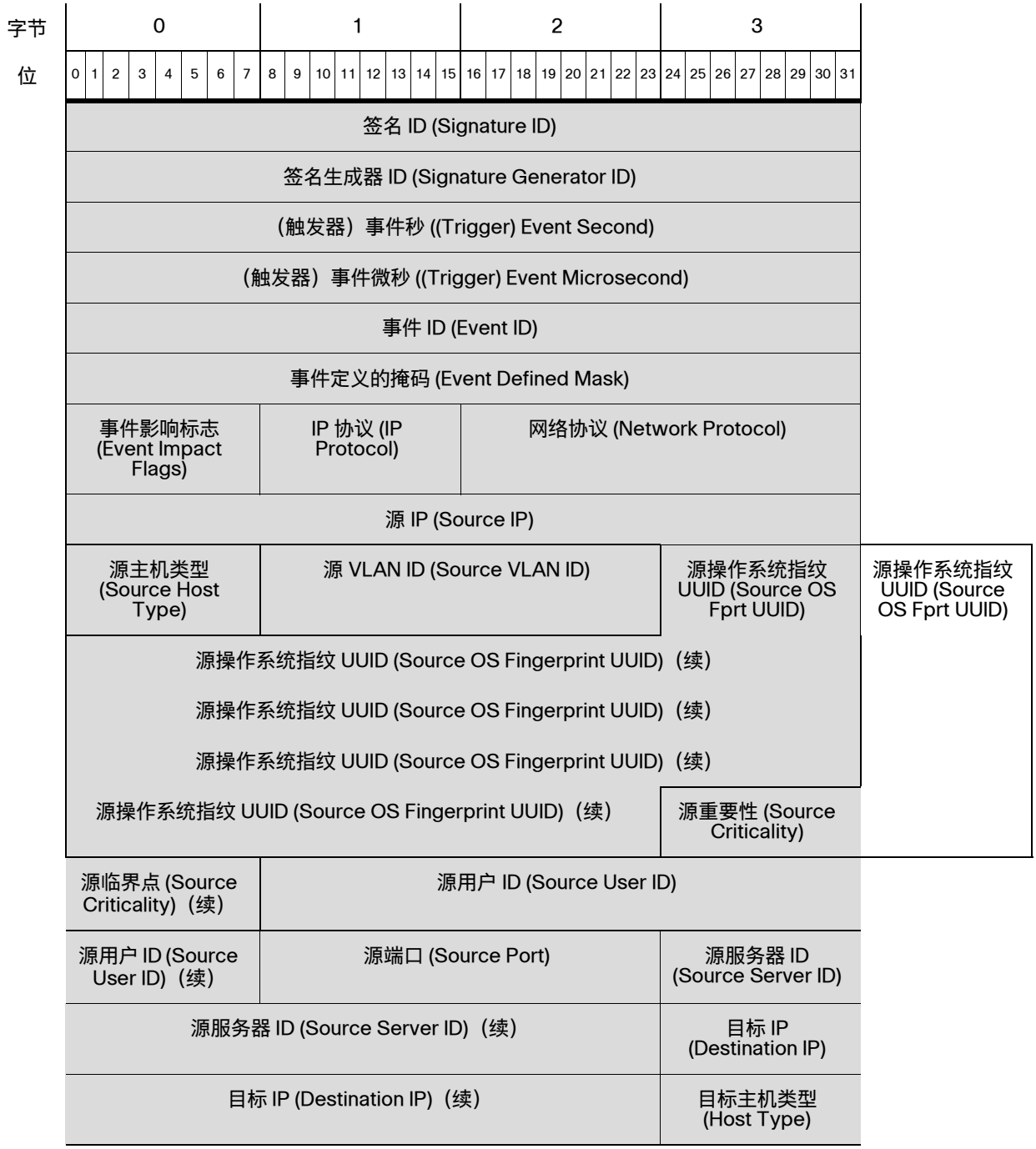
关联事件（在 5.0 之前的版本中称为合规性事件）包含关联策略违规的相关信息。此消息使用标准 eStreamer 消息报头并指定记录类型为 112，随后是类型为 116 的关联数据块。数据块类型 116 与其前身（块类型 107）的区别在于，其包含关联安全区和接口的其他相关信息。

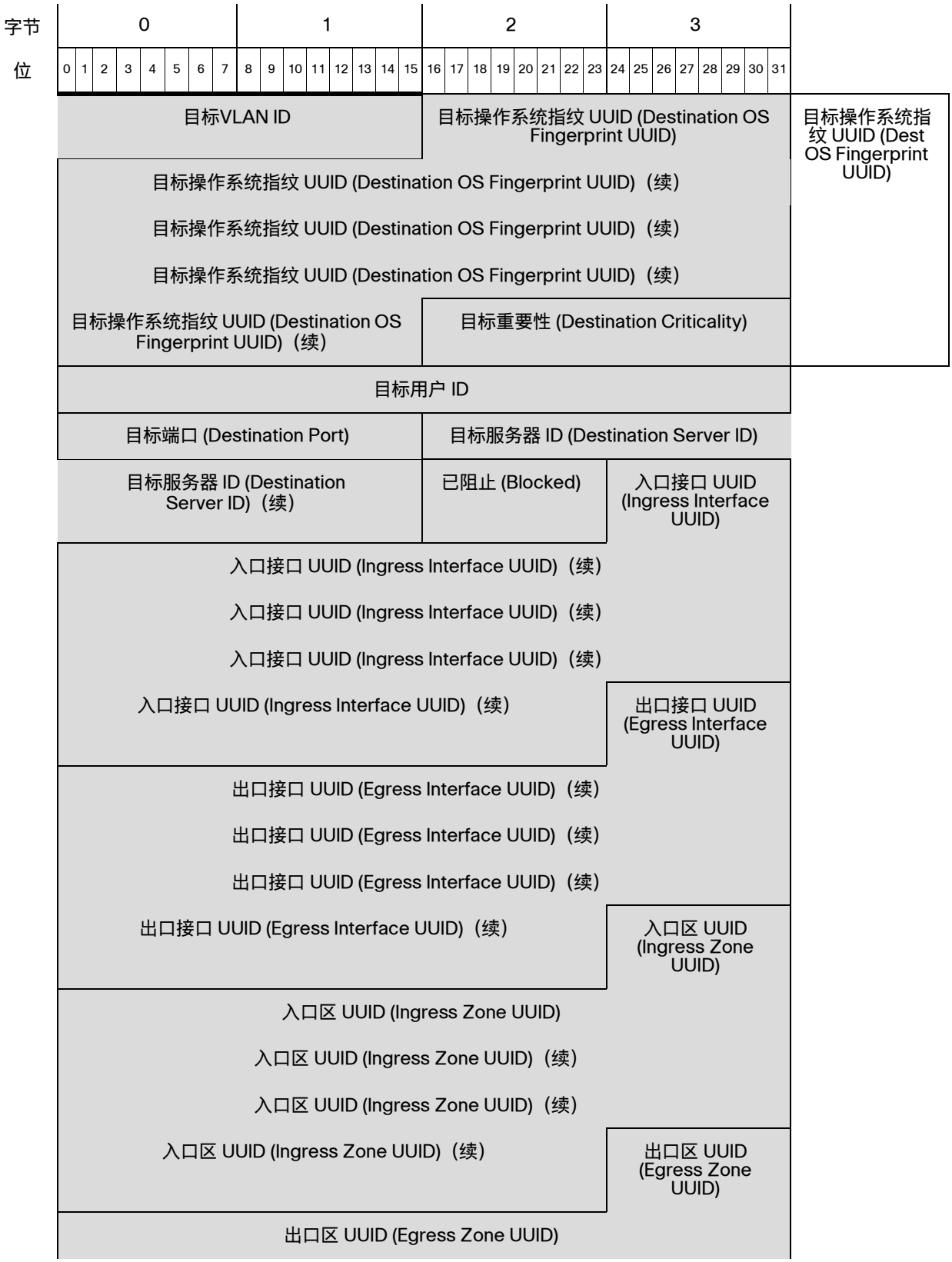
您可以通过扩展请求，仅从 eStreamer 请求 5.0 入侵事件，要提交扩展请求，您需要在流请求消息中请求事件类型代码 31 和版本代码 7（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。您可以选择启用初始事件流请求消息的标志字段中的位 23，以包含扩展事件报头。您也可以启用标志字段中的位 20，以包含用户元数据。

请注意，记录结构包含一个字符串块类型，该数据块为系列 1 中的数据块。有关系列 1 数据块的信息，请参阅了解发现（系列 1）块，第 4-60 页。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (112)（Record Type (112)）															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																
关联块类型 (116) (Correlation Block Type (116))																																
关联块长度 (Correlation Block Length)																																
设备 ID (设备 ID)																																
（关联）事件秒 ((Correlation) Event Second)																																
事件 ID (Event ID)																																
策略 ID (Policy ID)																																
规则 ID (Rule ID)																																
优先级 (Priority)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
说明... (Description...)																									事件类型 (Event Type)							
事件设备 ID (Event 设备 ID)																																

事件说明 (Description)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
签名 ID (Signature ID)
签名生成器 ID (Signature Generator ID)
（触发器）事件秒 ((Trigger) Event Second)
（触发器）事件微秒 ((Trigger) Event Microsecond)
事件 ID (Event ID)
事件定义的掩码 (Event Defined Mask)
事件影响标志 (Event Impact Flags)
IP 协议 (IP Protocol)
网络协议 (Network Protocol)
源 IP (Source IP)
源主机类型 (Source Host Type)
源 VLAN ID (Source VLAN ID)
源操作系统指纹 UUID (Source OS Fprt UUID)
源操作系统指纹 UUID (Source OS Fprt UUID)
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源重要性 (Source Criticality)
源临界点 (Source Criticality)（续）
源用户 ID (Source User ID)
源用户 ID (Source User ID)（续）
源端口 (Source Port)
源服务器 ID (Source Server ID)
源服务器 ID (Source Server ID)（续）
目标 IP (Destination IP)
目标 IP (Destination IP)（续）
目标主机类型 (Host Type)


