Fehlerbehebung bei Latenz von sicheren Web-Appliances

Inhalt

Einleitung

In diesem Dokument werden die Schritte zur Fehlerbehebung bei hoher Latenz, hoher Festplattenkapazität und hoher CPU in der Cisco Secure Web Appliance (SWA) beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco SWA-Verwaltung
- Proxy-Bereitstellungsmethoden (explizit und transparent)
- Befehle der SWA-Befehlszeilenschnittstelle (CLI)

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Hintergrundinformationen

Wenn Sie sich an den technischen Support von Cisco wenden, werden Sie gebeten, Details zu den ausgehenden und eingehenden Netzwerkaktivitäten des SWA anzugeben. Diese können überwacht werden, indem eine Paketerfassung ausgeführt wird, um Datenverkehr für Debugging- oder Verifizierungszwecke zu erfassen.

Häufige Ursachen für hohe Latenz in SWA

Allgemein gibt es drei Hauptkategorien für die hohe Latenz in SWA:

1. Unzureichende SWA-Größe oder überlastete Ressourcen
2. Komplexe Konfigurationen
3. Netzwerkbezogene Latenzprobleme

Eine der häufigsten Ursachen für die hohe Latenz in SWA ist die unzureichende Dimensionierung der Lösung. Die richtige Dimensionierung ist entscheidend, um sicherzustellen, dass das SWA-System über ausreichende Ressourcen verfügt, um aktuelle und erwartete Workloads zu verarbeiten. Wenn das System zu klein ist, kann es schwierig sein, Anfragen effizient zu bearbeiten, was zu Verzögerungen im Betrieb und einer reduzierten Leistung führt. Faktoren wie die Anzahl der Benutzer, der Umfang der Entschlüsselung und spezifische Scananforderungen müssen während der Bereitstellung sorgfältig evaluiert werden, um Ressourceneinschränkungen zu vermeiden. Wenn die SWA-Kapazität nicht an den geschäftlichen Anforderungen ausgerichtet wird, kann dies zu einer dauerhaften Latenz und einer Beeinträchtigung der Benutzerfreundlichkeit führen.

Komplexe Konfigurationen können die Leistung beeinträchtigen und Latenzen auf dem SWA

verursachen, insbesondere bei hoher Auslastung, da jede Anforderung unter verschiedenen Bedingungen verarbeitet werden muss.

Netzwerkbedingte Latenz kann vom SWA selbst, von Drittanbieterdiensten wie Active Directory, DLP, DNS oder von Netzwerkverzögerungen zwischen dem Client, SWA und den Upstream-Servern herrühren.

Die Analyse der an die SWA gesendeten Anfragen, einschließlich der Identifizierung der wichtigsten Benutzer und der URLs, auf die am häufigsten zugegriffen wird, kann dabei helfen, potenzielle Fehlverhalten aufzudecken und die Ursachen der Latenz zu ermitteln. Diese Informationen sind von unschätzbarem Wert für die Diagnose von Leistungsproblemen, die Verwaltung der Bandbreitennutzung und die Gewährleistung einer angemessenen Nutzung des Systems.

Tools zur Fehlerbehebung bei SWA-Latenz

Systemstatus

Gehen Sie folgendermaßen vor, um den aktuellen Ressourcenverbrauch in SWA zu überprüfen:

Schritt 1: Zugriff auf die grafische Benutzeroberfläche (GUI) von SWA

Schritt 2: Navigieren Sie zu Reporting > System Information > System Status.

Schritt 3: Überprüfen Sie diese wichtigen Metriken, um die Systemleistung zu bewerten:

- CPU-Verwendung (%): Zeigt die aktuelle CPU-Last an.
- RAM-Nutzung (%): Reflektiert die Speichernutzung
- Verwendung von Berichten/Protokollen (%): Zeigt den Prozentsatz des für Berichte und Protokolle verwendeten Festplattenspeichers an.
- Systembetriebszeit: Zeigt die Gesamtzeit an, die das System ohne Neustart ausgeführt wurde.

