了解安全Web设备访问日志

目录

简介

先决条件

- 要求
- 使用的组件

访问日志结构

- 纪元时间
- 运行时间
- 源 IP 地址
- 事务结果代码
- HTTP响应代码
- 已转移的总大小
- HTTP 方法
- 目的地
- 用户名和身份验证领域
- 访问类型
- 服务器地址
- MIME内容类型/子类型
- ACL决策标记
- 策略名称
- 身份策略
- 数据安全策略组
- 外部DLP策略组
- 路由策略组
- Web流量分接头
- URL类别缩写
- Web声誉得分
- Webroot扫描
- McAfee扫描
- Sophos扫描
- 思科数据安全扫描判定
- 外部DLP扫描判定
- 预定义的URL类别判定
- URL类别判定
- 统一入站DVS判定
- Web信誉过滤器威胁类型
- Google翻译封装的URL
- 应用控制(AVC/ADC)
- 安全浏览判定

平均带宽
带宽限制控制
用户类型
出站恶意软件扫描
高级恶意软件保护
存档扫描
Web轻触
YouTube URL类别
HTTP响应代码
ACL决策标记
恶意软件扫描判定值
相关内容

简介

本文档介绍安全网络设备(SWA)访问日志的结构。

先决条件

要求

建议掌握下列主题的相关知识：

- 访问SWA的命令行界面(CLI)。
- 对SWA的管理访问。
- 基本了解SWA工作流程。

使用的组件

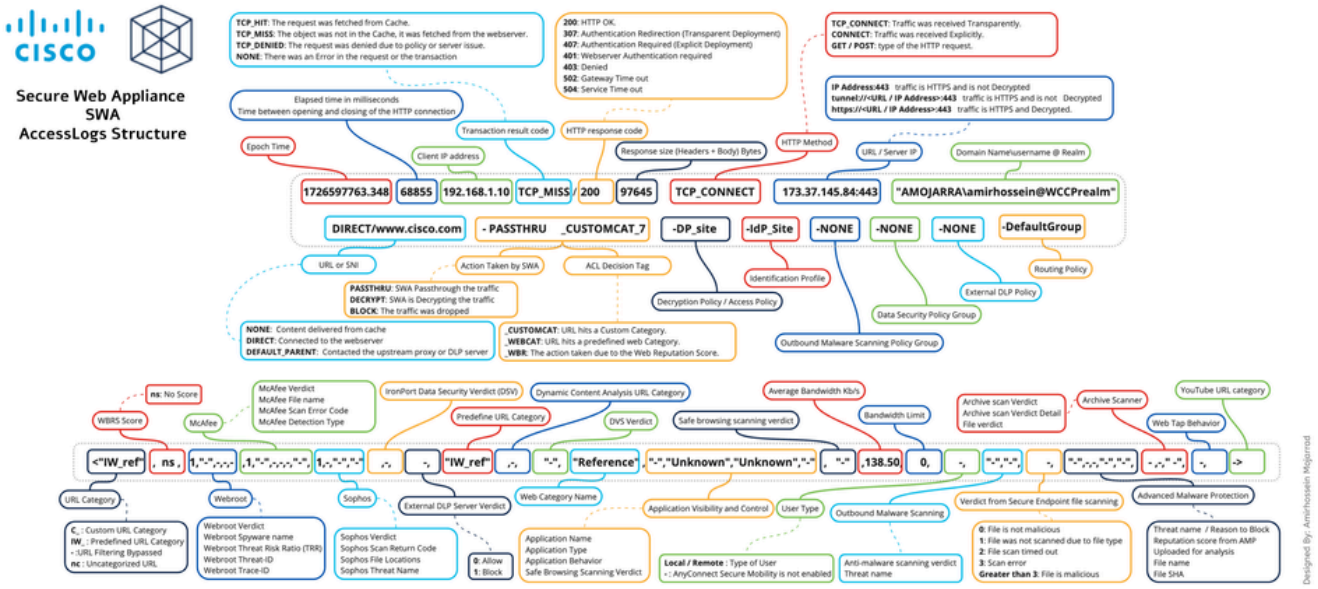
本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

访问日志结构

本文中的访问日志结构通过此示例进行说明：

```
1726597763.348 68855 192.168.1.10 TCP_MISS/200 97645 TCP_CONNECT 10.37.145.84:443 "AMOJARRA\amirhossein
```



图像 — 访问日志结构

注意：访问日志的结构取决于SWA的版本。每个Accesslog文件的开头都有一行显示其结构和格式说明符的顺序。

部分	AccessLog示例	格式说明符	详细信息
纪元时间	1726597763.348	%t	纪元时间（通常称为Unix时间或POSIX时系统，它通过计算自1970年1月1日00:00:秒数（或毫秒/微秒） 交易完成的纪元时间。 可以通过在线Epoch时间转换器或任何Lin
运行时间	68855	%e	请求完成/中止和连接关闭之前所花费的毫