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
目标VLAN ID
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)
目标操作系统指纹 UUID (Dest OS Fingerprint UUID)
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标重要性 (Destination Criticality)
目标用户 ID
目标端口 (Destination Port)
目标服务器 ID (Destination Server ID)
目标服务器 ID (Destination Server ID)（续）
已阻止 (Blocked)
入口接口 UUID (Ingress Interface UUID)
入口接口 UUID (Ingress Interface UUID)（续）
入口接口 UUID (Ingress Interface UUID)（续）
入口接口 UUID (Ingress Interface UUID)（续）
入口接口 UUID (Ingress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)
出口接口 UUID (Egress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)（续）
入口区 UUID (Ingress Zone UUID)
入口区 UUID (Ingress Zone UUID)
入口区 UUID (Ingress Zone UUID)（续）
入口区 UUID (Ingress Zone UUID)（续）
入口区 UUID (Ingress Zone UUID)（续）
出口区 UUID (Egress Zone UUID)
出口区 UUID (Egress Zone UUID)

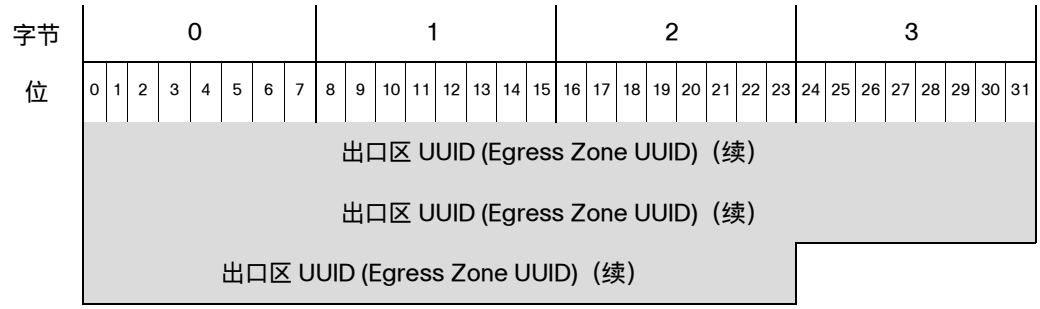


表 B-54　　关联事件 5.0 - 5.0.2 数据字段

字段	数据类型	说明 (Description)
关联块类型 (Correlation Block Type)	uint32	表示随后的关联事件数据块。此字段的值始终为 107。请参阅了解发现（系列 1）块，第 4-60 页。
关联块长度 (Correlation Block Length)	uint32	关联数据块的长度，包括关联块类型和长度的 8 个字节加上随后的关联数据。
设备 ID	uint32	生成关联事件的受管设备或防御中心的内部识别号。值您可以通过请求版本 3 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
（关联）事件秒 ((Correlation) Event Second)	uint32	表示生成关联事件的时间的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
事件 ID (Event ID)	uint32	关联事件标识号。
策略 ID (Policy ID)	uint32	违反的关联策略的标识号。有关如何从数据库获取策略标识号的信息，请参阅服务记录，第 4-14 页。
规则 ID (Rule ID)	uint32	触发策略违规事件的关联规则的标识号。有关如何从数据库获取策略标识号的信息，请参阅服务记录，第 4-14 页。
优先级 (Priority)	uint32	分配给事件的优先级。该项是从 0 到 5 的整数值。
字符串块类型 (String Block Type)	uint32	启动包含关联违规事件说明的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-67 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数，包括字符串块类型的四个字节，字符串块长度的四个字节加上说明中的字节数。
说明 (Description)	字符串	关联事件的说明。
事件类型 (Event Type)	uint8	表示关联事件是由入侵事件、主机发现事件还是用户事件触发的： ▪ 1 - 入侵 ▪ 2 - 主机发现 ▪ 3 - 用户

表 B-54 关联事件 5.0 - 5.0.2 数据字段 （续）

字段	数据类型	说明 (Description)
事件设备 ID (Event 设备 ID)	uint32	生成触发关联事件的事件的设备的标识号。您可以通过请求版本 3 元数据获取设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
签名 ID (Signature ID)	uint32	如果事件为入侵事件，则表示与事件对应的规则识别号。否则，该值为 0。
签名生成器 ID (Signature Generator ID)	uint32	如果事件为入侵事件，则表示生成事件的 Cisco Secure Firewall 系统预处理器或规则引擎的 ID 号码。
（触发器）事件秒 ((Trigger) Event Second)	uint32	表示事件触发关联策略规则的时间的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
（触发器）事件微秒 ((Trigger) Event Microsecond)	uint32	检测到事件的微秒（一秒的百万分之一）增量。
事件 ID (Event ID)	uint32	设备生成的事件的标识号。
事件定义的掩码 (Event Defined Mask)	bits[32]	此字段中的设置位表示后面消息中哪些是有效的字段。有关每个位值的列表，请参阅表 B-55在第 B-354 页。
事件影响标志	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据（位 6）。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。 以下影响级别值映射到“防御中心”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1: ▪ （0，未知）：00X00000 ▪ 红色（1，易受攻击）：XXXX1XXX•XXX1XXXX•X1XXXXXX•1XXXXXXX ▪ 橙色（2，可能易受攻击）：00X00111 ▪ 黄色（3，当前不易受攻击）：00X00011 ▪ 蓝色（4，未知目标）：00X00001

表 B-54 关联事件 5.0 - 5.0.2 数据字段 （续）

字段	数据类型	说明 (Description)
IP 协议 (IP Protocol)	uint8	与事件关联的
网络协议 (Network Protocol)	uint16	与事件关联的网络协议（如适用）。
源 IP (Source IP)	uint8[4]	事件中源主机的 IP 地址，采用 IP 地址八位组。
源主机类型	uint8	源主机的类型： ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥
源 VLAN ID	uint16	源主机的 VLAN 标识号（如适用）。
源操作系统指纹 UUID (Source OS Fingerprint UUID)	uint8[16]	充当源主机操作系统的唯一标识符的指纹 ID 号码。 有关获取映射到指纹 ID 的值的信息，请参阅服务记录，第 4-14 页。
源重要性 (Source Criticality)	uint16	源主机的用户定义临界值： ▪ 0 - 无 ▪ 1 - 低 ▪ 2 - 中 ▪ 3 - 高
源用户 ID (Source User ID)	uint32	系统识别的登录源主机的用户的标识号。
源端口 (Source Port)	uint16	事件中的源端口。
源服务器 ID (Source Server ID)	uint32	源主机上运行的服务器的标识号。
目标 IP 地址：	uint8[4]	与策略违规相关的目标主机的 IP 地址（如适用）。如果无目标 IP 地址，则此值为 0。
目标主机类型 (Destination Host Type)	uint8	目标主机的类型： ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥
目标 VLAN ID (Destination VLAN ID)	uint16	目标主机的 VLAN 标识号（如适用）。
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)	uint8[16]	充当目标主机操作系统的唯一标识符的指纹 ID 号码。 有关获取映射到指纹 ID 的值的信息，请参阅服务记录，第 4-14 页。

表 B-54 关联事件 5.0 - 5.0.2 数据字段 （续）

字段	数据类型	说明 (Description)
目标重要性 (Destination Criticality)	uint16	目标主机的用户定义临界值: ▪ 0 - 无 ▪ 1 - 低 ▪ 2 - 中 ▪ 3 - 高
目标用户 ID (Destination User ID)	uint32	系统识别的登录目标主机的用户的标识号。
目标端口 (Destination Port)	uint16	事件中的目标端口。
目标服务 ID (Destination Service ID)	uint32	源主机上运行的服务器的标识号。
已阻止 (Blocked)	uint8	表示触发入侵事件的数据包发生了什么情况的值。 ▪ 0 - 未丢弃入侵事件 ▪ 1 - 已丢弃入侵事件（当部署为内联、交换或路由式部署时丢弃） ▪ 2 - 如果已向在内联、交换或路由式部署中配置的设备应用入侵策略，则触发事件的数据包本应已丢弃。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当与关联事件相关的入口接口的唯一标识符的接口 ID。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当与关联事件相关的出口接口的唯一标识符的接口 ID。
入口区 UUID (Ingress Zone UUID)	uint8[16]	充当与关联事件相关的入口安全区的唯一标识符的区域 ID。
出口区 UUID (Egress Zone UUID)	uint8[16]	充当与关联事件相关的出口安全区的唯一标识符的区域 ID。

下表对每个事件定义的掩码值进行了说明。

表 B-55 事件定义的值

说明 (Description)	掩码值
事件影响标志 (Event Impact Flags)	0x00000001
IP 协议 (IP Protocol)	0x00000002
网络协议 (Network Protocol)	0x00000004
源 IP (Source IP)	0x00000008
源主机类型 (Source Host Type)	0x00000010
源 VLAN ID (Source VLAN ID)	0x00000020

