瞭解安全Web裝置訪問日誌

目錄

簡介

本檔案將說明安全Web裝置(SWA)訪問日誌的結構。

必要條件

需求

思科建議瞭解以下主題：

- 訪問SWA的命令列介面(Command Line Interface, CLI)。

- 對SWA的管理訪問。
- 對SWA工作流程有基礎認識。

採用元件

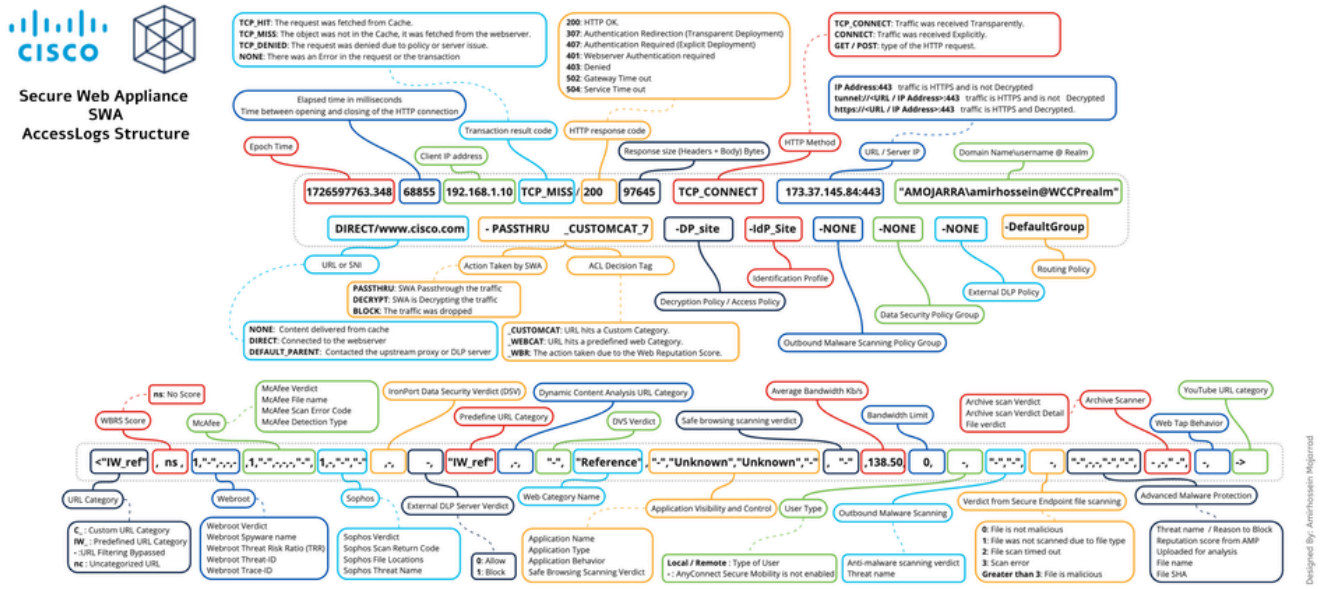
本文件所述內容不限於特定軟體和硬體版本。

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

訪問日誌結構

在此示例中，對Accesslog結構進行了說明：

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



影象 — 訪問日誌結構

附註：訪問日誌的結構取決於SWA的版本。每個Accesslog檔案的開頭都有一行顯示其結構和格式說明符的順序。

截面	Accesslog示例	格式說明符	詳細資料
紀元時間	1726597763.348	%t	紀元時間（通常稱為Unix時間或POSIX時間）是廣泛使用的系統，它通過計算從1970年1月1日00:00:00 UTC開始的總秒數（或毫秒/微秒）來跟蹤時間 交易完成的紀元時間。 可以通過線上Epoch時間轉換器或任何li
已用時間	68855	%e	請求在完成/中止和連線關閉之前花費的

源IP地址	192.168.1.10	%a	客戶端/源IP地址。
交易結果代碼	TCP_MISS	%w	事務結果代碼指示SWA如何解析客戶端 以下是事務結果代碼清單： 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></td></tr>
<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響應代碼</td><td>/200</td><td>%h</td><td>HTTP響應代碼表示Web伺服器響應客戶
態代碼。