源 IP 地址	192.168.1.10	%a	客户端/源IP地址。
事务结果代码	TCP_MISS	%w	事务结果代码指示SWA如何解析客户端请 以下是事务结果代码列表： TCP_HIT TCP_IMS_HIT TCP_MEM_HIT TCP_MISS TCP_REFRESH_HIT TCP_CLIENT_REFRESH_MISS

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>TCP_DENIED</td></tr>
<tr><td>TCP_DENIED_SSL HTTPS</td></tr>
<tr><td>TCP_CLIENT_REFRESH_MISS_SSL</td></tr>
<tr><td>TCP_MISS_SSL HTTPS</td></tr>
</table>
</td></tr>
<tr><td>HTTP响应代码</td><td>/200</td><td>%h</td><td>
HTTP响应代码表示Web服务器响应客户端
代码。

下面是最重要的HTTP响应代码列表，（有
本文的HTTP响应代码部分）
<table>
<tr><td>状态代码</td><td>含义</td></tr>
<tr><td>000</td><td>如果通信在TLS阶段或数据传输
非标准响应代码。</td></tr>
<tr><td>2xx成功</td><td></td></tr>
<tr><td>200</td><td>确定</td></tr>
<tr><td>204</td><td>无内容</td></tr>
<tr><td>206</td><td>部分内容（也称为范围请求）</td></tr>
<tr><td></td><td></td></tr>
<tr><td>3xx重定向</td><td></td></tr>
<tr><td>301</td><td>永久重定向。</td></tr>
<tr><td>302</td><td>临时重定向</td></tr>
<tr><td>304</td><td>未修改</td></tr>
<tr><td>307</td><td>用于身份验证的临时重定向

（通常在SWA对用户进行身份验
到）</td></tr>
<tr><td></td><td></td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td>
<table>
<tr><td>4xx客户端错误</td><td></td></tr>
<tr><td>400</td><td>错误的请求</td></tr>
<tr><td>401</td><td>需要Web服务器身份验证（通常份验证时在透明部署中看到）</td></tr>
<tr><td>403</td><td>已禁止</td></tr>
<tr><td>404</td><td>找不到</td></tr>
<tr><td>407</td><td>需要显式代理身份验证</td></tr>
<tr><td></td><td></td></tr>
<tr><td>5xx服务器错误</td><td></td></tr>
<tr><td>500</td><td>内部服务器错误</td></tr>
<tr><td>502</td><td>错误的网关</td></tr>
<tr><td>503</td><td>服务不可用</td></tr>
<tr><td>504</td><td>网关超时</td></tr>
</table>
</td></tr>
<tr><td>已转移的总大小</td><td>97645</td><td>%s</td><td>请求的传输字节总数。</td></tr>
<tr><td>HTTP 方法</td><td>TCP_CONNECT</td><td>%1r</td><td>HTTP方法是一种标准化的方法，客户端可对资源执行的所需操作，例如使用GET检交数据。
<table>
<tr><td>GET</td><td>HTTP GET方法用。它仅用于检索信文。简单地说，G</td></tr>
<tr><td>POST</td><td>HTTP POST方法务器，通常包含有用于提交表单、上务器状态的数据。</td></tr>
<tr><td>连接</td><td>HTTP CONNECT务器建立隧道，允服务器的直接TC HTTPS流量，以信。</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td></td><td>表示SWA明确接
户端配置为直接</td></tr>
<tr><td>TCP_CONNECT</td><td>表示SWA透明地
WCCP或第4层重</td></tr>
</table></td></tr>
<tr><td>目的地</td><td>10.37.145.84:443</td><td>%2r</td><td>此部分显示目标服务器URL和TCP端口号

在透明重定向中，在流量解密之前，SWA
号。

如果URL以tunnel:// 开头，则表示SWA尚

如果URL以https://开头，则表示SWA解密</td></tr>
<tr><td>用户名和身份验证领域</td><td>AMOJARRA\amirhossein@WCCPrealm</td><td>%A</td><td>用于此连接的凭证。

如果请求获得身份验证，SWA会将用户名
：

<Domain Name> \ <User Name> @ <Au
Name>

如果请求尚未进行身份验证或免于身份验
到连字符“ — ”</td></tr>
<tr><td>访问类型</td><td>直接/</td><td>%H</td><td>用于描述为检索请求内容联系了哪台服务

最常见的值包括：
<table>
<tr><td>NONE</td><td>Web代理具有内容，
他服务器来检索内容</td></tr>
<tr><td>直接</td><td>Web代理转到请求中
内容。</td></tr>
<tr><td>DEFAULT_PARENT</td><td>Web代理转到其主要
丢失(DLP)服务器以</td></tr>
</table></td></tr>
<tr><td>服务器地址</td><td>www.cisco.com</td><td>%d</td><td>数据源或服务器IP地址。</td></tr>
</table>

