了解发现和连接数据结构

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

发现事件包含两个事件子类别：

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

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

有关从 eStreamer 服务器请求发现或连接事件的信息，请参阅请求标志，第 2-11 页。

有关 eStreamer 事件数据消息的通用结构的信息，请参阅了解事件数据消息的组织，第 2-16 页。

有关发现和连接事件数据结构的详细信息，请参阅本章中的以下各节：

- 发现和连接事件数据消息，第 4-2 页提供 eStreamer 用于主机发现、用户以及连接消息的结构的高级视图。
- 发现和连接事件记录类型，第 4-2 页对发现和连接事件的记录类型进行了说明。
- 发现事件的元数据，第 4-5 页介绍要将数字和编码数据转换成文本（例如，将事件中的用户 ID 转换成用户名）并可以向其请求情景信息的元数据记录。
- 发现事件报头 5.2+，第 4-40 页对所有发现和连接消息中使用的标准事件报头的结构，以及事件类型和事件子类型字段中可能出现的值进行了说明。事件类型和子类型字段进一步定义消息中包含的数据记录的结构。
- 按事件类型划分的主机发现结构，第 4-44 页对 eStreamer 用于各种主机发现事件类型的数据记录的结构进行了说明。
- 按事件类型划分的用户数据结构，第 4-61 页对 eStreamer 用于各种用户事件类型的数据记录的结构进行了说明。
- 了解发现（系列 1）块，第 4-63 页对用于在发现和连接事件消息中传输复杂记录的数据块结构系列进行了说明。关联事件中也有系列 1 数据块。
- 用户漏洞数据块 5.0+，第 4-161 页对用于传输复杂用户事件记录的其他系列 1 数据块结构进行了说明。

提示 请参阅“数据结构示例”节，第 A-1 页了解说明样本发现事件的示例。

发现和连接事件数据消息

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

- 选项 netmap ID
- 定义记录类型的记录报头
- 识别和描述事件并明确标识事件类型和子类型的发现事件报头。有关信息，请参阅发现事件报头 5.2+，第 4-40 页。
- 由块报头和数据块组成的数据记录。发现和连接事件数据消息使用系列 1 数据块。有关信息，请参阅主机发现和连接数据块，第 4-64 页或用户漏洞数据块 5.0+，第 4-161 页。

发现和连接事件记录类型

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

表 4-1　　发现和连接事件记录类型

记录类型	包含块类型	系列	说明	记录状态	... 中描述的数据格式
10	139	1	检测到的新主机	当前	新主机消息与主机上次查看时间消息，第 4-45 页
11	103	1	新 TCP 服务器	当前	服务器消息，第 4-46 页
12	103	1	新 UDP 服务器	当前	服务器消息，第 4-46 页
13	4	1	新网络协议	当前	新网络协议消息，第 4-47 页
14	4	1	新传输协议	当前	新传输协议消息，第 4-47 页
15	122	1	新客户端应用	当前	客户端应用消息，第 4-47 页
16	103	1	TCP 服务器信息更新	当前	服务器消息，第 4-46 页
17	103	1	UDP 服务器信息更新	当前	服务器消息，第 4-46 页
18	53	1	操作系统信息更新	当前	操作系统更新消息，第 4-49 页
19	不适用	不适用	主机超时	当前	IP 地址已重用和主机超时 / 已删除主机消息，第 4-50 页
20	不适用	不适用	主机 IP 地址已重用	当前	IP 地址已重用和主机超时 / 已删除主机消息，第 4-50 页
21	不适用	不适用	已删除主机：已达主机限制	当前	IP 地址已重用和主机超时 / 已删除主机消息，第 4-50 页
22	不适用	不适用	跳数更改	当前	跳数更改消息，第 4-50 页
23	不适用	不适用	TCP 端口已关闭	当前	TCP 和 UDP 端口已关闭 / 超时消息，第 4-50 页
24	不适用	不适用	UDP 端口已关闭	当前	TCP 和 UDP 端口已关闭 / 超时消息，第 4-50 页

表 4-1　　发现和连接事件记录类型 （续）

记录类型	包含块类型	系列	说明	记录状态	... 中描述的数据格式
25	不适用	不适用	TCP 端口超时	当前	TCP 和 UDP 端口已关闭 / 超时消息，第 4-50 页
26	不适用	不适用	UDP 端口超时	当前	TCP 和 UDP 端口已关闭 / 超时消息，第 4-50 页
27	不适用	不适用	MAC 信息更改	当前	MAC 地址消息，第 4-51 页
28	不适用	不适用	为主机检测的其他 MAC	当前	MAC 地址消息，第 4-51 页
29	不适用	不适用	主机 IP 地址已更改	当前	IP 地址更改消息，第 4-48 页
31	不适用	不适用	识别为路由器 / 网桥的主机	当前	识别为路由器 / 网桥的主机消息，第 4-51 页
34	14	1	VLAN 标记信息更新	当前	VLAN 标签信息更新消息，第 4-52 页
35	122	1	客户端应用超时	当前	客户端应用消息，第 4-47 页
42	35	1	NetBIOS 名称更改	当前	更改 NetBIOS 名称消息，第 4-52 页
44	不适用	不适用	已丢弃主机：已达主机限制	当前	IP 地址已重用和主机超时 / 已删除主机消息，第 4-50 页
45	37	1	更新横幅	当前	更新横幅消息，第 4-53 页
46	55	1	添加主机属性	当前	属性消息，第 4-57 页
47	55	1	更新主机属性	当前	属性消息，第 4-57 页
48	55	1	删除主机属性	当前	属性消息，第 4-57 页
51	103	1	TCP 服务器置信度更新	传统	服务器消息，第 4-46 页
52	103	1	UDP 服务器置信度更新	传统	服务器消息，第 4-46 页
53	53	1	操作系统置信度更新	传统	操作系统更新消息，第 4-49 页
54	不适用	不适用	指纹元数据	当前	指纹记录，第 4-6 页
55	不适用	不适用	客户端应用元数据	当前	客户端应用记录，第 4-7 页
57	不适用	不适用	漏洞元数据	当前	漏洞记录，第 4-8 页
58	不适用	不适用	临界点元数据	当前	临界点记录，第 4-11 页
59	不适用	不适用	网络协议元数据	当前	网络协议记录，第 4-12 页
60	不适用	不适用	属性元数据	当前	属性记录，第 4-12 页
61	不适用	不适用	扫描类型元数据	当前	扫描类型记录，第 4-13 页
63	不适用	不适用	服务器元数据	当前	服务记录，第 4-14 页
71	144 个	1	连接统计信息	传统	连接统计信息数据块 5.2.x，第 B-144 页
71	152	1	连接统计信息	传统	连接统计信息数据块 5.3，第 B-162 页
71	154 种	1	连接统计信息	传统	连接统计信息数据块 5.3.1，第 B-170 页
71	155	1	连接统计信息	传统	连接统计信息数据块 5.4，第 B-178 页
71	157	1	连接统计信息	传统	连接统计信息数据块 5.4.1，第 B-194 页
71	160	1	连接统计信息	传统	连接统计信息数据块 6.0.x，第 B-210 页
71	163	1	连接统计信息	当前	连接统计信息数据块 6.2+，第 4-119 页

表 4-1　　发现和连接事件记录类型 （续）

记录类型	包含块类型	系列	说明	记录状态	... 中描述的数据格式
73	136	1	连接区块	当前	连接区块消息，第 4-55 页
74	不适用	不适用	用户设置操作系统	当前	用户服务器和操作系统消息，第 4-58 页
75	不适用	不适用	用户设置服务器	当前	用户服务器和操作系统消息，第 4-58 页
76	83	1	用户删除协议	当前	用户协议消息，第 4-59 页
77	60	1	用户删除客户端应用	当前	用户客户端应用消息，第 4-59 页
78	78	1	用户删除地址	当前	用户添加和删除主机消息，第 4-55 页
79	77	1	用户删除服务器	当前	用户删除服务器消息，第 4-56 页
80	80	1	用户设置有效漏洞	当前	用于版本 4.6.1+ 的用户设置漏洞消息，第 4-55 页
81	80	1	用户设置无效漏洞	当前	用于版本 4.6.1+ 的用户设置漏洞消息，第 4-55 页
82	81	1	用户设置主机临界点	当前	用户设置主机临界点消息，第 4-57 页
83	55	1	用户设置属性值 (User Set Attribute Value)	当前	属性值消息，第 4-58 页
84	82	1	用户删除属性值	当前	属性值消息，第 4-58 页
85	78	1	用户添加主机	当前	用户添加和删除主机消息，第 4-55 页
86	不适用	不适用	用户添加服务器	当前	用户服务器和操作系统消息，第 4-58 页
87	60	1	用户添加客户端应用	当前	用户客户端应用消息，第 4-59 页
88	83	1	用户添加协议	当前	用户协议消息，第 4-59 页
89	142	1	用户添加扫描结果	当前	添加扫描结果消息，第 4-60 页
90	不适用	不适用	源类型记录	当前	源类型记录，第 4-15 页
91	不适用	不适用	源应用记录	当前	源应用记录，第 4-16 页
92	120	1	已丢弃用户更改事件	当前	用户修改消息，第 4-62 页
93	120	1	已删除用户更改事件	当前	用户修改消息，第 4-62 页
94	120	1	新用户标识事件	当前	用户修改消息，第 4-62 页
95	121	1	用户登录更改事件	当前	用户信息更新消息块，第 4-62 页
96	不适用	不适用	源检测器记录	当前	源检测器记录，第 4-16 页
98	57	2	用户记录	当前	用户记录，第 4-19 页
101	不适用	不适用	新操作系统事件	当前	新操作系统消息，第 4-60 页
102	94	1	身份冲突事件	当前	身份冲突和身份超时系统消息，第 4-60 页
103	94	1	身份超时事件	当前	身份冲突和身份超时系统消息，第 4-60 页
106	不适用	不适用	第三方扫描仪漏洞记录	当前	第三方扫描仪漏洞记录，第 4-17 页
107	122	1	客户端应用更新	当前	客户端应用消息，第 4-47 页
109	不适用	不适用	Web 应用记录	当前	Web 应用记录，第 4-20 页
114	121	1	用户登录失败事件	当前	用户信息更新消息块，第 4-62 页
115	不适用	不适用	安全区名称记录	当前	安全区名称记录，第 3-29 页

表 4-1　　发现和连接事件记录类型 （续）

记录类型	包含块类型	系列	说明	记录状态	... 中描述的数据格式
116	14	2	接口名称记录	当前	接口名称记录，第 3-30 页
117	14	2	访问控制策略名称元数据	当前	访问控制策略名称记录，第 3-31 页
118	14	2	入侵策略名称记录	当前	入侵策略名称记录，第 4-21 页
119	14	2	访问控制规则 ID 记录	当前	访问控制规则 ID 记录元数据，第 3-32 页
120	不适用	不适用	访问控制规则操作记录	当前	访问控制规则操作记录元数据，第 4-23 页
121	不适用	不适用	URL 类别记录	当前	URL 类别记录元数据，第 4-24 页
122	不适用	不适用	URL 信誉元数据	当前	URL 信誉记录元数据，第 4-24 页
124	21	2	访问控制规则原因元数据	当前	访问控制规则原因元数据，第 4-25 页
145	64	2	访问控制策略元数据	当前	访问控制策略元数据，第 4-28 页
146	64	2	预过滤器策略元数据	当前	预过滤器策略元数据，第 4-29 页
147	21	2	隧道或预过滤器规则元数据	当前	隧道或预过滤器规则元数据，第 4-30 页
160	7	1	主机 IOC 设置消息	当前	主机 IOC 设置消息，第 4-61 页
161	39	2	用于 5.3+ 的 IOC 名称数据块	当前	用于 5.3+ 的 IOC 名称数据块，第 4-36 页
162	148	1	用户主机 IOC 删除	当前	用户 IOC 更改数据块 5.3+，第 4-80 页
163	148	1	用户主机 IOC 启用	当前	用户 IOC 更改数据块 5.3+，第 4-80 页
164	148	1	用户主机 IOC 禁用	当前	用户 IOC 更改数据块 5.3+，第 4-80 页
170	95	1	VPN 用户登录事件	当前	用户信息更新消息块，第 4-62 页
171	95	1	VPN 用户注销事件	当前	用户信息更新消息块，第 4-62 页
280	22	2	安全情报类别元数据	当前	安全情报类别元数据，第 4-32 页
281	不适用	不适用	安全情报源 / 目标记录	当前	安全情报源 / 目标记录，第 4-33 页

发现事件的元数据

您可以通过元数据版本号请求元数据。有关与您的 Firepower 系统的版本对应的元数据版本，请参阅了解元数据，第 2-37 页。有关 eStreamer 如何流传输元数据记录的重要信息，请参阅元数据传输，第 2-37 页。

有关主机发现和用户事件记录的各种元数据记录类型的结构的信息，请参阅：

- 指纹记录，第 4-6 页
- 客户端应用记录，第 4-7 页
- 漏洞记录，第 4-8 页
- 临界点记录，第 4-11 页
- 网络协议记录，第 4-12 页

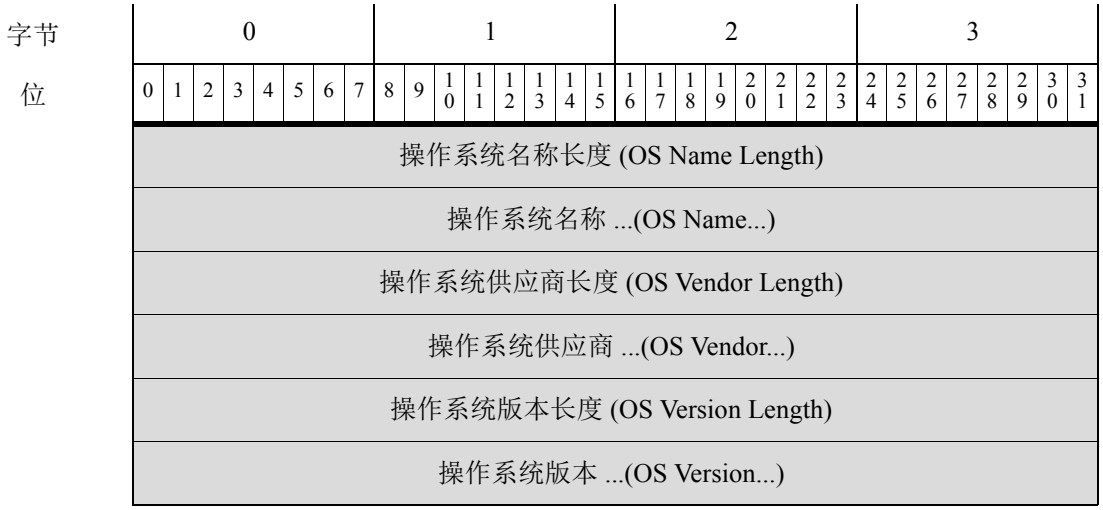
- 属性记录，第 4-12 页
- 扫描类型记录，第 4-13 页
- 服务记录，第 4-14 页
- 源类型记录，第 4-15 页
- 源应用记录，第 4-16 页
- 源检测器记录，第 4-16 页
- 第三方扫描仪漏洞记录，第 4-17 页
- 用户记录，第 4-19 页
- Web 应用记录，第 4-20 页
- 入侵策略名称记录，第 4-21 页
- 访问控制规则操作记录元数据，第 4-23 页
- URL 类别记录元数据，第 4-24 页
- URL 信誉记录元数据，第 4-24 页
- 访问控制规则原因元数据，第 4-25 页
- 安全情报类别元数据，第 4-32 页
- 安全情报源 / 目标记录，第 4-33 页

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

指纹记录

eStreamer 服务可传输用于指纹记录中的事件的指纹元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、 14、 15 或 20）时，发送指纹元数据。请参阅请求标志，第 2-11 页。）请注意， “ 记录类型 ”(Record Type) 字段（出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 54，表示指纹记录。

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



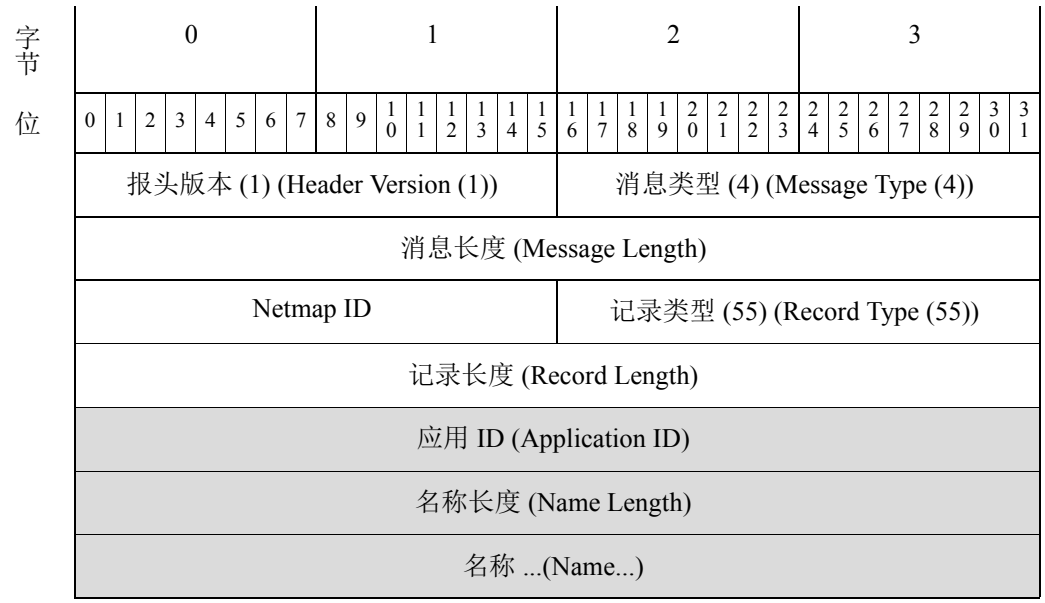
下表对指纹记录中的字段进行了说明。

表 4-2　　指纹记录字段

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

客户端应用记录

eStreamer 服务可传输用于客户端应用记录中的事件的客户端应用元数据，格式如下所示。（当设置其中一个元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、 14、 15 或 20）时，发送客户端应用元数据。请参阅请求标志，第 2-11 页。）请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 55，表示客户端应用记录。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (55) (Record Type (55))															
记录长度 (Record Length)																																
应用 ID (Application ID)																																
名称长度 (Name Length)																																
名称 ...(Name...)																																

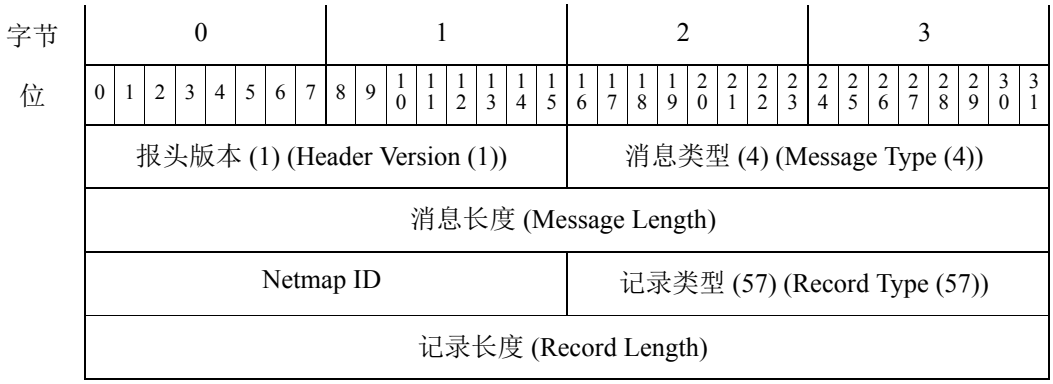
下表对客户端应用记录中的字段进行了说明。

表 4-3　　客户端应用记录字段

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

漏洞记录

eStreamer 服务可传输包含漏洞记录中的事件的漏洞信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的“请求标志”(Request Flags) 字段中的位 1、14、15 或 20）时，发送漏洞信息。请参阅请求标志，第 2-11 页。）请注意，“记录类型”(Record Type) 字段（出现在“消息长度”(Message Length) 字段后面）的值为 57，表示漏洞记录。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报头版本 (1) (Header Version (1))																	消息类型 (4) (Message Type (4))															
消息长度 (Message Length)																																
Netmap ID																	记录类型 (57) (Record Type (57))															
记录长度 (Record Length)																																

下表对漏洞记录中的字段进行了说明。

表 4-4　　漏洞记录字段

字段	数据类型	说明
漏洞 ID (Vulnerability ID)	uint32	漏洞 ID 号码。此字段是此记录的唯一密钥。
影响 (Impact)	uint32	漏洞影响，与通过入侵数据、主机发现事件和漏洞评估的关联确定的影响级别对应。其值可能为 1 至 10，其中 10 表示其严重程度最高。漏洞的影响级别由 Bugtraq 条目编写者确定。

表 4-4　　漏洞记录字段 （续）

字段	数据类型	说明
攻击 (Exploits)	uint8	指示是否存在已知的对漏洞的攻击。可能的值包括： • 0 - 是 • 1 - 否
远程 (Remote)	uint8	指示漏洞是否会通过网络被利用。可能的值包括： • 0 - 是 • 1 - 否 • 空白 - 受远程攻击的可能性未知
录入日期长度 (Entry Date Length)	uint32	录入日期字段的长度。
录入日期 (Entry Date)	字符串	在数据库中输入漏洞时的日期。
发布日期长度 (Published Date Length)	uint32	发布日期字段的长度。
发布日期 (Published Date)	字符串	发布漏洞的日期。
修改日期长度 (Modified Date Length)	uint32	修改日期字段的长度。
修改日期 (Modified Date)	字符串	最近修改漏洞的日期 （如果适用）。
标题长度 (Title Length)	uint32	标题字段的长度。
标题 (Title)	字符串	漏洞的标题。
简短说明长度 (Short Description Length)	uint32	简短说明字段的长度。
简短描述 (Short Description)	字符串	对漏洞的概述。
说明长度 (Description Length)	uint32	说明字段的长度。
说明 (Description)	字符串	对漏洞的一般说明。
技术说明长度 (Technical Description Length)	uint32	技术说明字段的长度。
技术说明 (Technical Description)	字符串	对漏洞的技术说明。

表 4-4　　漏洞记录字段 （续）

字段	数据类型	说明
解决方案长度 (Solution Length)	uint32	解决方案字段的长度。
解决方案 (Solution)	字符串	对漏洞的解决方案。

临界点记录

eStreamer 服务可传输包含临界点记录中的事件的主机临界点信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、14、15 或 20）时，发送临界点信息。请参阅请求标志，第 2-11 页。）请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 58，表示临界点记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (58) (Record Type (58))															
记录长度 (Record Length)																																
临界点 ID (Criticality ID)																																
名称长度 (Name Length)																																
名称 ...(Name...)																																

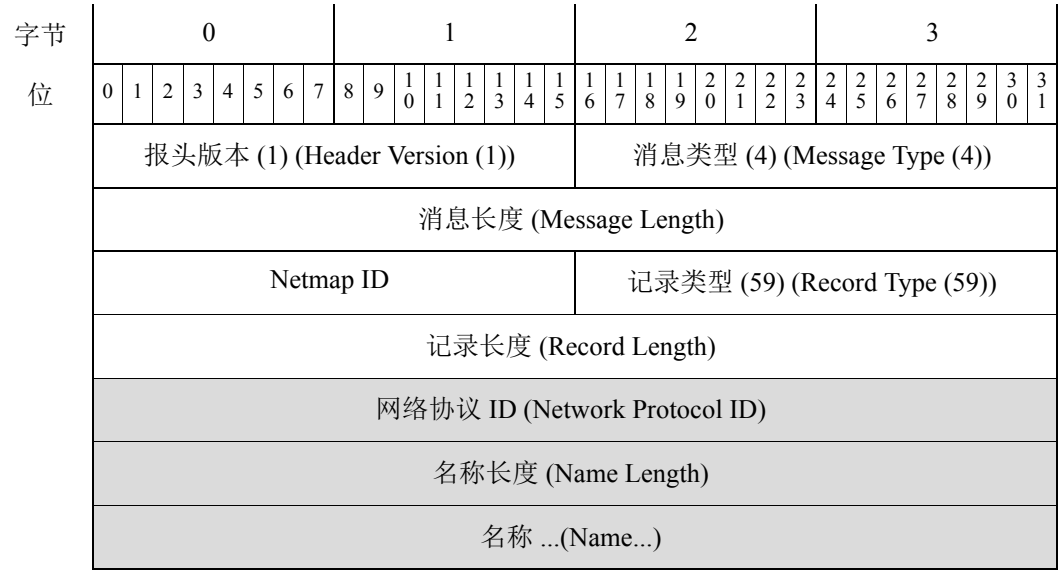
下表对临界点记录中的字段进行了说明。

表 4-5　　临界点记录字段

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

网络协议记录

eStreamer 服务可传输包含网络协议记录中的事件的网络协议信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、14、15 或 20）时，发送网络协议信息。请参阅请求标志，第 2-11 页。）请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 59，表示网络协议记录。



下表对网络协议记录中的字段进行了说明。

表 4-6　网络协议记录字段

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

属性记录

eStreamer 服务可传输包含属性记录中的事件的属性信息的元数据，格式如下所示。（当设置其中一个元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、 14、 15 或 20）时，发送属性信息。请参阅请求标志，第 2-11 页。）请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 60，表示属性记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (60) (Record Type (60))															
记录长度 (Record Length)																																
属性 ID (Attribute ID)																																
名称长度 (Name Length)																																
名称 ...(Name...)																																

下表对属性记录中的字段进行了说明。

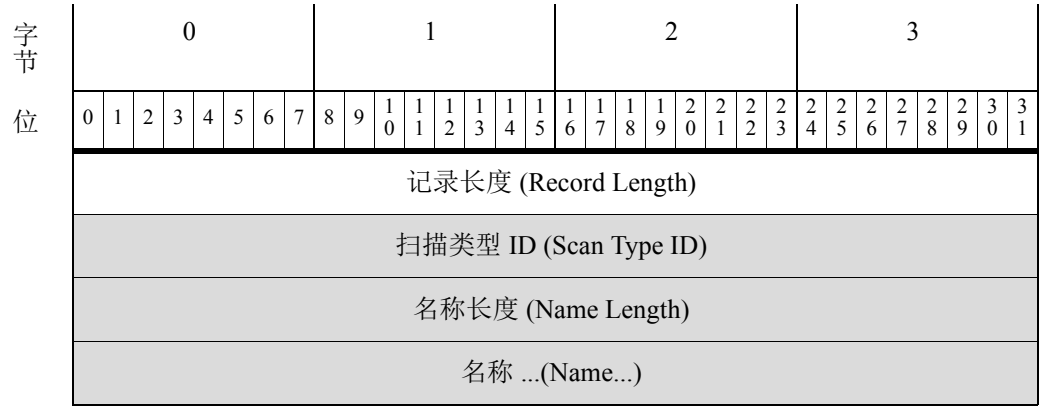
表 4-7　　属性记录字段

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

扫描类型记录

eStreamer 服务可传输包含扫描类型记录中的事件的扫描类型信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、14、15 或 20）时，发送扫描类型信息。请参阅请求标志，第 2-11 页。）请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 61，表示扫描类型记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (61) (Record Type (61))															



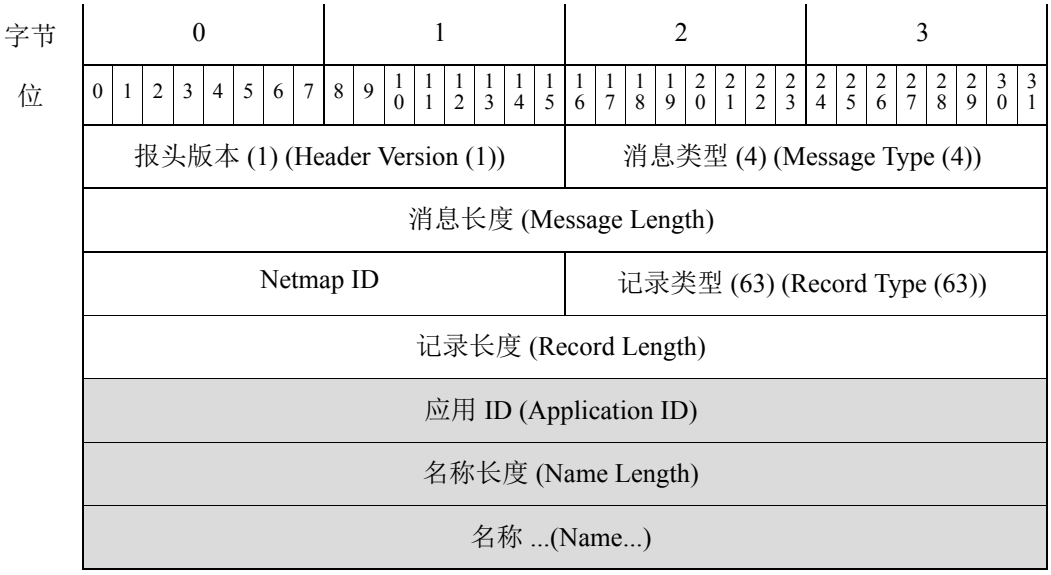
下表对扫描类型记录中的字段进行了说明。

表 4-8　　扫描类型记录字段

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

服务记录

eStreamer 服务可传输包含服务记录中事件的服务信息的元数据，格式如下所示。服务应用协议的应用 ID 提供对元数据的交叉引用。（当设置其中一个元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、 14、 15 或 20）时，发送服务信息。请参阅请求标志，第 2-11 页。）请注意， “ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 63，表示服务记录。



下表介绍服务记录中的字段。

表 4-9　　服务记录字段

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

源类型记录

eStreamer 服务可传输包含源类型记录中的事件的源应用相关信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、14、15 或 20）时，发送源类型信息。请参阅请求标志，第 2-11 页。）请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 90，表示源类型记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (90) (Record Type (90))															
记录长度 (Record Length)																																
源类型 ID (Source Type ID)																																
名称长度 (Name Length)																																
名称 ...(Name...)																																

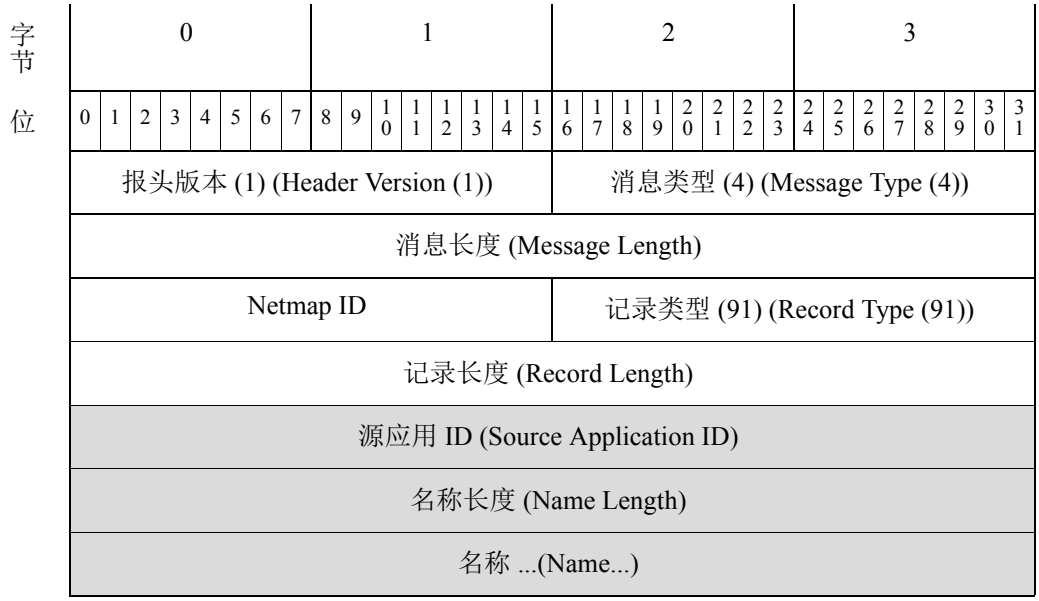
下表对源类型记录中的字段进行了说明。

表 4-10　　源类型记录字段

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

源应用记录

eStreamer 服务可传输包含源应用记录中的主机发现事件的源应用相关信息的元数据，格式如下所示。（当设置其中一个元数据标志（请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、14、15 或 20）时，发送源应用信息。请参阅请求标志，第 2-11 页。）请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 91，表示源应用记录。



下表对源应用记录中的字段进行了说明。

表 4-11　源应用记录字段

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

源检测器记录

eStreamer 服务可传输包含源类型记录中的主机发现事件的源应用相关信息的元数据，格式如下所示。（当设置其中一个元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、14、 15 或 20）时，发送源类型信息。请参阅请求标志，第 2-11 页。）请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 96，表示源检测器记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (96) (Record Type (96))															
记录长度 (Record Length)																																
源检测器 ID (Source Detector ID)																																
名称长度 (Name Length)																																
名称 ...(Name...)																																

下表对源检测器记录中的字段进行了说明。

表 4-12　　源检测器记录字段

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

第三方扫描仪漏洞记录

eStreamer 服务可传输包含第三方扫描仪漏洞记录中事件的第三方漏洞信息的元数据，格式如下所示。（当设置其中一个元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、 14、15 或 20）时，发送漏洞信息。请参阅请求标志，第 2-11 页。）请注意， “ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 106，表示第三方扫描仪漏洞记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (106) (Record Type (106))															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
记录长度 (Record Length)																																
漏洞 ID (Vulnerability ID)																																
扫描仪类型 (Scanner Type)																																
标题长度 (Title Length)																																
标题 ...(Title...)																																
说明长度 (Description Length)																																
说明 ...(Description...)																																
CVE ID 长度 (CVE ID Length)																																
CVE ID...																																
BugTraq 长度 (BugTraq Length)																																
BugTraq ID...																																

下表对漏洞记录中的字段进行了说明。

表 4-13　第三方扫描仪漏洞记录字段

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

表 4-13　第三方扫描仪漏洞记录字段 （续）

字段	数据类型	说明
BugTraq ID 长度 (BugTraq ID Length)	uint32	BugTraq ID 字段的长度。
BugTraq ID	字符串	漏洞的 BugTraq ID 号码。

用户记录

eStreamer 服务可传输包含用户记录中的系统检测到的用户的相关信息的元数据，格式如下所示。（当设置版本 4 元数据和策略事件请求标志 （分别为请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 20 和位 22）时，发送用户信息。请参阅请求标志，第 2-11 页。）请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 98，表示用户记录。

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

下表对用户记录中的字段进行了说明。

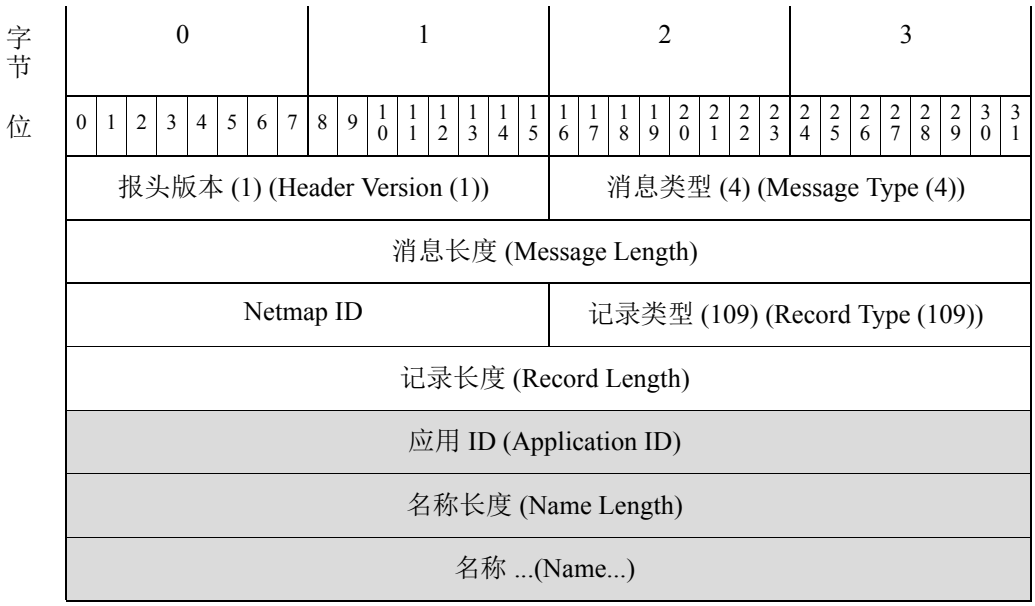
表 4-14　用户记录字段

字段	数据类型	说明
用户数据块类型 (User Data Block Type)	uint32	启动用户数据块。值始终为 57。块类型为系列 2 数据块。
用户数据块长度 (User Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的 8 个字节。
用户 ID (User ID)	uint32	用户的唯一标识符。此字段是此记录的唯一密钥。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值包括： • 165 - FTP • 426 - SIP • 547 - AOL 即时通信工具 • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle 数据库 • 788 - POP3 • 1755 - MDNS
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户名 ”(Username) 字段中的字节数。
用户名 (Username)	字符串	用户的名称

Web 应用记录

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

eStreamer 服务可传输用于 Web 应用记录中的事件的 Web 应用元数据，格式如下所示。（当设置其中一个元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、 14、 15 或 20）时，发送 Web 应用元数据。请参阅请求标志，第 2-11 页。）请注意， “ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 109，表示 Web 应用记录。



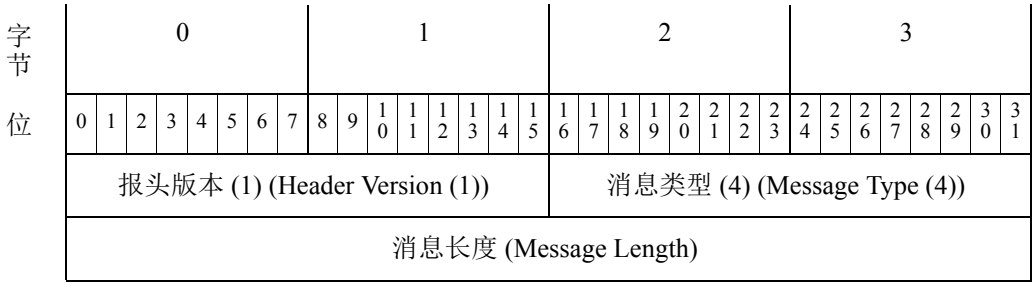
下表对 Web 应用记录中的字段进行了说明。

表 4-15　　Web 应用记录字段

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

入侵策略名称记录

eStreamer 服务可传输包含入侵策略名称记录中连接事件的入侵策略名称信息，格式如下所示。（当设置其中一个元数据标志（请求消息的 “ 请求标志 ”(Request Flags) 字段中的版本 4 元数据位 20）时，发送入侵策略名称信息。请参阅请求标志，第 2-11 页。）请注意，入侵策略名称记录字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 `118`，表示入侵策略名称记录。它包含一个 UUID 字符串数据块，该数据块的块类型为系列 2 数据块组中的 14。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (118) (Record Type (118))															
记录长度 (Record Length)																																
入侵策略名称数据块 (14) (Intrusion Policy Name Data Block (14))																																
入侵策略名称数据块长度 (Intrusion Policy Name Data Block Length)																																
入侵策略 UUID (Intrusion Policy UUID) 入侵策略 UUID (Intrusion Policy UUID) （续） 入侵策略 UUID (Intrusion Policy UUID) （续） 入侵策略 UUID (Intrusion Policy UUID) （续）																																
字符串块类型 (0) (String Block Type (0))																																
字符串块长度 (String Block Length)																																
入侵策略名称 ...(Intrusion Policy Name...)																																