以下是最重要的HTTP響應代碼清單，(有
文的HTTP響應代碼部分)
<table>
<tr><td>狀態代碼</td><td>含義</td></tr>
<tr><td>000</td><td>000是非標準響應代碼，如果在
間通訊中斷。</td></tr>
<tr><td>2xx成功</td><td></td></tr>
<tr><td>200</td><td>確定</td></tr>
<tr><td>204</td><td>無內容</td></tr>
<tr><td>206</td><td>部分內容（也稱為範圍請求）</td></tr>
<tr><td></td><td></td></tr>
<tr><td>3xx重新導向</td><td></td></tr>
<tr><td>301</td><td>永久重新導向。</td></tr>
<tr><td>302</td><td>臨時重新導向</td></tr>
<tr><td>304</td><td>未修改</td></tr>
<tr><td>307</td><td>用於身份驗證的臨時重定向</td></tr>
</table>
</td></tr>
</table>

			（通常在SWA對使用者進行身 看到）
		4xx客戶端錯誤	
		400	錯誤的請求
		401	需要Web伺服器身份驗證（通 身份驗證時在透明部署中出現
		403	禁止
		404	未找到
		407	需要顯式代理身份驗證
		5xx伺服器錯誤	
		500	內部伺服器錯誤
		502	錯誤的網關
		503	服務不可用
		504	網關超時
已轉移的總大小	97645	%s	請求的總傳輸位元組數。
HTTP方法	TCP_CONNECT	%1r	HTTP方法是一種標準化的方法，用於客 在資源上執行的所需操作，例如使用GE POST提交資料。
			GET：HTTP GET方法。它專門用於檢正文。簡單地訴
			POST：HTTP POST方服器，通常包含用於提交表單、服器狀態的資料
			CONNECT：HTTP CONNEC

			理伺服器的隧道 標伺服器的直接 HTTPS流量以后 訊。 表示SWA明確接 客戶端配置為直
			TCP_CONNECT 表示WSA透明地 WCCP或第4層
目的地	10.37.145.84:443	%2r	本節顯示目標伺服器URL和TCP埠號。 在透明重新導向中，在流量解密之前，S 址和連線埠號碼。 如果URL以tunnel:// 開頭，則表示SWA 如果URL以https://開頭，則表示SWA對
使用者名稱和身份驗證領域	"AMOJARRA\amirhossein@WCCPrealm"	%A	用於此連線的憑據。 如果請求經過身份驗證，SWA將記錄使 域，如下所示： <域名> \ <用戶名> @ <驗證領域名> 如果請求尚未通過驗證或免於驗證，則有 「 — 」
訪問型別	直接/	%H	描述為檢索請求內容而聯絡了哪台伺服器 最常見的值包括： NONE — Web代理具有內容 他伺服器以檢索內 直接 — Web代理轉到請求 內容。 DEFAULT_PARENT — Web代理轉到其主 服器以獲取內容。

<table>
<tr><td>伺服器地址</td><td>www.cisco.com</td><td>%d</td><td>資料來源或伺服器IP地址。</td></tr>
<tr><td>MIME內容型別/子型別</td><td>-</td><td>%c</td><td>MIME表示文檔、檔案或位元組分類的性
在IETF RFC 6838中定義和標準化

對於預設型別的角色，兩個主要MIME型

• text/plain是文本檔案的預設值。文
的，不能包含二進位制資料。
• application/octet-stream是所有其
的檔案型別必須使用此型別。瀏覽
特別小心，以保護使用者免受軟體
的侵害。

要獲取MIME型別的完整清單，請訪問：</td></tr>
<tr><td>ACL決策標籤</td><td>PASSTHRU_CUSTOMCAT_7-</td><td>%D</td><td>ACL決策標籤是訪問日誌條目中的一個欄
何處理事務。它包含來自Web信譽過濾器
擎的資訊。

注意:ACL決策標籤的末尾包含動態
在內部使用該數字來提高效能。您

以下是最重要的ACL決策標籤清單。(有
文的ACL決策標籤部分)

ACL決策標籤

ALLOW_CUSTOMCAT

ALLOW_WBR

AMP_FILE_VERDICT</td></tr>
</table>

			BLOCKADMIN
			BLOCK_ADMIN_CONNECT
			BLOCK_ADMIN_CUSTOM_USER_AG
			BLOCK_ADMIN_TUNNELING
			BLOCK_ADMIN_FILE型別
			BLOCK_ADMIN協定
			BLOCK_AMP_RESP
			塊_AVC
			BLOCK_CONTENT_UNSAFE
			BLOCK_CUSTOMCAT
			BLOCK_ICAP

