Solucionar problemas de latência do Secure Web Appliance

Contents

Introdução

Este documento descreve as etapas de solução de problemas para lidar com alta latência, alto disco e alta CPU no Cisco Secure Web Appliance (SWA).

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Administração do Cisco SWA
- Métodos de implantação de proxy (Explícito e Transparente)
- Comandos da interface de linha de comando (CLI) do SWA

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Informações de Apoio

Ao entrar em contato com o Suporte Técnico da Cisco, você será solicitado a fornecer detalhes sobre a atividade de rede de entrada e saída do SWA, que pode ser monitorada executando uma captura de pacote para coletar tráfego para fins de depuração ou verificação.

Causas frequentes de alta latência em SWA

Em geral, há três categorias principais para a alta latência em SWA:

1. Dimensionamento de SWA inadequado ou recursos sobrecarregados
2. Configurações complexas
3. Problemas de latência relacionados à rede

Uma das causas mais comuns de alta latência em SWA é o dimensionamento inadequado da solução. O dimensionamento apropriado é essencial para garantir que o sistema SWA tenha recursos suficientes para lidar com as cargas de trabalho atuais e esperadas. Se o sistema não tiver o tamanho necessário, ele pode se esforçar para processar as solicitações com eficiência, o que resulta em atrasos nas operações e redução do desempenho. Fatores como número de usuários, volume de descriptografia e demandas específicas de varredura devem ser cuidadosamente avaliados durante a implantação para evitar restrições de recursos. A falha em alinhar a capacidade SWA com as necessidades organizacionais pode resultar em latência persistente e experiência de usuário degradada.

Configurações complexas podem degradar o desempenho e causar latência no SWA, especialmente sob carga alta, já que cada solicitação deve ser processada através de várias condições.

A latência relacionada à rede pode ser originada do próprio SWA, de serviços de terceiros como Ative Diretory, DLP, DNS ou de atrasos na rede entre o cliente, SWA e servidores upstream.

A análise das solicitações enviadas ao SWA, incluindo a identificação dos principais usuários e dos URLs mais acessados, pode ajudar a descobrir possíveis comportamentos incorretos e identificar as causas raiz da latência. Essas informações são inestimáveis para diagnosticar problemas de desempenho, gerenciar o consumo de largura de banda e garantir o uso apropriado do sistema.

Ferramentas de Troubleshooting de Latência de SWA

Status do sistema

Siga estas etapas para verificar o consumo atual de recursos no SWA:

Etapa 1. Acessar a GUI (Graphical User Interface, interface gráfica do usuário) do SWA.

Etapa 2. Navegue até Emissão de Relatórios > Informações do Sistema > Status do Sistema.

Etapa 3. Verifique estas métricas críticas para avaliar o desempenho do sistema:

- Uso da CPU (%): Indica a carga de CPU atual
- Uso de RAM (%): Reflete a utilização da memória
- Uso de Relatórios/Logs (%): Mostra o percentual de espaço em disco que está sendo usado para relatórios e logs
- Tempo de atividade do sistema: Exibe o tempo total que o sistema esteve em execução sem uma reinicialização