<table>
<tr>
<td>MIME内容类型/子类型</td>
<td>-</td>
<td>%c</td>
<td>多用途Internet邮件扩展(MIME)指示文档质和格式。MIME类型在IETF RFC 6838中

对于默认类型的角色，两种主要MIME类型

• text/plain是文本文件的默认值。文本的，不能包含二进制数据。
• application/octet-stream是所有其它件类型必须使用此类型。在处理这些别小心地保护用户免受软件漏洞和可。

要获取MIME类型的完整列表，请访问：媒</td>
</tr>
<tr>
<td>ACL决策标记</td>
<td>PASSTHRU_CUSTOMCAT_7-</td>
<td>%D</td>
<td>ACL决策标记是访问日志条目中的一个字处理事务。它包括来自Web信誉过滤器、信息。

注意:ACL决策标记的末尾包含一个动，Web代理在内部使用该数字来提高号码。

下面列出了最重要的ACL决策标记。（有文的ACL决策标记部分）

ACL决策标记

ALLOW_CUSTOMCAT

允许_WBRS

AMP_FILE_VERDICT

BLOCKADMIN</td>
</tr>
</table>

			BLOCK_ADMIN_CONNECT
			BLOCK_ADMIN_CUSTOM_USER_AGE
			BLOCK_ADMIN_TUNNELING
			BLOCK_ADMIN_FILE_TYPE
			BLOCK_ADMIN_PROTOCOL
			BLOCK_AMP_RESP
			块_AVC
			BLOCK_CONTENT_UNSAFE
			BLOCK_CUSTOMCAT
			BLOCK_ICAP
			BLOCK_WBR

			BLOCK_WEBCAT
			BLOCK_TYPE
			DECRYPT_ADMIN
			DECRYPT_EUN_CUSTOMCAT
			DECRYPT_EUN_WBRS
			DECRYPT_EUN_WEBCAT
			DECRYPT_WEBCAT
			DECRYPT_WBRS
			DROP_ADMIN
			DROP_WEBCAT
			DROP_WBRS

			PASSTHRU_ADMIN PASSTHRU_WEBCAT PASSTHRU_WBRS OTHER（其他）
策略名称	DP站点 —	不适用	根据流量的类型，这显示： • 解密策略名称:如果流量为HTTPS且 • 访问策略名称:如果流量是HTTP或已
身份策略	IdP_Site-	不适用	显示标识配置文件名称
出站恶意软件扫描策略组	NONE-	不适用	出站恶意软件扫描策略组名称。 策略组名称中的任何空格都替换为下划线
数据安全策略组	NONE-	不适用	思科数据安全策略组名称。当事务与全局 时，此值为DefaultGroup。仅当启用思科 会显示此策略组名称。未应用数据安全策 策略组名称中的任何空格都替换为下划线
外部DLP策略组	NONE-	不适用	当事务与全局外部DLP策略匹配时，此值 未应用外部DLP策略，则显示NONE。 策略组名称中的任何空格都替换为下划线
路由策略组	默认组 —	不适用	路由策略组名称ProxyGroupName/ProxyS 当事务与全局路由策略匹配时，此值为De

<table>
<tr><td></td><td></td><td></td><td>用上游代理服务器时，此值为DIRECT
策略组名中的任何空格都替换为下划线(_)</td></tr>
<tr><td>Web流量分接头</td><td>NONE</td><td>不适用</td><td>Web流量轻触策略名称。</td></tr>
<tr><td>URL类别缩写</td><td><"C_Cisc",</td><td>%XC</td><td>请求匹配的URL类别。<table><tr><td>-</td><td>绕过URL过滤</td></tr><tr><td>NC</td><td>未分类的URL</td></tr><tr><td>错误</td><td>绕过URL过滤</td></tr><tr><td>IMP</td><td>不可能</td></tr><tr><td>IW_</td><td>如果类别名称以IW_开头，则
求命中思科预定义URL类别</td></tr><tr><td>C_</td><td>如果类别名称以IC_开头，则
求进入自定义URL类别</td></tr></table></td></tr>
<tr><td>Web声誉得分</td><td>-,</td><td>%XW</td><td>此字段显示Web信誉(WBRS)得分。
ns表示URL没有分数。</td></tr>
<tr><td>Webroot扫描</td><td>-,"-",-,-,-,-</td><td></td><td>这5个字段与Webroot扫描相关<table><tr><td>Webroot判定，</td><td>%Xv</td><td>恶意软件
到DVS引
Webroot
有关判定
访问本文
定值。</td></tr></table></td></tr>
</table>