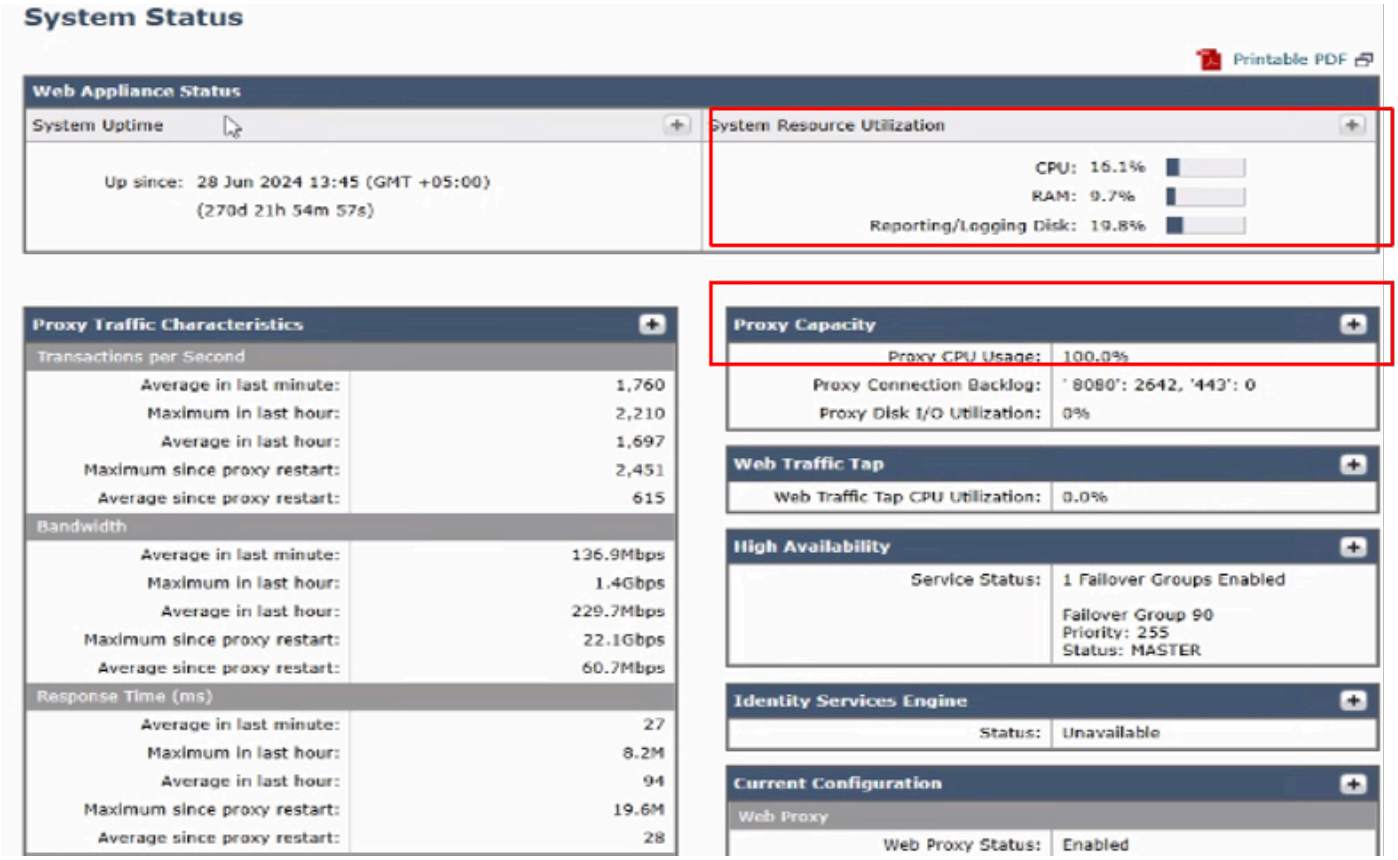


Bild - Systemstatus

Diese Seite bietet eine Übersicht über den aktuellen Status von RAM, CPU und Festplattennutzung. Um die Ressourcennutzung über einen bestimmten Zeitraum anzuzeigen, navigieren Sie von der SWA-GUI zu Reporting, und wählen Sie System Capacity (Systemkapazität).