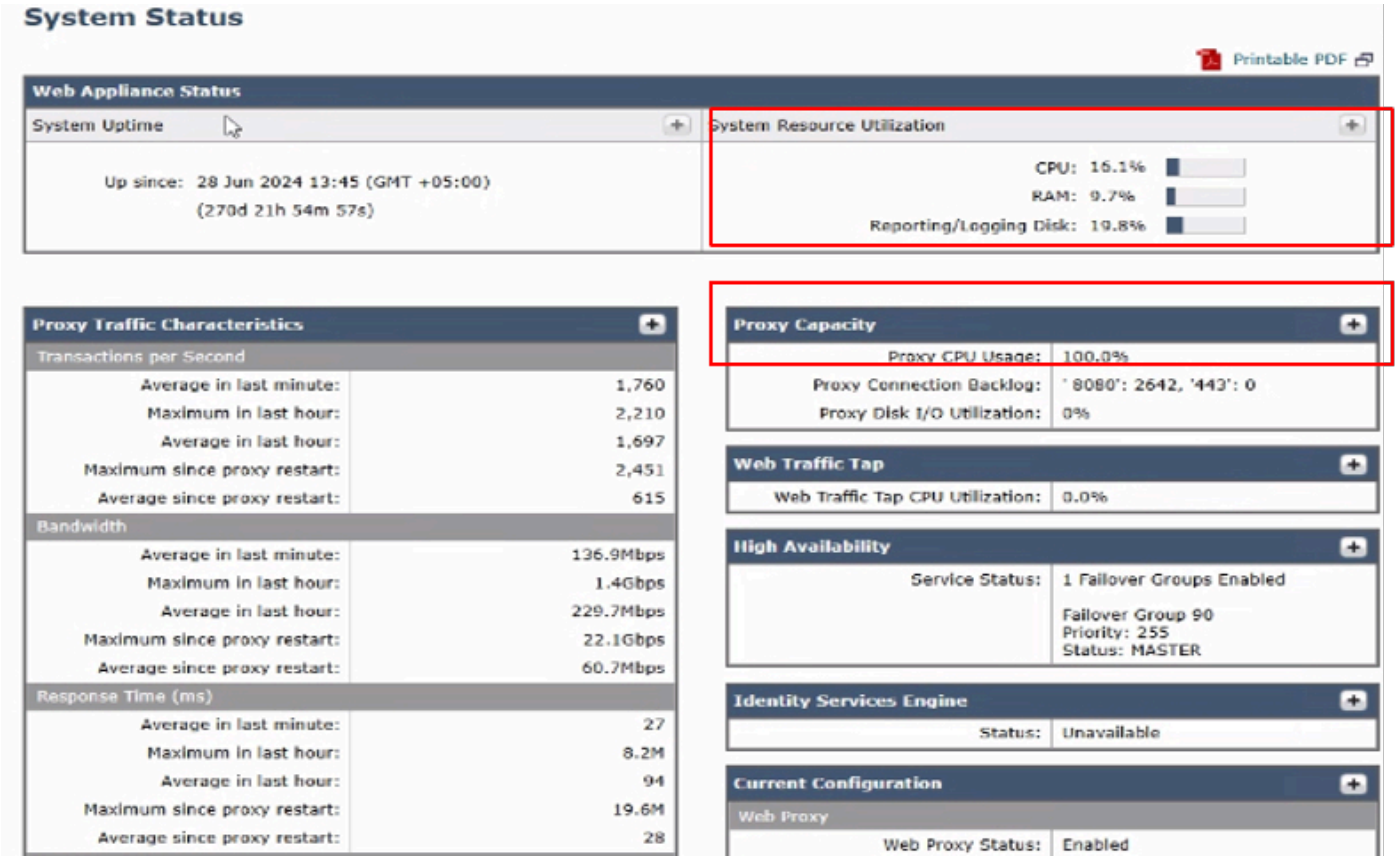


Imagem - Status do sistema

Esta página fornece uma visão geral do status atual da RAM, CPU e uso do disco. Para visualizar o uso de recursos ao longo do tempo, na GUI do SWA, navegue para Relatórios e escolha Capacidade do sistema.

Capacidade do sistema

A página Capacidade do sistema no SWA fornece uma visão abrangente da utilização de recursos e das métricas de desempenho em um intervalo de tempo especificado. Esta página oferece gráficos detalhados para ajudar a monitorar e analisar o comportamento do sistema, garantindo o desempenho ideal e identificando gargalos em potencial.

Os Gráficos e Métricas Disponíveis na página Capacidade do Sistema são:

1. Uso Geral da CPU: Exibe o uso total da CPU, fornecendo uma visão geral de alto nível do desempenho do sistema.
2. Uso da CPU por Função: divide o uso da CPU com base em funções específicas, incluindo:

- Proxy da Web
- Registro
- Relatórios
- McAfee
- Sophos
- Webroot
- Uso e reputação aceitáveis

3. Tempo de Resposta/Latência (milissegundos): Rastreia os tempos de resposta para identificar atrasos no processamento de solicitações.

4. Transações por Segundo: Mostra o número de transações que estão sendo tratadas pelo SWA por segundo.

5. Conexões de Saída: Monitora o número de conexões de saída estabelecidas.

6. Largura de Banda de Saída (Bytes): Mede a quantidade de largura de banda de saída que está sendo utilizada.

7. Memória de Buffer de Proxy (%): Exibe a porcentagem de memória usada pelo processo proxy.

Verifique as métricas para quaisquer sinais de alto uso de recursos neste painel.

