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

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...
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
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

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...
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
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 3-110 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

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...
608	不适用	不适用	SSL 流状态	当前	SSL 流状态，第 3-122 页
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 3-128 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...)																																

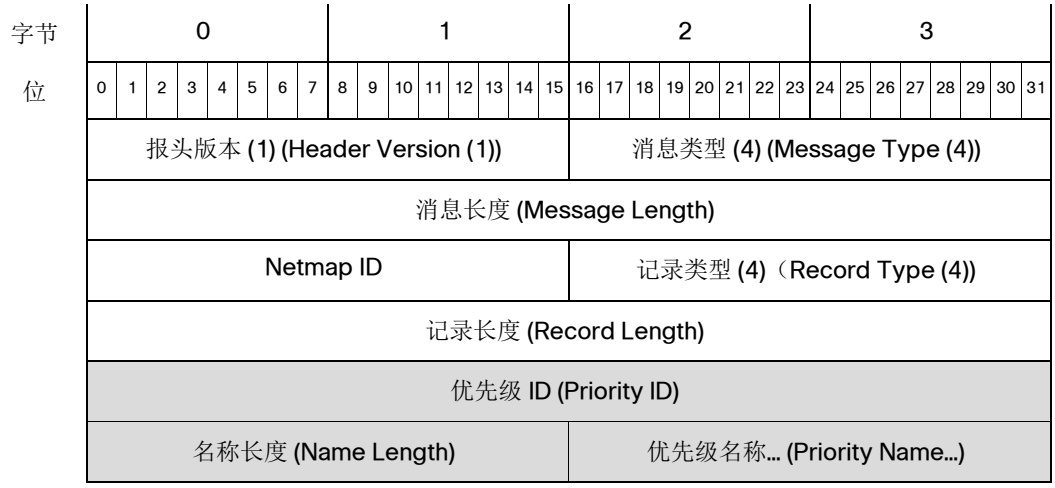
下表对数据包记录中的字段进行了说明。

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）。

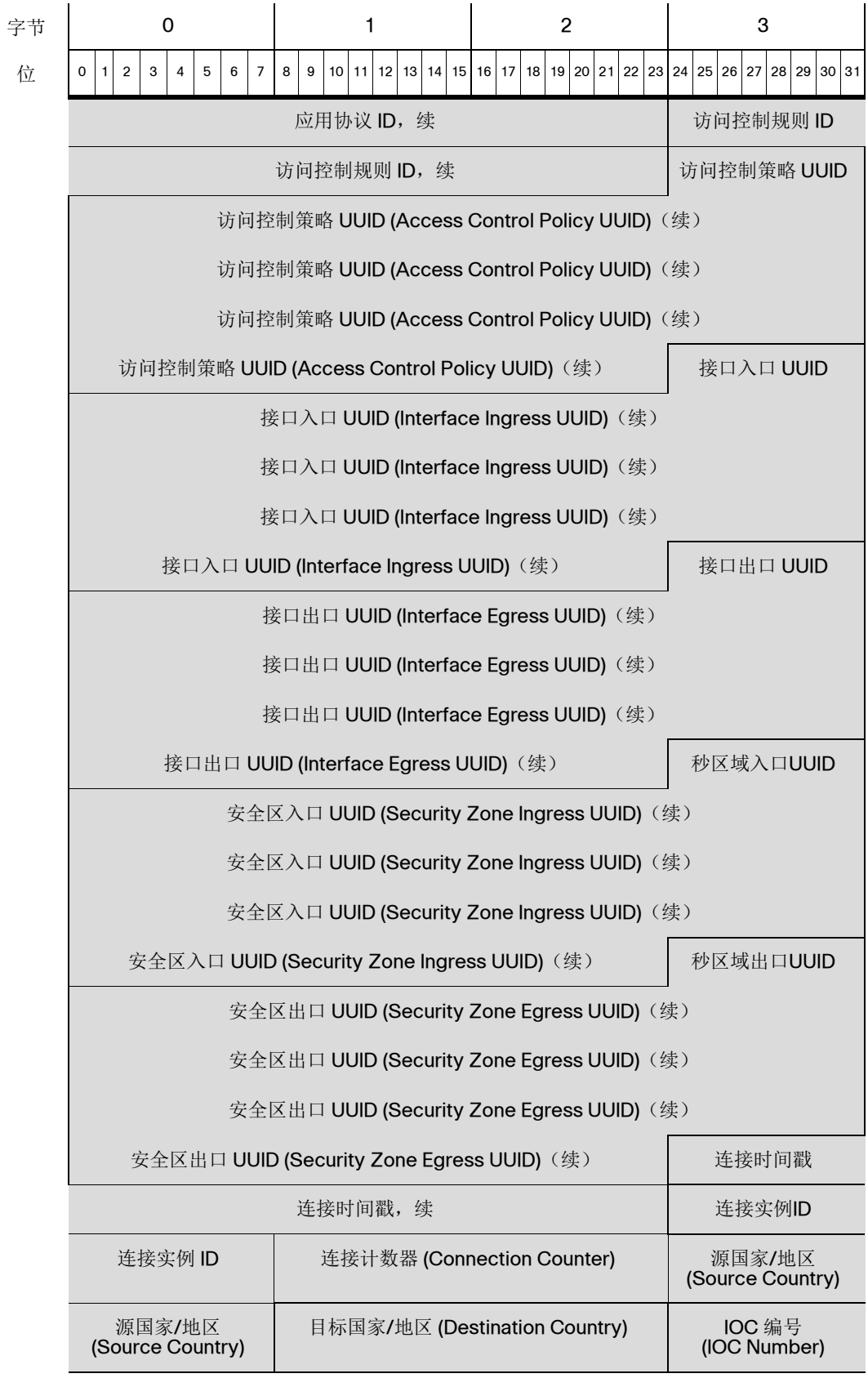
入侵事件记录 7.1+

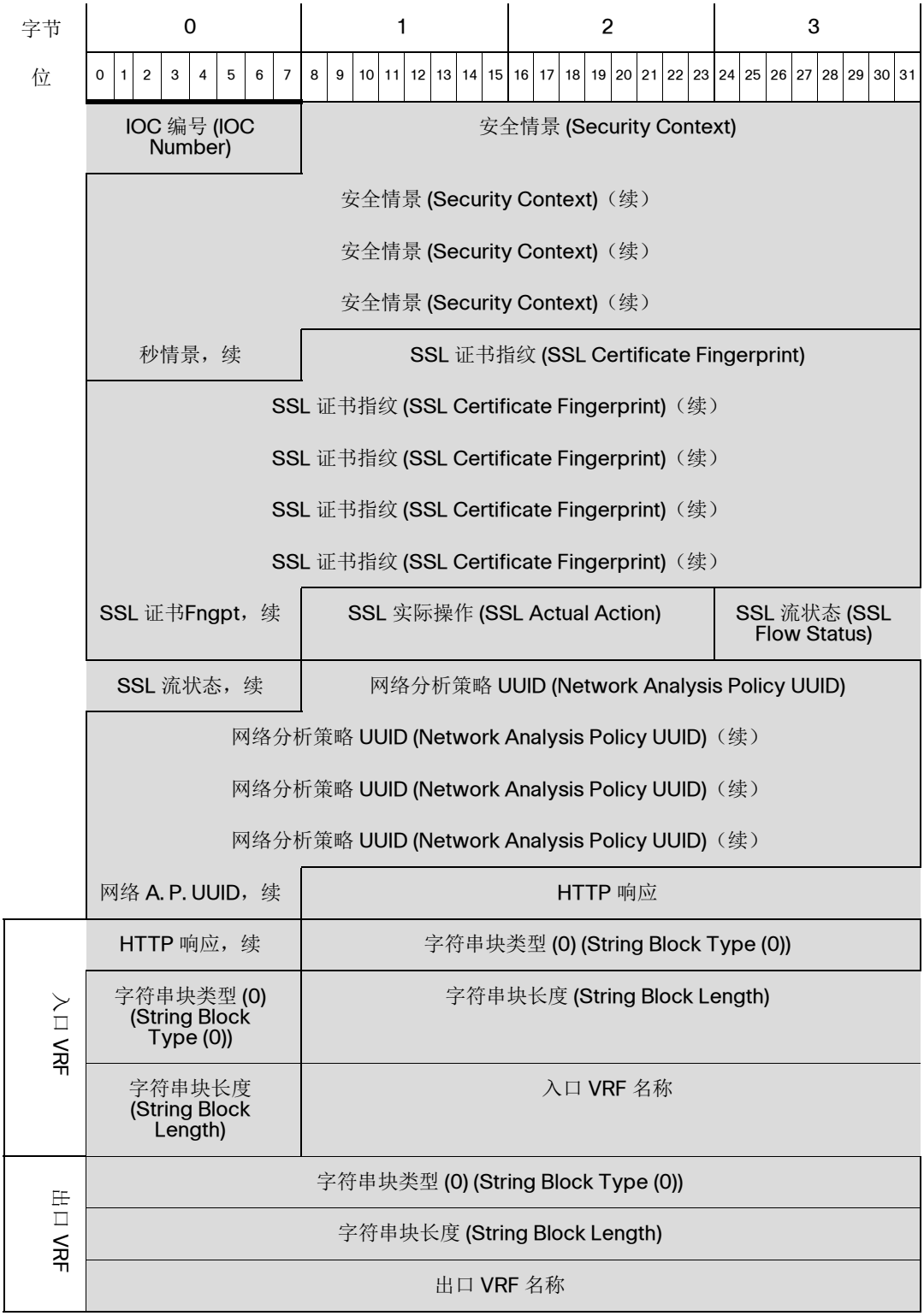
下图中的阴影部分表示入侵事件记录中的字段。此数据块的记录类型为系列 2 数据块组中的 400，块类型为系列 2 数据块组中的 85。它替代了块类型 81。添加了以前包含在额外事件数据中的 XFF 字段。

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(eStreamerServerTimestamp)（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
HTTP 响应，续
字符串块类型 (0) (String Block Type (0))
入口 VRF
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

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
HTTP 主机名 (HTTP Hostname)	Snort 版本								原始客户端 IP																字符串块类型 (0) (String 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）																								HTTP 主机名... (HTTP Hostname...)							
HTTP URI	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	HTTP URI...																															
SMTP 附件 (SMTP Attachments)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	SMTP 附件... (SMTP Attachments...)																															
SMTP 发件人	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	SMTP 发件人... (SMTP From...)																															
SMTP 报头	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	SMTP 报头... (SMTP Headers...)																															
SMTP 收件人	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	SMTP 收件人... (SMTP To...)																															

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

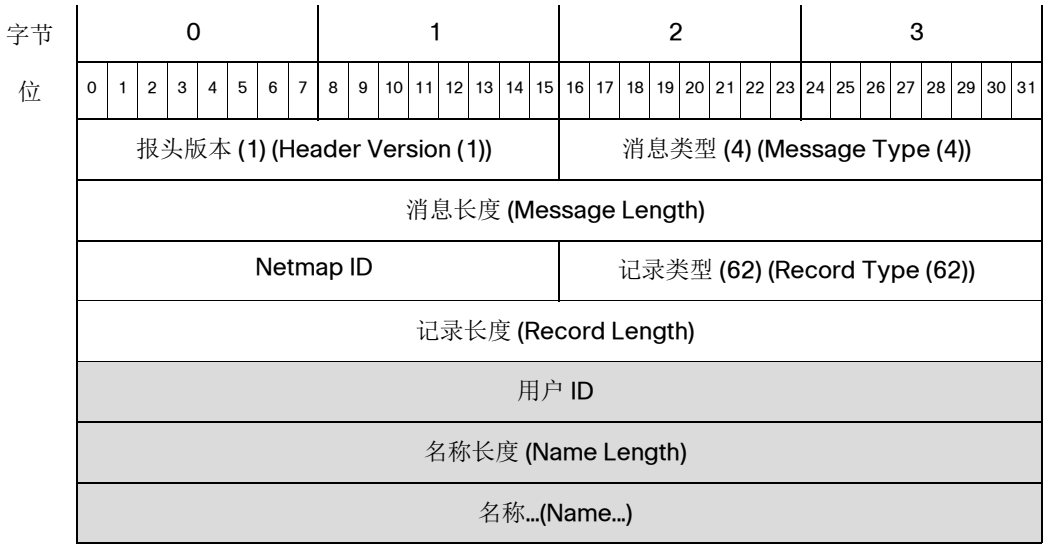
字段	数据类型	说明 (Description)
入侵影响警报块类型 (Intrusion Impact Alert Block Type)	uint32	表示后面是入侵影响警报数据块。此字段的值始终为153。请参阅入侵事件和元数据记录类型，第 3-1 页。
入侵影响警报块长度 (Intrusion Impact Alert Block Length)	uint32	表示入侵影响警报数据块的长度，包括后面的所有数据以及入侵影响警报块类型和长度的 8 个字节。
事件 ID (Event ID)	uint32	表示事件标识号。
设备 ID	uint32	表示受管设备标识号。
事件秒 (Event Second)	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。）



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

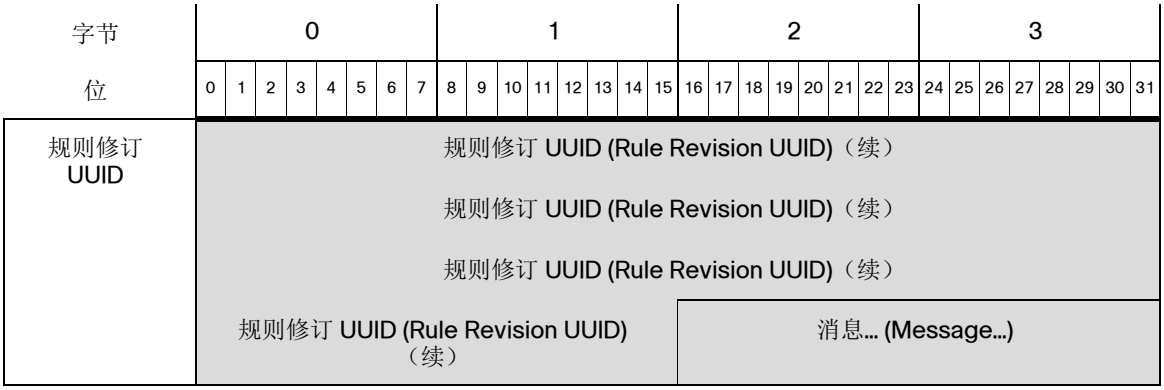
字段	数据类型	说明 (Description)
用户 ID (User ID)	uint32	用户 ID 号码。 此字段是此记录的唯一密钥。
名称长度 (Name Length)	uint32	用户名称中包含的字节数。
名称 (Name)	字符串	用户的名称。

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。

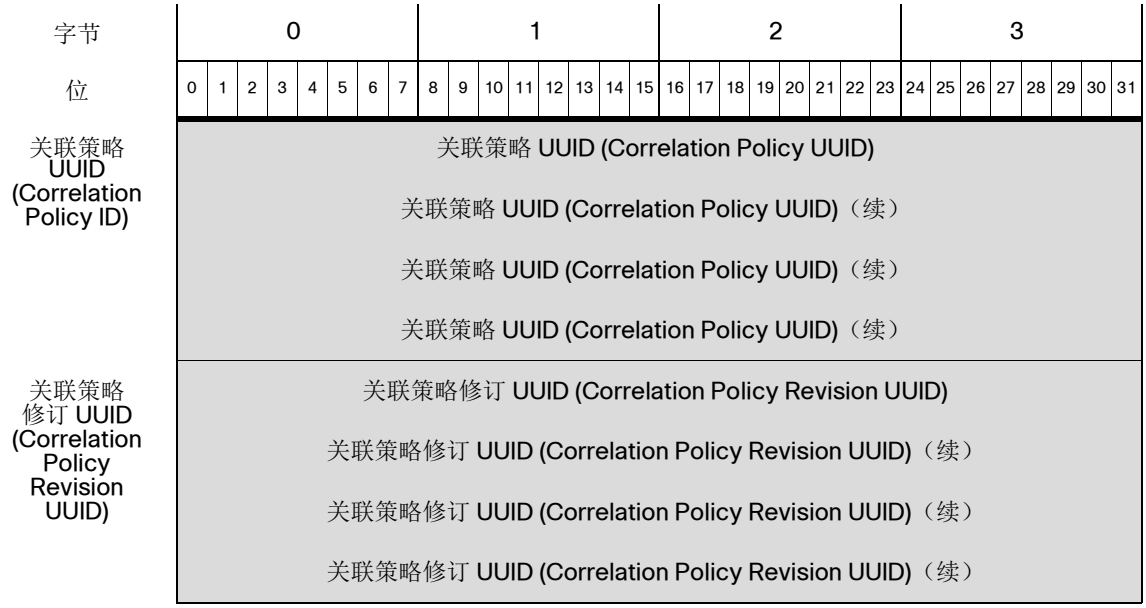
表 3-8 分类记录字段

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...)															