			BLOCK_WBRS
			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 其他
策略名稱	DP站點 —	不適用	視流量的型別而定，這顯示： • 解密策略名稱:如果流量為HTTPS • 訪問策略名稱:如果流量是HTTP或
身份策略	IdP_站點 —	不適用	顯示標識配置檔名稱
出站惡意軟體掃描策略組	NONE-	不適用	出站惡意軟體掃描策略組名稱。 策略組名稱中的任何空格都將被下劃線(
資料安全策略組	NONE-	不適用	思科資料安全策略組名稱。當事務與全 匹配時，此值為DefaultGroup。僅當啟 ，才會顯示此策略組名稱。未應用資料 。 策略組名稱中的任何空格都將被下劃線(

<table>
<tr><td>外部DLP策略組</td><td>NONE-</td><td>不適用</td><td>當事務與全域性外部DLP策略匹配時，此
果未應用外部DLP策略，則顯示「NONE
策略組名稱中的任何空格都將被下劃線(</td></tr>
<tr><td>路由策略組</td><td>預設組 —</td><td>不適用</td><td>路由策略組名為ProxyGroupName/Prox
當事務與全域性路由策略匹配時，此值為
使用上游代理伺服器時，此值為DIRECT
策略組名稱中的任何空格都將被下劃線(</td></tr>
<tr><td>Web流量分流器</td><td>NONE</td><td>不適用</td><td>Web流量分流器策略名稱。</td></tr>
<tr><td>URL類別縮寫</td><td><"C_Cisco",</td><td>%XC</td><td>請求匹配的URL類別。<table><tr><td>-</td><td>繞過的URL篩選</td></tr><tr><td>nc</td><td>未分類的URL</td></tr><tr><td>錯誤</td><td>繞過的URL篩選</td></tr><tr><td>imp</td><td>不可能</td></tr><tr><td>IW_</td><td>如果類別名稱以IW_開頭，
求進入Cisco預定義URL類</td></tr><tr><td>C_</td><td>如果類別名稱以IC_開頭，
求正在進入「自定義URL類</td></tr></table></td></tr>
<tr><td>Web聲譽分數</td><td>-、</td><td>%XW</td><td>此欄位顯示Web信譽(WBRS)分數。
ns表示URL沒有分數。</td></tr>
<tr><td>Webroot掃</td><td>-,"-",-,-,-,-</td><td></td><td>這5個欄位與Webroot掃描相關</td></tr>
</table>

描			Webroot判定，	%Xv	惡意軟體 遞到DV Webroo 有關裁決 本文中的 。
			Webroot Spyname、	"%Xn"	與對象關 。僅適用 響應。
			Webroot TRR、	%Xt	與威脅 Webroo 意軟體有 於Webr
			Webroot ThreatID、	%Xs	Webroo 值。思科 排解問題 於Webr
			Webroot TraceID、	%Xi	Webroo 值。思科 排解問題 於Webr
McAfee掃描	-,"-",-,-,-,"-",		這6個欄位與McAfee掃描相關。		
			McAfee裁決，	%Xd	惡意軟體 遞到DV McAfee 有關裁決 本文中的 。
			McAfee檔名，	"%Xe"	McAfee 於McAf
			McAfee掃描錯誤	%Xf	McAfee

			代碼，		科客戶支 題時使用 McAfee
			McAfee檢測型別 、	%Xg	McAfee 科客戶支 題時使用 McAfee
			McAfee病毒型別 、	%Xh	McAfee 科客戶支 題時使用 McAfee
			McAfee病毒名稱 、	"%Xj"	McAfee 適用於M
Sophos掃描	-,-,"-","-",		這4個欄位與Sophos掃描相關		
			Sophos判決，	%XY	惡意軟體 到DVS Sophos 有關裁決 本文中的 。
			Sophos掃描返回代碼，	%Xx	Sophos 。思科客 解問題時 Sophos
			Sophos檔案位置 ，	"%Xy"	Sophos 檔案的名 Sophos
			Sophos威脅名稱 、	%Xz"	Sophos 科客戶支 題時使用 Sophos

思科資料安全掃描判定結果	-、	%XI	思科資料安全掃描判定基於思科資料安全(Content)列中的操作。 此清單介紹了此欄位的可能值： 0.Allow 1.Block —（連字元）。思科資料安全過濾器未Data Security Filters被禁用，或URL類，將顯示該值。
外部DLP掃描判定	-、	%Xp	外部DLP掃描判定基於ICAP響應中給定 此清單介紹了此欄位的可能值： 0.Allow 1.Block —（連字元）。外部DLP伺服器未啟動DLP掃描被禁用，或者由於外部DLP策URL類別而未掃描內容時，將顯示該值。
預定義URL類別判定結果	"-",	%XQ	請求端掃描期間確定的預定義URL類別 禁用URL過濾時，此欄位將列出連字元(如果請求符合自定義URL類別，您仍可定義的URL類別名稱，但決定是由自定 有關URL類別縮寫的清單，請參閱URL
URL類別判定結果	-、	%XA	在響應端掃描期間由動態內容分析(DCA定，縮寫。 僅適用於Cisco Web Usage Controls UR nc:當啟用動態內容分析引擎並且在請求，此值出現在請求端掃描判定中，這表行分類之前，URL在初始請求階段未分
整合傳入DVS裁定	"-",	%XZ	統一響應端防惡意軟體掃描判定，提供惡意軟體類別。應用於由於伺服器響應事務。