			Webroot Spyname、	%Xn	与对象关。仅适用应。
			Webroot TRR、	%Xt	与威胁风Webroot软件存在Webroot
			Webroot ThreatID、	%X	Webroot思科客户时使用此Webroot
			Webroot TraceID、	%Xi	Webroot思科客户时使用此Webroot
McAfee扫描	-,"-",-,-,-,"-",		这6个字段与McAfee扫描相关。		
			McAfee判定，	%Xd	恶意软件到DVS引McAfee检 有关判定访问本文定值。
			McAfee文件名，	"%Xe"	McAfee扫适用于M
			McAfee扫描错误代码，	%Xf	McAfee用科客户支使用此值测到的响
			McAfee检测类型、	%Xg	McAfee用科客户支使用此值测到的响

<table>
<tr><td></td><td></td><td></td><td><table>
<tr><td>McAfee病毒类型
、</td><td>%Xh</td><td>McAfee
科客户支
使用此值
测到的响</td></tr>
<tr><td>McAfee病毒名称
、</td><td>%Xj"</td><td>McAfee
适用于M</td></tr>
</table></td></tr>
<tr><td>Sophos扫描</td><td>-,-,"-","-",</td><td></td><td>这4个字段与Sophos扫描相关<table>
<tr><td>Sophos判定，</td><td>%XY</td><td>恶意软件
到DVS引
Sophos检

有关判定
访问本文
定值。</td></tr>
<tr><td>Sophos扫描返回
代码，</td><td>%Xx</td><td>Sophos
。思科客
障时使用
Sophos检</td></tr>
<tr><td>Sophos文件位置
，</td><td>"%Xy"</td><td>Sophos
文件的名
Sophos检</td></tr>
<tr><td>Sophos威胁名称
、</td><td>"%Xz"</td><td>Sophos
科客户支
使用此值
测到的响</td></tr>
</table></td></tr>
<tr><td>思科数据安全扫描判定</td><td>-,</td><td>%Xl</td><td>思科数据安全扫描判定基于思科数据安全
。

此列表说明此字段的可能值：

0.允许

1.阻止

—（连字符）。思科数据安全过滤器未启</td></tr>
</table>

			据安全过滤器被禁用或URL类别操作被设，显示此值。
外部DLP扫描判定	-,	%Xp	外部DLP扫描判定基于互联网内容自适应的结果。 此列表说明此字段的可能值： 0.允许 1.阻止 —（连字符）。外部DLP服务器未启动任描被禁用时，或者由于“外部DLP策略”(Ex Policies)>“目标”(Destinations)页面上的免容时，显示此值。
预定义的URL类别判定	"-",	%XQ	在请求端扫描期间确定的预定义URL类别 当URL过滤被禁用时，此字段会列出连字 如果请求符合自定义URL类别，您仍然可定义的URL类别名称，但决定是由自定义 有关URL类别缩写的列表，请参阅URL类
URL类别判定	-,	%XA	动态内容分析(DCA)引擎在响应端扫描期间，缩写。 仅适用于思科网络使用控制URL过滤引擎 nc:当启用动态内容分析引擎且请求时未分显示在请求端扫描裁决中，这表示在响应前，URL在初始请求阶段未分类
统一入站DVS判定	"-",	%XZ	统一响应端防恶意软件扫描判定，提供独意软件类别。适用于由于服务器响应扫描务。
Web信誉过滤器威胁类型	"-",	%Xk	Category Name或Threat Type由Web信誉Web信誉较高时，返回Category Name；Threat Type。 通常情况下，此字段填充的是信誉为–4及

<table>
<tr><td>Google翻译封装的URL</td><td>"-",</td><td>%X#10#</td><td>封装在Google翻译引擎中的URL。如果没值为-。</td></tr>
<tr><td>应用控制(AVC/ADC)</td><td>"-","-","-",</td><td></td><td>在这三个字段中，记录应用可视性与可控控制(ADC)的统计信息。<table><tr><td>AVC/ADC应用名称</td><td>"%XO"</td><td>由AVC或ADC引称（如果适用）ADC引擎时适用</td></tr><tr><td>AVC/ADC应用类型</td><td>"%Xu"</td><td>AVC或ADC引擎果适用）。仅在时适用。</td></tr><tr><td>AVC/ADC应用行为</td><td>%Xb</td><td>AVC或ADC引擎果适用）。仅在时适用。
对于AVC_，对</td></tr></table></td></tr>
<tr><td>安全浏览判定</td><td>"-",</td><td>%XS</td><td>此值指示是否已将安全搜索或网站内容分<table><tr><td>ensrch</td><td>原始客户端请求不安全，并且已应</td></tr><tr><td>encrt</td><td>原始客户端请求不安全，并且已应。</td></tr><tr><td>unsupp</td><td>原始客户端请求被发送到不受支持</td></tr><tr><td>错误</td><td>原始客户端请求不安全，但是由于搜索和网站内容分级功能。</td></tr><tr><td>-</td><td>安全搜索和站点内容分级功能均未，因为功能被绕过（例如，事务在许），或者请求来自不受支持的应</td></tr></table></td></tr>
<tr><td>平均带宽</td><td>11.35,</td><td>%XB</td><td>为请求提供服务所消耗的平均带宽（以Kb</td></tr>
</table>