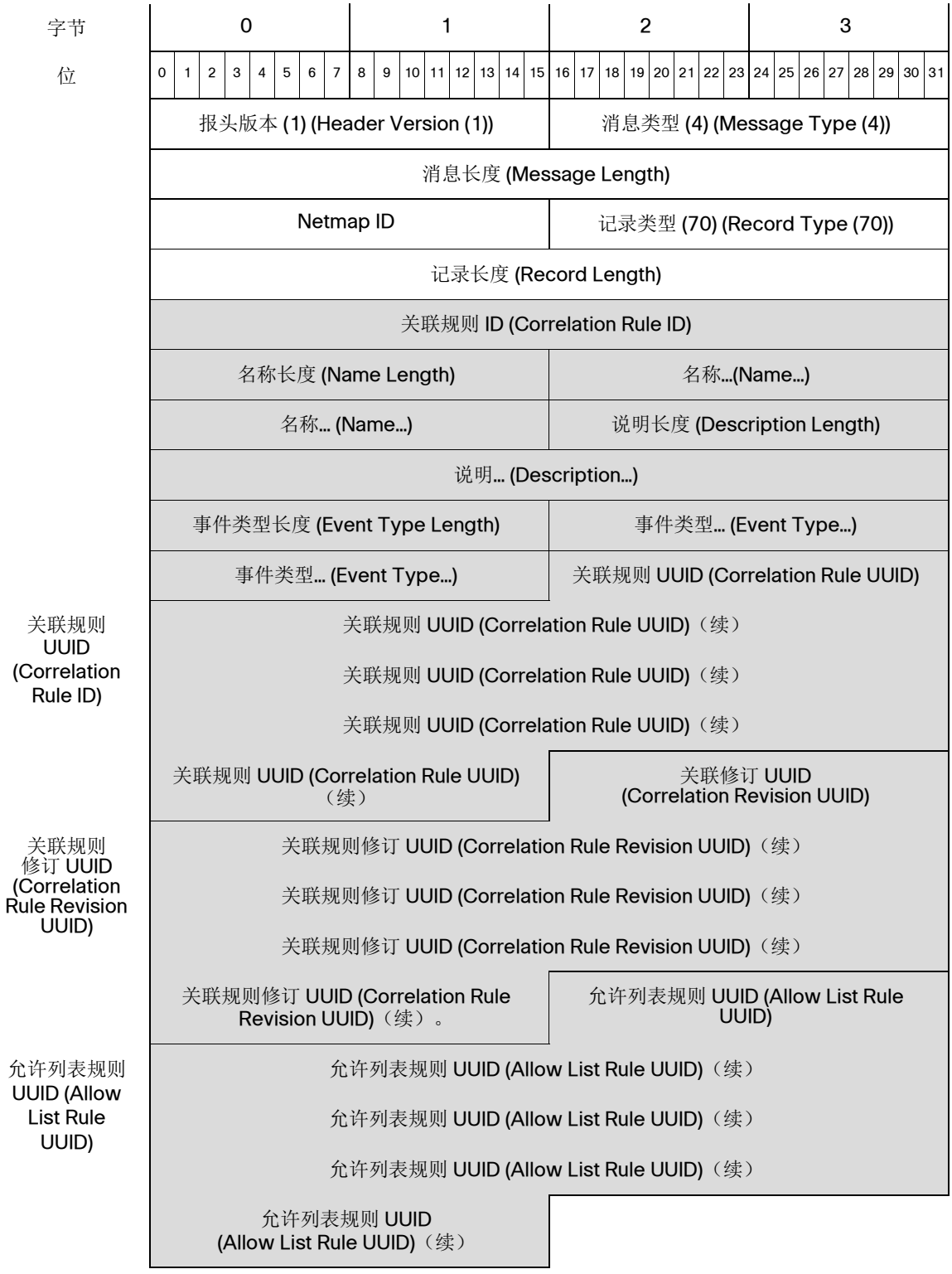
下表对关联策略记录中的字段进行了说明。

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。



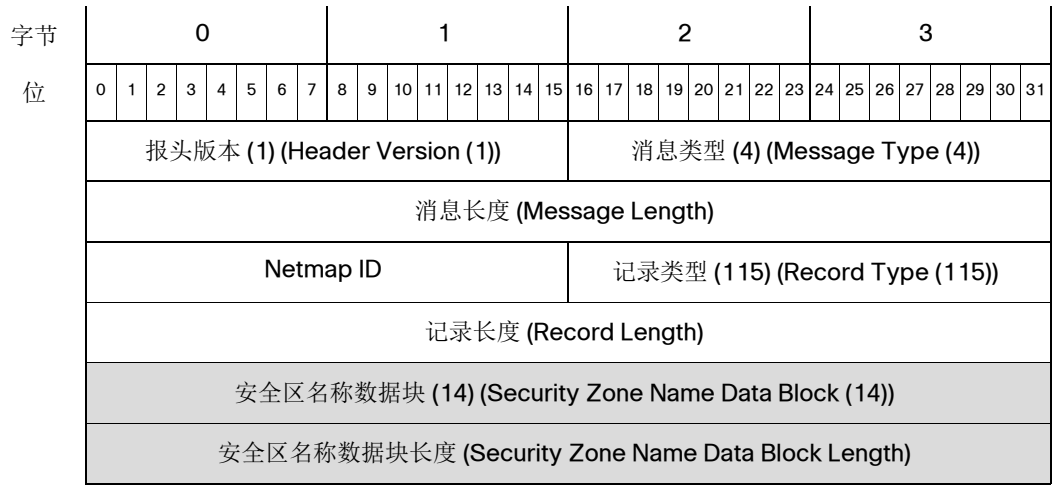
下表对关联规则记录中的字段进行了说明。

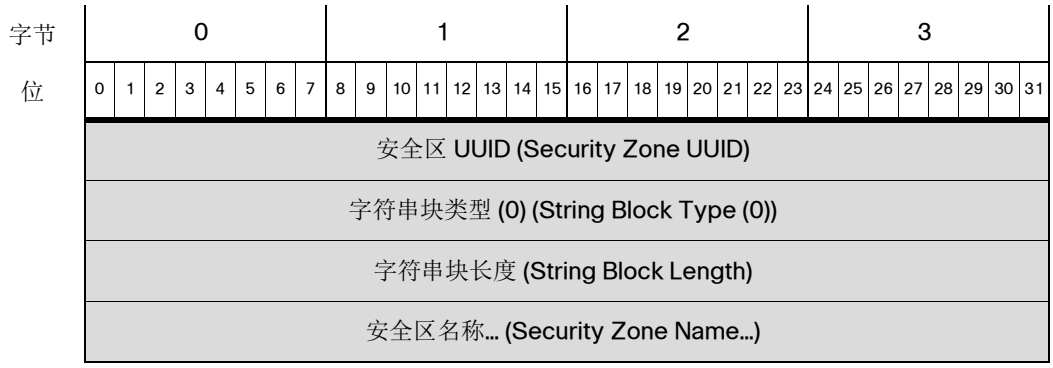
表 3-10　关联规则记录字段

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。





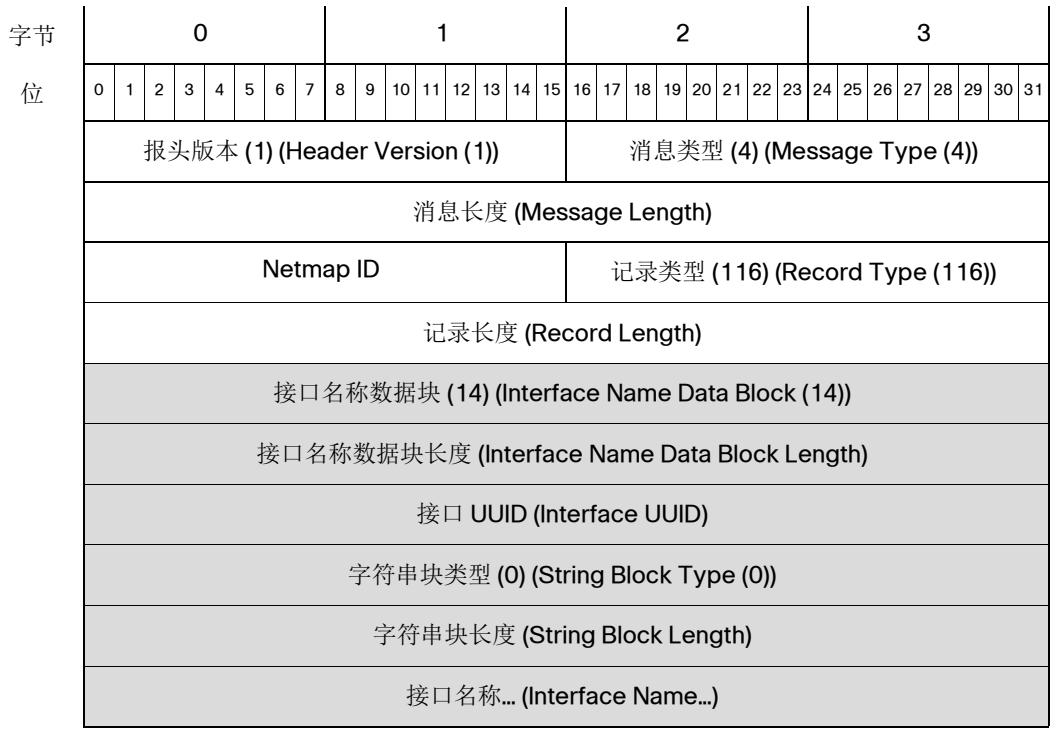
下表对安全区名称数据块中的字段进行了说明。

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

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (117) (Record Type (117))															
记录长度 (Record Length)																																
访问控制策略名称数据块 (14) (Access Control Policy Name Data Block (14))																																
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)																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
访问控制策略名称... (Access Control Policy Name...)																																

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...)																															

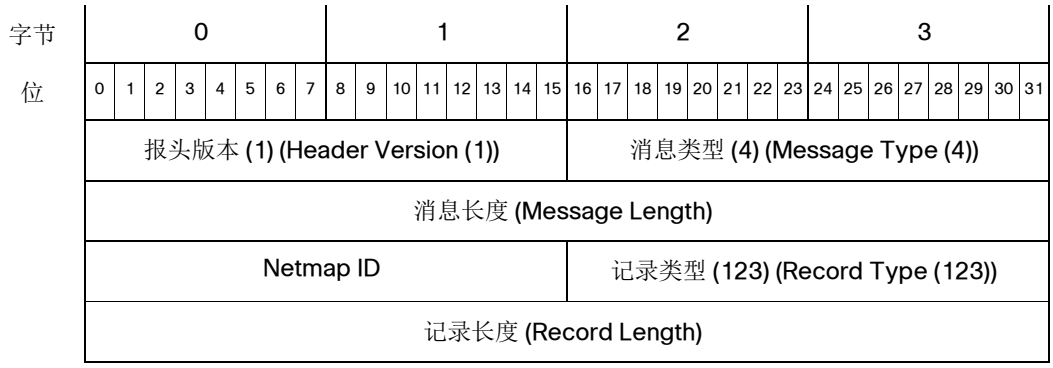
下表对访问控制规则 ID 数据块中的字段进行了说明。

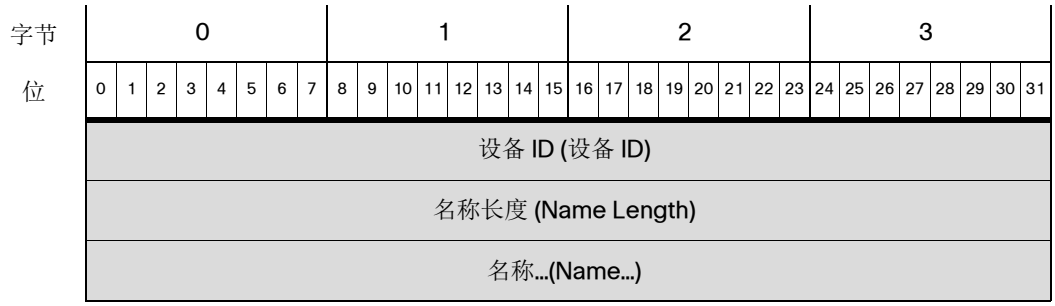
表 3-14 访问控制规则 ID 数据块字段

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。

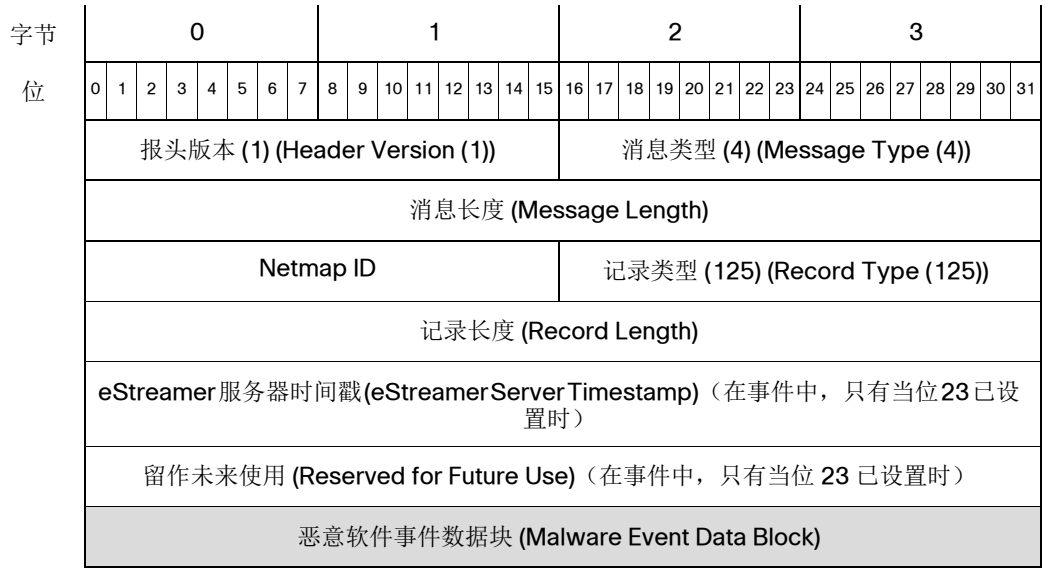
表 3-15　　受管设备记录字段

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...)																																