表 B-55　　事件定义的值 （续）

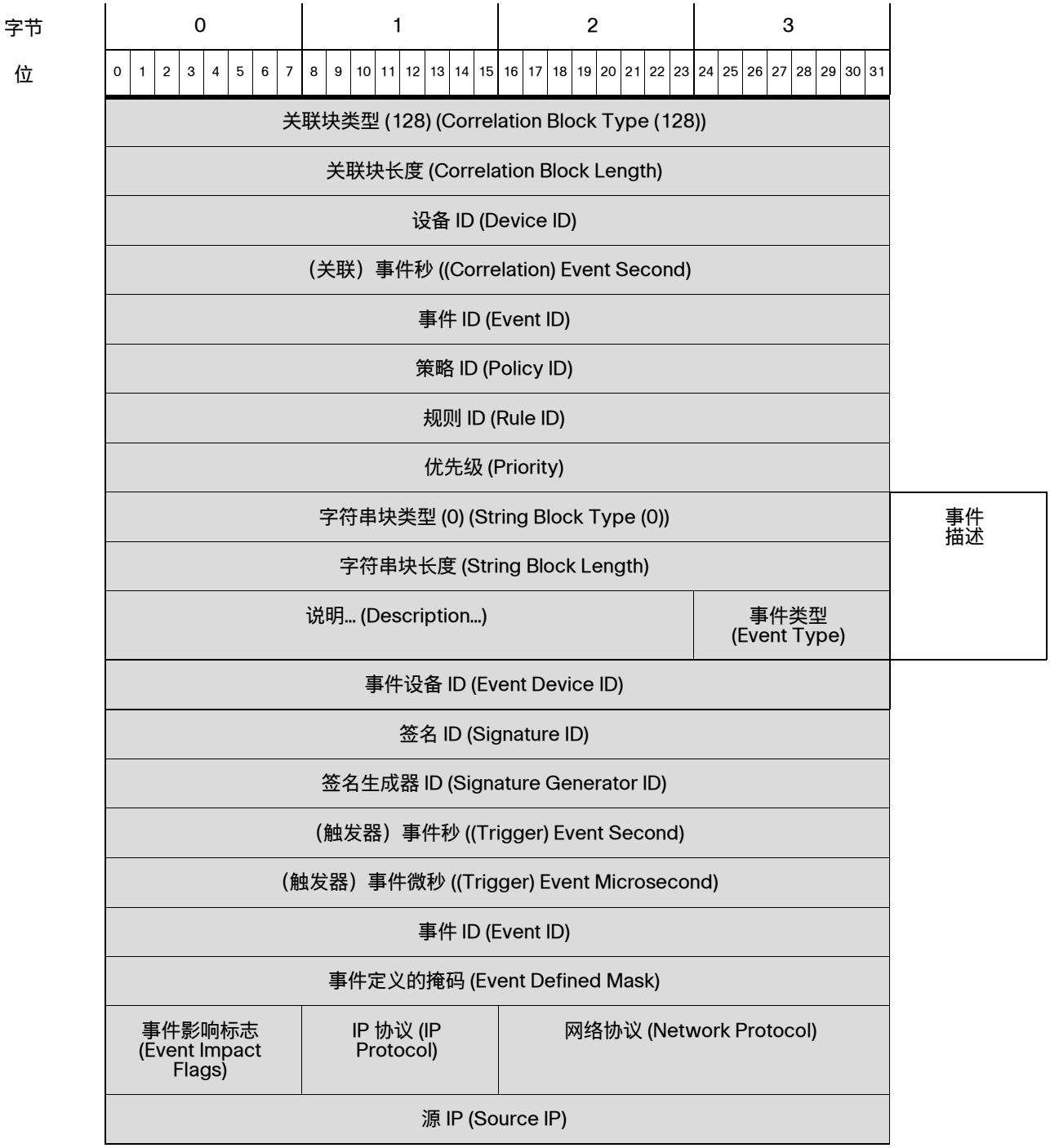
说明 (Description)	掩码值
源指纹 ID (Source Fingerprint ID)	0x00000040
源临界点 (Source Criticality)	0x00000080
源端口 (Source Port)	0x00000100
源服务器 (Source Server)	0x00000200
目标 IP (Destination IP)	0x00000400
目标主机类型 (Destination Host Type)	0x00000800
目标 VLAN ID (Destination VLAN ID)	0x00001000
目标指纹 ID (Destination Fingerprint ID)	0x00002000
目标临界点 (Destination Criticality)	0x00004000
目标端口 (Destination Port)	0x00008000
目标服务器 (Destination Server)	0x00010000
源用户 (Source User)	0x00020000
目标用户 (Destination User)	0x00040000

用于 5.1-5.3.x 的关联事件

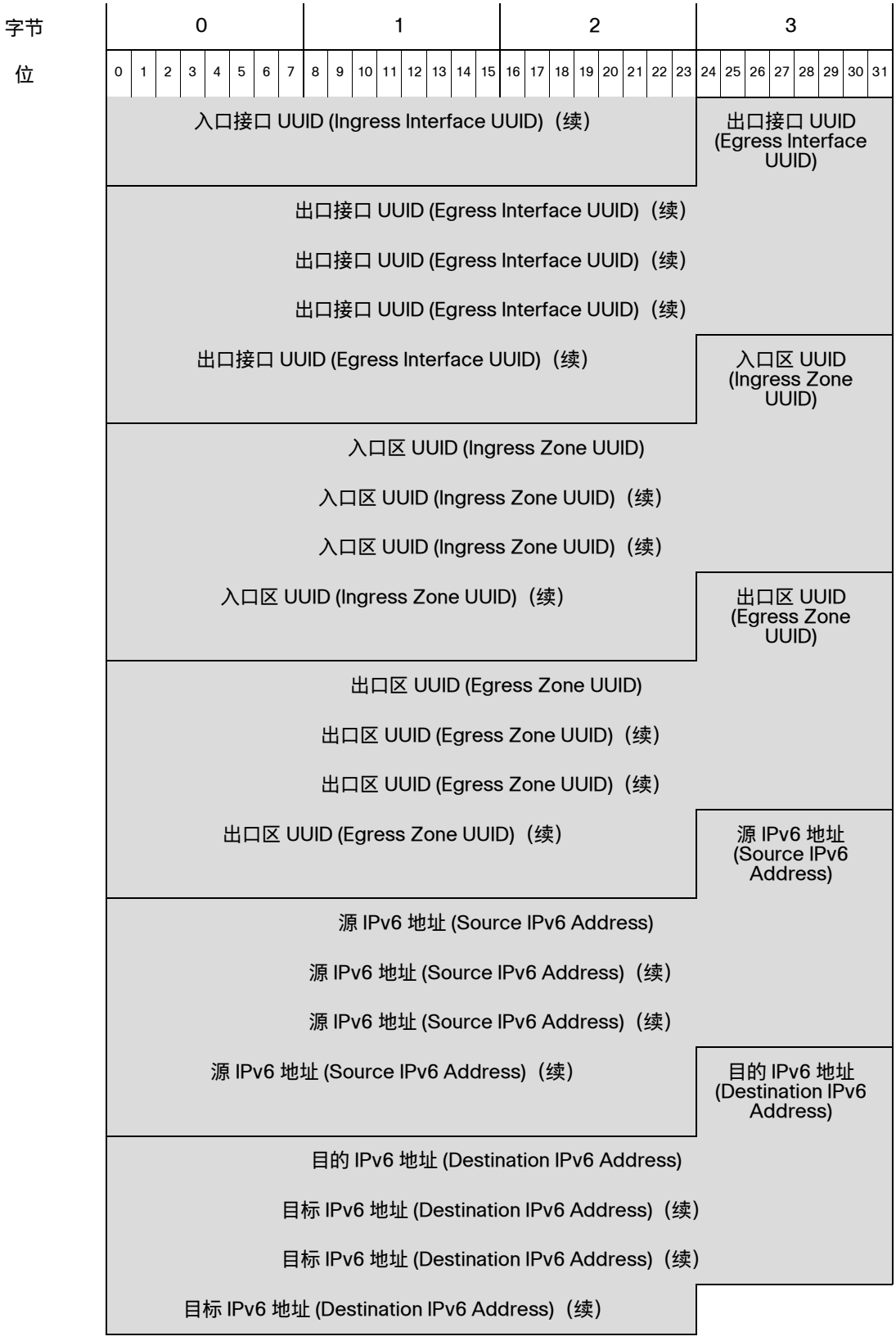
关联事件（在 5.0 之前的版本中称为合规性事件）包含关联策略违规的相关信息。此消息使用标准 eStreamer 消息报头并指定记录类型为 112，随后是类型为系列 1 数据块组中的 128 的关联数据块。数据块类型 128 与其前身（块类型 116）的区别在于其包含 IPv6 支持。

您可以通过扩展请求，仅从 eStreamer 请求 5.1-5.3.x 入侵事件，为此，您需要在流请求消息中请求事件类型代码 31 和版本代码 8（有关提交扩展请求的信息，请参阅提交扩展请求，第 2-4 页）。您可以选择启用初始事件流请求消息的标志字段中的位 23，以包含扩展事件报头。您也可以启用标志字段中的位 20，以包含用户元数据。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (112)（Record Type (112)）															
记录长度 (Record Length)																																
eStreamer 服务器时间戳 (eStreamer Server Timestamp)（在事件中，只有当位 23 已设置时）																																
留作未来使用 (Reserved for Future Use)（在事件中，只有当位 23 已设置时）																																


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
关联块类型 (128) (Correlation Block Type (128))
关联块长度 (Correlation Block Length)
设备 ID (Device ID)
（关联）事件秒 ((Correlation) Event Second)
事件 ID (Event ID)
策略 ID (Policy ID)
规则 ID (Rule ID)
优先级 (Priority)
字符串块类型 (0) (String Block Type (0))
字符串块长度 (String Block Length)
说明... (Description...)
事件类型 (Event Type)
事件描述
事件设备 ID (Event Device ID)
签名 ID (Signature ID)
签名生成器 ID (Signature Generator ID)
（触发器）事件秒 ((Trigger) Event Second)
（触发器）事件微秒 ((Trigger) Event Microsecond)
事件 ID (Event ID)
事件定义的掩码 (Event Defined Mask)
事件影响标志 (Event Impact Flags)
IP 协议 (IP Protocol)
网络协议 (Network Protocol)
源 IP (Source IP)


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
源主机类型 (Source Host Type)
源 VLAN ID (Source VLAN ID)
源操作系统指纹 UUID (Source OS Fprt UUID)
源操作系统指纹 UUID (Source OS Fprt UUID)
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源操作系统指纹 UUID (Source OS Fingerprint UUID)（续）
源重要性 (Source Criticality)
源临界点 (Source Criticality)（续）
源用户 ID (Source User ID)
源用户 ID (Source User ID)（续）
源端口 (Source Port)
源服务器 ID (Source Server ID)
源服务器 ID (Source Server ID)（续）
目标 IP (Destination IP)
目标 IP (Destination IP)（续）
目标主机类型 (Host Type)
目标VLAN ID
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)
目标操作系统指纹 UUID (Dest OS Fingerprint UUID)
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)（续）
目标重要性 (Destination Criticality)
目标用户 ID
目标端口 (Destination Port)
目标服务器 ID (Destination Server ID)
目标服务器 ID (Destination Server ID)（续）
已阻止 (Blocked)
入口接口 UUID (Ingress Interface UUID)
入口接口 UUID (Ingress Interface UUID)（续）
入口接口 UUID (Ingress Interface UUID)（续）
入口接口 UUID (Ingress Interface UUID)（续）