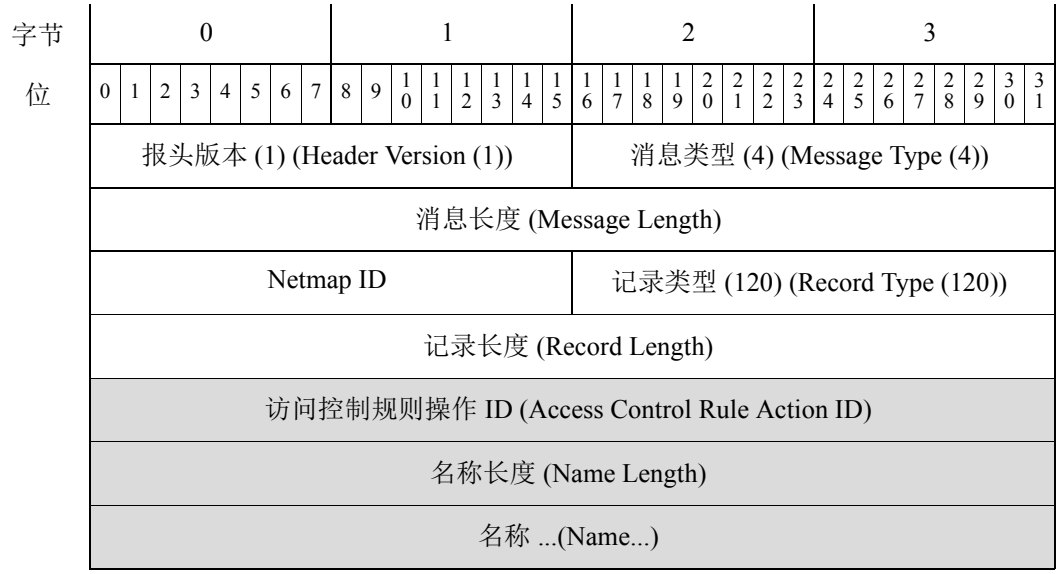
下表对入侵策略名称数据块中的字段进行了说明。

表 4-16　　入侵策略名称数据块字段

字段	数据类型	说明
入侵策略名称数据块类型 (Intrusion Policy Name Data Block Type)	uint32	启动入侵策略名称数据块。值始终为 14。块类型为系列 2 数据块。
入侵策略名称数据块长度 (Intrusion Policy Name Data Block Length)	uint32	数据块的长度。包括数据字节数加上两个数据块报头字段中的 8 个字节。
入侵策略 UUID (Intrusion Policy UUID)	uint8[16]	与连接事件相关的入侵策略的唯一标识符。此字段是此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含入侵策略名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	入侵策略名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上入侵策略名称中的字节数。
入侵策略名称 (Intrusion Policy Name)	字符串	入侵策略名称。

访问控制规则操作记录元数据

eStreamer 服务可传输包含与访问控制规则操作记录中已触发的访问控制规则相关的操作的元数据，格式如下所示。（当设置版本 4 元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 20）时，发送访问控制规则操作信息。请参阅请求标志，第 2-11 页。）请注意，访问控制规则操作记录字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 120，表示访问控制规则操作记录。



下表对访问控制规则操作记录中的字段进行了说明。

表 4-17　　访问控制规则操作记录字段

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

URL 类别记录元数据

eStreamer 服务可传输包含与 URL 类别记录的连接日志中的 URL 相关的类别名称的元数据，格式如下所示。（当设置版本 4 元数据标志（请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 20）时，发送 URL 类别信息。请参阅请求标志，第 2-11 页。）请注意，记录字段（出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 121，表示 URL 类别记录。

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

下表对 URL 类别记录中的字段进行了说明。

表 4-18　URL 类别记录字段

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

URL 信誉记录元数据

eStreamer 服务可传输包含与 URL 信誉记录内连接日志中的 URL 相关的信誉（即风险水平）的元数据，格式如下所示。（当设置版本 4 元数据标志（请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 20）时，发送 URL 信誉信息。请参阅请求标志，第 2-11 页。）请注意，URL 信誉元数据记录字段（出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 122，表示 URL 信誉元数据记录。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (122) (Record Type (122))															
记录长度 (Record Length)																																
URL 信誉 ID (URL Reputation ID)																																
名称长度 (Name Length)																																
名称 ...(Name...)																																

下表对 URL 信誉记录中的字段进行了说明。

表 4-19　　URL 信誉记录字段

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

访问控制规则原因元数据

eStreamer 服务可传输包含访问控制规则原因记录中访问控制规则触发入侵事件或连接事件的原因相关信息的元数据，格式如下所示。当设置版本 4 元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 20）时，发送访问控制规则原因元数据。请参阅请求标志，第 2-11 页。请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 124，表示访问控制规则原因记录。它包含访问控制规则原因块 （如访问控制规则原因数据块 6.0+，第 4-206 页中所记录）。访问控制规则原因数据块的块类型为系列 2 中的 59。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 (124) (Record Type (124))															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
记录长度 (Record Length)																																
访问控制规则原因块类型 (59) (Access Control Rule Reason Block Type (59))																																
访问控制规则块长度 (Access Control Rule Block Length)																																
访问控制规则原因 (Access Control Rule Reason)																																
字符串块类型 (0) (String Block Type (0))。																																
字符串块长度 (String Block Length)。																																
说明 ...(Description...)																																

下表对访问控制规则 ID 数据块中的字段进行了说明。

表 4-20　访问控制规则原因元数据字段

字段	数据类型	说明
访问控制规则原因块类型 (Access Control Rule Reason Block Type)	uint32	启动访问控制规则原因块。值始终为 59。此数据块为系列 2 数据块。
访问控制规则原因块长度 (Access Control Rule Reason Block Length)	uint32	访问控制规则原因块中的字节总数，包括访问控制规则原因块类型和长度字段的八个字节，加上随后的数据的字节数。

表 4-20　访问控制规则原因元数据字段 （续）

字段	数据类型	说明
访问控制规则原因 (Access Control Rule Reason)	uint32	访问控制规则记录连接的原因。此字段是此记录的唯一密钥。触发事件的规则的原因编号。 规则原因是一个可以在其中设置多个位的二进制位图。规则可能有多种原因。位值如下： • **1** - IP 阻止 • **2** - IP 监控 • **4** - 用户绕行 • **8** - 文件监控 • **16** - 文件阻止 • **32** - 入侵监控 • **64** - 入侵阻止 • **128** - 阻止继续传输文件 • **256** - 允许继续传输文件 • **512** - 文件自定义检测 • **1024** - SSL 阻止 • **2048** - DNS 阻止 • **4096** - DNS 监控 • **8192** - URL 阻止 • **16384** - URL 监控 • **32768** - 内容限制 • **65536** - 智能应用绕行 • **131072** - WSA 威胁
字符串块类型 (String Block Type)	uint32	启动包含与访问控制规则原因相关的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和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	对访问控制规则原因的说明。

访问控制策略元数据

eStreamer 服务在访问控制策略元数据记录内传输包含有关触发入侵事件或连接事件的访问控制策略信息的元数据，其格式如下所示。当设置版本 4 元数据标志 （请求消息的 “ 请求标志 ” 字段中的位 20）时，发送访问控制规则策略元数据。请参阅请求标志，第 2-11 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 145，表示访问控制策略元数据记录。它包含访问控制策略元数据块 （如访问控制策略元数据块 6.0+，第 4-211 页中所记录）。访问控制策略元数据块的块类型为系列 2 中的 64。

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

下表对访问控制策略数据块中的字段进行了说明。

表 4-21　访问控制策略元数据字段

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

预过滤器策略元数据

eStreamer 服务可传输包含预过滤器策略相关信息的元数据 （此策略会触发预过滤器策略记录中的入侵事件或连接事件），格式如下所示。当设置版本 4 元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 20）时，发送预过滤器策略元数据。请参阅请求标志，第 2-11 页。请注意，“ 记录类型 ” 字段 （出现在 “ 消息长度 ” 字段后面）的值为 146，表示预过滤器策略元数据记录。它包含访问控制策略元数据块 （如访问控制策略元数据块 6.0+，第 4-211 页中所记录）。访问控制策略元数据块的块类型为系列 2 中的 64。

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

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

下表对预过滤器策略元数据块中的字段进行了说明。

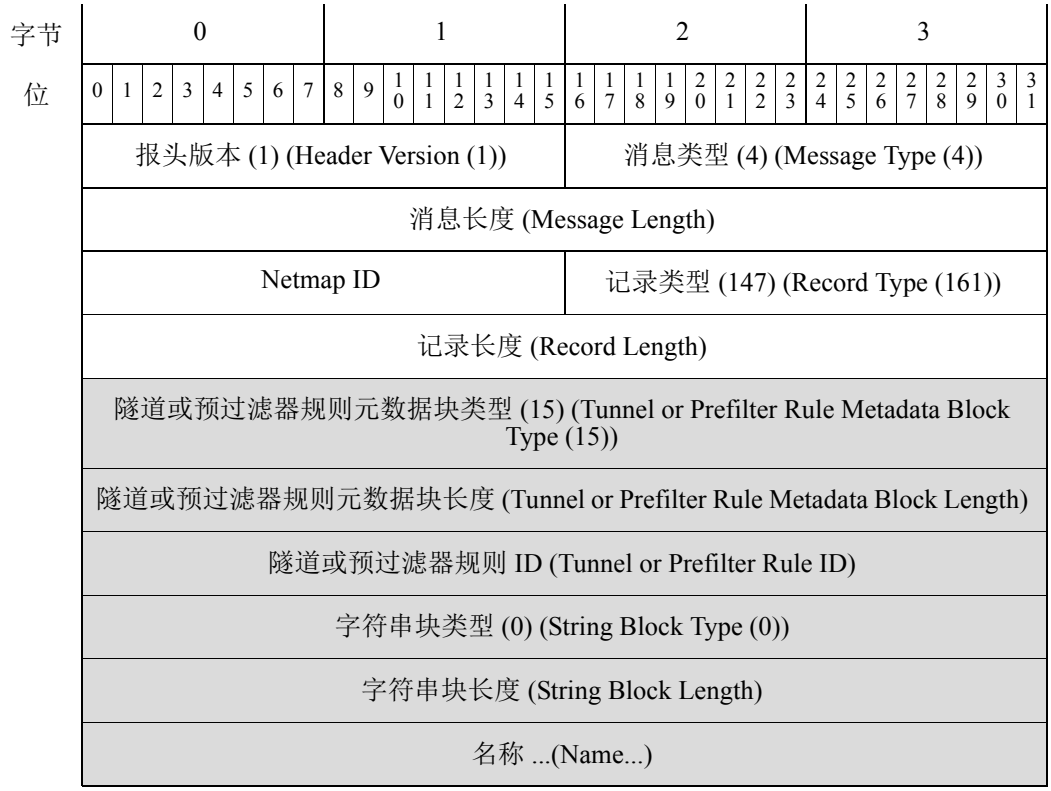
表 4-22　　预过滤器策略元数据字段

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

隧道或预过滤器规则元数据

eStreamer 服务可传输包含预过滤器规则原因相关信息的元数据 （此策略会触发预过滤器规则原因记录中的入侵事件或连接事件），格式如下所示。当设置版本 4 元数据标志 （请求消息的 “ 请求标志 ” (Request Flags) 字段中的位 20）时，发送隧道或预过滤器规则原因元数据。请参阅请求标志，第 2-11 页。请注意，“ 记录类型 ” 字段 （出现在 “ 消息长度 ” 字段后面）

的值为 147，表示隧道或预过滤器规则原因记录。由于它们的内容相同，因此它包含访问控制规则原因块 （如访问控制规则数据块，第 4-205 页中所记录）。访问控制规则原因数据块的块类型为系列 2 中的 59。



下表对隧道或预过滤器规则元数据块中的字段进行了说明。

表 4-23　隧道或预过滤器规则原因元数据字段

字段	数据类型	说明
隧道或预过滤器规则块类型 (Tunnel or Prefilter Rule Block Type)	uint32	启动访问控制规则块。值始终为 15。请注意，除了访问控制规则，此块还用于隧道和预过滤器规则。
隧道或预过滤器规则块长度 (Tunnel or Prefilter Rule Block Length)	uint32	隧道或预过滤器规则块中的字节总数，包括隧道或预过滤器块类型和长度字段的八个字节，加上随后的数据字节数。
隧道或预过滤器规则 ID (Tunnel or Prefilter Rule ID)	uint32	隧道或预过滤器规则的内部 Cisco 标识符。
字符串块类型 (String Block Type)	uint32	启动包含与隧道或预过滤器规则 UUID 以及隧道或预过滤器规则 ID 关联的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 名称 ”(Name) 字段中的字节数。
名称 (Name)	字符串	描述性名称。

安全情报类别元数据

eStreamer 服务可传输包含安全情报类别记录中的安全情报类别相关信息的元数据，格式如下所示。当设置版本 4 元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 20）时，发送安全情报类别元数据。请参阅请求标志，第 2-11 页。请注意，“ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 280，表示　安全情报类别记录。它包含安全情报类别数据块 （如安全情报类别数据块 5.1+，第 4-208 页中所记录）。安全情报数据块的块类型为系列 2 中的 22。

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

下表对安全情报类别记录中的字段进行了说明。

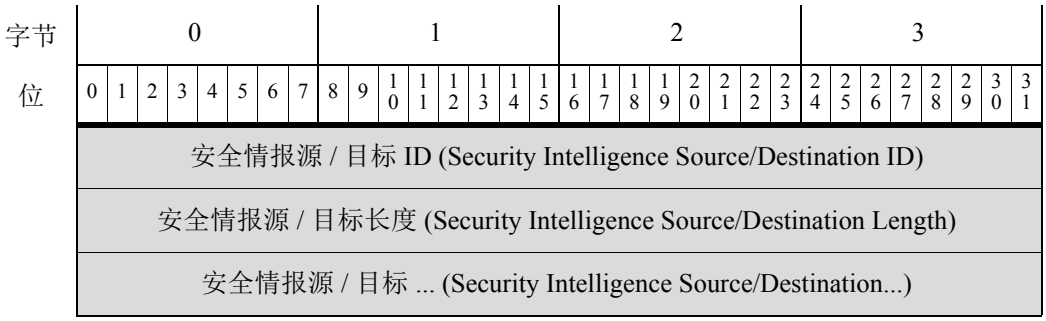
表 4-24　　安全情报类别元数据字段

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

安全情报源 / 目标记录

eStreamer 服务可传输包含安全情报源 / 目标记录中安全情报检测到的 IP 地址是源 IP 地址还是目标 IP 地址这一信息的元数据，格式如下所示。（当设置其中一个元数据标志 （请求消息的 “ 请求标志 ”(Request Flags) 字段中的位 1、 14、 15 或 20）时，发送源 / 目标 IP 信息。请参阅请求标志，第 2-11 页。）请注意， “ 记录类型 ”(Record Type) 字段 （出现在 “ 消息长度 ”(Message Length) 字段后面）的值为 281，表示安全情报源 / 目标记录。

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



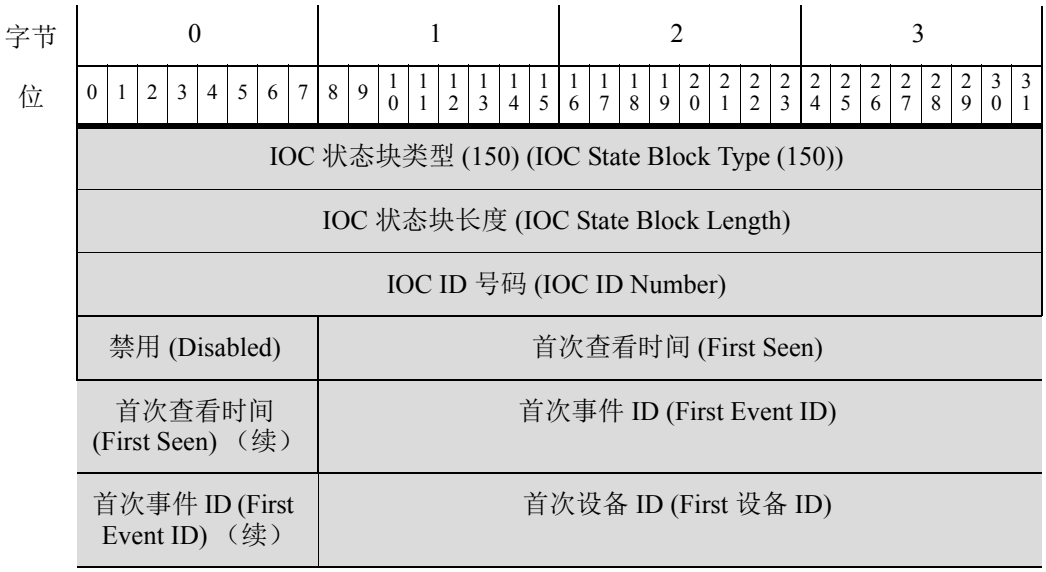
下表对安全情报源 / 目标记录中的字段进行了说明。

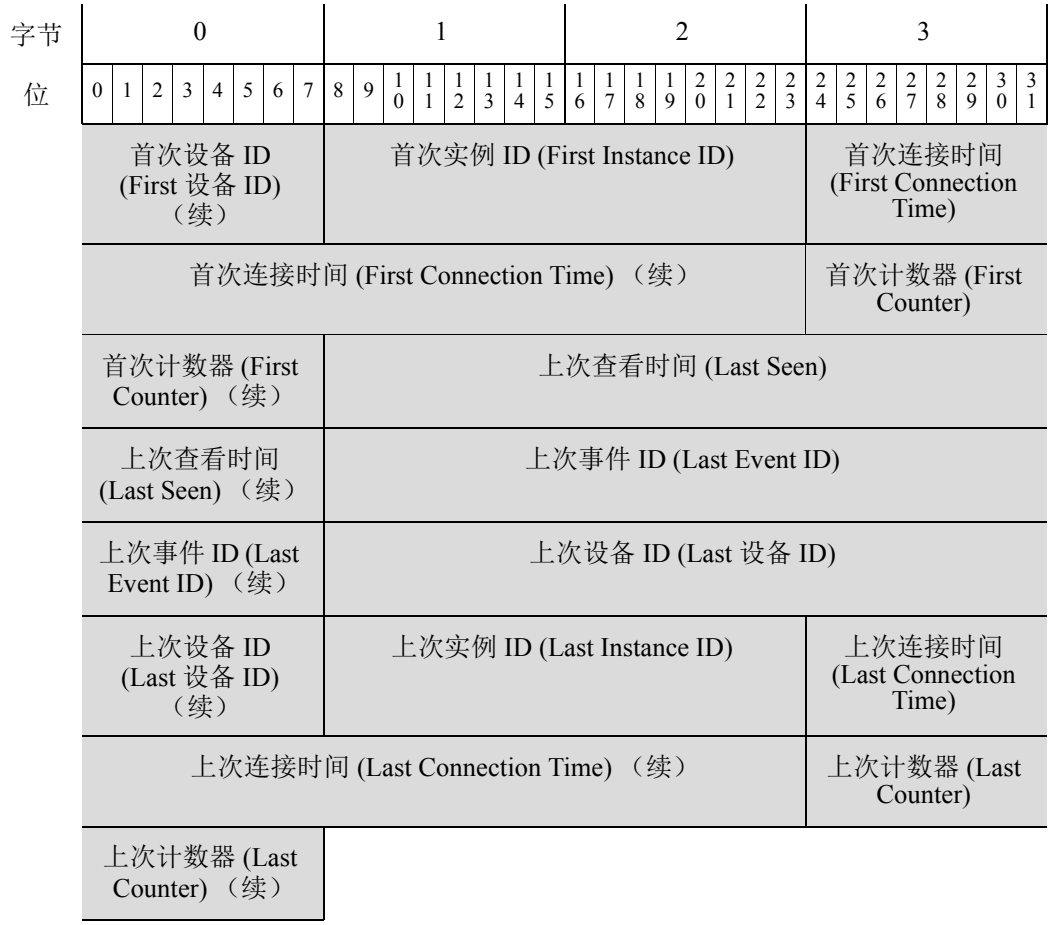
表 4-25　　安全情报源 / 目标记录字段

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

用于 5.3+ 的 IOC 状态数据块

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





下表对 IOC 状态数据块的组件进行了说明。

表 4-26　　IOC 状态数据块字段

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

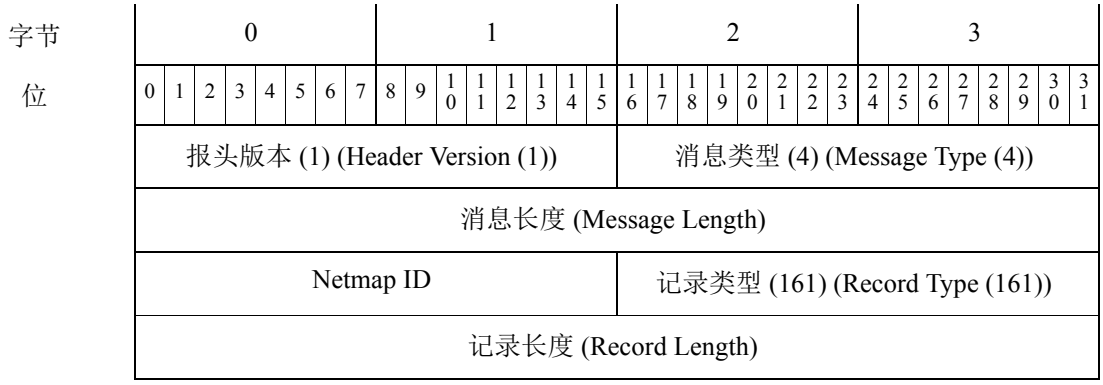
表 4-26　　IOC 状态数据块字段 （续）

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

用于 5.3+ 的 IOC 名称数据块

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

下图显示 IOC 名称数据块的结构：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IOC 名称块类型 (39) (IOC Name Block Type (39))																															
	IOC 名称块长度 (IOC Name Block Length)																															
	IOC ID 号码 (IOC ID Number)																															
类别	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	类别 ...(Category...)																															
事件类型	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	事件类型 ...(Event Type...)																															

下表对 IOC 名称数据块中的字段进行了说明。

表 4-27　　IOC 名称数据块字段

字段	数据类型	说明
IOC 名称数据块类型 (IOC Name Data Block Type)	uint32	启动 IOC 名称数据块。值始终为 39。
IOC 名称数据块长度 (IOC Name Data Block Length)	uint32	IOC 名称数据块中的字节总数，包括 IOC 名称数据块类型和长度字段的八个字节，加上随后的数据字节数。
IOC ID 号码 (IOC ID Number)	uint32	威胁的唯一 ID 编号。
字符串块类型 (String Block Type)	uint32	启动包含与危害相关的类别的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 类别 ”(Category) 字段中的字节数。

表 4-27　IOC 名称数据块字段 （续）

字段	数据类型	说明
类别	字符串	威胁的类别。可能的值包括： • CnC Connected • Exploit Kit • High Impact Attack • Low Impact Attack • Malware Detected • Malware Executed • Dropper Infection • Java Compromise • Word Compromise • Adobe Reader Compromise • Excel Compromise • PowerPoint Compromise • QuickTime Compromise
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。

表 4-27　　IOC 名称数据块字段 （续）

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

发现事件报头 5.2+

发现和连接事件消息包含发现事件报头。它传送事件的类型和子类型、事件发生的时间、出现该事件的设备以及消息中事件数据的结构。报头后面是实际主机发现、用户或连接事件数据。按事件类型划分的主机发现结构，第 4-44 页中介绍了与不同事件类型 / 子类型值相关的结构。此报头具有 IPv6 支持，并否决发现事件报头 5.0 - 5.1.1.x，第 B-91 页。

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

下图中的阴影行举例说明了发现事件报头的格式。

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

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	IPv6 地址 (IPv6 Address)																															
	IPv6 地址 (IPv6 Address) （续）																															
	IPv6 地址 (IPv6 Address) （续）																															
	IPv6 地址 (IPv6 Address) （续）																															

下表对发现事件报头进行了说明。

表 4-28　　发现事件报头字段

字段	数据类型	说明
设备 ID (Device ID)	uint32	生成发现事件的设备的 ID 号码。您可以通过请求版本 3 和版本 4 元数据获取设备的元数据。有关详细信息，请参阅受管设备记录元数据，第 3-34 页。
旧版 IP 地址 (Legacy IP Address)	uint32	保留此字段，但不再填充。 IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅 IP 地址，第 1-3 页。
MAC 地址 (MAC Address)	uint8[6]	事件所涉及主机的 MAC 地址。
具有 IPv6 (Has IPv6)	uint8	指示主机具有 IPv6 地址的标志。
留作未来使用 (Reserved for future use)	uint8	留作未来使用
事件秒 (Event Second)	uint32	系统生成事件的 UNIX 时间戳 （自 1970/01/01 起经过的秒数）。
事件微秒 (Event Microsecond)	uint32	系统生成事件的微秒 （一秒的百万分之一）增量。
事件类型 (Event Type)	uint32	事件类型 （新事件为 `1000`，变更事件为 `1001`，用户输入事件为 `1002`，完整主机配置文件为 `1050`）。有关可用事件类型列表，请参阅按事件类型划分的主机发现结构，第 4-44 页。
事件子类型 (Event Subtype)	uint32	事件子类型。有关可用事件子类型列表，请参阅按事件类型划分的主机发现结构，第 4-44 页。
文件编号 (File Number)	byte[4]	串行文件编号。此字段供 Cisco 内部使用，可以忽略。
文件位置 (File Position)	byte[4]	事件在串行文件中的位置。此字段供 Cisco 内部使用，可以忽略。
IPv6 地址 (IPv6 Address)	uin8[16]	IPv6 地址。若设置了 Has IPv6 标志，则此字段存在且可使用。

发现与连接事件类型和子类型

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

下表列出了发现事件与连接事件的事件类型和事件子类型。

表 4-29　　按类型和子类型划分的发现与连接事件

事件名称	事件类型	事件子类型
新主机	1000	1
新 TCP 服务器	1000	2
新网络协议	1000	3
新传输协议	1000	4
新 IP 到 IP 流量	1000	5
新 UDP 服务器	1000	6
新客户端应用	1000	7
新操作系统	1000	8
新 IPv6 到 IPv6 流量	1000	9
主机 IP 地址已更改	1001	1
操作系统信息更新	1001	2
主机 IP 地址已重用	1001	3
漏洞更改	1001	4
跳数更改	1001	5
TCP 服务器信息更新	1001	6
主机超时	1001	7
TCP 端口已关闭	1001	8
UDP 端口已关闭	1001	9
UDP 服务器信息更新	1001	10
TCP 端口超时	1001	11
UDP 端口超时	1001	12
MAC 信息更改	1001	13
为主机检测的其他 MAC	1001	14
主机上次查看时间	1001	15
识别为路由器 / 网桥的主机	1001	16
连接统计信息	1001	17
VLAN 标记信息更新	1001	18
已删除主机 : 已达主机限制	1001	19
客户端应用超时	1001	20
NetBIOS 名称更改	1001	21
NetBIOS 域更改	1001	22

表 4-29　　按类型和子类型划分的发现与连接事件 （续）

事件名称	事件类型	事件子类型
已丢弃主机：已达主机限制	1001	23
横幅更新	1001	24
TCP 服务器置信度更新	1001	25
UDP 服务器置信度更新	1001	26
身份冲突	1001	29
身份超时	1001	30
辅助主机更新	1001	31
客户端应用更新	1001	32
用户设置有效漏洞 （旧版本）	1002	1
用户设置无效漏洞 （旧版本）	1002	2
用户删除地址 （旧版本）	1002	3
用户删除服务器 （旧版本）	1002	4
用户设置主机临界点	1002	5
主机属性添加	1002	6
主机属性更新	1002	7
主机属性删除	1002	8
主机属性设置值 （旧版本）	1002	9
主机属性删除值 （旧版本）	1002	10
添加扫描结果	1002	11
用户设置漏洞限定条件	1002	12
用户策略控制	1002	13
删除协议	1002	14
删除客户端应用	1002	15
用户设置操作系统	1002	16
用户帐户查看	1002	17
用户帐户更新	1002	18
用户设置服务器	1002	19
用户删除地址 （当前版本）	1002	20
用户删除服务器 （当前版本）	1002	21
用户设置有效漏洞 （当前版本）	1002	22
用户设置无效漏洞 （当前版本）	1002	23
用户主机临界点	1002	24
主机属性设置值 （当前版本）	1002	25
主机属性删除值 （当前版本）	1002	26
用户添加主机	1002	27
用户添加服务器	1002	28

表 4-29　按类型和子类型划分的发现与连接事件 （续）

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

提示 有关用于每个事件类型 / 子类型的数据结构的信息，请参阅按事件类型划分的主机发现结构，第 4-44 页。

按事件类型划分的主机发现结构

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

- 新主机消息与主机上次查看时间消息，第 4-45 页
- 服务器消息，第 4-46 页
- 新网络协议消息，第 4-47 页
- 新传输协议消息，第 4-47 页
- 客户端应用消息，第 4-47 页
- IP 地址更改消息，第 4-48 页
- 操作系统更新消息，第 4-49 页
- IP 地址已重用和主机超时 / 已删除主机消息，第 4-50 页
- 跳数更改消息，第 4-50 页
- 跳数更改消息，第 4-50 页
- TCP 和 UDP 端口已关闭 / 超时消息，第 4-50 页
- MAC 地址消息，第 4-51 页

- 识别为路由器 / 网桥的主机消息，第 4-51 页
- VLAN 标签信息更新消息，第 4-52 页
- 更改 NetBIOS 名称消息，第 4-52 页
- 更新横幅消息，第 4-53 页
- 策略控制消息，第 4-54 页
- 连接统计信息数据消息，第 4-54 页
- 连接区块消息，第 4-55 页
- 用于版本 4.6.1+ 的用户设置漏洞消息，第 4-55 页
- 用户添加和删除主机消息，第 4-55 页
- 用户删除服务器消息，第 4-56 页
- 用户设置主机临界点消息，第 4-57 页
- 属性消息，第 4-57 页
- 属性值消息，第 4-58 页
- 用户服务器和操作系统消息，第 4-58 页
- 用户协议消息，第 4-59 页
- 用户客户端应用消息，第 4-59 页
- 添加扫描结果消息，第 4-60 页
- 新操作系统消息，第 4-60 页
- 身份冲突和身份超时系统消息，第 4-60 页
- 主机 IOC 设置消息，第 4-61 页

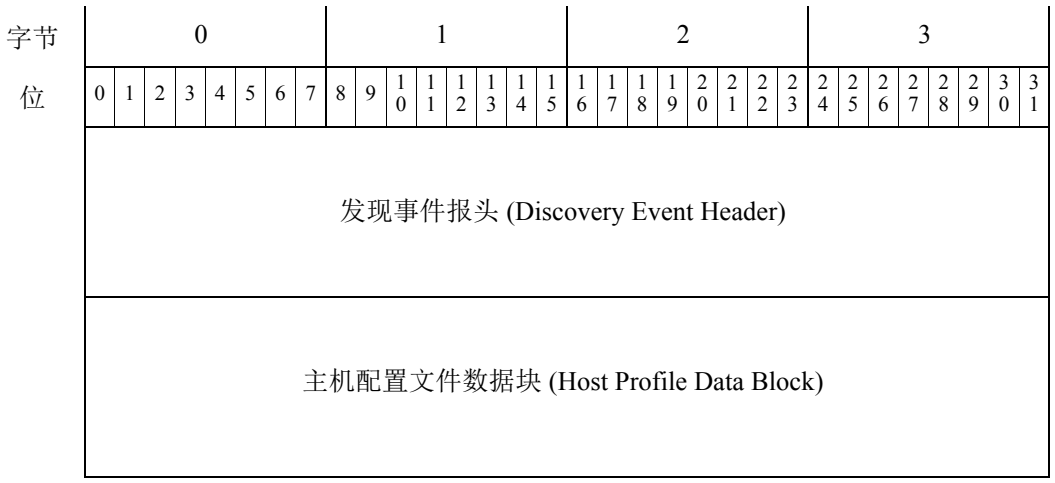
以下章节中的数据块图描绘了主机发现事件消息中返回的不同记录数据块。

新主机消息与主机上次查看时间消息

新主机消息与主机上次查看时间事件消息具有标准发现事件报头和主机配置文件数据块（如用于 5.2+ 的主机配置文件数据块，第 4-167 页中所记录）。主机配置文件数据块的块类型为系列 1 中的 139。

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

注　主机配置文件数据块因创建该消息的系统版本而异。有关主机配置文件数据块的旧版本的信息，请参阅旧版主机数据结构，第 B-297 页。



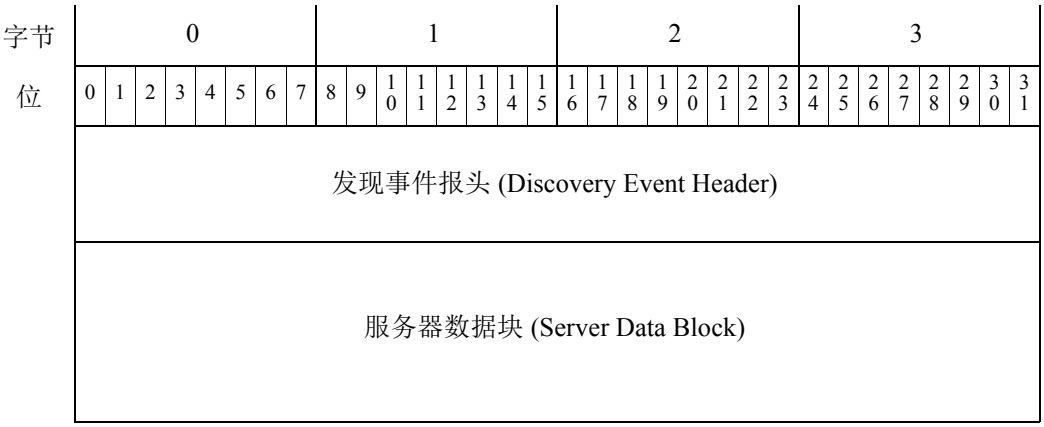
服务器消息

以下 TCP 和 UDP 服务器事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟服务器数据块（如主机服务器数据块 4.10.0+，第 4-141 页中所记录，系列 1 中的块类型 103）：

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

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

这些事件都使用以下格式：



新网络协议消息

新网络协议事件消息具有标准发现事件报头 （如发现事件报头 5.2+，第 4-40 页中所记录），后跟一个用于网络协议的两字节字段 （使用下表中描述的协议值）。

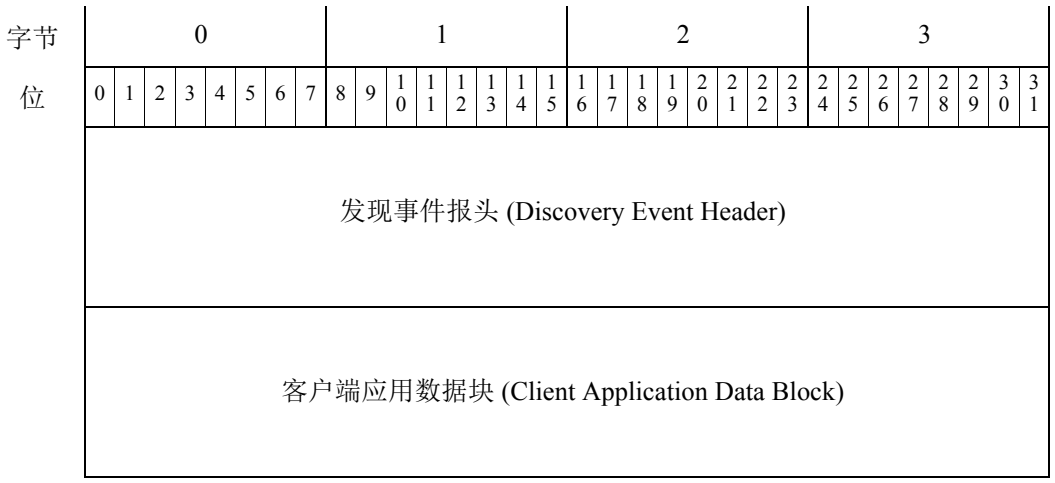
新传输协议消息

新传输协议事件消息具有标准发现事件报头 （如发现事件报头 5.2+，第 4-40 页中所记录，系列 1 中的块类型 4），以及一个用于传输协议号的单字节字段 （使用下表中描述的值）。

客户端应用消息

新客户端应用、客户端应用更新以及客户端应用超时事件具有相同格式，且都包含一个标准发现事件报头 （如发现事件报头 5.2+，第 4-40 页中所记录），后跟一个客户端应用数据块 （请参阅用于 5.0+ 的主机客户端应用数据块，第 4-160 页，系列 1 中的块类型 122）。发现事件报头具有不同的记录类型、事件类型和事件子类型，这取决于传输的事件。

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

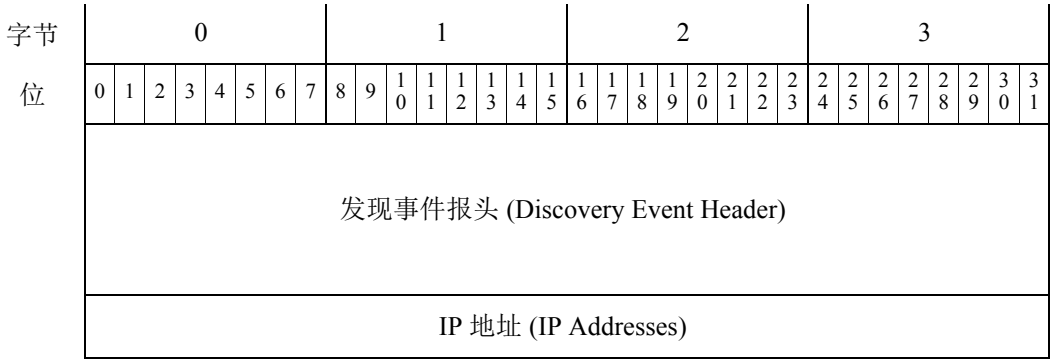


IP 地址更改消息

以下主机发现消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录）和两种不同的形式与结构，一种 IP 地址为四个字节，另一种 IP 地址为 16 个字节。