Systemkapazität

Die Seite "Systemkapazität" im SWA bietet eine umfassende Ansicht der Ressourcenauslastung und Leistungskennzahlen über einen festgelegten Zeitraum. Auf dieser Seite finden Sie detaillierte Diagramme zur Überwachung und Analyse des Systemverhaltens, zur Sicherstellung optimaler Leistung und zur Identifizierung potenzieller Engpässe.

Verfügbare Diagramme und Metriken auf der Seite "Systemkapazität" sind:

1. CPU-Auslastung insgesamt: Zeigt die gesamte CPU-Auslastung an und gibt einen allgemeinen Überblick über die Systemleistung.
2. CPU-Nutzung nach Funktion: Unterteilt die CPU-Nutzung anhand bestimmter Funktionen, darunter:

- Webproxy
- Protokollieren
- Berichterstellung
- McAfee
- Sophos
- Webroot

- Akzeptable Nutzung und Reputation

3. Reaktionszeit/Latenz (Millisekunden): Verfolgt Reaktionszeiten, um Verzögerungen bei der Verarbeitung von Anfragen zu identifizieren.

4. Transaktionen pro Sekunde: Zeigt die Anzahl der Transaktionen an, die vom SWA pro Sekunde verarbeitet werden.

5. Ausgehende Verbindungen: Überwacht die Anzahl der hergestellten ausgehenden Verbindungen.

6. Ausgangsbandbreite (Byte): Misst die ausgehende Bandbreite, die genutzt wird.

7. Proxy-Pufferspeicher (%): Zeigt den Prozentsatz des Speichers an, der vom Proxyprozess verwendet wird.

Prüfen Sie die Kennzahlen für Anzeichen einer hohen Ressourcennutzung in diesem Dashboard.