字节
位
0
1
2
3
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
入口接口 UUID (Ingress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)
出口接口 UUID (Egress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)（续）
出口接口 UUID (Egress Interface UUID)（续）
入口区 UUID (Ingress Zone UUID)
入口区 UUID (Ingress Zone UUID)（续）
入口区 UUID (Ingress Zone UUID)（续）
入口区 UUID (Ingress Zone UUID)（续）
出口区 UUID (Egress Zone UUID)
出口区 UUID (Egress Zone UUID)（续）
出口区 UUID (Egress Zone UUID)（续）
出口区 UUID (Egress Zone UUID)（续）
源 IPv6 地址 (Source IPv6 Address)
源 IPv6 地址 (Source IPv6 Address)（续）
源 IPv6 地址 (Source IPv6 Address)（续）
源 IPv6 地址 (Source IPv6 Address)（续）
目的 IPv6 地址 (Destination IPv6 Address)
目标 IPv6 地址 (Destination IPv6 Address)（续）
目标 IPv6 地址 (Destination IPv6 Address)（续）
目标 IPv6 地址 (Destination IPv6 Address)（续）

请注意，记录结构包含一个字符串块类型，该数据块为系列 1 中的数据块。有关系列 1 数据块的信息，请参阅了解发现（系列 1）块，第 4-60 页。

表 B-56　　关联事件 5.1-5.3.x 数据字段

字段	数据类型	说明 (Description)
关联块类型 (Correlation Block Type)	uint32	表示随后的关联事件数据块。此字段的值始终为 128。请参阅了解发现（系列 1）块，第 4-60 页。
关联块长度 (Correlation Block Length)	uint32	关联数据块的长度，包括关联块类型和长度的 8 个字节加上随后的关联数据。
设备 ID (Device ID)	uint32	生成关联事件的受管设备或防御中心的内部识别号。值您可以通过请求版本 3 元数据获取受管设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
（关联）事件秒 ((Correlation) Event Second)	uint32	表示生成关联事件的时间的 UNIX 时间戳（自 1970/01/01 起经过的秒数）。
事件 ID (Event ID)	uint32	关联事件标识号。
策略 ID (Policy ID)	uint32	违反的关联策略的标识号。有关如何从数据库获取策略标识号的信息，请参阅服务记录，第 4-14 页。
规则 ID (Rule ID)	uint32	触发策略违规事件的关联规则的标识号。有关如何从数据库获取策略标识号的信息，请参阅服务记录，第 4-14 页。
优先级 (Priority)	uint32	分配给事件的优先级。该项是从 0 到 5 的整数值。
字符串块类型 (String Block Type)	uint32	启动包含关联违规事件说明的字符串数据块。此值始终设置为 0。有关字符串块的详细信息，请参阅字符串数据块，第 4-67 页。
字符串块长度 (String Block Length)	uint32	事件说明字符串块中的字节数，包括字符串块类型的四个字节，字符串块长度的四个字节加上说明中的字节数。
说明 (Description)	字符串	关联事件的说明。
事件类型 (Event Type)	uint8	表示关联事件是由入侵事件、主机发现事件还是用户事件触发的: ▪ 1 - 入侵 ▪ 2 - 主机发现 ▪ 3 - 用户
事件设备 ID (Event Device ID)	uint32	生成触发关联事件的事件的设备的标识号。您可以通过请求版本 3 元数据获取设备名称。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
签名 ID (Signature ID)	uint32	如果事件为入侵事件，则表示与事件对应的规则识别号。否则，该值为 0。
签名生成器 ID (Signature Generator ID)	uint32	如果事件为入侵事件，则表示生成事件的 Cisco Secure Firewall 系统预处理器或规则引擎的 ID 号码。

表 B-56 关联事件 5.1-5.3.x 数据字段 （续）

字段	数据类型	说明 (Description)
（触发器）事件秒 ((Trigger) Event Second)	uint32	表示事件触发关联策略规则的时间的 UNIX 时间戳（自 1970/01/01 起经过的秒数）
（触发器）事件微秒 ((Trigger) Event Microsecond)	uint32	检测到事件的微秒（一秒的百万分之一）增量。
事件 ID (Event ID)	uint32	思科设备生成的事件的标识号。
事件定义的掩码 (Event Defined Mask)	bits[32]	此字段中的设置位表示后面消息中哪些是有效的字段。有关每个位值的列表，请参阅表 B-55在第 B-354 页。
事件影响标志	bits[8]	事件的影响标志值。低阶八位表示影响级别。值包括: ▪ 0x01（位 0）- 源或目标主机位于系统监控的网络中。 ▪ 0x02（位 1）- 源或目标主机存在于网络映射中。 ▪ 0x04（位 2）- 源或目标主机在事件中的端口上运行服务器（如果为 TCP 或 UDP）或使用 IP 协议。 ▪ 0x08（位 3）- 有漏洞映射到事件中的源或目标主机的操作系统。 ▪ 0x10（位 4）- 有漏洞映射到事件中检测到的服务器。 ▪ 0x20（位 5）- 事件导致受管设备丢弃会话（仅当设备在内联、交换或路由式部署中运行时才使用）。对应于 Cisco Secure Firewall 系统 Web 界面中的受阻状态。 ▪ 0x40（位 6）- 生成了此事件的规则包含将影响标志设置为红色的规则元数据。源或目标主机可能受到病毒、特洛伊木马或其他恶意软件片段的危害。 ▪ 0x80（位 7）- 有漏洞映射到事件中检测到的客户端。（仅限版本 5.0+） 以下影响级别值映射到“防御中心”(Defense Center) 上的特定优先级中。x 表示值可以为 0 或 1: ▪ （0，未知）： 00X00000 ▪ 红色（1，易受攻击）： XXXX1XXX、XXX1XXXX、X1XXXXXX、1XXXXXXX （仅限版本 5.0+） ▪ 橙色（2，可能易受攻击）： 00X0011X ▪ 黄色（3，当前不易受攻击）： 00X0001X ▪ 蓝色（4，未知目标）： 00X00001
IP 协议 (IP Protocol)	uint8	与事件关联的
网络协议 (Network Protocol)	uint16	与事件关联的网络协议（如适用）。
源 IP 地址 (Source IP Address)	uint8[4]	保留此字段，但不再填充。源 IPv4 地址存储在源 IPv6 地址字段中。有关详细信息，请参阅IP 地址，第 1-4 页。

表 B-56　　关联事件 5.1-5.3.x 数据字段 （续）

字段	数据类型	说明 (Description)
源主机类型	uint8	源主机的类型: ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥
源 VLAN ID	uint16	源主机的 VLAN 标识号（如适用）。
源操作系统指纹 UUID (Source OS Fingerprint UUID)	uint8[16]	充当源主机操作系统的唯一标识符的指纹 ID 号码。 有关获取映射到指纹 ID 的值的信息，请参阅服务记录，第 4-14 页。
源重要性 (Source Criticality)	uint16	源主机的用户定义临界值: ▪ 0 - 无 ▪ 1 - 低 ▪ 2 - 中 ▪ 3 - 高
源用户 ID (Source User ID)	uint32	系统识别的登录源主机的用户的标识号。
源端口 (Source Port)	uint16	事件中的源端口。
源服务器 ID (Source Server ID)	uint32	源主机上运行的服务器的标识号。
目标 IP 地址:	uint8[4]	保留此字段，但不再填充。目标 IPv4 地址存储在目标 IPv6 地址字段中。有关详细信息，请参阅IP 地址，第 1-4 页。
目标主机类型 (Destination Host Type)	uint8	目标主机的类型: ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥
目标 VLAN ID (Destination VLAN ID)	uint16	目标主机的 VLAN 标识号（如适用）。
目标操作系统指纹 UUID (Destination OS Fingerprint UUID)	uint8[16]	充当目标主机操作系统的唯一标识符的指纹 ID 号码。 有关获取映射到指纹 ID 的值的信息，请参阅服务记录，第 4-14 页。
目标重要性 (Destination Criticality)	uint16	目标主机的用户定义临界值: ▪ 0 - 无 ▪ 1 - 低 ▪ 2 - 中 ▪ 3 - 高
目标用户 ID (Destination User ID)	uint32	系统识别的登录目标主机的用户的标识号。

表 B-56 关联事件 5.1-5.3.x 数据字段 （续）

字段	数据类型	说明 (Description)
目标端口 (Destination Port)	uint16	事件中的目标端口。
目标服务 ID (Destination Service ID)	uint32	源主机上运行的服务器的标识号。
已阻止 (Blocked)	uint8	表示触发入侵事件的数据包发生了什么情况的值。 ▪ 0 - 未丢弃入侵事件 ▪ 1 - 已丢弃入侵事件（当部署为内联、交换或路由式部署时丢弃） ▪ 2 - 如果已向在内联、交换或路由式部署中配置的设备应用入侵策略，则触发事件的数据包本应已丢弃。
入口接口 UUID (Ingress Interface UUID)	uint8[16]	充当与关联事件相关的入口接口的唯一标识符的接口 ID。
出口接口 UUID (Egress Interface UUID)	uint8[16]	充当与关联事件相关的出口接口的唯一标识符的接口 ID。
入口区 UUID (Ingress Zone UUID)	uint8[16]	充当与关联事件相关的入口安全区的唯一标识符的区域 ID。
出口区 UUID (Egress Zone UUID)	uint8[16]	充当与关联事件相关的出口安全区的唯一标识符的区域 ID。
源 IPv6 地址 (Source IPv6 Address)	uint8[16]	事件中源主机的 IP 地址，采用 IPv6 地址八位组。
目的 IPv6 地址	uint8[16]	事件中目标主机的 IP 地址，采用 IPv6 地址八位组。

旧版主机数据结构

要请求这些结构，必须使用主机请求消息。要请求旧版结构，主机请求消息必须使用较旧的格式。有关详细信息，请参阅主机请求消息格式，第 2-24 页。

以下主题介绍旧版主机数据结构，包括主机配置文件结构和完整主机配置文件结构：

完整主机配置文件数据块 5.0 - 5.0.2

用于版本 5.0 - 5.0.2 的完整主机配置文件数据块包含一整套主机说明数据。其格式如下图中所示，并在下表中进行说明。请注意，除列表数据块之外，该图未显示封装数据块的字段。这些封装数据块在了解发现和连接数据结构，第 4-1 页中单独进行说明。完整主机配置文件数据块的块类型值为 111。