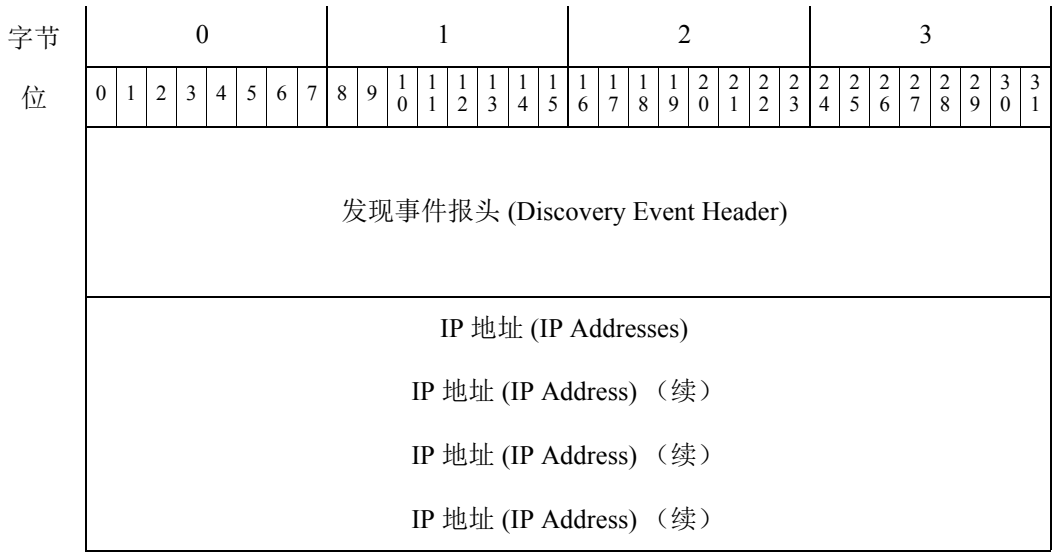
在以下情况下， IP 地址（采用 IP 地址八位组）为四个字节：

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



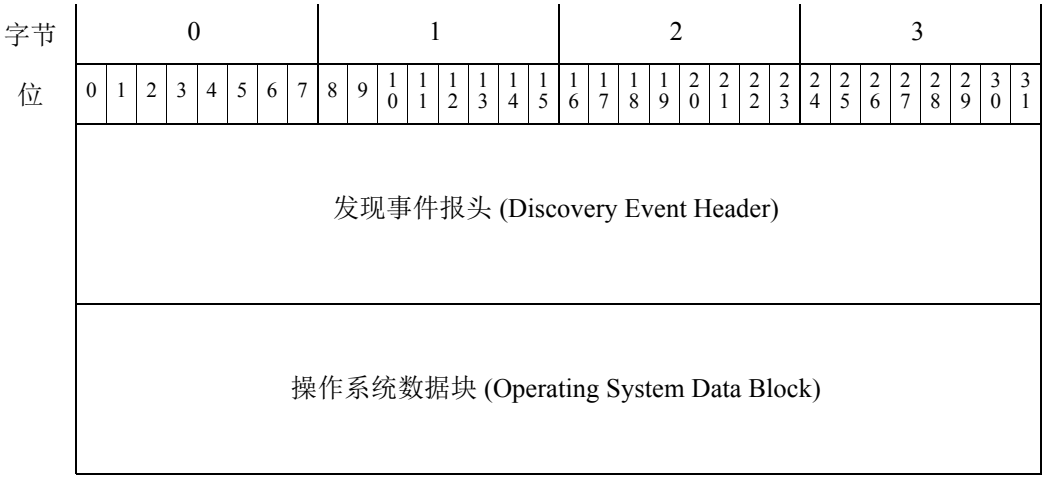
在以下情况下， IP 地址为 16 个字节：

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



操作系统更新消息

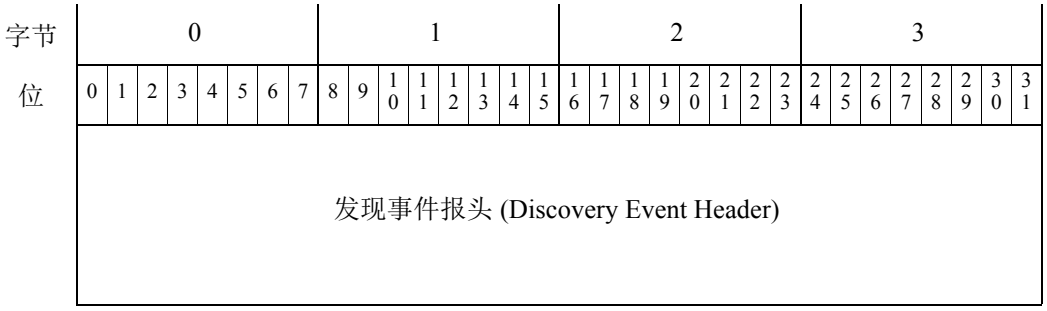
操作系统信息更新事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟操作系统数据块 （如操作系统数据块 3.5+，第 4-86 页中所记录，系列 1 中的块类型 53）。



IP 地址已重用和主机超时 / 已删除主机消息

以下主机事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），且无其他数据：

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



跳数更改消息

跳数更改事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟一个用于跳数计数的单字节字段。

TCP 和 UDP 端口已关闭 / 超时消息

TCP 和 UDP 端口已关闭和端口超时事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟一个用于端口号的两字节字段。

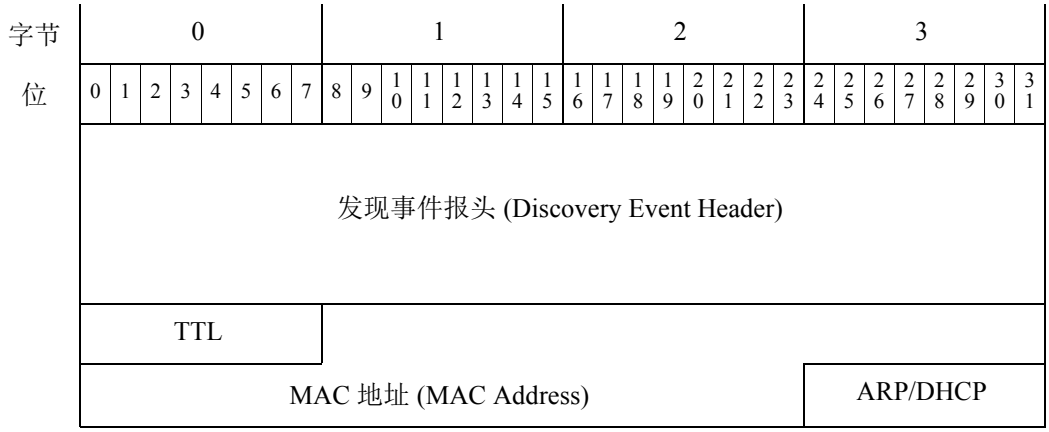
MAC 地址消息

MAC 信息更改和检测到主机的其他 MAC 消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），1 个字节用于 TTL 值，6 个字节用于 MAC 地址，1 个字节用于指示通过 ARP/DHCP 流量检测的 MAC 地址是否为实际 MAC 地址。

注

如果您从运行版本 4.9.x 的系统收到 MAC 地址消息，则必须检查该 MAC 地址数据块的长度并进行相应解码。如果该数据块的长度为 8 个字节（加报头共 16 个字节），请参阅 MAC 地址消息，第 4-51 页。如果该数据块的长度为 12 个字节（加报头共 20 个字节），请参阅主机 MAC 地址 4.9+，第 4-116 页。

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



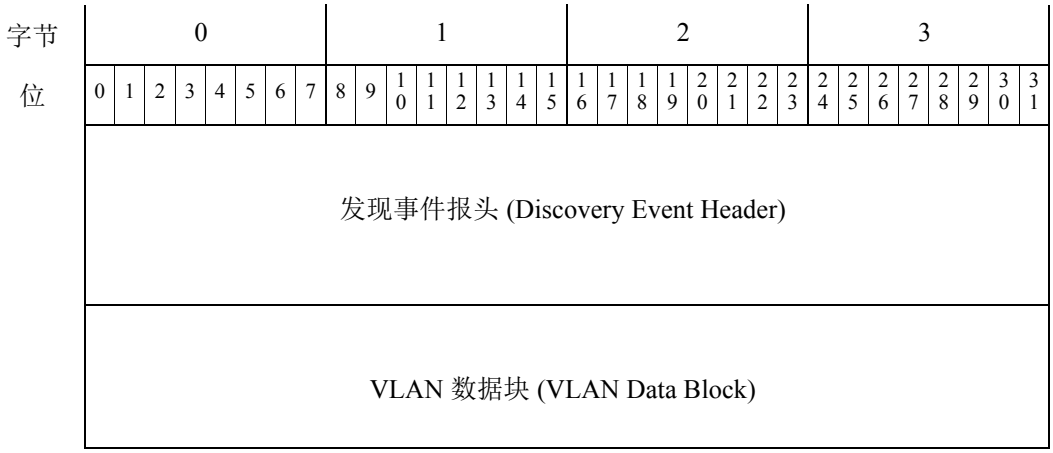
识别为路由器 / 网桥的主机消息

识别为路由器 / 网桥的主机事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟用于与主机类型匹配的值的四字节字段：

- 0 - 主机
- 1 - 路由器
- 2 - 网桥

VLAN 标签信息更新消息

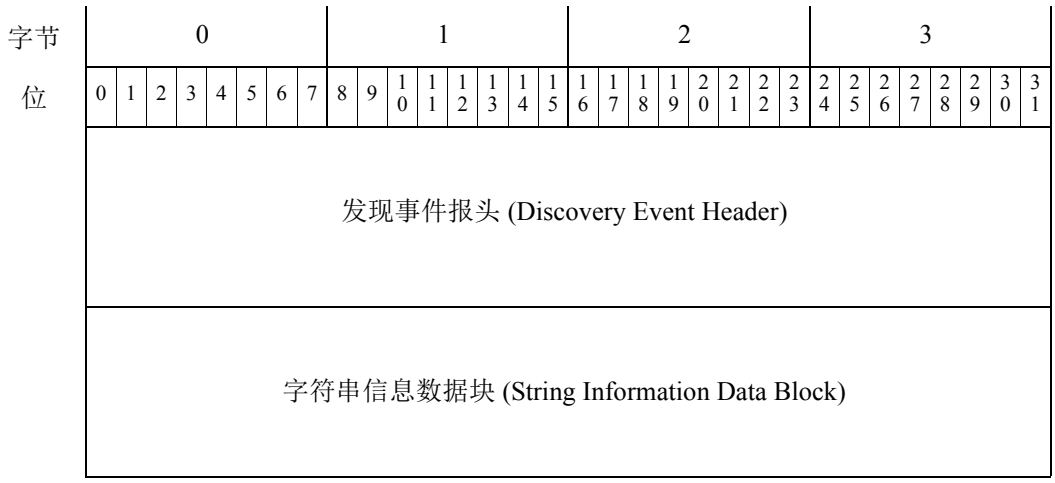
VLAN 标签信息更新事件具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟 VLAN 数据块 （如 VLAN 数据块，第 4-76 页中所记录）。 VLAN 数据块的块类型为系列 1 数据块组中的 14。



更改 NetBIOS 名称消息

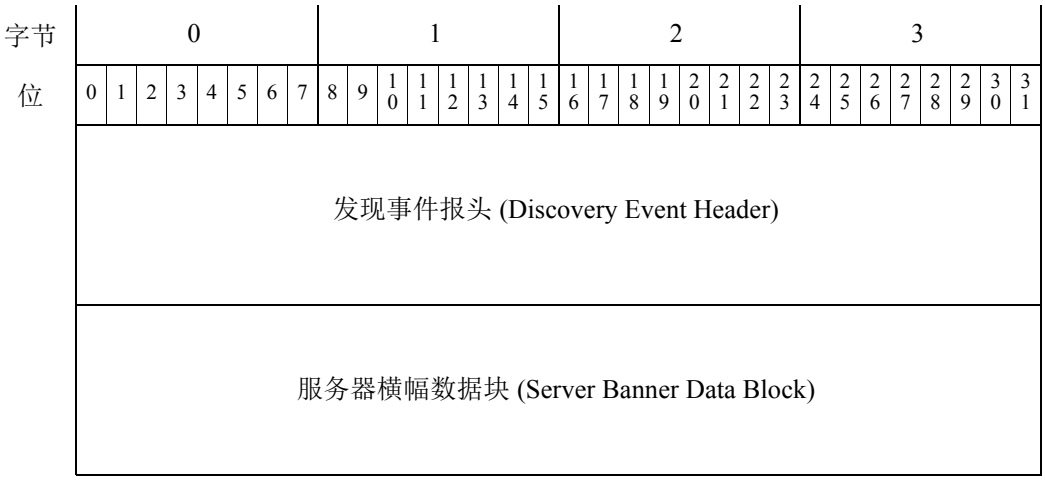
更改 NetBIOS 名称事件消息具有标准发现事件报头 （如发现事件报头 5.2+，第 4-40 页中所记录），后跟一个字符串信息数据块 （如字符串信息数据块，第 4-78 页中所记录）。字符串信息数据块的块类型为系列 1 中的 35。

注　目前， Firepower 系统不生成更改 NetBIOS 域事件。



更新横幅消息

更新横幅事件消息具有标准发现事件报头 （如发现事件报头 5.2+，第 4-40 页中所记录），后跟一个服务器横幅数据块 （如服务器横幅数据块，第 4-77 页中所记录）。服务器横幅数据块的块类型为系列 1 中的 37。



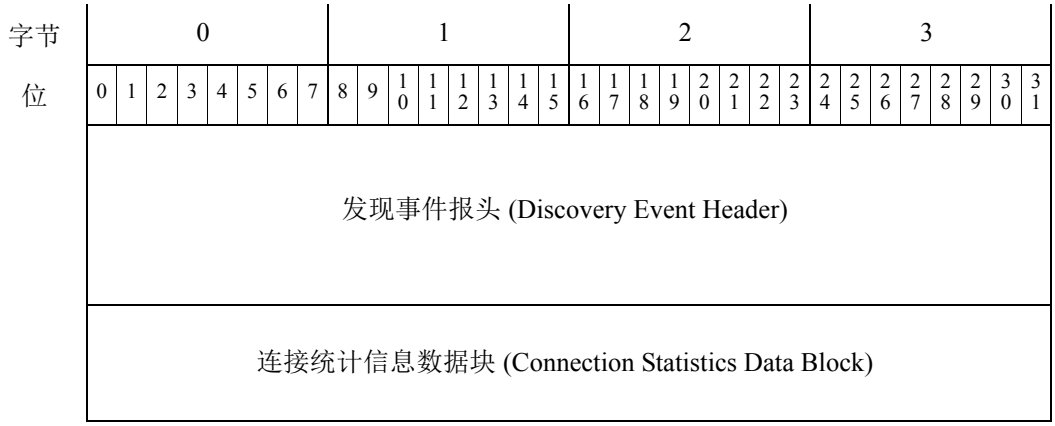
策略控制消息

策略控制消息事件具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟策略控制消息数据块。策略控制消息数据块的格式因系统版本而异。有关当前版本的策略控制消息数据块格式的信息，请参阅策略引擎控制消息数据块，第 4-87 页。

连接统计信息数据消息

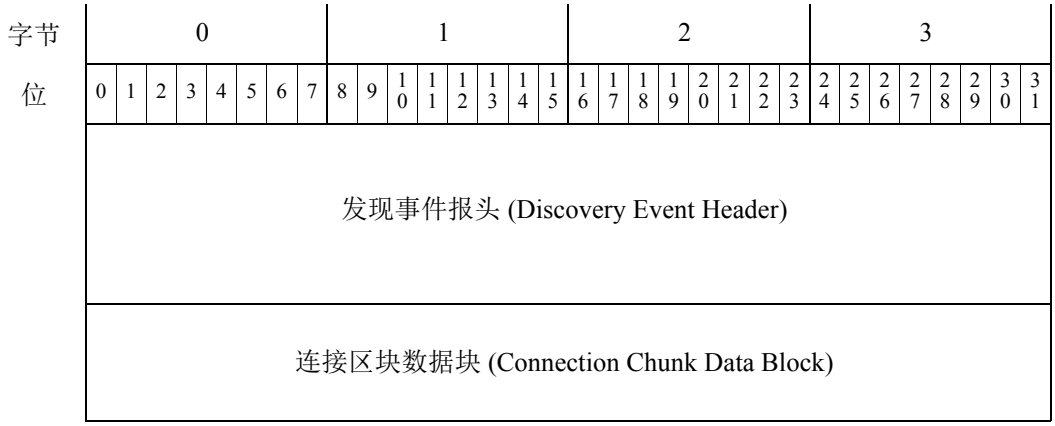
连接统计信息事件具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟连接统计信息数据块。连接统计信息数据块的每个版本的文档都包含使用该数据块的系统版本。有关用于版本 6.1+ 的连接统计信息数据块格式的信息，请参阅连接统计信息数据块 6.2+，第 4-119 页。

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



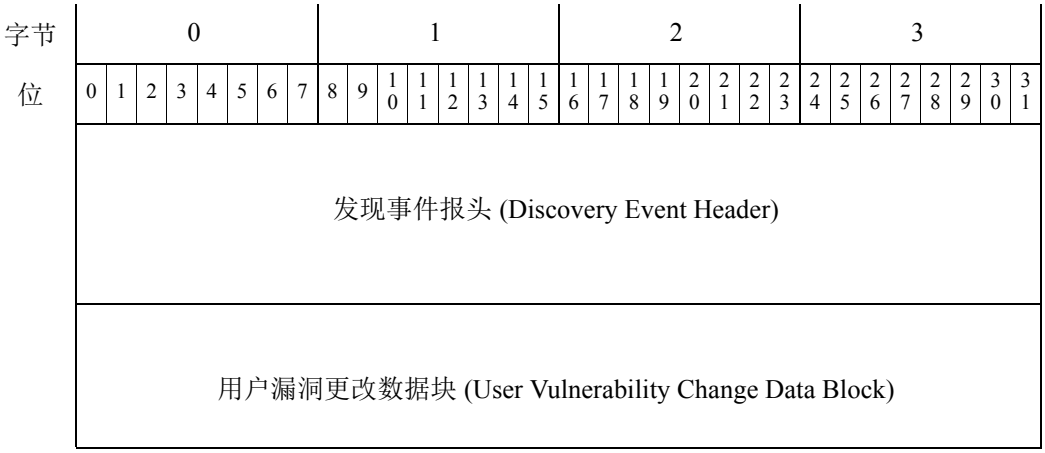
连接区块消息

连接区块事件具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟连接区块数据块。格式因系统版本而异。有关当前版本的连接区块数据块格式的信息，请参阅用于 6.1+ 的连接区块数据块，第 4-101 页。连接区块数据块的块类型为系列 1 中的 136。



用于版本 4.6.1+ 的用户设置漏洞消息

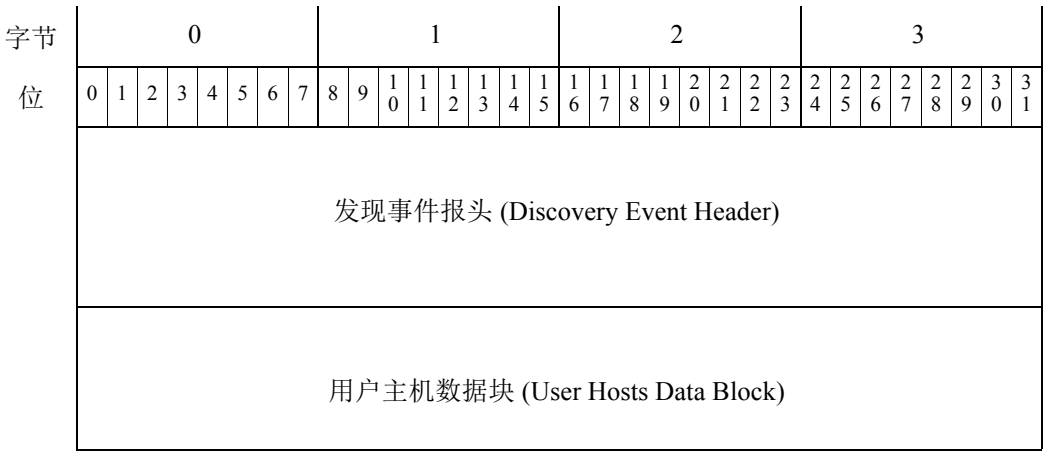
用户设置有效漏洞、用户设置无效漏洞以及用户漏洞限定条件消息使用相同的数据格式：标准发现事件报头（请参阅发现事件报头 5.2+，第 4-40 页），后跟用户漏洞更改数据块（请参阅用户漏洞更改数据块 4.7+，第 4-108 页，系列 1 中的块类型 80）。它们通过记录类型、事件类型和事件子类型进行区分。



用户添加和删除主机消息

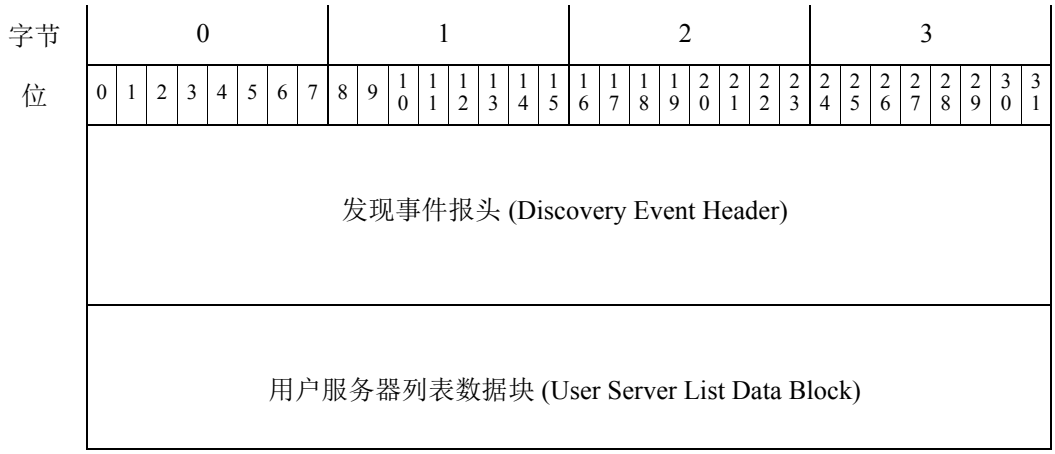
以下主机输入事件消息具有标准发现事件报头（请参阅发现事件报头 5.2+，第 4-40 页），后跟用户主机数据块
（请参阅用户主机数据块 4.7+，第 4-106 页，系列 1 中的块类型 78）：

- 用户删除地址
- 用户添加主机



用户删除服务器消息

用户删除服务器消息具有标准发现事件报头 （请参阅发现事件报头 5.2+，第 4-40 页），后跟用户服务器列表数据块 （请参阅用户服务器列表数据块，第 4-105 页）。用户服务器列表数据块的块类型为系列 1 中的 77。



用户设置主机临界点消息

用户设置主机临界点消息具有标准发现事件报头（请参阅发现事件报头 5.2+，第 4-40 页），后跟用户临界点更改数据块（请参阅用户临界点更改数据块 4.7+，第 4-109 页）。用户临界点更改数据块的块类型为系列 1 中的 81。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
发现事件报头 (Discovery Event Header)																																
用户临界点更改数据块 (User Criticality Change Data Block)																																

属性消息

以下事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟属性定义数据块（如用于 4.7+ 的属性定义数据块，第 4-88 页中所记录，系列 1 中的块类型 55）：

- 添加主机属性
- 更新主机属性
- 删除主机属性

这些事件都使用以下格式：

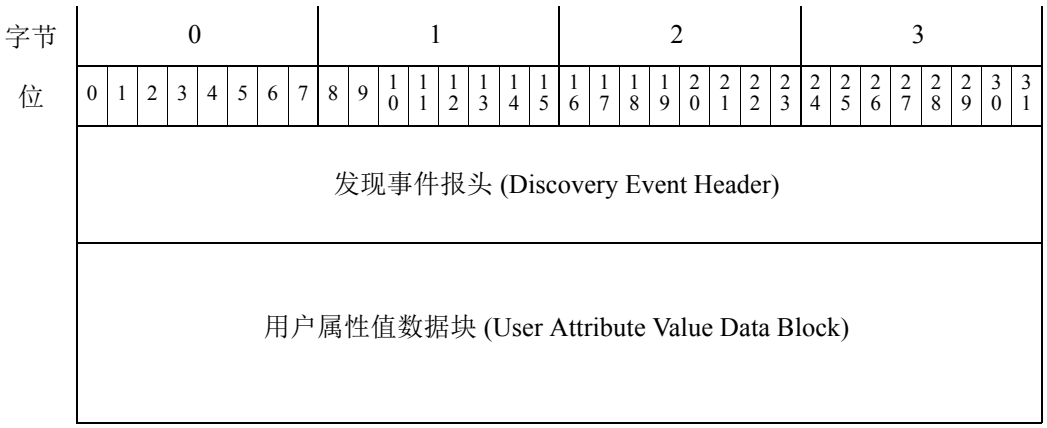
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
发现事件报头 (Discovery Event Header)																																
属性定义数据块 (Attribute Definition Data Block)																																

属性值消息

以下事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟用户属性值数据块（如用户属性值数据块 4.7+，第 4-111 页中所记录，系列 1 中的块类型 82）：

- 设置主机属性值
- 删除主机属性值

这些事件都使用以下格式：

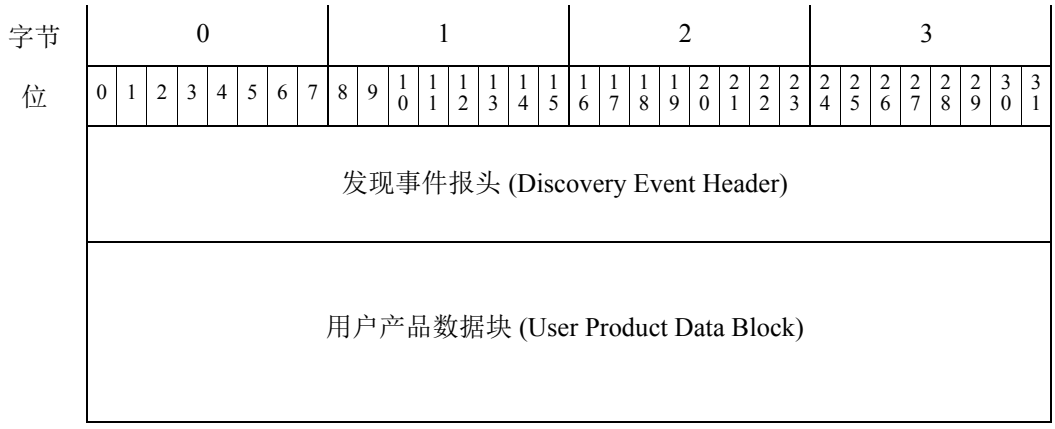


用户服务器和操作系统消息

以下事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟用户产品数据块（如用户产品数据块 5.1+，第 4-176 页中所记录，系列 1 中的块类型 60）：

- 设置操作系统定义
- 设置服务器定义
- 添加服务器

这些事件都使用以下格式：

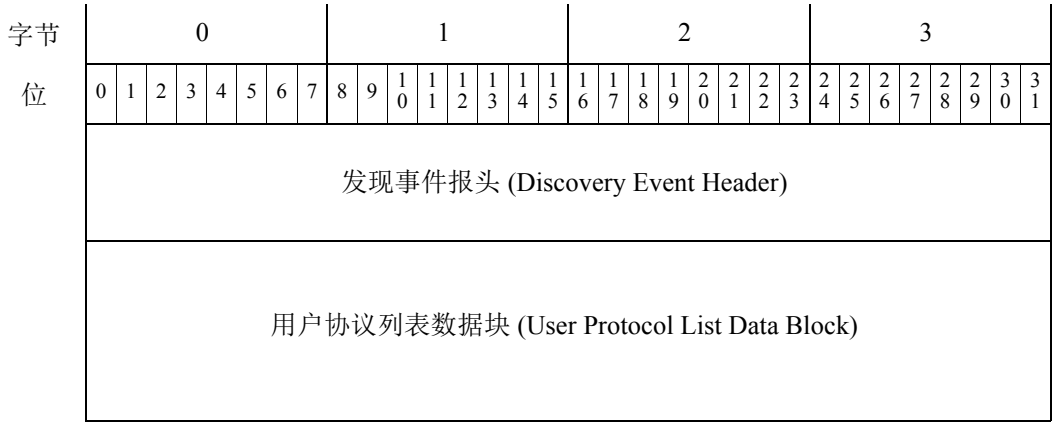


用户协议消息

以下事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟用户协议列表数据块（如用户协议列表数据块 4.7+，第 4-112 页中所记录，系列 1 中的块类型 83）：

- 删除协议
- 添加协议

这些事件都使用以下格式：

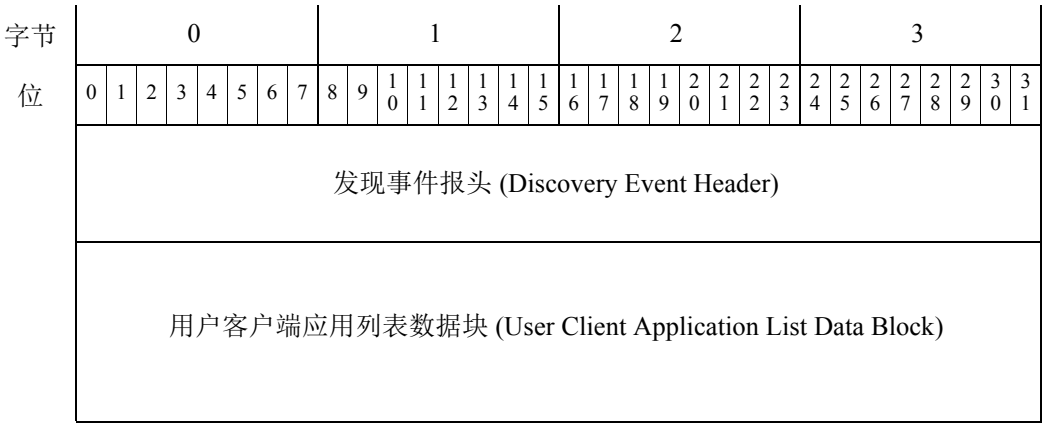


用户客户端应用消息

以下事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟用户客户端应用列表数据块（如用户客户端应用列表数据块，第 4-94 页中所记录，系列 1 中的块类型 60）：

- 删除客户端应用
- 添加客户端应用

这些事件都使用以下格式：



添加扫描结果消息

添加扫描结果事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟扫描结果数据块（如扫描结果数据块 5.2+，第 4-138 页中所记录）。扫描结果数据块的块类型为系列 1 中的 142。

此事件使用以下格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
发现事件报头 (Discovery Event Header)																																
扫描结果数据块 (Scan Result Data Block)																																

新操作系统消息

新操作系统事件消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟操作系统指纹数据块（如操作系统指纹数据块 5.1+，第 4-164 页中所记录）。

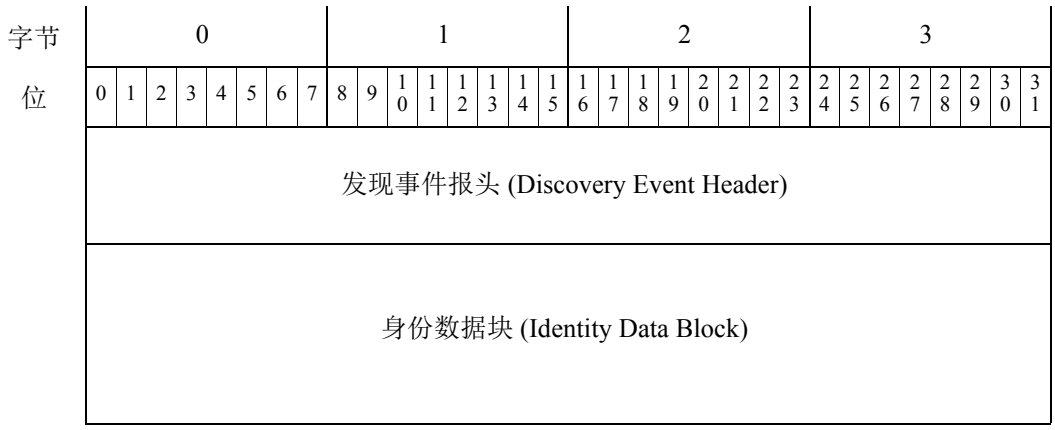
此事件使用以下格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
发现事件报头 (Discovery Event Header)																																
操作系统指纹数据块 (Operating System Fingerprint Data Block)																																

身份冲突和身份超时系统消息

身份冲突和身份超时事件消息都具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟身份数据块（如身份数据块，第 4-114 页中所记录）。身份数据块的块类型为系列 1 中的 94。当指纹源身份中存在冲突或超时时，系统生成这些消息。

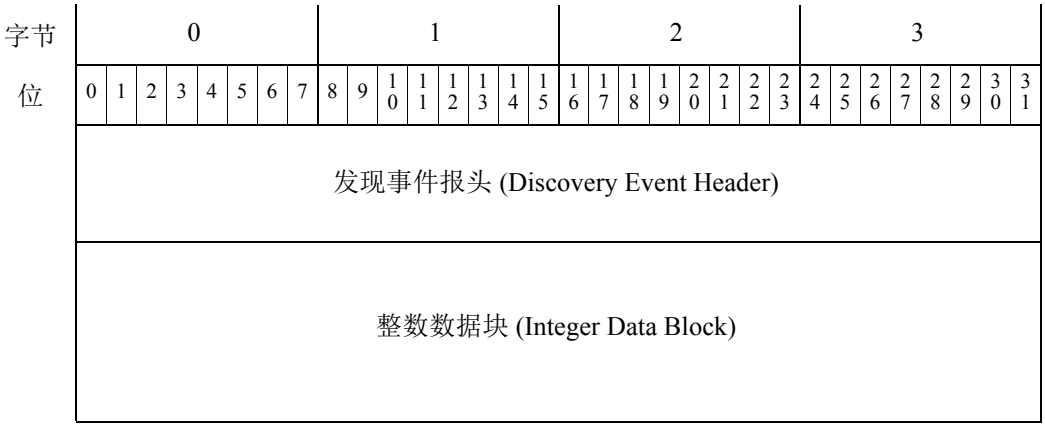
此事件使用以下格式：



主机 IOC 设置消息

主机 IOC 设置消息具有标准发现事件报头（如发现事件报头 5.2+，第 4-40 页中所记录），后跟整数数据块（如整数 (INT32) 数据块，第 4-75 页中所记录）。此整数数据块包含主机的 IOC 设置的 ID 号码。

此事件使用以下格式：



按事件类型划分的用户数据结构

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

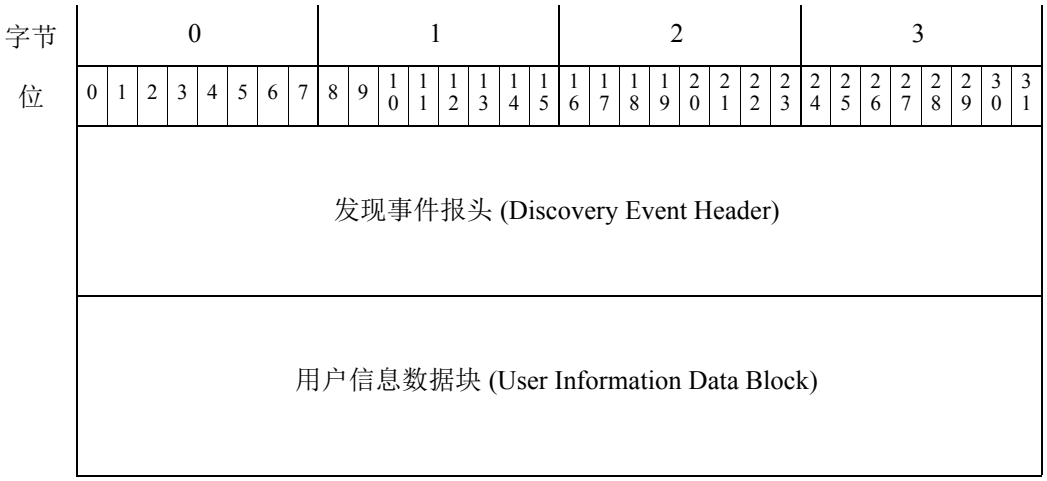
- 用户修改消息，第 4-62 页
- 用户信息更新消息块，第 4-62 页

用户修改消息

当通过系统检测发现以下任何事件时，系统会发送用户修改消息：

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

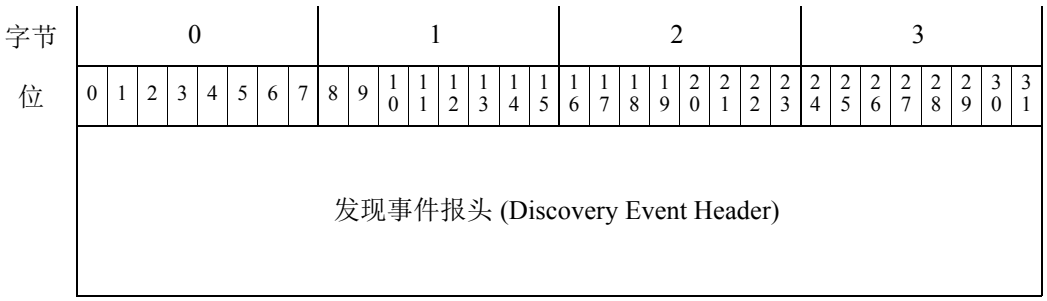
用户修改事件消息具有标准发现事件报头 （如发现事件报头 5.2+，第 4-40 页中所记录）和用户信息数据块（如用于 6.0+ 的用户信息数据块，第 4-194 页中所记录）。用户信息数据块的块类型为系列 1 中的 120。