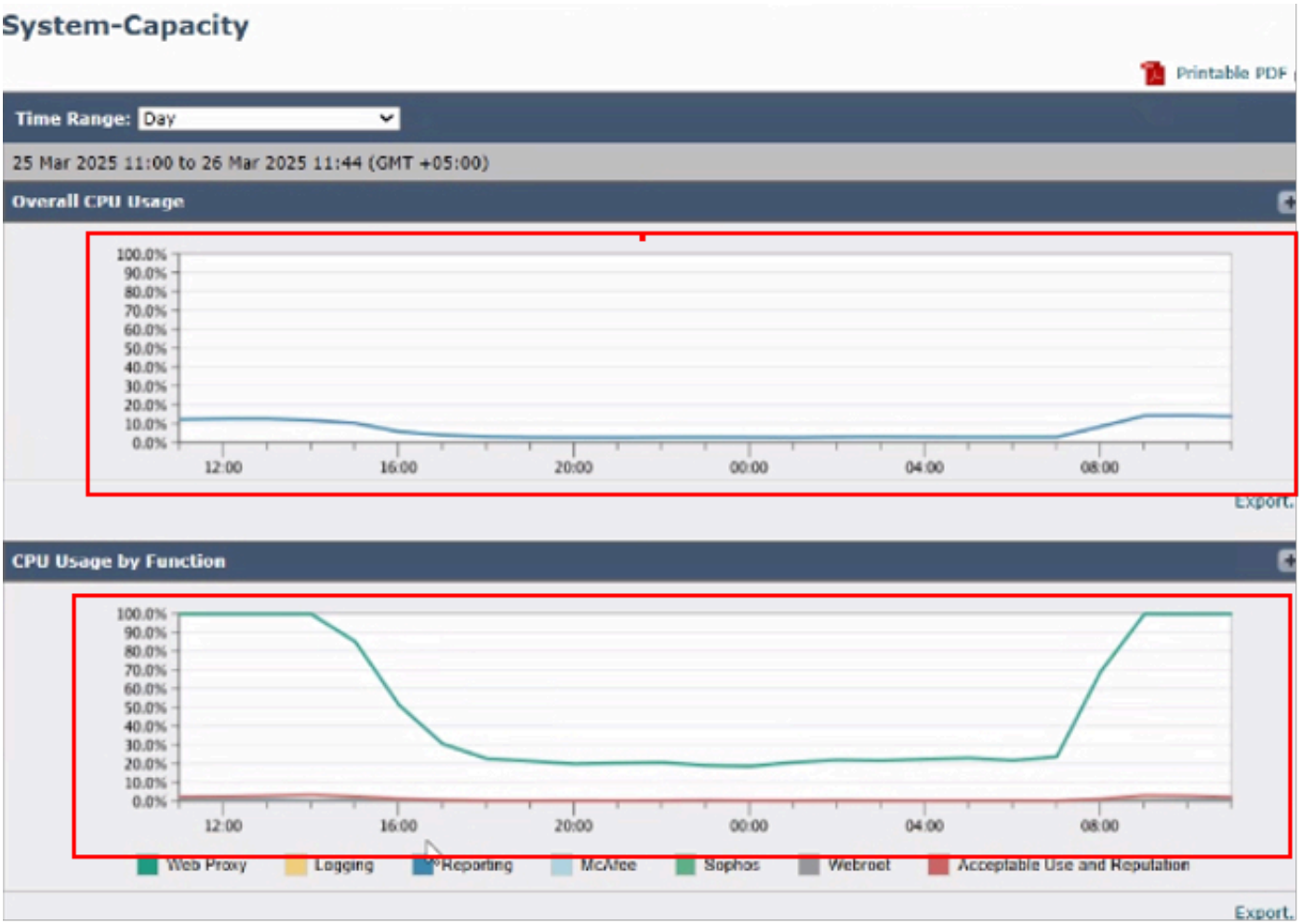


Imagem - Capacidade do sistema

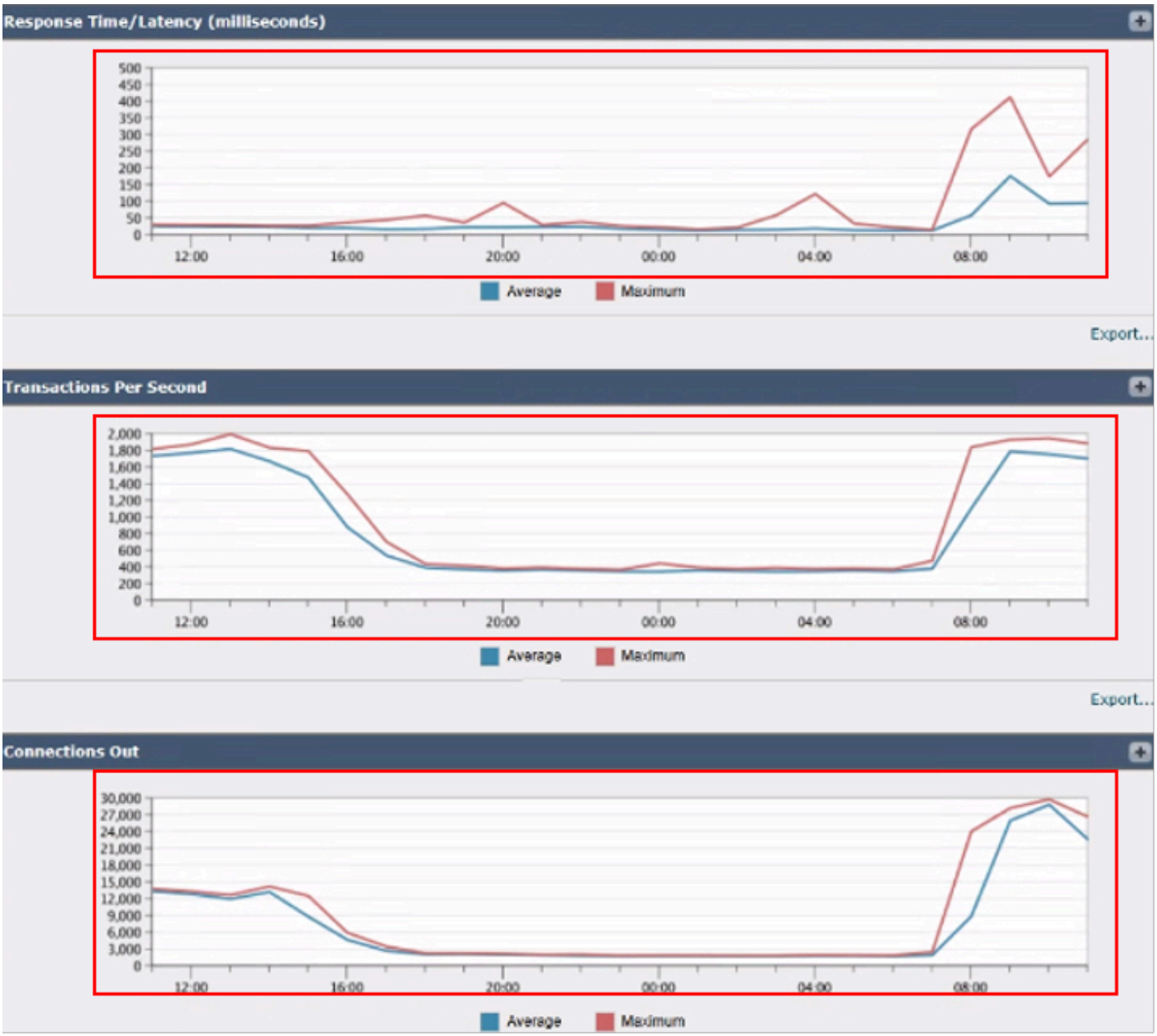


Imagem - Transações SWA por segundo e conexões de saída

Imagem - Uso de memória SWA

Analisar os principais destinos

Para analisar os principais destinos, navegue até a GUI do SWA, navegue até Reporting e selecione Websites. Revise a lista dos principais sites HTTP/HTTPS e identifique domínios de alto tráfego ou acessados com frequência.

Com base em suas descobertas, considere ignorar ou isentar URLs genéricas, como Microsoft Updates, Adobe, Office365 e plataformas de reunião online. Essa abordagem ajuda a reduzir o tráfego no SWA, levando à menor latência e a uma carga de processamento de proxy reduzida.