注释　下图中块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

	字节	0								1								2								3							
	位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
		完整主机配置文件数据块 (111) (Full Host Profile Data Block (111))																															
		数据块长度 (Data Block Length)																															
		IP 地址 (IP Addresses)																															
		跳数 (Hops)								通用列表块类型 (31) (Generic List Block Type (31))																							
		通用列表块类型 (Generic List Block Type)（续）								通用列表块长度 (Generic List Block Length)																							
源自操作系统的指纹 (OS Derived Fingerprints)		通用列表块长度 (Generic List Block Length)（续）								操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																							
		操作系统指纹块类型 (130) (OS Fingerprint Block Type (130))*（续）								操作系统指纹块长度 (Operating System Fingerprint Block Length)																							
		操作系统指纹块长度 (OS Fingerprint Block Length)（续）								源自操作系统的指纹数据... (Operating System Derived Fingerprint Data...)																							
		通用列表块类型 (31) (Generic List Block Type (31))																															
		通用列表块长度 (Generic List Block Length)																															
服务器指纹 (Server Fingerprints)		操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
		操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
		操作系统服务器指纹数据... (Operating System Server Fingerprint Data...)																															
		通用列表块类型 (31) (Generic List Block Type (31))																															
		通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
客户端指纹	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统客户端指纹数据... (Operating System Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 1 (VDB Native Fingerprints 1)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 2 (VDB Native Fingerprints 2)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
用户指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户指纹数据... (Operating System User Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
扫描指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统扫描指纹数据... (Operating System Scan Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
应用指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统应用指纹数据... (Operating System Application Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
冲突指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统冲突指纹数据... (Operating System Conflict Fingerprint Data...)																															
(TCP) 完整服务器数据	列表块类型 (11)... (List Block Type (11))...																															
	列表块长度... (List Block Length)...																															
	(TCP) 完整服务器数据块 (104) ((TCP) Full Server Data Blocks (104))*																															
(UDP) 完整服务器数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	(UDP) 完整服务器数据块 (104) ((UDP) Full Server Data Blocks (104))*																															
网络协议数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（网络）协议数据块 (4) ((Network) Protocol Data Blocks (4))*																															
传输协议数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（传输）协议数据块 (4) ((Transport) Protocol Data Blocks (4))*																															
MAC 地址数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	主机 MAC 地址数据块 (95) (Host MAC Address Data Blocks (95))*																															
	上次查看时间 (Last Seen)																															
	主机类型 (Host Type)																															
	业务临界点 (Business Criticality)																VLAN ID															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	VLAN 类型 (VLAN Type)								VLAN 优先级 (VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))															
主机客户端数据	通用列表块类型 (Generic List Block Type)（续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length)（续）																完整主机客户端应用数据块 (112) (Full Host Client Application Data Blocks (112))*															
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称字符串... (NetBIOS Name String...)																															
说明 (Description) 数据	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	注释字符串... (Notes String....)																															
(VDB) 主机漏洞 ((VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(VDB) 主机漏洞数据块 (85) ((VDB) Host Vulnerability Data Blocks (85))*																															
（第三方/VDB）主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方/VDB）主机漏洞数据块 (85) ((Third Party/VDB) Host Vulnerability Data Blocks (85))*																															
第三方扫描主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方扫描）具有原始漏洞 ID 的主机漏洞数据块 (85) ((Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85))*																															
属性值数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	属性值数据块 (Attribute Value Data Blocks) *																															

下表对用于 5.0 - 5.0.2 记录的完整主机配置文件的组件进行了说明。

表 B-57　　完整主机配置文件记录 5.0 - 5.0.2 字段

字段	数据类型	说明 (Description)
IP 地址	uint8[4]	主机的 IP 地址，采用 IP 地址八位组。
跳数 (Hops)	uint8	从主机到设备的网络跳数。
通用列表块类型 (Generic List Block	uint32	启动由传送源自主机的现有指纹的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
源自操作系统的指纹数据块 (Operating System Derived Fingerprint Data Blocks) *	变量	包含源自主机的现有指纹的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用思科 VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-57 完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明 (Description)
操作系统指纹 (VDB) 本机指纹 1) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks) *	变量	包含用思科漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用思科 VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 2) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks) *	变量	包含用思科漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用户添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（用户指纹）数据块 (Operating System Fingerprint (User Fingerprint) Data Blocks) *	变量	包含用户添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送漏洞扫描仪添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（扫描指纹）数据块 (Operating System Fingerprint (Scan Fingerprint) Data Blocks) *	变量	包含漏洞扫描仪添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送应用添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。

表 B-57　　完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（应用指纹）数据块 (Operating System Fingerprint (Application Fingerprint) Data Blocks) *	变量	包含应用添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送通过指纹冲突解决选择的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（冲突指纹）数据块 (Operating System Fingerprint (Conflict Fingerprint) Data Blocks) *	变量	包含通过指纹冲突解决选择的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(TCP) 完整服务器数据块 ((TCP) Full Server Data Blocks) *	变量	传输主机上的 TCP有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-141 页。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(UDP) 完整服务器数据块 ((UDP) Full Server Data Blocks) *	变量	传输主机上的 UDP 子服务器相关数据的完整主机数据块列表。有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-141 页。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（网络）协议数据块 ((Network) Protocol Data Blocks) *	变量	传输主机上的网络协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-72 页。

表 B-57 完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明 (Description)
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（传输）协议数据块 ((Transport) Protocol Data Blocks) *	变量	传送主机上的传输协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动包含主机 MAC 地址数据块的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装主机 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks) *	变量	主机 MAC 地址数据块列表。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-113 页。
上次查看时间 (Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。值包括: ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥 ▪ 3 - NAT（网络地址转换设备） ▪ 4 - LB（负载均衡器）
业务临界点 (Business Criticality)	uint16	表示主机到业务的临界点。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block	uint32	启动由传送客户端应用数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
完整主机客户端应用数据块 (Full Host Client Application Data Blocks) *	变量	客户端应用数据块列表。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-155 页。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。

表 B-57　完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动主机注释的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	注释字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上注释字符串中的字节数。
说明 (Description)	字符串	包含主机的主机属性注释的内容。
通用列表块类型 (Generic List Block	uint32	启动由传送 VDB 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks) *	变量	在思科漏洞数据库 (VDB) 中识别的漏洞的主机漏洞数据块列表。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
通用列表块类型 (Generic List Block	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方/VDB）主机漏洞数据块 ((Third Party/VDB) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪且包含已收录到思科漏洞数据库 (VDB) 中的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
通用列表块类型 (Generic List Block	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方扫描）主机漏洞数据块 ((Third Party Scan) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪的主机漏洞数据块。请注意，这些数据块的主机漏洞 ID 为第三方扫描仪 ID，而不是思科检测到的 ID。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
列表块类型 (List Block Type)	uint32	启动由传送属性数据的属性值数据块组成的列表数据块。值始终为 11。

表 B-57　　完整主机配置文件记录 5.0 - 5.0.2 字段 （续）

字段	数据类型	说明 (Description)
列表块长度 (List Block Length)	uint32	列表数据块中的字节数，包括列表报头以及所有封装数据块。
属性值数据块 (Attribute Value Data Blocks) *	变量	属性值数据块列表。有关此列表中的数据块的说明，请参阅属性值数据块，第 4-79 页。

完整主机配置文件数据块 5.1.1

用于版本 5.1.1 的完整主机配置文件数据块包含一整套主机说明数据。其格式如下图中所示，并在下表中进行说明。请注意，除列表数据块之外，该图未显示封装数据块的字段。这些封装数据块在了解发现和连接数据结构，第 4-1 页中单独进行说明。完整主机配置文件数据块的块类型值为 135。它否决了数据块 111。

