解決安全Web裝置延遲問題

目錄

簡介

本文檔介紹在Cisco Secure Web Appliance(SWA)中解決高延遲、高磁碟和高CPU問題的故障排除步驟。

必要條件

需求

思科建議您瞭解以下主題：

- Cisco SWA管理
- 代理部署方法（顯式和透明）
- SWA命令列介面(CLI)命令

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。

背景資訊

在聯絡思科技術支援時，您需要提供有關SWA出站和入站網路活動的詳細資訊，可通過運行資料包捕獲來監控此活動，以收集流量用於調試或驗證。

SWA高延遲的常見原因

一般來說，SWA中的高延遲主要有三個類別：

1. SWA規模不足或資源過載
2.複雜配置
3.與網路相關的延遲問題

在SWA中，導致高延遲的最常見原因之一是解決方案的規模不足。適當的規模對於確保SWA系統有足夠資源處理當前和預期的工作負載至關重要。如果系統規模過小，它可能難以高效處理請求，導致操作延遲和效能降低。部署過程中必須仔細評估使用者數量、解密量和特定掃描需求等因素，以避免資源限制。無法將SWA容量與組織需求相匹配會導致持續延遲和使用者體驗下降。

複雜的配置會降低效能並導致SWA上的延遲，特別是在高負載下，因為每個請求都必須經過多種條件處理。

與網路相關的延遲可能源自SWA本身、第三方服務（如Active Directory、DLP、DNS）或客戶端、SWA和上游伺服器之間的網路延遲。

分析傳送到SWA的請求，包括識別頂級使用者和訪問次數最多的URL，有助於發現潛在的不當行為，並查明延遲的根本原因。此資訊對於診斷效能問題、管理頻寬消耗和確保系統的正確使用是非常寶貴的。

SWA延遲故障排除工具

系統狀態

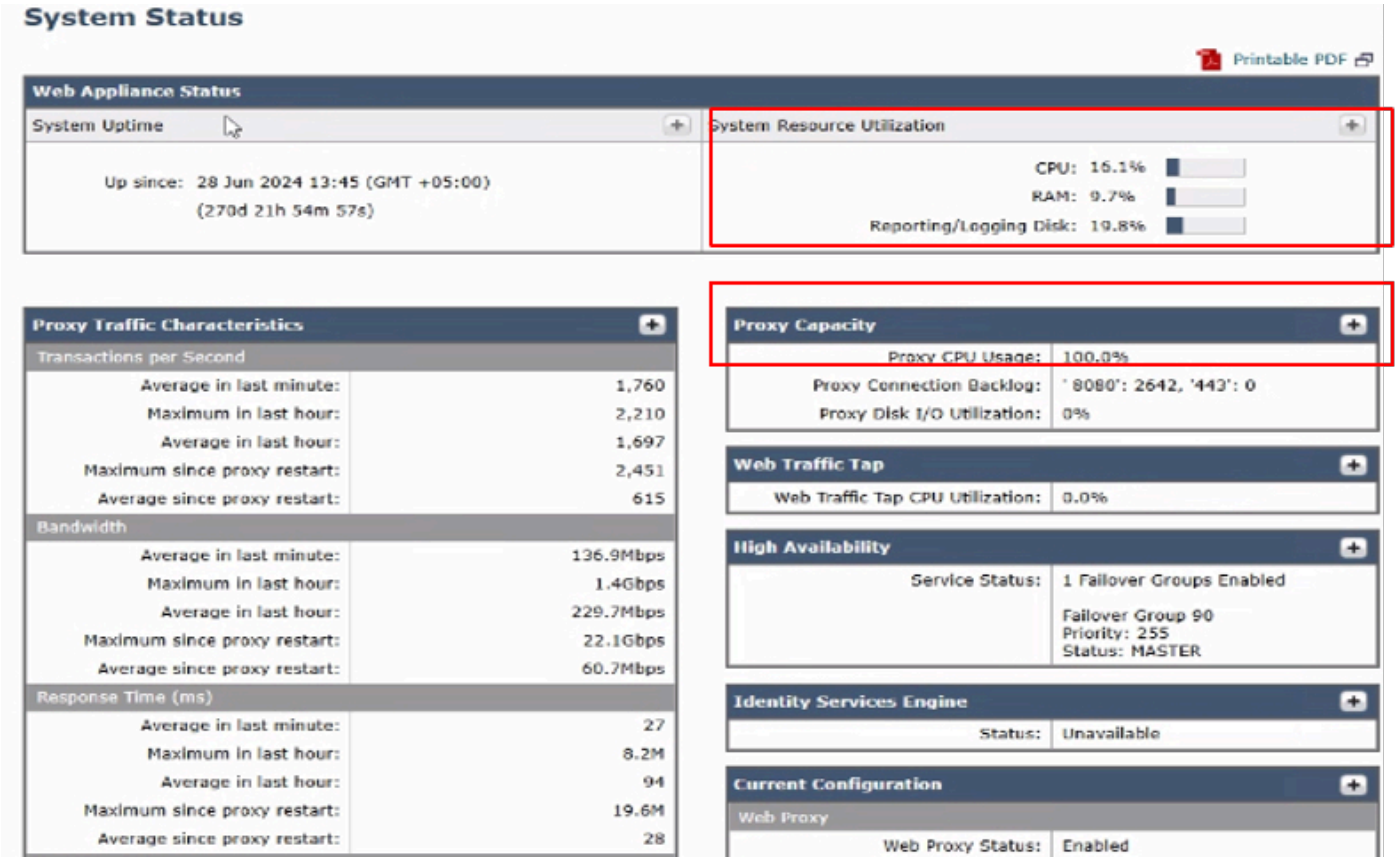
使用以下步驟檢查SWA中的當前資源消耗：

步驟1.訪問SWA圖形使用者介面(GUI)。

步驟2.導覽至Reporting > System Information > System Status。

步驟3.檢查以下關鍵指標以評估系統效能：

- CPU使用率(%):指示當前CPU負載
- RAM使用率(%):反映記憶體利用率
- 報告/日誌記錄使用率(%):顯示用於報告和日誌記錄的磁碟空間百分比
- 系統正常運行時間：顯示系統未重新啟動而運行的總時間



影象 — 系統狀態

此頁提供RAM、CPU和磁碟使用率的當前狀態的概述。要檢視一段時間的資源使用情況，請從SWA GUI導航到Reporting，然後選擇System Capacity。

系統容量

SWA中的System Capacity頁提供了指定時間範圍內資源利用率和效能度量的綜合檢視。此頁面提供詳細的圖表，以幫助監控和分析系統行為，確保最佳效能並識別潛在的瓶頸。