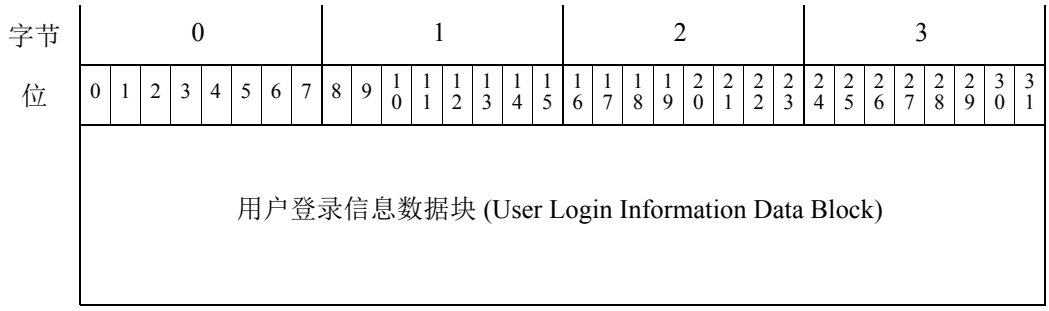


用户信息更新消息块

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

用户信息更新事件消息具有标准发现事件报头 （如发现事件报头 5.2+，第 4-40 页中所记录）和用户登录信息数据块 （如用户登录信息数据块 6.2+，第 4-200 页中所记录）。用户登录信息数据块的块类型为系列 1 中的 121。



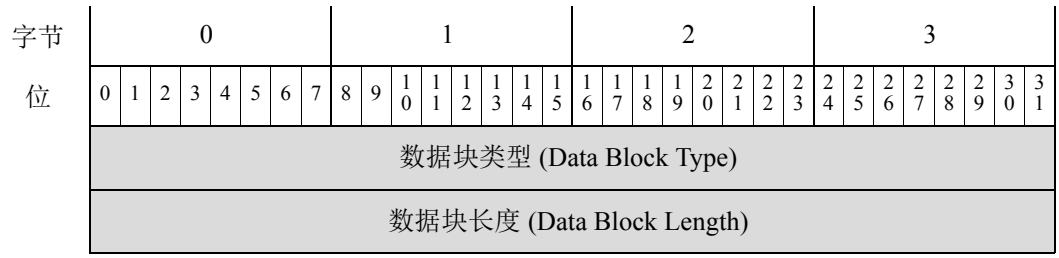


了解发现 （系列 1）块

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

系列 1 数据块报头

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



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

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

系列 1 基元数据块

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

- 字符串数据块，第 4-70 页
- BLOB 数据块，第 4-71 页
- 列表数据块，第 4-72 页
- 通用列表块，第 4-72 页

主机发现和连接数据块

有关主机发现和连接事件中的块类型列表，请参阅表 4-30，第 4-64 页。表 4-86，第 4-183 页对用户事件中的块类型进行了说明。这些都是系列 1 数据块。

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

表 4-30　主机发现和连接数据块类型

类型	内容	数据块状态	说明
0	字符串	当前	包含字符串数据。有关详细信息，请参阅字符串数据块，第 4-70 页。
1	子服务器	当前	包含在服务器上检测到的子服务器的相关信息。有关详细信息，请参阅子服务器数据块，第 4-73 页。
4	协议	当前	包含协议数据。有关详细信息，请参阅协议数据块，第 4-74 页。
7	整数数据	当前	包含整数（数字）数据。有关详细信息，请参阅整数 (INT32) 数据块，第 4-75 页。
10	BLOB	当前	包含一个原始二进制数据块，专门用于横幅。有关详细信息，请参阅 BLOB 数据块，第 4-71 页。
11	列表	当前	包含其他数据块列表。有关详细信息，请参阅列表数据块，第 4-72 页。
14	VLAN	当前	包含 VLAN 信息。有关详细信息，请参阅 VLAN 数据块，第 4-76 页。
20	入侵影响警报	当前	包含入侵影响警报信息。入侵影响警报事件的报头与其他数据块略有不同。有关详细信息，请参阅入侵影响警报数据 5.3+，第 3-16 页。
31	通用列表	当前	包含通用列表信息，例如用来将块（如客户端应用块）列表封装到主机配置文件块中。有关详细信息，请参阅通用列表块，第 4-72 页。
35	字符串信息	当前	包含字符串信息。例如，在扫描漏洞数据块中使用时，字符串信息数据块包含 CVE 标识号数据。请参阅字符串信息数据块，第 4-78 页。
37	服务器横幅	当前	包含服务器横幅数据。有关详细信息，请参阅服务器横幅数据块，第 4-77 页。
38	属性地址	传统	包含主机属性地址（如较早版本的产品中所记录）。后继块为 146。
39	属性列表项	当前	包含主机属性列表项值。有关详细信息，请参阅属性列表项数据块，第 4-81 页。
42	主机客户端应用	传统	包含用于新客户端应用事件的客户端应用信息（如较早版本的产品中所记录）。
47	完整主机配置文件	传统	包含完整主机配置文件信息（如较早版本的产品中所记录）。

表 4-30　主机发现和连接数据块类型 （续）

类型	内容	数据块状态	说明
48	属性值	当前	包含属性标识号和主机属性值。有关详细信息，请参阅属性值数据块，第 4-82 页。
51	完整子服务器	当前	包含在服务器上检测到的子服务器的相关信息。在完整服务器信息块和完整主机配置文件中引用。包含每个子服务器的漏洞信息。有关详细信息，请参阅完整子服务器数据块，第 4-83 页。
53	操作系统	当前	包含用于版本 3.5+ 的操作系统信息。有关详细信息，请参阅操作系统数据块 3.5+，第 4-86 页。
54	策略引擎控制消息	当前	包含有关用户策略控制更改的信息。有关详细信息，请参阅策略引擎控制消息数据块，第 4-87 页。
55	属性定义	当前	包含有关属性定义的信息。有关详细信息，请参阅用于 4.7+ 的属性定义数据块，第 4-88 页。
56	连接统计信息	传统	包含有关 4.7 - 4.9.0 中连接统计信息事件的信息（如较早版本的产品中所记录）。
57	用户协议	当前	包含用户输入的协议信息。有关详细信息，请参阅用户协议数据块，第 4-91 页。
59	用户客户端应用	传统	包含用户输入的客户端应用数据。有关详细信息，请参阅用于 5.0 - 5.1 的用户客户端应用数据块，第 B-94 页。被块 138 替代。
60	用户客户端应用列表	当前	包含用户客户端应用数据块的列表。有关详细信息，请参阅用户客户端应用列表数据块，第 4-94 页。
61	IP 范围规格	传统	包含 IP 地址范围规格。有关详细信息，请参阅用于 5.0 - 5.1.1.x 的 IP 范围规格数据块，第 B-338 页。被块 141 替代。
62	属性规格	当前	包含属性名称和值。有关详细信息，请参阅属性规格数据块，第 4-97 页。
63	MAC 地址规格	当前	包含 MAC 地址范围规格。有关详细信息，请参阅 MAC 地址规格数据块，第 4-99 页。
64	IP 地址规格	当前	包含 IP 和 MAC 地址规格块列表。有关详细信息，请参阅地址规格数据块，第 4-100 页。
65	用户产品	传统	包含从第三方应用导入的主机输入数据，包括第三方应用字符串映射。有关详细信息，请参阅用于 5.0.x 的用户产品数据块，第 B-99 页。 5.0 中引入的后继块类型 118 的结构与块类型 65 的结构相同。
66	连接区块	传统	包含连接区块信息。有关详细信息，请参阅用于 5.0 - 5.1 的连接区块数据块，第 B-151 页。5.0 中引入的后继块类型 119 的结构与块类型 66 的结构相同。
67	修复列表	当前	包含适用于主机的修复。有关详细信息，请参阅修复列表数据块，第 4-103 页。

表 4-30　主机发现和连接数据块类型 （续）

类型	内容	数据块状态	说明
71	一般扫描结果	传统	包含 Nmap 扫描的结果 （如较早版本的产品中所记录）。
72	扫描结果	传统	包含第三方扫描的结果 （如较早版本的产品中所记录）。
76	用户服务器	当前	包含用户输入事件的服务器信息。有关详细信息，请参阅用户服务器数据块，第 4-104 页。
77	用户服务器列表	当前	包含用户服务器块列表。有关详细信息，请参阅用户服务器列表数据块，第 4-105 页。
78	用户主机	当前	包含用户主机输入事件的主机范围的相关信息。有关详细信息，请参阅用户主机数据块 4.7+，第 4-106 页。
79	用户漏洞	传统	包含一个或多个主机的漏洞相关信息 （如较早版本的产品中所记录）。版本 5.0 中引入的后继块的块类型为 124。
80	用户主机漏洞更改	当前	包含停用或激活的漏洞的列表。有关详细信息，请参阅用户漏洞更改数据块 4.7+，第 4-108 页。
81	用户临界点	当前	包含一个或多个主机的临界点更改相关信息。有关详细信息，请参阅用户临界点更改数据块 4.7+，第 4-109 页。
82	用户属性值	当前	包含一个或多个主机的属性值更改。有关详细信息，请参阅用户属性值数据块 4.7+，第 4-111 页。
83	用户协议列表	当前	包含一个或多个主机的协议列表。有关详细信息，请参阅用户协议列表数据块 4.7+，第 4-112 页。
85	漏洞列表	当前	包含适用于主机的漏洞。有关详细信息，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
86	扫描漏洞	传统	包含有关扫描检测到的漏洞的信息 （如较早版本的产品中所记录）。
87	操作系统指纹	传统	包含操作系统指纹列表。有关详细信息，请参阅用于 5.0 - 5.0.2 的操作系统指纹数据块，第 B-129 页。版本 5.1 中引入的后继块的块类型为 130。
88	服务器信息	传统	包含服务器指纹中使用的服务器信息 （如较早版本的产品中所记录）。
89	主服务器	传统	包含主机的服务器信息 （如较早版本的产品中所记录）。
90	完整主机服务器	传统	包含主机的服务器信息 （如较早版本的产品中所记录）。
91	主机配置文件	传统	包含主机的配置文件信息。有关详细信息，请参阅用于 5.2+ 的主机配置文件数据块，第 4-167 页。版本 5.1 中引入的后继块的块类型为 132。
92	完整主机配置文件	传统	包含完整主机配置文件信息 （如较早版本的产品中所记录）。替代数据块 47。

表 4-30　　主机发现和连接数据块类型 （续）

类型	内容	数据块状态	说明
94	身份数据	当前	包含主机的身份数据。有关详细信息，请参阅身份数据块，第 4-114 页。
95	主机 MAC 地址	当前	包含主机的 MAC 地址信息。有关详细信息，请参阅主机 MAC 地址 4.9+，第 4-116 页。
96	辅助主机更新	当前	包含辅助辅助主机更新，第 4-117 页报告的 MAC 地址信息列表。
97	Web 应用程序	传统	包含 Web 应用数据列表 （如较早版本的产品中所记录）。版本 5.0 中引入的后继块的块类型为 123。
98	主服务器	传统	包含主机的服务器信息 （如较早版本的产品中所记录）。
99	完整主机服务器	传统	包含主机的服务器信息 （如较早版本的产品中所记录）。
100	主机客户端应用	传统	包含用于新客户端应用事件的客户端应用信息（如较早版本的产品中所记录）。版本 5.0 中引入的后继块类型 122 的结构与块类型 100 的结构相同。
101	连接统计信息	传统	包含有关 4.9.1+ 中连接统计信息事件的信息（如较早版本的产品中所记录）。
102	扫描结果	传统	包含漏洞的相关信息，且在 “ 添加扫描结果 ” 事件中使用。请参阅扫描结果数据块 5.0 - 5.1.1.x，第 B-96 页。
103	主服务器	当前	包含主机的服务器信息。有关详细信息，请参阅主机服务器数据块 4.10.0+，第 4-141 页。
104	完整主机服务器	当前	包含主机的服务器信息。有关详细信息，请参阅完整主机服务器数据块 4.10.0+，第 4-143 页。
105	服务器信息	传统	包含服务器指纹中使用的服务器信息。有关详细信息，请参阅用于 4.10.x、5.0 - 5.0.2 的服务器信息数据块，第 4-147 页。5.0 中引入的后继块类型 117 的结构与块类型 105 的结构相同。
106	完整服务器信息	当前	包含在主机上检测到的服务器的相关信息。有关详细信息，请参阅完整服务器信息数据块，第 4-150 页。
108	一般扫描结果	当前	包含 Nmap 扫描的结果。有关详细信息，请参阅用于 4.10.0+ 的一般扫描结果数据块，第 4-152 页。
109	扫描漏洞	当前	包含有关第三方扫描检测到的漏洞的信息。请参阅用于 4.10.0+ 的扫描漏洞数据块，第 4-155 页。
111	完整主机配置文件	传统	包含完整主机配置文件信息。有关详细信息，请参阅完整主机配置文件数据块 5.0 - 5.0.2，第 B-298 页。替代数据块 92。

表 4-30　主机发现和连接数据块类型 （续）

类型	内容	数据块状态	说明
112	完整主机客户端应用	当前	包含用于新客户端应用事件的客户端应用信息，且包含漏洞列表。有关详细信息，请参阅完整主机客户端应用数据块 5.0+，第 4-158 页。
115	连接统计信息	传统	包含 5.0 - 5.0.2 中连接统计信息事件的信息。有关详细信息，请参阅连接统计信息数据块 5.0 - 5.0.2，第 B-131 页。版本 5.1 中引入的后继块的块类型为 126。
117	服务器信息	当前	包含服务器指纹中使用的服务器信息。有关详细信息，请参阅用于 4.10.x、5.0 - 5.0.2 的服务器信息数据块，第 4-147 页。
118	用户产品	传统	包含从第三方应用导入的主机输入数据，包括第三方应用字符串映射。有关详细信息，请参阅用于 5.0.x 的用户产品数据块，第 B-99 页。先趋块类型 65 （在 5.0 中被替代）的结构与此块类型的结构相同。版本 5.1 中引入的后继块的块类型为 132。
119	连接区块	传统	包含用于版本 4.10.1 - 5.1 的连接区块信息。有关详细信息，请参阅用于 5.0 - 5.1 的连接区块数据块，第 B-151 页。后继块为 136。
122	主机客户端应用	当前	包含用于版本 5.0+ 的新客户端应用事件的客户端应用信息。有关详细信息，请参阅用于 5.0+ 的主机客户端应用数据块，第 4-160 页。它替代块类型 100。
123	Web 应用程序	当前	包含用于版本 5.0+ 的 Web 应用数据。有关详细信息，请参阅用于 5.0+ 的 Web 应用数据块，第 4-118 页。它替代块类型 97。
124	用户漏洞	当前	包含一个或多个主机的漏洞相关信息。请参阅用户漏洞数据块 5.0+，第 4-161 页。它替代块类型 79。
125	连接统计信息	传统	包含有关 4.10.2 中连接统计信息事件的信息（如较早版本的产品中所记录）。版本 5.1 中引入的后继块的块类型为 115。
126	连接统计信息	传统	包含 5.1 中连接统计信息事件的信息。有关详细信息，请参阅连接统计信息数据块 5.1，第 B-137 页。它替代块类型 115。此块类型被块类型 137 替代。
130	操作系统指纹	当前	包含操作系统指纹列表。有关详细信息，请参阅操作系统指纹数据块 5.1+，第 4-164 页。它替代块类型 87。
131	移动设备信息	当前	包含检测到的移动设备硬件的相关信息。有关详细信息，请参阅用于 5.1+ 的移动设备 信息数据块，第 4-166 页。
132 个	主机配置文件	传统	包含主机的配置文件信息。有关详细信息，请参阅完整主机配置文件数据块 5.2.x，第 B-319 页。它替代块类型 91。被块 139 替代。

表 4-30　　主机发现和连接数据块类型 （续）

类型	内容	数据块状态	说明
134	用户产品	当前	包含从第三方应用导入的主机输入数据，包括第三方应用字符串映射。有关详细信息，请参阅用户产品数据块 5.1+，第 4-176 页。这替代先趋块类型 118。
135	完整主机配置文件	传统	包含完整主机配置文件信息。有关详细信息，请参阅完整主机配置文件数据块 5.1.1，第 B-308 页。替代数据块 111。
136	连接区块	当前	包含连接区块信息。有关详细信息，请参阅用于 6.1+ 的连接区块数据块，第 4-101 页。替代块 119。
137	连接统计信息	传统	包含 5.1.1 中连接事件的信息。有关详细信息，请参阅用于 5.0 - 5.1 的连接区块数据块，第 B-151 页。它替代块类型 126。它被块类型 144 替代。
138	用户客户端应用	当前	包含用户输入的客户端应用数据。有关详细信息，请参阅用于 5.1.1+ 的用户客户端应用数据块，第 4-93 页。它替代块类型。
139	主机配置文件	当前	包含主机的配置文件信息。有关详细信息，请参阅用于 5.2+ 的主机配置文件数据块，第 4-167 页。它替代块类型 132。
140	完整主机配置文件	传统	包含完整主机配置文件信息。有关详细信息，请参阅完整主机配置文件数据块 5.3+，第 5-1 页。替代数据块 135。
141	IP 范围规格	当前	包含 IP 地址范围规格。有关详细信息，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-96 页。它替代块 61。
142	扫描结果	当前	包含漏洞的相关信息，且在 ” 添加扫描结果 “ 事件中使用。请参阅扫描结果数据块 5.2+，第 4-138 页。它替代块 102。
143	主机 IP	当前	包含主机的 IP 地址和上次查看时间信息。有关详细信息，请参阅主机 IP 地址数据块，第 4-98 页。
144 个	连接统计信息	传统	包含 5.2.x 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 5.2.x，第 B-144 页。它替代块类型 137。
146	属性地址	当前	包含 5.2+ 的主机属性地址。有关详细信息，请参阅属性地址数据块 5.2+，第 4-79 页。它替代块类型 38。
148	用户 IOC 更改	当前	包含有关用户 IOC 更改的信息。有关详细信息，请参阅用户 IOC 更改数据块 5.3+，第 4-80 页。
149	完整主机配置文件	当前	包含完整主机配置文件信息。有关详细信息，请参阅完整主机配置文件数据块 5.3+，第 5-1 页。替代数据块 135。

表 4-30　主机发现和连接数据块类型 （续）

类型	内容	数据块状态	说明
152	连接统计信息	传统	包含 5.3+ 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 5.3，第 B-162 页。它替代块类型 144。
154 种	连接统计信息	传统	包含 5.3 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 5.3.1，第 B-170 页。它替代块类型 152。
155	连接统计信息	传统	包含 5.4 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 5.4，第 B-178 页。它替代块类型 154。
157	连接统计信息	传统	包含 5.4.1 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 5.4.1，第 B-194 页。它替代块类型 155。
160	连接统计信息	传统	包含 5.4.1 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 6.0.x，第 B-210 页。它替代块类型 157。
163	连接统计信息	当前	包含 6.0+ 中连接事件的信息。有关详细信息，请参阅连接统计信息数据块 6.2+，第 4-119 页。它替代块类型 160。

字符串数据块

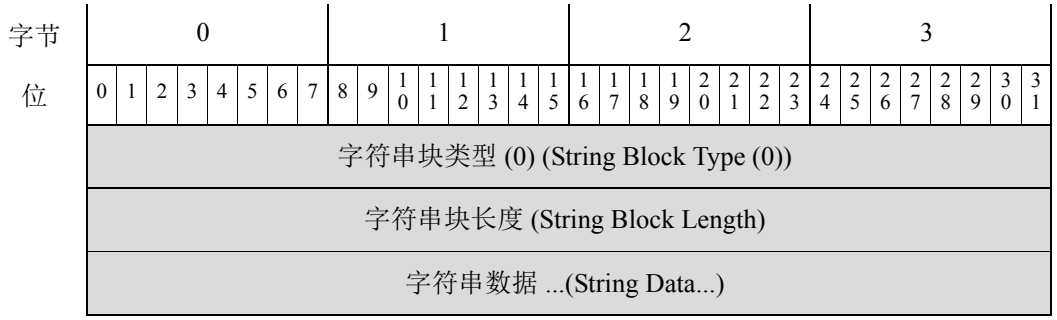
字符串数据块用于发送系列 1 块中的字符串数据。字符串数据块通常出现在其他系列 1 数据块中，用于描述操作系统或服务器名称等。

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

字符串数据块的块类型为系列 1 数据块组中的 0。

注　此数据块中返回的字符串不总是以空值终止 （即不总是以 0 终止）。

下图显示字符串数据块的格式：



下表对字符串数据块的字段进行了说明。

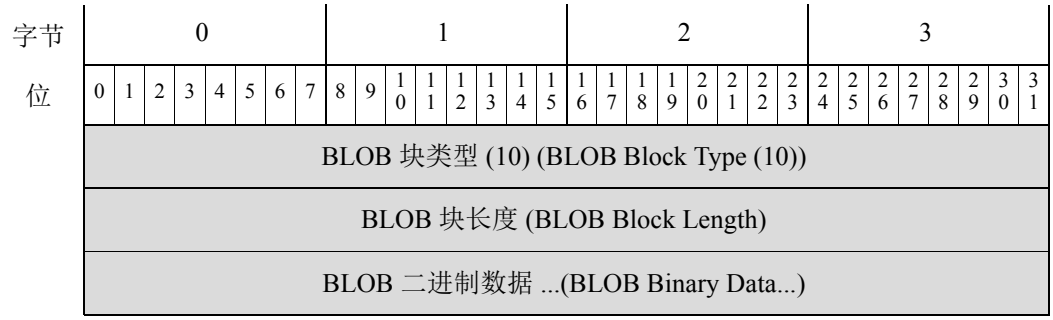
表 4-31　　字符串数据块字段

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

BLOB 数据块

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

下图显示 BLOB 数据块的格式：



下表对 BLOB 数据块的字段进行了说明。

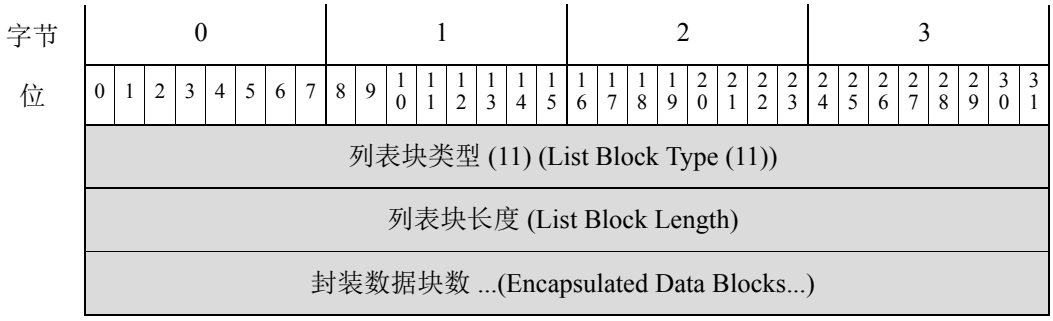
表 4-32　　BLOB 数据块字段

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

列表数据块

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

下图显示列表数据块的基本格式：



下表对列表数据块的字段进行了说明。

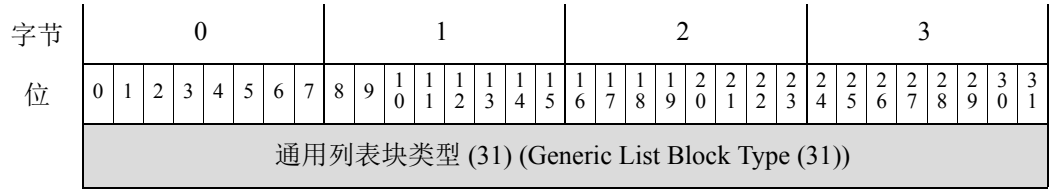
表 4-33　列表数据块字段

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

通用列表块

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

下图显示通用列表数据块的基本结构：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
通用列表块长度 (Generic List Block Length)																																
封装数据块数 ...(Encapsulated Data Blocks...)																																

下表对通用列表数据块的字段进行了说明。

表 4-34　通用列表数据块字段

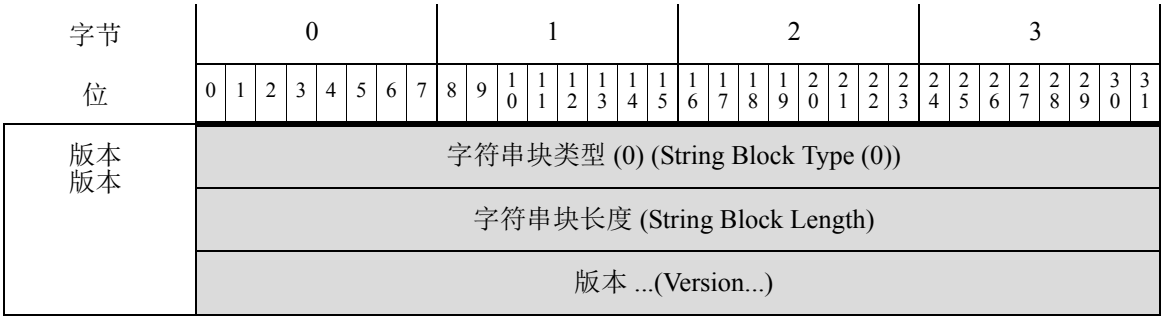
字段	字节数	说明
通用列表块类型 (Generic List Block Type)	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
封装数据块数 (Encapsulated Data Blocks)	变量	封装数据块数最多可以是列表块长度中的最大字节数。

子服务器数据块

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

下图显示子服务器数据块的格式：

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



下表对子服务器数据块的字段进行了说明。

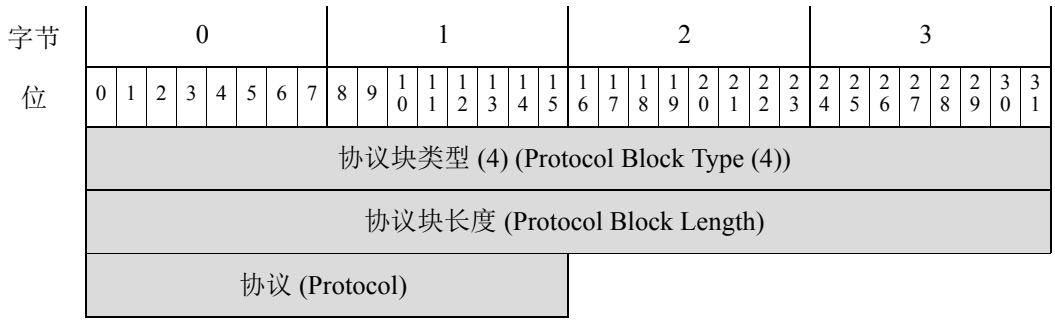
表 4-35　　子服务器数据块字段

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

协议数据块

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

下图显示协议数据块的格式：



下表对协议数据块的字段进行了说明。

表 4-36　协议数据块字段

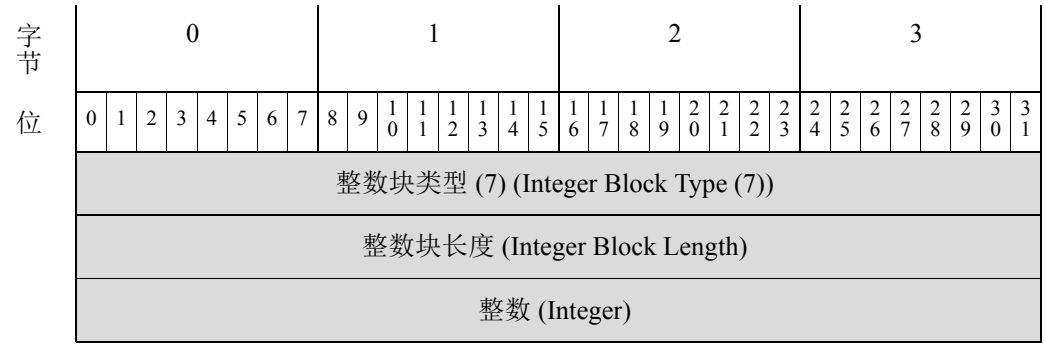
字段	数据类型	说明
协议块类型 (Protocol Block Type)	uint32	启动协议数据块。值始终为 4。
协议块长度 (Protocol Block Length)	uint32	协议数据块中的字节数。值始终为 10。
协议 (Protocol)	uint16	IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如： • 6 - TCP • 17 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如： • 2048 - IP

整数 (INT32) 数据块

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

整数数据块的块类型为系列 1 数据块组中的 7。

下图显示整数数据块的格式：



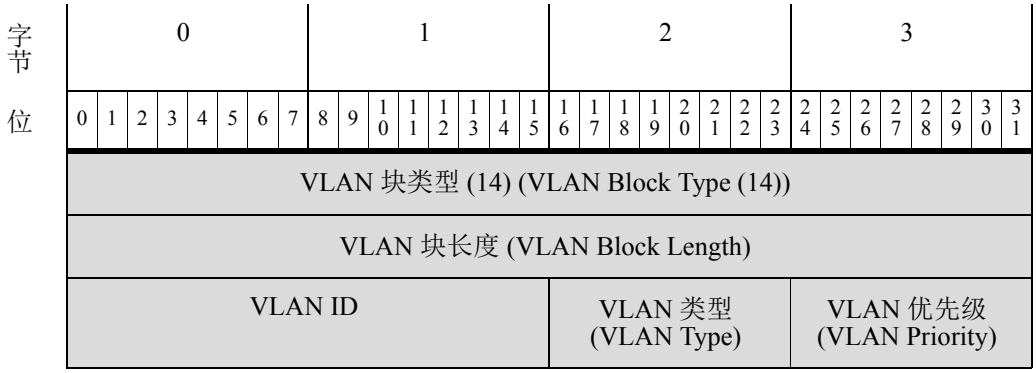
下表对整数数据块的字段进行了说明：

表 4-37　整数数据块字段

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

VLAN 数据块

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



下表对 VLAN 数据块的字段进行了说明。

表 4-38　VLAN 数据块字段

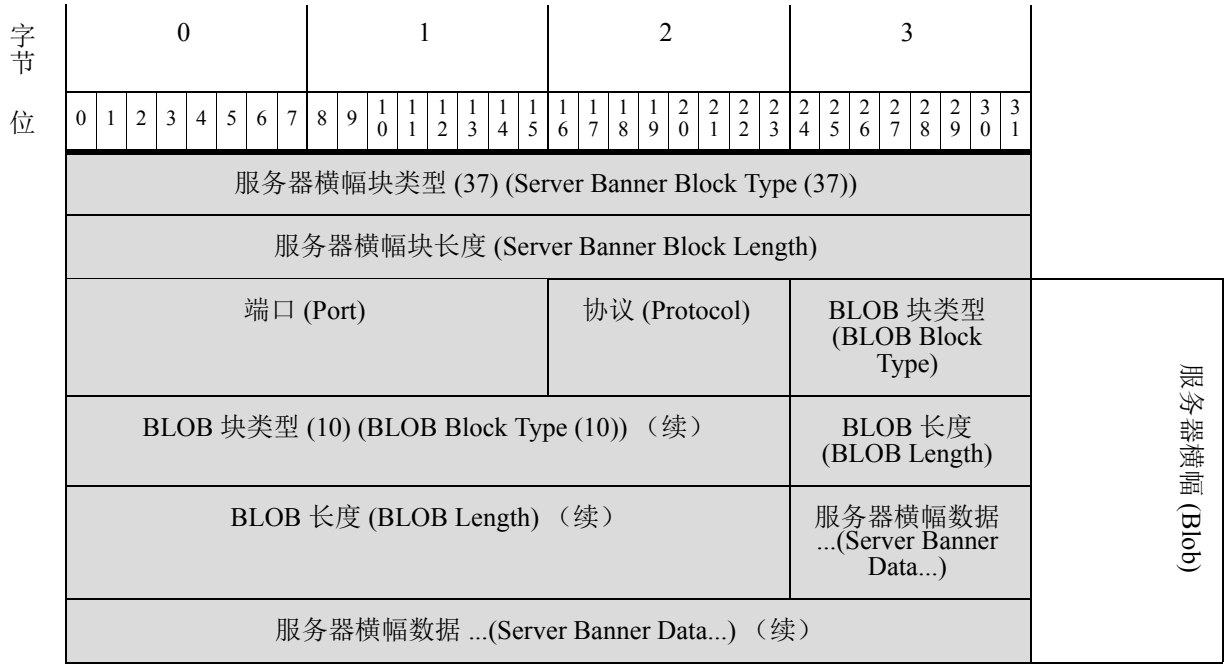
字段	数据类型	说明
VLAN 块类型 (VLAN Block Type)	uint32	启动 VLAN 数据块。值始终为 14。
VLAN 块长度 (VLAN Block Length)	uint32	VLAN 数据块中的字节数。值始终为 12。
VLAN ID	uint16	包含表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。 • 0 - 以太网 • 1 - 令牌环
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。

服务器横幅数据块

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

下图显示服务器横幅数据块的格式。

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



下表对服务器横幅数据块的字段进行了说明。

表 4-39　服务器横幅数据块字段

字段	数据类型	说明
服务器横幅块类型 (Server Banner Block Type)	uint32	启动服务器横幅数据块。值始终为 37。
服务器横幅块长度 (Server Banner Block Length)	uint32	服务器横幅数据块中的字节总数，包括服务器横幅块类型和长度字段的八个字节，加上随后的数据字节数。
端口 (Port)	uint16	服务器在其上运行的端口的端口号。
协议 (Protocol)	uint8	服务器的协议号。
BLOB 块类型 (BLOB Block Type)	uint32	启动包含服务器横幅数据的 BLOB 数据块。值始终为 10。

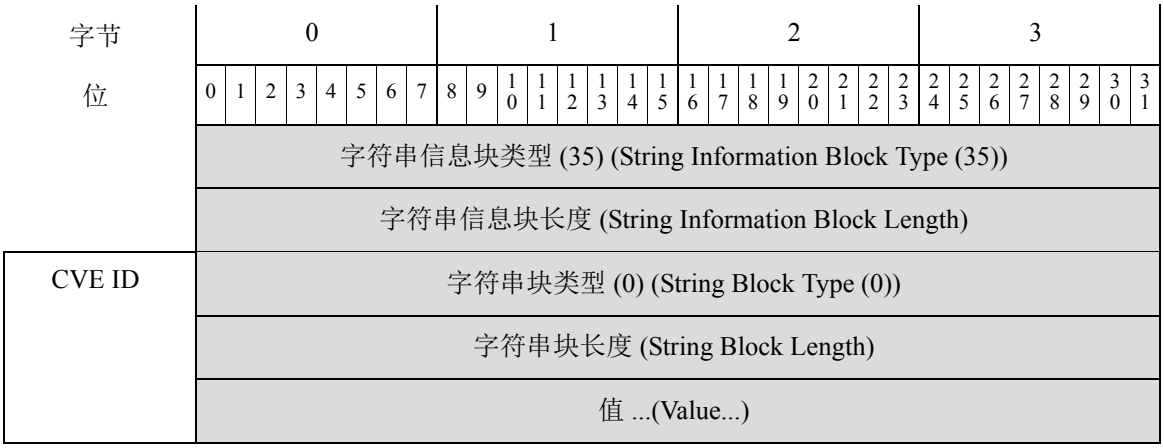
表 4-39　　服务器横幅数据块字段 （续）

字段	数据类型	说明
长度 (Length)	uint32	BLOB 数据块中的字节总数 （通常是 264 个字节）。
横幅 (Banner)	字节 [*n*]	服务器事件中涉及的数据包的前 *n* 个字节， 其中 *n* 小于或等于 256。

字符串信息数据块

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

下图显示字符串信息数据块的格式：



下表对字符串信息数据块的字段进行了说明。

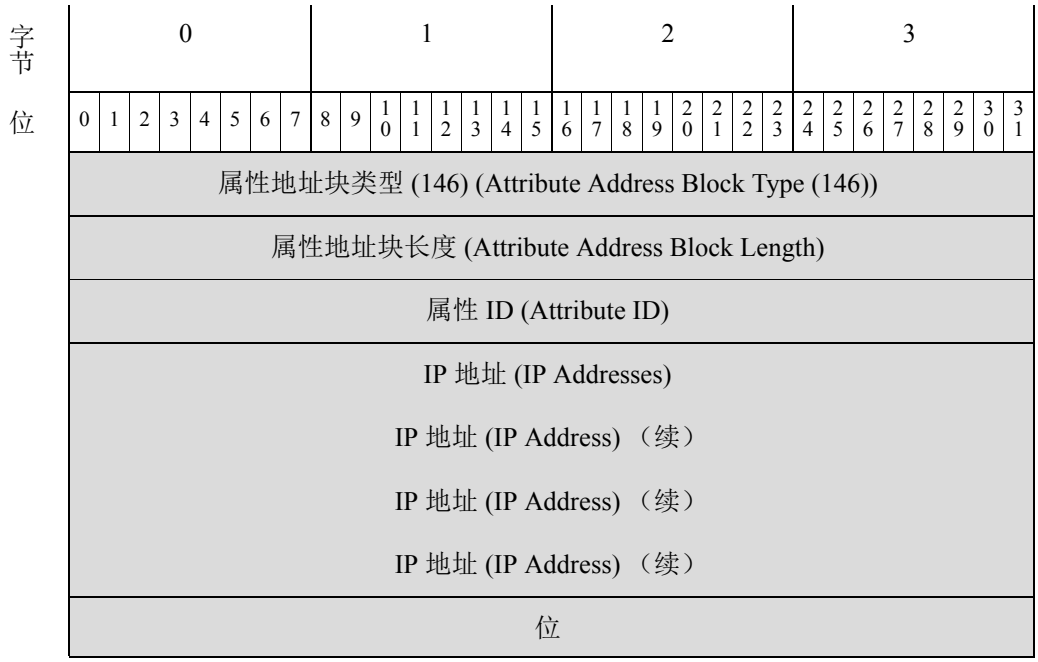
表 4-40　　字符串信息数据块字段

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

属性地址数据块 5.2+

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

下图显示属性地址数据块的基本结构：



下表对属性地址数据块的字段进行了说明。

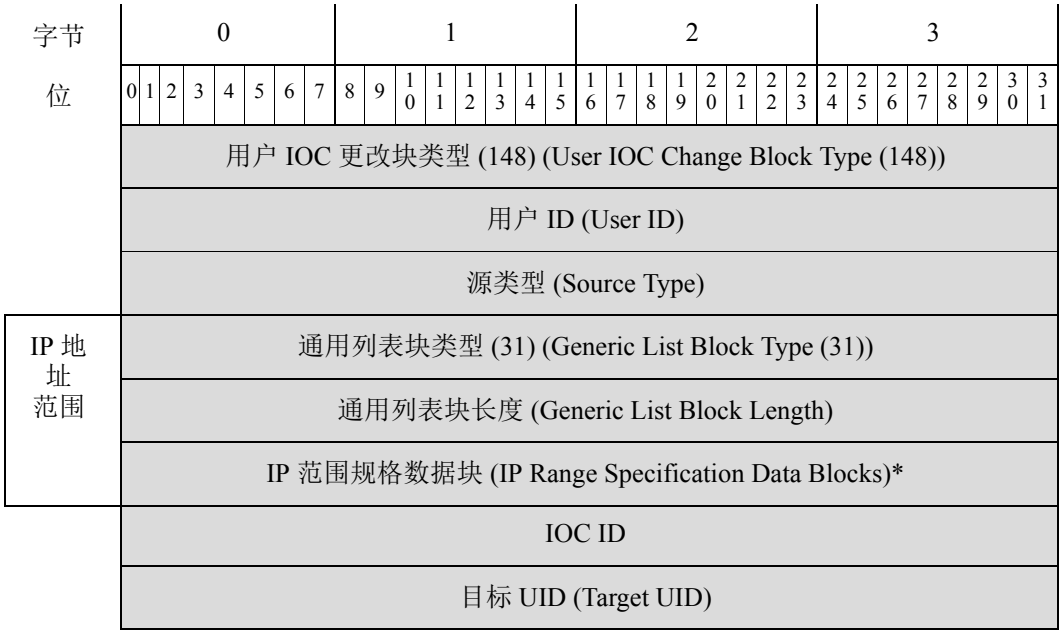
表 4-41　　属性地址数据块 5.2+ 字段

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

用户 IOC 更改数据块 5.3+

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

下图显示用户 IOC 更改数据块的基本结构：



下表对用户服务器数据块的字段进行了说明。

表 4-42　　用户 IOC 更改数据块 5.3+ 字段

字段	数据类型	说明
用户 IOC 更改块类型 (User IOC Change Block Type)	uint32	启动用户 IOC 更改数据块。值始终为 148。
用户 ID (User ID)	uint32	进行 IOC 更改的用户的 ID 号码。
源类型 (Source Type)	uint32	映射到数据源类型的数字： • 0 如果客户端数据由 RNA 检测到 • 1 如果客户端数据由用户提供 • 2 如果客户端数据由第三方扫描仪检测到 • 3 如果客户端数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。