<table>
<tr><td>带宽限制控制</td><td>0,</td><td>%XT</td><td>一个值，指示请求是否由于带宽限制控制
“1”表示请求已限制。
0表示请求未受限制。</td></tr>
<tr><td>用户类型</td><td>-,</td><td>%I</td><td>发出请求的用户的类型，[Local]或[Remot
仅在启用AnyConnect安全移动时适用。
未启用时，值为连字符(-)</td></tr>
<tr><td>出站恶意软件扫描</td><td>"-","-",</td><td></td><td>这2个字段适用于因应用出站恶意软件扫描而被阻止或受监控的事务。
<table>
<tr><td>统一出站DVS判定</td><td>"%X3"</td><td>统一请求端，与启用哎用于在应用略时由于客止或受监控</td></tr>
<tr><td>出站威胁名称</td><td>%X4</td><td>分配给因适描策略而被请求的威胁
此威胁名称软件扫描引</td></tr>
</table></td></tr>
<tr><td>高级恶意软件保护</td><td>-,"-",-,-"-","-",</td><td></td><td>以下6个字段与安全终端（也称为高级恶意
<table>
<tr><td>文件判定</td><td>%X#1#</td><td>安：
0:
1:扫
2:
3:
[4是</td></tr>
</table></td></tr>
</table>

			威胁名称	%X#2#	威 件 “-”
			信誉得分	%X#3#	来 信 务 定
			用于分析的上传操作	%X#4#	上 0表 传 1表 传
			文件名	%X#5#	正 名
			文件SHA	%X#6#	此 。
存档扫描	-、-、"-",		以下3个字段指示存档文件扫描的状态：		
			存档扫描判定	%X#7#	存档扫描判定。 ARCHIVESCAN_ALLCLEAR ARCHIVESCAN_BLOCKEDF

					ARCHIVESCAN_NESTEDTO
					ARCHIVESCAN_UNKNOWNI
					ARCHIVESCAN_UNSCANAB
					ARCHIVESCAN_FILETOOBI

			存档扫描判定详细信息	%Xd	存档扫描判定详细信息。如果检查的存档文件(ARCHIVESCAN_BLOCKEDF Objects Blocking设置，此Verd止文件的类型和被阻止文件的各 UnScanable Archive-Blocked或任何被阻止的文件类型。
			文件判定	%Xm	存档扫描程序的文件判定
Web轻触	-,	%XU	Web点击行为。		
YouTube URL类别	- >	%X#29#	分配给事务的YouTube URL类别（缩写）分配类别）。		

HTTP响应代码

以下是HTTP响应代码的完整列表

状态代码	含义
1xx信息	
100	继续
101	交换协议
102	处理
103	早期提示
2xx成功	
200	确定

201	已创建
202	已接受
203	非授权信息
204	无内容
205	重置内容
206	部分内容
207	多状态
208	已报告
226	已使用IM
3xx重定向	
300	多种选择
301	永久移动
302	已找到（以前称为“临时移动”）
303	查看其他
304	未修改
305	使用代理
306	交换机代理
307	用于身份验证的临时重定向 （通常在SWA对用户进行身份验证时的透明部署中看到）
308	永久重定向
4xx客户端错误	
400	错误的请求
401	需要Web服务器身份验证（通常在SWA对用户进行身份验证时在透明部署中看到）
402	需要付款
403	已禁止
404	找不到
405	不允许的方法
406	不可接受

407	需要显式代理身份验证
408	请求超时
409	冲突
410	消失
411	所需长度
412	预处理失败
413	负载过大
414	URI过长
415	不支持的媒体类型
416	范围无法满足
417	预期失败
418	我是茶壶
421	错误请求
422	无法处理的实体
423	已锁定
424	失败的依赖关系
425	太早
426	所需的升级
428	需要前提条件
429	请求过多
431	请求报头字段太大
451	因法律原因不可用
5xx服务器错误	
500	内部服务器错误
501	未实施
502	错误的网关
503	服务不可用
504	网关超时
505	不支持HTTP版本