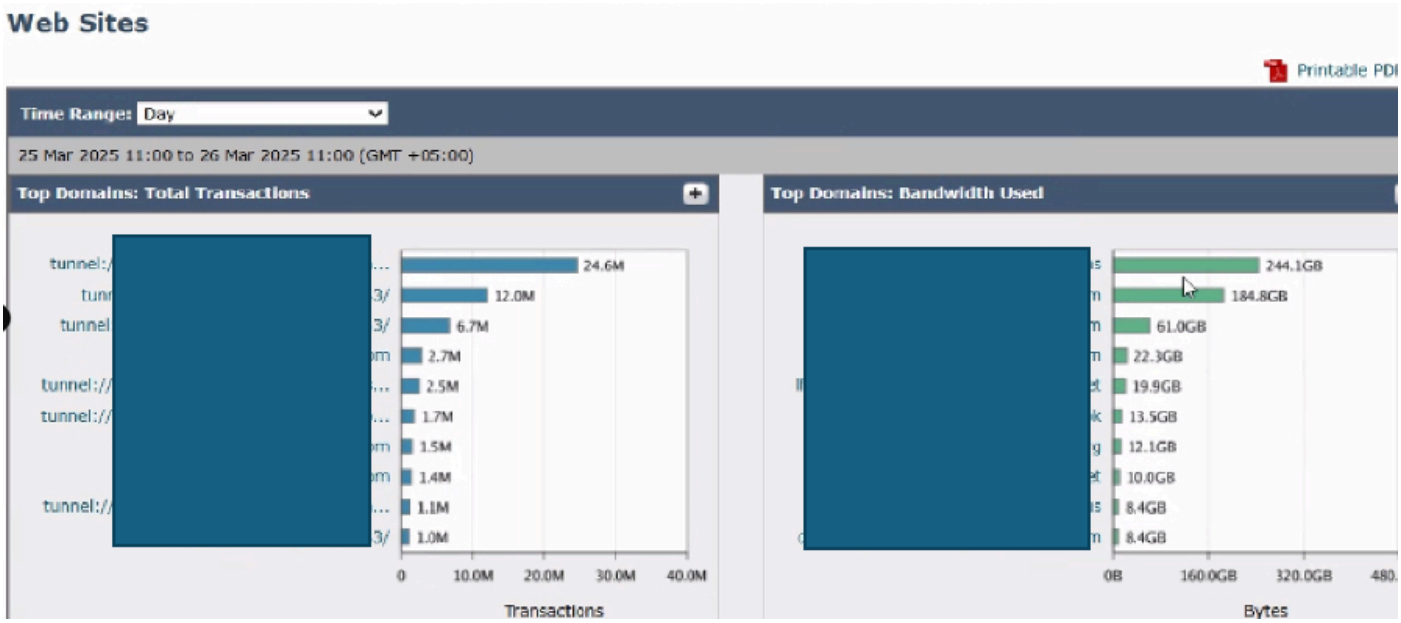


Imagem - Painel de Sites Principais do SWA

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

Imagem - Painel de domínios principais do SWA

Analisar usuários principais

Para identificar fontes potenciais de tráfego excessivo, navegue até a GUI do SWA em Relatórios e escolha Usuários.

Revise a lista para determinar quais usuários estão gerando o maior número de transações para o SWA. Além disso, verifique se há máquinas de usuário que estejam gerando o maior número de transações para o SWA e consumindo a largura de banda máxima.

Essa análise pode ajudar a identificar usuários ou dispositivos responsáveis por cargas de tráfego significativas, permitindo ações direcionadas para reduzir a sobrecarga geral do sistema.