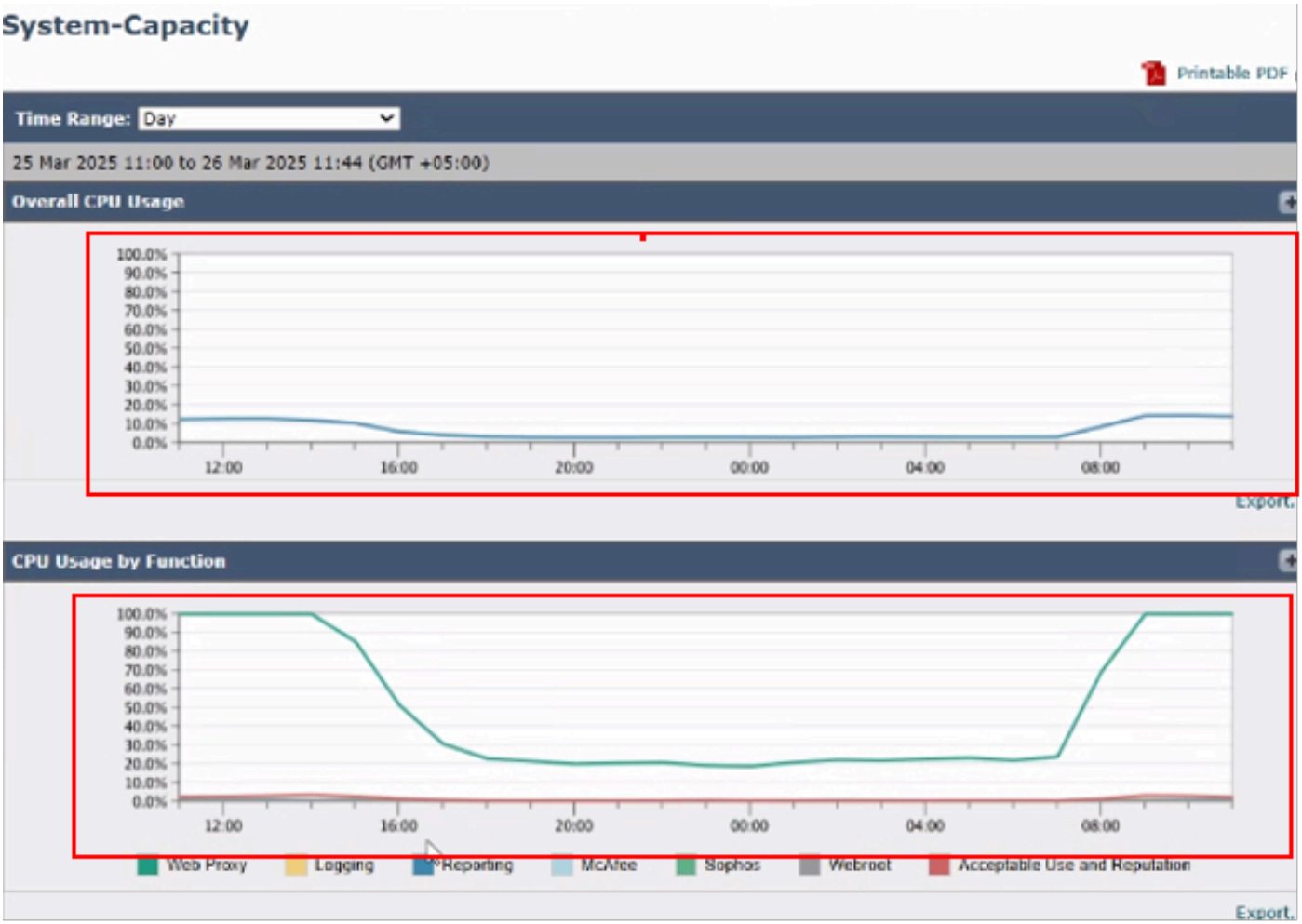


Image- Systemkapazität

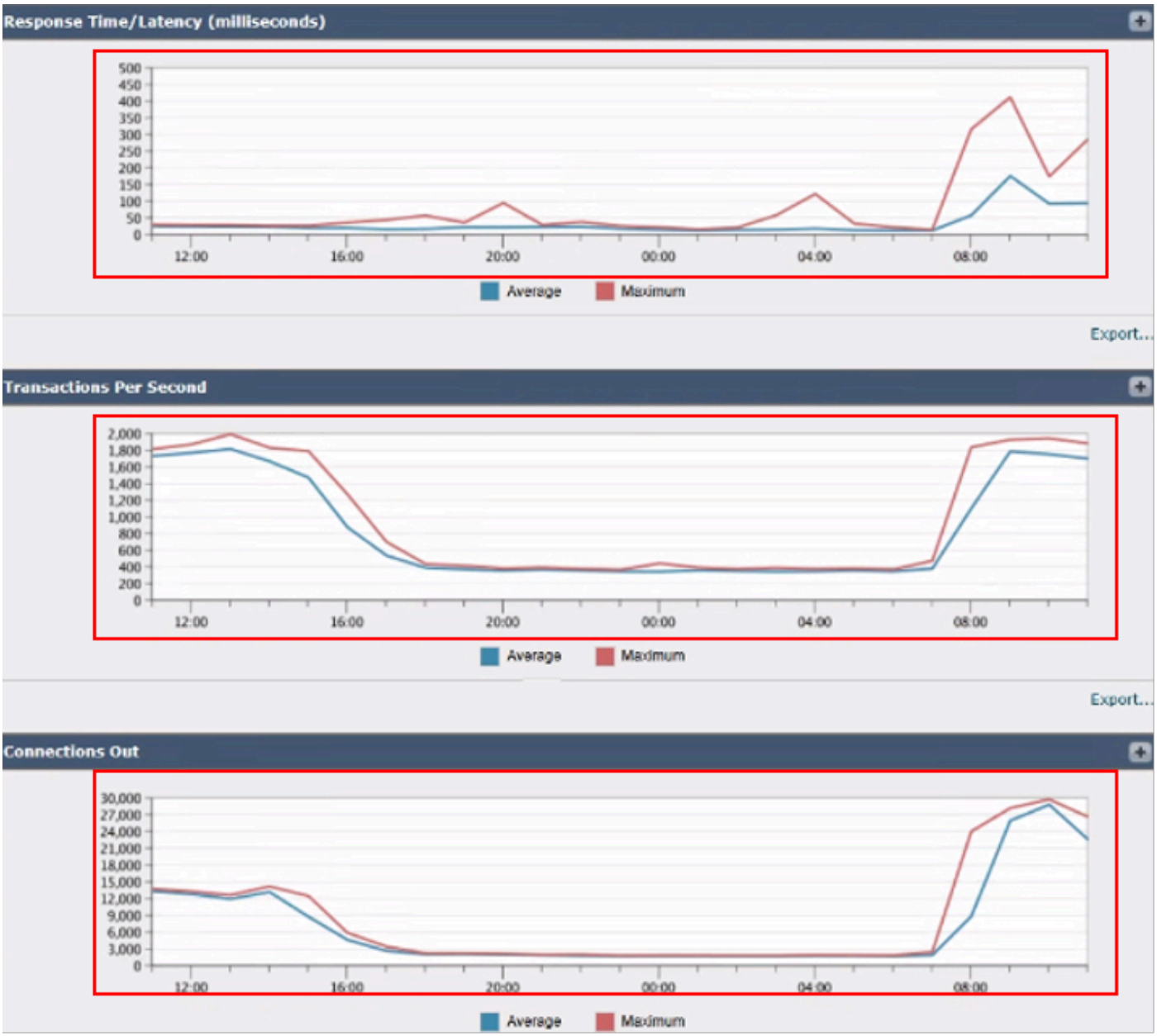


Bild: SWA-Transaktionen pro Sekunde und Verbindungsausgänge

Bild - SWA-Speicherauslastung

Häufigste Ziele analysieren

Um die wichtigsten Ziele zu analysieren, navigieren Sie zur SWA-GUI, navigieren Sie zu Reporting, und wählen Sie Websites aus. Überprüfen Sie die Liste der führenden HTTP-/HTTPS-Websites, und identifizieren Sie Domains mit hohem Datenverkehrsaufkommen oder Domains, auf die häufig zugegriffen wird.

Ziehen Sie auf der Grundlage Ihrer Ergebnisse in Betracht, generische URLs wie Microsoft Updates, Adobe, Office365 und Online-Meeting-Plattformen zu umgehen oder davon auszunehmen. Mit diesem Ansatz wird der Datenverkehr in den SWAs reduziert, was zu einer niedrigeren Latenz und einer geringeren Proxy-Verarbeitungslast führt.