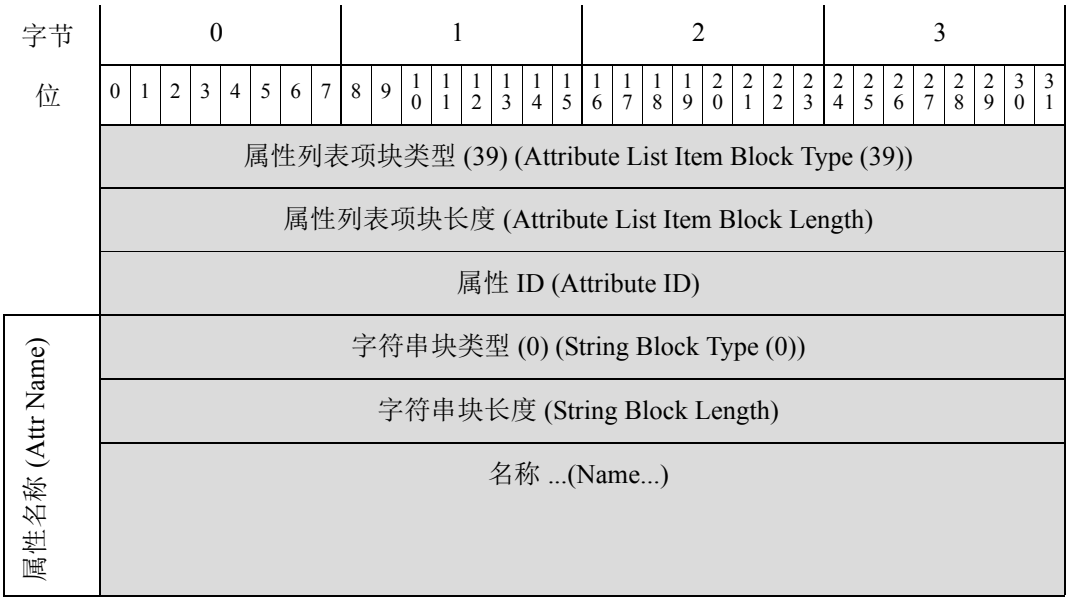
表 4-42　用户 IOC 更改数据块 5.3+ 字段 （续）

字段	数据类型	说明
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装 IP 范围规格数据块。
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-96 页。
IOC ID	uint32	正在更改的 IOC 的 ID 号码。
目标 UID (Target UID)	unit32	未在 eStreamer 输出支持的事件中使用。

属性列表项数据块

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

下图显示属性列表项数据块的基本结构：



下表对属性列表项数据块的字段进行了说明。

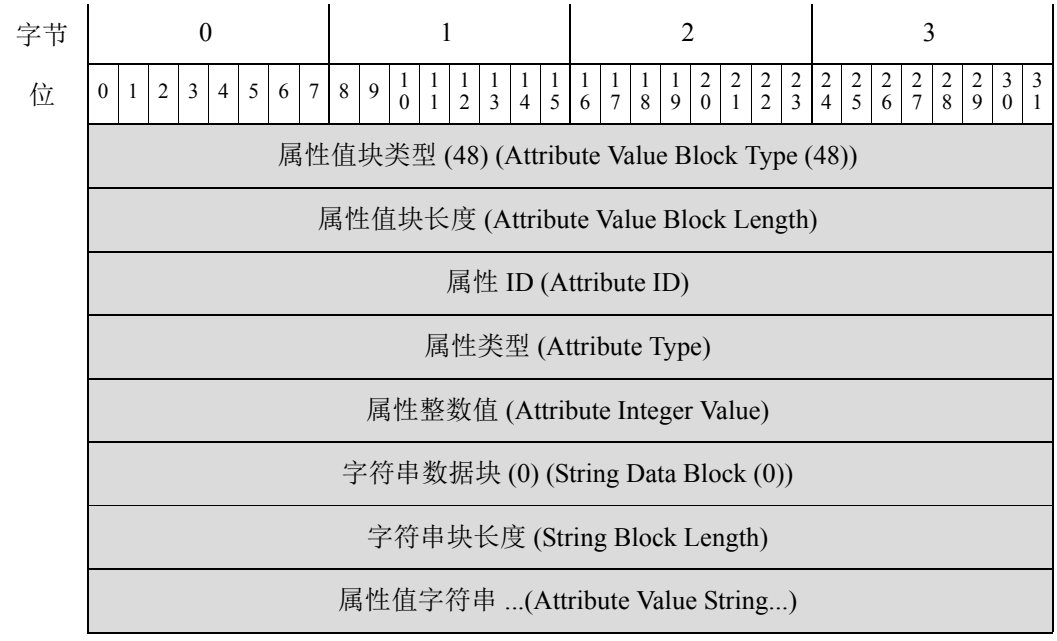
表 4-43　　属性列表项数据块字段

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

属性值数据块

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

下图显示属性值数据块的格式：



下表对属性值数据块的组件进行了说明。

表 4-44　　属性值数据块字段

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

完整子服务器数据块

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

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

下图显示完整子服务器数据块的格式：

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

下表对完整子服务器数据块的组件进行了说明。

表 4-45　完整子服务器数据块字段

字段	数据类型	说明
完整子服务器块类型 (Full Sub-Server Block Type)	uint32	启动完整子服务器数据块。值始终为 51。
完整子服务器块长度 (Full Sub-Server Block Length)	uint32	完整子服务器数据块中的字节总数，包括完整子服务器块类型和长度字段的八个字节，加上随后的完整子服务器数据中的字节数。
字符串块类型 (String Block Type)	uint32	启动包含子服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	子服务器名称字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上子服务器名称中的字节数。
子服务器名称 (Sub-Server Name)	字符串	子服务器名称。
字符串块类型 (String Block Type)	uint32	启动包含子服务器供应商名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	供应商名称字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上子服务器供应商名称中的字节数。
子服务器供应商名称 (Sub-Server Vendor Name)	字符串	子服务器供应商的名称。
字符串块类型 (String Block Type)	uint32	启动包含子服务器版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	子服务器版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上子服务器版本中的字节数。
子服务器版本 (Sub-Server Version)	字符串	子服务器版本。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 VDB 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装主机漏洞数据块。

表 4-45　完整子服务器数据块字段 （续）

字段	数据类型	说明
VDB 主机漏洞数据块 (VDB Host Vulnerability Data Blocks) *	变量	包含 Cisco 识别的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装主机漏洞数据块。
第三方扫描主机漏洞数据块 (Third Party Scan Host Vulnerability Data Blocks) *	变量	包含第三方漏洞扫描仪识别的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。

操作系统数据块 3.5+

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

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

下表对 v3.5 操作系统数据块的字段进行了说明。

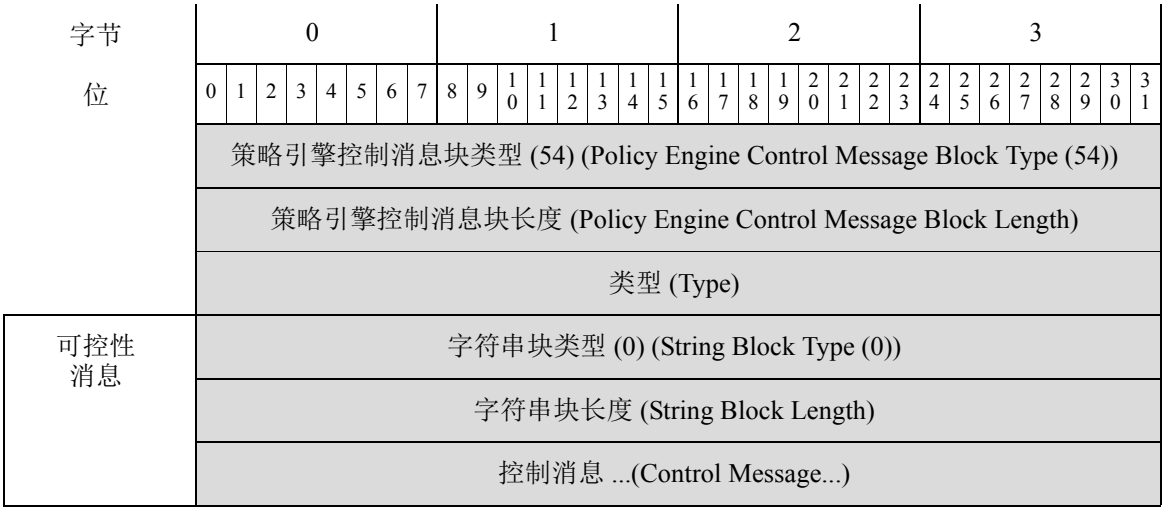
表 4-46　操作系统数据块 3.5+ 字段

字段	数据类型	说明
操作系统数据块类型 (Operating System Data Block Type)	uint32	启动操作系统数据块。值始终为 53。
操作系统数据块长度 (Operating System Data Block Length)	uint32	操作系统数据块中的字节数。此值应始终为 28：块类型和长度字段的八个字节，加上置信度值的四个字节以及指纹 UUID 值的十六个字节。
置信 (Confidence)	uint32	置信度百分比值。
指纹 UUID (Fingerprint UUID)	uint8[16]	采用八位组的指纹识别号，用作操作系统的唯一标识符。在 Cisco 数据库中，指纹 UUID 映射到操作系统名称、供应商和版本。

策略引擎控制消息数据块

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

下图显示策略引擎控制消息数据块的格式：



下表对策略引擎控制消息数据块的组件进行了说明。

表 4-47　策略引擎控制消息数据块字段

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

用于 4.7+ 的属性定义数据块

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

有关这些事件的详细信息，请参阅属性消息，第 4-57 页。

下图显示属性定义数据块的基本结构：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
属性定义块类型 (55) (Attribute Definition Block Type (55))																																
属性定义块长度 (Attribute Definition Block Length)																																
源 ID (Source ID)																																
UUID UUID （续） UUID （续） UUID （续）																																
ID																																

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名称 ...(Name...)																															
	属性类型 (Attribute Type)																															
	属性类别 (Attribute Category)																															
	整数范围的起始值 (Starting Value for Integer Range)																															
	整数范围的结束值 (Ending Value for Integer Range)																															
	自动分配的 IP 地址标志 (Auto-Assigned IP Address Flag)																															
	属性列表项块类型 (39) (Attribute List Item Block Type (39))																															
	属性列表项块长度 (Attribute List Item Block Length)																															
列表项 (List Item)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	属性列表项 ...(Attribute List Items...)																															
	属性地址块类型 (38) (Attribute Address Block Type (38))																															
	属性地址块长度 (Attribute Address Block Length)																															
地址列表 (Address List)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	属性地址列表 ...(Attribute Address List...)																															

属性列表项块类型 (39) (Attribute List Item Block Type (39))	属性列表项列表 (List of Attribute List Items)
属性列表项块长度 (Attribute List Item Block Length)	
列表块类型 (11) (List Block Type (11))	
列表块长度 (List Block Length)	
属性列表项 ...(Attribute List Items...)	
属性地址块类型 (38) (Attribute Address Block Type (38))	属性地址
属性地址块长度 (Attribute Address Block Length)	
列表块类型 (11) (List Block Type (11))	
列表块长度 (List Block Length)	
属性地址列表 ...(Attribute Address List...)	

下表对属性定义数据块的字段进行了说明。

表 4-48　　属性定义数据块字段

字段	数据类型	说明
属性定义块类型 (Attribute Definition Block Type)	uint32	启动属性定义数据块。值始终为 55。
属性定义块长度 (Attribute Definition Block Length)	uint32	属性定义数据块中的字节数，包括属性定义块类型和长度字段的八个字节，加上随后的属性定义数据的字节数。
源 ID (Source ID)	uint32	映射到属性数据源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
UUID	uint8[16]	充当受影响属性的唯一标识符的 ID 号码。
属性 ID (Attribute ID)	uint32	受影响属性的标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动属性定义名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	属性定义名称字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上属性定义名称中的字节数。
名称 (Name)	字符串	属性定义名称。
属性类型 (Attribute Type)	uint32	属性的类型。可能的值包括： • 0 - 值为文本的属性；这使用字符串数据 • 1 - 具有范围值的属性；这使用整数数据 • 2 - 具有可能值列表的属性；这使用整数数据 • 3 - 值为 URL 的属性；这使用字符串数据 • 4 - 值为二进制 BLOB 的属性；这使用字符串数据
属性类别 (Attribute Category)	uint32	属性类别。
范围的起始值 (Starting Value for Range)	uint32	定义属性的整数范围中的第一个整数。
范围的结束值 (Ending Value for Range)	uint32	定义属性的整数范围中的最后一个整数。
自动分配的 IP 地址标志 (Auto-Assigned IP Address Flag)	uint32	表示 IP 地址是否是根据属性自动分配的标志。
列表块类型 (List Block Type)	uint32	启动由传送属性列表项的属性列表项数据块组成的列表数据块。值始终为 11。

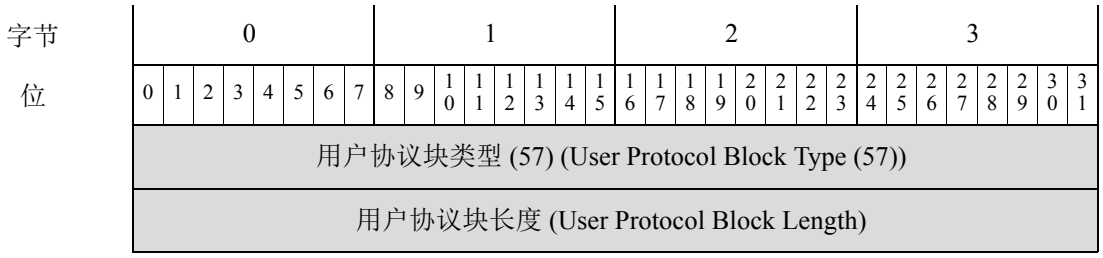
表 4-48　　属性定义数据块字段 （续）

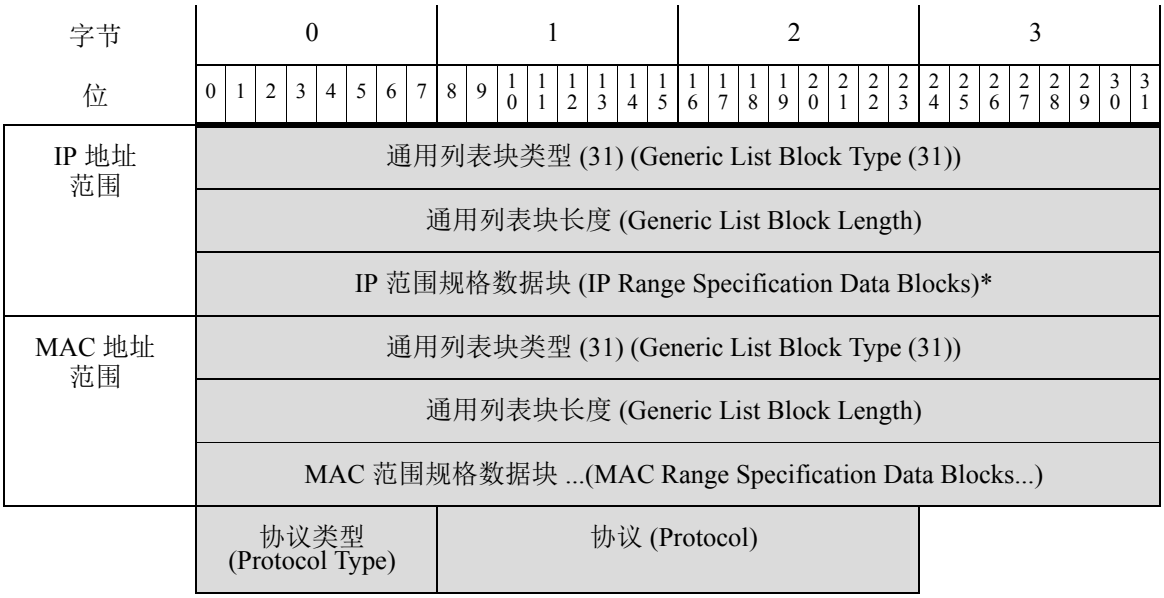
字段	数据类型	说明
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装属性列表项数据块。 此字段后面是零个或多个属性列表项数据块。
属性列表项块类型 (Attribute List Item Block Type)	uint32	启动第一个属性列表项数据块。此数据块后面可以跟随最大长度为列表块长度字段中定义的限值的其他属性列表项数据块。
属性列表项块长度 (Attribute List Item Block Length)	uint32	属性列表项字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上属性列表项中的字节数。
属性列表项 (Attribute List Item)	变量	属性列表项数据，如属性列表项数据块，第 4-81 页中所记录。
列表块类型 (List Block Type)	uint32	启动由传输带该属性的主机的 IP 地址的属性地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装属性地址数据块。 此字段后面是零个或多个属性地址数据块。
属性地址块类型 (Attribute Address Block Type)	uint32	启动第一个属性地址数据块。此数据块后面可以跟随最大长度为列表块长度字段中定义的限值的其他属性地址数据块。
属性地址块长度 (Attribute Address Block Length)	uint32	属性地址数据块中的字节数，包括块类型和报头字段的八个字节，加上属性地址中的字节数。
属性地址 (Attribute Address)	变量	属性地址数据，如属性地址数据块 5.2+，第 4-79 页中所记录。

用户协议数据块

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

下图显示用户协议数据块的基本结构：





下表对用户协议数据块的字段进行了说明。

表 4-49　用户协议数据块字段

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

表 4-49　用户协议数据块字段 （续）

字段	字节数	说明
MAC 范围规格数据块 (MAC Range Specification Data Blocks) *	变量	包含用于用户输入的 MAC 地址范围相关信息的 MAC 范围规格数据块。有关此数据块的说明，请参阅 MAC 地址规格数据块，第 4-99 页。
协议类型 (Protocol Type)	uint8	指示协议的类型。对于 IP 等网络层协议，协议为 0，对于 TCP 或 UDP 等传输层协议，协议为 1。
协议 (Protocol)	uint16	启动用于数据块中包含的数据的协议。

用于 5.1.1+ 的用户客户端应用数据块

用户客户端应用数据块包含客户端应用数据来源、添加数据的用户的标识号以及 IP 地址范围数据块列表的相关信息。版本 6.3 中添加的负载 ID 指定与记录相关的应用实例。用户客户端应用数据块的块类型为系列 1 数据块组中的 138。它取代块类型 59。

下图显示用户客户端应用数据块的基本结构：

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

下表对用户客户端应用数据块的字段进行了说明。

表 4-50　用户客户端应用数据块字段

字段	字节数	说明
用户客户端应用块类型 (User Client Application Block Type)	uint32	启动用户客户端应用数据块。值始终为 138。
用户客户端应用块长度 (User Client Application Block Length)	uint32	用户客户端应用数据块中的字节总数，包括用户客户端应用块类型和长度字段的八个字节，加上随后的用户客户端应用数据的字节数。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装 IP 范围规格数据块。
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-96 页。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号 （如适用）。
客户端应用 ID (Client Application ID)	uint32	被检测客户端应用的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动包含客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	客户端应用版本字符串数据块中的字节数，包括字符串块类型和长度字段，加上版本中的字节数。
版本 (Version)	字符串	客户端应用版本。
负载类型 (Payload Type)	uint32	包括此字段以向后兼容。它始终是 0。
Web 应用 ID (Web Application ID)	uint32	Web 应用 （如适用）的内部标别号。

用户客户端应用列表数据块

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

下图显示用户客户端应用列表数据块的基本结构：

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

下表对用户客户端应用列表数据块的字段进行了说明。

表 4-51　　用户客户端应用列表数据块字段

字段	字节数	说明
用户客户端应用列表块类型 (User Client Application List Block Type)	uint32	启动用户客户端应用列表数据块。值始终为 60。
用户客户端应用列表块长度 (User Client Application List Block Length)	uint32	用户客户端应用列表数据块中的字节总数，包括用户客户端应用列表块类型和长度字段的八个字节，加上随后的用户客户端应用列表数据的字节数。
源类型 (Source Type)	uint32	映射到数据源类型的数字： • 0 如果客户端数据由 RNA 检测到 • 1 如果客户端数据由用户提供 • 2 如果客户端数据由第三方扫描仪检测到 • 3 如果客户端数据由命令行工具 （如 nmimport.pl）或主机输入 API 客户端提供
源 ID (Source ID)	uint32	映射到添加受影响客户端应用的源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
通用列表块类型 (Generic List Block Type)	uint32	启动通用列表数据块。值始终为 31。

表 4-51　用户客户端应用列表数据块字段 （续）

字段	字节数	说明
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
用户客户端应用块 (User Client Application Blocks)	变量	封装用户客户端应用数据块数最多可以是列表块长度中的最大字节数。有关用户客户端应用数据块的详细信息，请参阅用于 5.1.1+ 的用户客户端应用数据块，第 4-93 页。

用于 5.2+ 的 IP 地址范围数据块

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

下图显示 IP 地址范围数据块的格式：

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

下表对 IP 地址范围规格数据块的组件进行了说明。

表 4-52　　IP 地址范围数据块字段

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

属性规格数据块

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

下图显示属性规格数据块的格式：

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

下表对属性规格数据块的组件进行了说明。

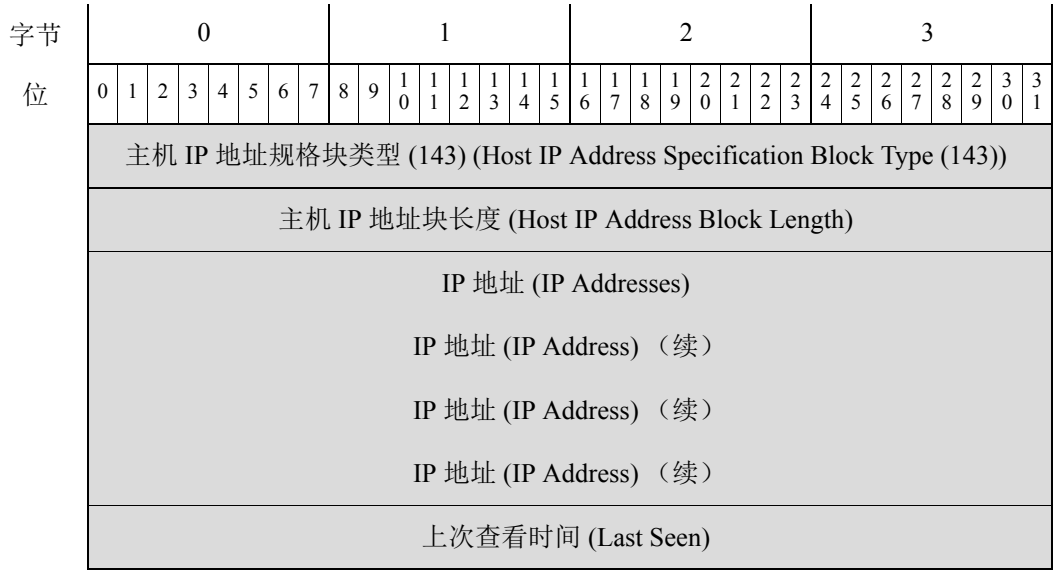
表 4-53　　属性规格数据块字段

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

主机 IP 地址数据块

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

下图显示主机 IP 地址数据块的格式：



下表对主机 IP 地址数据块的组件进行了说明。

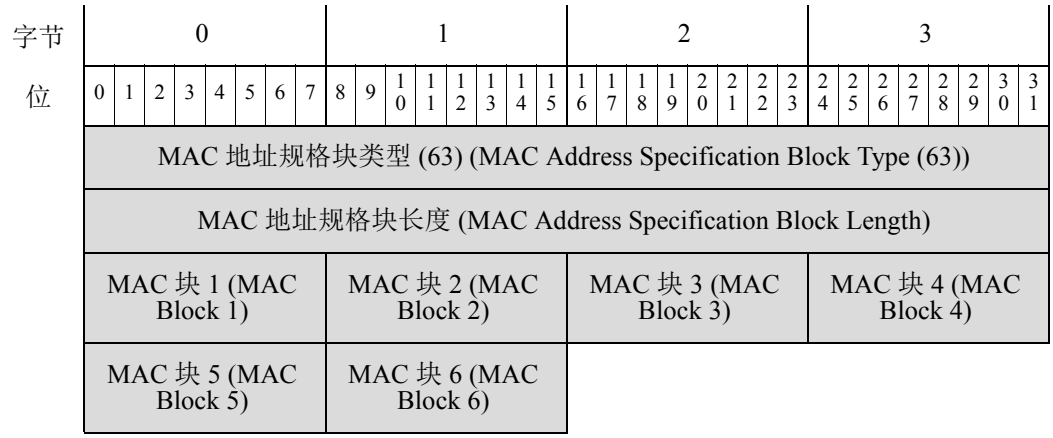
表 4-54　　主机 IP 地址数据块字段

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

MAC 地址规格数据块

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

下图显示 MAC 地址规格数据块的格式：



下表对 MAC 地址规格数据块的组件进行了说明。

表 4-55　　MAC 地址规格数据块字段

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

地址规格数据块

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

下图显示地址规格数据块的基本结构：

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

下表对地址规格数据块的字段进行了说明。

表 4-56　地址规格数据块字段

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

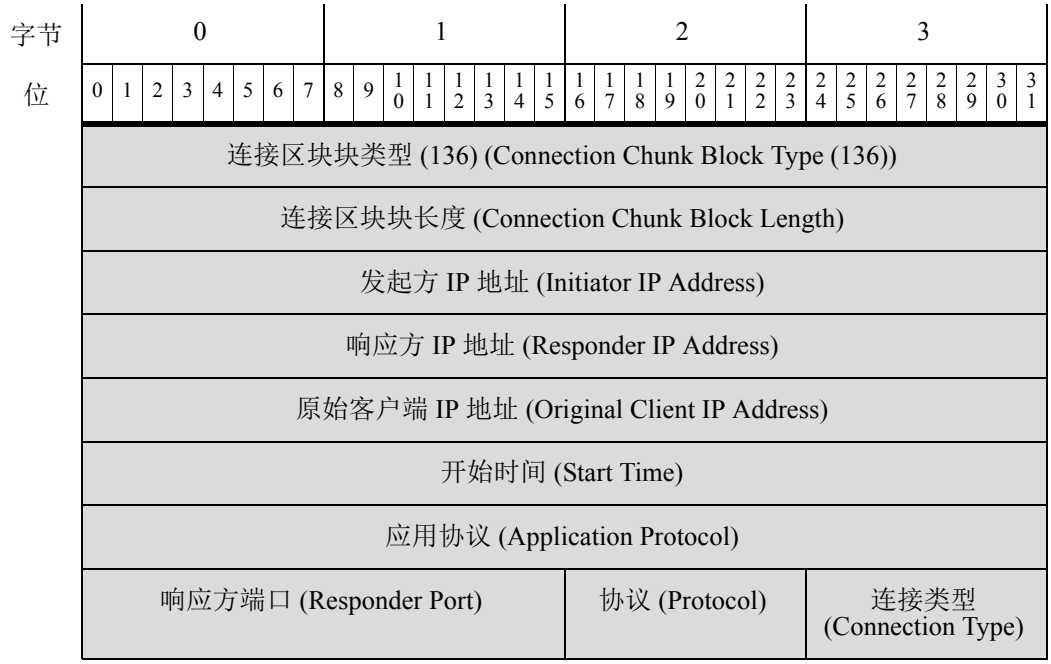
表 4-56　地址规格数据块字段 （续）

字段	字节数	说明
IP 地址范围规格数据块 (IP Address Range Specification Data Blocks)	变量	封装 IP 地址范围规格数据块数最多可以是列表块长度中的最大字节数。有关详细信息，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-96 页。
通用列表块类型 (Generic List Block Type)	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
MAC 地址规格数据块 (MAC Address Specification Data Blocks)	变量	封装 MAC 地址规格数据块数最多可以是列表块长度中的最大字节数。有关详细信息，请参阅 MAC 地址规格数据块，第 4-99 页。

用于 6.1+ 的连接区块数据块

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

下图显示连接区块数据块的格式：



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
NetFlow 检测器 IP 地址 (NetFlow Detector IP Address)																																
发送的数据包数 (Packets Sent) 发送的数据包数 (Packets Sent) （续）																																
接收的数据包数 (Packets Received) 接收的数据包数 (Packets Received) （续）																																
发送的字节数 (Bytes Sent) 发送的字节数 (Bytes Sent) （续）																																
接收的字节数 (Bytes Received) 接收的字节数 (Bytes Received) （续）																																
连接 (Connections)																																

下表对连接区块数据块的组件进行了说明。

表 4-57　　连接区块数据块字段

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

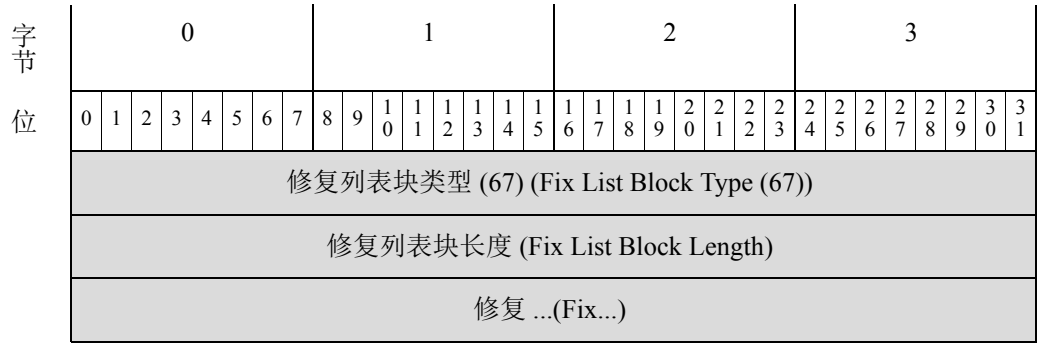
表 4-57　　连接区块数据块字段 （续）

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

修复列表数据块

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

下图显示修复列表数据块的格式：



下表对修复列表数据块的组件进行了说明。

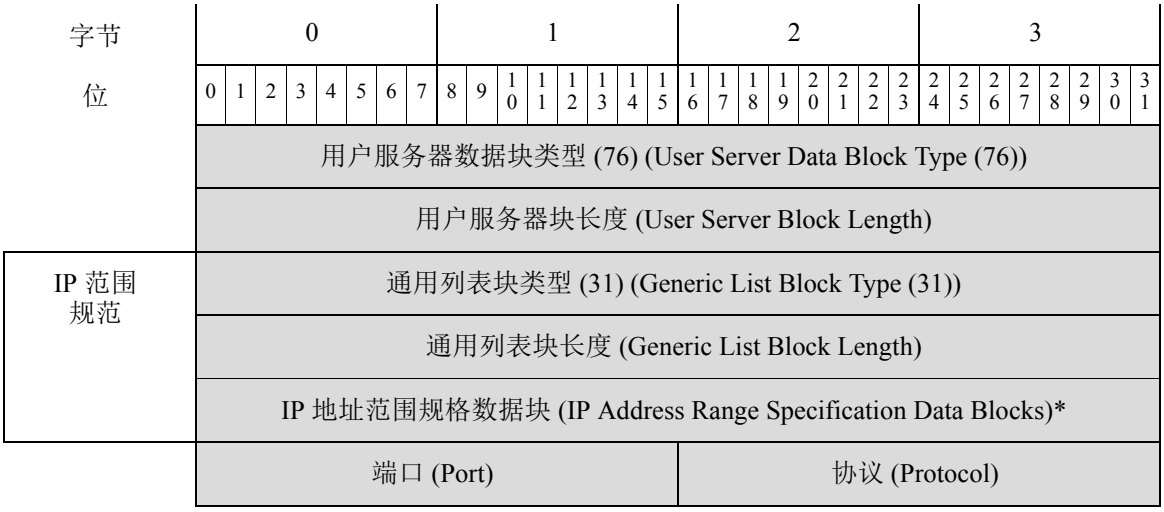
表 4-58　修复列表数据块字段

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

用户服务器数据块

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

下图显示用户服务器数据块的基本结构：



下表对用户服务器数据块的字段进行了说明。

表 4-59　用户服务器数据块字段

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

表 4-59　　用户服务器数据块字段 （续）

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

用户服务器列表数据块

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

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

下表对用户服务器列表数据块的字段进行了说明。

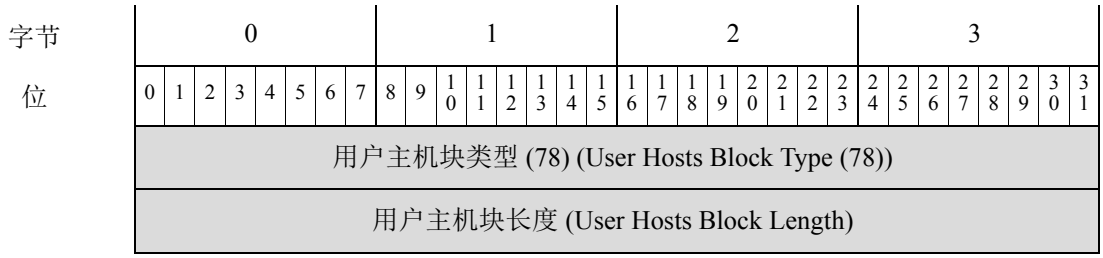
表 4-60　用户服务器列表数据块字段

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

用户主机数据块 4.7+

用户主机数据块在用户添加和删除主机消息，第 4-55 页中使用，用于包含用户主机输入事件的主机范围以及用户和源身份的相关信息。用户主机数据块的块类型为系列 1 数据块组中的 78。

下图显示用户主机数据块的基本结构：



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

下表对用户主机数据块的字段进行了说明：

表 4-61　　用户主机数据块字段

字段	字节数	说明
用户主机块类型 (User Hosts Block Type)	uint32	启动用户主机数据块。值始终为 78。
用户主机块长度 (User Hosts Block Length)	uint32	用户主机数据块中的字节总数，包括用户主机块类型和长度字段的八个字节，加上随后的用户主机数据的字节数。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装 IP 范围规格数据块。
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-96 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 MAC 地址范围数据的 MAC 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装 MAC 范围规格数据块。

表 4-61　用户主机数据块字段 （续）

字段	字节数	说明
MAC 范围规格数据块 (MAC Range Specification Data Blocks) *	变量	包含用于用户输入的 MAC 地址范围相关信息的 MAC 范围规格数据块。有关此数据块的说明，请参阅 MAC 地址规格数据块，第 4-99 页。
源 ID (Source ID)	uint32	映射到添加或更新主机数据的源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
源类型 (Source Type)	uint32	映射到数据源类型的数字： • 0 如果主机数据由 RNA 检测到 • 1 如果主机数据由用户提供 • 2 如果主机数据由第三方扫描仪检测到 • 3 如果主机数据由命令行工具 （如 nmimport.pl）或主机输入 API 客户端提供

用户漏洞更改数据块 4.7+

用户漏洞更改数据块包含主机的停用漏洞列表、停用漏洞的用户的标识号、提供漏洞更改的源的相关信息以及临界点值。用户漏洞更改数据块的块类型为系列 1 数据块组中的 80。对之前用户漏洞更改数据块的更改包括新源类型字段以及用通用列表数据块代替列表数据块来存储漏洞停用。此数据块在用户漏洞更改消息中使用，如用于版本 4.6.1+ 的用户设置漏洞消息，第 4-55 页中所记录。