「系統容量」頁中的可用圖形和度量包括：

1. 總體CPU使用率：顯示總CPU使用率，簡要概述系統效能。
2. 按功能劃分的CPU使用率：根據特定功能劃分CPU使用率，包括：

- Web代理
- 日誌記錄
- 報告
- McAfee
- Sophos
- Webroot
- 可接受的使用和信譽

3.響應時間/延遲（毫秒）：跟蹤響應時間，以確定處理請求過程中的任何延遲。

4.每秒交易量：顯示SWA每秒處理的事務數。

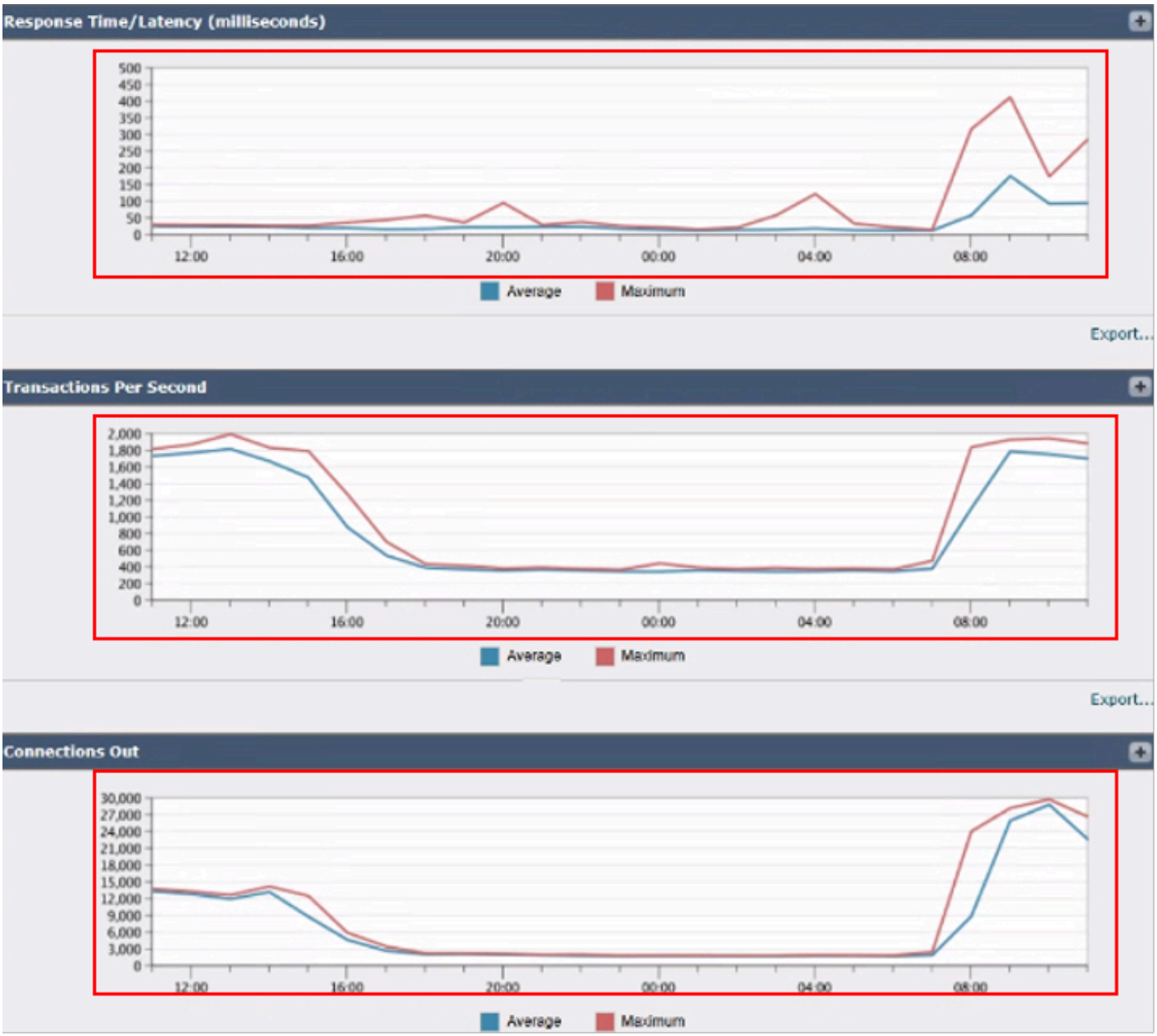
5.外聯：監控正在建立的出站連線數。

6.輸出頻寬（位元組）：測量正在使用的出站頻寬量。

7.代理緩衝區記憶體(%):顯示代理進程使用的記憶體百分比。

檢查度量是否有此儀表板中資源使用率高的跡象。

映像 — 系統容量



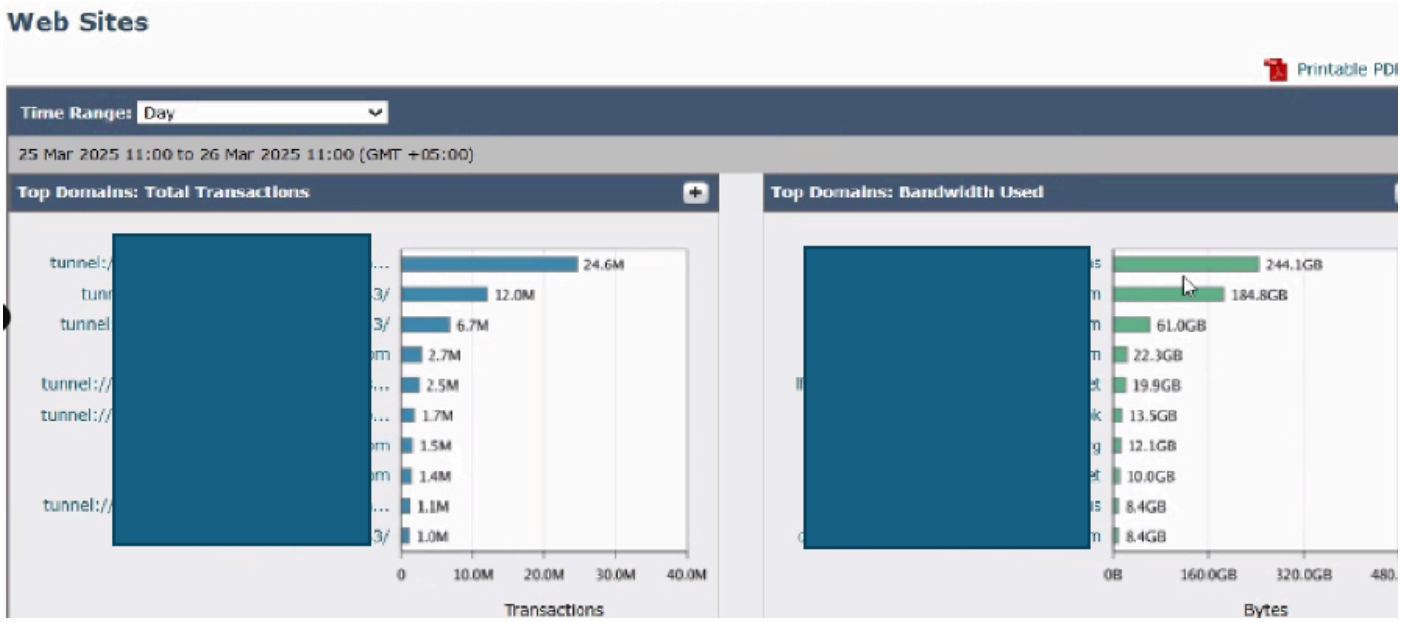
影象 — 每秒的SWA事務數和輸出連線

映像 — SWA記憶體使用情況

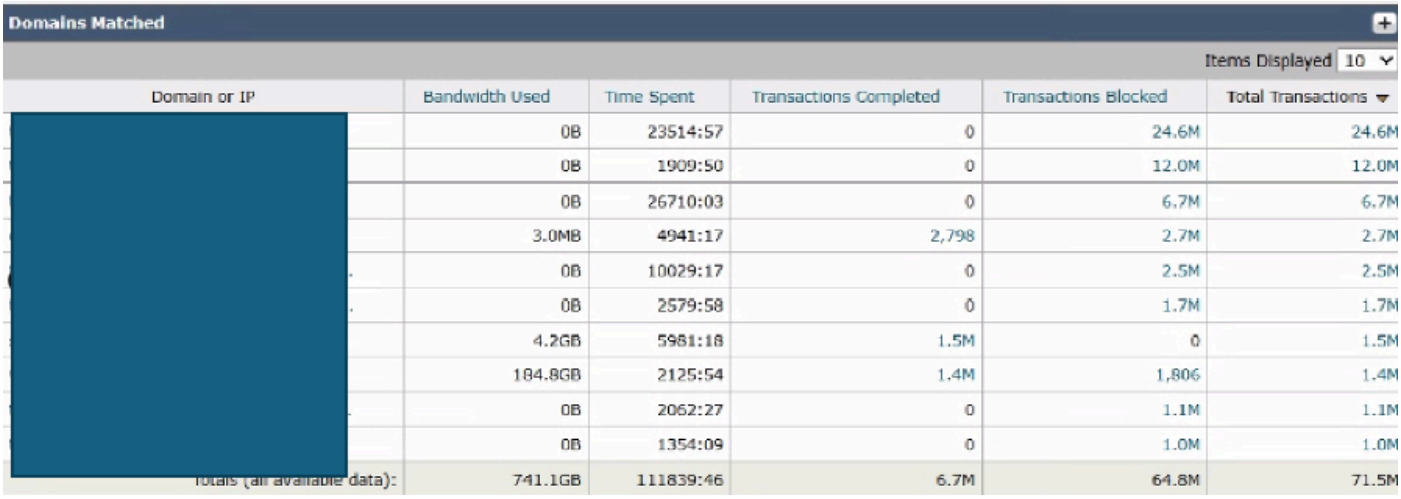
分析熱門目標

要分析排名靠前的目標，請導航到SWA GUI，導航到Reporting，然後選擇Websites。檢視頂級HTTP/HTTPS網站清單並確定高流量或經常訪問的域。

根據您的調查結果，考慮繞過或免除通用URL，例如Microsoft Updates、Adobe、Office365和線上會議平台。此方法有助於減少SWA上的流量，從而降低延遲並降低代理處理負載。



影象 — SWA熱門網站控制面板



Domains Matched

Items Displayed 10

Domain or IP	Bandwidth Used	Time Spent	Transactions Completed	Transactions Blocked	Total Transactions
[redacted]	0B	23514:57	0	24.6M	24.6M
	0B	1909:50	0	12.0M	12.0M
	0B	26710:03	0	6.7M	6.7M
	3.0MB	4941:17	2,798	2.7M	2.7M
	0B	10029:17	0	2.5M	2.5M
	0B	2579:58	0	1.7M	1.7M
	4.2GB	5981:18	1.5M	0	1.5M
	184.8GB	2125:54	1.4M	1,806	1.4M
	0B	2062:27	0	1.1M	1.1M
	0B	1354:09	0	1.0M	1.0M
Totals (all available data):	741.1GB	111839:46	6.7M	64.8M	71.5M

