排除安全Web设备延迟故障

目录

简介

本文档介绍在思科安全网络设备(SWA)中解决高延迟、高磁盘和高CPU问题的故障排除步骤。

先决条件

要求

Cisco 建议您了解以下主题：

- 思科SWA管理
- 代理部署方法（显式和透明）
- SWA命令行界面(CLI)命令

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。

背景信息

在联系Cisco技术支持时，您需要提供有关SWA出站和入站网络活动的详细信息，可以通过运行数据包捕获来监控此活动，从而收集流量以供调试或验证之用。

SWA高延迟的常见原因

一般来说，SWA中的高延迟主要有三个类别：

1. SWA规模不足或资源过载
2.复杂配置
3.与网络相关的延迟问题

在SWA中，导致高延迟的最常见原因之一是解决方案的规模不足。适当的规模对于确保SWA系统有足够资源处理当前和预期工作负载至关重要。如果系统规模过小，它可能难以有效地处理请求，从而导致运营延迟和性能降低。在部署过程中，必须仔细评估用户数量、解密量和特定扫描需求等因素，以避免资源限制。如果SWA容量无法与组织需求保持一致，可能导致持续延迟和降低用户体验。

复杂的配置会降低性能并导致SWA上的延迟，特别是在高负载下，因为每个请求都必须经过多种条件处理。

网络相关延迟可能源于SWA本身、第三方服务（如Active Directory、DLP、DNS）或客户端、SWA和上游服务器之间的网络延迟。

分析发送到SWA的请求，包括识别排名靠前的用户和访问次数最多的URL，有助于发现潜在的不当行为和查明延迟的根本原因。这些信息对于诊断性能问题、管理带宽消耗和确保系统的正确使用非常宝贵。

SWA延迟故障排除工具

系统状态

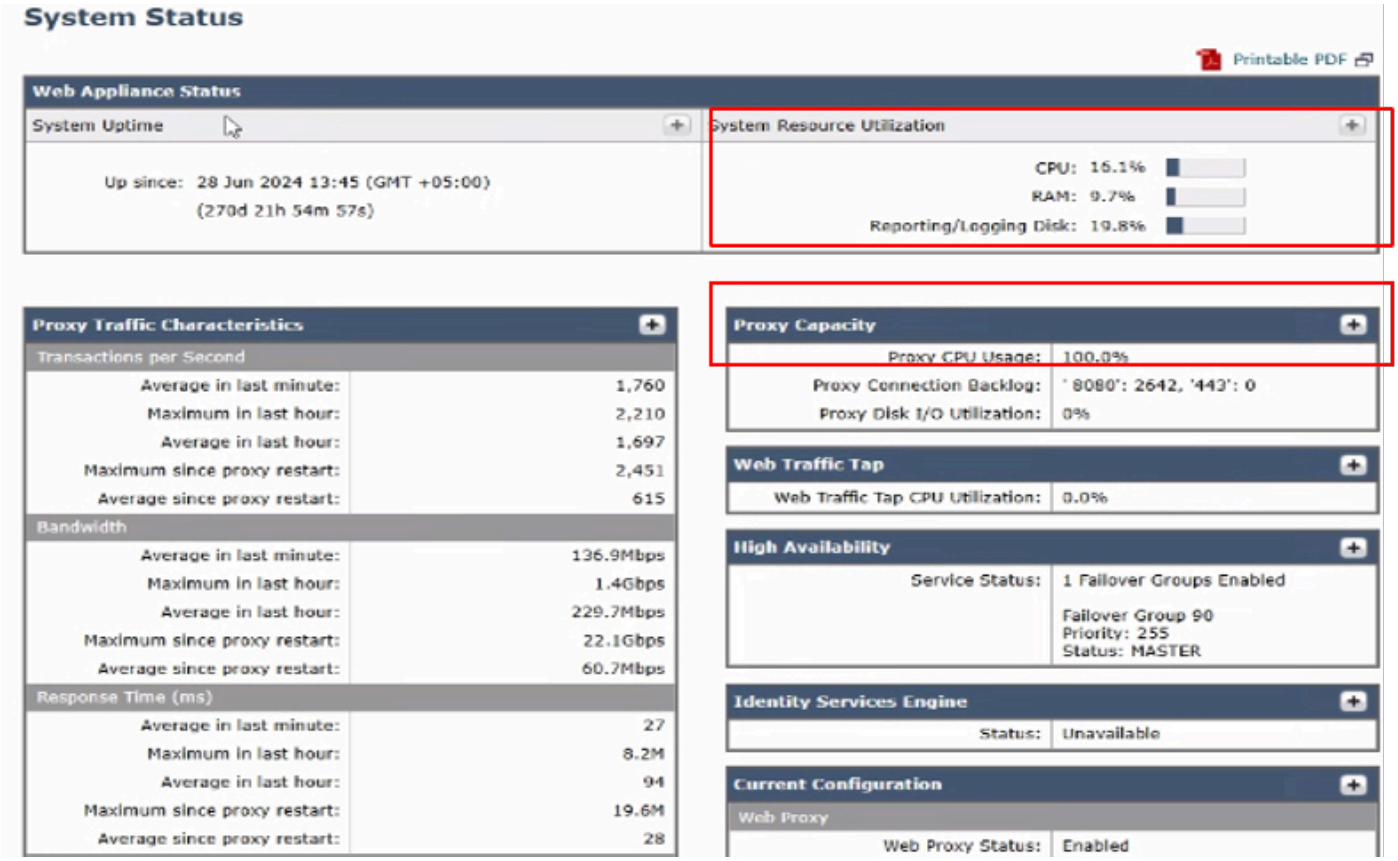
使用以下步骤检查SWA中的当前资源消耗：

步骤1.访问SWA图形用户界面(GUI)。

第2步：导航到报告>系统信息>系统状态。

步骤3.检查以下关键指标以评估系统性能：

- CPU使用率(%):指示当前CPU负载
- RAM使用率(%):反映内存利用率
- 报告/日志记录使用率(%):显示用于报告和日志记录的磁盘空间百分比
- 系统运行时间:显示系统未重新启动而运行的总时间



