



了解主机数据结构

本章介绍传送描述单个主机的一组数据的完整主机配置文件数据块的格式。eStreamer 根据对主机数据的请求生成并发送这些数据块。有关客户端请求程序、消息结构以及交付方法的信息，请参阅[主机数据和多主机数据消息格式](#)，第 2-28 页。

eStreamer 使用系列 1 数据块结构打包这些完整主机配置文件数据块。有关系列 1 数据块的一般结构，请参阅[系列 1 数据块报头](#)，第 4-60 页。完整主机配置文件数据块包含许多封装数据块，[了解发现和连接数据结构](#)，第 4-1 页中定义这些数据块的子节中有对这些数据块的单独说明。

有关当前和旧版完整主机配置文件数据块的详细信息，请参阅以下各节：

- [完整主机配置文件数据块 5.3+](#)，第 5-1 页介绍当前完整主机配置文件数据块结构。
- [完整主机配置文件数据块 5.0 - 5.0.2](#)，第 B-363 页介绍用于版本 5.0 - 5.0.2 的旧版完整主机配置文件数据块结构。

完整主机配置文件数据块 5.3+

用于版本 5.3+ 的完整主机配置文件数据块包含一整套主机说明数据。其格式如下图中所示，并在下表中进行说明。请注意，除列表数据块之外，该图未显示封装数据块的字段。这些封装数据块在[了解发现和连接数据结构](#)，第 4-1 页中单独进行说明。完整主机配置文件数据块的块类型值为 149。它替代了之前的版本，之前版本的块类型为 140。



注释

下图中块名称旁边的星号 (*) 表示可能会出现多个数据块实例。

下图显示用于 5.3+ 的完整主机配置文件数据块的格式：

字节 位	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
完整主机配置文件数据块 (149) (Full Host Profile Data Block (149))																																
数据块长度 (Data Block Length)																																
主机 ID																																
主机 ID (Host ID) (续)																																
主机 ID (Host ID) (续)																																
主机 ID (Host ID) (续)																																
IP 地址 (IP Address)	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	IP 地址数据块 (143) (IP Address Data Blocks (143))*																															
跳数 (Hops)								通用列表块类型 (31) (Generic List Block Type (31))																								
通用列表块类型 (Generic List Block Type) (续)								通用列表块长度 (Generic List Block Length)																								
源自操作系统的 指纹 (OS Derived Fingerprints)	通用列表块长度 (Generic List Block Length) (续)								操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																							
	操作系统指纹块类型 (130) (OS Fingerprint Block Type (130))* (续)								操作系统指纹块长度 (Operating System Fingerprint Block Length)																							
	操作系统指纹块长度 (OS Fingerprint Block Length) (续)								源自操作系统的指纹数据... (Operating System Derived Fingerprint Data...)																							
通用列表块类型 (31) (Generic List Block Type (31))																																
通用列表块长度 (Generic List Block Length)																																
服务器 指纹 (Server Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统服务器指纹数据... (Operating System Server Fingerprint Data...)																															
通用列表块类型 (31) (Generic List Block Type (31))																																

字节 位	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	通用列表块长度 (Generic List Block Length)																															
客户端 指纹	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统客户端指纹数据... (Operating System Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机 指纹 1 (VDB Native Fingerprints 1)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
VDB 本机 指纹 2 (VDB Native Fingerprints 2)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 VDB 指纹数据... (Operating System VDB Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
用户 指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户指纹数据... (Operating System User Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
扫描 指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统扫描指纹数据... (Operating System Scan Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节 位	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
应用 指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统应用指纹数据... (Operating System Application Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
冲突 指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统冲突指纹数据... (Operating System Conflict Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
移动 (Mobile) 指纹 (Mobile Device Fingerprint)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统移动指纹数据... (Operating System Mobile Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
IPv6 服务器 指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 IPv6 服务器指纹数据... (Operating System IPv6 Server Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
IPv6 客户端 指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 IPv6 客户端指纹数据... (Operating System IPv6 Client Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															

字节 位	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IPv6 DHCP 指纹 (User Agent Fingerprints)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统 IPv6 DHCP 指纹数据... (Operating System IPv6 DHCP Fingerprint Data...)																															
	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
用户代理 指纹 (User Agent Fingerprint)	操作系统指纹块类型 (130) (Operating System Fingerprint Block Type (130))*																															
	操作系统指纹块长度 (Operating System Fingerprint Block Length)																															
	操作系统用户代理指纹数据... (Operating System User Agent Fingerprint Data...)																															
(TCP) 完整 服务器数据	列表块类型 (11)... (List Block Type (11))...																															
	列表块长度... (List Block Length)...																															
	(TCP) 完整服务器数据块 (104) ((TCP) Full Server Data Blocks (104))*																															
(UDP) 完整 服务器数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	(UDP) 完整服务器数据块 (104) ((UDP) Full Server Data Blocks (104))*																															
网络 协议数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	(网络) 协议数据块 (4) ((Network) Protocol Data Blocks (4))*																															
传输 协议数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	(传输) 协议数据块 (4) ((Transport) Protocol Data Blocks (4))*																															
MAC 地址数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	主机 MAC 地址数据块 (95) (Host MAC Address Data Blocks (95))*																															
	上次查看时间 (Last Seen)																															
	主机类型 (Host Type)																															
	业务临界点 (Business Criticality)																VLAN ID															

