Risoluzione dei problemi relativi alla latenza di Secure Web Appliance

Sommario

Introduzione

In questo documento viene descritto come risolvere i problemi relativi a latenza e disco elevati e CPU elevate in Cisco Secure Web Appliance (SWA).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Amministrazione Cisco SWA
- Metodi di distribuzione proxy (espliciti e trasparenti)
- Comandi CLI (Command Line Interface) SWA

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

Quando si contatta il supporto tecnico Cisco, viene chiesto di fornire dettagli sull'attività della rete SWA in entrata e in uscita, che possono essere monitorati eseguendo un'acquisizione di pacchetti per raccogliere il traffico a scopo di debug o verifica.

Cause frequenti dell'alta latenza in SWA

In generale, esistono tre categorie principali per l'alta latenza nell'SWA:

1. Dimensionamento SWA inadeguato o sovraccarico di risorse
2. Configurazioni complesse
3. Problemi di latenza correlati alla rete

Una delle cause più comuni dell'alta latenza in SWA è il dimensionamento inadeguato della soluzione. Un dimensionamento corretto è fondamentale per garantire che il sistema SWA disponga di risorse sufficienti per gestire i carichi di lavoro correnti e previsti. Se il sistema è di dimensioni ridotte, può avere difficoltà a elaborare le richieste in modo efficiente, causando ritardi nelle operazioni e una riduzione delle prestazioni. Fattori quali il numero di utenti, il volume di decrittografia e le specifiche richieste di analisi devono essere valutati attentamente durante la distribuzione per evitare vincoli di risorse. Il mancato allineamento della capacità SWA con le esigenze dell'organizzazione può causare una latenza persistente e un peggioramento dell'esperienza utente.

Configurazioni complesse possono ridurre le prestazioni e causare latenza sull'SWA, soprattutto in condizioni di carico elevato, in quanto ogni richiesta deve essere elaborata in numerose condizioni.

La latenza correlata alla rete può derivare dallo stesso SWA, da servizi di terze parti come Active Directory, DLP, DNS o da ritardi di rete tra il client, il SWA e i server upstream.

L'analisi delle richieste inviate all'SWA, inclusa l'identificazione degli utenti principali e degli URL a cui si accede di più, può aiutare a individuare potenziali comportamenti errati e a individuare le cause principali della latenza. Queste informazioni sono preziose per diagnosticare i problemi di prestazioni, gestire il consumo della larghezza di banda e garantire un utilizzo appropriato del sistema.

Strumenti di risoluzione dei problemi di latenza SWA

Stato del sistema

Per controllare il consumo corrente delle risorse in SWA, attenersi alla procedura descritta di seguito.

Passaggio 1. Accedere all'interfaccia grafica utente (GUI) SWA.

Passo 2: passare a Reporting > System Information > System Status (Informazioni di sistema).

Passaggio 3. Controllare le seguenti metriche critiche per valutare le prestazioni del sistema:

- Utilizzo CPU (%): Indica il carico della CPU corrente
- Utilizzo RAM (%): Riflette l'utilizzo della memoria
- Segnalazione/registrazione utilizzo (%): Mostra la percentuale di spazio su disco utilizzato per la creazione di report e la registrazione
- Tempo di attività del sistema: Visualizza il tempo totale di esecuzione del sistema senza un riavvio