映像 — 系统状态

此页提供RAM、CPU和磁盘使用率的当前状态的概览。要查看一段时间的资源使用情况，请从SWA GUI导航到报告，然后选择系统容量。

系统容量

SWA中的System Capacity页面提供指定时间范围内资源利用率和性能度量的综合视图。此页面提供详细的图表，以帮助监控和分析系统行为，确保最佳性能并确定潜在的瓶颈。

“系统容量”(System Capacity)页面中的“可用图形和度量”(Available Graphs and Metrics)如下：

1. 总体CPU使用率：显示总CPU使用率，提供系统性能的高级概述。
2. 按功能划分的CPU使用情况：根据特定功能划分CPU使用情况，包括：

- Web代理
- 日志记录
- 报告
- McAfee
- Sophos
- Webroot
- 可接受的使用和信誉

3.响应时间/延迟（毫秒）：跟踪响应时间，以确定处理请求过程中的任何延迟。

4.每秒交易数：显示SWA每秒处理的事务数。

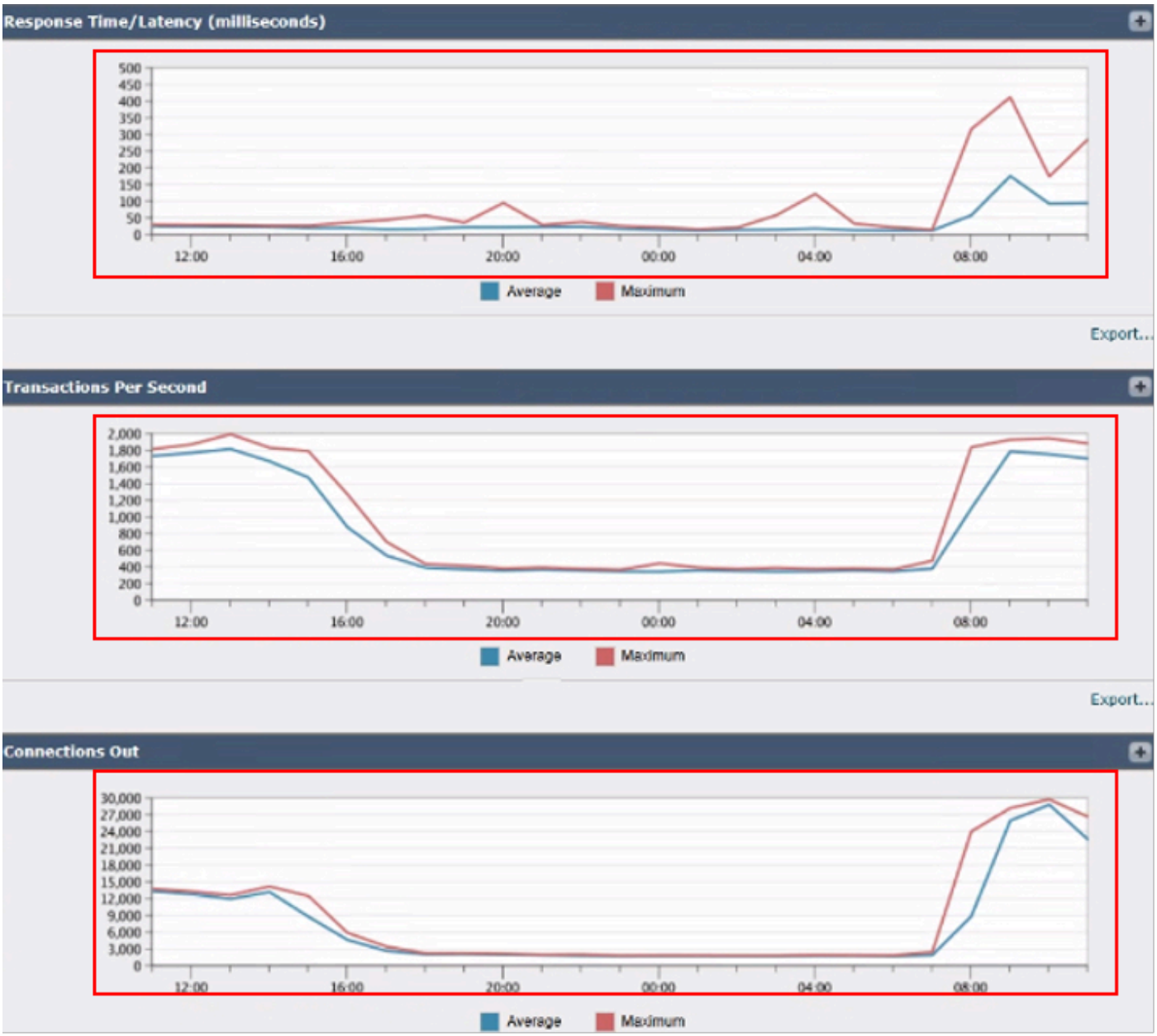
5.外部连接：监控正在建立的出站连接数。

6.输出带宽（字节）：测量使用的出站带宽量。

7.代理缓冲区内存(%):显示代理进程使用的内存百分比。

检查指标以了解此控制面板中是否有任何高资源使用率的迹象。

映像 — 系统容量



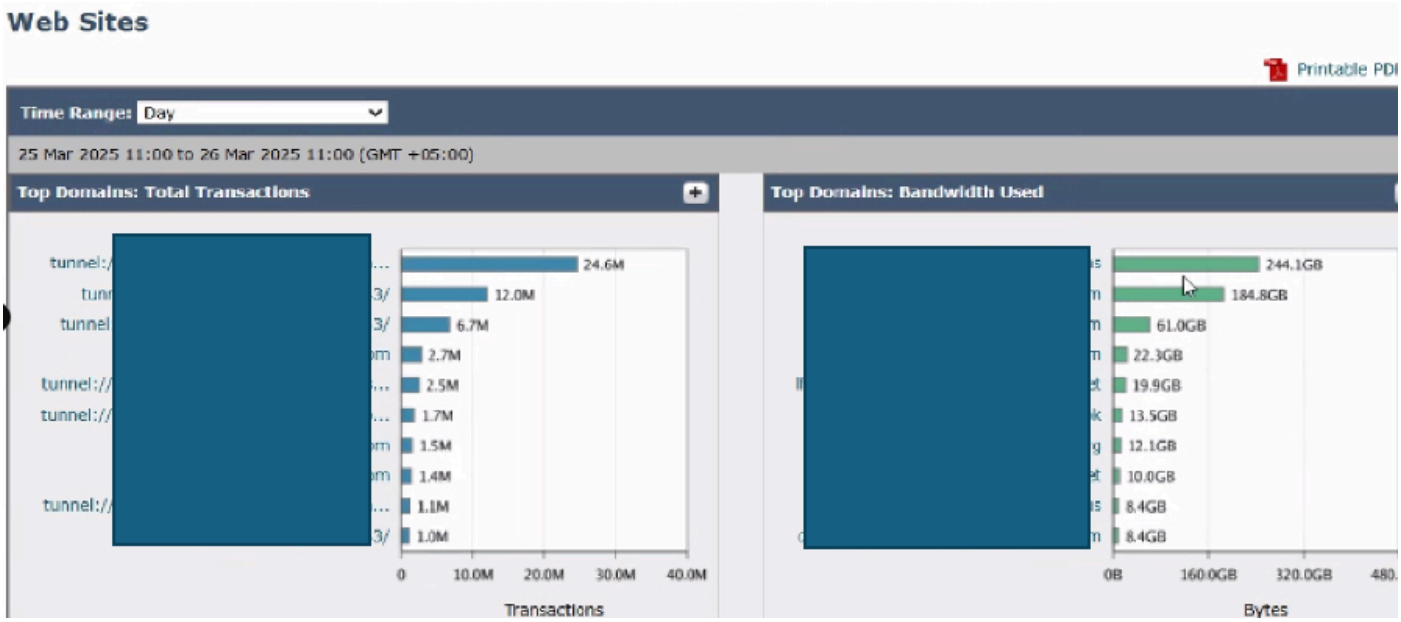
映像 — 每秒的SWA事务数及连接输出

映像 — SWA内存使用情况

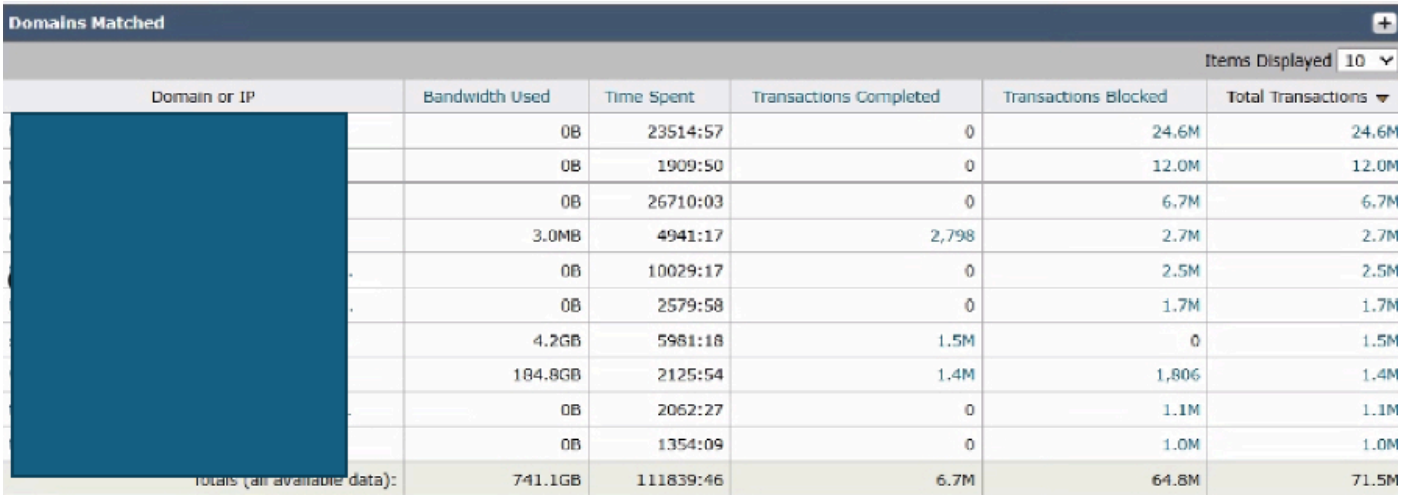
分析排名靠前的目标

要分析排名靠前的目标，请导航到SWA GUI，导航到报告，然后选择网站。查看排名靠前的HTTP/HTTPS网站列表并确定高流量或经常访问的域。

根据您的调查结果，考虑绕过或免除通用URL，例如Microsoft Updates、Adobe、Office365和在线会议平台。此方法有助于减少SWA上的流量，从而降低延迟和代理处理负载。