下图显示用户漏洞更改数据块的基本结构：

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

下表对通用列表数据块的字段进行了说明。

表 4-62　用户漏洞更改数据块字段

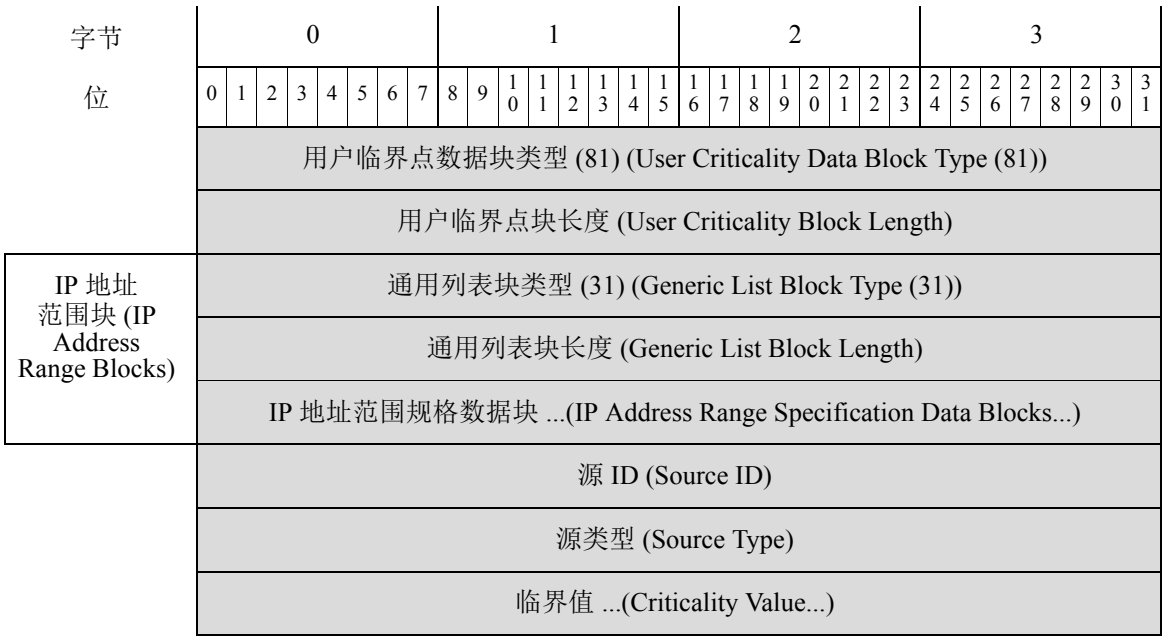
字段	字节数	说明
用户漏洞更改数据块类型 (User Vulnerability Change Data Block Type)	uint32	启动用户漏洞更改数据块。值始终为 80。
用户漏洞更改块长度 (User Vulnerability Change Block Length)	uint32	用户漏洞更改数据块中的字节总数，包括主机漏洞块类型和长度字段的八个字节，加上随后的主机漏洞数据的字节数。
源 ID (Source ID)	uint32	映射到更新或添加主机漏洞更改值的源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
源类型 (Source Type)	uint32	映射到数据源类型的数字： • 0 如果主机漏洞数据由 RNA 检测到 • 1 如果主机漏洞数据由用户提供 • 2 如果主机漏洞数据由第三方扫描仪检测到 • 3 如果主机漏洞数据由命令行工具 （如 nmimport.pl） 或主机输入 API 客户端提供
类型 (Type)	uint32	漏洞的类型。
通用列表块类型 (Generic List Block Type)	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
用户漏洞数据块 (User Vulnerability Data Blocks)	变量	封装用户漏洞数据块数最多可以是列表块长度中的最大字节数。有关详细信息，请参阅用户漏洞数据块 5.0+，第 4-161 页。

用户临界点更改数据块 4.7+

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

用户临界点数据块在用户设置主机临界点消息中使用，如用户设置主机临界点消息，第 4-57 页中所记录。

下图显示用户临界点数据块的基本结构：



下表对用户临界点数据块的字段进行了说明。

表 4-63　　用户临界点数据块字段

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

表 4-63　　用户临界点数据块字段 （续）

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

用户属性值数据块 4.7+

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

下图显示用户属性值数据块的结构：

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

下表对用户属性值数据块的字段进行了说明。

表 4-64　用户属性值数据块字段

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

用户协议列表数据块 4.7+

用户协议列表数据块用于包含协议数据源、添加数据的用户的标识号以及用户协议数据块列表的相关信息。用户协议列表数据块的块类型为系列 1 数据块组中的 83。有关用户协议数据块的详细信息，请参阅用户协议数据块，第 4-91 页。

用户协议列表数据块在用户协议消息中使用，如用户协议消息，第 4-59 页中所记录。

下图显示用户协议列表数据块的基本结构：

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

下表对通用列表数据块的字段进行了说明。

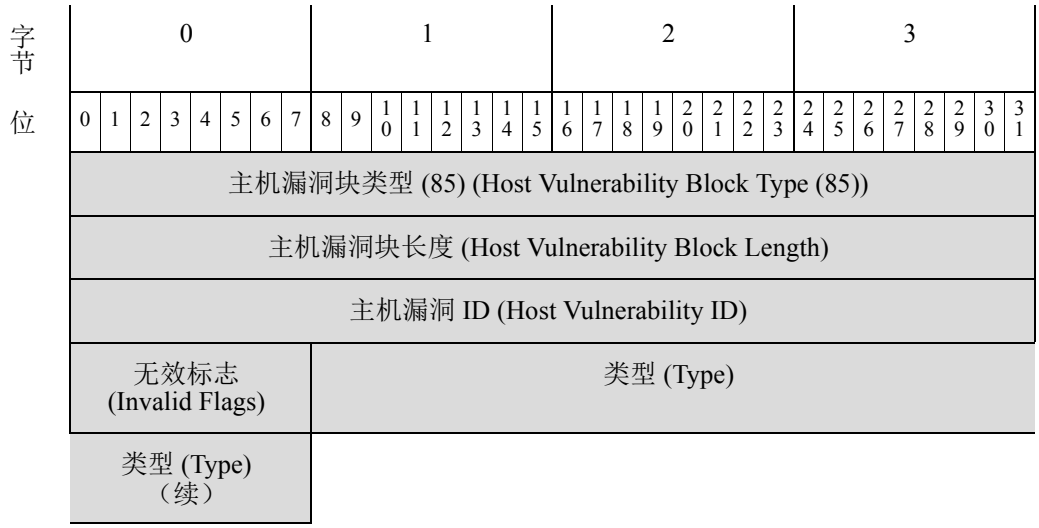
表 4-65　　用户协议列表数据块字段

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

主机漏洞数据块 4.9.0+

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

下图显示主机漏洞数据块的格式：



下表对主机漏洞数据块的组件进行了说明。

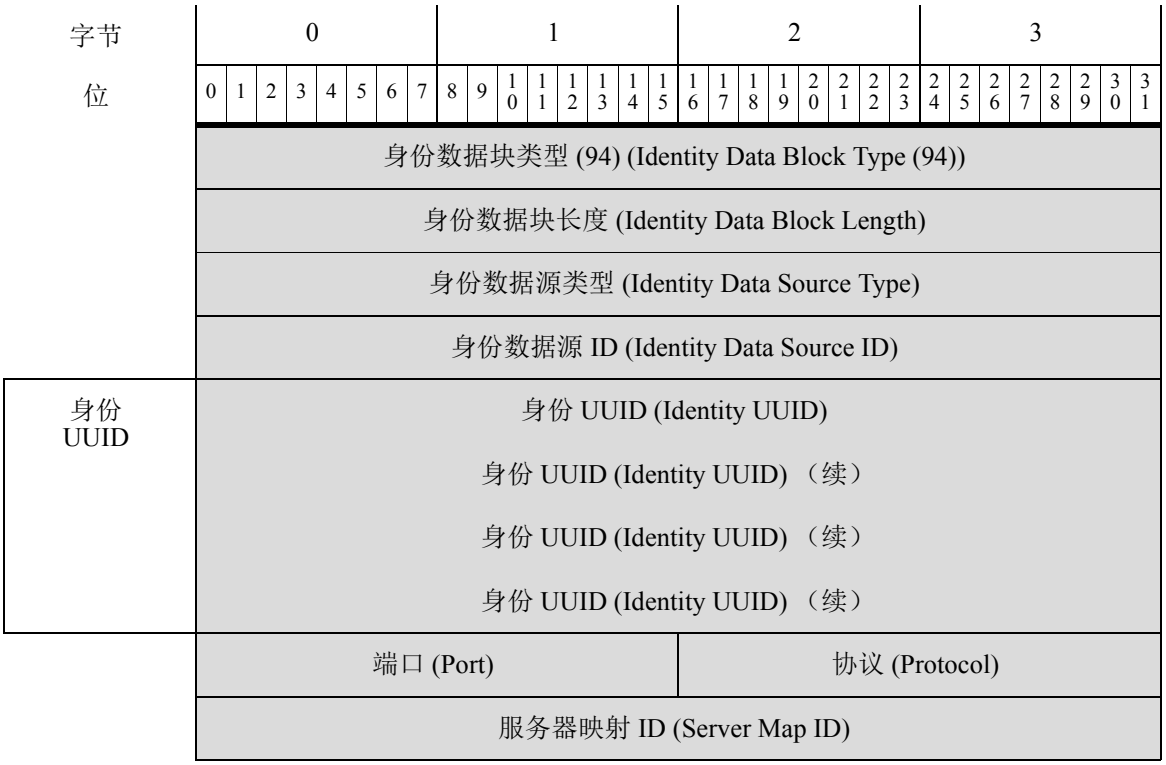
表 4-66　主机漏洞数据块字段

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

身份数据块

身份数据块的块类型为系列 1 数据块组中的 94。身份数据块在身份冲突和身份超时消息中使用，表示操作系统或服务器指纹源的身份冲突或超时的时间。数据块描述已被识别为与活动的源身份冲突的报告身份 （用户、扫描仪或应用）。有关详细信息，请参阅身份冲突和身份超时系统消息，第 4-60 页。

下图显示用于 4.9+ 的身份数据块的格式：



下表对 Cisco 身份数据块的字段进行了说明。

表 4-67　　身份数据块字段

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

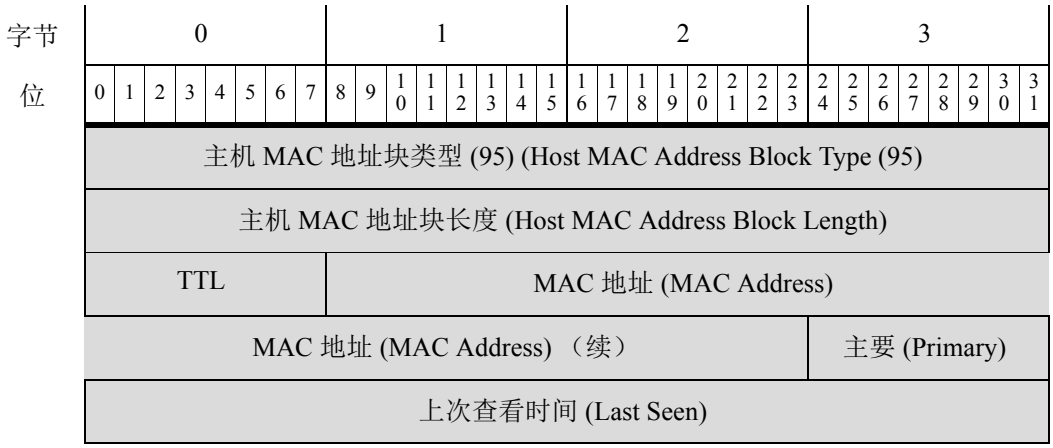
表 4-67　　身份数据块字段 （续）

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

主机 MAC 地址 4.9+

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

下图显示 4.9+ 中的主机 MAC 地址数据块的格式：



下表对主机 MAC 地址数据块的字段进行了说明。

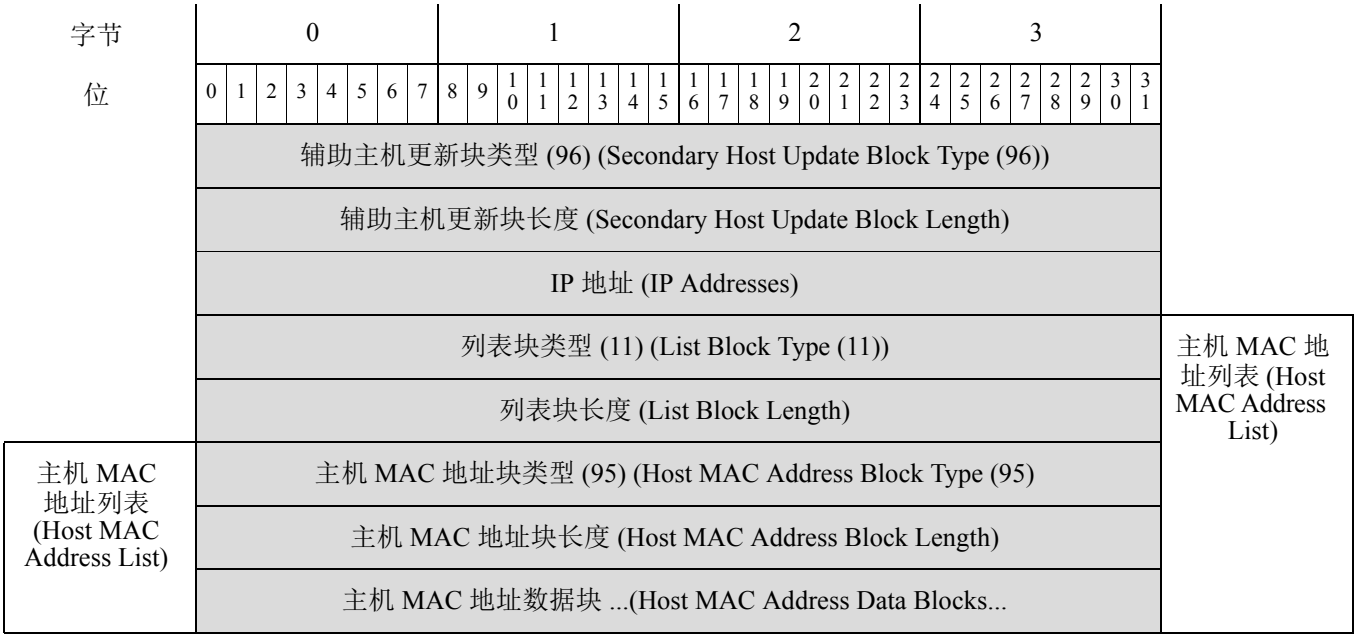
表 4-68　　主机 MAC 地址数据块字段

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

辅助主机更新

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

下图显示辅助主机更新数据块的格式：



下表对辅助主机更新数据块的字段进行了说明。

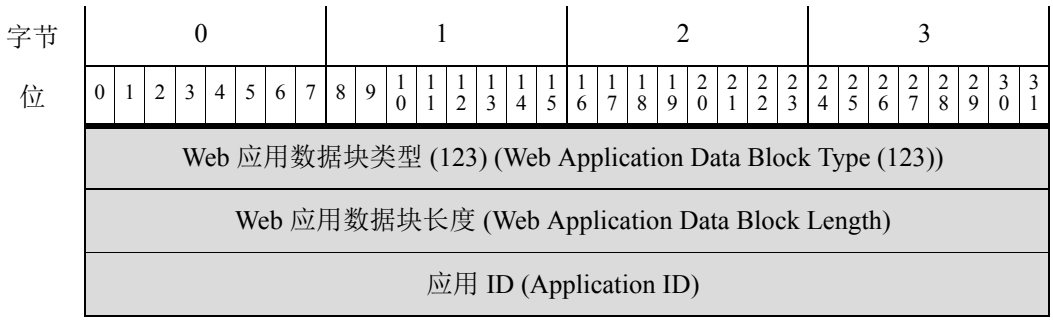
表 4-69　辅助主机更新数据块字段

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

用于 5.0+ 的 Web 应用数据块

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

下图显示 5.0+ 中的 Web 应用数据块的格式：



下表对 Web 应用数据块的字段进行了说明。

表 4-70　　Web 应用数据块字段

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

连接统计信息数据块 6.2+

连接统计信息数据块在连接数据消息中使用。用于 6.2+ 的连接统计信息数据块中添加了第三个安全情报字段。用于版本 6.2+ 的连接统计信息数据块的块类型为系列 1 数据块组中的 168。它替代块类型 163，连接统计信息数据块 6.1.x，第 B-229 页。

您可以通过在事件版本为 13 且事件代码为 71 的请求消息中设置扩展事件标志 （“ 请求标志 ” (Request Flags) 字段中的位 30）请求连接事件记录。请参阅请求标志，第 2-11 页。如果您启用位 23，则记录中会包含扩展事件报头。

有关连接统计信息数据消息的详细信息，请参阅连接统计信息数据消息，第 4-54 页。

下图显示用于 6.2+ 的连接统计信息数据块的格式：

7

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
连接统计信息数据块类型 (168) (Connection Statistics Data Block Type (168))																																
连接统计信息数据块长度 (Connection Statistics Data Block Length)																																
设备 ID (Device ID)																																
入口区 (Ingress Zone) 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续） 入口区 (Ingress Zone) （续）																																
出口区 (Egress Zone) 出口区 (Egress Zone) （续）																																

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

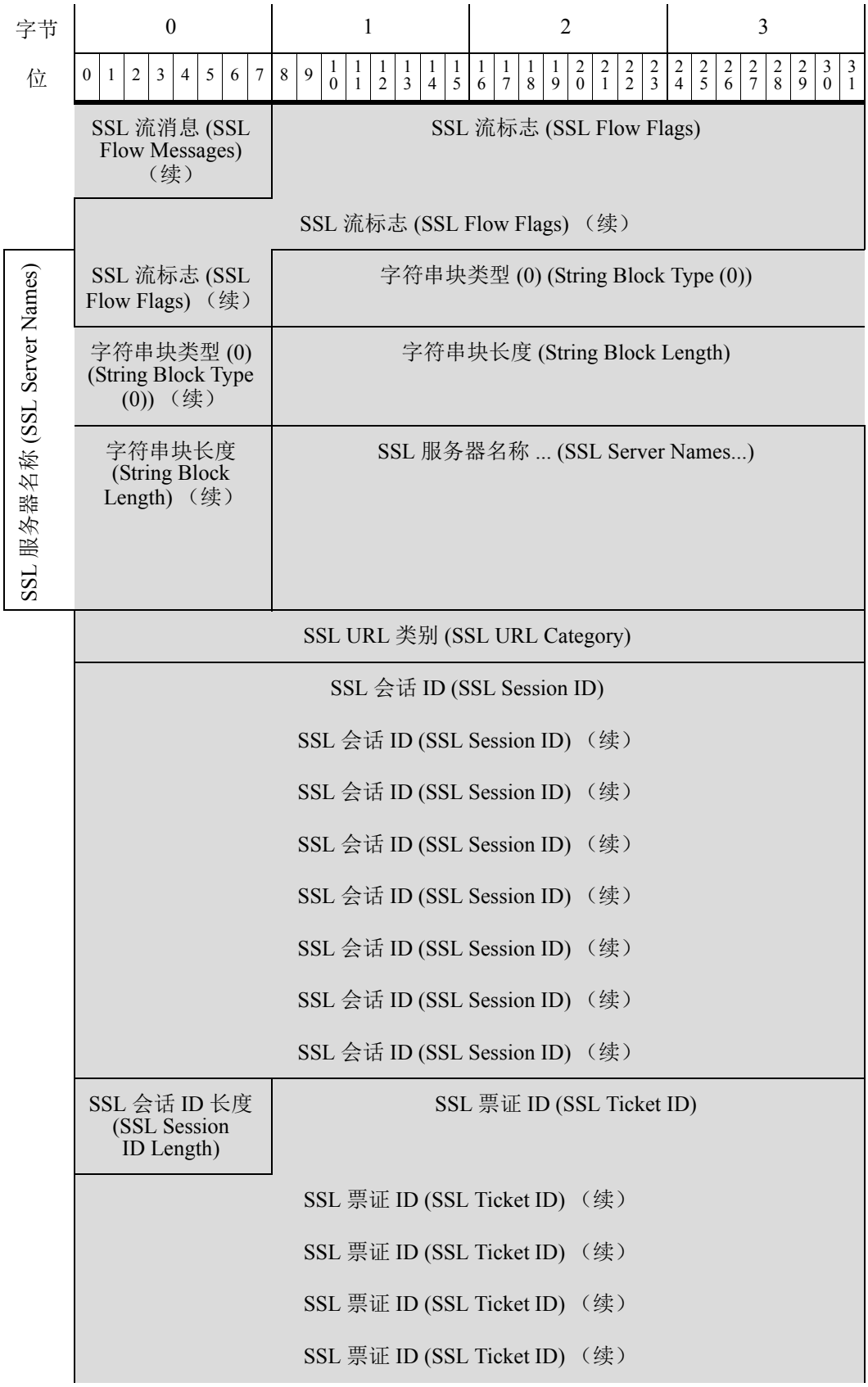

字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
策略修订 (Policy Revision) （续）
策略修订 (Policy Revision) （续）
规则 ID (Rule ID)
隧道规则 ID (Tunnel Rule ID)
规则操作 (Rule Action)
规则原因 (Rule Reason)
规则原因 (Rule Reason) （续）
发起方端口 (Initiator Port)
响应方端口 (Responder Port)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

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

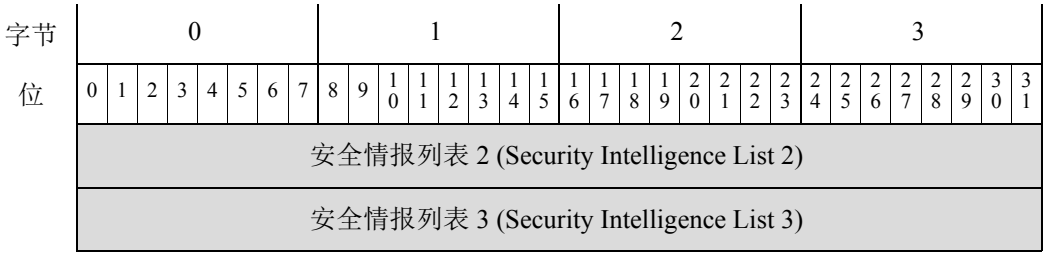
字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	客户端应用 ID (Client App ID)（续）								Web 应用 ID (Web Application ID)																							
客户端 URL	Web 应用 ID (Web App. ID)（续）								字符串块类型 (0) (Str. Block Type (0))																							
	字符串块类型（续）								字符串块长度 (String Block Length)																							
	字符串块长度（续）								客户端应用 URL... (Client App. URL...)																							
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	NetBIOS 名称 ...(NetBIOS Name...)																															
客户端应用版本 (Client App Version)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用版本 ...(Client Application Version...)																															
	监控器规则 1 (Monitor Rule 1)																															
	监控器规则 2 (Monitor Rule 2)																															
	监控器规则 3 (Monitor Rule 3)																															
	监控器规则 4 (Monitor Rule 4)																															
	监控器规则 5 (Monitor Rule 5)																															
	监控器规则 6 (Monitor Rule 6)																															
	监控器规则 7 (Monitor Rule 7)																															
	监控器规则 8 (Monitor Rule 8)																															
	安全接口源 / 目标 (Sec. Int. Src/Dst)								安全接口层 (Sec. Int. Layer)								文件事件计数 (File Event Count)															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	入侵事件计数 (Intrusion Event Count)																发起方国家 / 地区 (Initiator Country)															
	响应方国家 / 地区 (Responder Country)																原始客户端国家 / 地区 (Original Client Country)															
	IOC 编号 (IOC Number)																源自治系统 (Source Autonomous System)															
	源自治系统 (Source Autonomous System) （续）																目标自治系统 (Destination Autonomous System)															
	目标自治系统 (Destination Autonomous System)																SNMP 输入 (SNMP In)															
	SNMP 输出 (SNMP Out)																源 TOS (Source TOS)								目标 TOS (Destination TOS)							
	源掩码 (Source Mask)								目标掩码 (Destination Mask)								安全情景 (Security Context)															
	安全情景 (Security Context)																															
	安全情景 (Security Context) （续）																															
	安全情景 (Security Context) （续）																															
	安全情景 (Security Context) （续）																VLAN ID															
引用的主机 (Referenced Host)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	引用的主机 (Referenced Host)...(Referenced Host...)																															
用户代理	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户代理 ... (User Agent...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 引用站点 (HTTP Referrer)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	HTTP 引用站点 ...(HTTP Referrer...)																															
	SSL 证书指纹 (SSL Certificate Fingerprint)																															
	SSL 证书指纹 (SSL Certificate Fingerprint) （续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint) （续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint) （续）																															
	SSL 证书指纹 (SSL Certificate Fingerprint) （续）																															
	SSL 策略 ID (SSL Policy ID)																															
	SSL 策略 ID (SSL Policy ID) （续）																															
	SSL 策略 ID (SSL Policy ID) （续）																															
	SSL 策略 ID (SSL Policy ID) （续）																															
	SSL 规则 ID (SSL Rule ID)																															
	SSL 密码套件 (SSL Cipher Suite)																SSL 版本 (SSL Version)								SSL 服务器证书统计信息 (SSL Srv Cert. Stat.)							
	SSL 服务器证书统计信息 (SSL Srv Cert. Stat.) （续）																								SSL 实际操作 (SSL Actual Action)							
	SSL 实际操作 (SSL Actual Action) （续）								SSL 预期操作 (SSL Expected Action)																SSL 流状态 (SSL Flow Status)							
	SSL 流状态 (SSL Flow Status) （续）								SSL 流误差 (SSL Flow Error)																								
	SSL 流误差 (SSL Flow Error) （续）								SSL 流消息 (SSL Flow Messages)																								


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 流消息 (SSL Flow Messages) （续）
SSL 流标志 (SSL Flow Flags)
SSL 流标志 (SSL Flow Flags) （续）
SSL 服务器名称 (SSL Server Names)
SSL 流标志 (SSL Flow Flags) （续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
SSL 服务器名称 ... (SSL Server Names...)
SSL URL 类别 (SSL URL Category)
SSL 会话 ID (SSL Session ID)
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID (SSL Session ID) （续）
SSL 会话 ID 长度 (SSL Session ID Length)
SSL 票证 ID (SSL Ticket ID)
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID (SSL Ticket ID) （续）


字节
0
1
2
3
位
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
SSL 票证 ID (SSL Ticket ID) （续）
SSL 票证 ID 长度 (SSL Ticket ID Length)
网络分析策略修订 (Network Analysis Policy Revision)
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）
网络分析策略修订 (Network Analysis Policy Revision) （续）
终端配置文件 ID (Endpoint Profile ID)
终端配置文件 ID (Endpoint Profile ID) （续）
安全组 ID (Security Group ID)
安全组 ID (Security Group ID) （续）
位置 IPv6 (Location IPv6)
位置 IPv6 (Location IPv6) （续）
位置 IPv6 (Location IPv6) （续）
位置 IPv6 (Location IPv6) （续）
位置 IPv6 (Location IPv6) （续）
HTTP 响应 (HTTP Response)
DNS 查询
HTTP 响应 (HTTP Response) （续）
字符串块类型 (0) (String Block Type (0))
字符串块类型 (0) (String Block Type (0)) （续）
字符串块长度 (String Block Length)
字符串块长度 (String Block Length) （续）
DNS 查询 ...(DNS Query...)
DNS 记录类型 (DNS Record Type)
DNS 响应类型 (DNS Response Type)
DNS TTL
Sinkhole UUID
Sinkhole UUID （续）
Sinkhole UUID （续）
Sinkhole UUID （续）
安全情报列表 1 (Security Intelligence List 1)



下表对用于 6.2+ 的连接统计信息数据块的字段进行了说明。

表 4-71　连接统计信息数据块 6.2+ 字段

字段	数据类型	说明
连接统计信息数据块类型 (Connection Statistics Data Block Type)	uint32	启动用于 6.2+ 的连接统计信息数据块。值始终为 168。
连接统计信息数据块长度 (Connection Statistics Data Block Length)	uint32	连接统计信息数据块中的字节数，包括连接统计信息块类型和长度字段的八个字节，加上随后的连接数据中的字节数。
设备 ID (Device ID)	uint32	检测到连接事件的设备。
入口区 (Ingress Zone)	uint8[16]	触发策略违规的事件的入口安全区。
出口区 (Egress Zone)	uint8[16]	触发策略违规的事件的出口安全区。
入口接口 (Ingress Interface)	uint8[16]	用于入站流量的接口。
出口接口 (Egress Interface)	uint8[16]	用于出站流量的接口。
发起方 IP 地址 (Initiator IP Address)	uint8[16]	发起连接事件中描述的会话的主机的 IP 地址，采用 IP 地址八位组。
响应方 IP 地址 (Responder IP Address)	uint8[16]	响应发起主机的主机的 IP 地址，采用 IP 地址八位组。
原始客户端 IP 地址 (Original Client IP Address)	uint8[16]	位于发起请求的代理后面的主机的 IP 地址，采用 IP 地址八位组。
策略修订 (Policy Revision)	uint8[16]	与触发的关联事件相关的规则版本号 （如适用）。
规则 ID (Rule ID)	uint32	触发事件的规则的内部标识符 （如适用）。

表 4-71　连接统计信息数据块 6.2+ 字段 （续）

字段	数据类型	说明
隧道规则 ID (Tunnel Rule ID)	uint32	触发事件的隧道规则的内部标识符 （如适用）。
规则操作 (Rule Action)	uint16	在用户界面中选择的针对该规则的操作 （允许、阻止等）。
规则原因 (Rule Reason)	uint32	规则触发事件的原因。
发起方端口 (Initiator Port)	uint16	发起主机使用的端口。
响应方端口 (Responder Port)	uint16	响应主机使用的端口。
TCP 标志 (TCP Flags)	uint16	表示连接事件的任何 TCP 标志。
协议 (Protocol)	uint8	IANA 指定的协议号。
NetFlow 源 (NetFlow Source)	uint8[16]	导出连接数据的支持 NetFlow 的设备的 IP 地址。
实例 ID (Instance ID)	uint16	生成事件的受管设备上 Snort 实例的数字 ID。
连接计数器 (Connection Counter)	uint16	用于区别同一秒发生的连接事件的值。
第一个数据包时间戳 (First Packet Timestamp)	uint32	在会话中交换第一个数据包的日期和时间的 UNIX 时间戳。
最后一个数据包时间戳 (Last Packet Timestamp)	uint32	在会话中交换最后一个数据包的日期和时间的 UNIX 时间戳。
发起方传输的数据包数 (Initiator Transmitted Packets)	uint64	发起主机传输的数据包数。
响应方传输的数据包数 (Responder Transmitted Packets)	uint64	响应主机传输的数据包数。
发起方传输的字节数 (Initiator Transmitted Bytes)	uint64	发起主机传输的字节数。
响应方传输的字节数 (Responder Transmitted Bytes)	uint64	响应主机传输的字节数。

表 4-71　连接统计信息数据块 6.2+ 字段 （续）

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

表 4-71　连接统计信息数据块 6.2+ 字段 （续）

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

表 4-71　连接统计信息数据块 6.2+ 字段 （续）

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

表 4-71　连接统计信息数据块 6.2+ 字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	引用的主机字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 引用的主机 ”(Referenced Host) 字段中的字节数。
引用的主机 (Referenced Host)	字符串	HTTP 或 DNS 中提供的主机名信息。
字符串块类型 (String Block Type)	uint32	启动包含用户代理的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户代理字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户代理 ”(User Agent) 字段中的字节数。
用户代理 (User Agent)	字符串	会话中用户代理报头字段中的信息。
字符串块类型 (String Block Type)	uint32	启动包含 HTTP 引用站点的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	HTTP 引用站点字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “HTTP 引用站点 ”(HTTP Referrer) 字段中的字节数。
HTTP 引用站点 (HTTP Referrer)	字符串	页面起源的站点。该站点可在 HTTP 流量中引用的报头信息中找到。
SSL 证书指纹 (SSL Certificate Fingerprint)	uint8[20]	SSL 服务器证书的 SHA1 散列。
SSL 策略 ID (SSL Policy ID)	uint8[16]	处理连接的 SSL 策略的 ID 编号。
SSL 规则 ID (SSL Rule ID)	uint32	处理连接的 SSL 规则或默认操作的 ID 编号。
SSL 密码套件 (SSL Cipher Suite)	uint16	SSL 连接使用的加密套件。该值以十进制格式存储。有关该值指定的密码套件，请参阅 www.iana.org/assignments/tls-parameters/tls-parameters.xhtml。
SSL 版本 (SSL Version)	uint8	用来加密连接的 SSL 或 TLS 协议版本。

表 4-71　　连接统计信息数据块 6.2+ 字段 （续）

字段	数据类型	说明
SSL 服务器证书状态 (SSL Server Certificate Status)	uint32	SSL 证书的状态。可能的值包括： • 0 - 未检查 - 服务器证书状态未评估。 • 1 - 未知 - 服务器证书状态无法确定。 • 2 - 有效 - 服务器证书有效。 • 4 - 自签 - 服务器证书已自签。 • 16 - 颁发者无效 - 服务器证书的颁发者无效。 • 32 - 签名无效 - 服务器证书的签名无效。 • 64 - 过期 - 服务器证书已过期。 • 128 - 尚未生效 - 服务器证书尚未生效。 • 256 - 撤销 - 服务器证书已被撤销。
SSL 实际操作 (SSL Actual Action)	uint16	根据 SSL 规则对连接执行的操作。由于规则中指定的操作可能无法执行，此操作可能与预期操作不同。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’
SSL 预期操作 (SSL Expected Action)	uint16	根据 SSL 规则应该对连接执行的操作。可能的值包括： • 0 -‘ 未知 ’ • 1 -‘ 请勿解密 ’ • 2 -‘ 阻止 ’ • 3 -‘ 阻止并重置 ’ • 4 -‘ 解密 （已知密钥） ’ • 5 -‘ 解密 （更换秘钥） ’ • 6 -‘ 解密 （放弃） ’

表 4-71　连接统计信息数据块 6.2+ 字段 （续）

字段	数据类型	说明
SSL 流状态 (SSL Flow Status)	uint16	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 流误差 (SSL Flow Error)	uint32	详细的 SSL 错误代码。这些值可用于提供支持。

表 4-71　连接统计信息数据块 6.2+ 字段 （续）

字段	数据类型	说明
SSL 流消息 (SSL Flow Messages)	uint32	在 SSL 握手期间，客户端和服务器之间交换的消息。有关详细信息，请参阅 http://tools.ietf.org/html/rfc5246。 • 0x00000001 - NSE_MT__HELLO_REQUEST • 0x00000002 - NSE_MT__CLIENT_ALERT • 0x00000004 - NSE_MT__SERVER_ALERT • 0x00000008 - NSE_MT__CLIENT_HELLO • 0x00000010 - NSE_MT__SERVER_HELLO • 0x00000020 - NSE_MT__SERVER_CERTIFICATE • 0x00000040 - NSE_MT__SERVER_KEY_EXCHANGE • 0x00000080 - NSE_MT__CERTIFICATE_REQUEST • 0x00000100 - NSE_MT__SERVER_HELLO_DONE • 0x00000200 - NSE_MT__CLIENT_CERTIFICATE • 0x00000400 - NSE_MT__CLIENT_KEY_EXCHANGE • 0x00000800 - NSE_MT__CERTIFICATE_VERIFY • 0x00001000 - NSE_MT__CLIENT_CHANGE_CIPHER_SPEC • 0x00002000 - NSE_MT__CLIENT_FINISHED • 0x00004000 - NSE_MT__SERVER_CHANGE_CIPHER_SPEC • 0x00008000 - NSE_MT__SERVER_FINISHED • 0x00010000 - NSE_MT__NEW_SESSION_TICKET • 0x00020000 - NSE_MT__HANDSHAKE_OTHER • 0x00040000 - NSE_MT__APP_DATA_FROM_CLIENT • 0x00080000 - NSE_MT__APP_DATA_FROM_SERVER
SSL 流标志 (SSL Flow Flags)	uint64	加密连接的调试级别标志。可能的值包括： • 0x00000001 - NSE_FLOW__VALID - 必须设置此字段，其他字段才有效 • 0x00000002 - NSE_FLOW__INITIALIZED - 内部结构已准备就绪进行处理 • 0x00000004 - NSE_FLOW__INTERCEPT - SSL 会话已被拦截
字符串块类型 (String Block Type)	uint32	启动包含 SSL 服务器名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	SSL 服务器名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “SSL 服务器名称 ”(SSL Server Name) 字段中的字节数。

表 4-71　连接统计信息数据块 6.2+ 字段 （续）

字段	数据类型	说明
SSL 服务器名称 (SSL Server Name)	字符串	在 SSL 客户端欢迎界面中服务器名称显示中提供的名称。
SSL URL 类别 (SSL URL Category)	uint32	根据服务器名称和证书常用名识别的流量类别。
SSL 会话 ID (SSL Session ID)	uint8[32]	当客户端和服务器同意进行会话重用时， SSL 握手期间使用的会话 ID 值
SSL 会话 ID 长度 (SSL Session ID Length)	uint8	SSL 会话 ID 的长度。尽管会话 ID 不能超过 32 个字节，此值可能小于 32 个字节。
SSL 票证 ID (SSL Ticket ID)	uint8[20]	当客户端和服务器同意使用会话票证时使用的会话票证散列。
SSL 票证 ID 长度 (SSL Ticket ID Length)	uint8	SSL 票证 ID 的长度。尽管票证 ID 不能超过 20 个字节，此值可能小于 20 个字节。
网络分析策略修订 (Network Analysis Policy Revision)	uint8[16]	与连接事件相关的网络分析策略的修订。
终端配置文件 ID (Endpoint Profile ID)	uint32	ISE 识别的连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	由 ISE 根据策略分配给用户的 ID 号码。
位置 IPv6 (Location IPv6)	uint8[16]	与 ISE 通信的接口的 IP 地址。可以是 IPv4 或 IPv6。
HTTP 响应 (HTTP Response)	uint32	HTTP 请求的响应代码。
字符串块类型 (String Block Type)	uint32	启动 DNS 查询的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 DNS 查询字符串中的字节数。
DNS 查询 (DNS Query)	字符串	发送到 DNS 服务器的查询的内容。
DNS 记录类型 (DNS Record Type)	uint16	DNS 记录类型的数字值。
DNS 响应类型 (DNS Response Type)	uint16	DNS 响应类型的数字值。