字节 位	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	VLAN 类型 (VLAN Type)								VLAN 优先级(VLAN Priority)								通用列表块类型 (31) (Generic List Block Type (31))															
主机客户端 数据	通用列表块类型 (Generic List Block Type) (续)																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length) (续)																完整主机客户端应用数据块 (112) (Full Host Client Application Data Blocks (112))*															
NetBIOS 名称 (NetBIOS Name)	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	名称 (Name) NetBIOS 名称字符串... (NetBIOS Name String...)																															
说明 (Description) 数据	字符串块类型 (0) (String Block Type (0))																															
	字符串块长度 (String Block Length)																															
	注释字符串... (Notes String....)																															
(VDB) 主机 漏洞 ((VDB) Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(VDB) 主机漏洞数据块 (85) ((VDB) Host Vulnerability Data Blocks (85))*																															
(第三方 /VDB) 主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(第三方/VDB) 主机漏洞数据块 (85) ((Third Party/VDB) Host Vulnerability Data Blocks (85))*																															
第三方扫描 主机漏洞 (3rd Pty Scan Host Vulns)	通用列表块类型 (31) (Generic List Block Type (31))																															
	通用列表块长度 (Generic List Block Length)																															
	(第三方扫描) 具有原始漏洞 ID 的主机漏洞数据块 (85) ((Third Party Scan) Host Vulnerability Data Blocks with Original Vuln IDs (85))*																															
属性 值数据	列表块类型 (11) (List Block Type (11))																															
	列表块长度 (List Block Length)																															
	属性值数据块 (Attribute Value Data Blocks) *																															
	移动 (Mobile)								Jailbroken								通用列表块类型 (31) (Generic List Block Type (31))															

字节 位	0								1								2								3							
	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
IOC 状态 (IOC State)	通用列表块类型 (Generic List Block Type) (续)																通用列表块长度 (Generic List Block Length)															
	通用列表块长度 (Generic List Block Length) (续)																IOC 状态数据块 (150) (IOC State Data Blocks (150))*															

下表描述的是用于 5.3+ 记录的完整主机配置文件的组件。

表 5-1 完整主机配置文件记录 5.3+ 字段

字段	数据类型	说明 (Description)
主机 ID	uint8[16]	主机的唯一 ID 号码。这是一个 UUID。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务数据的 IP 地址数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装 IP 地址数据块的长度。
IP 地址 (IP Address)	变量	主机的 IP 地址以及上次看到每个 IP 地址的时间。有关此数据块的说明，请参阅 主机 IP 地址数据块 ，第 4-95 页。
跳数 (Hops)	uint8	从主机到设备的网络跳数。
通用列表块类型 (Generic List Block)	uint32	启动由传送源自主机的现有指纹的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
源自操作系统的指纹数据块 (Operating System Derived Fingerprint Data Blocks) *	变量	包含源自主机的现有指纹的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅 操作系统指纹数据块 5.1+ ，第 4-161 页。
通用列表块类型 (Generic List Block)	uint32	启动由传送用服务器指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。

表 5-1 完整主机配置文件记录 5.3+ 字段 (续)

字段	数据类型	说明 (Description)
操作系统指纹 (服务器指纹) 数据块 (Operating System Fingerprint (Server Fingerprint) Data Blocks) *	变量	包含用服务器指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明, 请参阅 操作系统指纹数据块 5.1+, 第 4-161 页 。
通用列表块类型 (Generic List Block)	uint32	启动由传送用客户端指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数, 包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (客户端指纹) 数据块 (Operating System Fingerprint (Client Fingerprint) Data Blocks) *	变量	包含用客户端指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明, 请参阅 操作系统指纹数据块 5.1+, 第 4-161 页 。
通用列表块类型 (Generic List Block)	uint32	启动由传送用思科VDB指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数, 包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 1) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 1) Data Blocks) *	变量	包含用思科漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明, 请参阅 操作系统指纹数据块 5.1+, 第 4-161 页 。
通用列表块类型 (Generic List Block)	uint32	启动由传送用思科VDB指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。

表 5-1 完整主机配置文件记录 5.3+ 字段 (续)