506	变体也进行协商
507	存储空间不足
508	检测到环路
510	未扩展
511	需要网络身份验证

ACL决策标记

以下是ACL决策标记的完整列表：

ACL决策标记	描述
ALLOW_ADMIN_ERROR_PAGE	Web代理允许事务进入通知页面以及在该页面使用的任何徽标。
ALLOW_CUSTOMCAT	Web代理基于访问策略组的自定义URL类别过设置允许事务。
ALLOW_REFERENCE	Web代理允许基于嵌入式/引用内容豁免的事务
允许_WBRS	Web代理基于访问策略组的Web信誉过滤器设允许事务。
AMP_FILE_VERDICT	表示来自AMP信誉服务器的文件判定的值：
	1 — 未知
	2 — 清洁
	3 — 恶意
	4 — 不可扫描
ARCHIVESCAN_ALLCLEAR	存档扫描判定
ARCHIVESCAN_BLOCKEDFILETYPE	ARCHIVESCAN_ALLCLEAR — 检查的存档中

	有阻止的文件类型。
ARCHIVESCAN_NESTEDTOODEEP	ARCHIVESCAN_BLOCKEDFILETYPE — 检 的存档中存在受阻止的文件类型。日志条目中 下一个字段（判定详细信息）提供详细信息， 其是被阻止文件的类型和被阻止文件的名称。
ARCHIVESCAN_UNKNOWNFMT	ARCHIVESCAN_NESTEDTOODEEP — 存档 阻止，因为它包含的“封装”或嵌套的存档数多于 配置的最大数量。Verdict Detail字段包含“Un- Scanable Archive-Blocked”。
ARCHIVESCAN_UNSCANABLE	ARCHIVESCAN_UNKNOWNFMT — 存档被阻 止，因为它包含未知格式的文件类型。判定详 信息为“Un-Scannable Archive-Blocked”。
ARCHIVESCAN_FILETOOBIG	ARCHIVESCAN_UNSCANABLE — 存档被阻 ，因为它包含无法扫描的文件。判定详细信息 “Un-Scannable Archive-Blocked”。
	ARCHIVESCAN_FILETOOBIG — 存档被阻止 ，因为存档大小大于配置的最大值。判定详细 息为“UnScannable Archive-Blocked”。
	存档扫描判定详细信息。
	日志条目中的字段和Verdict字段提供有关裁决 其他信息，例如受阻文件类型和受阻文件的名 、“无法扫描的存档受阻”或“ — ”以指示存档不 含任何受阻文件类型。
	例如，如果根据访问策略阻止了可检查的存档 件 (ARCHIVESCAN_BLOCKEDFILETYPE):Cus Objects Blocking设置，Verdict Detail条目包括 阻止文件的类型和被阻止文件的名称。
	请参阅访问策略：Blocking Objects and Archi Inspection Settings以了解有关Archive Inspection的详细信息。

BLOCKADMIN	基于访问策略组的某些默认设置阻止的事务。
BLOCK_ADMIN_CONNECT	根据访问策略组的HTTP CONNECT Ports设置定义的目标TCP端口阻止的事务。
BLOCK_ADMIN_CUSTOM_USER_AGENT	根据访问策略组的Block Custom User Agents置中定义的用户代理阻止的事务。
BLOCK_ADMIN_TUNNELING	Web代理基于访问策略组的HTTP端口上的非HTTP流量的隧道阻止了事务。
BLOCK_ADMIN_HTTPS_NonLocalDestination	事务被阻止；客户端尝试使用SSL端口作为显代理绕过身份验证。为防止这种情况，如果SSL连接是与SWA本身，则仅允许对实际SW定向主机名的请求。
BLOCK_ADMIN_IDS	根据数据安全策略组中定义的请求正文内容的MIME类型阻止的事务。
BLOCK_ADMIN_FILE_TYPE	根据访问策略组中定义的文件类型阻止的事务
BLOCK_ADMIN_PROTOCOL	根据访问策略组的Block Protocols设置中定义协议阻止的事务。
BLOCK_ADMIN_SIZE	根据访问策略组的对象大小设置中定义的响应小阻止的事务。
BLOCK_ADMIN_SIZE_IDS	根据数据安全策略组中定义的请求正文内容的小阻止的事务。
BLOCK_AMP_RESP	Web代理基于访问策略组的高级恶意软件防护置阻止了响应。
BLOCK_AMW_REQ	Web代理基于出站恶意软件扫描策略组的防恶软件设置阻止了请求。请求正文生成了正恶意件判定。
BLOCK_AMW_RESP	Web代理基于访问策略组的防恶意软件设置阻