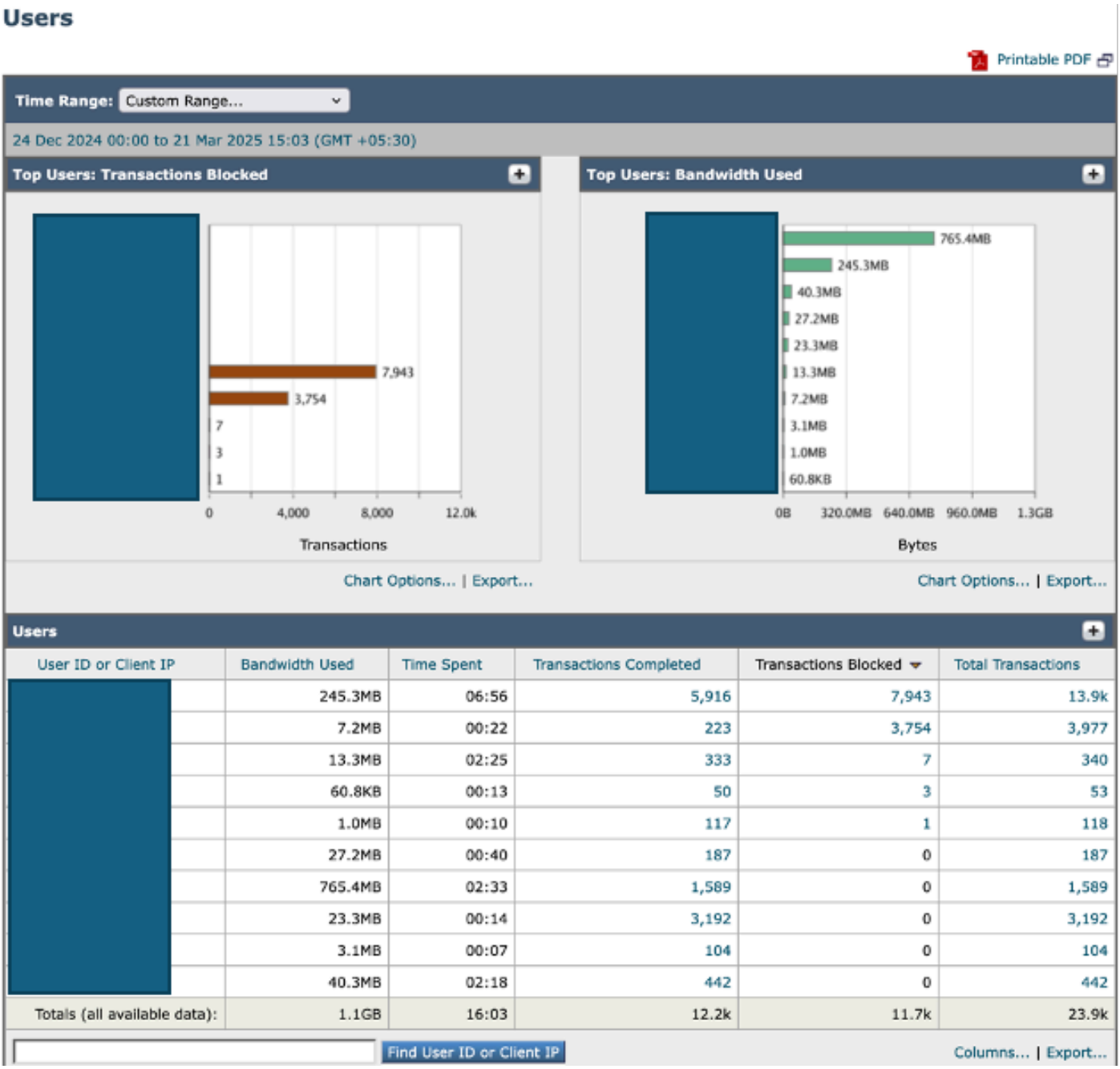


Imagem-Painel de usuários principais do SWA

Logs SHD

Ao revisar o SHD_log, você pode analisar algumas das métricas de desempenho, como o número de sessões de usuários para SWA (CliConn), o número de sessões de SWA para a Internet (SrvConn), a média de solicitações por segundos (Reqs) e assim por diante.

Para obter mais informações sobre o Log do SHD, consulte o link Solução de problemas de desempenho do dispositivo da Web seguro com logs do SHD,

Alguns parâmetros-chave a serem revisados nos logs SHD são:

- ConnsCliente: Número de conexões de cliente ativas

- ConnsServidor: Número de conexões ativas do servidor
- ProxLd: Carga média do processo de Proxy
- CPULD: Carga geral média da CPU
- RAMUTIL: utilização da RAM
- Latência: Tempo médio de serviço em um minuto
- DiskUtil: uso do disco e desempenho de I/O