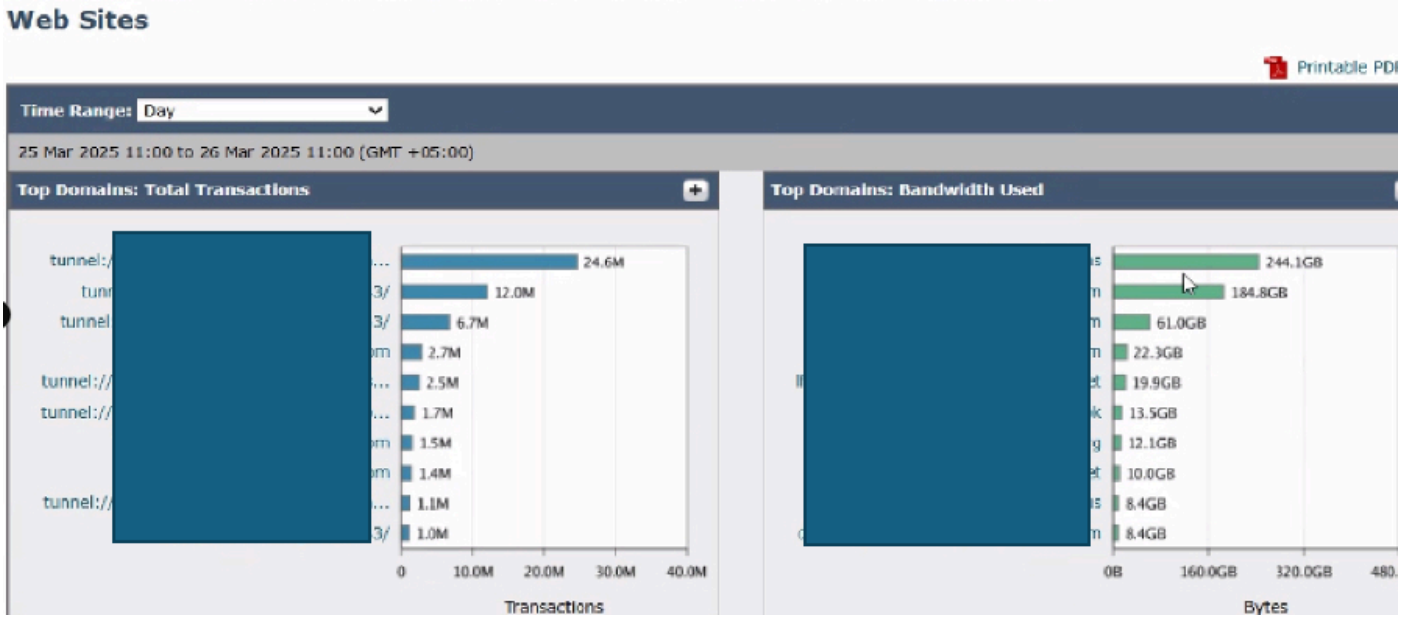


Bild - SWA Top Websites Dashboard

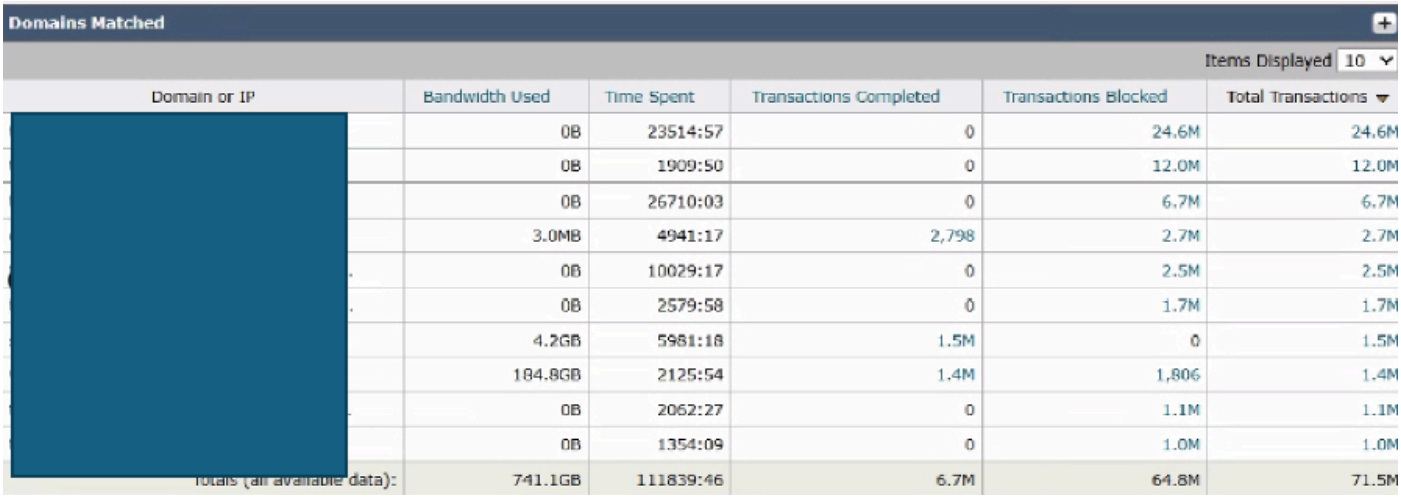


Bild - SWA Top Domains Dashboard

Analyse der Hauptbenutzer

Um potenzielle Quellen für übermäßigen Datenverkehr zu identifizieren, navigieren Sie aus Reporting zur SWA-GUI und wählen Sie Users (Benutzer) aus.

Prüfen Sie die Liste, um zu ermitteln, welche Benutzer die höchste Anzahl an Transaktionen für den SWA generieren. Prüfen Sie außerdem, ob Benutzersysteme die höchste Anzahl von Transaktionen mit dem SWA generieren und die maximale Bandbreite beanspruchen.