影象 — SWA頂級域控制面板

分析熱門使用者

要確定可能引起過多流量的來源，請從報告選擇Users導航到SWA GUI。

檢視清單以確定哪些使用者正在生成到SWA的最大數量的事務。此外，檢查哪些使用者電腦生成到SWA的事務數量最多且佔用最大頻寬。

此分析可幫助確定負責大量流量負載的使用者或裝置，從而實施有針對性的操作以減少整體系統壓力。

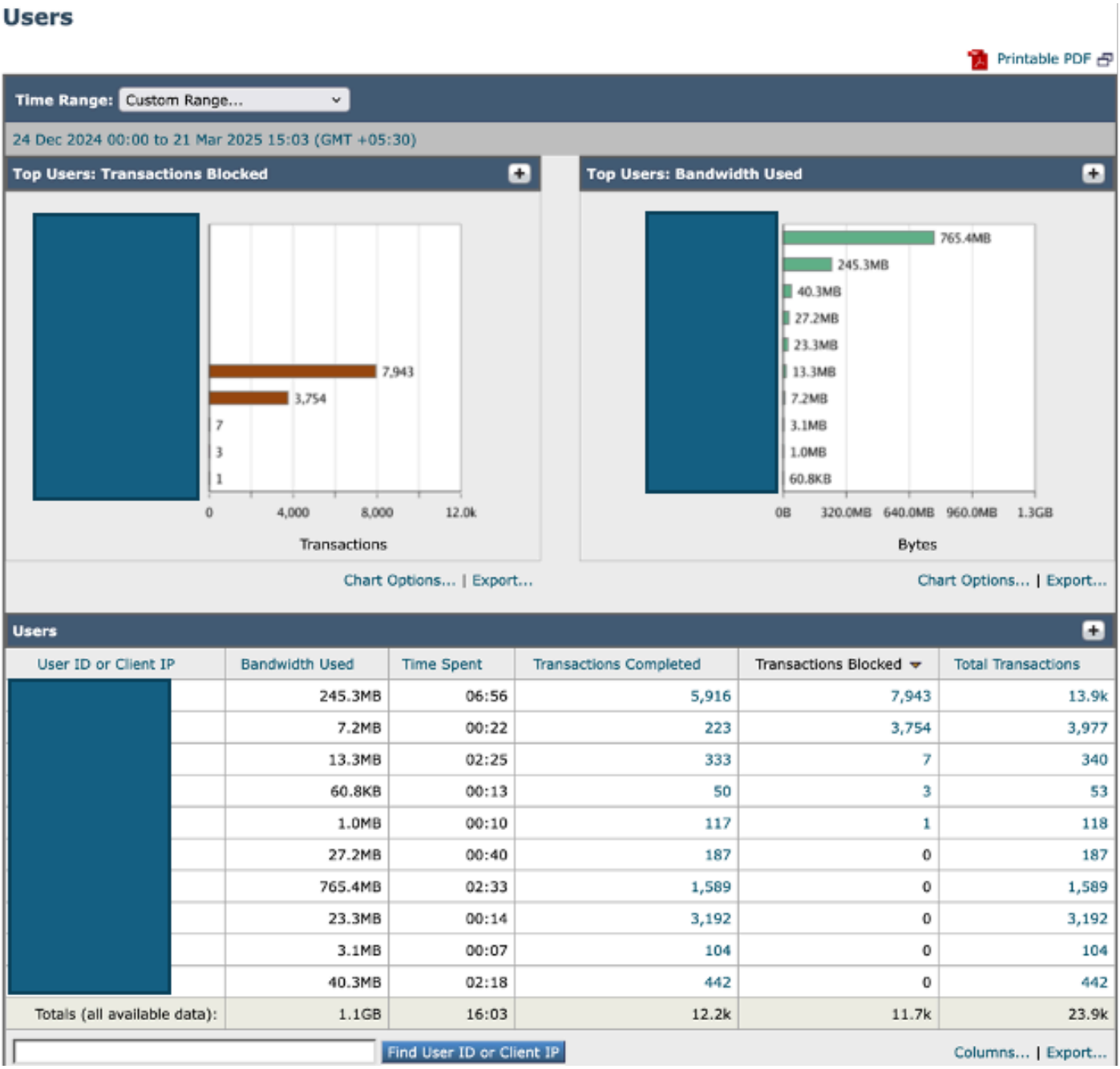


Image-SWA頂級使用者控制面板

SHD日誌

通過檢視SHD_log，您可以分析某些效能指標，例如從使用者到SWA的會話數(CliConn)、從SWA到Internet的會話數(SrvConn)、每秒平均請求數(Reqs)等。

有關SHD日誌的詳細資訊，請參閱使用SHD日誌排除安全Web裝置效能故障連結

在SHD日誌中要檢視的一些關鍵引數包括：

- ClientConns:活動客戶端連線數
- 伺服器連線：活動伺服器連線數
- 代理Ld:平均代理進程負載

- CPULD:平均總CPU負載
- RAMUTIL:RAM利用率
- 延遲：一分鐘內的平均服務時間
- DiskUtil：磁盤使用率和I/O效能

如本例所示，每秒1,600個請求會導致較高的代理進程負載。

```
Wed Mar 26 11:09:30 2025 Info: Status: CPULd 16.3 DskUtil 19.9 RAMUtil 9.3 Reqs 1661 Band 152966 Latenc
Wed Mar 26 11:10:31 2025 Info: Status: CPULd 13.6 DskUtil 19.9 RAMUtil 9.5 Reqs 1699 Band 107048 Latenc
Wed Mar 26 11:11:31 2025 Info: Status: CPULd 15.0 DskUtil 19.9 RAMUtil 9.5 Reqs 1669 Band 178803 Latenc
Wed Mar 26 11:12:31 2025 Info: Status: CPULd 17.6 DskUtil 19.9 RAMUtil 9.2 Reqs 1785 Band 143721 Latenc
```

使用訪問日誌排除延遲問題

當通過SWA代理的流量出現延遲問題時，訪問日誌可作為確定可能根本原因的有用工具。要加強故障排除工作，您可以修改現有的訪問日誌設定或建立新的訪問日誌。通過在自定義欄位中包含效能引數，您可以更深入地瞭解導致延遲的因素，從而進行更有效的分析和解決。

有關效能引數和配置步驟的詳細資訊，請參閱連結：在訪問日誌中配置效能引數

以下是在SWA中收集日誌的詳細指南：訪問安全Web裝置日誌

可以通過檢查關鍵引數來分析延遲源，這些引數有助於確定客戶端和SWA、SWA內部進程或SWA和Web伺服器之間是否出現延遲。需要考慮的重要指標包括基於網路的服務，例如DNS解析、身份驗證時間以及伺服器或客戶端響應時間。此外，必須評估掃描引擎（如AMP、Sophos和AVC）導致的延遲，以確定它們對整體延遲的影響。

```
1750344193.093 272 10.10.20.30 TCP_MISS_SSL/200 39 CONNECT tunnel://cisco.com:443/ "cisco\user@cisco.com" DIRECT/www.cisco.com-DECRYPT_WEBCAT_7-DefaultGroup-Authentication_Profile-DefaultGroup-NONE-NONE-DefaultGroup-NONE<"C_Cis",6.3,1,"-",-,-,-,-,"-",-,-,-,"-",-,-,"-","-",-,-,"IW_Com",-,"-","Computer","-","Unknown","Unknown","-","-","-",0.06,0,-,"-","-","-",-,"-",-,-,"-","-",-,-,"-",-,-> - - [ Request Details: ID = 169121930, User Agent = "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/137.0.0.0 Safari/537.36", AD Group Memberships = ( NTLMSSP ) "Cisco\Users" ] [ Tx Wait Times (in ms): 1st byte to server = 3, Request Header = 0, Request to Server = 0, 1st byte to client = 3 Response Header = 0, Client Body = 9 ] [ Rx Wait Times (in ms): 1st request byte = 0, Request Header = 0,Client Body = 0,1st response byte = 0,Response header = 0 Server response = 13, Disk Cache = 0; Auth response = 0, Auth total = 3; DNS response = 0, DNS total = 0 WBRS response = 0, WBRS total = 0, AVC response = 0, AVC total = 0, DCA response = 0, DCA total = 0, McAfee response = 0 McAfee total = 0, Sophos response = 0, Sophos total = 0, Webroot response = 0, Webroot total = 0,Anti-Spyware response=0 , Anti-Spyware total = 0; AMP response = 0, AMP total = 0; Latency = 143; " 19/Jun/2025:14:43:13 +0000" ] [Client Port = 57785, Server IP = 10.20.30.40, Server Port = 443]
```