<table>
<tr><td>Web信譽過濾器威脅型別</td><td>"-",</td><td>%Xk</td><td>類別名稱或威脅型別由Web信譽過濾器
時返回Category Name，當信譽較低時

通常，此欄位填充的站點信譽為–4或更</td></tr>
<tr><td>Google翻譯封裝的URL</td><td>"-",</td><td>%X#10#</td><td>封裝在Google翻譯引擎中的URL。如果
位值為「-」。</td></tr>
<tr><td>應用控制(AVC/ADC)</td><td>"-","-","-",</td><td></td><td>在以下3個欄位中，將記錄應用可視性與
索與控制(ADC)的統計資訊。<table><tr><td>AVC/ADC應用程式名稱</td><td>"%XO"</td><td>由AVC或ADC
稱（如果適用
ADC引擎時適</td></tr><tr><td>AVC/ADC應用程式型別</td><td>"%Xu"</td><td>AVC或ADC引
（如果適用）
ADC引擎時適</td></tr><tr><td>AVC/ADC應用程序行為</td><td>%Xb"</td><td>AVC或ADC引
（如果適用）
ADC引擎時適

對於AVC為「
Unknown」。</td></tr></table></td></tr>
<tr><td>安全瀏覽裁決</td><td>"-",</td><td>%XS</td><td>此值指示是否對事務應用了安全搜尋或
<table><tr><td>ensrch</td><td>原始客戶端請求不安全，並且應</td></tr><tr><td>encrt</td><td>原始客戶端請求不安全，並且應
。</td></tr><tr><td>unsupp</td><td>原始客戶端請求被傳送到不受支</td></tr><tr><td>錯誤</td><td>原始客戶端請求不安全，但是由
搜尋和網站內容分級功能。</td></tr></table></td></tr>
</table>

<table>
<tr><td></td><td></td><td></td><td><table><tr><td>-</td><td>安全搜尋和站點內容分級功能均
，因為已跳過這些功能（例如，
許該事務），或者請求來自不受</td></tr></table></td></tr>
<tr><td>平均頻寬</td><td>11.35,</td><td>%XB</td><td>為請求提供服務所用的平均頻寬（Kb/秒</td></tr>
<tr><td>頻寬限制控制</td><td>0,</td><td>%XT</td><td>一個值，指示請求是否由於頻寬限制控制
「1」表示請求已限制。
"0"表示請求未受限制。</td></tr>
<tr><td>使用者型別</td><td>-、</td><td>%l</td><td>發出請求的使用者型別，可以是「[Loca
僅在啟用AnyConnect Secure Mobility時
未啟用時，值為連字元(-)</td></tr>
<tr><td>出站惡意軟體掃描</td><td>"-","-",</td><td></td><td>這2個欄位適用於在應用出站惡意軟體掃
求掃描而被阻止或受監控的事務。<table><tr><td>整合傳出DVS裁定</td><td>"%X3"</td><td>統一請求
結果，與
。應用於
描策略時
被阻止或</td></tr><tr><td>出站威脅名稱</td><td>%X4"</td><td>分配給由
掃描策略
端請求的
此威脅名
體掃描引</td></tr></table></td></tr>
<tr><td>高級惡意軟體防護</td><td>-,"-",-,-"-","-","-",</td><td></td><td>以下6個欄位與安全終端（也稱為高級惡<table><tr><td>檔案判定</td><td>%X#1#</td><td>V
E
0
1</td></tr></table></td></tr>
</table>

					檔 2 3 [4 是
			威脅名稱	%X#2#	威 E
			聲譽得分	%X#3#	聲 E 分 無 定 。
			用於分析的上傳操作	%X#4#	上 " E 檔 " E 案
			檔案名稱	%X#5#	正 。
			檔案SHA	%X#6#	此 符
存檔掃描	-、-、"-",		以下3個欄位指示存檔檔案掃描的狀態：		
			存檔掃描判定	%X#7#	存檔掃描判定。