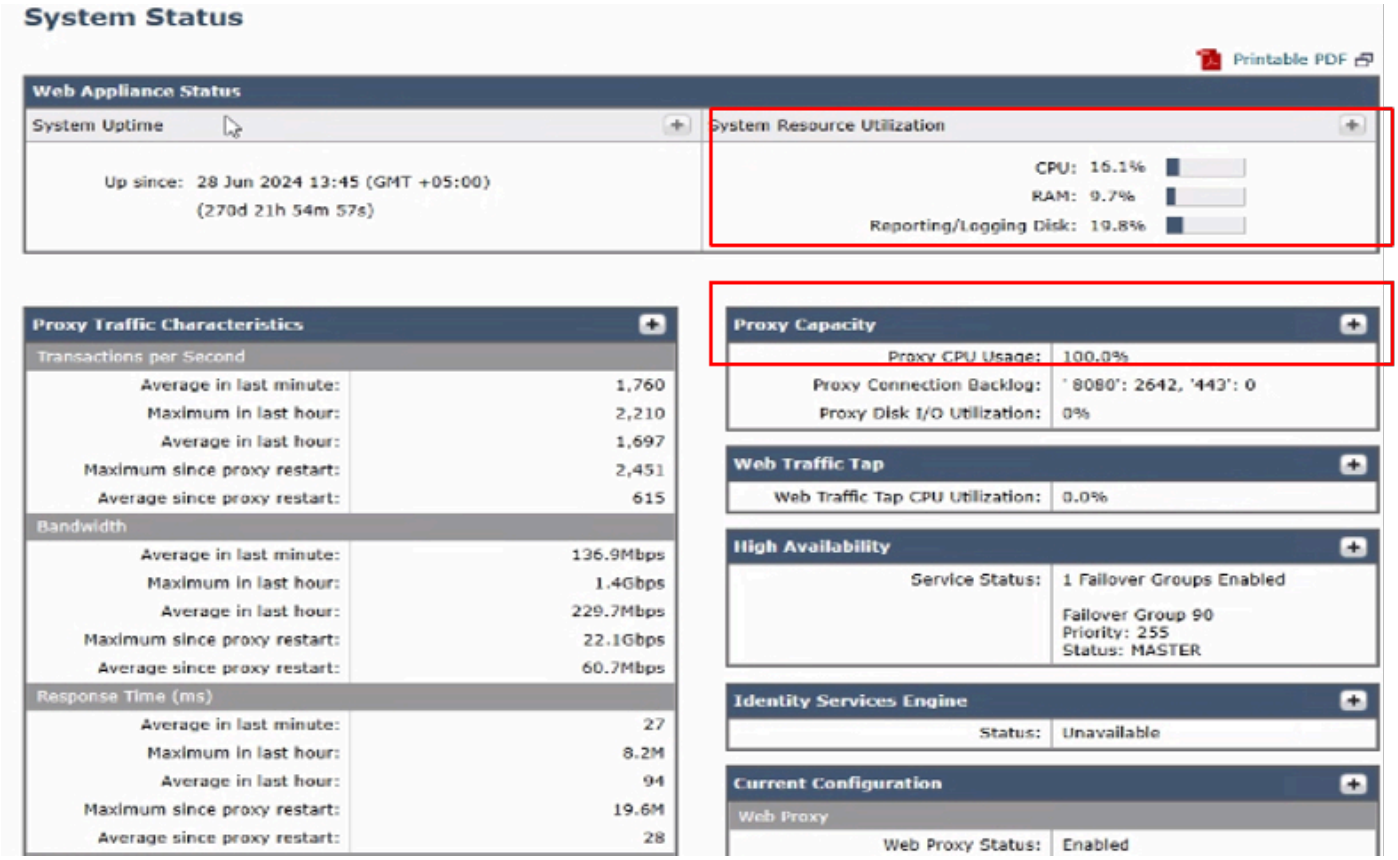


Immagine - Stato del sistema

Questa pagina fornisce una panoramica dello stato corrente della RAM, della CPU e dell'utilizzo del disco. Per visualizzare l'uso delle risorse nel tempo, dalla GUI SWA, passare a Reporting e scegliere Capacità sistema.

Capacità del sistema

La pagina Capacità del sistema nell'SWA fornisce una vista completa delle metriche relative all'utilizzo delle risorse e alle prestazioni in un intervallo di tempo specificato. Questa pagina contiene grafici dettagliati che aiutano a monitorare e analizzare il comportamento del sistema, garantendo prestazioni ottimali e identificando potenziali colli di bottiglia.

Di seguito sono riportati i grafici e le metriche disponibili nella pagina Capacità del sistema.

1. Utilizzo CPU complessivo: Visualizza l'utilizzo totale della CPU, fornendo una panoramica di alto livello delle prestazioni del sistema.
2. Utilizzo CPU per funzione: suddivide l'utilizzo della CPU in base a funzioni specifiche, tra cui:

- Proxy Web
- Registrazione
- Creazione di report
- McAfee
- Sophos
- Webroot
- Utilizzo accettabile e reputazione

3. Tempo di risposta/latenza (millisecondi): tiene traccia dei tempi di risposta per identificare eventuali ritardi nell'elaborazione delle richieste.

4. Transazioni al secondo: Mostra il numero di transazioni gestite dall'SWA al secondo.

5. Collegamenti in uscita: Controlla il numero di connessioni in uscita stabilite.

6. Larghezza di banda in uscita (byte): Misura la quantità di larghezza di banda in uscita utilizzata.

7. Memoria buffer proxy (%): Visualizza la percentuale di memoria utilizzata dal processo proxy.

Controllare le metriche per individuare eventuali segni di utilizzo elevato delle risorse in questo dashboard.