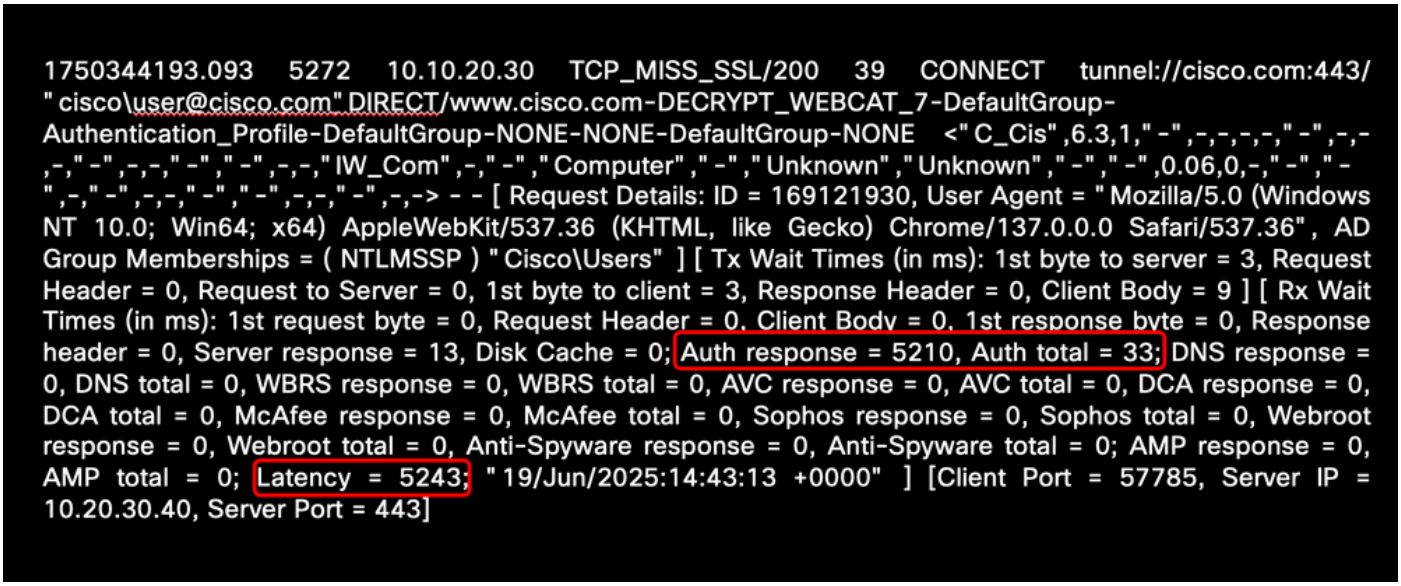
映像 — AccessLog中的效能引數

高身份驗證時間

如果驗證回應時間過長，則TAC需要以下資訊來更好更快地解決驗證延遲問題：

- 當前SWA配置
- 處於調試或跟蹤模式的身份驗證日誌
- 資料包捕獲來自
    - 客戶端電腦。
    - SWA（使用過濾器捕獲客戶端流量和到達在領域設定中配置的所有活動目錄的SWA流量。）
- 確保Accesslogs具有自定義欄位%m和%g，以識別身份驗證機制和組
- 重現問題時從客戶端發出HAR檔案
- testauthconfig命令從CLI的輸出

此範例顯示與驗證相關的高延遲時間：



影象 — 高身份驗證延遲的示例

高DNS時間

如果DNS響應時間過長，則TAC需要以下資訊來解決DNS延遲問題：

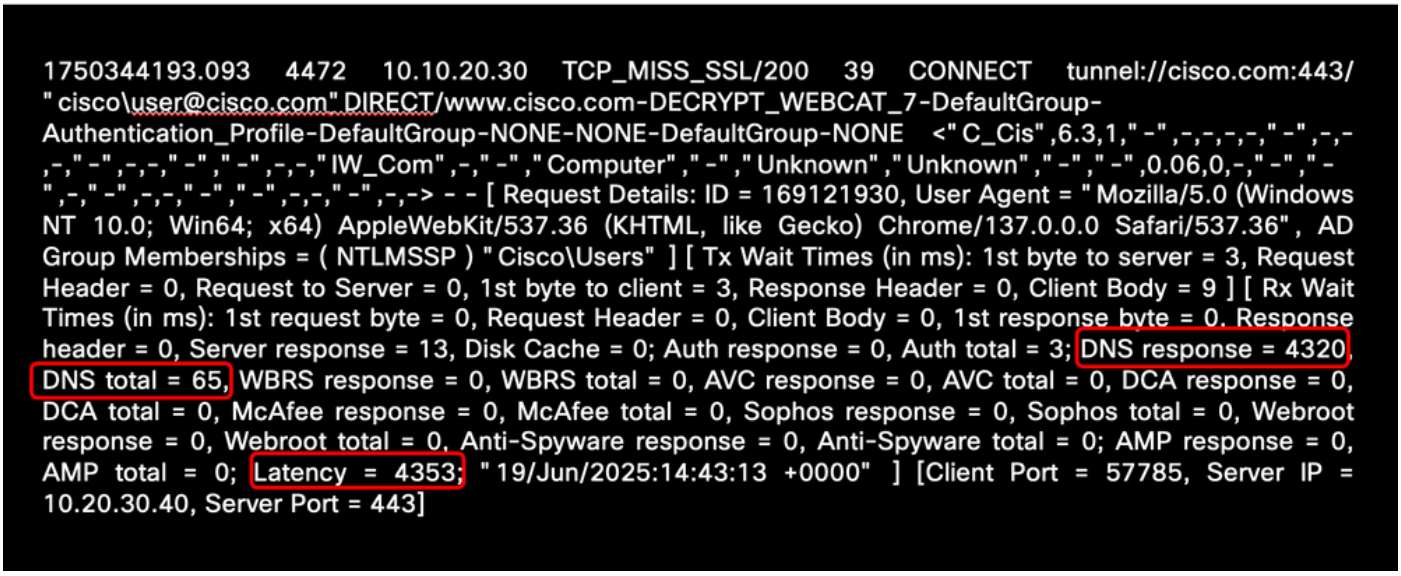
- 當前SWA配置
- 跟蹤模式下的系統日誌
- DNS伺服器IP地址
- 資料包捕獲來自
    - 客戶端電腦