图像 — SWA热门网站控制面板



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

图像 — SWA顶级域控制面板

分析顶级用户

要确定可能产生的过多流量，请从报告选择用户导航到SWA GUI。

查看列表，确定哪些用户正在向SWA生成最大数量的事务。此外，还要检查哪些用户计算机生成了最大数量的事务到SWA并消耗了最大带宽。

此分析可帮助确定负责大量流量负载的用户或设备，从而实施有针对性的操作来减轻整体系统压力。

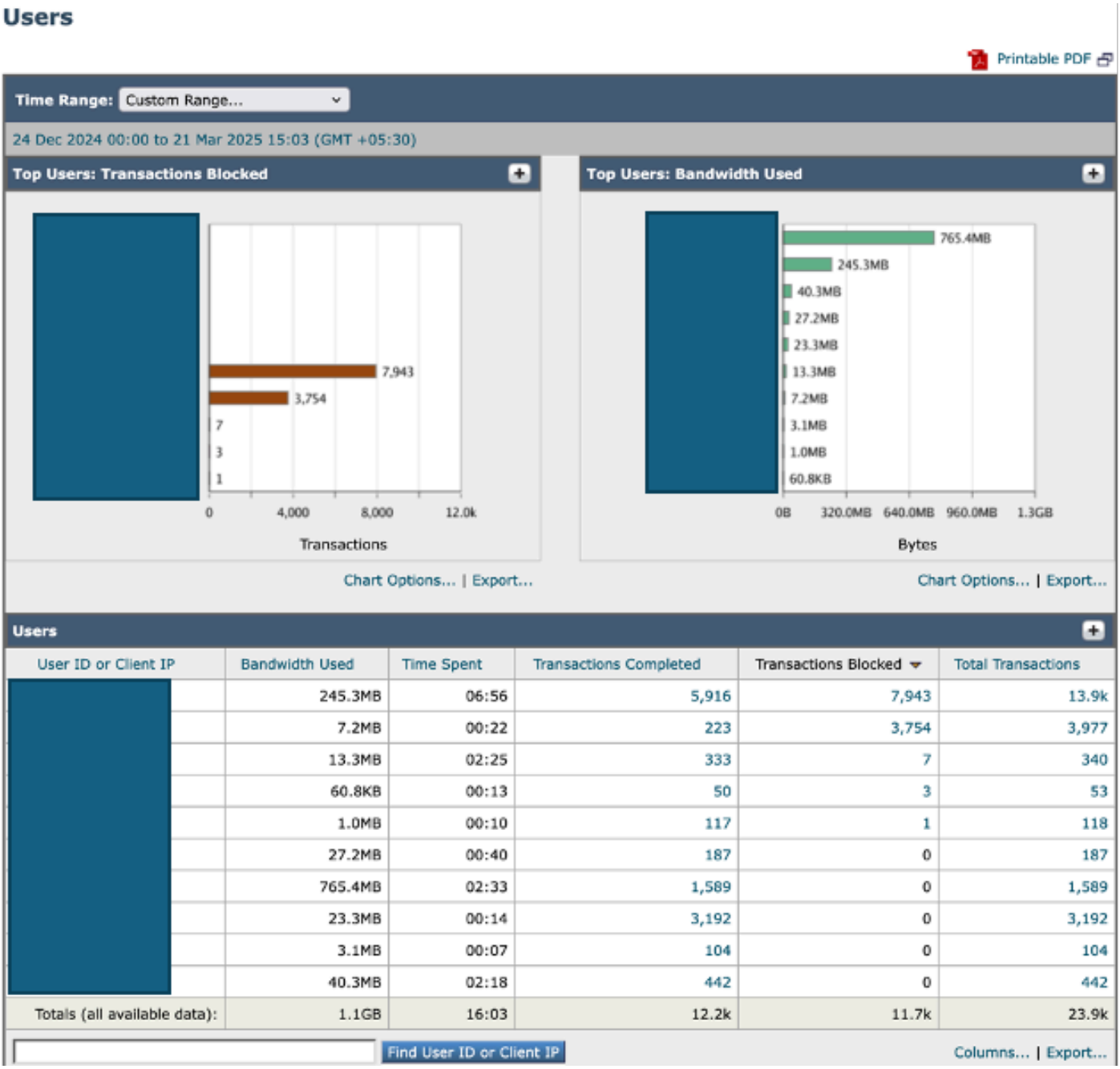


Image-SWA主要用户控制面板

SHD日志

通过查看SHD_log，您可以分析某些性能指标，例如从用户到SWA的会话数(CliConn)、从SWA到Internet的会话数(SrvConn)、每秒平均请求数(Reqs)等。

有关SHD日志的详细信息，请参阅使用SHD日志排除安全Web设备性能故障链接

在SHD日志中需要查看的一些关键参数包括：

- 客户端连接：活动客户端连接数
- 服务器连接：活动服务器连接数
- 代理Ld:平均代理进程负载

- CPULD:平均总CPU负载
- RAMUTIL:RAM利用率
- 延迟：一分钟内的平均服务时间
- DiskUtil:磁盘使用率和I/O性能

在本例中，每秒1,600个请求会导致较高的代理进程负载。

```
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
```

使用访问日志排除延迟问题

当通过SWA代理的流量出现延迟问题时，访问日志可用作确定可能根本原因的有用工具。要增强故障排除工作，您可以修改现有访问日志设置或创建新的访问日志。通过在自定义字段中包含性能参数，您可以更深入地了解导致延迟的因素，从而更有效地进行分析和解决问题。

有关性能参数和配置步骤的详细信息，请参阅链接：在访问日志中配置性能参数

以下是在SWA中收集日志的详细指南：访问安全Web设备日志

可以通过检查关键参数来分析延迟源，这些参数有助于确定客户端和SWA、SWA内部进程之间或SWA和Web服务器之间是否出现延迟。需要考虑的重要指标包括基于网络的服务，例如DNS解析、身份验证时间以及服务器或客户端响应时间。此外，必须评估扫描引擎（如AMP、Sophos和AVC）导致的延迟，以确定其对整体延迟的影响。

```
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]
```