					ARCHIVESCAN_ALLCLEAR
					ARCHIVESCAN_BLOCKED
					ARCHIVESCAN_NESTEDT
					ARCHIVESCAN_UNKNOWN

					ARCHIVESCAN_UNSCANA
					ARCHIVESCAN_FILETOOB
			存檔掃描判定詳細資訊	%Xc	存檔掃描判定詳細資訊。如果Inspectable Archive檔案(ARCHIVESCAN_BLOCKED象阻止設定，此「判定詳細資案的型別和阻止的檔案的名稱 "UnScanable Archive-Blocke含任何被阻止的檔案型別。
			檔案判定	%Xm	存檔掃描程式進行檔案判定
Web Tap	-、	%XU	Web分流器行為。		
YouTube URL類別	->	%X#29#	分配給事務的YouTube URL類別（縮寫類別時的「nc」。		

HTTP響應代碼

以下是HTTP響應代碼的完整清單

狀態代碼	含義
1xx資訊	
100	繼續
101	交換通訊協定
102	正在處理
103	早期提示
2xx成功	
200	確定
201	建立時間
202	已接受
203	非授權資訊
204	無內容
205	重設內容
206	部分內容
207	多狀態
208	已報告
226	已使用的IM
3xx重新導向	
300	多種選擇
301	已永久移動
302	已找到（以前「已暫時移動」）
303	檢視其他
304	未修改
305	使用代理
306	交換器代理
307	用於身份驗證的臨時重定向

	（通常在SWA對使用者進行身份驗證時的透明部署中看到）
308	永久重新導向
4xx客戶端錯誤	
400	錯誤的請求
401	需要Web伺服器身份驗證（通常在SWA對使用者進行身份驗證時在透明部署中出現）
402	需要付款
403	禁止
404	未找到
405	不允許的方法
406	不可接受
407	需要顯式代理身份驗證
408	請求超時
409	衝突
410	消失
411	需要長度
412	預處理失敗
413	負載過大
414	URI過長
415	不支援的媒體型別
416	範圍無法滿足
417	預期失敗
418	我是茶壺
421	錯誤請求
422	無法處理的實體
423	已鎖定
424	失敗的依賴項
425	太早
426	需要升級

428	需要前提條件
429	請求過多
431	請求報頭欄位太大
451	因法律原因不可用
5xx伺服器錯誤	
500	內部伺服器錯誤
501	未實施
502	錯誤的網關
503	服務不可用
504	網關超時
505	不支援HTTP版本
506	變體也會協商
507	儲存不足
508	檢測到環路
510	未擴展
511	需要網路身份驗證

ACL決策標籤

以下是ACL決策標籤的完整清單：

ACL決策標籤	說明
ALLOW_ADMIN_ERROR_PAGE	Web代理允許事務進入通知頁面以及在該頁面上使用的任何徽標。
ALLOW_CUSTOMCAT	Web代理基於訪問策略組的自定義URL類別過濾設定允許該事務。
ALLOW_REFERER	Web代理允許基於嵌入式/引用內容豁免的交易。
ALLOW_WBR	Web代理基於訪問策略組的Web信譽過濾器設定允許事務。
AMP_FILE_VERDICT	表示來自AMP信譽伺服器的檔案的裁決的值：
	1 — 未知
	2 — 清除

	3 — 惡意
	4 — 無法掃描
ARCHIVESCAN_ALLCLEAR	存檔掃描判定
ARCHIVESCAN_BLOCKEDFILETYPE	ARCHIVESCAN_ALLCLEAR — 檢查的存檔中沒有阻止的檔案型別。
ARCHIVESCAN_NESTEDTODEEP	ARCHIVESCAN_BLOCKEDFILETYPE — 檢查的存檔中存在阻止的檔案型別。日誌條目中的下一個欄位（判定詳細資訊）提供詳細資訊，特別是被阻止的檔案的型別和被阻止檔案的名稱。
ARCHIVESCAN_UNKNOWNFMT	ARCHIVESCAN_NESTEDTODEEP — 存檔被阻止，因為它包含的「封裝」或巢狀的存檔數比配置的最大數還多。判定詳細資訊欄位包含「Un-Scanable Archive-Blocked」。
ARCHIVESCAN_UNSCANABLE	ARCHIVESCAN_UNKNOWNFMT — 存檔被阻止，因為它包含未知格式的檔案型別。判定詳細資訊為「Un-Scannable Archive-Blocked」。
ARCHIVESCAN_FILETOOBIG	ARCHIVESCAN_UNSCANABLE — 存檔被阻止，因為它包含無法掃描的檔案。判定詳細資訊為「Un-Scannable Archive-Blocked」。
	ARCHIVESCAN_FILETOOBIG — 存檔被阻止，因為存檔的大小大於配置的最大值。判定詳細資訊為「Un-Scannable Archive-Blocked」。
	存檔掃描判定詳細資訊
	日誌條目中的欄位和Verdict欄位提供有關裁決的其他資訊，例如被阻止的檔案的型別和被阻止檔案的名稱、「無法掃描的存檔被阻止」或「 — 」以指示存檔不包含任何被阻止的檔案型別。
	例如，如果根據訪問策略阻止Inspectable Archive檔案(ARCHIVESCAN_BLOCKEDFILETYPE):自定義對象阻止設定，判定詳細資訊條目包括阻止的檔案的型別和阻止的檔案的名稱。
	請參閱存取原則：「阻止對象」和「存檔檔案檢查設定」以瞭解有關存檔檔案檢查的詳細資訊。
BLOCKADMIN	基於訪問策略組的某些預設設定阻止的事務。