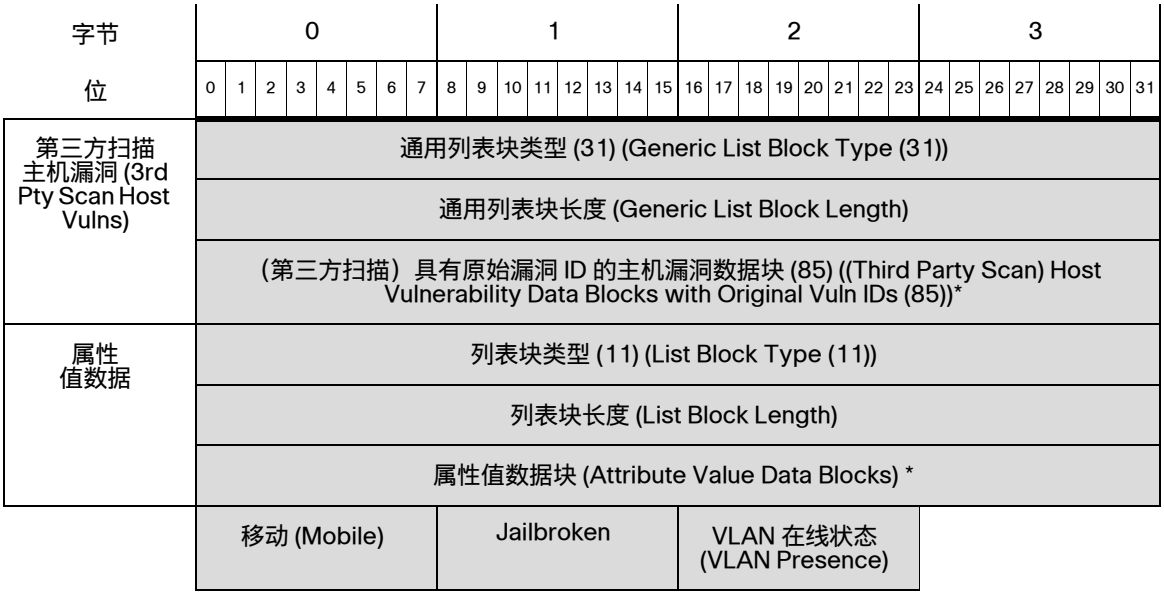
注释　下图中块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	完整主机配置文件数据块 (135) (Full Host Profile Data Block (135))																															
	数据块长度 (Data Block Length)																															
	IP 地址 (IP Addresses)																															
	跳数 (Hops)								通用列表块类型 (31) (Generic List Block Type (31))																							
	通用列表块类型 (Generic List Block Type)（续）								通用列表块长度 (Generic List Block Length)																							
源自操作系统的指纹 (OS Derived Fingerprints)	通用列表块长度 (Generic List Block Length)（续）								操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																							
	操作系统指纹块类型 (130) (OS Fingerprint Block Type (130))*（续）								操作系统指纹块长度 (Operating System Fingerprint Block Length)																							
	操作系统指纹块长度 (OS Fingerprint Block Length)（续）								源自操作系统的指纹数据... (Operating System Derived Fingerprint Data...)																							
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
服务器指纹 (Server Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统服务器指纹数据... (Operating System Server Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
客户端指纹	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统客户端指纹数据... (Operating System Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 1 (VDB Native Fingerprints 1)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 2 (VDB Native Fingerprints 2)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
用户指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户指纹数据... (Operating System User Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
扫描指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统扫描指纹数据... (Operating System Scan Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
应用指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统应用指纹数据... (Operating System Application Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
冲突指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统冲突指纹数据... (Operating System Conflict Fingerprint Data...)																															
(TCP) 完整服务器数据	列表块类型 (11)... (List Block Type (11))...																															
	列表块长度... (List Block Length)...																															
	(TCP) 完整服务器数据块 (104) ((TCP) Full Server Data Blocks (104))*																															
(UDP) 完整服务器数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	(UDP) 完整服务器数据块 (104) ((UDP) Full Server Data Blocks (104))*																															
网络协议数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（网络）协议数据块 (4) ((Network) Protocol Data Blocks (4))*																															
传输协议数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（传输）协议数据块 (4) ((Transport) Protocol Data Blocks (4))*																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
MAC 地址数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	主机 MAC 地址数据块 (95) (Host MAC Address Data Blocks (95))*																															
	上次查看时间 (Last Seen)																															
	主机类型 (Host Type)																															
	业务临界点 (Business Criticality)																VLAN ID															
	VLAN 类型 (VLAN Type)								VLAN 优先级 (VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))															
主机客户端数据	通用列表块类型 (Generic List Block Type)（续）																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length)（续）																完整主机客户端应用数据块 (112) (Full Host Client Application Data Blocks (112))*															
NetBIOS 名称 (Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称字符串... (NetBIOS Name String...)																															
说明 (Description) 数据	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	注释字符串... (Notes String....)																															
(VDB) 主机漏洞 ((VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(VDB) 主机漏洞数据块 (85) ((VDB) Host Vulnerability Data Blocks (85))*																															
(第三方/VDB) 主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方/VDB）主机漏洞数据块 (85) ((Third Party/VDB) Host Vulnerability Data Blocks (85))*																															



下表对用于 5.1.1 记录的完整主机配置文件的组件进行了说明。

表 B-58 完整主机配置文件记录 5.1.1 字段

字段	数据类型	说明 (Description)
IP 地址	uint8[4]	主机的 IP 地址，采用 IP 地址八位组。
跳数 (Hops)	uint8	从主机到设备的网络跳数。
通用列表块类型 (Generic List Block	uint32	启动由传送源自主机的现有指纹的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
源自操作系统的指纹数据块 (Operating System Derived Fingerprint Data Blocks) *	变量	包含源自主机的现有指纹的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。

表 B-58　完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用思科 VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 1) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks) *	变量	包含用思科漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用思科 VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 2) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks) *	变量	包含用思科漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用户添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（用户指纹）数据块 (Operating System Fingerprint (User Fingerprint) Data Blocks) *	变量	包含用户添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送漏洞扫描仪添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。

表 B-58 完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（扫描指纹）数据块 (Operating System Fingerprint (Scan Fingerprint) Data Blocks) *	变量	包含漏洞扫描仪添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送应用添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（应用指纹）数据块 (Operating System Fingerprint (Application Fingerprint) Data Blocks) *	变量	包含应用添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送通过指纹冲突解决选择的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（冲突指纹）数据块 (Operating System Fingerprint (Conflict Fingerprint) Data Blocks) *	变量	包含通过指纹冲突解决选择的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
列表块类型 (List Block Type)	uint32	启动由传送TCP服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(TCP) 完整服务器数据块 ((TCP) Full Server Data Blocks) *	变量	传输主机上的 TCP有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-141 页。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。

表 B-58　完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明 (Description)
(UDP) 完整服务器数据块 ((UDP) Full Server Data Blocks) *	变量	传输主机上的 UDP 子服务器相关数据的完整主机数据块列表。有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-141 页。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（网络）协议数据块 ((Network)Protocol Data Blocks) *	变量	传输主机上的网络协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（传输）协议数据块 ((Transport) Protocol Data Blocks) *	变量	传送主机上的传输协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动包含主机 MAC 地址数据块的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装主机 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks) *	变量	主机 MAC 地址数据块列表。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-113 页。
上次查看时间 (Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。值包括: ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥 ▪ 3 - NAT（网络地址转换设备） ▪ 4 - LB（负载均衡器）
业务临界点 (Business Criticality)	uint16	表示主机到业务的临界点。
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。

表 B-58 完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明 (Description)
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block	uint32	启动由传送客户端应用数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
完整主机客户端应用数据块 (Full Host Client Application Data Blocks) *	变量	客户端应用数据块列表。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-155 页。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动主机注释的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	注释字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上注释字符串中的字节数。
说明 (Description)	字符串	包含主机的主机属性注释的内容。
通用列表块类型 (Generic List Block	uint32	启动由传送 VDB 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks) *	变量	在思科漏洞数据库 (VDB) 中识别的漏洞的主机漏洞数据块列表。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
通用列表块类型 (Generic List Block	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方/VDB）主机漏洞数据块 ((Third Party/VDB) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪且包含已收录到思科漏洞数据库 (VDB) 中的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。

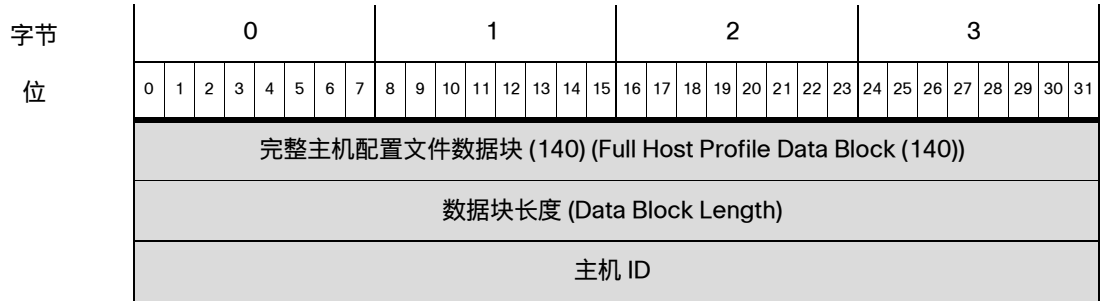
表 B-58　　完整主机配置文件记录 5.1.1 字段 （续）

字段	数据类型	说明 (Description)
通用列表块类型 (Generic List Block	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方扫描）主机漏洞数据块 ((Third Party Scan) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪的主机漏洞数据块。请注意，这些数据块的主机漏洞 ID 为第三方扫描仪 ID，而不是思科检测到的 ID。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
列表块类型 (List Block Type)	uint32	启动由传送属性数据的属性值数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表数据块中的字节数，包括列表报头以及所有封装数据块。
属性值数据块 (Attribute Value Data Blocks) *	变量	属性值数据块列表。有关此列表中的数据块的说明，请参阅属性值数据块，第 4-79 页。
移动 (Mobile)	uint8	指示操作系统是否在移动设备上运行的一个真假标志。
Jailbroken	uint8	指示移动设备操作系统是否被越狱的一个真假标志。
VLAN 在线状态 (VLAN Presence)	uint8	表示是否存在 VLAN: ▪ 0 - 是 ▪ 1 - 否

完整主机配置文件数据块 5.2.x

用于版本 5.2.x 的完整主机配置文件数据块包含一整套主机说明数据。其格式如下图中所示，并在下表中进行说明。请注意，除列表数据块之外，该图未显示封装数据块的字段。这些封装数据块在了解发现和连接数据结构，第 4-1 页中单独进行说明。完整主机配置文件数据块的块类型值为 140。它替代了之前的版本，之前版本的块类型为 135。