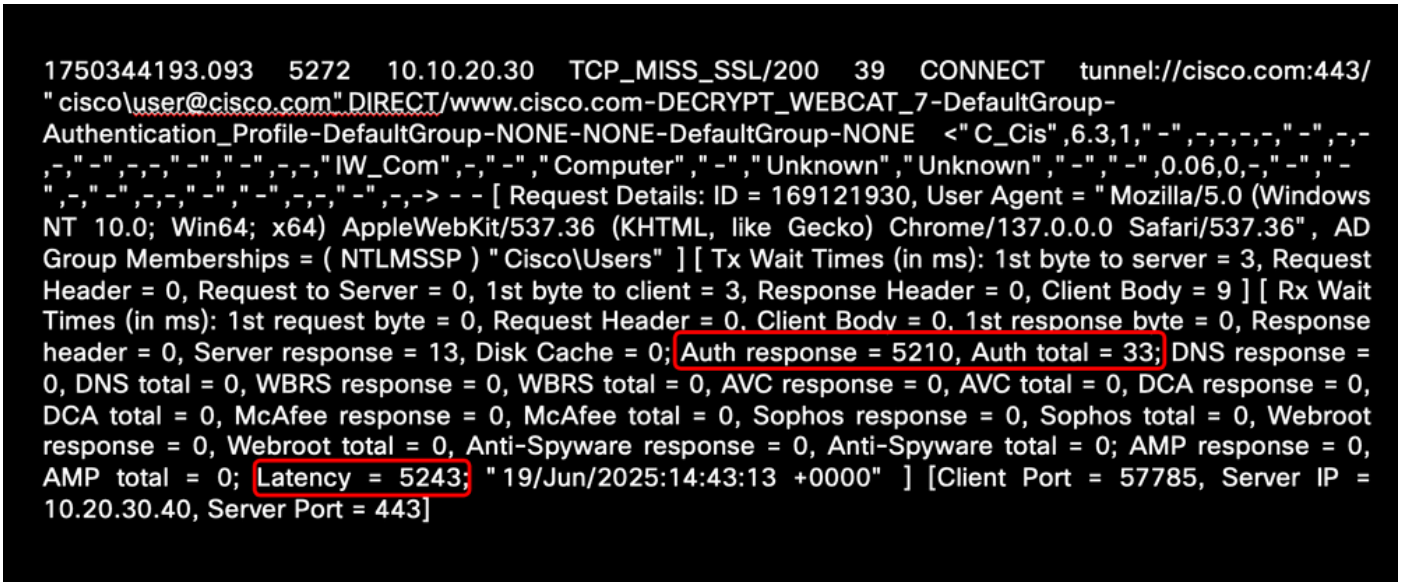
映像 — 访问日志中的性能参数

高身份验证时间

如果身份验证响应时间过长，则TAC需要以下信息来更好更快地排除身份验证延迟故障：

- 当前SWA配置
- 在调试或跟踪模式下的身份验证日志
- 数据包捕获来自
    - 客户端计算机。
    - SWA（使用过滤器捕获客户端流量和流向领域设置中配置的所有活动目录的SWA流量。）
- 确保Accesslogs具有自定义字段%m和%g，以标识身份验证机制和组
- 重现问题时来自客户端的HAR文件
- testauthconfig命令从CLI的输出

此示例显示与身份验证相关的高延迟时间：



图像 — 高身份验证延迟示例

高DNS时间

如果DNS响应时间过长，则TAC需要以下信息来解决DNS延迟问题：

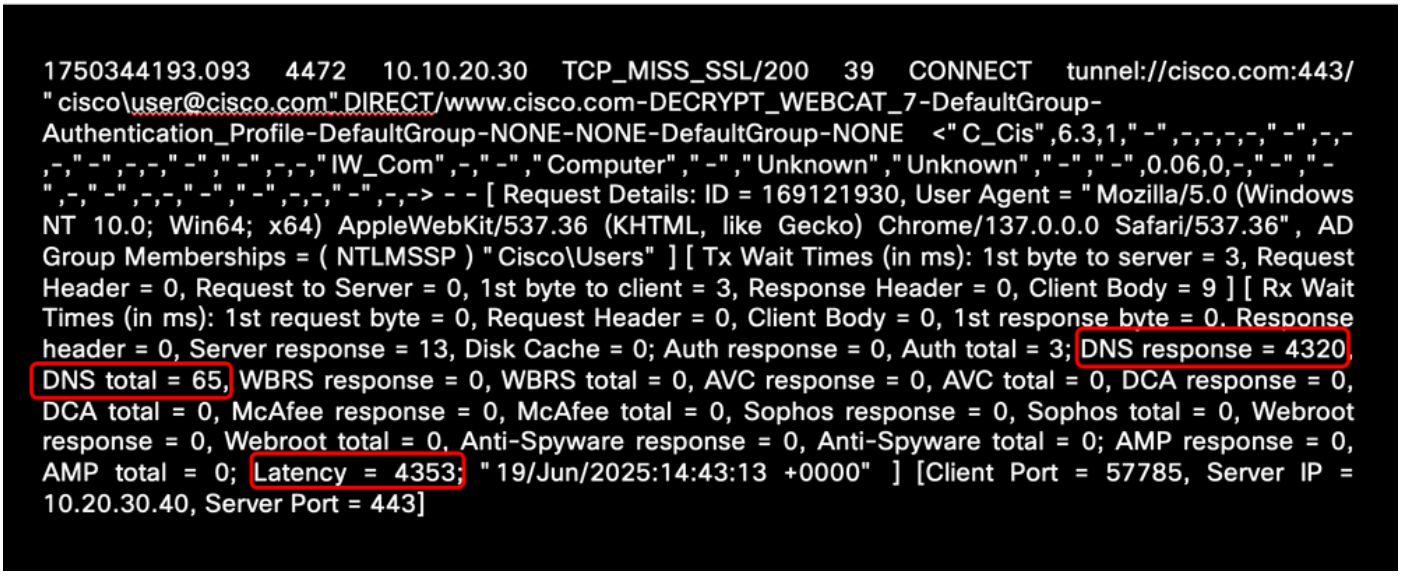
- 当前SWA配置
- 跟踪模式下的系统日志
- DNS服务器IP地址
- 数据包捕获来自
    - 客户端计算机