字段	数据类型	说明 (Description)
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (VDB) 本机指纹 2) 数据块 (Operating System Fingerprint (VDB) Native Fingerprint 2) Data Blocks) *	变量	包含用思科漏洞数据库 (VDB) 中的指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅 操作系统指纹数据块 5.1+ ，第 4-161 页。
通用列表块类型 (Generic List Block)	uint32	启动由传送用户添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (用户指纹) 数据块 (Operating System Fingerprint (User Fingerprint) Data Blocks) *	变量	包含用户添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅 操作系统指纹数据块 5.1+ ，第 4-161 页。
通用列表块类型 (Generic List Block)	uint32	启动由传送漏洞扫描仪添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (扫描指纹) 数据块 (Operating System Fingerprint (Scan Fingerprint) Data Blocks) *	变量	包含漏洞扫描仪添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅 操作系统指纹数据块 5.1+ ，第 4-161 页。

表 5-1 完整主机配置文件记录 5.3+ 字段 (续)

字段	数据类型	说明 (Description)
通用列表块类型 (Generic List Block)	uint32	启动由传送应用添加的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (应用指纹) 数据块 (Operating System Fingerprint (Application Fingerprint) Data Blocks) *	变量	包含应用添加的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅 操作系统指纹数据块 5.1+ ， 第 4-161 页 。
通用列表块类型 (Generic List Block)	uint32	启动由传送通过指纹冲突解决选择的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (冲突指纹) 数据块 (Operating System Fingerprint (Conflict Fingerprint) Data Blocks) *	变量	包含通过指纹冲突解决选择的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅 操作系统指纹数据块 5.1+ ， 第 4-161 页 。
通用列表块类型 (Generic List Block)	uint32	启动由传送移动设备指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (移动) 数据块 (Operating System Fingerprint (Mobile) Data Blocks) *	变量	包含移动设备主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明，请参阅 操作系统指纹数据块 5.1+ ， 第 4-161 页 。

表 5-1 完整主机配置文件记录 5.3+ 字段 (续)

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

表 5-1 完整主机配置文件记录 5.3+ 字段 (续)

字段	数据类型	说明 (Description)
操作系统指纹 (IPv6 DHCP) 数据块 (Operating System Fingerprint (IPv6 DHCP) Data Blocks) *	变量	包含用 IPv6 DHCP 指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明, 请参阅 操作系统指纹数据块 5.1+, 第 4-161 页 。
通用列表块类型 (Generic List Block)	uint32	启动由传送用户代理指纹识别的指纹数据的操作系统指纹数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数, 包括列表报头以及所有封装操作系统指纹数据块。
操作系统指纹 (用户代理) 数据块 (Operating System Fingerprint (User Agent) Data Blocks) *	变量	包含用用户代理指纹识别的主机上的操作系统相关信息的操作系统指纹数据块。有关此数据块的说明, 请参阅 操作系统指纹数据块 5.1+, 第 4-161 页 。
列表块类型 (List Block Type)	uint32	启动由传送 TCP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节, 加上所有封装完整服务器数据块的长度。
(TCP) 完整服务器数据块 ((TCP) Full Server Data Blocks) *	变量	传输主机上的 TCP 有关此数据块的说明, 请参阅 完整主机服务器数据块 4.10.0+, 第 4-141 页 。
列表块类型 (List Block Type)	uint32	启动由传送 UDP 服务数据的完整服务器数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节, 加上所有封装完整服务器数据块的长度。
(UDP) 完整服务器数据块 ((UDP) Full Server Data Blocks) *	变量	传输主机上的 UDP 子服务器相关数据的完整主机数据块列表。有关此数据块的说明, 请参阅 完整主机服务器数据块 4.10.0+, 第 4-141 页 。

表 5-1 完整主机配置文件记录 5.3+ 字段 (续)

字段	数据类型	说明 (Description)
列表块类型 (List Block Type)	uint32	启动由传送网络协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
(网络) 协议数据块 ((Network) Protocol Data Blocks) *	变量	传输主机上的网络协议相关数据的协议数据块列表。有关此数据块的说明，请参阅 协议数据块，第 4-72 页 。
列表块类型 (List Block Type)	uint32	启动由传送传输协议数据的协议数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数。此字节数包括列表块类型和长度字段的八个字节，加上所有封装协议数据块的长度。
(传输) 协议数据块 ((Transport) Protocol Data Blocks) *	变量	传送主机上的传输协议相关数据的协议数据块列表。有关此数据块的说明，请参阅 协议数据块，第 4-72 页 。
列表块类型 (List Block Type)	uint32	启动包含主机 MAC 地址数据块的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表中的字节数，包括列表报头以及所有封装主机 MAC 地址数据块。
主机 MAC 地址数据块 (Host MAC Address Data Blocks) *	变量	主机 MAC 地址数据块列表。有关此数据块的说明，请参阅 主机 MAC 地址 4.9+ ，第 4-113 页。
上次查看时间 (Last Seen)	uint32	表示系统上次检测到主机活动的 UNIX 时间戳。
主机类型 (Host Type)	uint32	表示主机类型。值包括： <ul style="list-style-type: none"> ▪ 0 - 主机 ▪ 1 - 路由器 ▪ 2 - 网桥 ▪ 3 - NAT (网络地址转换设备) ▪ 4 - LB (负载均衡器)
业务临界点 (Business Criticality)	uint16	表示主机到业务的临界点。