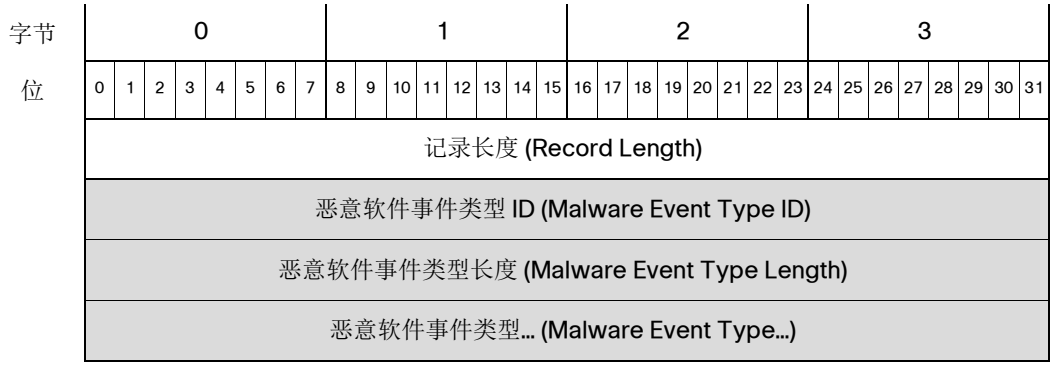
下表对思科高级恶意软件防护云名称数据块中的字段进行了说明。

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。



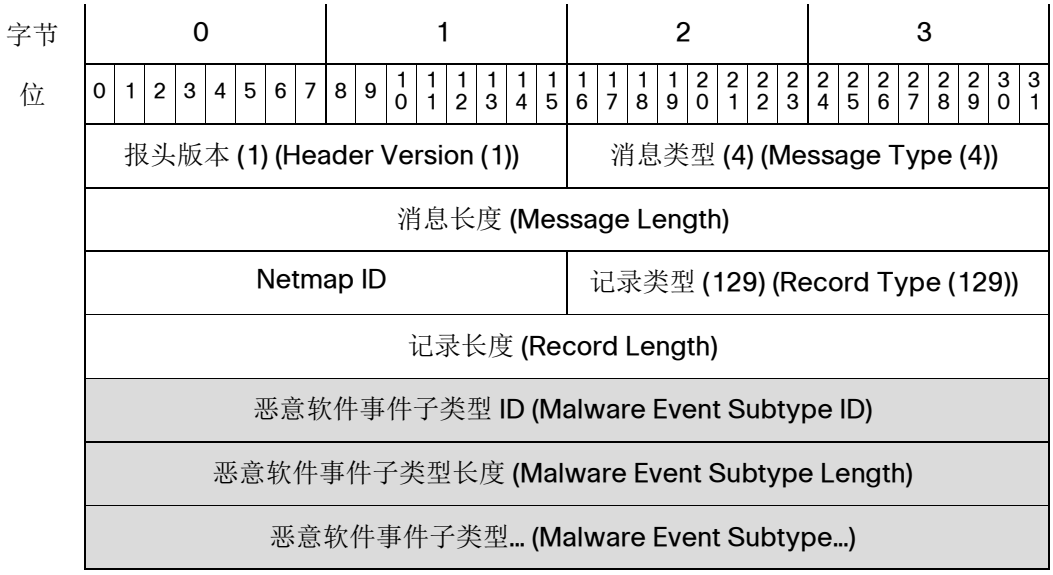
下表对恶意软件事件类型记录中的字段进行了说明。

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。



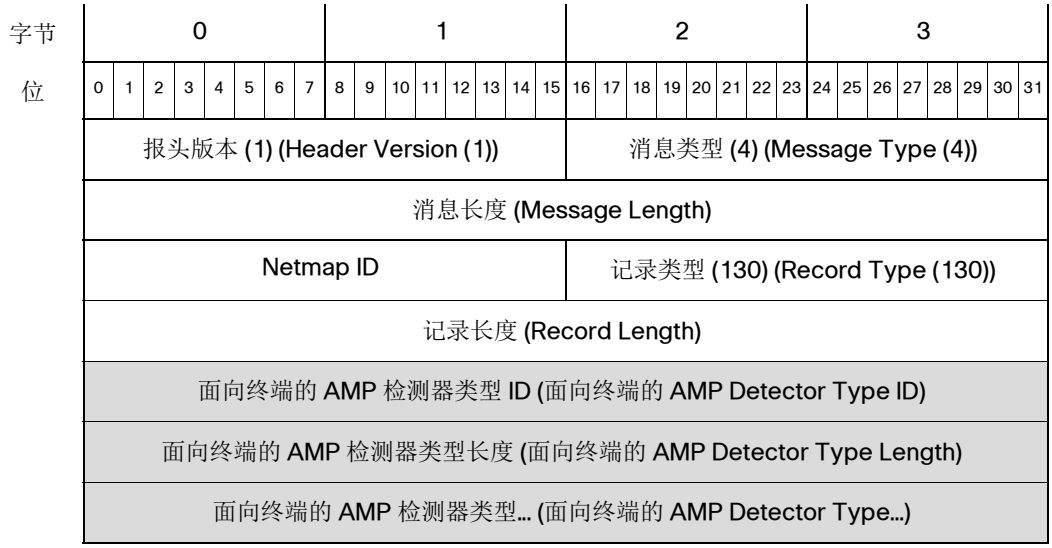
下表对恶意软件事件子类型记录中的字段进行了说明。

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”(RequestFlags)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。

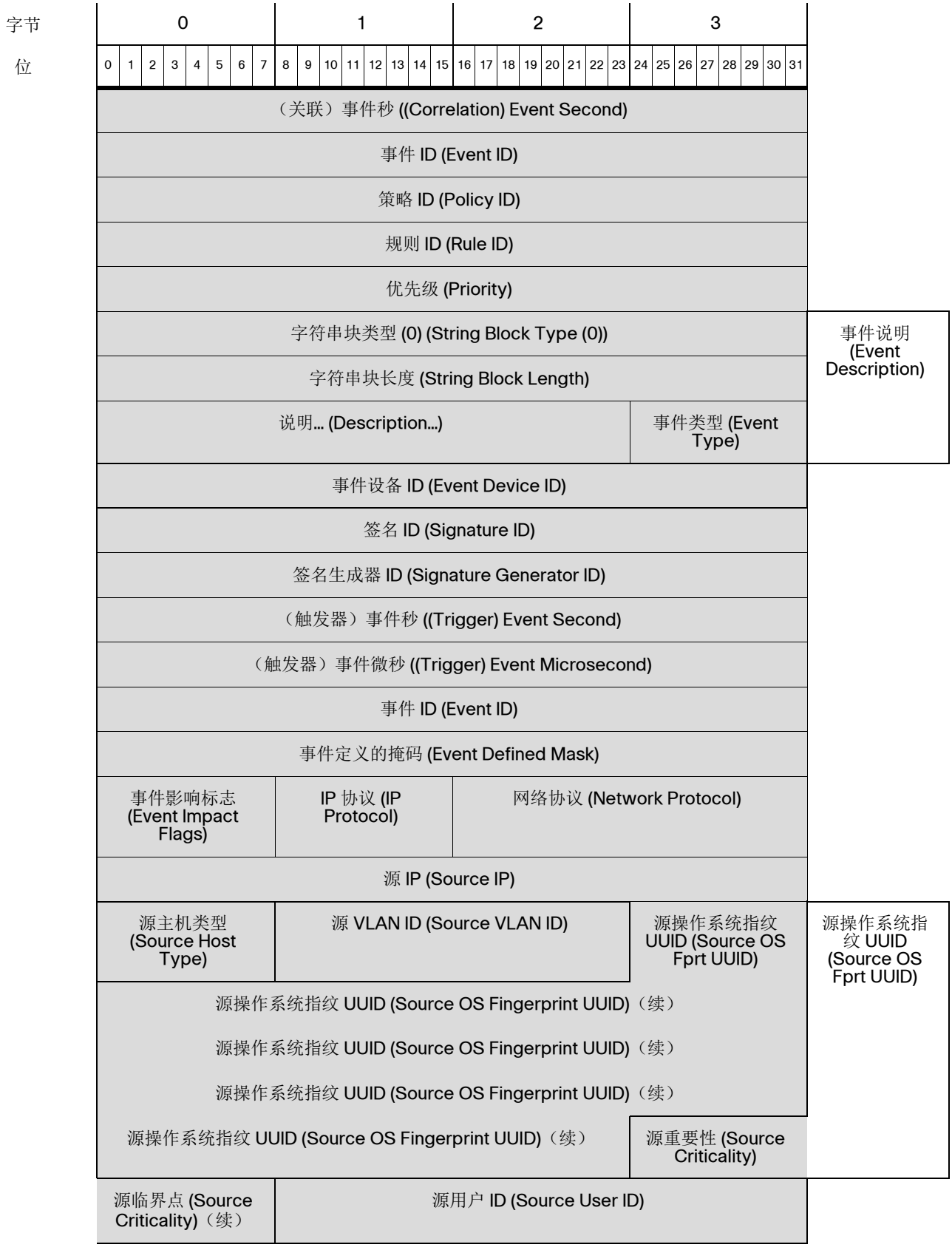
用于 5.4+ 的关联事件

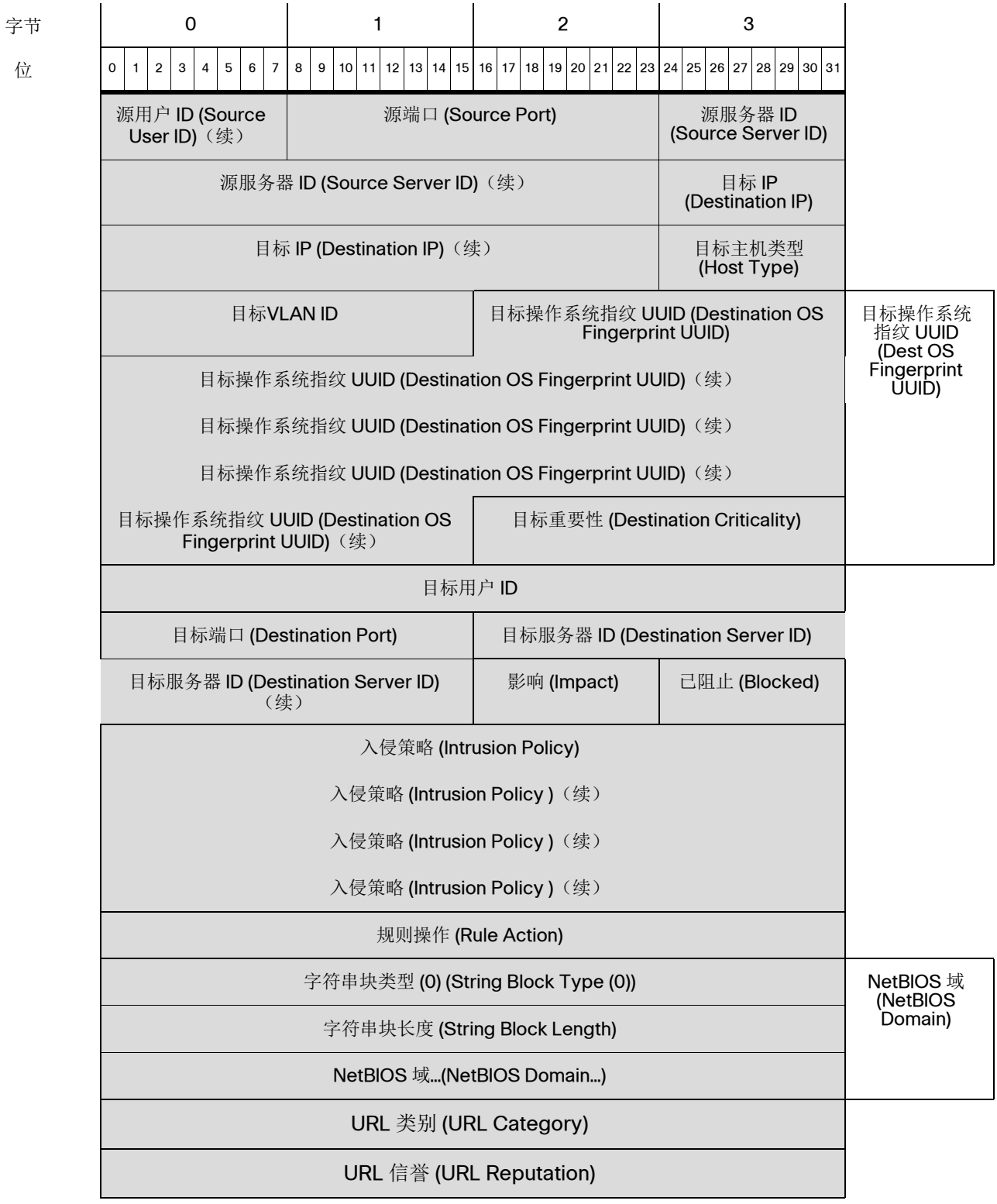
关联事件（在 5.0 之前的版本中称为合规性事件）包含关联策略违规的相关信息。此消息使用标准 eStreamer 消息报头并指定记录类型为 112，随后是类型为系列 1 数据块组中的 156 的关联数据块。数据块类型 156 与其前身（块类型 128）的区别在于其包含 IPv6 支持。