- SWA（使用DNS服务器IP地址过滤。）

- 确保您的访问日志在自定义字段中同时包含%:<d和%:>d
- 重现问题时来自客户端的HAR文件

要了解有关DNS配置和故障排除的详细信息，请参阅对安全Web设备DNS服务进行故障排除链接

此示例显示与DNS名称解析相关的高延迟时间：



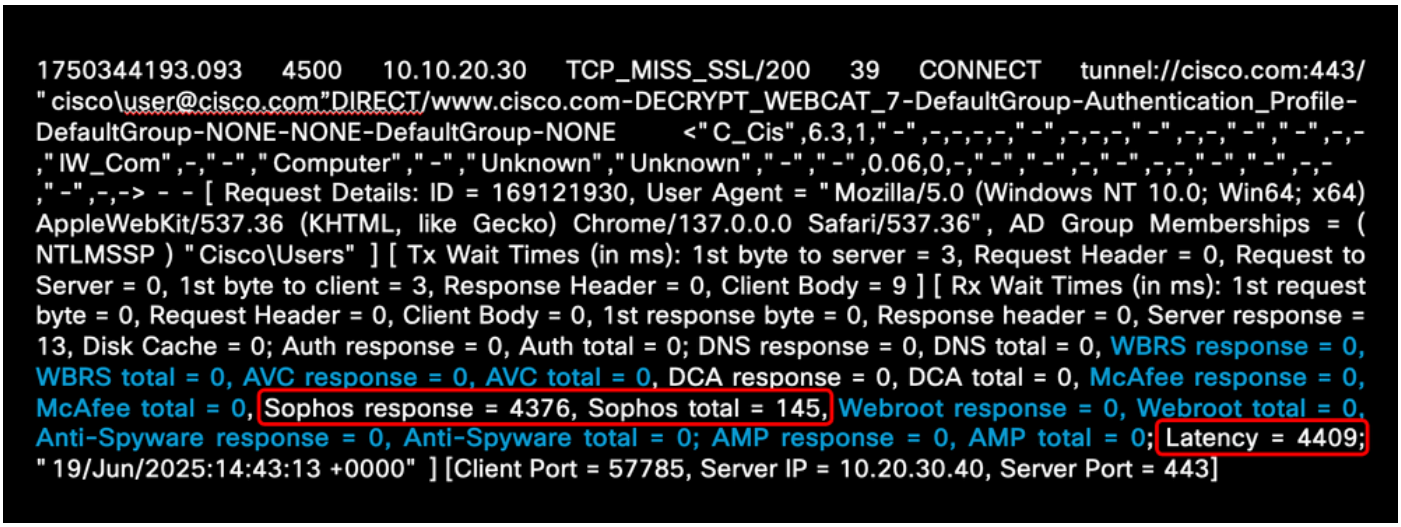
图像 — 高DNS解析延迟示例

扫描引擎时间过长

如果Web信誉得分(WBRS)、应用和可见性控制(AVC)以及恶意软件扫描引擎的响应时间较长，则TAC需要以下信息对扫描引擎高响应时间进行故障排除：

- 当前SWA配置。
- 根据响应时间较长的引擎，将日志记录级别更改为debug。

此示例显示与Sophos引擎相关的高延迟时间：



图像 — 恶意软件扫描引擎高延迟

如果扫描引擎显示高响应，则对于立即恢复，可以使用以下步骤从CLI重新启动扫描服务：

步骤1.键入diagnostic，然后按Enter（这是一个隐藏命令，您需要键入确切的命令。）

步骤2.选择SERVICES。

步骤3.要重新启动WBRS服务，请选择WBRS，否则跳到步骤6。

步骤4.选择RESTART。

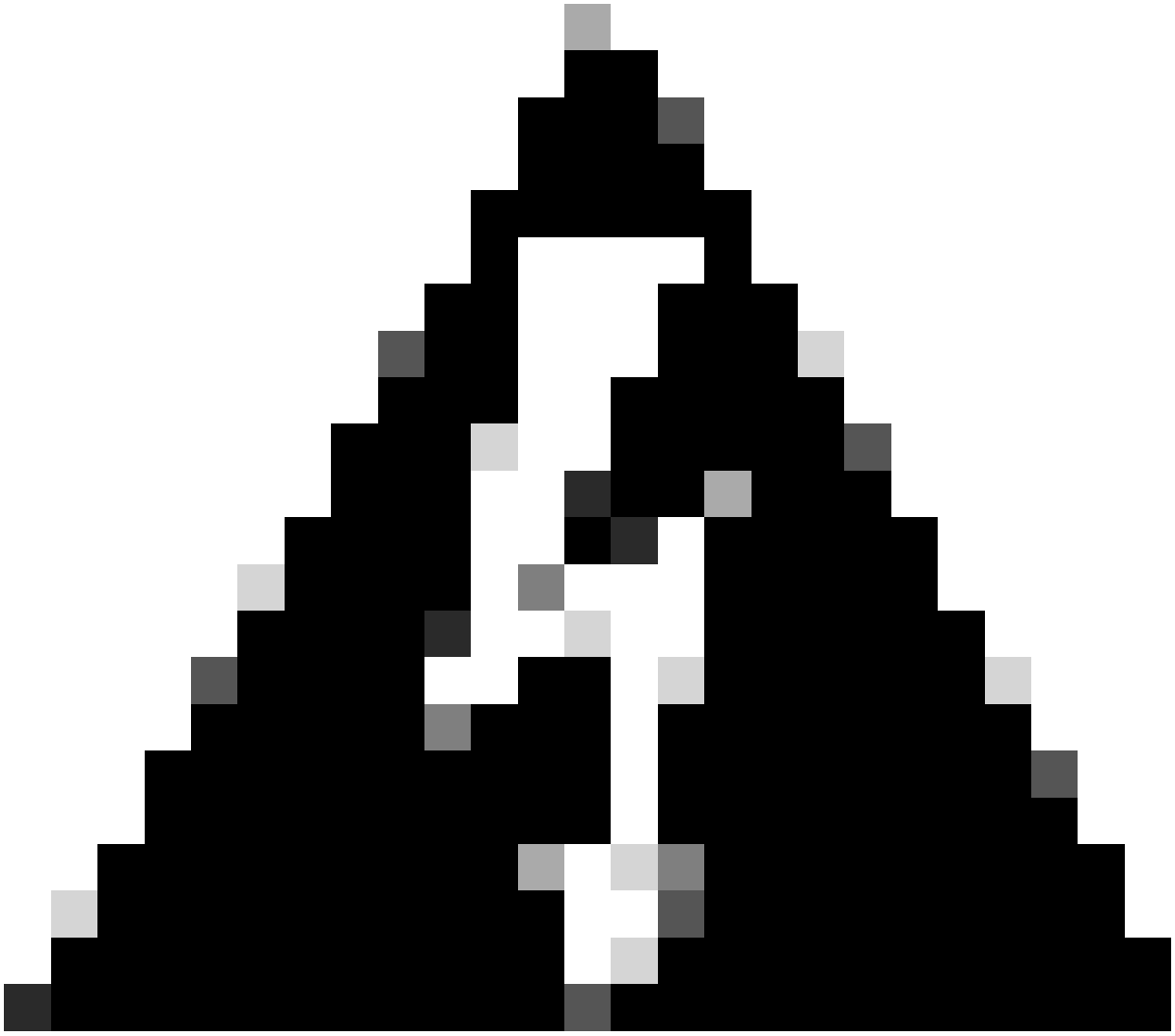
步骤5.继续按Enter退出向导。

步骤6.如果您计划重新启动任何恶意软件扫描引擎，请选择ANTIVIRUS。

步骤7.选择您的扫描仪。

步骤8.选择RESTART。

步骤9.继续按Enter退出向导。



警告：重新启动内部服务会导致服务中断。建议在非生产时执行该操作，否则请小心执行。

连接数据包捕获时的最佳实践

在执行任何数据包捕获时，请收集此信息并与思科TAC共享。

- 客户端 IP 地址.
- 您尝试访问的URL。
- 为来自客户端PC和SWA的URL解析的IP地址。
- 用户体验（例如页面未加载或有部分加载，如果出现任何错误消息，请截取屏幕截图）。
- 测试的时间戳。
- 关闭客户端计算机上的所有其他浏览器和应用。访问网站，在记事本中捕获一次成功/失败尝试的日志，并与思科支持共享。

有关如何在SWA中执行数据包捕获的详细信息，请参阅链接在内容安全设备上配置数据包捕获

配置复杂性