- SWA（使用DNS伺服器IP地址進行過濾。）

- 確保訪問日誌在自定義欄位中同時具有%:<d和%:>d
- 重現問題時從客戶端發出HAR檔案

要瞭解有關DNS配置和故障排除的詳細資訊，請參閱安全Web裝置DNS服務故障排除」連結

此範例顯示與DNS名稱解析相關的高延遲時間：



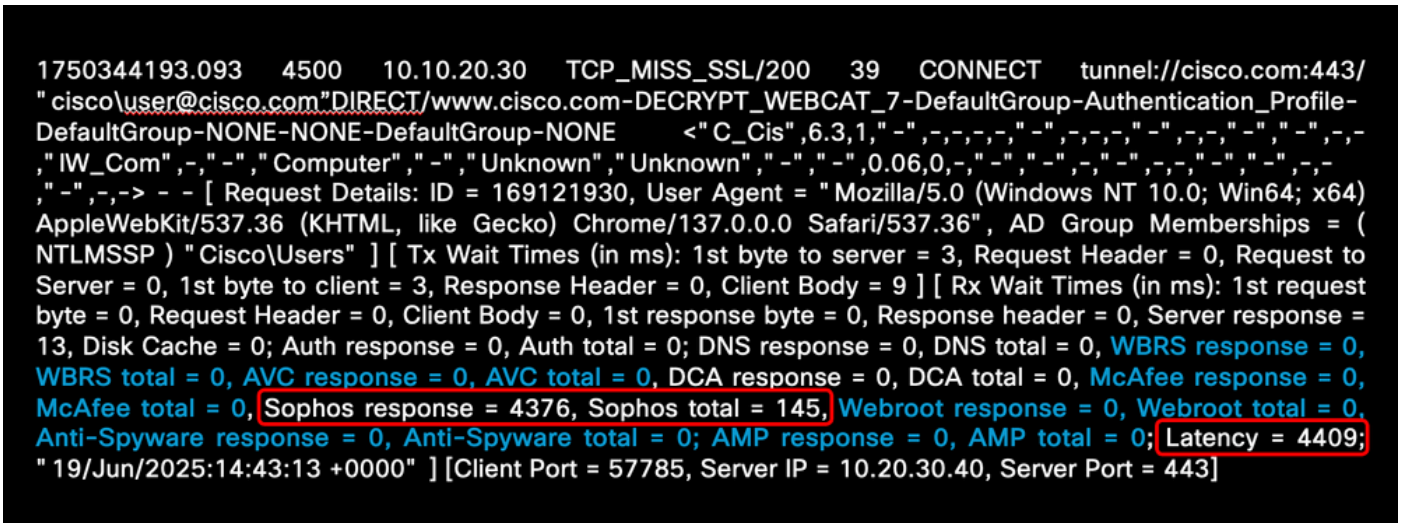
影象 — 高DNS解析延遲示例

掃描引擎時間過長

如果Web聲譽得分(WBRS)、應用與可見性控制(AVC)和惡意軟體掃描引擎的響應時間較長，則TAC需要以下資訊對掃描引擎高響應時間進行故障排除：

- 當前SWA配置。
- 根據響應時間較長的引擎，將日誌記錄級別更改為debug。

此示例顯示與Sophos引擎相關的高延遲時間：



影象 — 惡意軟體掃描引擎高延遲

如果掃描引擎顯示高響應，則為了立即恢復，可以使用以下步驟從CLI重新啟動掃描服務：

步驟1。輸入diagnostic並按Enter（這是一個隱藏命令，您需要鍵入確切的命令。）

步驟2.選擇SERVICES。

步驟3.要重新啟動WBRS服務，請選擇WBRS，否則跳至步驟6。

步驟4.選擇RESTART。

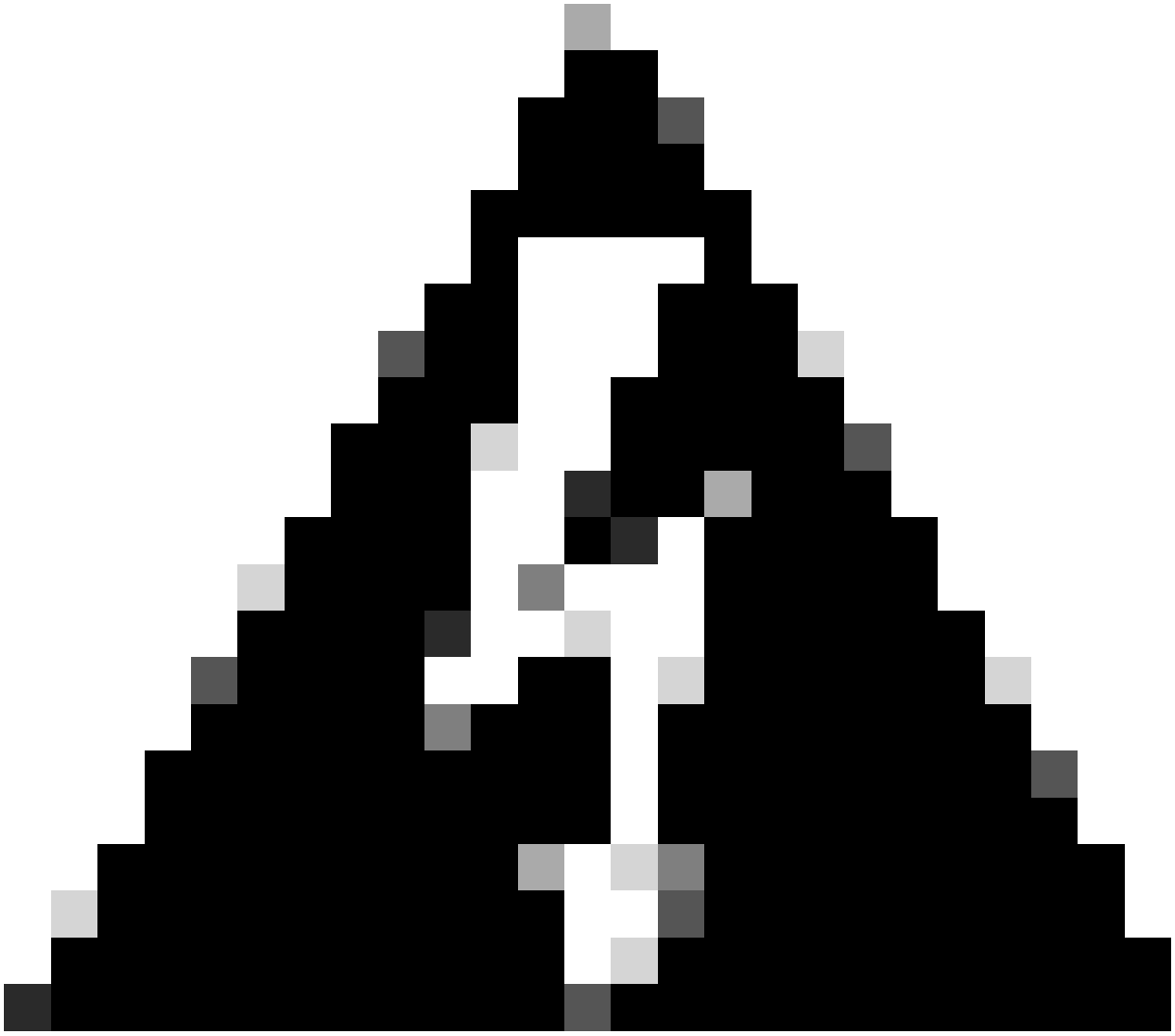
步驟5.繼續按Enter退出嚮導。

步驟6.如果您計畫重新啟動任何惡意軟體掃描引擎，請選擇ANTIVIRUS。

步驟7.選擇您的掃描器。

步驟8.選擇RESTART。

步驟9.繼續按Enter退出嚮導。



警告：重新啟動內部服務會導致服務中斷。建議在非生產時執行該操作，否則請注意。

連線資料包捕獲的最佳實踐

在執行任何資料包捕獲時，請收集此資訊並與Cisco TAC共用。

- 客戶端IP地址。
- 您嘗試訪問的URL。
- 為來自客戶端PC和SWA的URL解析的IP地址。
- 使用者體驗（例如頁面未載入或部分載入，如果存在任何錯誤消息，請擷取螢幕截圖）。
- 測試的時間戳。
- 關閉客戶端電腦上的所有其他瀏覽器和應用。訪問網站，在記事本中捕獲一次成功/失敗嘗試的日誌，並與思科支持共用。