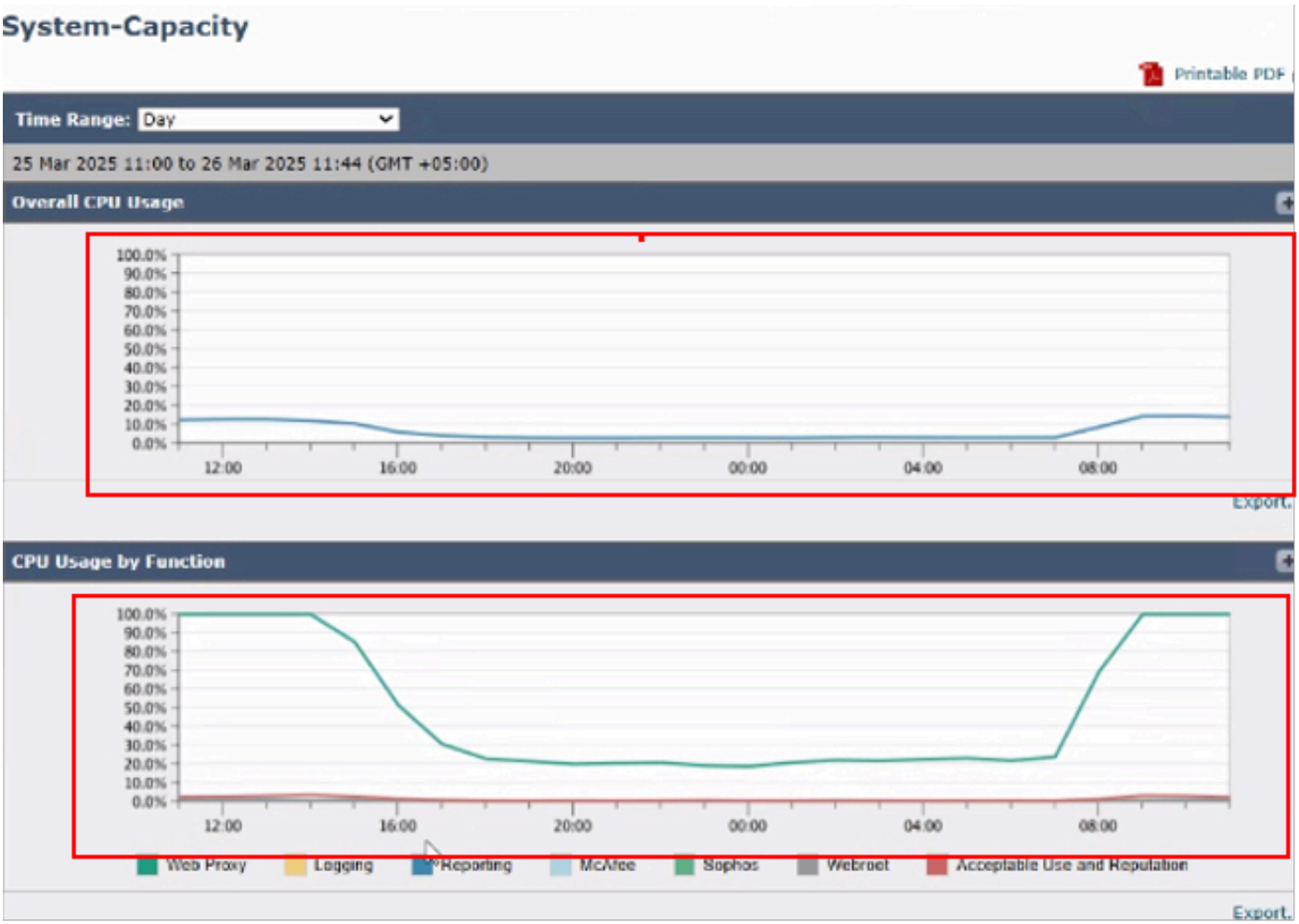


Immagine - Capacità del sistema

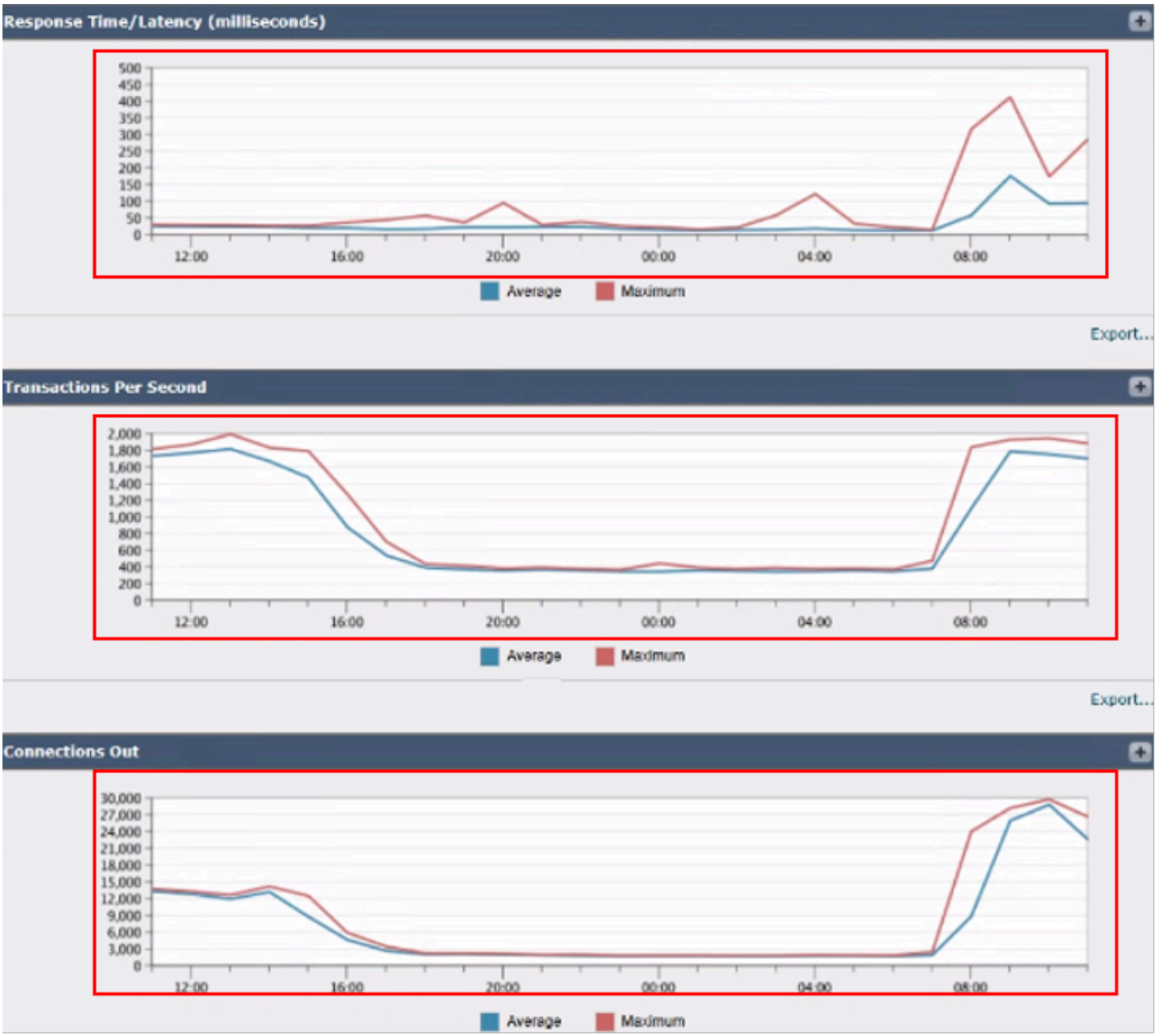


Immagine - Transazioni SWA al secondo e connessioni in uscita

Immagine - Utilizzo memoria SWA

Analizza prime destinazioni

Per analizzare le destinazioni principali, passare alla GUI SWA, passare a Reporting e selezionare Siti Web. Esaminare l'elenco dei principali siti Web HTTP/HTTPS e identificare i domini a traffico elevato o a cui si accede di frequente.

In base ai risultati ottenuti, è consigliabile ignorare o esentare gli URL generici, ad esempio Microsoft Update, Adobe, Office365 e le piattaforme per riunioni online. Questo approccio contribuisce a ridurre il traffico sull'SWA, riducendo la latenza e il carico di elaborazione dei proxy.