高延迟和性能差的另一个常见原因是配置复杂性。当SWA配置了过多条件、配置文件和策略时，会发生这种情况。这种复杂性会显着增加响应时间并给代理进程带来沉重负担。当流量处于最高水平时，这一问题往往会在高峰期更加明显。

以下是优化配置的一些提示：

1. 限制HTTPS解密：仅解密对安全策略至关重要的流量。尽可能减少处理开销，同时保持安全性。
2. 确定策略优先级，提高效率：在策略列表的顶部安排最常用的策略。这通过首先处理要求最苛刻的流量确保了更快的处理。
3. 简化策略设计：通过尽可能减少策略数量来简化策略。这样可以减少不必要的处理并提高整体系统性能。
4. 优化防恶意软件和防病毒扫描：查看防恶意软件和防病毒流程的扫描配置。它们可能占用大量CPU，因此微调它们可以显着降低资源消耗，而不会影响安全性。
5. 使用轻量正则表达式：避免使用复杂或资源密集的正则表达式。确保点(.)和星号(*)等字符正确转义，以减少处理负担并防止效率低下。

有关SWA最佳实践的详细信息，请访问使用安全Web设备最佳实践

CLI命令

version

使用version命令验证硬件分配（用于虚拟SWA）和RAID状态（用于物理SWA）。检查硬件配置：确保CPU核心、内存和硬盘数量按预期分配。在虚拟模型中，RAID状态显示为“未知”，如果RAID状态在物理设备中为“降级”或“失败”，请与Cisco TAC联系以便从后端查看磁盘状态。

下面是分配更多CPU到SWA的示例，该示例可能导致错误行为：

```
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
```

显示警报

使用displayalerts命令检查可指示根本原因的SWA网络相关警报消息。

在本示例中，IP地址为10.10.10.10的DNS服务器没有响应，消息“The File Reputation service is not reachable”可能表示网络连接问题。

```
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命令查看SWA内部服务的进程和内存使用情况。

如果Prox进程（处理流量代理的主要进程）在几分钟内持续超过100%的使用率，则表明该进程持续承受高负载。但是，Prox或其他进程上的CPU使用率偶尔短暂峰值是正常且预期的。

<#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
```