	了响应。
BLOCK_AMW_REQ_URL	Web代理怀疑HTTP请求中的URL不安全，因此，它基于访问策略组的防恶意软件设置，在请求时阻止了事务。
块_AVC	根据为访问策略组配置的应用设置阻止的事务
BLOCK_CONTENT_UNSAFE	基于访问策略组的网站内容分级设置阻止的事务。客户端请求用于成人内容，并且策略配置为阻止成人内容。
BLOCK_CONTINUE_CONTENT_UNSAFE	事务已阻止并显示基于Access Policy组中的站点内容分级设置的Warn and Continue页面。客户端请求用于成人内容，并且策略配置为向访问成人内容的用户提供警告。
BLOCK_CONTINUE_CUSTOMCAT	事务被阻止并显示“警告并继续”(Warn and Continue)页面，该页面基于配置为Warn的“访问策略”(Access Policy)组中的自定义URL类别。
BLOCK_CONTINUE_WEBCAT	事务被阻止并显示“警告并继续”(Warn and Continue)页面，该页面基于配置为Warn的“访问策略”(Access Policy)组中的预定义URL类别。
BLOCK_CUSTOMCAT	基于访问策略组的自定义URL类别过滤设置阻止的事务。
BLOCK_ICAP	Web代理根据外部DLP策略组中定义的外部DLP系统的判定阻止了请求。
BLOCK_SEARCH_UNSAFE	客户端请求包含不安全的搜索查询，并且访问策略配置为强制执行安全搜索，因此原始客户端请求被阻止。
BLOCK_SUSPECT_USER_AGENT	基于访问策略组的可疑用户代理设置阻止的事务。
BLOCK_UNSUPPORTED_SEARCH_APP	基于访问策略组的安全搜索设置阻止的事务。

	务用于不受支持的搜索引擎，并且策略配置为 止不受支持的搜索引擎。
BLOCK_WBR	基于访问策略组的Web信誉过滤器设置阻止的 务。
BLOCK_WBRS_IDS	Web代理基于数据安全策略组的Web信誉过滤 设置阻止了上传请求。
BLOCK_WEBCAT	基于访问策略组的URL类别过滤设置阻止的事 。
BLOCK_WEBCAT_IDS	Web代理基于数据安全策略组的URL类别过滤 置阻止了上传请求。
BLOCK_TYPE	Web代理基于访问策略组的预定义YouTube类 过滤设置阻止了事务。
BLOCK_CONTINUE_YTCAT	Web代理阻止了事务，并根据配置为Warn的访 策略组中的预定义YouTube类别显示“警告并继 ”页面。
DECRYPT_ADMIN	Web代理基于解密策略组的某些默认设置解密 事务。
DECRYPT_ADMIN_EXPIRED_CERT	Web代理解密了事务，尽管服务器证书已过期
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	启用EUN时，Web代理基于默认设置解密事务 ，作为解密策略组的丢弃连接。
DECRYPT_EUN_ADMIN_EXPIRED_CERT	当HTTPS代理设置丢弃启用了EUN的过期证书 ，Web代理解密了事务。
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	当HTTPS代理设置丢弃启用了EUN的无效枝叶 书时，Web代理解密了事务。
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	当HTTPS代理设置丢弃启用了EUN的不匹配主 名时，Web代理解密了事务。

DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	当HTTPS代理设置丢弃在线证书状态协议(OCSP)，并且启用EUN时出现其他错误时，Web代理解密了事务。
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	当HTTPS代理设置丢弃启用了EUN的OCSP撤证书时，Web代理解密了事务。
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	当HTTPS代理设置丢弃无法识别的根授权或颁者证书（启用EUN）时，Web代理解密了事务
DECRYPT_EUN_CUSTOMCAT	Web代理基于解密策略组的自定义URL类别过设置解密了事务。如果启用EUN，流量将被丢。
DECRYPT_EUN_WBRS	Web代理基于解密策略组的Web信誉过滤器设解密了事务。如果启用EUN，流量将被丢弃。
DECRYPT_EUN_WBRS_NO_SCORE	Web代理基于解密策略组中无分数URL的Web誉过滤器设置解密了事务。如果启用EUN，流将被丢弃。
DECRYPT_EUN_WEBCAT	Web代理基于解密策略组的URL类别过滤设置密了事务。如果启用EUN，流量将被丢弃。
DECRYPT_WEBCAT	Web代理基于解密策略组的URL类别过滤设置密了事务。
DECRYPT_WBRS	Web代理基于解密策略组的Web信誉过滤器设解密了事务。
DEFAULT_CASE	Web代理允许客户端访问服务器，因为所有AsyncOS服务（如Web信誉或防恶意软件扫描）均未对事务执行任何操作。
DENY_ADMIN	Web代理拒绝了该事务。当HTTPS代理设置中要身份验证且禁用Decrypt for Authentication时，HTTPS请求会发生这种情况。
DROP_ADMIN	Web代理基于解密策略组的某些默认设置丢弃