注释　下图中块名称旁边的星号 (*) 表示可能会出现多个数据块实例。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	主机 ID (Host ID)（续）																															
	主机 ID (Host ID)（续）																															
	主机 ID (Host ID)（续）																															
IP 地址 (IP Address)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	IP 地址数据块 (143) (IP Address Data Blocks (143))*																															
	跳数 (Hops)								通用列表块类型 (31) (Generic List Block Type (31))																							
	通用列表块类型 (Generic List Block Type)（续）								通用列表块长度 (Generic List Block Length)																							
源自操作系统的指纹 (OS Derived Fingerprints)	通用列表块长度 (Generic List Block Length)（续）								操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																							
	操作系统指纹块类型 (130) (OS Fingerprint Block Type (130))*（续）								操作系统指纹块长度 (Operating System Fingerprint Block Length)																							
	操作系统指纹块长度 (OS Fingerprint Block Length) (续)								源自操作系统的指纹数据... (Operating System Derived Fingerprint Data...)																							
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
服务器指纹 (Server Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统服务器指纹数据... (Operating System Server Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
客户端指纹	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统客户端指纹数据... (Operating System Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 1 (VDB Native Fingerprints 1)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机指纹 2 (VDB Native Fingerprints 2)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
用户指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户指纹数据... (Operating System User Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
扫描指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统扫描指纹数据... (Operating System Scan Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
应用指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统应用指纹数据... (Operating System Application Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
冲突指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统冲突指纹数据... (Operating System Conflict Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
移动 (Mobile) 指纹 (Mobile Device Fingerprint)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统移动指纹数据... (Operating System Mobile Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
IPv6 服务器指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 IPv6 服务器指纹数据... (Operating System IPv6 Server Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
Ipv6 客户端指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 Ipv6 客户端指纹数据... (Operating System Ipv6 Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
Ipv6 DHCP 指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 IPv6 DHCP 指纹数据... (Operating System IPv6 DHCP Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
用户代理指纹 (User Agent Fingerprint)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户代理指纹数据... (Operating System User Agent Fingerprint Data...)																															
(TCP) 完整服务器数据	列表块类型 (11)... (List Block Type (11))...																															
	列表块长度... (List Block Length)...																															
	(TCP) 完整服务器数据块 (104) ((TCP) Full Server Data Blocks (104))*																															
(UDP) 完整服务器数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	(UDP) 完整服务器数据块 (104) ((UDP) Full Server Data Blocks (104))*																															
网络协议数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（网络）协议数据块 (4) ((Network) Protocol Data Blocks (4))*																															
传输协议数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	（传输）协议数据块 (4) ((Transport) Protocol Data Blocks (4))*																															
MAC 地址数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	主机 MAC 地址数据块 (95) (Host MAC Address Data Blocks (95))*																															
	上次查看时间 (Last Seen)																															
	主机类型 (Host Type)																															
	业务临界点 (Business Criticality)																VLAN ID															
	VLAN 类型 (VLAN Type)								VLAN 优先级 (VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))														
主机客户端数据	通用列表块类型 (Generic List Block Type)（续）																通用列表块长度 (Generic List Block Length)														
	通用列表块长度 (Generic List Block Length)（续）																完整主机客户端应用数据块 (112) (Full Host Client Application Data Blocks (112))*														

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetBIOS 名称 (NetBIOS Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
名称 (Name)	NetBIOS 名称字符串... (NetBIOS Name String...)																															
说明 (Description) 数据	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	注释字符串... (Notes String....)																															
(VDB) 主机漏洞 ((VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(VDB) 主机漏洞数据块 (85) ((VDB) Host Vulnerability Data Blocks (85))*																															
(第三方/VDB) 主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(第三方/VDB) 主机漏洞数据块 (85) ((Third Party/VDB) Host Vulnerability Data Blocks (85))*																															
第三方扫描主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(第三方扫描) 具有原始漏洞 ID 的主机漏洞数据块 (85) ((Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85))*																															
属性值数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	属性值数据块 (Attribute Value Data Blocks) *																															
	移动 (Mobile)								Jailbroken																							

下表对用于 5.2.x 记录的完整主机配置文件的组件进行了说明。

表 B-59　　完整主机配置文件记录 5.2.x 字段

字段	数据类型	说明 (Description)
主机 ID	uint8[16]	主机的唯一 ID 号码。这是一个 UUID。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务数据的 IP 地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装 IP 地址数据块的长度。
IP 地址 (IP Address)	变量	主机的 IP 地址以及上次看到每个 IP 地址的时间。有关此数据块的说明，请参阅主机 IP 地址数据块，第 4-95 页。
跳数 (Hops)	uint8	从主机到设备的网络跳数。
通用列表块类型 (Generic List Block	uint32	启动由传送源自主机的现有指纹的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
源自操作系统的指纹数据块 (Operating System Derived Fingerprint Data Blocks) *	变量	包含源自主机的现有指纹的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-59 完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用思科 VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 1) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks) *	变量	包含用思科漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用思科 VDB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 2) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks) *	变量	包含用思科漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用户添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-59　完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
操作系统指纹（用户指纹）数据块(Operating System Fingerprint (User Fingerprint) Data Blocks) *	变量	包含用户添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型(Generic List Block	uint32	启动由传送漏洞扫描仪添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度(Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（扫描指纹）数据块(Operating System Fingerprint (Scan Fingerprint) Data Blocks) *	变量	包含漏洞扫描仪添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型(Generic List Block	uint32	启动由传送应用添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度(Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（应用指纹）数据块(Operating System Fingerprint (Application Fingerprint) Data Blocks) *	变量	包含应用添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型(Generic List Block	uint32	启动由传送通过指纹冲突解决选择的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度(Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-59 完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
操作系统指纹（冲突指纹）数据块(Operating System Fingerprint (Conflict Fingerprint) Data Blocks) *	变量	包含通过指纹冲突解决选择的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型(Generic List Block	uint32	启动由传送移动设备指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度(Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（移动）数据块(Operating System Fingerprint (Mobile) Data Blocks) *	变量	包含移动设备主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型(Generic List Block	uint32	启动由传送用 IPv6 服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度(Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（IPv6 服务器指纹）数据块(Operating System Fingerprint (IPv6 Server Fingerprint) Data Blocks) *	变量	包含用 IPv6 服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型(Generic List Block	uint32	启动由传送用 IPv6 客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度(Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 B-59　完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
操作系统指纹（IPv6 客户端指纹）数据块 (Operating System Fingerprint (IPv6 Client Fingerprint) Data Blocks) *	变量	包含用 IPv6 客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 IPv6 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (IPv6 DHCP) 数据块 (Operating System Fingerprint (IPv6 DHCP) Data Blocks) *	变量	包含用 IPv6 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用用户代理指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（用户代理）数据块 (Operating System Fingerprint (User Agent) Data Blocks) *	变量	包含用用户代理指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(TCP) 完整服务器数据块 ((TCP) Full Server Data Blocks) *	变量	传输主机上的 TCP有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-141 页。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。

表 B-59　完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整服务器数据块的长度。
(UDP) 完整服务器数据块 ((UDP) Full Server Data Blocks) *	变量	传输主机上的 UDP 子服务器相关数据的完整主机数据块列表。有关此数据块的说明，请参阅完整主机服务器数据块 4.10.0+，第 4-141 页。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（网络）协议数据块 ((Network) Protocol Data Blocks) *	变量	传输主机上的网络协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
（传输）协议数据块 ((Transport) Protocol Data Blocks) *	变量	传送主机上的传输协议相关数据的协议数据块列表。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动包含主机 MAC 地址数据块的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装主机 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks) *	变量	主机 MAC 地址数据块列表。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-113 页。
上次查看时间 (Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。值包括： ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥 ▪ 3 - NAT（网络地址转换设备） ▪ 4 - LB（负载均衡器）
业务临界点 (Business Criticality)	uint16	表示主机到业务的临界点。

表 B-59　完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block	uint32	启动由传送客户端应用数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
完整主机客户端应用数据块 (Full Host Client Application Data Blocks) *	变量	客户端应用数据块列表。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-155 页。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动主机注释的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	注释字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上注释字符串中的字节数。
说明 (Description)	字符串	包含主机的主机属性注释的内容。
通用列表块类型 (Generic List Block	uint32	启动由传送 VDB 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks) *	变量	在思科漏洞数据库 (VDB) 中识别的漏洞的主机漏洞数据块列表。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。

表 B-59 完整主机配置文件记录 5.2.x 字段 （续）

字段	数据类型	说明 (Description)
通用列表块类型 (Generic List Block	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方/VDB）主机漏洞数据块 ((Third Party/VDB) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪且包含已收录到思科漏洞数据库 (VDB) 中的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
通用列表块类型 (Generic List Block	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。
（第三方扫描）主机漏洞数据块 ((Third Party Scan) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪的主机漏洞数据块。请注意，这些数据块的主机漏洞 ID 为第三方扫描仪 ID，而不是思科检测到的 ID。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-111 页。
列表块类型 (List Block Type)	uint32	启动由传送属性数据的属性值数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表数据块中的字节数，包括列表报头以及所有封装数据块。
属性值数据块 (Attribute Value Data Blocks) *	变量	属性值数据块列表。有关此列表中的数据块的说明，请参阅属性值数据块，第 4-79 页。
移动 (Mobile)	uint8	指示操作系统是否在移动设备上运行的一个真假标志。
Jailbroken	uint8	指示移动设备操作系统是否被越狱的一个真假标志。

用于 5.1.x 的主机配置文件数据块

下图显示主机配置文件数据块的格式。该数据块也不包含主机临界值，但包含 VLAN 在线状态指示器。此外，数据块还可以传输主机的 NetBIOS 名称。主机配置文件数据块的块类型为 132。

注释　下图中块类型字段旁边的星号 (*) 表示该消息可能包含零个或多个系列 1 数据块实例。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	主机配置文件块类型 (132) (Host Profile Block Type (132))																															
	主机配置文件块长度 (Host Profile Block Length)																															
	IP 地址 (IP Address)																															
服务器指纹 (Server Fingerprints)	跳数 (Hops)								主要/次要 (Primary/Secondary)								通用列表块类型 (31) (Generic List Block Type (31))														
	通用列表块类型 (Generic List Block Type)（续）																通用列表块长度 (Generic List Block Length)														
	通用列表块长度 (Generic List Block Length)（续）																服务器指纹数据块 (Server Fingerprint Data Blocks)*														
客户端指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	客户端指纹数据块 (Client Fingerprint Data Blocks)*																															
中小企业指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	SMB 指纹数据块 (SMB Fingerprint Data Blocks)*																															
DHCP 指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	DHCP 指纹数据块 (DHCP Fingerprint Data Blocks)*																															
移动设备指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	移动设备指纹数据块 (Mobile Device Fingerprint Data Blocks)*																															

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
TCP 服务器块*	列表块类型 (11) (List Block Type (11))																																TCP 服务器
	列表块长度 (List Block Length)																																
	TCP 服务器数据块 (TCP Server Data Blocks)																																
UDP 服务器块*	列表块类型 (11) (List Block Type (11))																																UDP 服务器
	列表块长度 (List Block Length)																																
	UDP 服务器数据块 (UDP Server Data Blocks)																																
网络协议块*	列表块类型 (11) (List Block Type (11))																																网络协议 (Protocol)
	列表块长度 (List Block Length)																																
	网络协议数据块 (Network Protocol Data Blocks)																																
传输协议块*	列表块类型 (11) (List Block Type (11))																																传输协议 (Protocol)
	列表块长度 (List Block Length)																																
	传输协议数据块 (Transport Protocol Data Blocks)																																
MAC 地址块*	列表块类型 (11) (List Block Type (11))																																MAC 地址
	列表块长度 (List Block Length)																																
	主机 MAC 地址数据块 (Host MAC Address Data Blocks)																																
	主机上次查看时间 (Host Last Seen)																																
	主机类型 (Host Type)																																
	移动 (Mobile)								Jailbroken								VLAN 在线状态 (VLAN Presence)								VLAN ID								
客户端应用数据	VLAN ID（续）								VLAN 类型 (VLAN Type)								VLAN 优先级 (VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))								客户端应用
	通用列表块类型 (31) (Generic List Block Type (31))（续）																								通用列表块长度 (Generic List Block Length)								
	通用列表块长度 (Generic List Block Length)（续）																								客户端应用数据块 (Client Application Data Blocks)								

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 字符串数据...(NetBIOS String Data...)																															