Como neste exemplo, ter cerca de 1.600 solicitações por segundo, leva a uma carga elevada do 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
```

Uso de logs de acesso para solucionar problemas de latência

Quando ocorrem problemas de latência com o tráfego sendo encaminhado por proxy através de um SWA, os logs de acesso podem servir como uma ferramenta valiosa para identificar a causa raiz provável. Para aprimorar os esforços de solução de problemas, você pode modificar as configurações existentes do Log de Acesso ou criar um novo Log de Acesso. Incluindo os parâmetros de desempenho no campo personalizado, você pode obter insights mais profundos sobre os fatores que contribuem para a latência, permitindo uma análise e resolução mais eficazes.

Para obter mais informações sobre os Parâmetros de Desempenho e as etapas de configuração, consulte o link: Configurar Parâmetro de Desempenho em Logs de Acesso

Aqui está o guia detalhado para coletar logs no SWA: Acessar logs do dispositivo da Web seguro

As fontes de latência podem ser analisadas examinando os principais parâmetros que ajudam a determinar se ocorrem atrasos entre o cliente e o SWA, dentro dos processos internos do SWA ou entre o SWA e o servidor Web. Indicadores importantes a serem considerados incluem serviços baseados em rede, como resolução DNS, tempo de autenticação e tempos de resposta de servidor ou cliente. Além disso, os atrasos causados por mecanismos de verificação como AMP, Sophos e AVC devem ser avaliados para identificar seu impacto na latência geral.

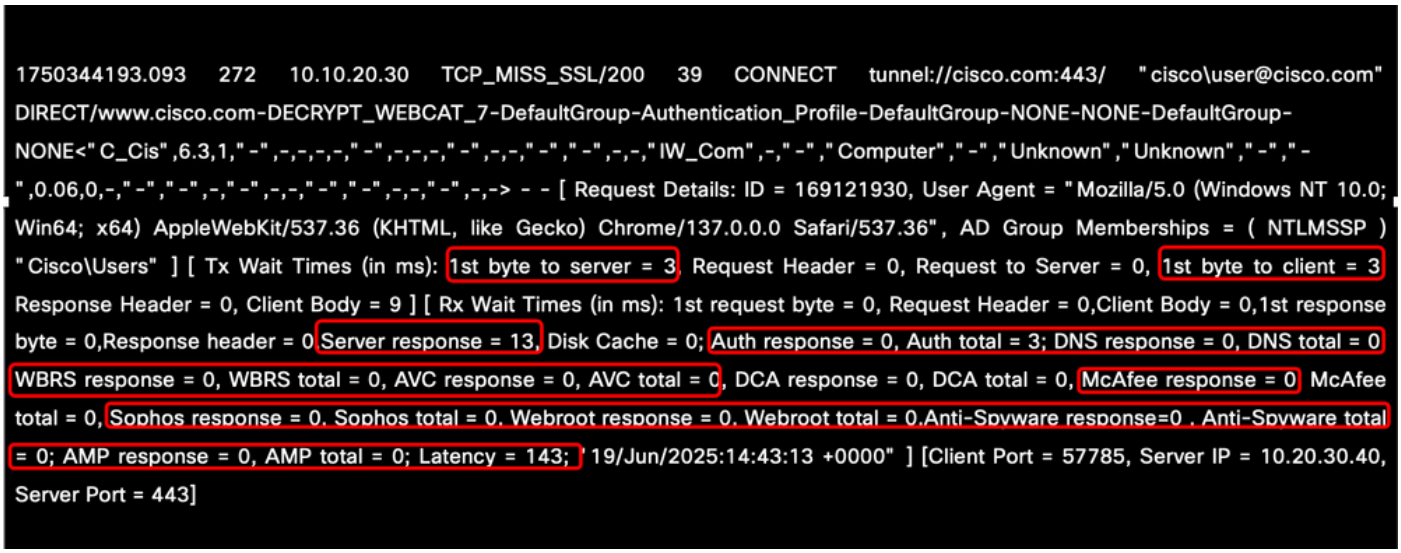


Imagem - Parâmetros de desempenho no AccessLog

Tempo de Autenticação Alto

Se o tempo de resposta de autenticação for alto, essas informações serão necessárias para que o TAC solucione melhor e mais rapidamente os problemas de latência de autenticação:

- Configuração atual de SWA
- Logs de autenticação no modo de depuração ou rastreamento
- Capturas de pacotes de
    - Máquina cliente.
    - SWA (Com filtro para capturar o tráfego do cliente e o tráfego SWA para todos os diretórios ativos configurados nas configurações do território.)
- Certifique-se de que os registros de acesso tenham os campos personalizados %m e %g para identificar o mecanismo e os grupos de autenticação
- Arquivo HAR do cliente ao reproduzir o problema
- A saída do comando testauthconfig da CLI

Este exemplo mostra o tempo de alta latência relacionado à Autenticação:

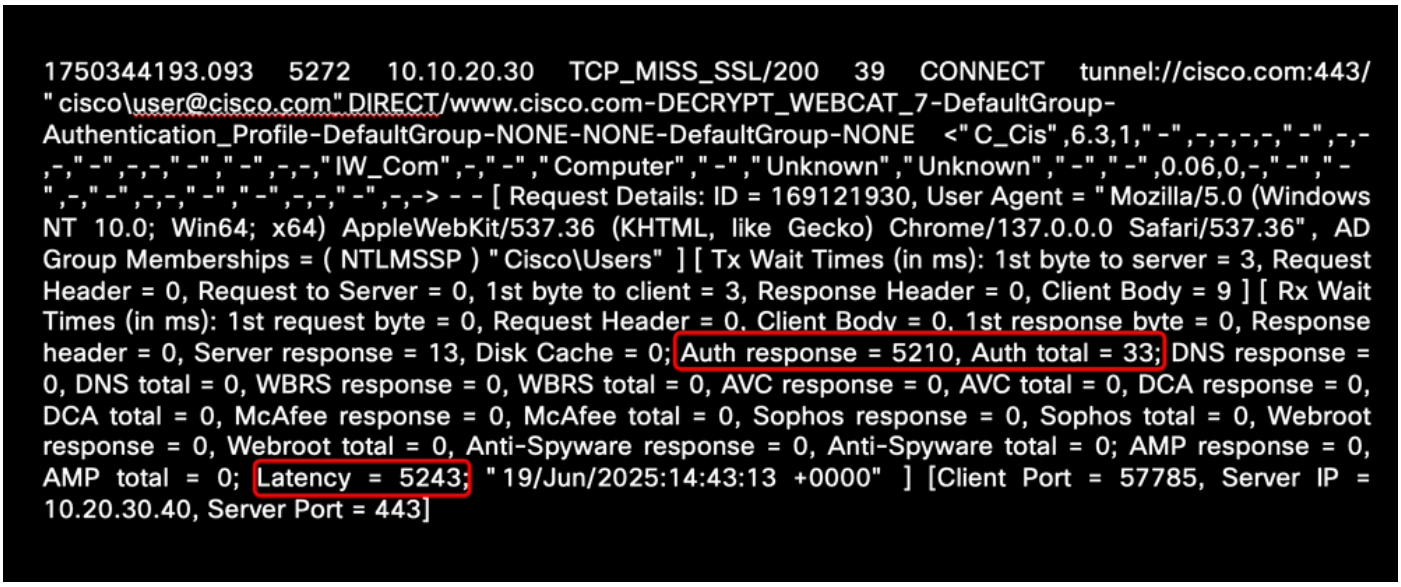


Imagem - Exemplo de alta latência de autenticação

Tempo de DNS Alto

Se o tempo de resposta do DNS for alto, essas informações serão necessárias para que o TAC solucione problemas de latência de DNS:

- Configuração atual de SWA
- Logs do sistema no modo de rastreamento
- Endereço IP dos servidores DNS
- Capturas de pacotes de
    - Máquina cliente
    - SWA (Filtragem com endereço IP de servidores DNS.)
- Certifique-se de que seus registros de acesso tenham %:<d e %:>d no campo personalizado
- Arquivo HAR do cliente ao reproduzir o problema

Para ler mais sobre a configuração e a solução de problemas do DNS, consulte o link [Troubleshoot Secure Web Appliance DNS Service]

Este exemplo mostra o tempo de alta latência relacionado à resolução de nomes 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]
```

Imagem - Exemplo de Alta Latência de Resolução DNS

Tempo Alto do Mecanismo de Verificação

Se o tempo de resposta for alto para os mecanismos de Web Reputation Score (WBRS), Application and Visibility Control (AVC) e Malware Scanning, essas informações serão necessárias para que o TAC solucione problemas relacionados ao alto tempo de resposta do mecanismo de varredura:

- Configuração SWA atual.
- Depende do Mecanismo que tem tempo de resposta alto, altere o nível de log para debug.