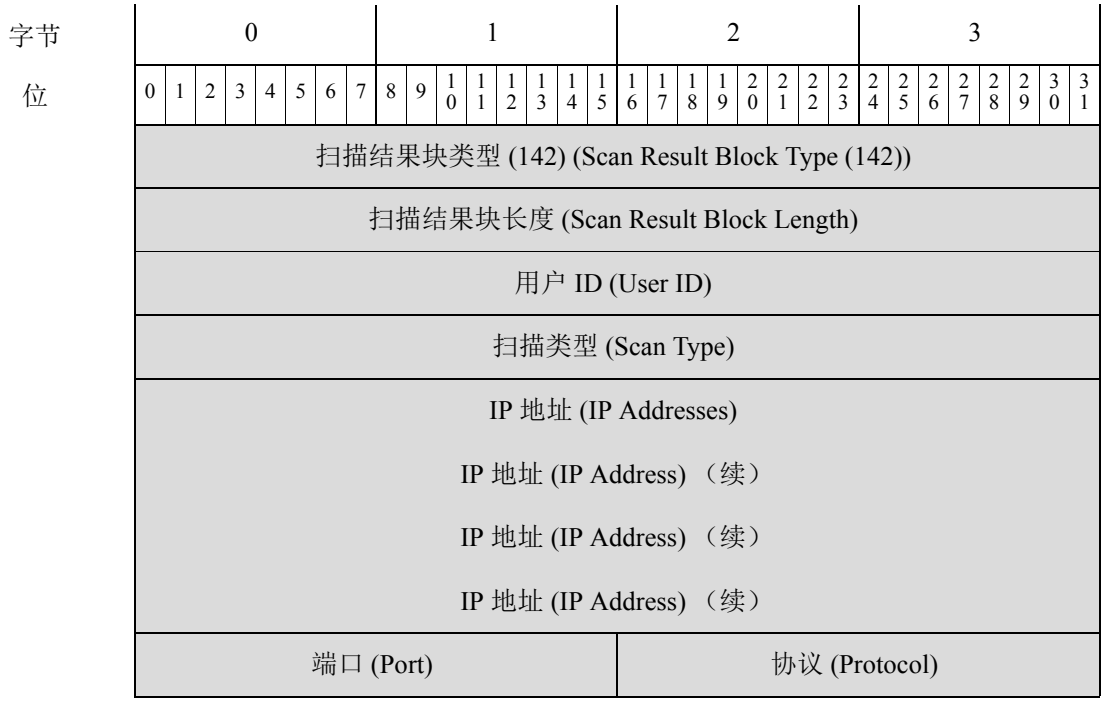
表 4-71　　连接统计信息数据块 6.2+ 字段 （续）

字段	数据类型	说明
DNS TTL	uint32	DNS 响应的生存时间 （秒数）
Sinkhole UUID	uin8[16]	与此 sinkhole 对象关联的修订 UUID。
安全情报列表 1 (Security Intelligence List 1)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能有三个与连接关联的安全情报列表。
安全情报列表 2 (Security Intelligence List 2)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能有三个与连接关联的安全情报列表。
安全情报列表 3 (Security Intelligence List 3)	uint32	与事件关联的安全情报列表。这映射到关联元数据中的安全情报列表。可能有三个与连接关联的安全情报列表。

扫描结果数据块 5.2+

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

下图显示扫描结果数据块的格式：



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

下表对扫描结果数据块的字段进行了说明。

表 4-72　　扫描结果数据块字段

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

表 4-72　　扫描结果数据块字段 （续）

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

表 4-72　扫描结果数据块字段 （续）

字段	数据类型	说明
一般扫描结果数据 (Generic Scan Results Data)	字符串	每个扫描结果的相关信息。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送第三方应用中的主机输入数据的用户产品数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装用户产品数据块。
用户产品数据块 (User Product Data Blocks) *	变量	包含主机输入数据的用户产品数据块。有关此数据块的说明，请参阅用户产品数据块 5.1+，第 4-176 页。

主机服务器数据块 4.10.0+

主机服务器数据块传输在主机上检测到的服务器的相关信息。它包含每个检测到的服务器的块，且包含服务器运行的 Web 应用的 Web 应用数据块列表。新 TCP 和 UDP 服务器和更改 TCP 和 UDP 服务器的消息中包含主机服务器数据块。有关详细信息，请参阅服务器消息，第 4-46 页。主机服务器数据块的块类型为系列 1 数据块组中的 103。

注　下图中数据块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示主机服务器数据块的格式：

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

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

下表对主机服务器数据块的字段进行了说明。

表 4-73　　主机服务器数据块字段

字段	数据类型	说明
主机服务器块类型 (Host Server Block Type)	uint32	启动主机服务器数据块。值始终为 103。
主机服务器块长度 (Host Server Block Length)	uint32	主机服务器数据块中的字节总数，包括主机服务器块类型和长度字段的八个字节，加上随后的数据的字节数。
端口 (Port)	uint16	服务器在其上运行的端口的端口号。
命中数 (Hits)	uint32	服务器接收的命中数。
上次使用时间 (Last Used)	uint32	表示系统上次检测到使用中的服务器的 UNIX 时间戳。
通用列表块类型 (Generic List Block Type)	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装子服务器信息数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。

表 4-73　主机服务器数据块字段 （续）

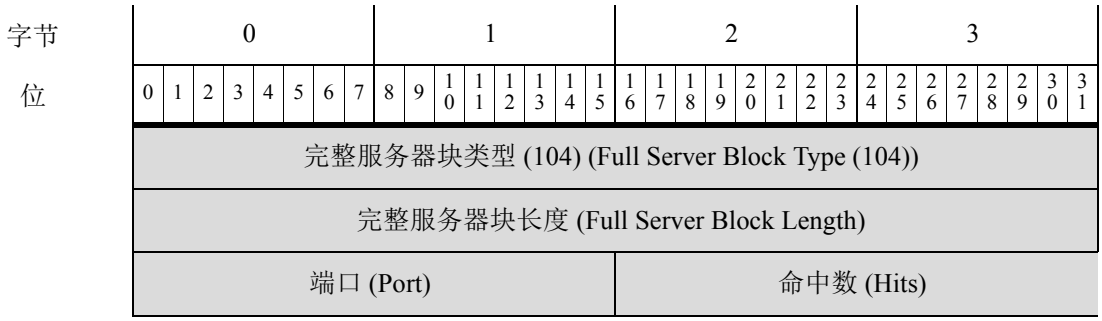
字段	数据类型	说明
服务器信息数据块 (Server Information Data Blocks)*	变量	服务器信息数据块数最多可以是列表块长度中的最大字节数。有关详细信息，请参阅用于 4.10.x、 5.0 - 5.0.2 的服务器信息数据块，第 4-147 页。
置信 (Confidence)	uint32	置信度百分比。
通用列表块类型 (Generic List Block Type)	uint32	启动通用数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用块和封装 Web 应用数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装 Web 应用数据块中的字节数。
Web 应用数据块 (Client Application Data Blocks)*	变量	封装 Web 应用数据块数最多可以是列表块长度中的最大字节数。有关详细信息，请参阅用于 5.0+ 的 Web 应用数据块，第 4-118 页。

完整主机服务器数据块 4.10.0+

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

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

下图显示完整服务器数据块的格式：



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

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
第三方主机漏洞	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	（第三方）主机漏洞数据块 (85) ((Third Party) Host Vulnerability Data Blocks (85))*																															
Web 应用	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	Web 应用数据 (123) (Web Application Data (123))*																															

下表对完整服务器数据块的组件进行了说明。

表 4-74　　完整服务器数据块 4.10.0+ 字段

字段	数据类型	说明
完整服务器块类型 (Full Server Block Type)	uint32	启动完整服务器数据块。值始终为 104。
完整服务器块长度 (Full Server Block Length)	uint32	完整服务器数据块中的字节总数，包括完整服务器块类型和长度字段的八个字节，加上随后的完整服务器数据的字节数。
端口 (Port)	uint16	服务器端口号。
命中数 (Hits)	uint32	服务器接收的命中数。
通用列表块类型 (Generic List Block Type)	uint32	启动由检测到的子服务器数据的数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装子服务器信息数据块。
子服务器信息 - 思科数据块 (Sub-Server Information - Cisco Data Blocks) *	变量	包含 Cisco 检测到的主机服务器的子服务器的相关信息的完整主机信息数据块。有关此数据块的说明，请参阅完整服务器信息数据块，第 4-150 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用户添加的子服务器数据的子服务器信息数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装服务器信息数据块。

表 4-74　完整服务器数据块 4.10.0+ 字段 （续）

字段	数据类型	说明
子服务器信息 - 用户添加数据块 (Sub-Server Information- User Added Data Blocks) *	变量	包含用户添加的主机上的子服务器的相关信息的完整主机信息数据块。有关此数据块的说明，请参阅完整服务器信息数据块，第 4-150 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送扫描仪添加的子服务器数据的子服务器信息数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装子服务器信息数据块。
子服务器信息 - 扫描添加数据块 (Sub-Server Information- Scan Added Data Blocks) *	变量	包含扫描仪所添加主机上子服务器的相关信息的完整信息数据块。有关此数据块的说明，请参阅完整服务器信息数据块，第 4-150 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送应用添加的子服务器数据的子服务器信息数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装子服务器信息数据块。
子服务器信息 - 应用添加数据块 (Sub-Server Information - Application Added Data Blocks) *	变量	包含应用添加的主机上的子服务器的相关信息的完整主机信息数据块。有关此数据块的说明，请参阅完整服务器信息数据块，第 4-150 页。
置信 (Confidence)	uint32	Cisco 在正确识别完整服务器数据方面的置信度百分比。
BLOB 块类型 (BLOB Block Type)	uint32	启动包含横幅数据的 BLOB 数据块。值始终为 10。
BLOB 块长度 (BLOB Block Length)	uint32	BLOB 数据块中的字节总数，包括块类型和长度字段的八个字节，加上横幅中的字节数。
服务器横幅数据 (Server Banner Data)	字节 [*n*]	服务器事件中涉及的数据包的前 *n* 个字节，其中 *n* 小于或等于 256。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 Cisco 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装主机漏洞数据块。
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks) *	变量	包含漏洞数据库 (VDB) 中主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。

表 4-74　完整服务器数据块 4.10.0+ 字段 （续）

字段	数据类型	说明
通用列表块类型 (Generic List Block Type)	uint32	启动由主机漏洞数据块组成的通用列表数据块，这些主机漏洞数据块传输源自第三方扫描仪的第三方主机漏洞数据，并且包含已收录到 VDB 的漏洞信息。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装主机漏洞数据块。
（第三方 /VDB）主机漏洞数据块 ((Third Party/VDB) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪且包含已收录到漏洞数据库 (VDB) 中的主机漏洞相关信息的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传输第三方扫描仪生成的第三方主机漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装主机漏洞数据块。
第三方扫描主机漏洞数据块 (Third Party Scan Host Vulnerability Data Blocks) *	变量	包含第三方扫描仪识别但未收录到 VDB 中的漏洞的第三方漏洞数据的主机漏洞数据块。有关此数据块的说明，请参阅主机漏洞数据块 4.9.0+，第 4-114 页。
通用列表块类型 (Generic List Block Type)	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装 Web 应用数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
Web 应用数据块 (Client Application Data Blocks)*	变量	封装 Web 应用数据块数最多可以是列表块长度中的最大字节数。

用于 4.10.x、 5.0 - 5.0.2 的服务器信息数据块

服务器信息数据块传输服务器的相关信息，包括服务器 ID、服务器供应商和版本以及源信息。在 4.10.x 中，服务器信息数据块的块类型为系列 1 数据块组中的 105，在 5.0 - 5.0.2 中，块类型为系列 1 数据块组中的 117。服务器信息数据块在主机服务器块和完整主机服务器数据块中的列表中传输。有关详细信息，请参阅主机服务器数据块 4.10.0+，第 4-141 页和完整主机服务器数据块 4.10.0+，第 4-143 页。

下图显示服务器信息数据块的格式：

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

下表对服务器信息数据块的组件进行了说明。

表 4-75　服务器信息数据块字段

字段	数据类型	说明
服务器信息块类型 (Server Information Block Type)	uint32	启动服务器信息数据块。在 4.10.x 中，块类型为 105，在 5.0+ 中，块类型为 117。
服务器信息块长度 (Server Information Block Length)	uint32	服务器信息数据块中的字节总数，包括服务器信息块类型和长度字段的八个字节，服务器 ID 的四个字节，供应商名称块类型和长度的八个字节，供应商名称的另外四个字节，版本字符串块类型和长度的八个字节，版本字符串的另外四个字节，以及上次使用时间、源类型以及源 ID 字段的各四个字节。
应用 ID (Application ID)	uint32	在检测到的服务器上运行的应用协议的应用 ID。
字符串块类型 (String Block Type)	uint32	启动包含服务器供应商名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	供应商名称字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上服务器供应商名称中的字节数。
服务器供应商名称 (Server Vendor Name)	字符串	服务器供应商的名称。
字符串块类型 (String Block Type)	uint32	启动包含服务器版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	服务器版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上服务器版本中的字节数。
服务器版本 (Server Version)	字符串	服务器版本。
上次使用时间 (Last Time Used)	uint32	指示上次在流量中使用服务器信息的时间。
源类型 (Source Type)	uint32	映射到数据源类型的数字： • 0 如果服务器数据由 RNA 提供 • 1 如果服务器数据由用户提供 • 2 如果服务器数据由第三方扫描仪提供 • 3 如果服务器数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
源 ID (Source ID)	uint32	映射到服务器数据源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
列表块类型 (List Block Type)	uint32	启动子服务器数据块列表。值始终为 11。
列表块长度 (List Block Length)	uint32	列表数据块中的字节数，包括列表块类型和长度字段的八个字节，加上随后的封装子服务器数据块中的字节数。

表 4-75　服务器信息数据块字段 （续）

字段	数据类型	说明
子服务器块类型 (Sub-Server Block Type)	uint32	启动第一个子服务器数据块。此数据块后面可以跟随最大长度为列表块长度字段中定义的限值的其他子服务器数据块。
子服务器块长度 (Sub-Server Block Length)	uint32	每个子服务器数据块中的字节总数，包括子服务器块类型和长度字段的八个字节，加上随后的数据的字节数。
子服务器数据 (Sub-Server Data)	变量	子服务器数据，如子服务器数据块，第 4-73 页中所记录。

完整服务器信息数据块

完整服务器信息数据块传输在主机上检测到的服务器的相关信息，包括服务器的应用协议、供应商和版本及其关联子服务器的列表。对于每个子服务器，完整子服务器数据块包含其信息（请参阅完整子服务器数据块，第 4-83 页）。完整服务器信息数据块的块类型为系列 1 数据块组中的 106。

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

下图显示完整服务器信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	完整服务器块类型 (106) (Full Server Block Type (106))																															
	完整服务器块长度 (Full Server Block Length)																															
	应用协议 ID (Application Protocol ID)																															
供应商	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	供应商名称字符串 ...(Vendor Name String...)																															
版本	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	版本字符串 ...(Version String...)																															
	上次使用时间 (Last Used)																															
	源类型 (Source Type)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	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 ID (Source ID)																															
	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
子服务器 (Sub-Servers)	完整子服务器块类型 (51) (Full Sub-Server Block Type (51)) *																															
	完整子服务器块长度 (Full Sub-Server Block Length)																															
	完整子服务器数据 ...(Full Sub-Server Data...)																															

下表对完整服务器信息数据块的组件进行了说明。

表 4-76　　完整服务器信息数据块字段

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

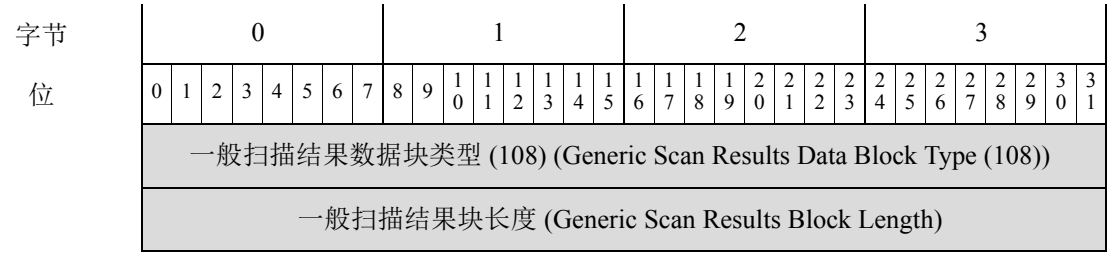
表 4-76　完整服务器信息数据块字段 （续）

字段	数据类型	说明
上次使用时间 (Last Used)	uint32	表示系统上次检测到使用中的服务器的 UNIX 时间戳。
源类型 (Source Type)	uint32	映射到数据源类型的数字： • 0 如果服务器数据由 RNA 提供 • 1 如果服务器数据由用户提供 • 2 如果客户端数据由第三方扫描仪提供 • 3 如果服务器数据由命令行工具（如 nmimport.pl）或主机输入 API 客户端提供
源 ID (Source ID)	uint32	映射到服务器数据源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
列表块类型 (List Block Type)	uint32	启动由传输子服务器数据的完整服务器信息数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装完整子服务器数据块。 此字段后面是零个或多个完整子服务器数据块。
完整子服务器块类型 (Full Sub-Server Block Type)	uint32	启动第一个完整子服务器数据块。此数据块后面可以跟随最大长度为列表块长度字段中定义的限值的其他完整子服务器数据块。
完整子服务器块长度 (Full Sub-Server Block Length)	uint32	每个完整子服务器数据块中的字节总数，包括完整子服务器块类型和长度字段的八个字节，加上随后的数据的字节数。
完整子服务器数据块 (Full Sub-Server Data Blocks) *	uint32	包含服务器的子服务器的完整子服务器数据块。有关此数据块的说明，请参阅完整子服务器数据块，第 4-83 页。

用于 4.10.0+ 的一般扫描结果数据块

一般扫描结果数据块包含扫描结果，并在扫描结果数据块 5.2+，第 4-138 页中使用。一般扫描结果数据块的块类型为系列 1 数据块组中的 108。

下图显示一般扫描结果数据块的基本结构：



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

下表对一般扫描结果数据块的字段进行了说明。

表 4-77　　一般扫描结果数据块字段

字段	字节数	说明
一般扫描结果数据块类型 (Generic Scan Results Data Block Type)	uint32	启动一般扫描结果数据块。值始终为 `108`。
一般扫描结果块长度 (Generic Scan Results Block Length)	uint32	一般扫描结果数据块中的字节总数，包括一般扫描结果块类型和长度字段的八个字节，加上随后的扫描结果数据的字节数。
端口 (Port)	uint16	受结果中的漏洞影响的服务器使用的端口。

表 4-77　　一般扫描结果数据块字段 （续）

字段	字节数	说明
协议 (Protocol)	uint16	IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如： • 6 - TCP • 17 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如： • 2048 - IP
字符串块类型 (String Block Type)	uint32	启动包含子服务器的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	子服务器字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上子服务器中的字节数。
扫描结果子服务器 (Scan Result Sub-Server)	字符串	子服务器。
字符串块类型 (String Block Type)	uint32	启动包含该值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	值字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上值中的字节数。
扫描结果值 (Scan Result Value)	字符串	扫描结果值。
字符串块类型 (String Block Type)	uint32	启动包含子服务器的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	子服务器字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上子服务器中的字节数。
扫描结果子服务器 (Scan Result Sub-Server)	字符串	子服务器 （未格式化）。
字符串块类型 (String Block Type)	uint32	启动包含该值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	值字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上值中的字节数。
扫描结果值 (Scan Result Value)	字符串	扫描结果值 （未格式化）。

用于 4.10.0+ 的扫描漏洞数据块

扫描漏洞数据块对漏洞进行说明，在扫描结果数据块中使用，扫描结果数据块在添加扫描结果事件 （事件类型 1002，子类型 11）中使用。有关详细信息，请参阅扫描结果数据块 5.2+，第 4-138 页和添加扫描结果消息，第 4-60 页。扫描漏洞数据块的块类型为系列 1 数据块组中的 109。

下图显示扫描漏洞数据块的格式：

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

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

下表对扫描漏洞数据块的字段进行了说明。

表 4-78　　扫描漏洞数据块字段

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

表 4-78　扫描漏洞数据块字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动漏洞名称的字符串数据块。
字符串块长度 (String Block Length)	uint32	漏洞名称字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上漏洞名称中的字节数。
名称 (Name)	字符串	漏洞的名称。
字符串块类型 (String Block Type)	uint32	启动漏洞说明的字符串数据块。
字符串块长度 (String Block Length)	uint32	漏洞说明字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上漏洞说明中的字节数。
说明 (Description)	字符串	对漏洞的说明。
字符串块类型 (String Block Type)	uint32	启动漏洞名称的字符串数据块。
字符串块长度 (String Block Length)	uint32	漏洞名称字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上漏洞名称中的字节数。
名称清除 (Name Clean)	字符串	漏洞的名称 （未格式化）。
字符串块类型 (String Block Type)	uint32	启动漏洞说明的字符串数据块。
字符串块长度 (String Block Length)	uint32	漏洞说明字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上漏洞说明中的字节数。
说明清除 (Description Clean)	字符串	对漏洞的说明 （未格式化）。
列表块类型 (List Block Type)	uint32	启动 Bugtraq 标识号列表的列表数据块。
列表块长度 (List Block Length)	uint32	Bugtraq 标识号列表的列表数据块中的字节数，包括字符串块类型和长度的八个字节，加上包含 Bugtraq ID 的整数数据块中的字节数。
Bugtraq ID	字符串	包含零个或多个形成 Bugtraq 标识号列表的整数 (INT32) 数据块。有关这些数据块的详细信息，请参阅整数 (INT32) 数据块，第 4-75 页。
列表块类型 (List Block Type)	uint32	启动通用漏洞披露 (CVE) 标识号列表的列表数据块。

表 4-78　扫描漏洞数据块字段 （续）

字段	数据类型	说明
列表块长度 (List Block Length)	uint32	CVE 标识号的列表数据块中的字节数，包括字符串块类型和长度的八个字节，加上 CVE 标识号中的字节数。
CVE ID	字符串	包含零个或多个形成 CVE 标识号列表的字符串信息数据块。有关这些数据块的详细信息，请参阅字符串信息数据块，第 4-78 页。

完整主机客户端应用数据块 5.0+

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

下图显示用于 5.0+ 的完整主机客户端应用数据块的基本结构：

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

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

下表对完整主机客户端应用数据块的字段进行了说明。

表 4-79　　完整主机客户端应用数据块 5.0+ 字段

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

表 4-79　完整主机客户端应用数据块 5.0+ 字段 （续）

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

用于 5.0+ 的主机客户端应用数据块

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

下图显示用于 5.0+ 的主机客户端应用数据块的基本结构：

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

下表对主机客户端应用数据块的字段进行了说明。

表 4-80　主机客户端应用数据块字段

字段	数据类型	说明
客户端应用块类型 (Client Application Block Type)	uint32	启动主机客户端应用数据块。值始终为 122。
客户端应用块长度 (Client Application Block Length)	uint32	客户端应用数据块中的字节数，包括客户端应用块类型和长度的八个字节，加上随后的客户端应用数据中的字节数。
命中数 (Hits)	uint32	系统检测到在使用的客户端应用的次数。
上次使用时间 (Last Used)	uint32	表示系统上次检测到使用中的客户端的 UNIX 时间戳。
ID	uint32	被检测客户端应用的标识号 （如适用）。
应用协议 ID (Application Protocol ID)	uint32	应用协议的内部标识号 （如适用）。
字符串块类型 (String Block Type)	uint32	启动客户端应用版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用于客户端应用版本的字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上客户端应用版本中的字节数。
版本 (Version)	字符串	客户端应用版本。
通用列表块类型 (Generic List Block Type)	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装 Web 应用数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
Web 应用数据块 (Web Application Data Blocks)	变量	封装 Web 应用数据块数最多可以是列表块长度中的最大字节数。请参阅用于 5.0+ 的 Web 应用数据块，第 4-118 页了解有关封装数据块的信息 （块类型 123）。

用户漏洞数据块 5.0+

用户漏洞数据块对漏洞进行说明，并在用户漏洞更改数据块中使用。用户漏洞更改数据块在用户设置有效漏洞事件和用户设置无效漏洞事件中使用。用于 5.0+ 的用户漏洞数据块的块类型为系列 1 数据块组中的 124。它替代块类型 79。有关用户漏洞更改数据块的详细信息，请参阅用户漏洞更改数据块 4.7+，第 4-108 页。

下图显示用户漏洞数据块的格式：

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

下表对用户漏洞数据块的字段进行了说明。

表 4-81　用户漏洞数据块字段

字段	数据类型	说明
用户漏洞块类型 (User Vulnerability Block Type)	uint32	启动用户漏洞数据块。值始终为 124。
用户漏洞块长度 (User Vulnerability Block Length)	uint32	用户漏洞数据块中的字节数，包括用户漏洞块类型和长度字段的八个字节，加上随后的用户漏洞数据的字节数。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装 IP 范围规格数据块。
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	用户输入的 IP 地址范围。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-96 页。
端口 (Port)	uint16	受漏洞影响的服务器使用的端口。对于客户端应用漏洞，值为 0。
协议 (Protocol)	uint16	受漏洞影响的服务器使用的协议的 IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如： • 6 - TCP • 17 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如： • 2048 - IP 对于客户端应用漏洞，值为 0。
漏洞 ID (Vulnerability ID)	uint32	Cisco 漏洞 ID。
第三方漏洞 UUID (Third-Party Vulnerability UUID)	uint8 [16]	第三方漏洞的唯一 ID 号码 （如果存在）。否则，该值为 0。
字符串块类型 (String Block Type)	uint32	启动漏洞名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	漏洞名称字符串数据块中的字节数，包括字符串块类型和长度的八个字节，加上漏洞名称中的字节数。

表 4-81　　用户漏洞数据块字段 （续）

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

操作系统指纹数据块 5.1+

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

下图显示 5.1+ 中操作系统指纹数据块的格式：

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

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

下表对操作系统指纹数据块的字段进行了说明。

表 4-82　　操作系统指纹数据块字段

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

表 4-82　操作系统指纹数据块字段 （续）

字段	数据类型	说明
通用列表块类型 (Generic List Block Type)	uint32	启动通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表块和封装数据块中的字节数。此数字包括通用列表块报头字段的八个字节，加上所有封装数据块中的字节数。
移动设备信息数据块 (Mobile 设备 Information Data Blocks)	变量	封装移动设备信息数据块数最多可以是列表块长度中的最大字节数。有关此数据块的说明，请参阅用于 5.1+ 的移动设备 信息数据块，第 4-166 页。

用于 5.1+ 的移动设备 信息数据块

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

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

下表对 5.1+ 返回的移动设备信息数据块的字段进行了说明。

表 4-83　　移动设备信息数据块 5.1+ 字段

字段	数据类型	说明
移动设备信息块类型 (131) (Mobile 设备 Information Block Type (131))	uint32	启动操作系统数据块。值始终为 131。
移动设备信息块长度 (Mobile Device Information Block Length)	uint32	移动设备信息数据块中的字节数，包括移动设备信息数据块块类型和长度的八个字节，加上随后的移动设备信息数据中的字节数。
字符串块类型 (String Block Type)	uint32	启动移动设备字符串的字符串数据块。此值设置为 0 以表示字符串数据。
字符串块长度 (String Block Length)	uint32	移动设备字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上随后的移动设备字符串数据中的字节数。
移动设备字符串数据 (Mobile Device String Data)	变量	包含检测到的主机的移动设备硬件信息。
移动设备上次查看时间 (Mobile 设备 Last Seen)	uint32	包含上次查看移动设备的时间戳。
移动 (Mobile)	uint32	指示主机是否为移动设备的一个真假标志。
Jailbroken	uint32	指示主机是否为已被越狱的移动设备的一个真假标志。

用于 5.2+ 的主机配置文件数据块

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

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

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
主机配置文件块类型 (139) (Host Profile Block Type (139))																																
主机配置文件块长度 (Host Profile Block Length)																																
IP 地址 (IP Addresses)																																
IP 地址 (IP Address) （续）																																
IP 地址 (IP Address) （续）																																
IP 地址 (IP Address) （续）																																

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

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IPv6 DHCP 指纹 (IPv6 DHCP Fingerprints)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	IPv6 DHCP 指纹数据块 (Ipv6 DHCP Fingerprint Data Blocks)*																															
用户代理指纹 (User Agent Fingerprint)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	用户代理指纹数据块 (User Agent Fingerprint Data Blocks)*																															
TCP 服务器块 (TCP Server Block)*	列表块类型 (11) (List Block Type (11))																															TCP 服务器
	列表块长度 (List Block Length)																															
	TCP 服务器数据块 (TCP Server Data Blocks)																															
UDP 服务器块 (UDP Server Block)*	列表块类型 (11) (List Block Type (11))																															UDP 服务器
	列表块长度 (List Block Length)																															
	UDP 服务器数据块 (UDP Server Data Blocks)																															
网络协议块 (Network Protocol Block)*	列表块类型 (11) (List Block Type (11))																															网络协议
	列表块长度 (List Block Length)																															
	网络协议数据块 (Network Protocol Data Blocks)																															
传输协议块 (Transport Protocol Block)*	列表块类型 (11) (List Block Type (11))																															传输协议
	列表块长度 (List Block Length)																															
	传输协议数据块 (Transport Protocol Data Blocks)																															
MAC 地址块 (MAC Address Block)*	列表块类型 (11) (List Block Type (11))																															MAC 地址
	列表块长度 (List Block Length)																															
	主机 MAC 地址数据块 (Host MAC Address Data Blocks)																															
	主机上次查看时间 (Host Last Seen)																															
	主机类型 (Host Type)																															
	移动 (Mobile)								Jailbroken								VLAN 在线状态 (VLAN Presence)								VLAN ID							

字节	0								1								2								3								
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
客户端应用数据	VLAN ID （续）								VLAN 类型 (VLAN Type)								VLAN 优先级 (VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))								客户端应用
	通用列表块类型 (31) (Generic List Block Type (31)) （续）																								通用列表块长度 (Generic List Block Length)								
	通用列表块长度 (Generic List Block Length) （续）																								客户端应用数据块 (Client Application Data Blocks)								
NetBIOS 名称	字符串块类型 (0) (String Block Type (0))																																
	字符串块长度 (String Block Length)																																
	NetBIOS 字符串数据 ...(NetBIOS String Data...)																																

下表对 5.2+ 返回的主机配置文件数据块的字段进行了说明。

表 4-84　　主机配置文件数据块 5.2+ 字段

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

表 4-84　主机配置文件数据块 5.2+ 字段 （续）

字段	数据类型	说明
操作系统指纹（服务器指纹）数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（客户端指纹）数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 SMB 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（SMB 指纹）数据块 (Operating System Fingerprint (SMB Fingerprint) Data Blocks) *	变量	包含用 SMB 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 4-84　主机配置文件数据块 5.2+ 字段 （续）

字段	数据类型	说明
操作系统指纹（DHCP 指纹）数据块 (Operating System Fingerprint (DHCP Fingerprint) Data Blocks) *	变量	包含用 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用移动设备指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（移动）数据块 (Operating System Fingerprint (Mobile) Data Blocks) *	变量	包含用移动设备指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 IPv6 服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（IPv6 服务器）数据块 (Operating System Fingerprint (IPv6 Server) Data Blocks) *	变量	包含用 IPv6 服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 IPv6 客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 4-84　主机配置文件数据块 5.2+ 字段 （续）

字段	数据类型	说明
操作系统指纹（IPv6 客户端）数据块 (Operating System Fingerprint (IPv6 Client) Data Blocks) *	变量	包含用 IPv6 客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用 IPv6 DHCP 指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（IPv6 DHCP 指纹）数据块 (Operating System Fingerprint (IPv6 DHCP Fingerprint) Data Blocks) *	变量	包含用 IPv6 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送用用户代理指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹（用户代理指纹）数据块 (Operating System Fingerprint (User Agent Fingerprint) Data Blocks) *	变量	包含用用户代理指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅操作系统指纹数据块 5.1+，第 4-164 页。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
TCP 服务器数据块 (TCP Server Data Blocks)	变量	描述 TCP 服务器的主机服务器数据块。有关此数据块的说明，请参阅主机服务器数据块 4.10.0+，第 4-141 页。

表 4-84　主机配置文件数据块 5.2+ 字段 （续）

字段	数据类型	说明
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务器数据的服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装服务器数据块。 此字段后面是零个或多个服务器数据块。
UDP 服务器数据块 (UDP Server Data Blocks)	uint32	描述 UDP 服务器的主机服务器数据块。有关此数据块的说明，请参阅主机服务器数据块 4.10.0+，第 4-141 页。
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个协议数据块。
网络协议数据块 (Network Protocol Data Blocks)	uint32	描述网络协议的协议数据块。有关此数据块的说明，请参阅协议数据块，第 4-74 页。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块。 此字段后面是零个或多个传输协议数据块。
传输协议数据块 (Transport Protocol Data Blocks)	uint32	描述传输协议的协议数据块。有关此数据块的说明，请参阅协议数据块，第 4-74 页。
列表块类型 (List Block Type)	uint32	启动由 MAC 地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks)	uint32	描述主机 MAC 地址的主机 MAC 地址数据块。有关此数据块的说明，请参阅主机 MAC 地址 4.9+，第 4-116 页。
主机上次查看时间 (Host Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。

表 4-84　主机配置文件数据块 5.2+ 字段 （续）

字段	数据类型	说明
主机类型 (Host Type)	uint32	表示主机类型。可能会出现以下值： • 0 - 主机 • 1 - 路由器 • 2 - 网桥 • 3 - NAT 设备 • 4 - LB （负载均衡器）
移动 (Mobile)	uint8	指示主机是否为移动设备的一个真假标志。
Jailbroken	uint8	指示主机是否同样为已被越狱的移动设备的一个真假标志。
VLAN 在线状态 (VLAN Presence)	uint8	表示是否存在 VLAN： • 0 - 是 • 1 - 否
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
字符串块类型 (String Block Type)	uint32	启动主机客户端应用数据的字符串数据块。值始终为 112。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上主机客户端应用数据中的字节数。
主机客户端应用数据块 (Host Client Application Data Blocks)	变量	客户端应用数据块列表。有关此数据块的说明，请参阅完整主机客户端应用数据块 5.0+，第 4-158 页。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。

用户产品数据块 5.1+

用户产品数据块传输从第三方应用导入的主机输入数据，包括第三方应用字符串映射。此数据块在扫描结果数据块 5.2+，第 4-138 页和用户服务器和操作系统消息，第 4-58 页中使用。在版本 4.7 - 4.10.1 中，用户产品数据块的块类型为系列 1 数据块组中的 65；在版本 4.10.2 - 5.0.x 中，块类型为 118；在版本 5.1+ 中，块类型为系列 1 数据块组中的 134。块类型 65 与 118 的结构相同。

注　下图中数据块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示用户产品数据块的格式：

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

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

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

下表对用户产品数据块的组件进行了说明。

表 4-85　用户产品数据块字段

字段	数据类型	说明
用户产品数据块类型 (User Product Data Block Type)	uint32	启动用户产品数据块。在版本 5.1+ 中，此值为 134。
用户产品块长度 (User Product Block Length)	uint32	用户产品数据块中的字节总数，包括用户产品块类型和长度字段的八个字节，加上随后的用户产品数据中的字节数。
源 ID (Source ID)	uint32	映射到导入数据的源的标识号。根据源类型，这可能映射到 RNA、用户、扫描仪或第三方应用。
源类型 (Source Type)	uint32	映射到数据源类型的数字： • 0 如果数据由 RNA 提供 • 1 如果数据由用户提供 • 2 如果数据由第三方扫描仪提供 • 3 如果数据由命令行工具 （如 nmimport.pl）或主机输入 API 客户端提供
通用列表块类型 (Generic List Block Type)	uint32	启动由传送 IP 地址范围数据的 IP 范围规格数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装 IP 范围规格数据块。
IP 范围规格数据块 (IP Range Specification Data Blocks) *	变量	包含用于用户输入的 IP 地址范围相关信息的 IP 范围规格数据块。有关此数据块的说明，请参阅用于 5.2+ 的 IP 地址范围数据块，第 4-96 页。
端口 (Port)	uint16	用户指定的端口。
协议 (Protocol)	uint16	IANA 协议号或 Ethertype。这对传输协议和网络层协议的处理方式不同。 传输层协议由 IANA 协议号识别。例如： • 6 - TCP • 17 - UDP 网络层协议由 IEEE 注册权威机构 Ethertype 的十进制形式识别。例如： • 2048 - IP
丢弃用户产品 (Drop User Product)	uint32	表示是否已从主机中删除用户操作系统定义： • 0 - 否 • 1 - 是
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义供应商名称的字符串数据块。值始终为 0。

表 4-85　用户产品数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	自定义供应商字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上供应商名称中的字节数。
自定义供应商名称 (Custom Vendor Name)	字符串	在用户输入中指定的自定义供应商名称。
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义产品名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	自定义产品字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上产品名称中的字节数。
自定义产品名称 (Custom Product Name)	字符串	在用户输入中指定的自定义产品名称。
字符串块类型 (String Block Type)	uint32	启动包含在用户输入中指定的自定义版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	自定义版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
自定义版本 (Custom Version)	字符串	在用户输入中指定的自定义版本。
软件 ID (Software ID)	uint32	数据库中服务器或操作系统特定修订版的标识符。
服务器 ID (Server ID)	uint32	在用户输入中指定的主机服务器上的应用协议的 Firepower 系统应用标识符。
供应商 ID (Vendor ID)	uint32	在第三方操作系统映射到 Firepower 系统操作系统定义时指定的第三方操作系统的供应商的标识符。
产品 ID (Product ID)	uint32	在第三方操作系统字符串映射到 Firepower 系统操作系统定义时指定的第三方操作系统字符串的产品标识字符串。
字符串块类型 (String Block Type)	uint32	启动包含用户输入中的第三方操作系统字符串映射到的 Firepower 系统操作系统定义的主版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	主版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
主版本	字符串	第三方操作系统字符串映射到的 Firepower 系统操作系统定义的主版本。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Firepower 系统操作系统定义的次版本号的字符串数据块。值始终为 0。

表 4-85　用户产品数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	次版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
次版本 (Minor Version)	字符串	用户输入中的第三方操作系统字符串映射到的 Firepower 系统操作系统定义的次版本号。
字符串块类型 (String Block Type)	uint32	启动包含用户输入中的第三方操作 Firepower 系统系统字符串映射到的 操作系统定义的修订号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	修订版字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修订号中的字节数。
修订版 (Revision)	字符串	用户输入中的第三方操作系统字符串映射到的 Firepower 系统操作系统定义的修订号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Firepower 系统操作系统定义的最新主版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至主版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
至主版本 (To Major)	字符串	用户输入中的第三方操作系统字符串映射到的 Firepower 系统操作系统定义的一系列主版本号中的最新版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Firepower 系统操作系统定义的最新次版本的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至次版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上版本中的字节数。
至次版本 (To Minor)	字符串	用户输入中的第三方操作系统字符串映射到的 Firepower 系统操作系统定义的一系列次版本号中的最新版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Firepower 系统操作系统定义的最新修订号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	至修订版字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修订号中的字节数。
至修订版 (To Revision)	字符串	用户输入中的第三方操作系统字符串映射到的 Firepower 系统操作系统定义的一系列修订号中的最新修订号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Firepower 系统操作系统的内部版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	内部版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上内部版本号中的字节数。