下表对版本 5.1.x 返回的主机配置文件数据块的字段进行了说明

表 B-60　　主机配置文件数据块 5.1.x 字段

字段	数据类型	说明 (Description)
主机配置文件块类型 (Host Profile Block Type)	uint32	启动用于 5.1.x 的主机配置文件数据块。值始终为 132。
主机配置文件块长度 (Host Profile Block Length)	uint32	主机配置文件数据块中的字节数，包括主机配置文件块类型和长度字段的八个字节，加上随后的主机配置文件数据中的字节数。
IP 地址 (IP Address)	uint8[4]	配置文件中描述的主机的 IP 地址，采用 IP 地址八位组。
跳数 (Hops)	uint8	从主机到设备的跳数。
主/辅助 (Primary/ Secondary)	uint8	表示主机是位于检测到其的设备的主网络中还是辅助网络中： ▪ 0 - 主机位于主网络中。 ▪ 1 - 主机位于辅助网络中。
通用列表块类型 (Generic List Block	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。

表 B-60 主机配置文件数据块 5.1.x 字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 SMB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（SMB指纹）数据块(Operating System Fingerprint (SMB Fingerprint) Data Blocks) *	变量	包含用 SMB 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（DHCP 指纹）数据块 (Operating System Fingerprint (DHCP Fingerprint) Data Blocks) *	变量	包含用 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
通用列表块类型 (Generic List Block	uint32	启动由传送用 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。

表 B-60　主机配置文件数据块 5.1.x 字段 （续）

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（移动设备指纹）数据块 (Operating System Fingerprint (Mobile 设备 Fingerprint) Data Blocks) *	变量	包含用移动设备指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-161 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
TCP 服务器数据块 (TCP Server Data Blocks)	变量	描述 TCP 服务器的主机服务器数据块（按照产品早期版本的记录）。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
UDP 服务器数据块 (UDP Server Data Blocks)	uint32	描述 UDP 服务器的主机服务器数据块（按照产品早期版本的记录）。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个协议数据块。
网络协议数据块 (Network Protocol Data Blocks)	uint32	描述网络协议的协议数据块。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个传输协议数据块。

表 B-60 主机配置文件数据块 5.1.x 字段 （续）

字段	数据类型	说明 (Description)
传输协议数据块 (Transport Protocol Data Blocks)	uint32	描述传输协议的协议数据块。有关此数据块的说明，请参阅协议数据块，第 4-72 页。
列表块类型 (List Block Type)	uint32	启动由 MAC 地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks)	uint32	描述主机 MAC 地址的主机 MAC 地址数据块。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-113 页。
主机上次查看时间 (Host Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。可能会出现以下值： ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥 ▪ 3 - NAT 设备 ▪ 4 - LB（负载均衡器）
移动 (Mobile)	uint8	指示主机是否为移动设备的一个真假标志。
Jailbroken	uint8	指示主机是否同样为已被越狱的移动设备的一个真假标志。
VLAN 在线状态 (VLAN Presence)	uint8	表示是否存在 VLAN： ▪ 0 - 是 ▪ 1 - 否
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block	uint32	启动由传送客户端应用数据的客户端应用数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
客户端应用数据块 (Client Application Data Blocks)	uint32	描述客户端应用的客户端应用数据块。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-155 页。

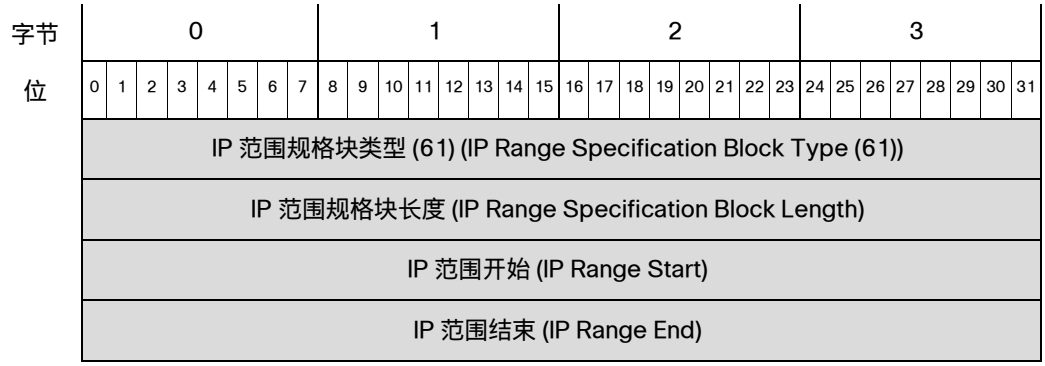
表 B-60　　主机配置文件数据块 5.1.x 字段 （续）

字段	数据类型	说明 (Description)
字符串块类型 (String Block Type)	uint32	启动 NetBIOS 名称的字符串数据块。此值设置为 0 以表示字符串数据。
字符串块长度 (String Block Length)	uint32	表示 NetBIOS 名称字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称的字节数。
NetBIOS 字符串数据 (NetBIOS String Data)	变量	包含主机配置文件中描述的主机的 NetBIOS 名称。

用于 5.0 - 5.1.1.x 的 IP 范围规格数据块

IP 范围规格数据块传输一系列 IP 地址。IP 范围规格数据块在用户协议、用户客户端应用、地址规格、用户产品、用户服务器、用户主机、用户漏洞、用户临界点以及用户属性值数据块中使。IP 范围规格数据块的块类型为 61。

下图显示 IP 范围规格数据块的格式:



下表对 IP 范围规格数据块的组件进行了说明。

表 B-61　　IP 范围规格数据块字段

字段	数据类型	说明 (Description)
IP 范围规格块类型 (IP Range Specification Block Type)	uint32	启动 IP 范围规格数据块。值始终为 61。
IP 范围规格块长度 (IP Range Specification Block Length)	uint32	IP 范围规格数据块中的字节总数，包括 IP 范围规格块类型和长度字段的八个字节，加上随后的 IP 范围规格数据的字节数。

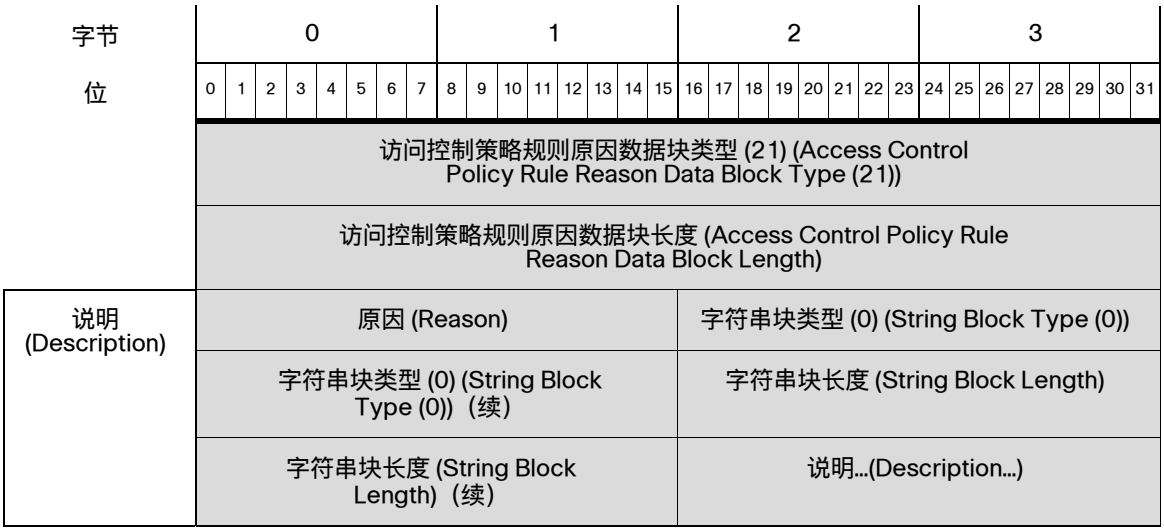
表 B-61 IP 范围规格数据块字段 （续）

字段	数据类型	说明 (Description)
IP 范围规格开始 (IP Range Specification Start)	uint32	IP 地址范围的开始 IP 地址。
IP 范围规格结束 (IP Range Specification End)	uint32	IP 地址范围的结束 IP 地址。

访问控制策略规则原因数据块

eStreamer 服务用访问控制规则策略规则原因数据块包含有关访问控制策略规则 ID 的信息。此数据块的块类型为系列 2 中的 21。

下图显示访问控制策略规则 ID 元数据块的结构。



下表对访问控制策略规则 ID 元数据块中的字段进行了说明。

表 B-62　访问控制策略规则原因数据块字段

字段	数据类型	说明 (Description)
访问控制策略规则原因数据块类型 (Access Control Policy Rule Reason Data Block Type)	uint32	启动访问控制策略规则原因数据块。值始终为 21。
访问控制策略规则原因数据块长度 (Access Control Policy Rule Reason Data Block Length)	uint32	访问控制策略规则原因数据块中的字节总数，包括访问控制策略规则原因数据块类型和长度字段的八个字节，加上随后的数据的字节数。
原因 (Reason)	uint16	触发事件的规则的原因编号。
字符串块类型 (String Block Type)	uint32	启动包含访问控制策略规则原因的说明的字符串数据块。值始终为 0。
字符串块长度(String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上说明 (Description) 字段中的字节数。
说明 (Description)	字符串	规则原因的说明。