表 5-1 完整主机配置文件记录 5.3+ 字段 (续)

字段	数据类型	说明 (Description)
VLAN ID	uint16	表示主机所属 VLAN 的 VLAN 标识号。
VLAN 类型 (VLAN Type)	uint8	VLAN 标签中封装的数据包类型。
VLAN 优先级 (VLAN Priority)	uint8	VLAN 标签中包含的优先级值。
通用列表块类型 (Generic List Block)	uint32	启动由传送客户端应用数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装客户端应用数据块。
完整主机客户端应用数据块 (Full Host Client Application Data Blocks) *	变量	客户端应用数据块列表。有关此数据块的说明，请参阅 完整主机客户端应用数据块 5.0+，第 4-155 页 。
字符串块类型 (String Block Type)	uint32	启动主机 NetBIOS 名称的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上 NetBIOS 名称字符串中的字节数。
NetBIOS 名称 (NetBIOS Name)	字符串	主机 NetBIOS 名称字符串。
字符串块类型 (String Block Type)	uint32	启动主机注释的字符串数据块。值始终为 0。
字符串块长度 (String Block Length)	uint32	注释字符串数据块中的字节数，包括字符串块类型和长度字段的八个字节，加上注释字符串中的字节数。
说明 (Description)	字符串	包含主机的主机属性注释的内容。
通用列表块类型 (Generic List Block)	uint32	启动由传送 VDB 漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表报头以及所有封装数据块。

表 5-1 完整主机配置文件记录 5.3+ 字段 (续)

字段	数据类型	说明 (Description)
(VDB) 主机漏洞数据块 ((VDB) Host Vulnerability Data Blocks) *	变量	在思科漏洞数据库 (VDB) 中识别的漏洞的主机漏洞数据块列表。有关此数据块的说明, 请参阅 主机漏洞数据块4.9.0+ , 第 4-111页。
通用列表块类型 (Generic List Block)	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数, 包括列表报头以及所有封装数据块。
(第三方/VDB) 主机漏洞数据块 ((Third Party/VDB) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪且包含已收录到思科漏洞数据库 (VDB) 中的主机漏洞的相关信息的主机漏洞数据块。有关此数据块的说明, 请参阅 主机漏洞数据块 4.9.0+ , 第 4-111 页。
通用列表块类型 (Generic List Block)	uint32	启动由传送第三方扫描漏洞数据的主机漏洞数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数, 包括列表报头以及所有封装数据块。
(第三方扫描) 主机漏洞数据块 ((Third Party Scan) Host Vulnerability Data Blocks) *	变量	源自第三方扫描仪的主机漏洞数据块。请注意, 这些数据块的主机漏洞 ID 为第三方扫描仪 ID, 而不是思科检测到的 ID。有关此数据块的说明, 请参阅 主机漏洞数据块 4.9.0+ , 第 4-111 页。
列表块类型 (List Block Type)	uint32	启动由传送属性数据的属性值数据块组成的列表数据块。值始终为 11。
列表块长度 (List Block Length)	uint32	列表数据块中的字节数, 包括列表报头以及所有封装数据块。
属性值数据块 (Attribute Value Data Blocks) *	变量	属性值数据块列表。有关此列表中的数据块的说明, 请参阅 属性值数据块, 第 4-79 页 。
移动 (Mobile)	uint8	指示操作系统是否在移动设备上运行的一个真假标志。

表 5-1 完整主机配置文件记录 5.3+ 字段 (续)

字段	数据类型	说明 (Description)
Jailbroken	uint8	指示移动设备操作系统是否被越狱的一个真假标志。
通用列表块类型 (Generic List Block)	uint32	表示由 IOC 状态数据块组成的通用列表数据块。值始终为 31。
通用列表块长度 (Generic List Block Length)	uint32	通用列表数据块中的字节数，包括列表标头以及所有封装 IOC 状态数据块。
IOC 状态数据块 (IOC State Data Blocks) *	变量	包含主机存在的威胁的相关信息的 IOC 状态数据块。有关此数据块的说明，请参阅 用于 5.3+ 的 IOC 状态数据块 ，第 4-33 页。

当地语言翻译版本说明

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