BLOCK_ADMIN_CONNECT	根據訪問策略組的HTTP CONNECT埠設定中定義的目標的TCP埠阻止的事務。
BLOCK_ADMIN_CUSTOM_USER_AGENT	根據在Access Policy組的Block Custom User Agents設定中定義的使用者代理阻止事務。
BLOCK_ADMIN_TUNNELING	Web代理基於訪問策略組的HTTP埠上的非HTTP流量的隧道阻止了事務。
BLOCK_ADMIN_HTTPS_NonLocalDestination	事務被阻止；客戶端嘗試使用SSL埠作為顯式代理繞過身份驗證。為防止這種情況，如果SSL連線是WSA本身，則僅允許對實際WSA重定向主機名的請求。
BLOCK_ADMIN_IDS	根據資料安全策略組中定義的請求正文內容的MIME型別阻止的事務。
BLOCK_ADMIN_FILE型別	根據訪問策略組中定義的檔案型別阻止的事務。
BLOCK_ADMIN協定	根據Access Policy組的Block Protocols設定中定義的協定阻止的事務。
BLOCK_ADMIN_SIZE	根據在Access Policy組的Object Size設定中定義的響應大小阻止事務。
BLOCK_ADMIN_SIZE_IDS	根據資料安全策略組中定義的請求正文內容大小阻止的事務。
BLOCK_AMP_RESP	Web代理基於訪問策略組的高級惡意軟體防護設定阻止了響應。
BLOCK_AMW_REQ	Web代理基於出站惡意軟體掃描策略組的防惡意軟體設定阻止了請求。請求正文生成了正惡意軟體判定結果。
BLOCK_AMW_RESP	Web代理基於訪問策略組的防惡意軟體設定阻止了響應。
BLOCK_AMW_REQ_URL	Web代理懷疑HTTP請求中的URL不安全，因此它基於訪問策略組的防惡意軟體設定，在請求時阻止了事務。
塊_AVC	根據為訪問策略組配置的應用程式設定阻止的事務。
BLOCK_CONTENT_UNSAFE	基於訪問策略組的網站內容分級設定阻止的事務。客戶端請求用於成人內容，並且策略配置為阻止成人內容。
BLOCK_CONTINUE_CONTENT_UNSAFE	事務已阻止並顯示基於Access Policy組中的站點內容評級設定的「警告並繼續」頁面。客戶端請求用於成人內容，並且策略配置為向訪問成人內容的使用者提供警告。
BLOCK_CONTINUE_CUSTOMCAT	事務已阻止並顯示「警告並繼續」頁面，該頁面基於配置為「警告」的Access Policy組中的自定義URL類別。
BLOCK_CONTINUE_WEBCAT	事務已阻止並顯示「警告並繼續」頁面，該頁面基於配置為「警告」的Access