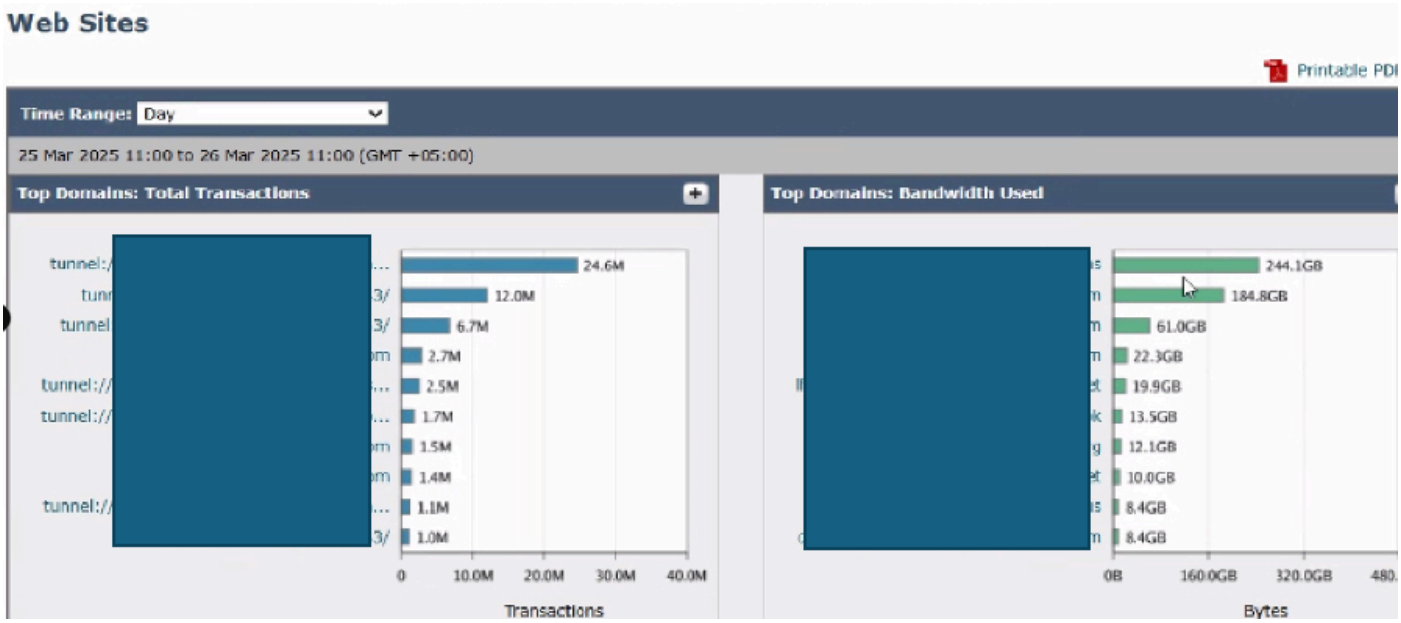


Immagine - Dashboard dei siti Web principali SWA

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

Immagine - Dashboard dei domini principali SWA

Analizza primi utenti

Per identificare le potenziali fonti di traffico eccessivo, passare alla GUI SWA da Reporting e scegliere Users.

Esaminare l'elenco per determinare quali utenti stanno generando il numero più alto di transazioni per l'SWA. Inoltre, verificare se sono presenti computer utente che generano il numero più elevato di transazioni per l'SWA e utilizzano la massima larghezza di banda.

Questa analisi consente di individuare gli utenti o i dispositivi responsabili di carichi di traffico significativi, consentendo azioni mirate per ridurre il carico complessivo del sistema.

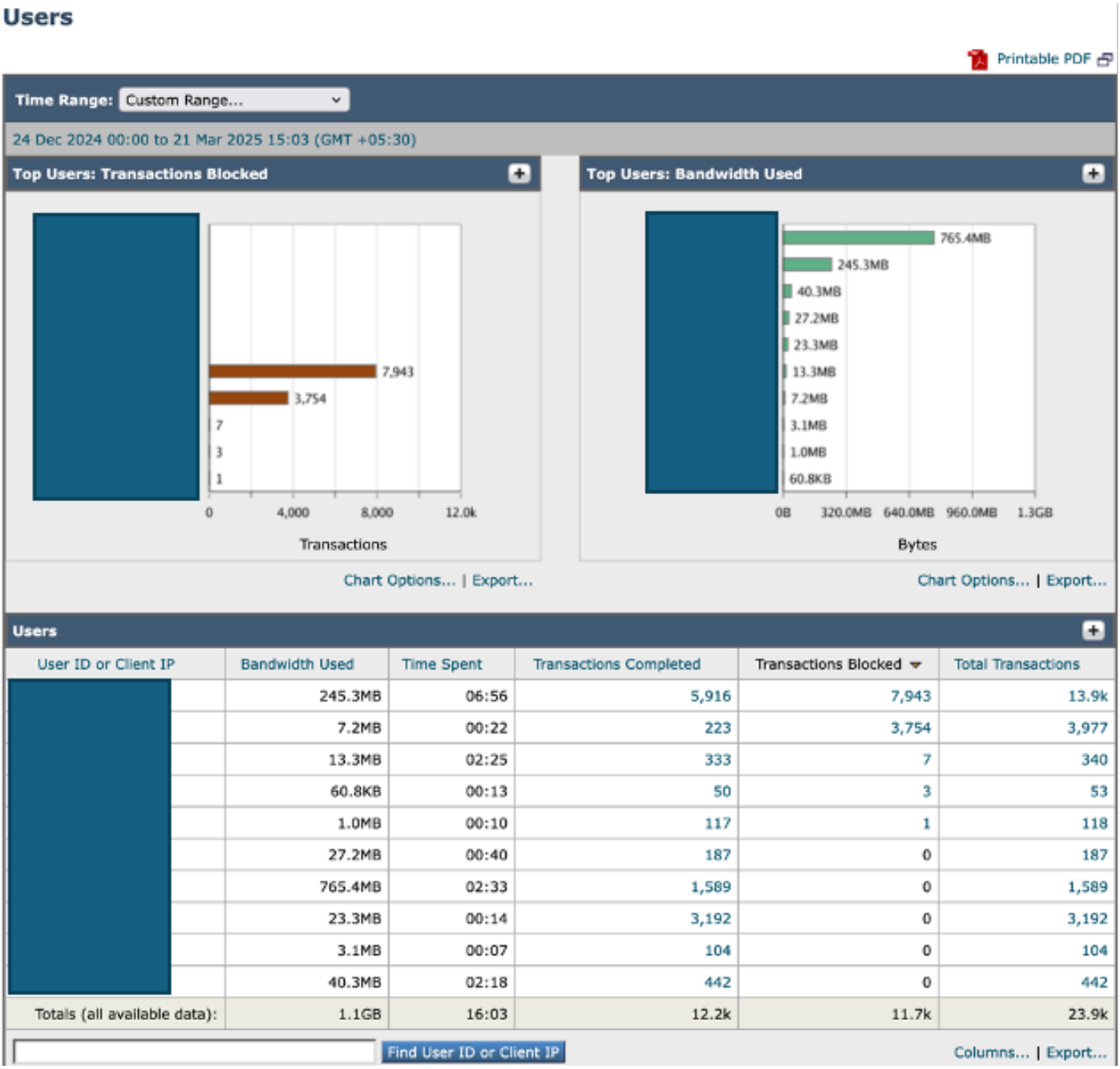


Image-SWA Top Users Dashboard

Registri SHD

Esaminando SHD_log, è possibile analizzare alcune metriche delle prestazioni, ad esempio il numero di sessioni da utenti a SWA (CliConn), il numero di sessioni da SWA a Internet (SrvConn), la media di richieste al secondo (Reqs) e così via.