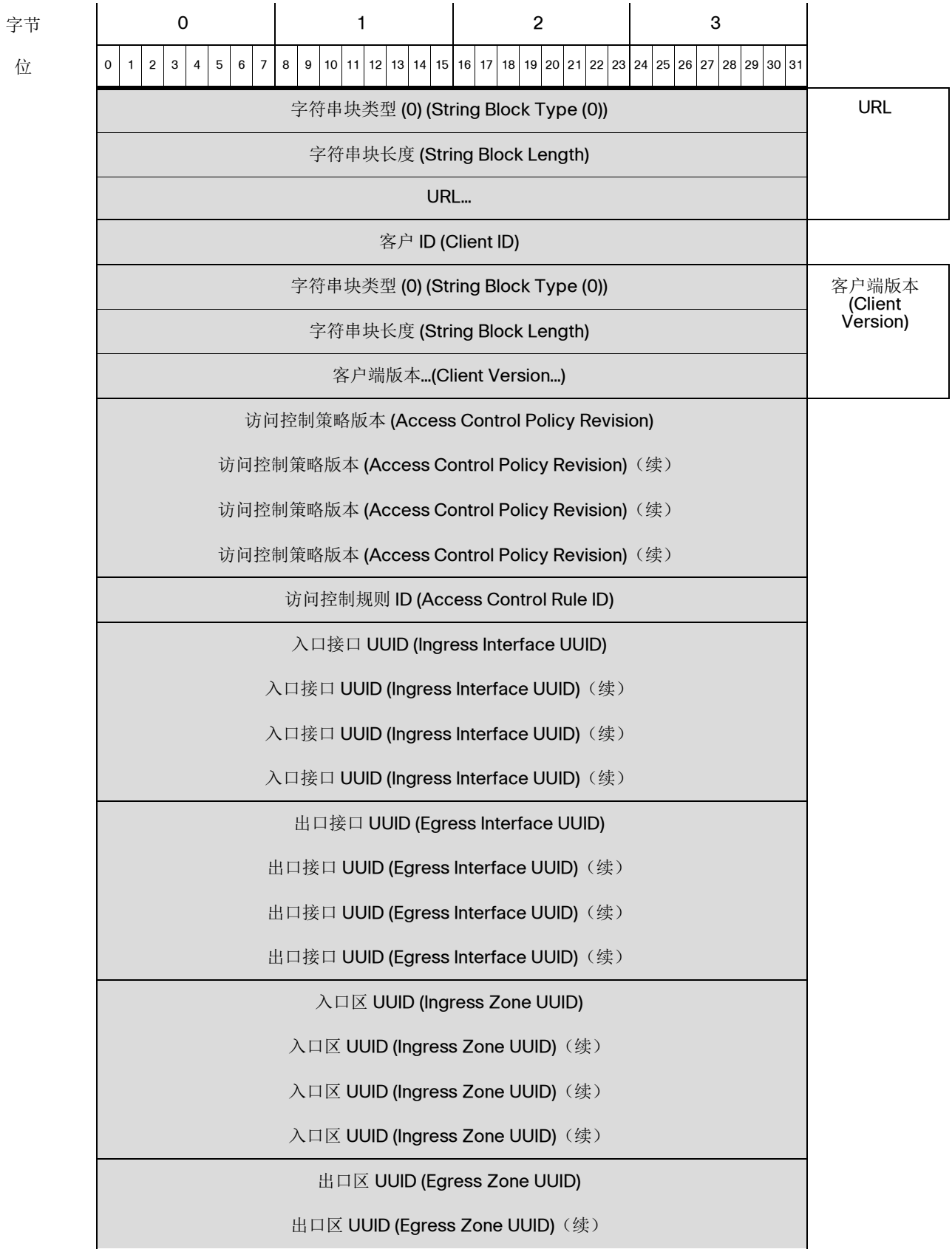
关联事件的 5.4+ 版本具有地理位置、安全情报以及 SSL 支持等新字段。

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

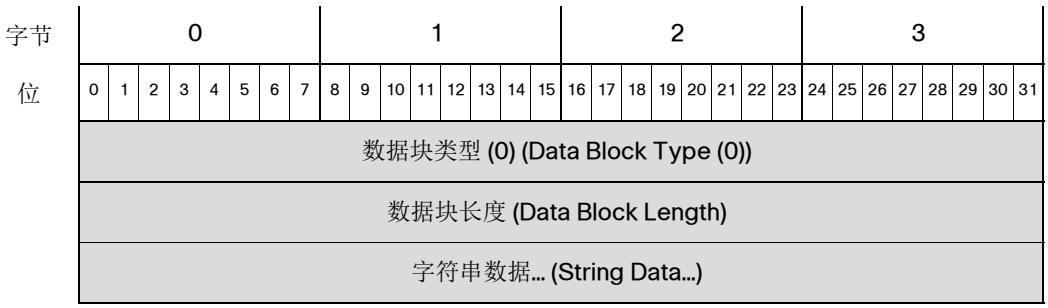
eStreamer 服务使用字符串数据块发送消息中的字符串数据。这些块常出现在其他数据块中，用于识别，例如，操作系统或服务器名称。

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。

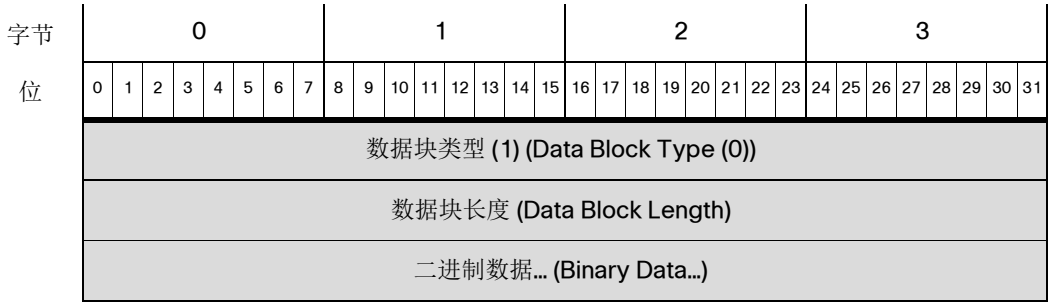
表 3-25 字符串块字段

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。

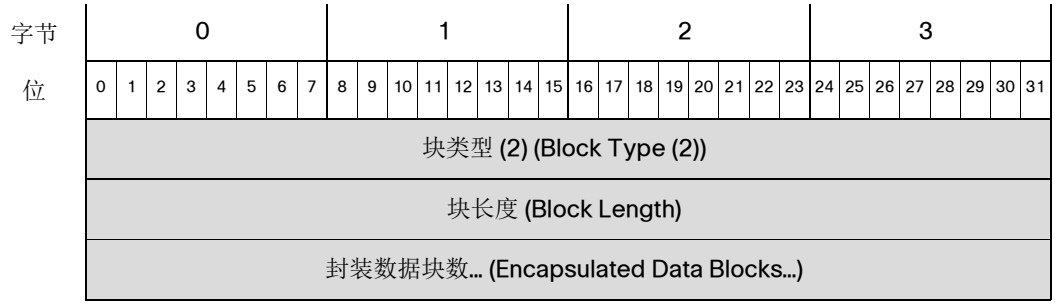
表 3-26　　BLOB 数据块字段

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。

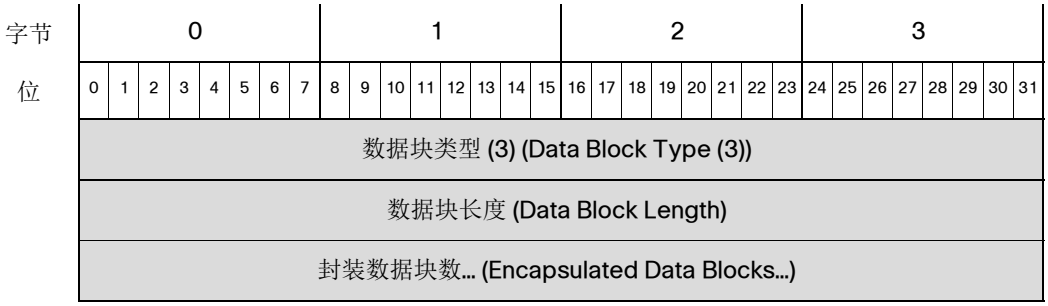
表 3-27　　列表数据块字段

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。

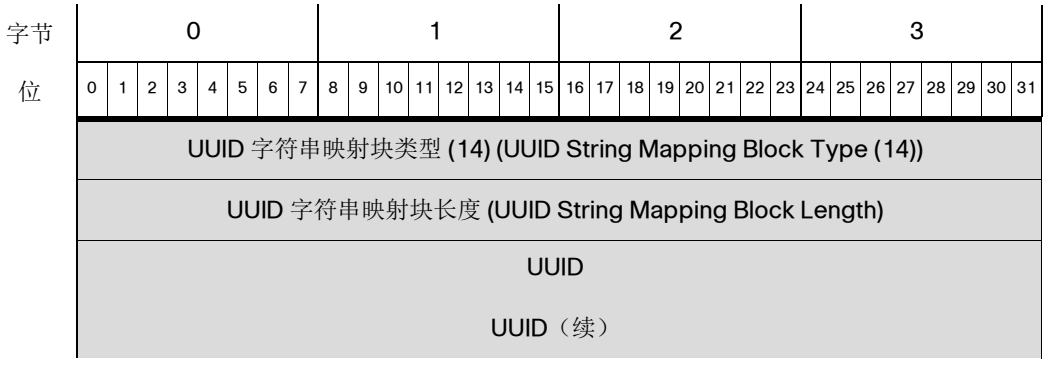
表 3-28 通用列表数据块字段

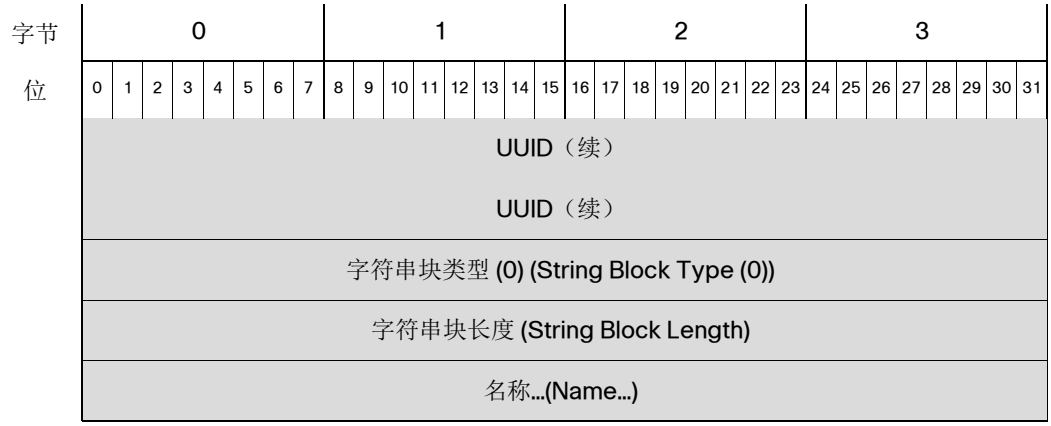
字段	字节数	说明 (Description)
数据块类型 (Data Block Type)	uint32	启动通用列表数据块。值始终为 3。
数据块长度 (Data Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节总数。
封装数据块数 (Encapsulated Data Blocks)	变量	封装数据块数最多可以是通用列表块长度中的最大字节数。

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。

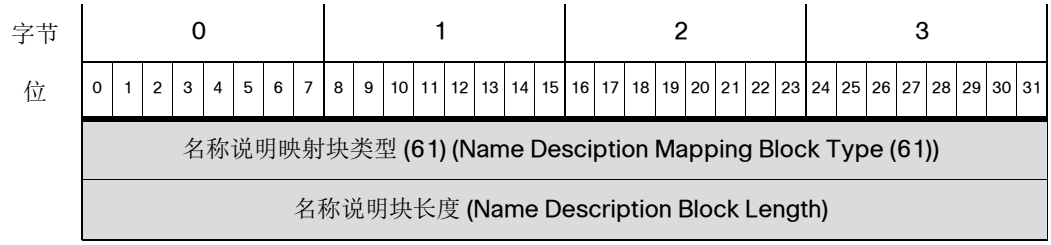
表 3-29　UUID 字符串映射数据块字段

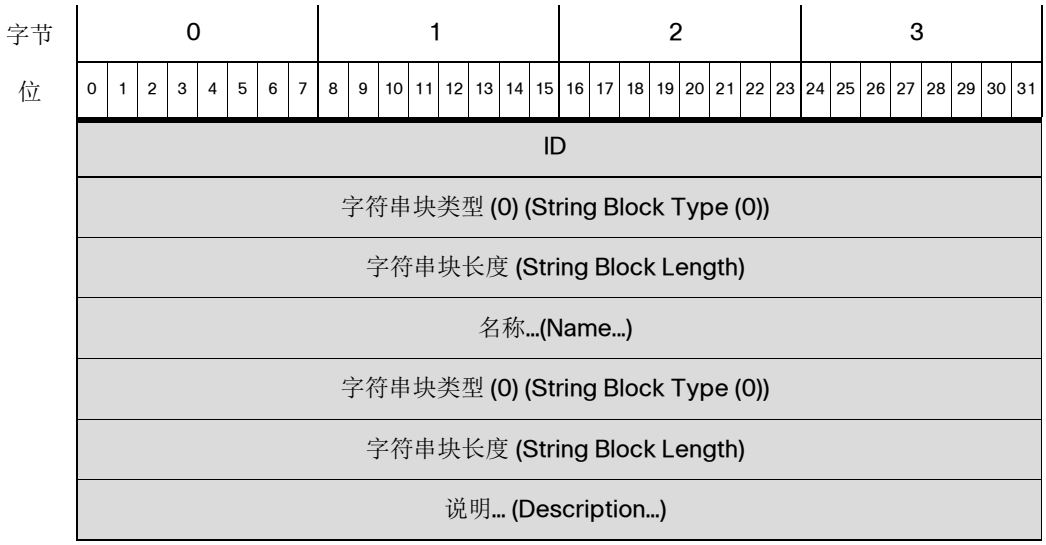
字段	数据类型	说明 (Description)
UUID 字符串映射块类型 (UUID String Mapping Block Type)	uint32	启动 UUID 字符串映射块。值始终为 14。
UUID 字符串映射块长度 (UUID String Mapping Block Length)	uint32	UUID 字符串映射块中的字节总数，包括 UUID 字符串映射块类型和长度字段的八个字节，加上随后的数据字节数。
UUID	uint8[16]	UUID识别的事件或其他对象的唯一标识符。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	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。