有關如何在SWA中執行資料包捕獲的詳細資訊，請參閱在內容安全裝置上配置資料包捕獲連結

配置複雜性

高延遲和效能低下的另一個常見原因是配置複雜性。當SWA配置的條件、配置檔案和策略數量過多時，會發生這種情況。這種複雜性會顯著增加響應時間並加重代理進程的負擔。當流量達到最高點時，此問題通常會在高峰時段更加明顯。

以下是最佳化配置的一些提示：

1. 限制HTTPS解密：僅解密對您的安全策略至關重要的流量。儘可能減少處理開銷，同時保持安全性。
2. 優先使用策略以提高效率：在策略清單的頂部排列最常用的策略。這通過首先解決要求最苛刻的流量確保了更快的處理。
3. 簡化策略設計：通過儘可能減少策略數量來簡化策略。這減少了不必要的處理並提高了整體系統效能。
4. 最佳化防惡意軟體和防病毒掃描：檢視防惡意軟體和防病毒流程的掃描配置。它們可能佔用大量CPU，因此微調它們可以顯著降低資源消耗，同時不影響安全性。
5. 使用輕量正規表示式：避免使用複雜或資源密集的正規表示式。確保點(.)和星號(*)等字元正確轉義，以減少處理負擔，防止低效。

有關SWA最佳實踐的詳細資訊，請訪問使用安全Web裝置最佳實踐

CLI命令

版本

使用version命令驗證硬體分配（用於虛擬SWA）和RAID狀態（用於物理SWA）。檢查硬體配置：確保按預期分配了CPU核心、記憶體和硬碟數量。在虛擬模型中，RAID狀態顯示為「未知」，如果物理裝置中的RAID狀態為「已降級」或「失敗」，請與Cisco TAC聯絡以從後端檢視磁碟狀態。

以下是分配更多CPU到SWA可能導致不當行為的示例：

```
SWA Lab> version
Current Version
===============
Product: Cisco S100V Secure Web Appliance
Model: S100V
BIOS: 6.00
CPUs: 3 expected, 4 allocated
Memory: 8192 MB expected, 8192 MB allocated
Hard disk: 200 GB, or 250 GB expected; 200 GB allocated
RAID: NA
RAID Status: Optimal
```

顯示警報

使用displayalerts命令檢查可指示根本原因的SWA網路相關警報消息。

在本示例中，IP地址為10.10.10.10的DNS伺服器沒有響應，消息「The File Reputation service is not reachable」可能表示網路連線問題。

```
SWA LAB> displayalerts
Date and Time Stamp           Description
--------------------------------------------------------------------------------
26 Mar 2025 11:20:07 +0500 The File Reputation service is not reachable.
26 Mar 2025 11:20:07 +0500 Critical: Reached maximum failures querying DNS server 10.10.10.10
26 Mar 2025 11:20:07 +0500 Critical: Reached maximum failures querying DNS server 10.10.10.10
26 Mar 2025 10:16:18 +0500 Warning: Communication with the File Reputation service has been established
```

process_status

使用process_status命令檢視SWA內部服務的進程和記憶體使用情況。

如果Prox進程（處理流量代理的主要進程）在幾分鐘內始終超過100%的使用率，則表明進程上的負載持續較高。但是，Prox或其他進程上的CPU使用率偶爾短暫的峰值是正常的，而且是預期的。

<#root>

```
SWA LAB> process_status
USER     PID
```

%CPU

%MEM

```
   VSZ     RSS TT  STAT STARTED           TIME
```

COMMAND

```
root      11 2805.4  0.0       0     512  -  RNL  28Jun24 11863204:12.63 idle
root   71189
```

102.0

19.5

```
 6670700 6478032  -  R    23Feb25    18076:32.80
```

prox

```
root   91880   99.0  0.6  369564  214832  -  R    28Jun24    58854:51.78 counterd
root   91267   76.0  0.9  379804  292324  -  R    28Jun24    59371:01.26 counterd
root      12   25.9  0.0       0    1600  -  WL   28Jun24    30899:57.88 intr
root   46955   25.0  0.2   91260   59336  -  S    23Jan25     7547:02.96 wbnpd
root   95056   23.0 11.2 5369332 3710348  -  I    28Jun24    31719:23.99 java
root   93190   12.0  1.4 3118384  456088  -  S    01:15         29:57.05 beakerd
root   64579   11.0  0.2  101336   71204  -  S     6Aug24    12074:55.55 coeuslogd
```

狀態詳細資訊

status detail命令提供系統資源使用情況、網路流量度量和連線統計資訊的即時摘要，反映SWA的整體運行狀況和效能。它映象GUI中的「System Status（系統狀態）」檢視，以便進行快速監控和故障排除。

<#root>

```
SWA LAB> Status detail

Status as of:                  Wed Mar 26 11:51:27 2025 PKT


Up since:                      Fri Jun 28 13:45:43 2024 PKT (270d 22h 5m 43s)


System Resource Utilization:

CPU                                    16.0%


  RAM                                  10.3%


  Reporting/Logging Disk               19.8%


Transactions per Second:
  Average in last minute                1745
  Maximum in last hour                  2210
  Average in last hour                  1708
  Maximum since proxy restart           2451
  Average since proxy restart            615
Bandwidth (Mbps):
  Average in last minute              149.699
  Maximum in last hour               1356.387
  Average in last hour                229.634
  Maximum since proxy restart       22075.244
  Average since proxy restart          60.689
Response Time (ms):
  Average in last minute                  99
  Maximum in last hour                 8194128
  Average in last hour                    87
  Maximum since proxy restart          19608632
  Average since proxy restart             28
Cache Hit Rate:
  Average in last minute                   3
  Maximum in last hour                     6
  Average in last hour                     2
  Maximum since proxy restart             89
  Average since proxy restart              2
Connections:
  Idle client connections               3481
  Idle server connections                754


Total client connections               21866
```

```
  Total server connections               19049


SSLJobs:
  In queue Avg in last minute                0
  Average in last minute                 12050
  SSLInfo Average in last min                0
Network Events:
  Average in last minute                  16.0
  Maximum in last minute                   171
  Network events in last min            151918
```