Per ulteriori informazioni sul registro SHD, fare riferimento al collegamento Risoluzione dei problemi relativi alle prestazioni di Secure Web Appliance con i registri SHD,

Di seguito sono riportati alcuni parametri chiave da esaminare nei log di SHD:

- Connessioni client: Numero di connessioni client attive

- Conn. server: Numero di connessioni server attive
- LedProx: Carico medio processo proxy
- CPULD: Carico medio complessivo della CPU
- RAMUTIL: utilizzo RAM
- Latenza: tempo medio di servizio in un minuto
- DiskUtil: utilizzo del disco e prestazioni I/O

Come in questo esempio, la presenza di circa 1.600 richieste al secondo determina un carico elevato del processo proxy.

```
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
```

Utilizzo dei log degli accessi per la risoluzione dei problemi di latenza

Quando si verificano problemi di latenza durante l'inoltro del traffico tramite un'interfaccia SWA, i log degli accessi possono essere uno strumento utile per identificare la root cause probabile. Per ottimizzare le operazioni di risoluzione dei problemi, è possibile modificare le impostazioni del log degli accessi esistente o crearne uno nuovo. Includendo Parametri prestazioni nel campo personalizzato, è possibile ottenere informazioni più dettagliate sui fattori che contribuiscono alla latenza, consentendo un'analisi e una risoluzione più efficaci.

Per ulteriori informazioni sui parametri delle prestazioni e sui passaggi di configurazione, fare riferimento al collegamento Configura parametro delle prestazioni nei log degli accessi

Di seguito è riportata la guida dettagliata per la raccolta dei log nell'SWA: Accesso ai registri protetti di Web Appliance

Le fonti di latenza possono essere analizzate esaminando i parametri chiave che aiutano a determinare se si verificano ritardi tra il client e l'SWA, all'interno dei processi interni dell'SWA o tra l'SWA e il server Web. Tra gli indicatori importanti da prendere in considerazione sono inclusi i servizi basati sulla rete, quali la risoluzione DNS, il tempo di autenticazione e i tempi di risposta del server o del client. Inoltre, i ritardi causati da motori di scansione come AMP, Sophos e AVC devono essere valutati per identificarne l'impatto sulla latenza complessiva.

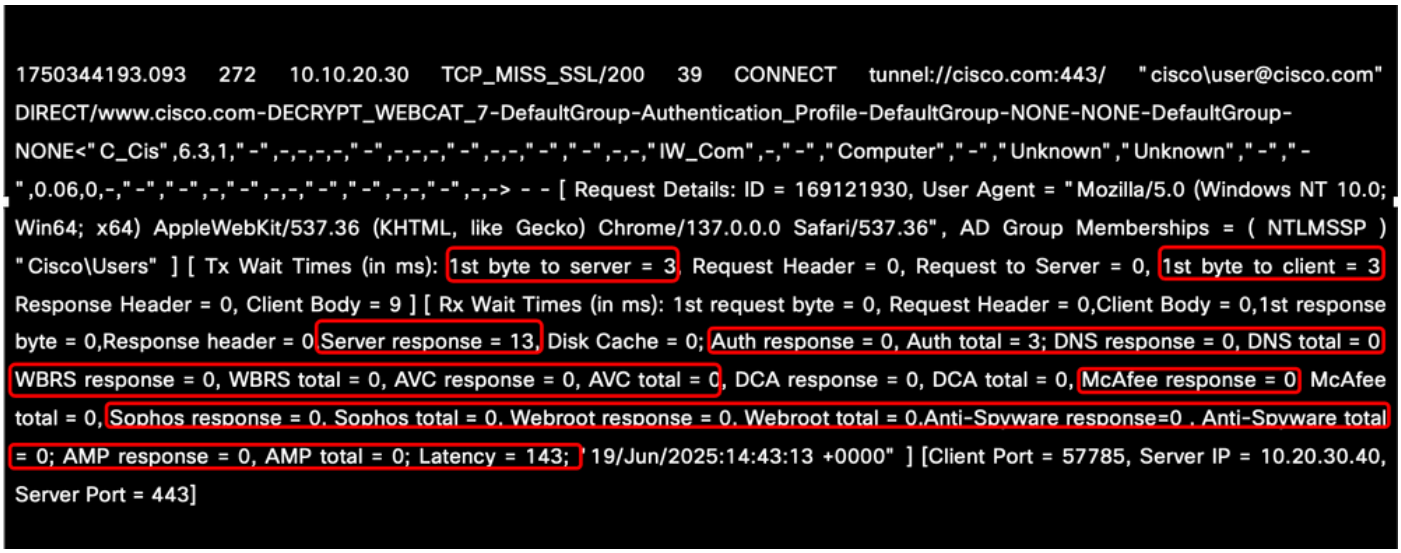


Immagine - Parametri delle prestazioni nel log degli accessi

Tempo di autenticazione elevato

Se il tempo di risposta dell'autenticazione è elevato, queste informazioni sono necessarie per consentire a TAC di risolvere meglio e più rapidamente la latenza di autenticazione:

- Configurazione SWA corrente
- Log di autenticazione in modalità debug o traccia
- Acquisizioni di pacchetti da
    - Computer client.
    - SWA (con filtro per acquisire il traffico del client e il traffico SWA verso tutte le directory attive configurate nelle impostazioni del realm).
- Verificare che il campo personalizzato %m e %g sia presente in Accesslogs per identificare il meccanismo di autenticazione e i gruppi
- File HAR dal client durante la riproduzione del problema
- L'output del comando testauthconfig dalla CLI

Nell'esempio viene mostrato il tempo di latenza elevata relativo all'autenticazione:

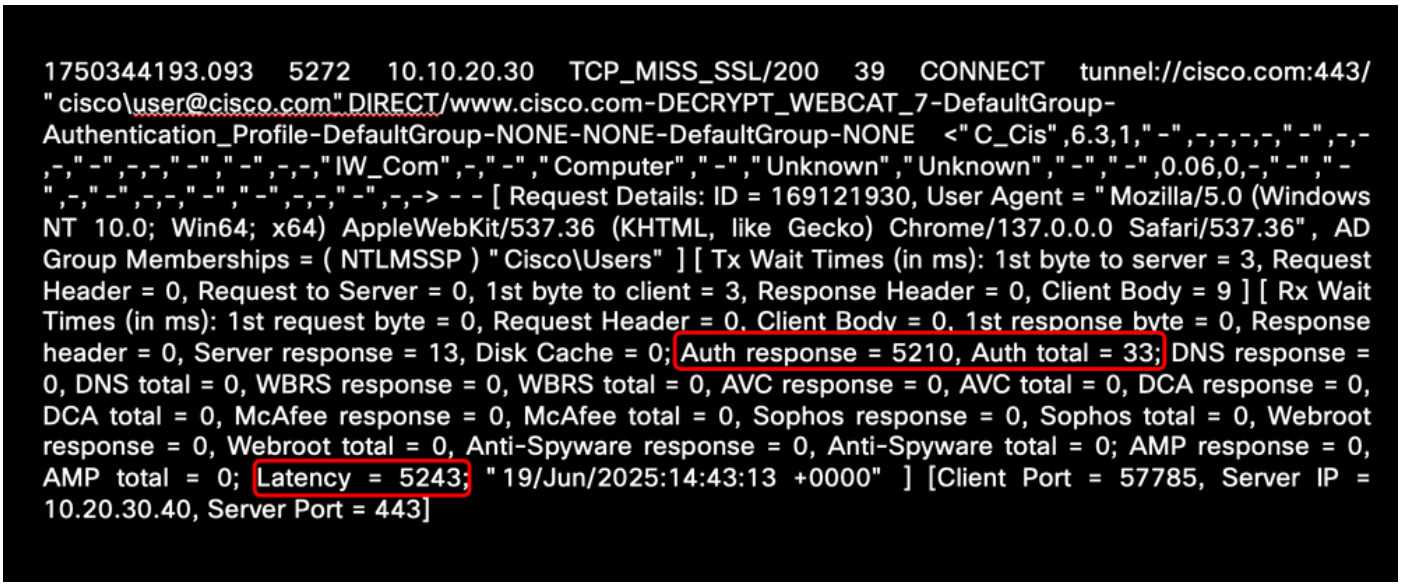


Immagine - Esempio di latenza di autenticazione elevata

Tempo DNS elevato

Se il tempo di risposta DNS è elevato, queste informazioni sono necessarie per consentire a TAC di risolvere i problemi di latenza DNS:

- Configurazione SWA corrente
- Registri di sistema in modalità traccia
- Indirizzo IP server DNS
- Acquisizioni di pacchetti da
  - Computer client
  - SWA (filtraggio con indirizzo IP dei server DNS).
- Verificare che nel campo personalizzato dei log degli accessi sia presente %:<d e %:>d
- File HAR dal client durante la riproduzione del problema

Per ulteriori informazioni sulla configurazione DNS e la risoluzione dei problemi, fare riferimento al collegamento Risoluzione dei problemi relativi al servizio DNS Secure Web Appliance

In questo esempio viene illustrato il tempo di latenza elevata correlato alla risoluzione dei nomi DNS:

```
1750344193.093   4472   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 = 4320,
DNS total = 65, 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 = 4353; " 19/Jun/2025:14:43:13 +0000" ] [Client Port = 57785, Server IP =
10.20.30.40, Server Port = 443]
```

Immagine - Esempio di latenza con alta risoluzione DNS

Tempo elevato del motore di scansione

Se il tempo di risposta per Web Reputation Score (WBRS), Application and Visibility Control (AVC) e Malware Scanning Engine è elevato, queste informazioni sono necessarie per consentire a TAC di risolvere i problemi relativi all'elevato tempo di risposta del motore di scansione:

- Configurazione SWA corrente.
- A seconda del motore con tempi di risposta elevati, modificare il livello di registrazione in debug.

Nell'esempio viene mostrato il tempo di latenza elevata relativo a Sophos Engine:

```
1750344193.093   4500   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 = 0; 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 = 4376, Sophos total = 145, Webroot response = 0, Webroot total = 0,
Anti-Spyware response = 0, Anti-Spyware total = 0; AMP response = 0, AMP total = 0; Latency = 4409;
" 19/Jun/2025:14:43:13 +0000" ] [Client Port = 57785, Server IP = 10.20.30.40, Server Port = 443]
```

Immagine - Motore di scansione malware ad alta latenza

Se i motori di scansione mostrano una risposta elevata, per il ripristino immediato è possibile riavviare il servizio di scansione dalla CLI eseguendo la procedura seguente:

Passaggio 1. Digitare diagnostic e premere Invio (si tratta di un comando nascosto ed è necessario digitare il comando esatto).

Passaggio 2. Scegliere SERVICES.

Passaggio 3. Per riavviare il servizio WBRS, scegliere WBRS, altrimenti andare al passaggio 6.

Passaggio 4. Scegliere RIAVVIA.

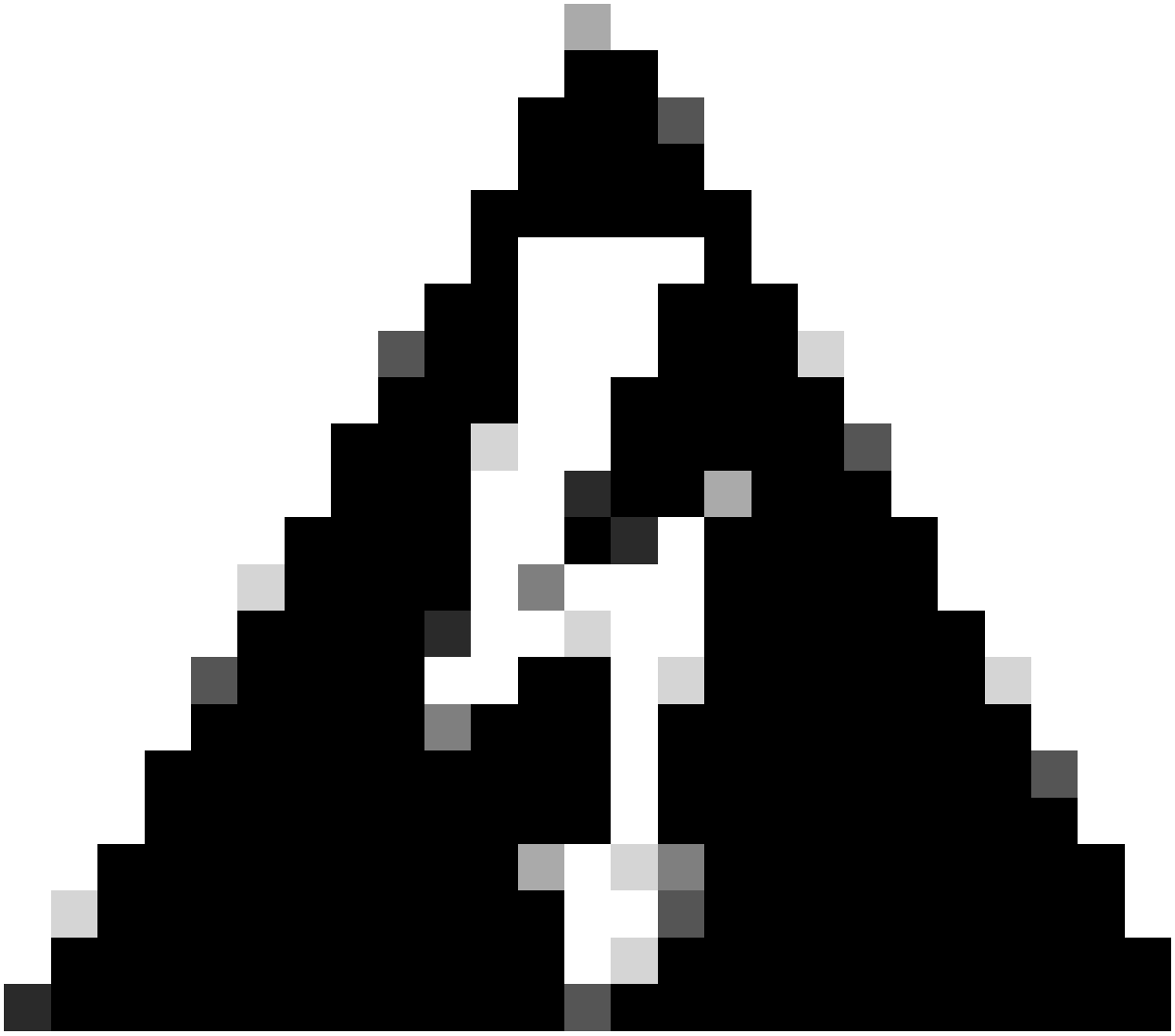
Passaggio 5. Continuare a premere Invio per uscire dalla procedura guidata.