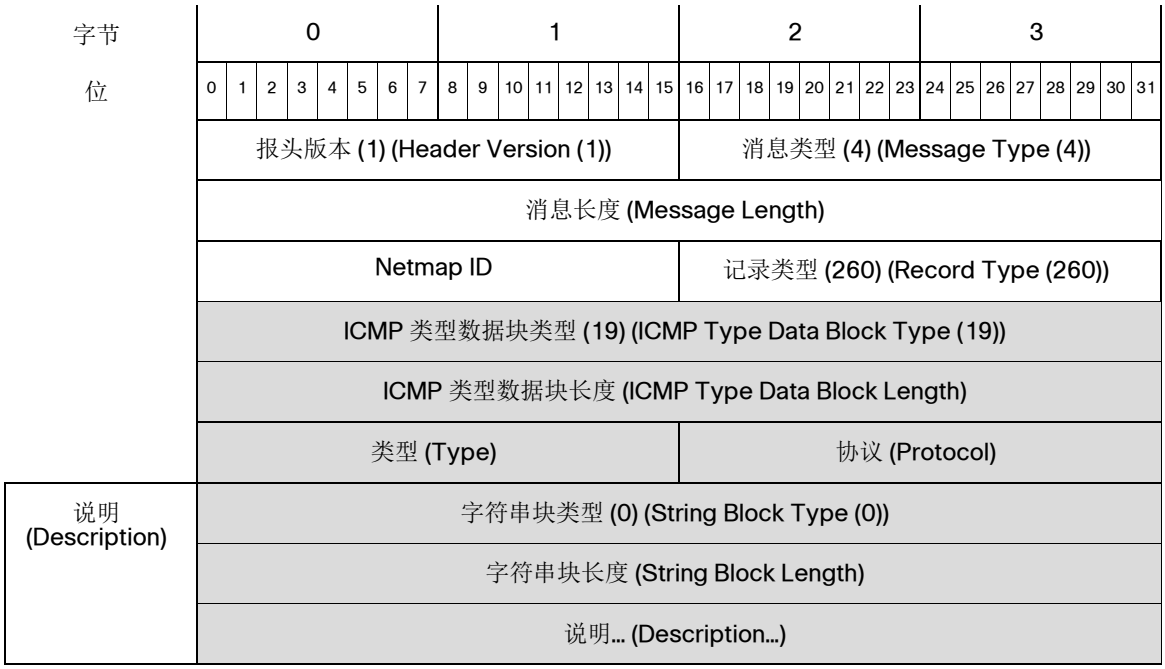
表 3-31 访问控制策略规则 ID 元数据块字段 （续）

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。



下表对 ICMP 类型数据块中的字段进行了说明。

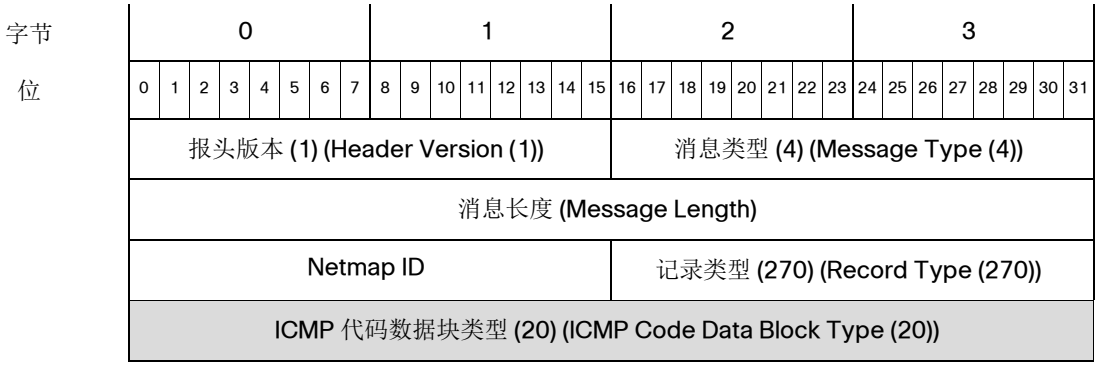
表 3-32　　ICMP 类型数据块字段

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...)															

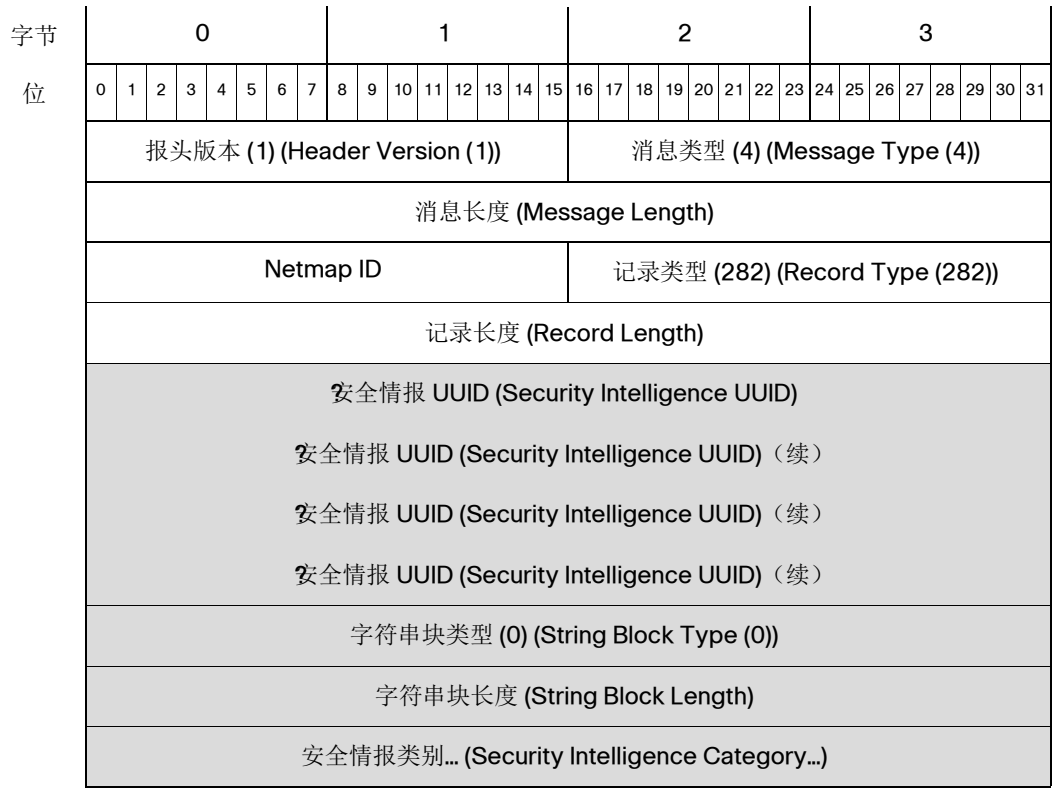
下表对 ICMP 代码数据块中的字段进行了说明。

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。



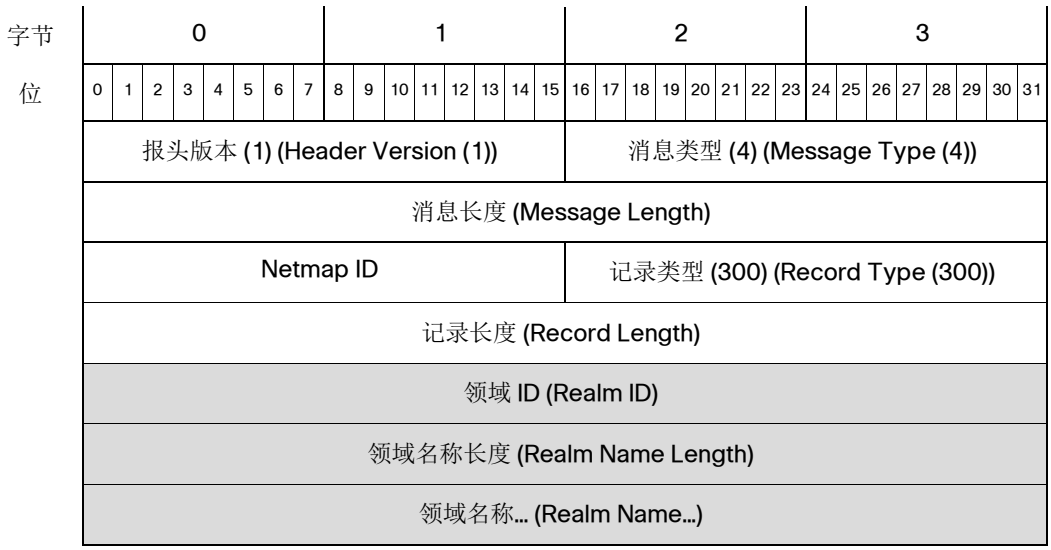
下表对安全情景名称记录中的字段进行了说明。

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。

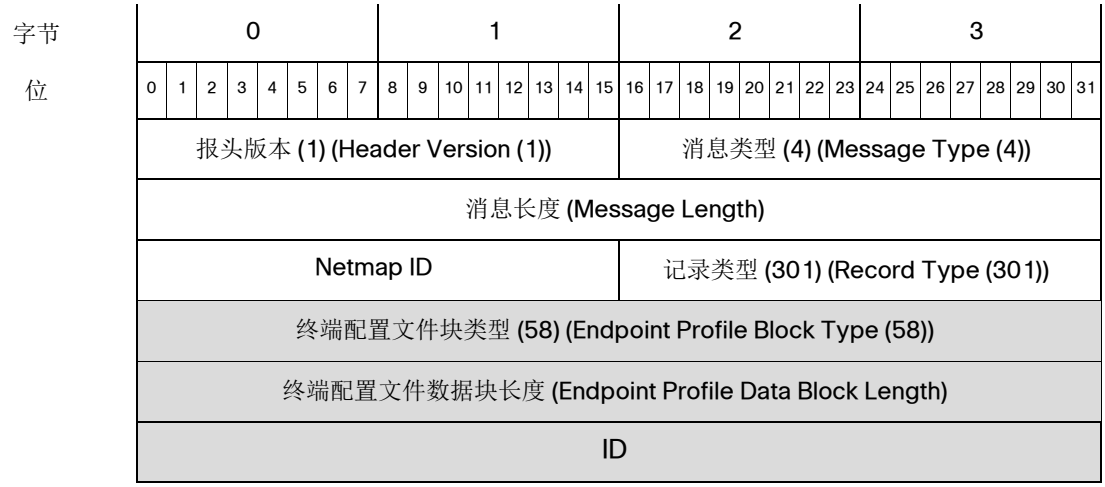
表 3-35 领域元数据记录字段

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。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (302) (Record Type (302))															
记录长度 (Record Length)																																
安全组 ID (Security Group ID)																																
安全组名称长度 (Security Group Name Length)																																
安全组名称... (Security Group Name...)																																

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
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message 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
	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...)																															

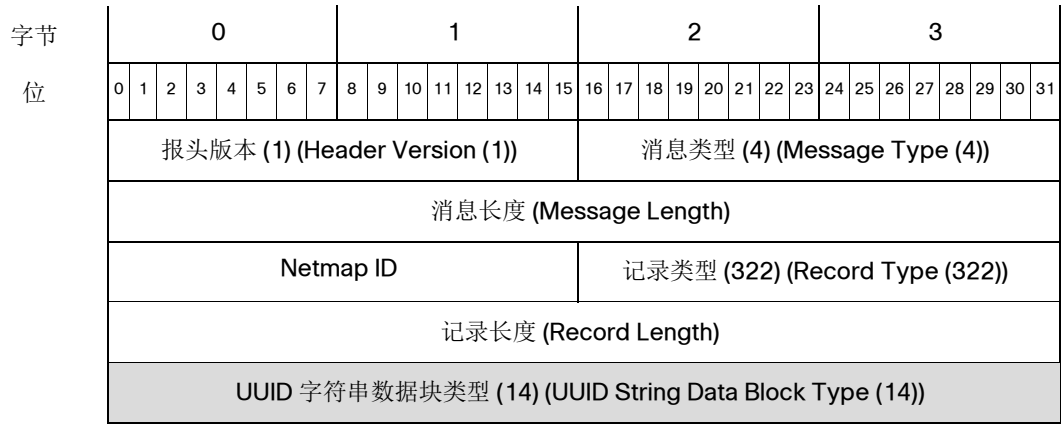
下表对 DNS 响应类型元数据记录中的字段进行了说明。

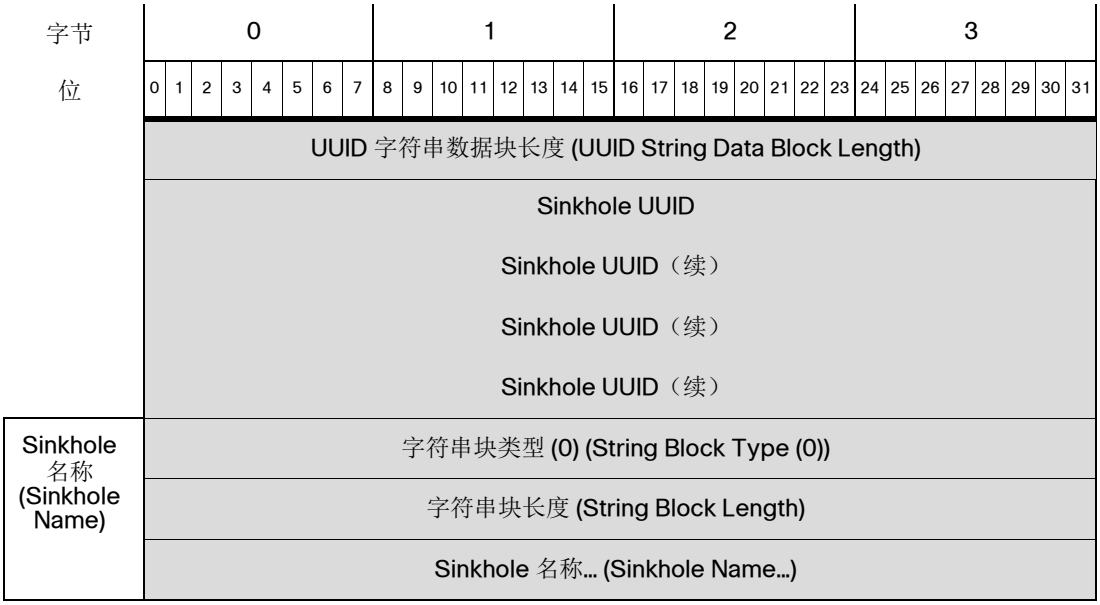
表 3-39　　DNS 响应类型元数据字段

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(DNSResponse 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。