Ipcheck

ipcheck命令顯示安全Web裝置的詳細系統資訊，包括硬體規格、磁碟使用情況、網路介面、已安裝軟體金鑰和版本詳細資訊，從而提供裝置當前狀態的綜合快照。

<#root>

```
SWA LAB > ipcheck
  Ipcheck Rev           1
  Date                  Fri Mar 21 16:34:56 2025
  Model                 S100V
  Platform              vmware (VMware Virtual Platform)
  Secure Web Appliance Version  Version: 15.2.1-011
  Build Date            2024-10-03
  Install Date          2025-02-13 17:49:24
  Burn-in Date          Unknown
  BIOS Version          6.00
  RAID Version          NA
  RAID Status           Unknown
  RAID Type             NA
  RAID Chunk            Unknown
  BMC Version           NA
  Disk 0                200GB VMware Virtual disk 1.0 at mpt0 bus 0 scbus2 target 0 lun 0
  Disk Total            200GB

  Root                  4GB 64%


  Nextroot              4GB 65%


  Var                   400MB 38%


  Log                   130GB 24%


  DB                    2GB 0%


  Swap                  8GB
  Proxy Cache           50GB
```

```
  RAM Total             8192M
```

速率

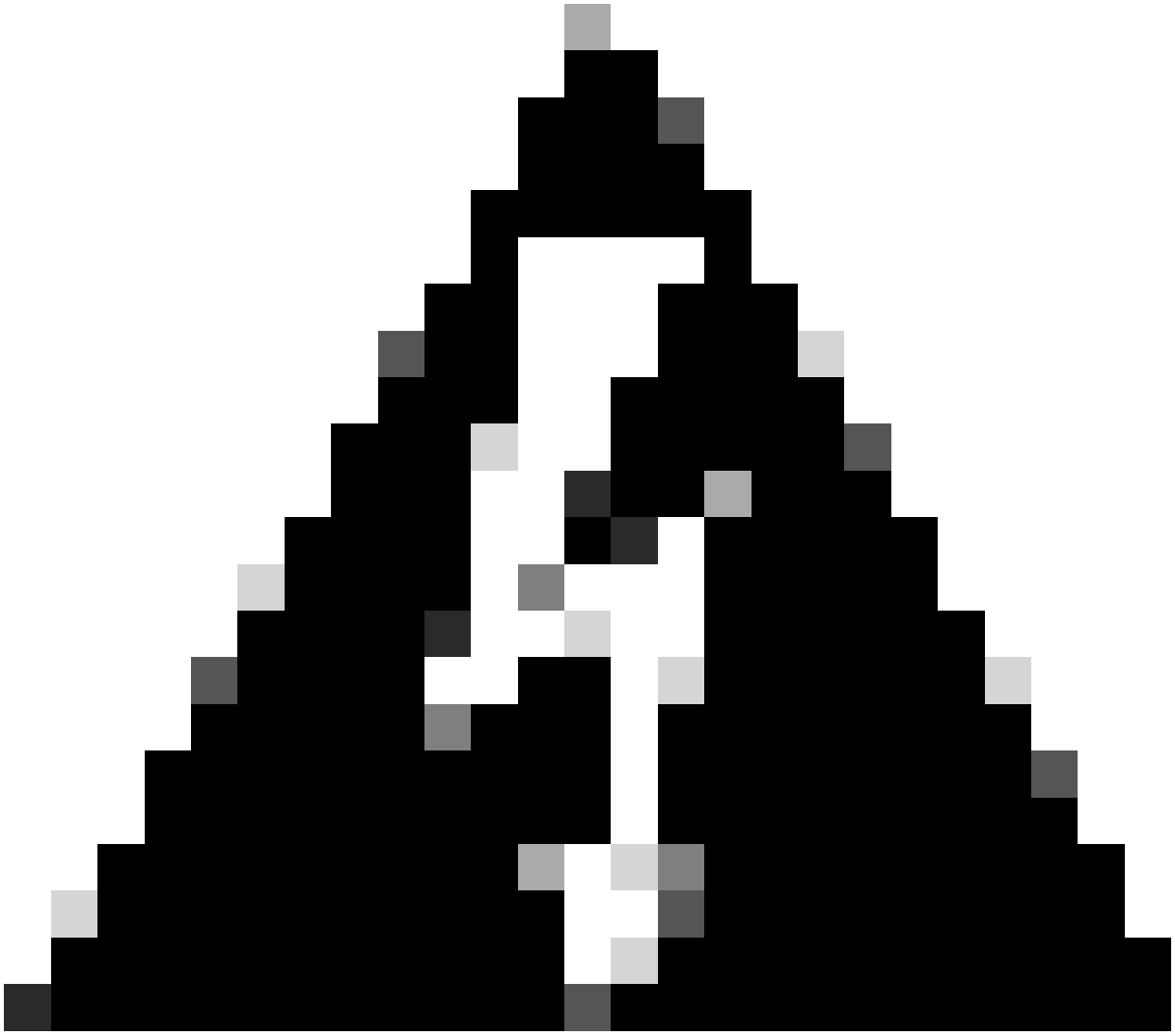
rate命令列印每10秒的連線速率和每秒請求數。

<#root>

```
SWA LAB> rate
Press Ctrl-C to stop.

%proxy  reqs                        client    server    %bw  disk disk

  CPU  /sec    hits blocks misses    kb/sec    kb/sec  saved  wrs   rds

100.00  1800     17  16352   1626    178551    178551    0.0  2366   0

100.00  1813     18  16453   1659    226301    224952    0.6  3008   0

99.00  1799      10  16338   1645    206234    206234    0.0  3430   1
```

收集高延遲日誌

這取決於您看到的訪問日誌響應時間較高或SHD日誌進程負載較高部分，為了進行進一步的故障排除，最好將相應的日誌訂閱更改為Debug。



警告：將日誌級別設定為debug或trace會導致資源使用率增加，並導致日誌檔案快速旋轉或覆蓋。

訪問日誌欄位	SHD日誌欄位	相應的日誌訂閱
身份驗證響應，身份驗證總計	—	authlogs
DNS響應，DNS總計	—	系統日誌
WBRS響應，WBRS總計	Wbrs_WucLd	聯絡Cisco TAC
AVC響應，AVC總計	—	avc_logs

McAfee響應， McAfee總計	McafeeLd	mcafee_logs
Sophos響應，Sophos總計	SophosLd	sophos_logs
Webroot響應， Webroot總計	WebrootLd	webrootlogs
AMP響應，AMP總計	AMPLd	amp_logs

相關資訊

使用SHD日誌排除安全Web裝置效能故障

訪問安全Web裝置日誌

在內容安全裝置上配置資料包捕獲

使用安全Web裝置最佳做法

配置訪問日誌中的效能引數

排除SWA中的異常進程狀態故障

確定SWA中的解密速率

對安全Web裝置DNS服務進行故障排除

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）。