表 4-85　用户产品数据块字段 （续）

字段	数据类型	说明
内部版本 (Build)	字符串	用户输入中的第三方操作系统字符串映射到的 Firepower 系统操作系统的内部版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Firepower 系统操作系统的修补版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	修补版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上修补版本号中的字节数。
修补 (Patch)	字符串	用户输入中的第三方操作系统字符串映射到的 Firepower 系统操作系统的修补版本号。
字符串块类型 (String Block Type)	uint32	启动包含第三方操作系统字符串映射到的 Firepower 系统操作系统的扩展版本号的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	扩展版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上扩展版本号中的字节数。
分机 (Extension)	字符串	用户输入中的第三方操作系统字符串映射到的 Firepower 系统操作系统的扩展版本号。
UUID	uint8 [x16]	包含操作系统的唯一标识号。
字符串块类型 (String Block Type)	uint32	启动包含用户输入中设备硬件信息的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	内部版本字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上内部版本号中的字节数。
设备字符串 (Device String)	字符串	移动设备硬件信息。
移动 (Mobile)	uint8	指示操作系统是否在移动设备上运行的一个真假标志。
Jailbroken	uint8	指示移动设备操作系统是否被越狱的一个真假标志。
通用列表块类型 (Generic List Block Type)	uint32	启动由传送有关应用到特定 IP 地址范围中指定主机的修复的用户输入数据的修复列表数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装修复列表数据块。
修复列表数据块 (Fix List Data Blocks) *	变量	包含应用到主机的修复的相关信息的修复列表数据块。有关此数据块的说明，请参阅修复列表数据块，第 4-103 页。

用户数据块

用户数据块在用户事件消息中出现。它们是系列 1 数据块的子集。有关系列 1 数据块的通用格式的信息，请参阅了解发现 （系列 1）块，第 4-63 页。

注 用户数据块报头的数据块长度字段包含该数据块中的字节数，包括两个数据块报头字段的八个字节。

下表列出了可能在用户事件消息中出现的用户数据块。数据块按数据块类型列出。当前版本数据块是最新版本。当前版本的 Firepower 系统支持旧数据块，但不产生旧数据块。

表 4-86　用户数据块类型

类型	内容	数据块类别	说明
73	用户登录信息	传统	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用于 5.0 - 5.0.2 的用户登录信息数据块，第 B-105 页。5.0 中引入的后继块类型的结构与块类型 73 的结构相同，但字段中的数据不同。
74	用户帐户更新消息	当前	包含用户帐户信息中的更改。有关详细信息，请参阅用户帐户更新消息数据块，第 4-184 页。
75	用于 4.7 - 4.10.x 的用户信息	传统	包含系统检测到的用户信息中的更改。有关详细信息，请参阅用于 5.x 的用户信息数据块，第 B-119 页。版本 6.0 中引入的后继块的块类型为 158。
120	用于 5.x 的用户信息	当前	包含系统检测到的用户信息中的更改。有关详细信息，请参阅用于 5.x 的用户信息数据块，第 B-119 页。替代块类型 75。它被块类型 158 替代。
121	用户登录信息	传统	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用于 5.0 - 5.0.2 的用户登录信息数据块，第 B-105 页。与块 73 的不同在于 “ 协议 ”(Protocol) 字段的内容，该字段存储在事件中检测到的应用协议 ID 的版本 5.0+ 应用 ID。版本 5.1 中引入的后继块的块类型为 127。
127	用户登录信息	传统	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用户登录信息数据块 5.1 - 5.4.x，第 B-107 页。它替代块类型 121。版本 6.0 中引入的后继块的块类型为 159。
150	IOC 状态	当前	包含有关危害的信息。有关详细信息，请参阅用于 5.3+ 的 IOC 状态数据块，第 4-34 页。
158	用于 6.0+ 的用户信息	当前	包含系统检测到的用户信息中的更改。有关详细信息，请参阅用于 6.0+ 的用户信息数据块，第 4-194 页。替代块类型 120。
159	用户登录信息	传统	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用户登录信息数据块 6.0.x，第 B-109 页。它替代块类型 127。

表 4-86　　用户数据块类型 （续）

类型	内容	数据块类别	说明
165	用户登录信息	传统模式	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用户登录信息数据块 6.1.x，第 B-116 页。它替代块类型 159。它被块类型 167 替代。
166	VPN 会话信息	当前	包含系统检测到的有关 VPN 会话的信息。有关详细信息，请参阅用于 6.2+ 的 VPN 会话数据块，第 4-197 页。
167	用户登录信息	当前	包含系统检测到的用户登录信息中的更改。有关详细信息，请参阅用户登录信息数据块 6.2+，第 4-200 页。它替代块类型 165。

用户帐户更新消息数据块

用户帐户更新消息数据块传输对用户帐户信息的更新相关信息。

用户帐户更新消息数据块的块类型为系列 1 数据块组中的 74。

下图显示用户帐户更新消息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户帐户更新消息块类型 (74) (User Account Update Message Block Type (74))																															
	用户帐户更新消息块长度 (User Account Update Message Block Length)																															
用户名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名 ...(User Name...)																															
第一页名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名字 ...(First Name...)																															
中间首字母缩写	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	中间名首字母缩写 ...(Middle Initials...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
最后一页名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	姓氏 ...(Last Name...)																															
全称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	全名 ...(Full Name...)																															
职位	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	职位 ...(Title...)																															
员工身份	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	员工身份 ...(Staff Identity...)																															
地址	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	地址 ...(Address...)																															
城市	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	城市 ...(City...)																															
省 / 自治区	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	省 / 自治区 ...(State...)																															
国家 / 地区	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	国家 / 地区 ...(Country/Region...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
邮政代码	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	邮政编码 ...(Postal Code...)																															
建筑	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	建筑 ...(Building...)																															
位置	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	位置 (Location)…																															
会议室	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	室 ...(Room...)																															
公司	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	公司 ...(Company...)																															
部门	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	分部 ...(Division...)																															
系	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	部门 ...(Department...)																															
办公室	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	办公室 ...(Office...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
Mailstop	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	Mailstop...																															
电子邮件	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件 ...(Email...)																															
电话	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电话 ...(Phone...)																															
IP 电话	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	IP 电话 ...(IP Phone...)																															
用户 1	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 1...(User 1...)																															
用户 2	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 2...(User 2...)																															
用户 3	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 3...(User 3...)																															
用户 4	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户 4...(User 4...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
邮件别名 1 (Email Alias 1)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	邮件别名 1...(Email Alias 1...)																															
邮件别名 2 (Email Alias 2)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	邮件别名 2...(Email Alias 2...)																															
邮件别名 3 (Email Alias 3)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	邮件别名 3...(Email Alias 3...)																															

下表对用户帐户更新消息数据块的组件进行了说明。

表 4-87　　用户帐户更新消息数据块字段

字段	数据类型	说明
用户帐户更新消息块类型 (User Account Update Message Block Type)	uint32	启动用户帐户更新消息数据块。值始终为 74。
用户帐户更新消息块长度 (User Account Update Message Block Length)	uint32	用户帐户更新消息数据块中的字节总数，包括用户帐户更新消息块类型和长度字段的八个字节，加上随后的用户帐户更新消息数据中的字节数。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
字符串块类型 (String Block Type)	uint32	启动包含用户的名字的字符串数据块。值始终为 0。

表 4-87　用户帐户更新消息数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	名字字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上名字中的字节数。
名字 (First Name)	字符串	用户的名字。
字符串块类型 (String Block Type)	uint32	启动包含用户的中间名首字母缩写的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	中间名首字母缩写字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上中间名首字母缩写中的字节数。
中间名首字母缩写 (Middle Initials)	字符串	用户的中间名首字母缩写。
字符串块类型 (String Block Type)	uint32	启动包含用户的姓氏的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	姓氏字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上姓氏中的字节数。
姓氏	字符串	用户的姓氏。
字符串块类型 (String Block Type)	uint32	启动包含用户的全名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	全名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上全名中的字节数。
全称 (Full Name)	字符串	用户的全名。
字符串块类型 (String Block Type)	uint32	启动包含用户的职位的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	职位字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上职位中的字节数。
职位 (Title)	字符串	用户的职位。
字符串块类型 (String Block Type)	uint32	启动包含用户的员工标识的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	员工身份字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上员工身份中的字节数。
员工身份 (Staff Identity)	字符串	用户的员工身份。

表 4-87　用户帐户更新消息数据块字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动包含用户的地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上地址中的字节数。
地址 (Address)	字符串	用户的地址。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的城市的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	城市字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上城市中的字节数。
城市 (City)	字符串	用户地址中的城市。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的省 / 自治区的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	省 / 自治区字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上省 / 自治区中的字节数。
省 / 自治区 (State)	字符串	用户所在的省 / 自治区。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的国家或地区的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	国家或地区字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上国家或地区中的字节数。
国家或地区 (Country or Region)	字符串	用户地址中的国家或地区。
字符串块类型 (String Block Type)	uint32	启动包含用户地址的邮政编码的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮政编码字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮政编码中的字节数。
邮政编码 (Postal Code)	字符串	用户地址的邮政编码。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的建筑的字符串数据块。值始终为 0。

表 4-87　用户帐户更新消息数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	建筑字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上建筑名称中的字节数。
建筑 (Building)	字符串	用户地址中的建筑。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的位置的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	位置字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上位置名称中的字节数。
位置 (Location)	字符串	用户地址中的位置。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的室的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	室字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上室中的字节数。
会议室 (Room)	字符串	用户地址中的室。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的公司的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	公司字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上公司名称中的字节数。
公司 (Company)	字符串	用户地址中的公司。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的分部的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	分部字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上分部名称中的字节数。
分部 (Division)	字符串	用户地址中的分部。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的部门的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	部门字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上部门中的字节数。
部门 (Dept)	字符串	用户地址中的部门。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的办公室的字符串数据块。值始终为 0。

表 4-87　用户帐户更新消息数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	办公室字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上办公室中的字节数。
办公室 (Office)	字符串	用户地址中的办公室。
字符串块类型 (String Block Type)	uint32	启动包含用户地址中的 mailstop 的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	Mailstop 字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上 mailstop 中的字节数。
Mailstop	字符串	用户地址中的 mailstop。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
字符串块类型 (String Block Type)	uint32	启动包含用户的电话号码的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	电话号码字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电话号码中的字节数。
电话 (Phone)	字符串	用户的电话号码。
字符串块类型 (String Block Type)	uint32	启动包含用户的网络电话号码的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	网络电话号码字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上网络电话号码中的字节数。
网络电话 (Internet Phone)	字符串	用户的网络电话号码。
字符串块类型 (String Block Type)	uint32	启动包含用户的替代用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户 1 (User 1)	字符串	用户的替代用户名。

表 4-87　用户帐户更新消息数据块字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动包含用户的替代用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户 2 (User 2)	字符串	用户的替代用户名。
字符串块类型 (String Block Type)	uint32	启动包含用户的替代用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户 3 (User 3)	字符串	用户的替代用户名。
字符串块类型 (String Block Type)	uint32	启动包含用户的替代用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户 4 (User 4)	字符串	用户的替代用户名。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件别名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件别名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件别名中的字节数。
邮件别名 1 (Email alias 1)	字符串	用户的邮件别名。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件别名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件别名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件别名中的字节数。
邮件别名 2 (Email alias 2)	字符串	用户的邮件别名。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件别名的字符串数据块。值始终为 0。

表 4-87　用户帐户更新消息数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	邮件别名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件别名中的字节数。
邮件别名 3 (Email alias 3)	字符串	用户的邮件别名。

用于 6.0+ 的用户信息数据块

用户信息数据块在用户修改消息中使用，传送检测到、删除或丢弃的用户的信息。有关详细信息，请参阅用户修改消息，第 4-62 页

在版本 6.0+ 中，用户信息数据块的块类型为系列 1 数据块组中的 158。它具有新终端配置文件、安全情报和 IPv6 字段。

在版本 4.7 - 4.10.x 中，用户信息数据块的块类型为系列 1 数据块组中的 75，在版本 5.x 中，块类型为系列 1 数据块组中的 120。有关详细信息，请参阅用于 5.x 的用户信息数据块，第 B-119 页。

下图显示用户信息数据块的格式。

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户信息块类型 (158) (User Information Block Type (158))																															
	用户信息块长度 (User Information Block Length)																															
	用户 ID (User ID)																															
用户名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名 ...(User Name...)																															
	领域 ID (Realm ID)																															
	协议 (Protocol)																															
第一页名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名字 ...(First Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
最后一页名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	姓氏 ...(Last Name...)																															
电子邮件	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件 ...(Email...)																															
部门	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	部门 ...(Department...)																															
电话	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电话 ...(Phone...)																															
	终端配置文件 ID (Endpoint Profile ID)																															
	安全组 ID (Security Group ID)																															
	位置 IPv6 地址 (Location IPv6 Address)																															
	位置 IPv6 地址 (Location IPv6 Address) （续）																															
	位置 IPv6 地址 (Location IPv6 Address) （续）																															
	位置 IPv6 地址 (Location IPv6 Address) （续）																															

下表对用户信息数据块的组件进行了说明。

表 4-88　用户信息数据块字段

字段	数据类型	说明
用户信息块类型 (User Information Block Type)	uint32	启动用户信息数据块。值为 158。
用户信息块长度 (User Information Block Length)	uint32	用户信息数据块中的字节总数，包括用户信息块类型和长度字段的八个字节，加上随后的用户信息数据中的字节数。
用户 ID (User ID)	uint32	用户的标识号。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
领域 ID (Realm ID)	uint32	与身份领域对应的整数 ID。
协议 (Protocol)	uint32	用于包含用户信息的数据包的协议。
字符串块类型 (String Block Type)	uint32	启动包含用户的名字的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名字字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上名字中的字节数。
名字 (First Name)	字符串	用户的名字。
字符串块类型 (String Block Type)	uint32	启动包含用户的姓氏的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户姓氏字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上姓氏中的字节数。
姓氏 (Last Name)	字符串	用户的姓氏。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
字符串块类型 (String Block Type)	uint32	启动包含用户所在部门的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	部门字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上部门中的字节数。
部门 (Dept)	字符串	用户所在部门。
字符串块类型 (String Block Type)	uint32	启动包含用户的电话号码的字符串数据块。值始终为 0。

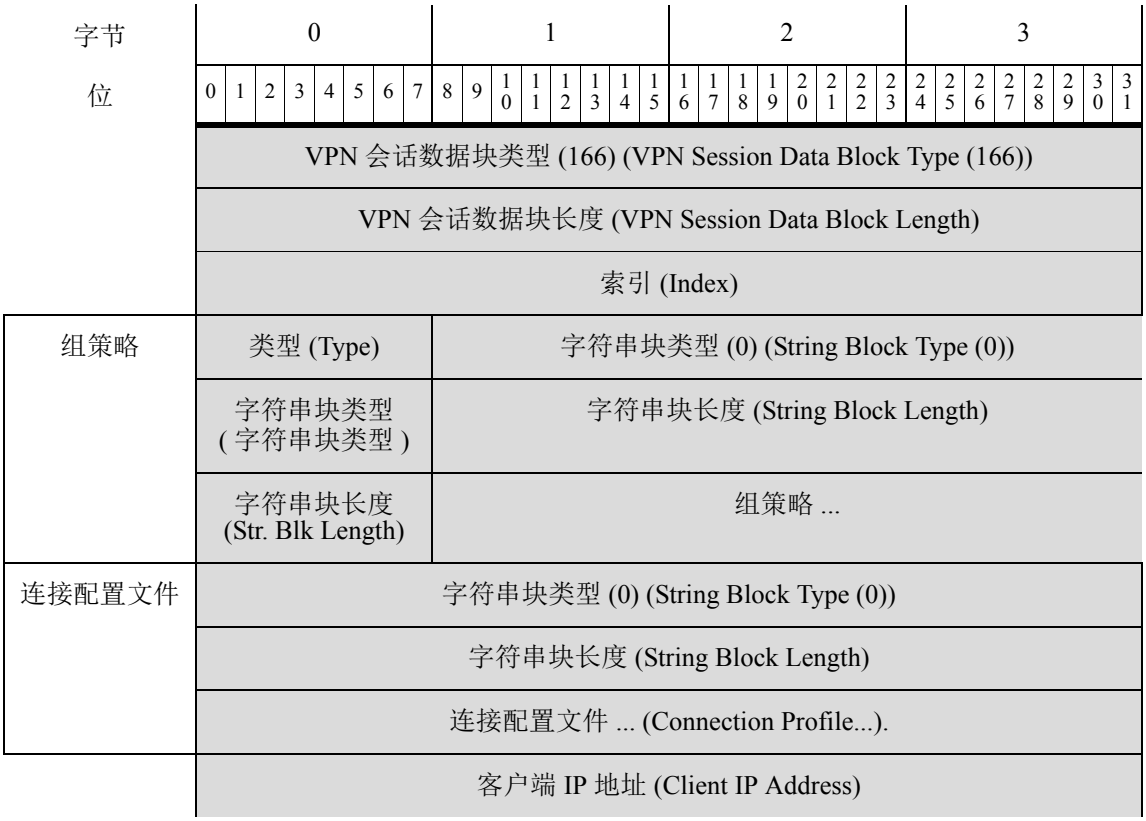
表 4-88　　用户信息数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	电话号码字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上电话号码中的字节数。
电话 (Phone)	字符串	用户的电话号码。
终端配置文件 ID (Endpoint Profile ID)	uint32	连接终端使用的设备类型的 ID 号码。这是每个防御中心特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	网络流量组的 ID 号码。
位置 IPv6 地址 (Location IPv6 Address)	uint16[8]	与 ISE 通信的接口的 IP 地址。可以是 IPv4 或 IPv6。

用于 6.2+ 的 VPN 会话数据块

用于 6.2+ 的 VPN 会话数据块的块类型为系列 1 数据块组中的 166。该数据块描述 VPN 会话信息。

下图显示 6.2+ 中的 VPN 会话数据块的格式。



字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	客户端 IP 地址 (Client IP Address) （续）																															
	客户端 IP 地址 (Client IP Address) （续）																															
	客户端 IP 地址 (Client IP Address) （续）																															
客户端操作系统	客户端国家 / 地区 (Client Country)																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）																客户端操作系统 ... (Client Operating System...)															
客户端应用	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	客户端应用 ... (Client Application...)																															
	连接持续时间 (Connection Duration)																															
	传输的字节数 (Bytes Transmitted)																															
	传输的字节数 (Bytes Transmitted) （续）																															
	接收的字节数 (Bytes Received)																															
	接收的字节数 (Bytes Received) （续）																															

下表对 VPN 会话数据块的字段进行了说明。

表 4-89　　VPN 会话数据块字段

字段	数据类型	说明
VPN 会话数据块类型 (VPN Session Data Block Type)	uint32	启动 VPN 会话数据块。值始终为 166。
VPN 会话块长度 (VPN Session Block Length)	uint32	VPN 会话数据块中的字节数，包括 VPN 会话数据块类型和长度的八个字节，加上随后的 “VPN 会话 ” 数据字段中的字节数。
索引 (Index)	uint32	由 VPN 设备生成的用于标识会话的编号。

表 4-89　　VPN 会话数据块字段 （续）

字段	数据类型	说明
类型 (Type)	uint8	VPN 会话的类型。可能的值包括： • 0 - 未知 • 1- 思科 IKEv1 客户端 • 2- AnyConnect IKEv1 客户端 • 3 - AnyConnect SSL • 4 - WebVPN 无客户端 • 5 - 站点间 IKEv2 • 6 - 站点间 IKEv2 • 7 - 通用 IKEv2 RA 客户端
字符串块类型 (String Block Type)	uint32	启动包含 VPN 会话的组策略的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上组策略中的字节数。
组策略 (Group Policy)	字符串	在建立 VPN 会话时分配给客户端的组策略的名称。
字符串块类型 (String Block Type)	uint32	启动包含 VPN 会话的连接配置文件的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上连接配置文件中的字节数。
连接配置文件 (Connection Profile)	字符串	VPN 会话使用的连接配置文件 （隧道组）的名称。
客户端 IP 地址 (Client IP Address)	uint8[16]	VPN 客户端设备的 IP 地址。
客户端国家 / 地区 (Client Country)	uint16	VPN 客户端的国家 / 地区代码。
字符串块类型 (String Block Type)	uint32	启动包含客户端设备所使用操作系统的字符串数据块。 值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上操作系统名称中的字节数。
客户端操作系统 (Client Operating System)	字符串	客户端设备的操作系统。

表 4-89　VPN 会话数据块字段 （续）

字段	数据类型	说明
字符串块类型 (String Block Type)	uint32	启动包含客户端设备所使用 VPN 应用的字符串数据块。值始终为 0。
字符串块长度 (String block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上 VPN 应用中的字节数。
客户端应用 (Client Application)	字符串	客户端设备的 VPN 应用。
连接持续时间 (Connection Duration)	uint32	VPN 会话的持续时间 （以秒为单位）。仅指定用于 VPN 注销操作，否则值为 0。
传输的字节数 (Bytes Transmitted)	uint64	VPN 会话期间传输到 VPN 客户端的字节数。仅 指定用于 VPN 注销操作，否则值为 0。
接收的字节数 (Bytes Received)	uint64	VPN 会话期间从 VPN 客户端接收的字节数。仅指定用于 VPN 注销操作，否则值为 0。

用户登录信息数据块 6.2+

用户登录信息数据块在用户信息更新消息中使用，传送检测到的用户的登录信息变更。有关详细信息，请参阅用户信息更新消息块，第 4-62 页。

在版本 6.2+ 中，用户登录信息数据块的块类型为系列 1 数据块组中的 167。它的一些新字段用于支持 VPN。它替代块类型 165。有关详细信息，请参阅用户登录信息数据块 6.1.x，第 B-113 页。

下图显示用户登录信息数据块的格式：

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	用户登录信息块类型 (167) (User Login Information Block Type (159))																															
	用户登录信息块长度 (User Login Information Block Length)																															
	时间戳 (Timestamp)																															
	IPv4 地址 (IPv4 Addresses)																															
用户名称	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	用户名 ...(User Name...)																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
域	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	域 ...(Domain...)																															
	用户 ID (User ID)																															
	领域 ID (Realm ID)																															
	终端配置文件 ID (Endpoint Profile ID)																															
	安全组 ID (Security Group ID)																															
	协议 (Protocol)																															
	端口 (Port)																范围开始 (Range Start)															
	开始端口 (Start Port)																结束端口 (End Port)															
电子邮件	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	电子邮件 ...(Email...)																															
	IPv6 地址 (IPv6 Address)																															
	IPv6 地址 (IPv6 Address) （续）																															
	IPv6 地址 (IPv6 Address) （续）																															
	IPv6 地址 (IPv6 Address) （续）																															
	位置 IPv6 地址 (Location IPv6 Address)																															
	位置 IPv6 地址 (Location IPv6 Address) （续）																															
	位置 IPv6 地址 (Location IPv6 Address) （续）																															
	位置 IPv6 地址 (Location IPv6 Address) （续）																															

字节	0								1								2								3							
位	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
报告者 (Reported By)	登录类型 (Login Type)								身份验证类型 (Auth. Type)								字符串块类型 (0) (String Block Type (0))															
	字符串块类型 (0) (String Block Type (0)) （续）																字符串块长度 (String Block Length)															
	字符串块长度 (String Block Length) （续）																报告者 ...(Reported By...)															
说明	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	说明 ...(Description...)																															
VPN 会话	VPN 会话数据块类型 (166) (VPN Session Data Block Type (166))																															
	VPN 会话数据块长度 (VPN Session Data Block Length)																															
	VPN 会话 ... (VPN Session...)																															

下表对用户登录信息数据块的组件进行了说明。

表 4-90　　用户登录信息数据块字段

字段	数据类型	说明
用户登录信息块类型 (User Login Information Block Type)	uint32	启动用户登录信息数据块。在版本 6.2+ 中，此值为 167。
用户登录信息块长度 (User Login Information Block Length)	uint32	用户登录信息数据块中的字节总数，包括用户登录信息块类型和长度字段的八个字节，加上随后的用户登录信息数据中的字节数。
时间戳 (Timestamp)	uint32	事件的时间戳。
IPv4 地址 (IPv4 Addresses)	uint32	保留此字段，但不再填充。 IPv4 地址存储在 IPv6 地址字段中。有关详细信息，请参阅 IP 地址，第 1-3 页。
字符串块类型 (String Block Type)	uint32	启动包含用户的用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上用户名中的字节数。
用户名 (Username)	字符串	用户的用户名。
字符串块类型 (String Block Type)	uint32	启动包含域的字符串数据块。值始终为 0。

表 4-90　用户登录信息数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上域中的字节数。
域 (Domain)	字符串	用户登录的域。
用户 ID (User ID)	uint32	用户的标识号。
领域 ID (Realm ID)	uint32	与身份领域对应的整数 ID。
终端配置文件 ID (Endpoint Profile ID)	uint32	连接终端使用的设备类型的 ID 号码。这是每个 DC 特有的，在元数据中进行解析。
安全组 ID (Security Group ID)	uint32	网络流量组的 ID 号码。
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值如下： • 165 - FTP • 426 - SIP • 547 - AOL 即时通信工具 • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle 数据库 • 788 - POP3 • 1755 - MDNS
端口 (Port)	uint16	在其上检测到用户的端口号。
范围开始 (Range Start)	uint16	TS 代理使用的端口范围内的起始端口。
开始端口 (Start Port)	uint16	TS 代理分配给单个用户的端口范围内的起始端口。
结束端口 (End Port)	uint16	TS 代理分配给单个用户的端口范围内的结束端口。
字符串块类型 (String Block Type)	uint32	启动包含用户的邮件地址的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	邮件地址字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上邮件地址中的字节数。
电子邮件 (Email)	字符串	用户的邮件地址。
IPv6 地址 (IPv6 Addresses)	uint8[16]	检测到用户登录的主机的 IPv6 地址，采用 IP 地址八位组。
位置 IPv6 地址 (Location IPv6 Address)	uint8[16]	用户最新登录的 IP 地址。可以是 IPv4 或 IPv6 地址。
登录类型 (Login Type)	uint8	检测到的用户登录类型。

表 4-90 用户登录信息数据块字段 （续）

字段	数据类型	说明
身份验证类型 (Authentication Type)	uint8	用户使用的身份验证类型。值可能是： • 0 - 无需授权 • 1 - 被动身份验证、 AD 代理或 ISE 会话 • 2 - 强制网络门户身份验证成功 • 3 - 强制网络门户访客身份验证 • 4 - 强制网络门户身份验证失败
字符串块类型 (String Block Type)	uint32	启动包含报告者值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	报告者字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上 “ 报告者 ”(Reported By) 字段中的字节数。
报告者 (Reported By)	字符串	此活动的报告者，例如 Active Directory 服务器的名称。
字符串块类型 (String Block Type)	uint32	启动包含说明值的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	说明字符串数据块中的字节数，包括块类型和长度字段的八个字节，加上 “ 说明 ”(Description) 字段中的字节数。
说明 (Description)	字符串	登录或注销活动的说明。
VPN 会话块类型 (VPN Session Block Type)	uint32	启动包含 VPN 会话数据的 VPN 会话数据块。值始终为 166。
VPN 会话数据块长度 (VPN Session Data Block Length)	uint32	VPN 会话数据块中的字节数，包括块类型和长度字段的八个字节，加上 VPN 会话数据块中的字节数。
VPN 会话数据 (VPN Session data)	VPN 会话数据	有关检测到的 VPN 会话的信息 （如果登录与 VPN 会话关联）。这仅在有 VPN 会话时使用。

发现和连接事件系列 2 数据块

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

表 4-91 发现和连接事件系列 2 块类型

类型	内容	数据块状态	说明
15	访问控制规则	当前	访问控制规则元数据消息用其将策略 UUID 和规则 ID 值映射到描述性字符串。请参阅访问控制规则数据块，第 4-205 页。
21	访问控制规则原因	传统	访问控制规则元数据消息用其将访问控制规则原因映射到描述性字符串。请参阅用于 5.1-5.3.x 的关联事件，第 B-289 页。

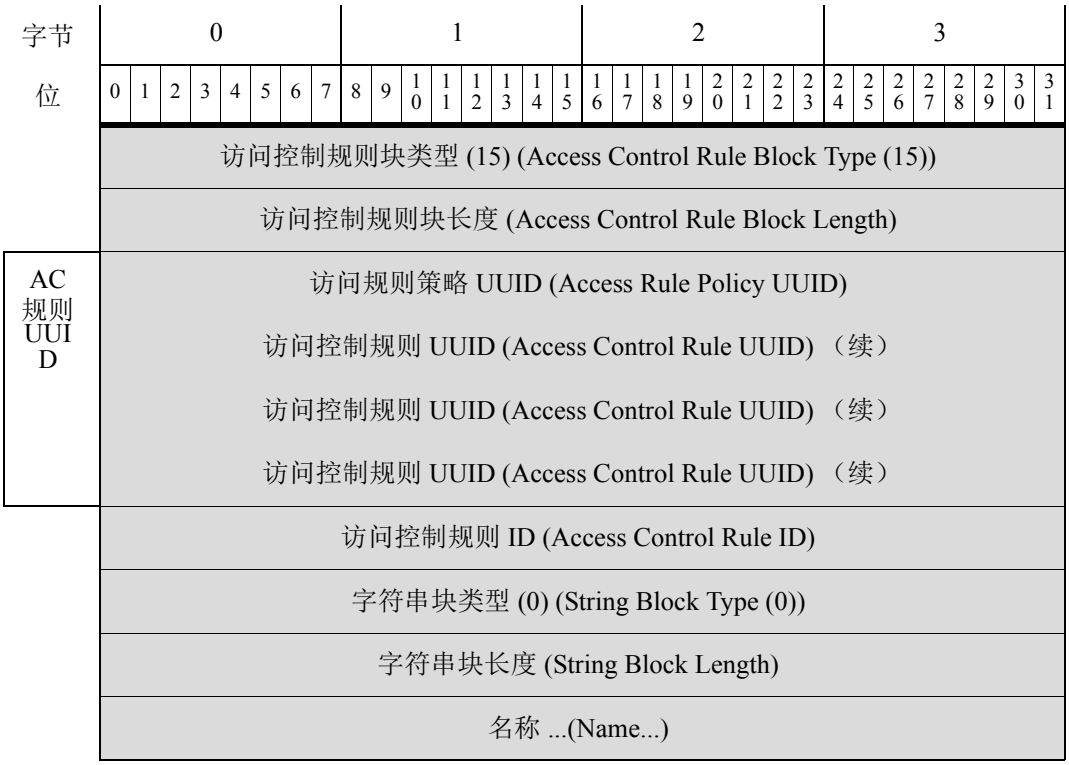
表 4-91　　发现和连接事件系列 2 块类型 （续）

类型	内容	数据块状态	说明
22	安全情报类别	当前	用于存储安全情报信息。请参阅安全情报类别数据块 5.1+，第 4-208 页。
57	用户数据	当前	用户记录元数据消息用其提供用户 ID 号码、检测到用户所依据的协议以及用户名。请参阅用户数据块，第 4-210 页。
59	访问控制规则原因	当前	访问控制规则元数据消息用其将访问控制规则原因映射到描述性字符串。请参阅访问控制规则原因数据块 6.0+，第 4-206 页。

访问控制规则数据块

eStreamer 服务使用访问控制规则元数据消息中的访问控制规则数据块将策略 UUID 和规则 ID 组合映射到描述性字符串。访问控制规则数据块的块类型为系列 2 数据块组中的 15。

下图显示访问控制规则数据块的结构：



下表对访问控制规则数据块中的字段进行了说明。

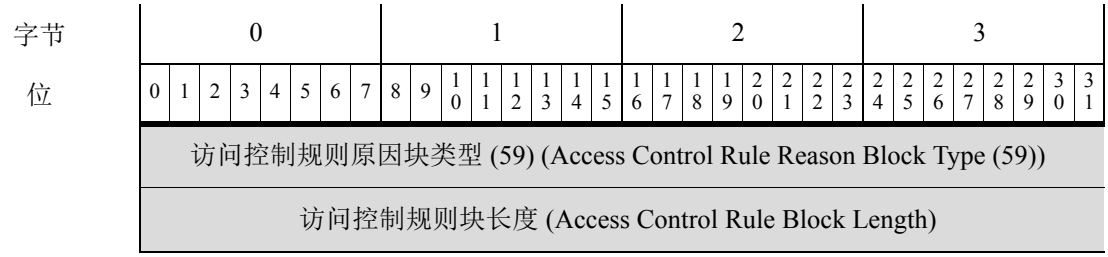
表 4-92　访问控制规则数据块字段

字段	数据类型	说明
访问控制规则块类型 (Access Control Rule Block Type)	uint32	启动访问控制规则块。值始终为 15。
访问控制规则块长度 (Access Control Rule Block Length)	uint32	访问控制规则块中的字节总数，包括访问控制规则块类型和长度字段的八个字节，加上随后的数据的字节数。
访问控制规则 UUID (Access Control Rule UUID)	uint8[16]	访问控制规则的唯一标识符。此字段与访问控制规则 ID 一起构成此记录的唯一密钥。
访问控制规则 ID (Access Control Rule ID)	uint32	访问控制规则的内部 Cisco 标识符。此字段与访问控制规则 UUID 一起构成此记录的唯一密钥。
字符串块类型 (String Block Type)	uint32	启动包含与访问控制策略规则 UUID 和访问控制规则 ID 相关的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 名称 ”(Name) 字段中的字节数。
名称 (Name)	字符串	描述性名称。

访问控制规则原因数据块 6.0+

eStreamer 服务使用访问控制规则原因元数据消息中的访问控制规则原因数据块将访问控制原因映射到描述性字符串。访问控制规则原因数据块的块类型为系列 2 数据块组中的 59。它替代了块类型 21。

下图显示访问控制规则原因数据块的结构：



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

下表对访问控制规则原因数据块中的字段进行了说明。

表 4-93　　访问控制规则原因数据块字段

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

表 4-93　访问控制规则原因数据块字段 （续）

字段	数据类型	说明
访问控制规则原因 (Access Control Rule Reason)	uint32	访问控制规则记录连接的原因。此字段是此记录的唯一密钥。 触发事件的规则的原因编号。 规则原因是一个可以在其中设置多个位的二进制位图。规则可能有多种原因。位值如下： • **1** - IP 阻止 • **2** - IP 监控 • **4** - 用户绕行 • **8** - 文件监控 • **16** - 文件阻止 • **32** - 入侵监控 • **64** - 入侵阻止 • **128** - 阻止继续传输文件 • **256** - 允许继续传输文件 • **512** - 文件自定义检测 • **1024** - SSL 阻止 • **2048** - DNS 阻止 • **4096** - DNS 监控 • **8192** - URL 阻止 • **16384** - URL 监控 • **32768** - 内容限制 • **65536** - 智能应用绕行 • **131072** - WSA 威胁
字符串块类型 (String Block Type)	uint32	启动包含与访问控制规则原因相关的描述性名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 ” 说明 “(Description) 字段中的字节数。
名称 (Name)	字符串	对访问控制规则原因的说明。

安全情报类别数据块 5.1+

eStreamer 服务使用访问控制规则元数据消息中的安全情报类别数据块流传输安全情报信息。安全情报类别数据块的块类型为系列 2 数据块组中的 22。

下图显示安全情报类别数据块的结构：

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

下表对安全情报类别数据块中的字段进行了说明：

表 4-94　　安全情报类别数据块字段

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

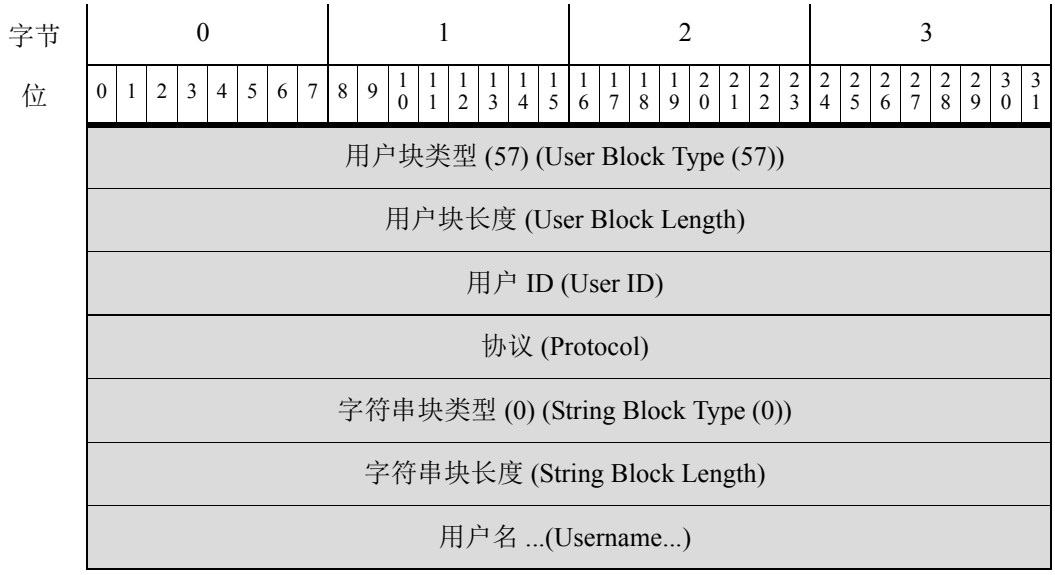
表 4-94　　安全情报类别数据块字段 （续）

字段	数据类型	说明
字符串块长度 (String Block Length)	uint32	名称字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 安全情报列表名称 ”(Security Intelligence Name) 字段中的字节数。
安全情报列表名称 (Security Intelligence List Name)	字符串	连接触发的安全情报类别 IP 阻止列表或允许列表的名称。

用户数据块

eStreamer 服务使用用户记录元数据消息中的用户数据块提供用户 ID 号码、在其上检测到用户的协议以及用户名。用户数据块的块类型为系列 2 数据块组中的 57。

下图显示用户数据块的结构：



下表对用户数据块中的字段进行了说明。

表 4-95　　用户数据块字段

字段	数据类型	说明
用户块类型 (User Block Type)	uint32	启动用户块。值始终为 57。
用户块长度 (User Block Length)	uint32	用户块中的字节总数，包括用户块类型和长度字段的八个字节，加上随后的数据字节数。
用户 ID (User ID)	uint32	用户的唯一标识符。此字段是此记录的唯一密钥。

表 4-95　　用户数据块字段 （续）

字段	数据类型	说明
协议 (Protocol)	uint32	用于检测或报告用户的协议。可能的值如下： • 165 - FTP • 426 - SIP • 547 - AOL 即时通信工具 • 683 - IMAP • 710 - LDAP • 767 - NTP • 773 - Oracle 数据库 • 788 - POP3 • 1755 - MDNS
字符串块类型 (String Block Type)	uint32	启动包含用户名的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	用户名字符串数据块中的字节数，包括块类型和报头字段的八个字节，加上 “ 用户名 ”(Username) 字段中的字节数。
用户名 (Username)	字符串	用户的名称

访问控制策略元数据块 6.0+

eStreamer 服务使用访问控制策略元数据消息中的访问控制策略元数据块来提供访问控制策略信息。访问控制策略元数据块的块类型为系列 2 数据块组中的 64。

下图显示访问控制策略元数据块的结构：

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

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

下表对访问控制策略元数据块中的字段进行了说明。

表 4-96　　访问控制策略元数据块字段

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