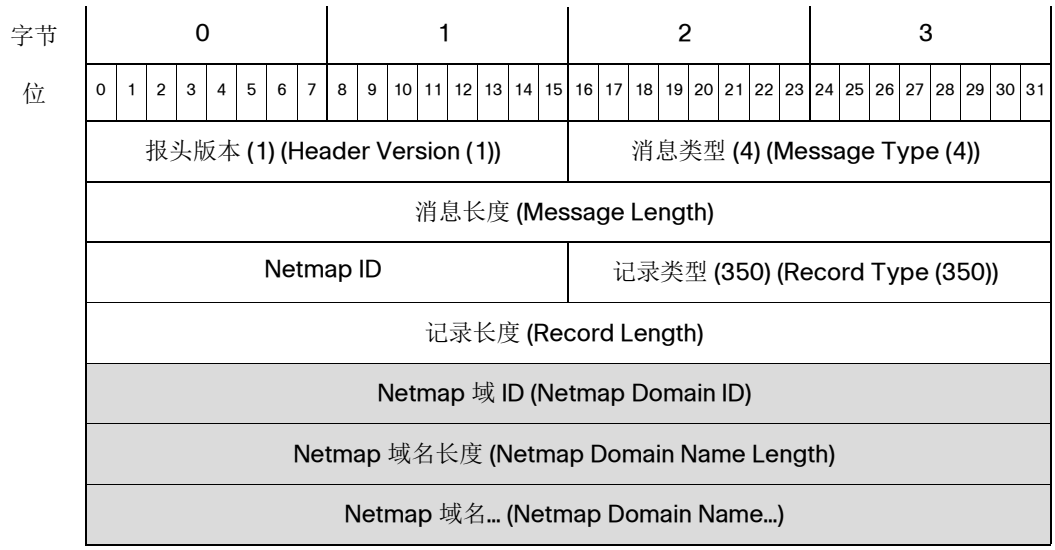
下表对 Sinkhole 元数据记录中的字段进行了说明。

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。

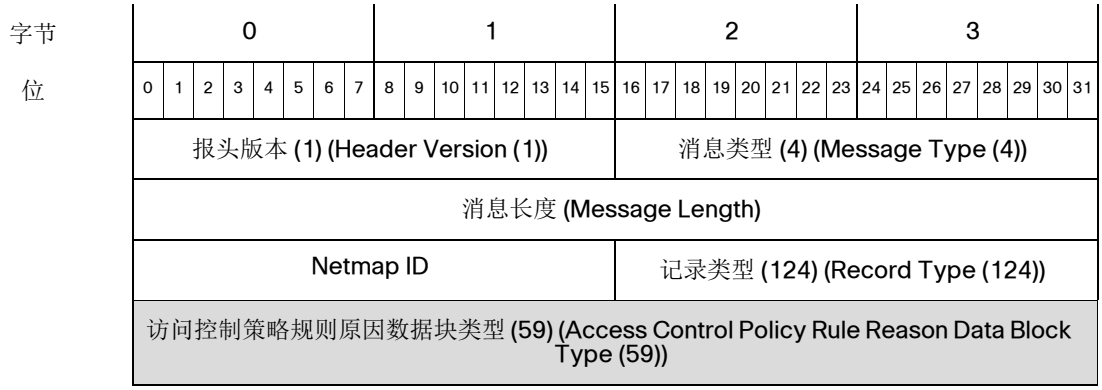
表 3-41　Sinkhole 元数据记录字段

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

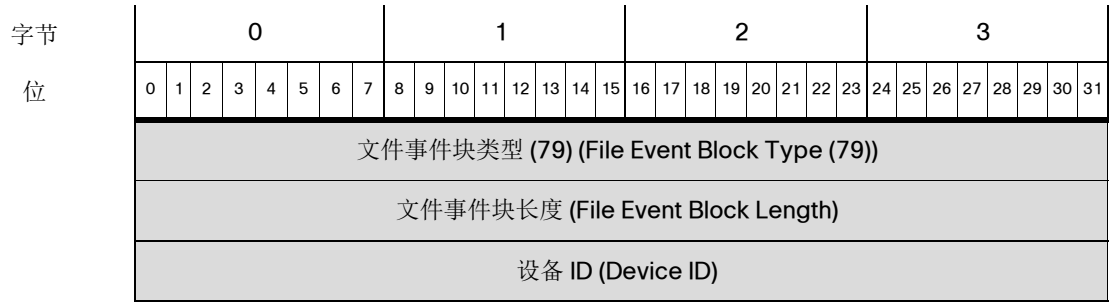
字段	数据类型	说明 (Description)
IP 信誉类别数据块类型 (IP Reputation Category Data Block Type)	uint32	启动 IP 信誉类别数据块。值始终为 22。
IP 信誉类别数据块长度 (IP Reputation Category Data Block Length)	uint32	IP 信誉类别数据块的字节总数，包括 IP 信誉类别数据块类型和长度字段的八个字节，加上随后的数据字节数。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符。
策略 UUID (Policy UUID)	uint8[16]	触发事件的策略的 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。



字节	0	1	2	3
位	0 1 2 3 4 5 6 7	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)
	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...)			

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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）																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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）																															
	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...)																							
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 响应代码 (HTTP Response																							
入口 VRF	HTTP Rsp 代码 (HTTP Rsp Code)（续）								字符串块类型 (0) (String Block Type (0))																							
	字符串块类型 (Blk Type)（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-CUSTOMSIGNATURE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）

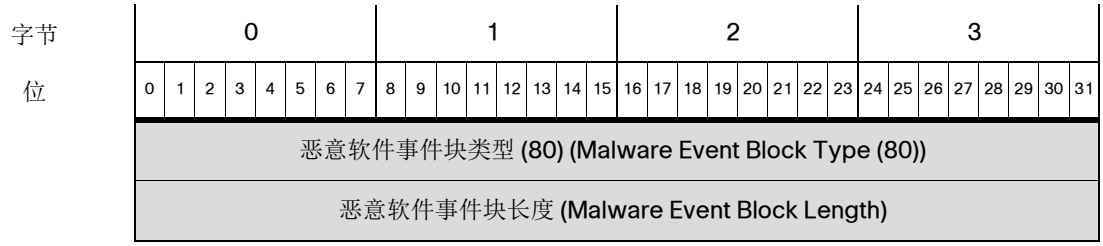
字段	数据类型	说明 (Description)
存档 SHA (Archive SHA)	字符串	包含该文件的父存档的 SHA1 散列。
字符串块类型 (String Block Type)	uint32	启动包含“存档名称”(Archive Name) 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	存档名称字符串数据块中的字节数，包括块类型和信头字段的八个字节，加上入侵策略名称中的字节数。
存档名称 (Archive Name)	字符串	父存档的名称。
存档深度 (Archive Depth)	uint8	嵌套文件的层数。例如，如果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。

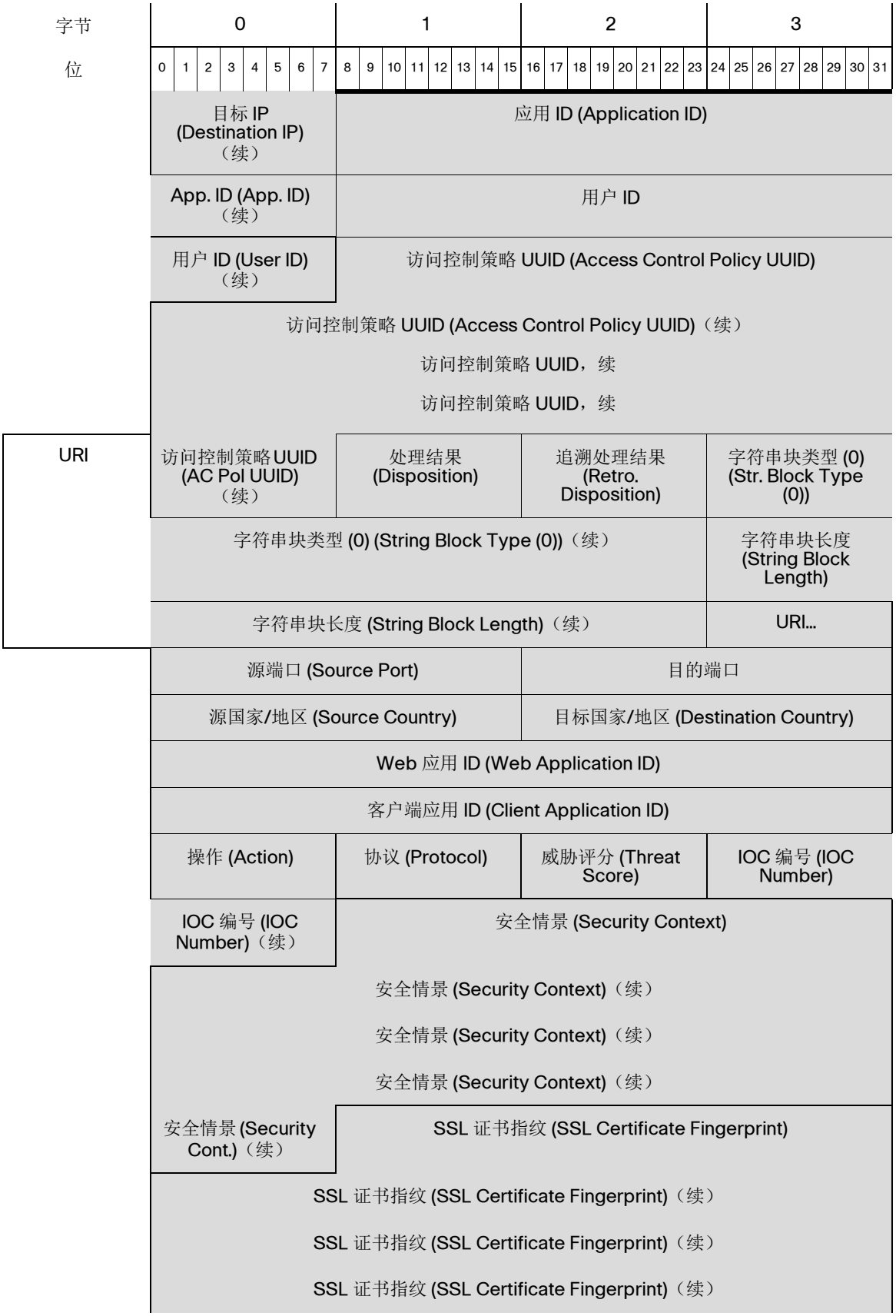
您可以通过在事件版本为 8 且事件代码为 101 的请求消息中设置恶意软件事件标志（“请求标志”(Request Flags) 字段中的位 30），将该事件作为恶意软件事件记录的一部分进行请求。

下图显示恶意软件事件数据块的结构。



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

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (510) (Record Type (510))															
记录长度 (Record Length)																																
文件类型 ID (File Type ID)																																
文件类型长度 (File Type Length)																																
文件类型名称... (File Type Name...)																																

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）

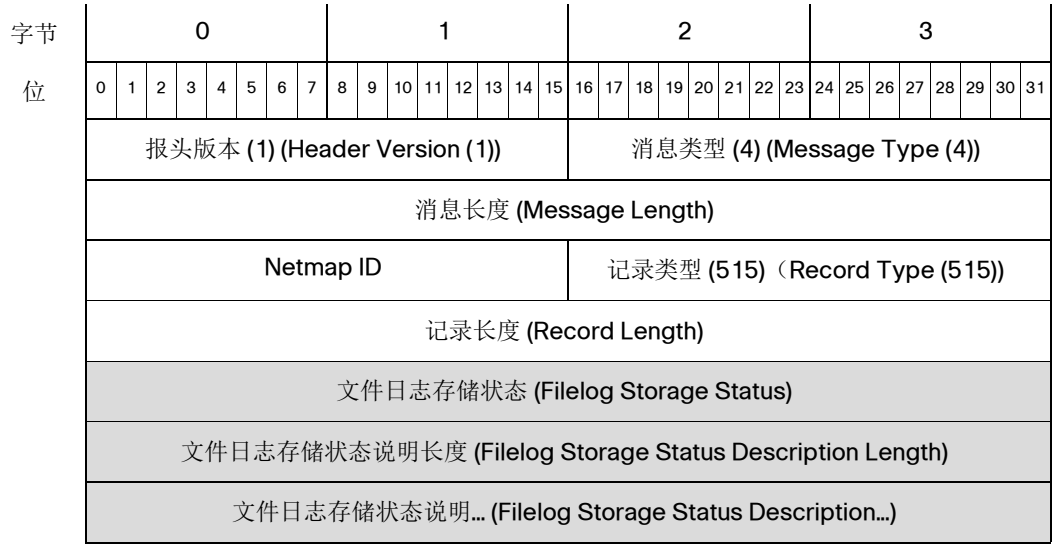
字段	数据类型	说明 (Description)
攻击情景 (Attack Scenarios)	字符串	可能的攻击的示例。
字符串块类型 (String Block Type)	uint32	启动包含与规则相关的易攻击性的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“易攻击性”(Ease of Attack) 字段中的字节数。
易攻击性 (Ease of Attack)	字符串	攻击是被视为简单、中等、困难还是艰难，以及是否可以使用脚本执行此攻击。
字符串块类型 (String 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。

表 3-49　规则文档数据块字段 （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“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。