	Policy組中的預定義URL類別。
BLOCK_CUSTOMCAT	基於訪問策略組的自定義URL類別過濾設定阻止的事務。
BLOCK_ICAP	Web代理根據外部DLP策略組中定義的外部DLP系統的判定阻止了請求。
BLOCK_SEARCH_UNSAFE	客戶端請求包含不安全的搜尋查詢，並且訪問策略配置為強制安全搜尋，因此原始客戶端請求被阻止。
BLOCK_SUSPECT_USER_AGENT	基於訪問策略組的可疑使用者代理設定阻止的事務。
BLOCK_UNSUPPORTED_SEARCH_APP	基於訪問策略組的安全搜尋設定阻止的事務。該事務用於不受支援的搜尋引擎，並且策略被配置為阻止不受支援的搜尋引擎。
BLOCK_WBRS	基於訪問策略組的Web信譽過濾器設定阻止的事務。
BLOCK_WBRS_IDS	Web代理基於資料安全策略組的Web信譽過濾器設定阻止了上載請求。
BLOCK_WEBCAT	基於訪問策略組的URL類別過濾設定阻止的事務。
BLOCK_WEBCAT_IDS	Web代理基於資料安全策略組的URL類別篩選設定阻止了上載請求。
BLOCK_TYPE	Web代理基於訪問策略組的預定義YouTube類別過濾設定阻止了事務。
BLOCK_CONTINUE_YTCAT	Web代理阻止了事務，並根據配置為「警告」的訪問策略組中的預定義YouTube類別顯示「警告並繼續」頁面。
DECRYPT_ADMIN	Web代理基於解密策略組的一些預設設定解密事務。
DECRYPT_ADMIN_EXPIRED_CERT	Web代理解密了事務，儘管伺服器證書已過期。
DECRYPT_EUN_ADMIN_DEFAULT_ACTION	啟用EUN時，Web代理基於預設設定將事務解密為解密策略組的丟棄連線。
DECRYPT_EUN_ADMIN_EXPIRED_CERT	當HTTPS代理設定刪除已啟用EUN的過期證書時，Web代理解密了事務。
DECRYPT_EUN_ADMIN_INVALID_LEAF_CERT	當HTTPS代理設定刪除啟用EUN的無效枝葉證書時，Web代理解密了事務。
DECRYPT_EUN_ADMIN_MISMATCHED_HOSTNAME	當HTTPS代理設定刪除啟用EUN的不匹配主機名時，Web代理解密了事務。
DECRYPT_EUN_ADMIN_OCSP_OTHER_ERROR	當HTTPS代理設定丟棄具有啟用EUN的其他錯誤的OCSP時，Web代理解密了事務。
DECRYPT_EUN_ADMIN_OCSP_REVOKED_CERT	當HTTPS代理設定刪除啟用EUN的OCSP吊銷證書時，Web代理解密了事務。
DECRYPT_EUN_ADMIN_UNRECOGNIZED_ROOT_CERT	當HTTPS代理設定刪除啟用了EUN的無法識別的根授權或頒發者證書時，Web代理解

	密了事務。
DECRYPT_EUN_CUSTOMCAT	Web代理基於解密策略組的自定義URL類別過濾設定對事務進行解密。如果啟用EUN，流量會遭到捨棄。
DECRYPT_EUN_WBRS	Web代理基於解密策略組的Web信譽過濾器設定解密事務。如果啟用EUN，流量會遭到捨棄。
DECRYPT_EUN_WBRS_NO_SCORE	Web代理基於解密策略組中無分數URL的Web信譽過濾器設定解密事務。如果啟用EUN，流量會遭到捨棄。
DECRYPT_EUN_WEBCAT	Web代理基於解密策略組的URL類別過濾設定對事務進行解密。如果啟用EUN，流量會遭到捨棄。
DECRYPT_WEBCAT	Web代理基於解密策略組的URL類別過濾設定對事務進行解密。
DECRYPT_WBRS	Web代理基於解密策略組的Web信譽過濾器設定解密事務。
DEFAULT_CASE	Web代理允許客戶端訪問伺服器，因為所有AsyncOS服務（如Web信譽或防惡意軟體掃描）均未對事務執行任何操作。
DENY_ADMIN	Web代理拒絕該事務。當需要身份驗證且在HTTPS代理設定中禁用了Decrypt for Authentication時，HTTPS請求會發生這種情況。
DROP_ADMIN	Web代理基於解密策略組的某些預設設定丟棄了事務。
DROP_ADMIN_EXPIRED_CERT	由於伺服器證書已過期，Web代理丟棄了事務。
DROP_WEBCAT	Web代理基於解密策略組的URL類別過濾設定丟棄了事務。
DROP_WBRS	Web代理基於解密策略組的Web信譽過濾器設定丟棄了事務。
MONITOR_ADMIN_EXPIRED_CERT	由於伺服器證書已過期，Web代理監控了伺服器響應。
MONITOR_AMP_RESP	Web代理基於訪問策略組的高級惡意軟體防護設定監控伺服器響應。
MONITOR_AMW_RESP	Web代理基於訪問策略組的防惡意軟體設定監控伺服器響應。
MONITOR_AMW_RESP_URL	Web代理懷疑HTTP請求中的URL可能不安全，但它基於訪問策略組的防惡意軟體設定監控事務。
監控_AVC	Web代理基於訪問策略組的應用程式設定監視事務。
MONITOR_CONTINUE_CONTENT_UNSAFE	最初，Web代理阻止了事務，並根據Access Policy組中的站點內容評級設定顯