Passaggio 6. Se si intende riavviare un modulo di ricerca malware, scegliere ANTIVIRUS.

Passaggio 7. Selezionare gli scanner.

Passaggio 8. Scegliere RIAVVIA.

Passaggio 9. Continuare a premere Invio per uscire dalla procedura guidata.



Avviso: Il riavvio dei servizi interni provoca l'interruzione del servizio. Si consiglia di eseguire questa operazione nelle ore di produzione o con cautela.

Best Practice Durante La Connessione All'Acquisizione Dei Pacchetti

Durante l'acquisizione di qualsiasi pacchetto, raccogli e condividi queste informazioni con Cisco TAC.

- Indirizzo IP del client.
- L'URL a cui si stava tentando di accedere.
- L'indirizzo IP risolto per l'URL dal PC client e dall'SWA.
- Esperienza dell'utente (ad esempio, la pagina non è stata caricata o è stata caricata parzialmente e, in caso di messaggi di errore, scattare una schermata).
- Timestamp del test.
- Chiudere tutti gli altri browser e le altre app nel computer client. Accedere al sito Web,

acquisire i log nel Blocco note per un tentativo di operazione riuscita/non riuscita e condividerli con il supporto Cisco.

Per informazioni dettagliate su come eseguire l'acquisizione dei pacchetti in SWA, fare riferimento al collegamento Configure Packet Capture on Content Security Appliance

Complessità della configurazione

Un'altra causa comune di latenza elevata e prestazioni ridotte è la complessità della configurazione. Questo si verifica quando l'SWA è configurato con un numero eccessivo di condizioni, profili e criteri. Questa complessità può aumentare notevolmente i tempi di risposta e sovraccaricare notevolmente il processo proxy. Questo problema tende ad accentuarsi durante le ore di punta, quando il traffico raggiunge i massimi livelli.

Di seguito sono riportati alcuni suggerimenti per ottimizzare la configurazione:

1. Limita decrittografia HTTPS: Decrittografare solo il traffico essenziale per i criteri di sicurezza. Ove possibile, ridurre il sovraccarico di elaborazione mantenendo la sicurezza.
2. Assegnazione di priorità ai criteri per l'efficienza: Disporre i criteri utilizzati più di frequente in cima all'elenco dei criteri. Ciò assicura un'elaborazione più rapida, in quanto affronta prima il traffico più impegnativo.
3. Semplificazione della progettazione delle policy: Semplificare le politiche riducendo il più possibile il loro numero. Ciò riduce l'elaborazione non necessaria e migliora le prestazioni complessive del sistema.
4. Ottimizzazione della scansione di antimalware e antivirus: rivedere le configurazioni di scansione per i processi antimalware e antivirus. Questi possono richiedere un utilizzo intensivo della CPU, pertanto l'ottimizzazione può ridurre in modo significativo il consumo di risorse senza compromettere la sicurezza.
5. Usa espressioni regolari leggere: Evitare espressioni regolari complesse o che richiedono molte risorse. Assicuratevi che caratteri quali punti (.) e stelle (*) siano correttamente escape per ridurre il carico di elaborazione e prevenire inefficienze.

Per informazioni dettagliate sulle procedure ottimali SWA, visitare il sito Web Use Secure Web Appliance Best Practices

Comandi CLI

Version

Utilizzare il comando version per verificare l'allocazione dell'hardware (per SWA virtuale) e lo stato RAID (per SWA fisico). Controllare la configurazione dell'hardware: Verificare che il numero di core CPU, la memoria e i dischi rigidi siano allocati come previsto. Nei modelli virtuali lo stato RAID è Sconosciuto. Se lo stato RAID è Danneggiato o In errore nell'accessorio fisico, contattare Cisco TAC per rivedere lo stato del disco dal back-end.

Di seguito è riportato un esempio di allocazione di più CPU al file SWA che può causare un

comportamento errato:

```
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
```

visualizzarerevisioni

Usare il comando displayalert per controllare i messaggi di allarme relativi alla rete SWA che possono indicare la causa principale.

Nell'esempio il server DNS con indirizzo IP 10.10.10.10 non risponde e il messaggio "The File Reputation service is not reachable" (Reputazione file non raggiungibile) può indicare un problema di connettività di rete.

```
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
```

stato_processo

Usare il comando process_status per visualizzare l'uso dei processi e della memoria dei servizi interni SWA.

Se il processo Prox, che è il processo principale per la gestione del traffico di inoltro, supera costantemente l'utilizzo del 100% per diversi minuti, indica un carico elevato sostenuto sul processo. Tuttavia, picchi occasionali di utilizzo della CPU sul proxy o su altri processi sono normali e previsti.