	事务。
DROP_ADMIN_EXPIRED_CERT	由于服务器证书已过期，Web代理丢弃了事务
DROP_WEBCAT	Web代理基于解密策略组的URL类别过滤设置 弃了事务。
DROP_WBRS	Web代理基于解密策略组的Web信誉过滤器设 丢弃了事务。
MONITOR_ADMIN_EXPIRED_CERT	Web代理监控了服务器响应，因为服务器证书 过期。
MONITOR_AMP_RESP	Web代理基于访问策略组的高级恶意软件防护 置监控服务器响应。
MONITOR_AMW_RESP	Web代理基于访问策略组的防恶意软件设置监 服务器响应。
MONITOR_AMW_RESP_URL	Web代理怀疑HTTP请求中的URL不安全，但 基于访问策略组的防恶意软件设置监控事务。
监控_AVC	Web代理基于访问策略组的应用程序设置监控 务。
MONITOR_CONTINUE_CONTENT_UNSAFE	最初，Web代理阻止了事务，并根据“访问策略 ”组中的站点内容分级设置显示“警告并继续”页 。客户端请求用于成人内容，并且策略配置为 访问成人内容的用户提供警告。用户接受警告 继续访问最初请求的站点，随后没有其他扫描 擎阻止该请求。
MONITOR_CONTINUE_CUSTOMCAT	最初，Web代理阻止了事务，并根据配置为“警 ”的访问策略组中的自定义URL类别显示“警告并 继续”页面。 用户接受警告并继续访问最初请求 的站点，随后没有其他扫描引擎阻止该请求。
MONITOR_CONTINUE_WEBCAT	最初，Web代理阻止了事务，并根据配置为 Warn的访问策略组中的预定义URL类别显示“警

	告并继续”页面。用户接受警告并继续访问最初求的站点，而其他扫描引擎随后不会阻止该请。
MONITOR_CONTINUE_TYPE	最初，Web代理阻止了事务，并根据配置为Warn的访问策略组中的预定义YouTube类别显“警告并继续”页面。用户接受警告并继续访问最初请求的站点，随后没有其他扫描引擎阻止该求。
MONITOR_IDS	Web代理使用数据安全策略或外部DLP策略扫上传请求，但未阻止该请求。它根据访问策略估请求。
MONITOR_SUSPECT_USER_AGENT	Web代理基于访问策略组的可疑用户代理设置控事务。
监控_WBRS	Web代理基于访问策略组的Web信誉过滤器设监控事务。
NO授权	Web代理不允许用户访问应用，因为用户已根身份验证领域进行身份验证，但未根据应用身验证策略中配置的任何身份验证领域进行身份证。
NO_PASSWORD	用户身份验证失败。
PASSTHRU_ADMIN	Web代理基于解密策略组的某些默认设置通过事务。
PASSTHRU_ADMIN_EXPIRED_CERT	Web代理通过事务，尽管服务器证书已过期。
PASSTHRU_WEBCAT	Web代理基于解密策略组的URL类别过滤设置过了事务。
PASSTHRU_WBRS	Web代理基于解密策略组的Web信誉过滤器设通过事务。
REDIRECT_CUSTOMCAT	Web代理基于配置为Redirect的Access Policy

	中的自定义URL类别将事务重定向到其他URL
SAAS_AUTH	Web代理允许用户访问应用，因为用户是根据用身份验证策略中配置的身份验证领域进行透身份验证的。
OTHER（其他）	Web代理由于错误（例如授权失败、服务器断连接或客户端中止）未完成请求。

恶意软件扫描判定值

恶意软件扫描判定是分配给URL请求或服务器响应的值，用于确定其中包含恶意软件的概率。Webroot、McAfee和Sophos扫描引擎将恶意软件扫描判定返回到DVS引擎，以便DVS引擎可以确定是监控还是阻止扫描的对象。编辑特定访问策略的Anti-Malware设置时，每个恶意软件扫描判定与Access Policies > Reputation和Anti-Malware Settings页面上列出的恶意软件类别相对应。

此列表显示不同的恶意软件扫描判定值和每个对应的恶意软件类别：

恶意软件扫描判定值	恶意软件类别
-	未设置
0	未知
1	未扫描
2	超时
3	错误
4	不可扫描
10	通用间谍软件
12	浏览器帮助程序对象

恶意软件扫描判定值	恶意软件类别
13	广告软件
14	系统监视器
18	商业系统监控
19	拨号程序
20	劫机者
21	网络钓鱼URL
22	特洛伊木马下载程序
23	特洛伊木马程序
24	特洛伊网络钓鱼程序
25	蠕虫
26	加密文件
27	病毒
33	其他恶意软件
34	PUA
35	已中止
36	病毒爆发启发式算法
37	已知的恶意和高风险文件

相关内容

- 思科安全Web设备AsyncOS 15.2用户指南
- 使用安全Web设备最佳实践
- 确保VMware环境中适当的虚拟WSA HA组功能
- 配置访问日志中的性能参数
- 了解安全Web设备中的HTTPS访问日志格式
- 访问安全Web设备日志

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。