	示「警告並繼續」頁面。客戶端請求用於成人內容，並且策略配置為向訪問成人內容的使用者提供警告。該使用者接受該警告並繼續訪問最初請求的站點，隨後沒有其他掃描引擎阻止該請求。
MONITOR_CONTINUE_CUSTOMCAT	最初，Web代理阻止了事務，並根據配置為「警告」的訪問策略組中的自定義URL類別顯示「警告並繼續」頁面。 該使用者接受該警告並繼續訪問最初請求的站點，隨後沒有其他掃描引擎阻止該請求。
MONITOR_CONTINUE_WEBCAT	最初，Web代理阻止了事務，並根據配置為「警告」的Access Policy組中的預定義URL類別顯示「警告並繼續」頁面。 該使用者接受該警告並繼續訪問最初請求的站點，隨後沒有其他掃描引擎阻止該請求。
MONITOR_CONTINUE_TYPE	最初，Web代理阻止了事務，並根據配置為「警告」的訪問策略組中的預定義YouTube類別顯示「警告並繼續」頁面。該使用者接受該警告並繼續訪問最初請求的站點，隨後沒有其他掃描引擎阻止該請求。
MONITOR_IDS	Web代理使用資料安全策略或外部DLP策略掃描上傳請求，但未阻止該請求。它根據訪問策略評估請求。
MONITOR_SUSPECT_USER_AGENT	Web代理基於訪問策略組的可疑使用者代理設定監控事務。
監控_WBRS	Web代理基於訪問策略組的Web信譽過濾器設定監控事務。
NO_AUTHORIZATION	Web代理不允許使用者訪問應用程式，因為使用者已經根據身份驗證領域進行身份驗證，而不是根據應用程式身份驗證策略中配置的任何身份驗證領域進行身份驗證。
NO_PASSWORD	使用者身份驗證失敗。
PASSTHRU_ADMIN	Web代理基於解密策略組的某些預設設定傳遞了事務。
PASSTHRU_ADMIN_EXPIRED_CERT	Web代理通過事務，但伺服器證書已過期。
PASSTHRU_WEBCAT	Web代理基於解密策略組的URL類別過濾設定傳遞了事務。
PASSTHRU_WBRS	Web代理基於解密策略組的Web信譽過濾器設定傳遞了事務。
REDIRECT_CUSTOMCAT	Web代理根據配置為「Redirect」的訪問策略組中的自定義URL類別，將事務重定向到其他URL。
SAAS_AUTH	Web代理允許使用者訪問應用程式，因為使用者已根據應用程式身份驗證策略中配置的身份驗證領域進行透明身份驗證。

其他	Web代理未完成請求，因為出現錯誤（如授權失敗、伺服器斷開連線或從客戶端中止）。

惡意軟體掃描判定值

惡意軟體掃描判定值是分配給URL請求或伺服器響應的值，用於確定它包含惡意軟體的概率。Webroot、McAfee和Sophos掃描引擎將惡意軟體掃描判定返回到DVS引擎，以便DVS引擎可以確定是監視還是阻止掃描的對象。編輯特定訪問策略的Anti-Malware設定時，每個惡意軟體掃描判定結果都與Access Policies > Reputation and Anti-Malware Settings頁上列出的惡意軟體類別相對應。

此清單顯示了不同的惡意軟體掃描判定值和每個相應的惡意軟體類別：

惡意軟體掃描判定值	惡意軟體類別
-	未設定
0	未知
1	未掃描
2	逾時
3	錯誤
4	無法掃描
10	通用間諜軟體
12	瀏覽器幫助程式對象
13	廣告軟體
14	系統監控器
18	商業系統監控器

惡意軟體掃描判定值	惡意軟體類別
19	撥號器
20	劫機者
21	網路釣魚URL
22	特洛伊木馬下載程式
23	特洛伊木馬
24	特洛伊木馬釣魚程式
25	蠕蟲
26	加密的檔案
27	病毒
33	其他惡意軟體
34	PUA
35	已中止
36	爆發啟發式
37	已知惡意和高風險檔案

相關資訊

- Cisco Secure Web Appliance AsyncOS 15.2使用手冊
- 使用安全Web裝置最佳做法

- 確保VMware環境中適當的虛擬WSA HA組功能
- 配置訪問日誌中的效能引數
- 瞭解Secure Web Appliance中的HTTPS訪問日誌格式
- 訪問安全Web裝置日誌

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。