状态详细信息

status detail命令提供系统资源使用情况、网络流量指标和连接统计信息的实时摘要，反映SWA的整体运行状况和性能。它镜像GUI中的“系统状态”视图，以便快速监控和故障排除。

<#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命令显示安全Web设备的详细系统信息，包括硬件规格、磁盘使用情况、网络接口、已安装软件密钥和版本详细信息，从而提供设备当前状态的全面快照。

<#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

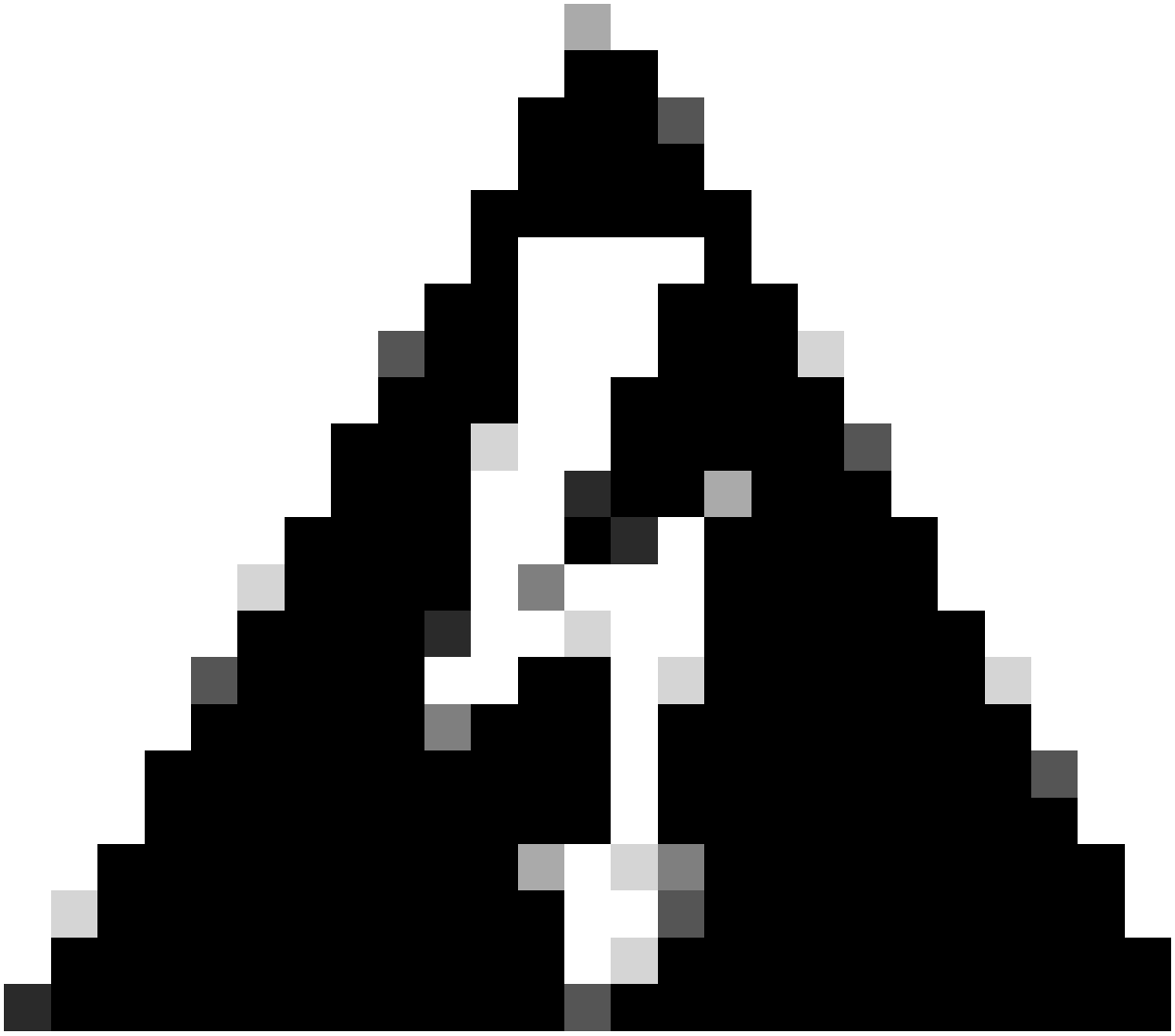
rate命令每10秒打印一次连接速率和每秒请求数。

<#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
```

收集高延迟日志

这取决于您在访问日志中看到的高响应时间或SHD日志中看到的高进程负载部分，对于进一步的故障排除，最好将相应的日志订阅更改为Debug。



警告：将日志级别设置为debug或trace会导致资源使用率增加，并导致日志文件快速旋转或覆盖。

访问日志字段	SHD日志字段	对应的日志订阅
身份验证响应，身份验证总计	—	authlogs
DNS响应，DNS总计	—	系统日志
WBRS响应，WBRS总计	Wbrs_WucLd	联系思科TAC
AVC响应，AVC总计	—	avc_logs

McAfee响应，McAfee总数	McafeeLd	mcafee_logs
Sophos响应，Sophos总计	SophosLd	sophos_logs
Webroot响应，Webroot总数	WebrootLd	webrootlogs
AMP响应，AMP总计	AMPLd	amp_logs

相关信息

使用SHD日志对安全Web设备性能进行故障排除

访问安全Web设备日志

在内容安全设备上配置数据包捕获

使用安全Web设备最佳实践

配置访问日志中的性能参数

排除SWA中的异常进程状态故障

确定SWA中的解密速率

安全网络设备DNS服务故障排除

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）。