Este exemplo mostra o tempo de alta latência relacionado ao 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]
```

Imagem - Alta Latência do Mecanismo de Verificação de Malware

Se os mecanismos de varredura mostrarem alta resposta, para recuperação imediata, você poderá reiniciar o serviço de varredura a partir da CLI, usando estas etapas:

Etapa 1. Digite diagnostic e pressione Enter (Este é um comando oculto e você precisa digitar o comando exato.)

Etapa 2. Selecione SERVICES.

Etapa 3. Para reiniciar o serviço WBRS, escolha WBRS ou vá para a etapa 6.

Etapa 4. Escolha REINICIAR.

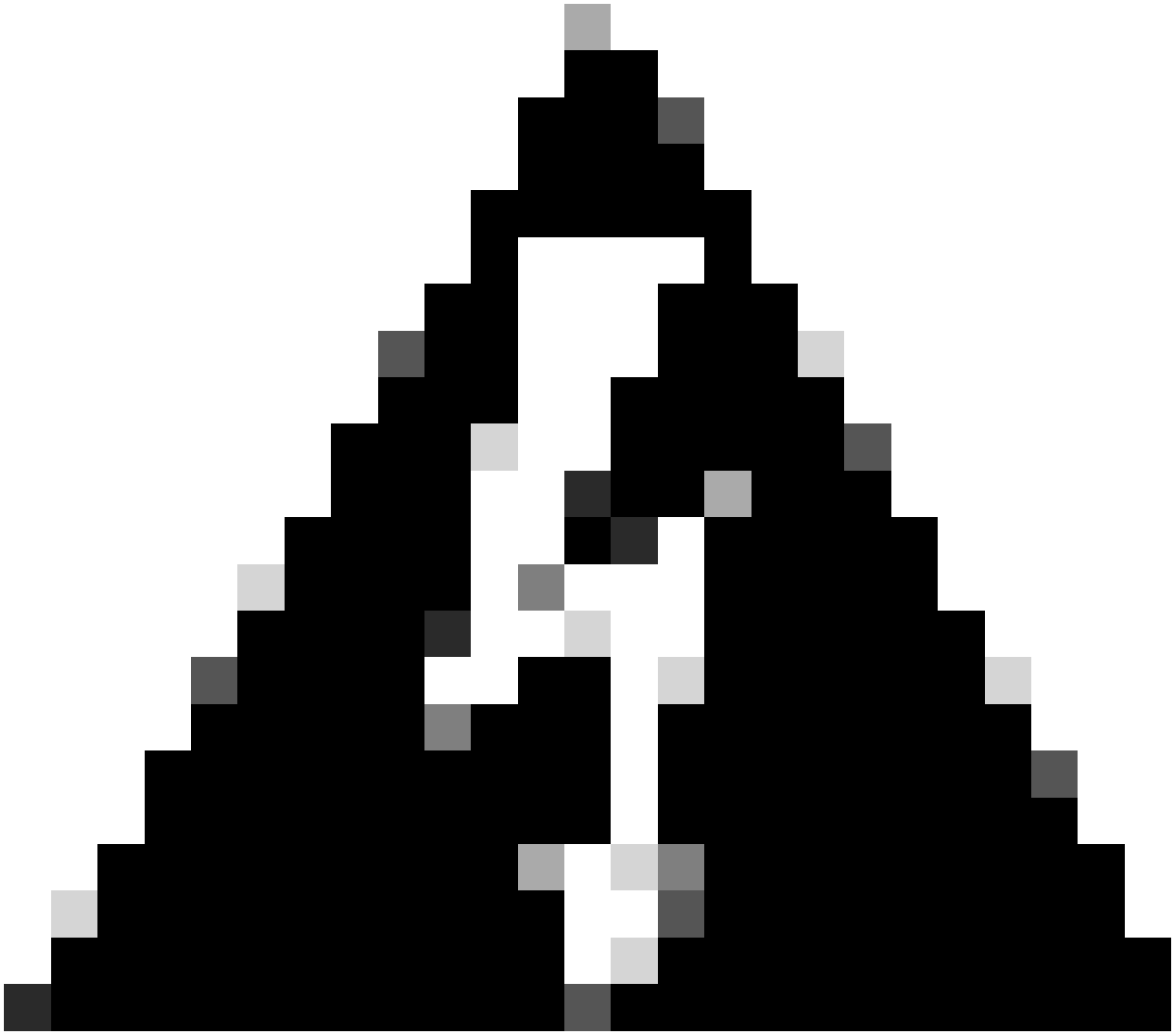
Etapa 5. Continue pressionando Enter para sair do assistente.

Etapa 6. Caso você esteja planejando reiniciar qualquer mecanismo de varredura de malware, escolha ANTIVÍRUS.

Etapa 7. Selecione seus scanners.

Etapa 8. Escolha REINICIAR.

Etapa 9. Continue pressionando Enter para sair do assistente.



aviso: Reiniciar os serviços internos causa a interrupção do serviço. É recomendável executar isso em horas fora da produção ou com cuidado.

Prática recomendada ao conectar a captura de pacotes

Durante a captura de qualquer pacote, colete e compartilhe essas informações com o TAC da Cisco.

- Endereço IP do cliente.
- A URL que você estava tentando acessar.
- O endereço IP resolvido para essa URL no PC cliente e no SWA.
- Experiência do usuário (por exemplo, a página não foi carregada ou está parcialmente carregada e, se houver alguma mensagem de erro, faça uma captura de tela).
- Carimbo de data e hora do teste.
- Feche todos os outros navegadores e aplicativos na máquina cliente. Acesse o site, capture logs no Bloco de Notas para uma tentativa bem-sucedida/malsucedida e compartilhe com o

Suporte da Cisco.

Para obter informações detalhadas sobre como executar a captura de pacotes no SWA, consulte o link Configurar a Captura de Pacotes no Content Security Appliance

Complexidade da configuração

Outra causa comum de alta latência e baixo desempenho é a complexidade da configuração. Isso ocorre quando o SWA é configurado com um número excessivo de condições, perfis e políticas. Essa complexidade pode aumentar significativamente os tempos de resposta e colocar uma carga pesada sobre o processo de proxy. Esse problema tende a se tornar mais pronunciado durante os horários de pico, quando o tráfego está no seu ponto mais alto.

Aqui estão algumas dicas para otimizar a configuração:

1. Limitar descriptografia HTTPS: Somente descriptografe o tráfego essencial para suas políticas de segurança. Sempre que possível, reduza a sobrecarga de processamento enquanto mantém a segurança.
2. Priorize políticas para eficiência: Organize as políticas usadas com mais frequência no início da lista de políticas. Isso garante um processamento mais rápido, tratando primeiro do tráfego mais exigente.
3. Simplificar o design de políticas: Simplifique as políticas minimizando o número possível. Isso reduz o processamento desnecessário e melhora o desempenho geral do sistema.
4. Otimizar a verificação de antimalware e antivírus: revise as configurações de verificação para processos antimalware e antivírus. Elas podem exigir muito da CPU, portanto, seu ajuste pode reduzir significativamente o consumo de recursos sem comprometer a segurança.
5. Usar Expressões Regulares Lightweight: Evite expressões regulares complexas ou que consomem muitos recursos. Certifique-se de que caracteres como pontos (.) e estrelas (*) sejam escapados corretamente para reduzir a tensão de processamento e evitar ineficiências.

Para obter informações detalhadas sobre a prática recomendada de SWA, visite Usar práticas recomendadas de dispositivos da Web seguros

Comandos CLI

Versão

Use o comando version para verificar a alocação de hardware (para SWA virtual) e o status de RAID (para SWA físico). Verifique a configuração de hardware: Verifique se o número de núcleos de CPU, memória e discos rígidos está alocado conforme esperado. Em modelos virtuais, o status de RAID é mostrado como Desconhecido; se o status de RAID for Degradado ou Falha no dispositivo físico, entre em contato com o TAC da Cisco para revisar o status do disco no back-end.

Aqui está um exemplo de alocação de mais CPU para o SWA que pode levar a um comportamento incorreto:

```
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
```

exibealertas

Use o comando displayalerts para verificar mensagens de alerta relacionadas à rede SWA que possam indicar a causa raiz.

Neste exemplo, o servidor DNS no endereço IP 10.10.10.10 não estava respondendo e a mensagem "O serviço de reputação de arquivo não está acessível" pode indicar um problema de conectividade de rede.

```
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

Use o comando process_status para exibir o uso do processo e da memória dos serviços internos do SWA.

Se o processo Prox, que é o processo principal de tratamento de proxying de tráfego, exceder consistentemente 100% de uso por vários minutos, ele indicará uma carga alta sustentada no processo. No entanto, pequenos picos ocasionais no uso da CPU no Prox ou em outros processos são normais e esperados.

<#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
```

detalhe de status

O comando status detail fornece um resumo em tempo real do uso de recursos do sistema, métricas de tráfego de rede e estatísticas de conexão, refletindo a integridade geral e o desempenho do SWA. Ele espelha a exibição Status do sistema na GUI para monitoramento e solução de problemas rápidos.

<#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

O comando ipcheck exibe informações detalhadas do sistema para o Secure Web Appliance, incluindo especificações de hardware, uso de disco, interfaces de rede, chaves de software instaladas e detalhes da versão, fornecendo um instantâneo abrangente do estado atual do equipamento.

<#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
```

taxa

O comando rate imprime as taxas de conexão e o número de solicitações por segundo para cada 10 segundos .

<#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
```

Coletando logs para alta latência

Depende da seção que você está vendo o tempo de resposta alto dos Logs de Acesso ou a carga de processo alta dos logs SHD. Para obter mais soluções de problemas, é melhor alterar a assinatura de log correspondente para Depurar.

aviso: Definir o nível de log como debug ou trace pode levar a um aumento no uso de recursos e fazer com que os arquivos de log girem ou sejam substituídos rapidamente.

Campo Log de Acesso	Campo de Log do SHD	Inscrição de log

		correspondente
Resposta de autenticação , Total de autenticação	—	logs de autenticação
Resposta DNS, total DNS	—	logs_do_sistema
Resposta WBRS, total WBRS	Wbrs_WucLd	Entre em contato com o Cisco TAC
Resposta AVC, total AVC	—	avc_logs
Resposta da McAfee, total da McAfee	McafeeLd	mcafee_logs
Resposta Sophos, total Sophos	SophosLd	sophos_logs
Resposta do Webroot, total do Webroot	WebrootLD	webrootlogs
Resposta da AMP, total da AMP	AMPLd	amp_logs

Informações Relacionadas

Solucionar problemas de desempenho do Secure Web Appliance com registros SHD

Acessar logs do dispositivo da Web seguro

Configurar a captura de pacotes no dispositivo de segurança de conteúdo

Use as práticas recomendadas de dispositivos da Web seguros

Configurar Parâmetro de Desempenho em Logs de Acesso

Solucionar problemas de estados de processo incomuns em SWA

Determinar a taxa de descriptografia em SWA

Solucionar problemas do serviço DNS do Secure Web Appliance

Acessar logs do dispositivo da Web seguro

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.