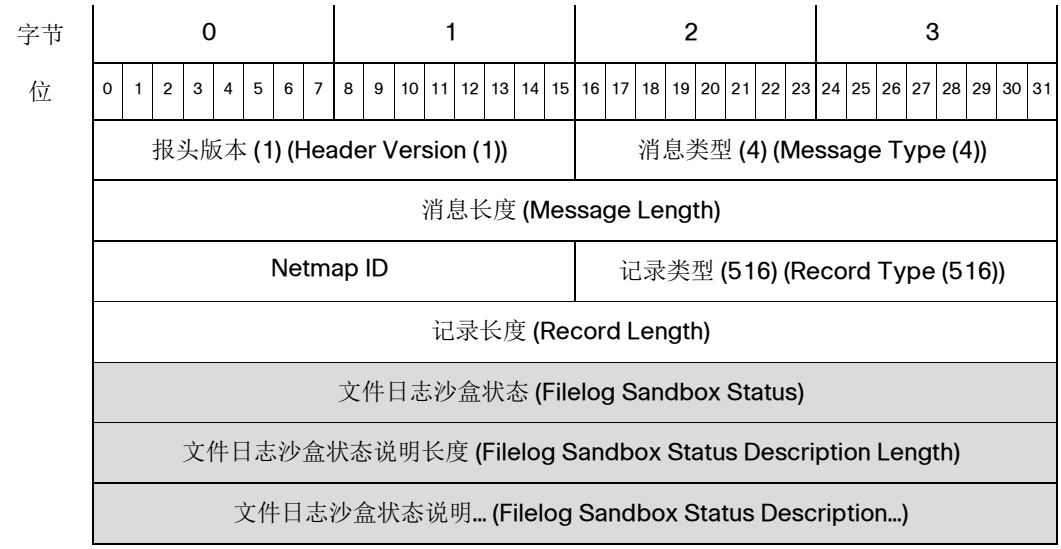
下表对文件日志存储元数据记录中的字段进行了说明。

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。



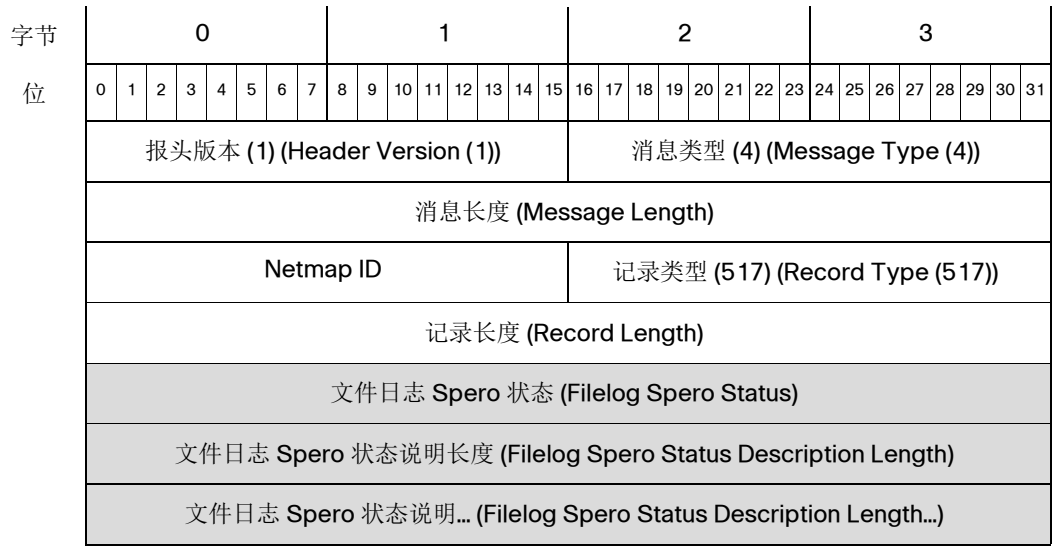
下表对文件日志沙盒元数据记录中的字段进行了说明。

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。



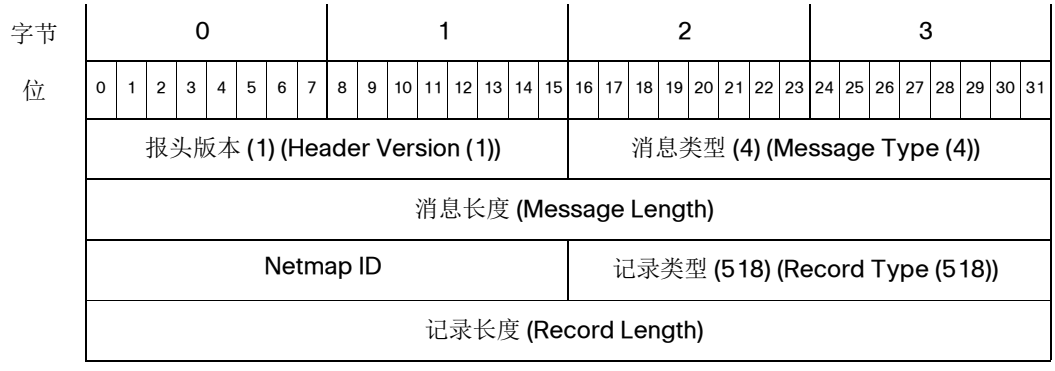
下表对文件日志 Spero 元数据记录中的字段进行了说明。

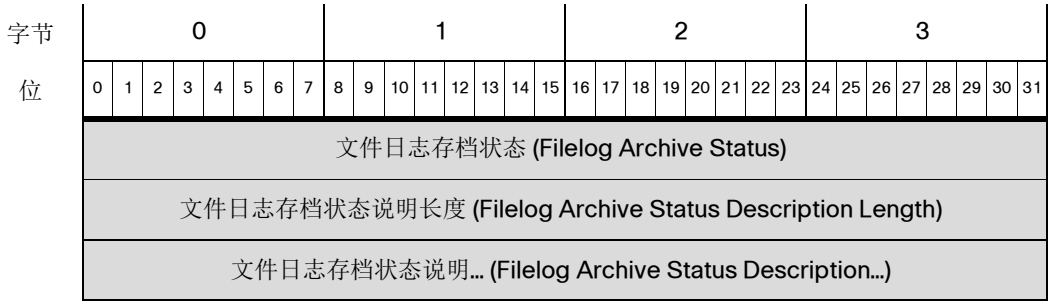
表 3-52　　文件日志 Spero 元数据记录字段

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。





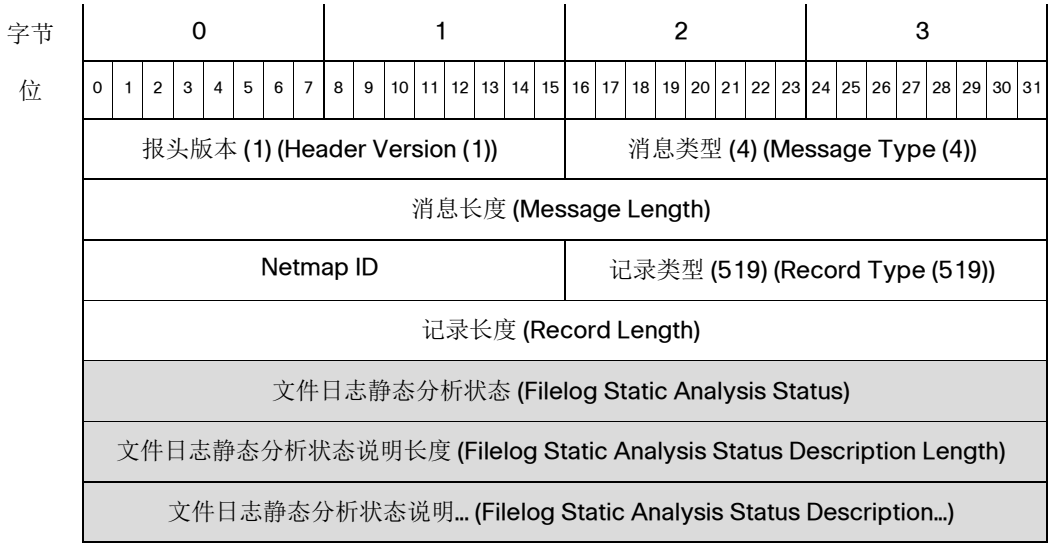
下表对文件日志存档元数据记录中的字段进行了说明。

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。

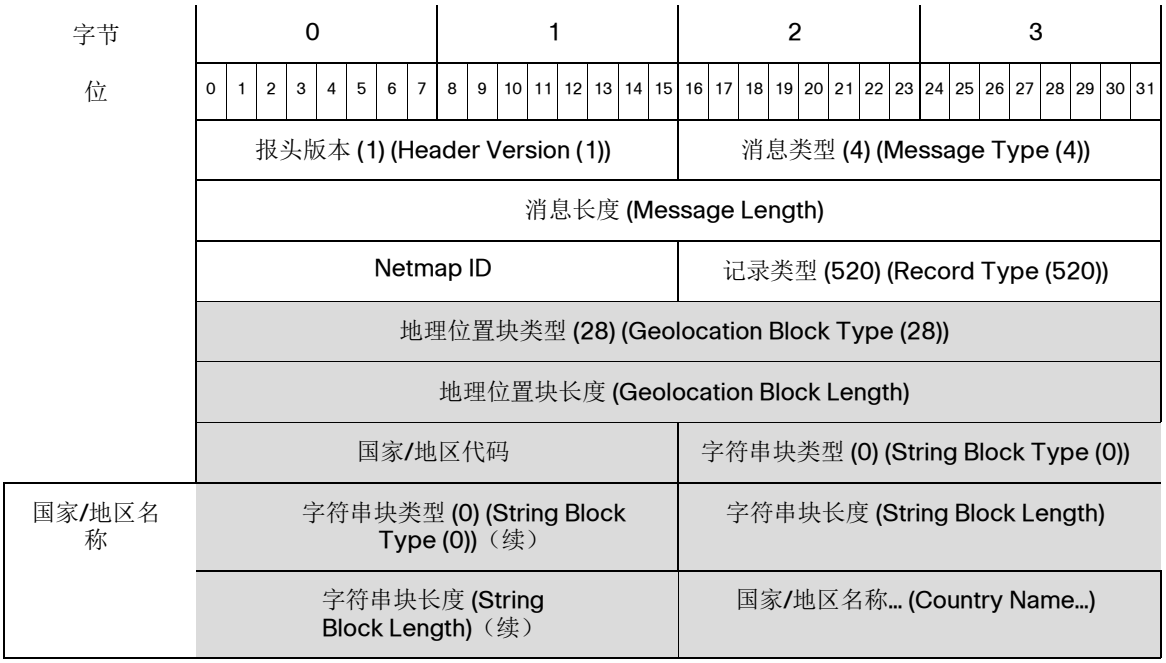
表 3-54　　文件日志静态分析元数据记录字段

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：



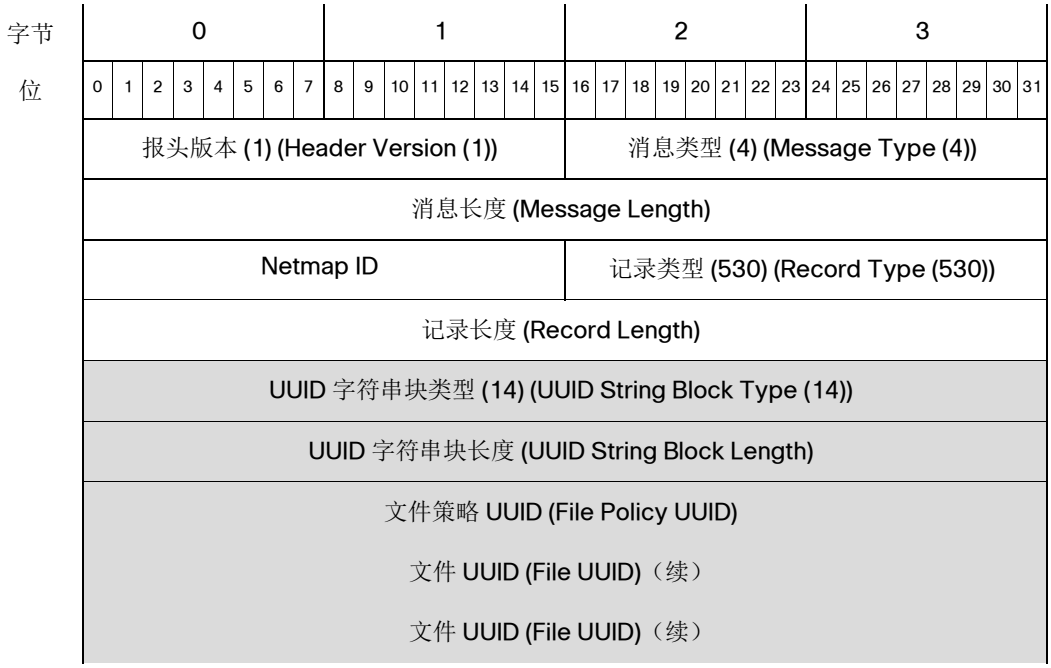
下表对地理位置数据块中的字段进行了说明。

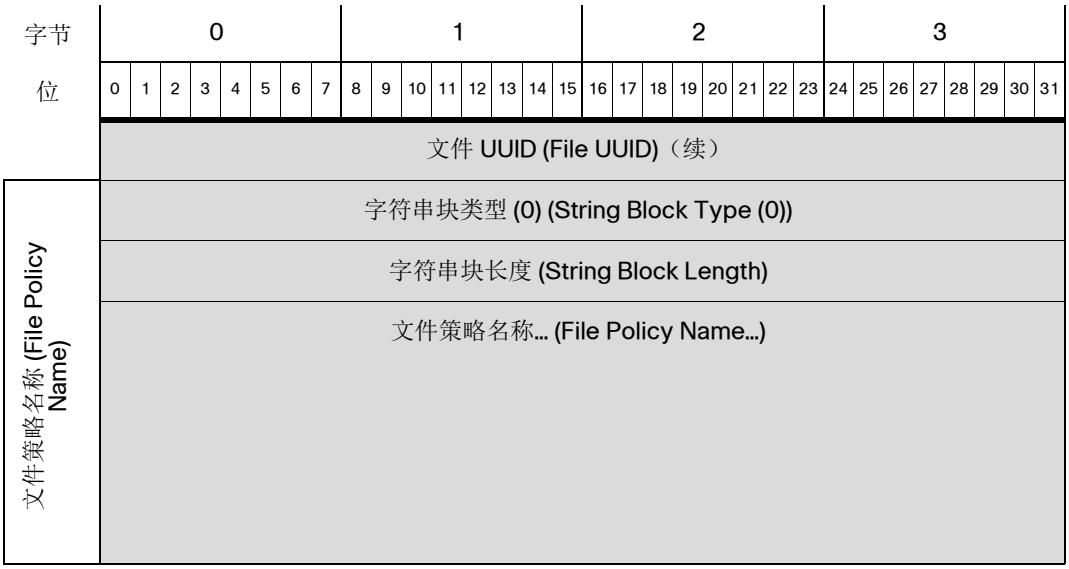
表 3-55　　地理位置数据块字段

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。





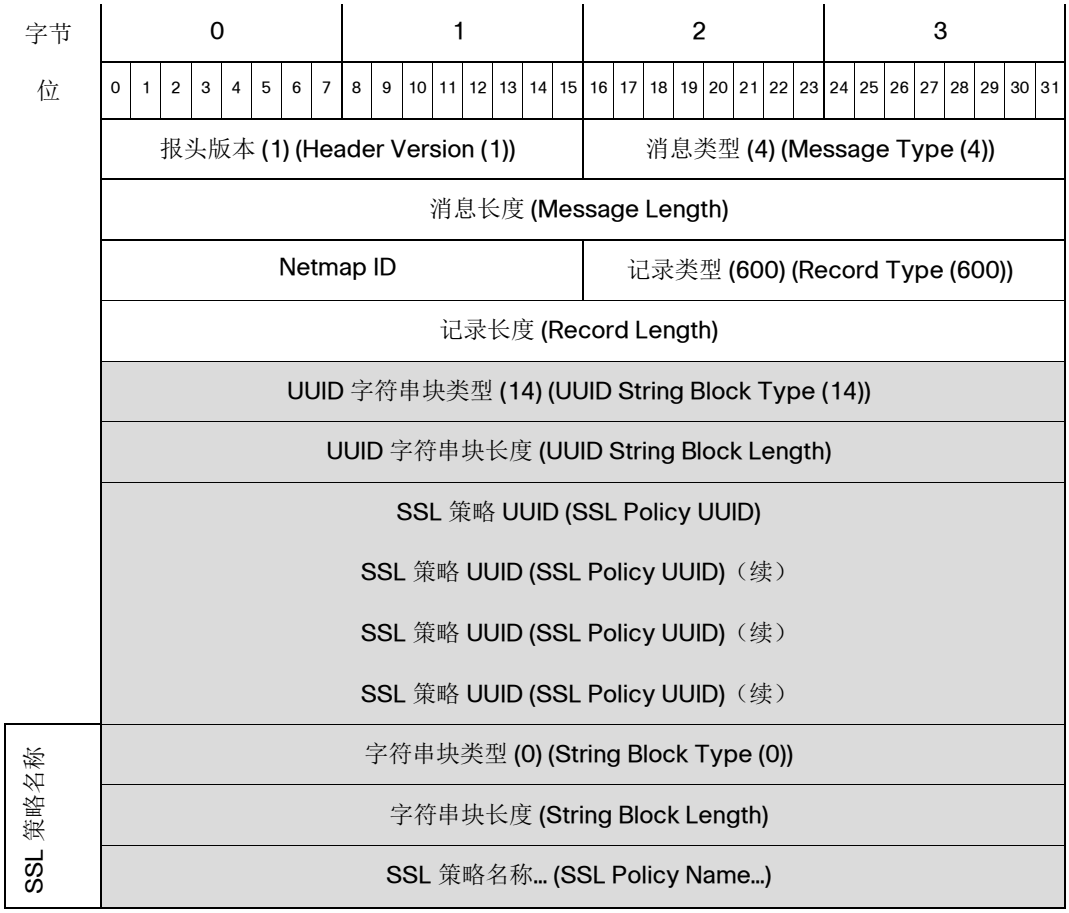
下表对文件策略名称记录中的字段进行了说明。

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。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (604) (Record Type (604))														
记录长度 (Record Length)																																
SSL 版本 ID (SSL Version ID)																																
SSL 版本名称长度 (SSL Version Name Length)																																
SSL 版本名称... (SSL Version Name...)																																