<#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

dettagli stato

Il comando status detail fornisce un riepilogo in tempo reale dell'utilizzo delle risorse di sistema, delle metriche del traffico di rete e delle statistiche delle connessioni, che riflette lo stato e le prestazioni generali dell'interfaccia SWA. Riflette la visualizzazione dello stato del sistema nella GUI per un monitoraggio e una risoluzione dei problemi rapidi.

<#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

Il comando ipcheck consente di visualizzare informazioni di sistema dettagliate per l'appliance Web sicura, tra cui le specifiche hardware, l'utilizzo del disco, le interfacce di rete, le chiavi software installate e i dettagli sulla versione, fornendo un'istantanea completa dello stato corrente dell'appliance.

<#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
```

velocità

Il comando rate stampa le velocità di connessione e il numero di richieste al secondo ogni 10 secondi.

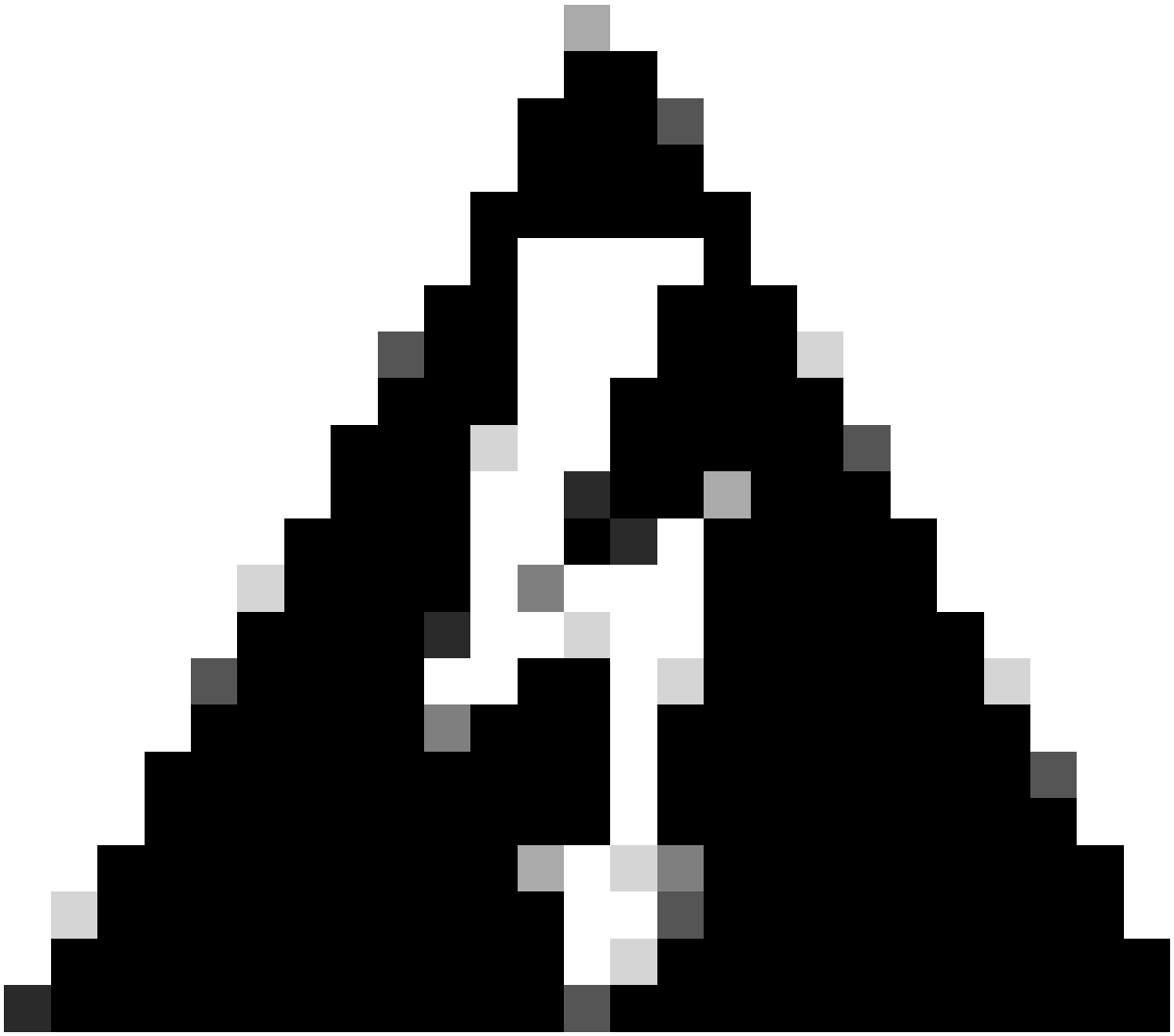
<#root>

```
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
```

Raccolta dei log per l'alta latenza

Dipende dalla sezione in cui si riscontra un tempo di risposta elevato dai log degli accessi o un carico di elaborazione elevato dai log SHD. Per ulteriori informazioni sulla risoluzione dei problemi, è consigliabile modificare la sottoscrizione del log corrispondente in Debug.



Avviso: L'impostazione del livello di registro su debug o traccia può aumentare l'utilizzo delle risorse e causare una rapida rotazione o sovrascrittura dei file di registro.

Campo log degli accessi	Campo registro SHD	Sottoscrizione log corrispondente

Risposta Auth, totale Auth	—	authlogs
Risposta DNS, totale DNS	—	registri_sistema
Risposta WBRS, totale WBRS	Wbrs_WucLd	Contatta Cisco TAC
Risposta AVC, totale AVC	—	avc_log
Risposta di McAfee, McAfee totale	McafeeLd	log_mcafee
Risposta Sophos, Sophos totale	SophosLd	registri_sophos
Risposta Webroot, totale Webroot	WebrootLd	webrootlog
risposta AMP, totale AMP	AMP	log_amp

Informazioni correlate

Risoluzione dei problemi relativi alle prestazioni di Secure Web Appliance con i registri SHD

Accesso ai registri protetti di Web Appliance

Configurazione dell'acquisizione pacchetti su Content Security Appliance

Utilizzare le procedure ottimali per Secure Web Appliance

Configura parametro prestazioni nei log degli accessi

Risoluzione dei problemi relativi agli stati di processo insoliti in SWA

Determinazione della velocità di decrittografia in SWA

Risoluzione dei problemi relativi al servizio DNS Secure Web Appliance

Accesso ai registri protetti di Web Appliance

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).