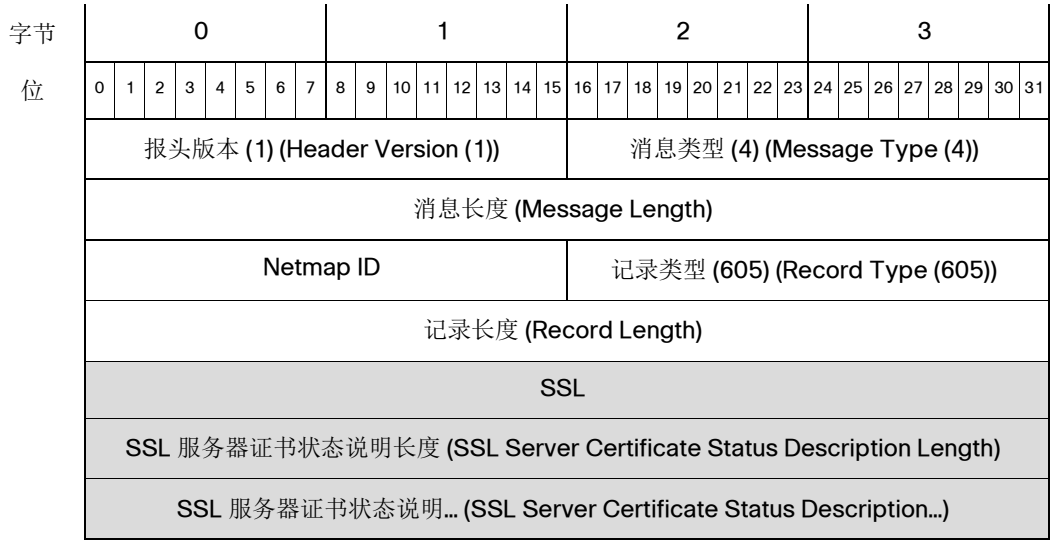
下表对 SSL 版本记录中的字段进行了说明。

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(SSLVersionName)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。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (606) (Record Type (606))															
记录长度 (Record Length)																																
SSL 实际操作编号 (SSL Actual Action Number)																																
SSL 实际操作说明长度 (SSL Actual Action Description Length)																																
SSL 实际操作说明... (SSL Actual Action Description...)																																

下表对 SSL 实际操作记录中的字段进行了说明。

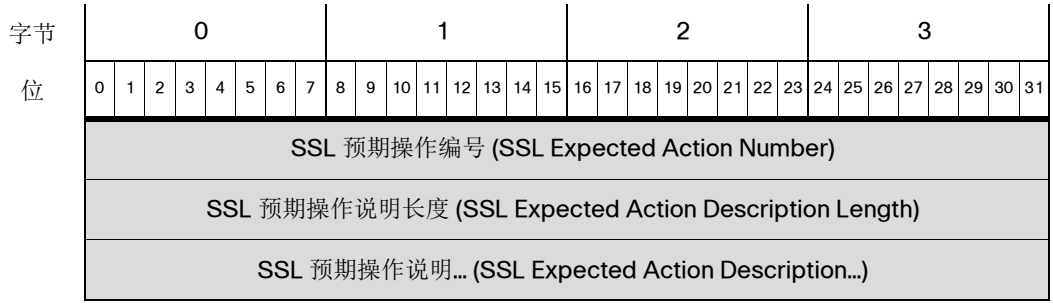
表 3-62　　SSL 实际操作字段

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。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (607) (Record Type (607))															
记录长度 (Record Length)																																



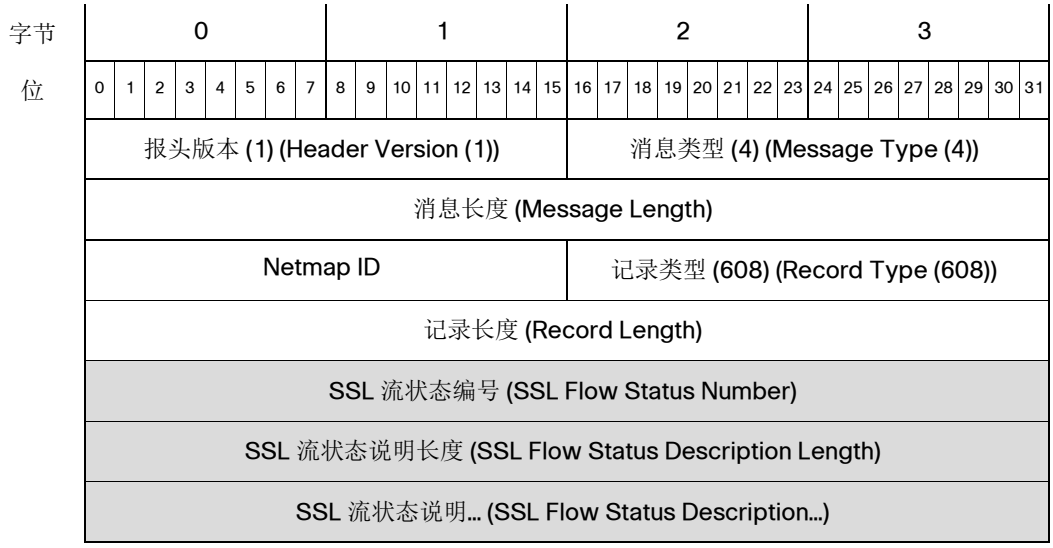
下表对 SSL 预期操作记录中的字段进行了说明。

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 SSLURL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。

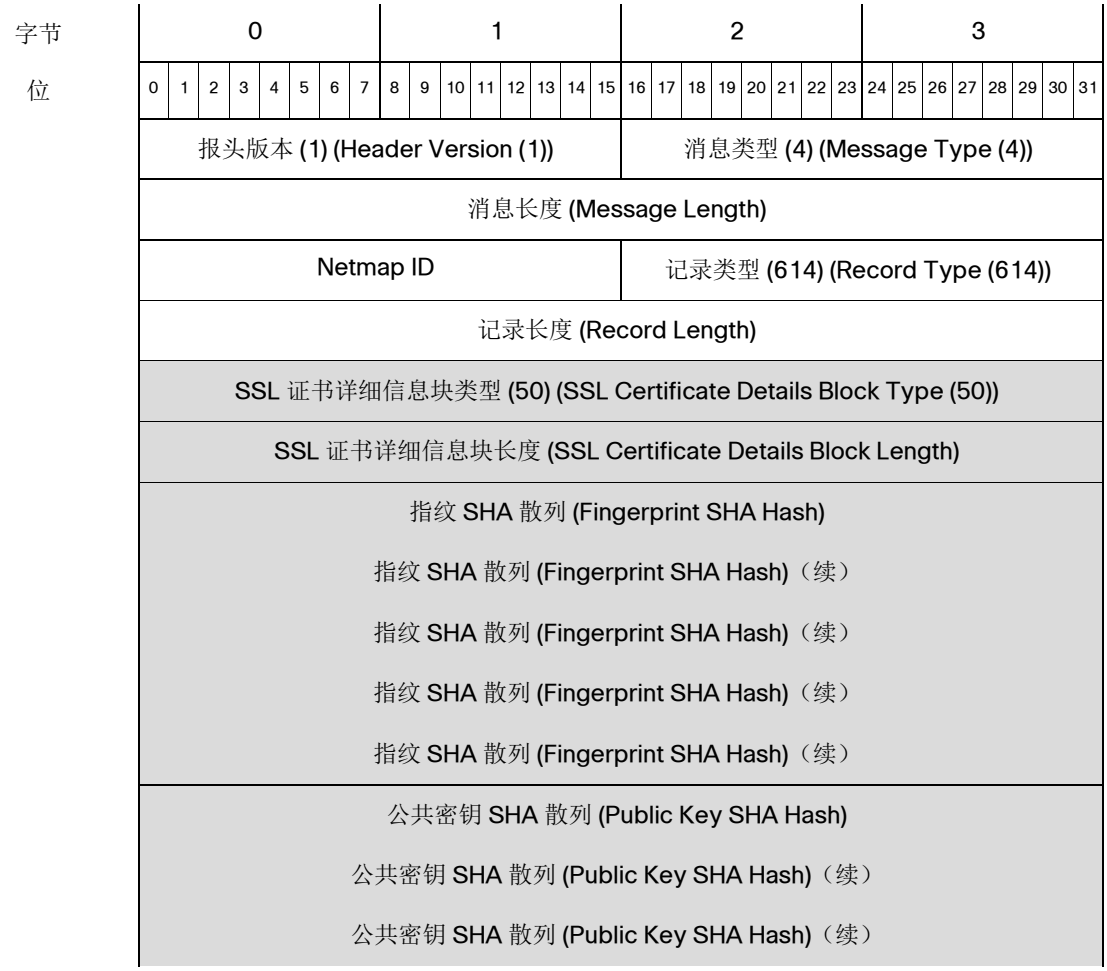
表 3-65 SSL URL 类别字段

字段	数据类型	说明 (Description)
SSLURL类别编号(SSLURL Category Number)	uint32	指示 SSL URL 类别的编号。此字段是此记录的唯一密钥。
SSLURL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。
SSLURL类别说明(SSL URL Category Description)	字符串	对 SSL URL 类别的说明。

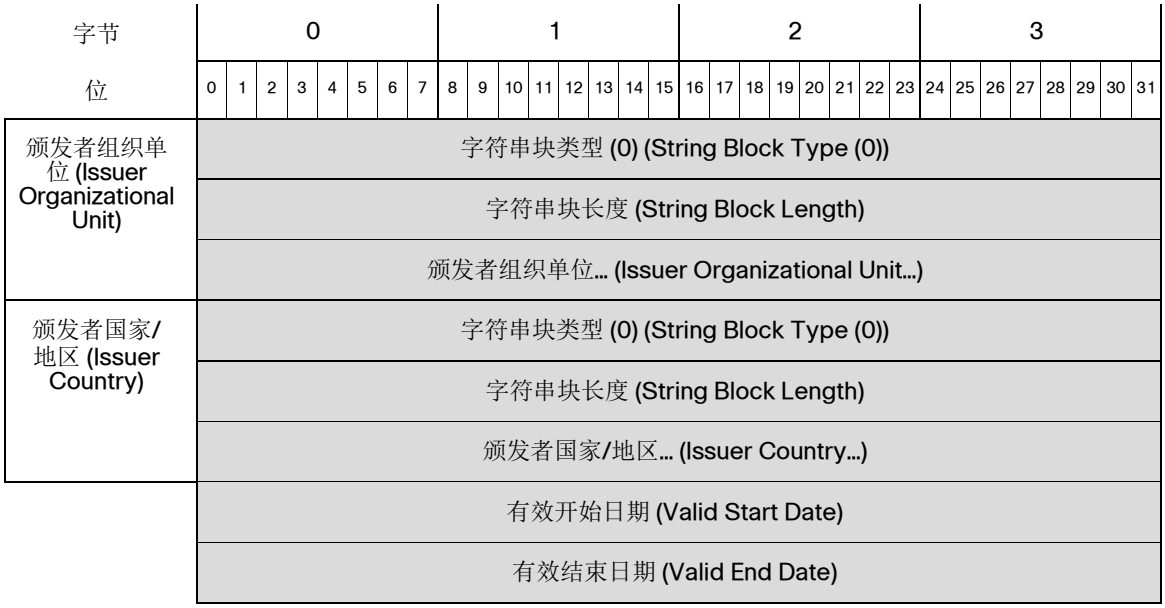
用于 5.4+ 的 SSL 证书详细信息数据块

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）																															
	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...)																															
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...)																															



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。
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。

表 3-66　SSL 证书详细信息数据块字段 （续）

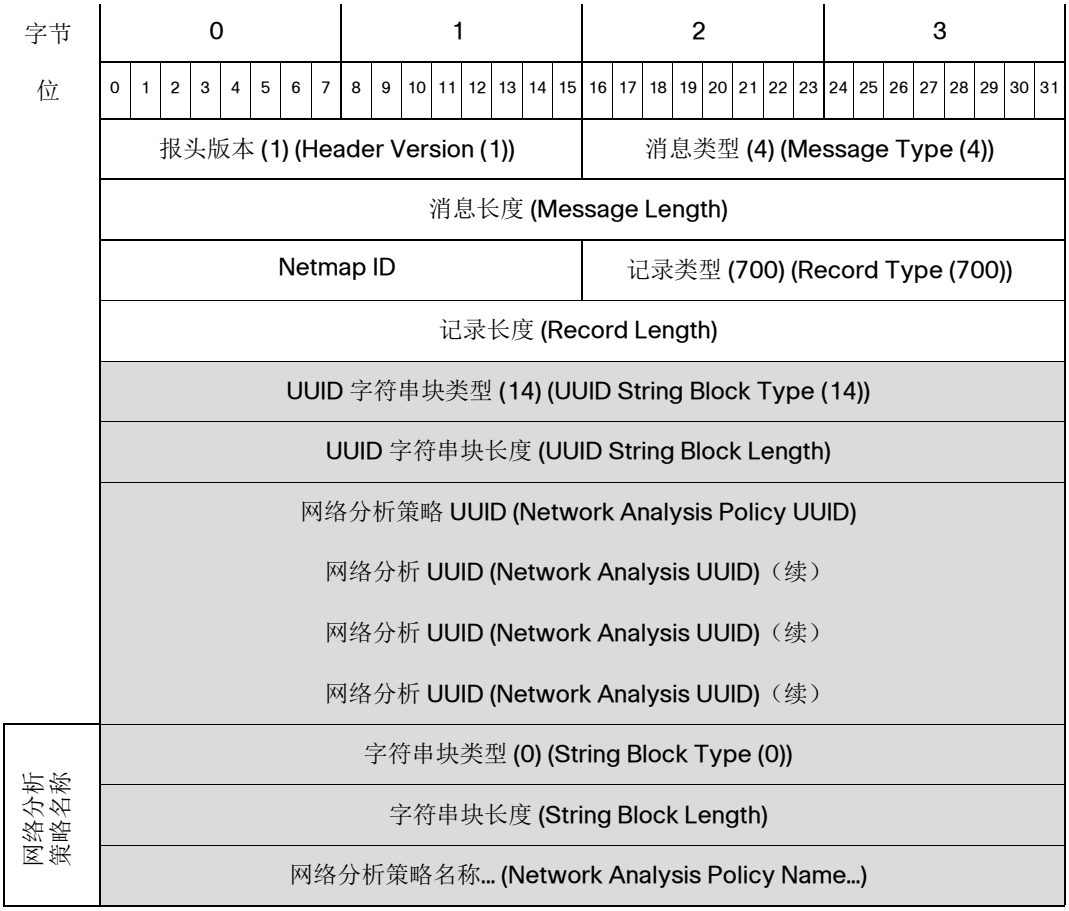
字段	数据类型	说明 (Description)
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上“类别”(Category) 字段中的字节数。
持有者常用名 (Subject Common Name)	字符串	SSL证书的持有者常用名。这通常是证书持有者的主机和域名，但也可能包含其他信息。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的事件类型的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，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。
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。

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。



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。
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。

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)
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。

当地语言翻译版本说明

思科可能会在某些地方提供本内容的当地语言翻译版本。请注意，翻译版本仅供参考，如有任何不一致之处，以本内容的英文版本为准。