Diese Analyse kann dabei helfen, Benutzer oder Geräte zu identifizieren, die für erhebliche Datenverkehrslasten verantwortlich sind, und ermöglicht gezielte Maßnahmen zur Verringerung der Gesamtsystembelastung.

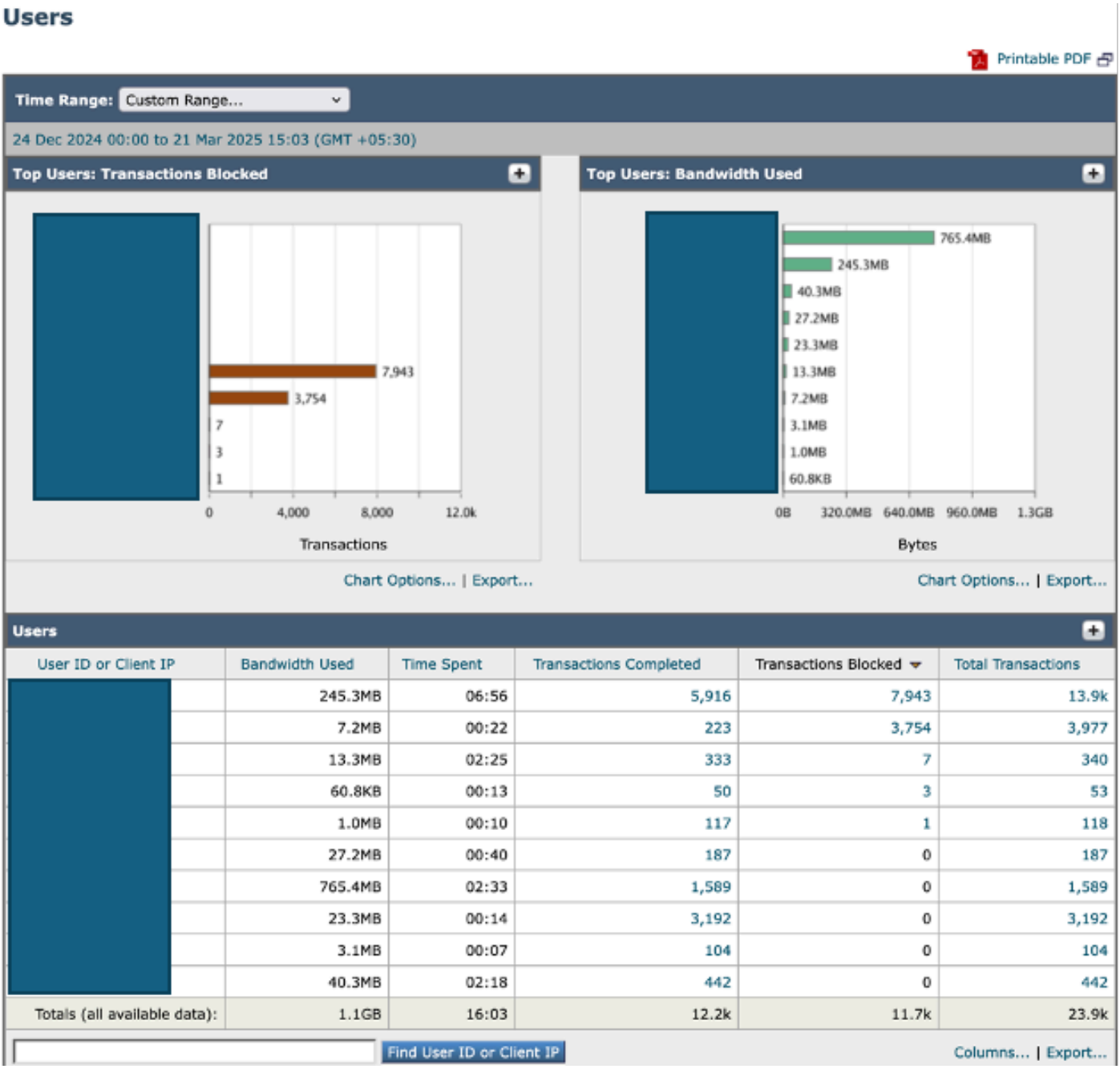


Bild-SWA-Dashboard für Top-Benutzer

SHD-Protokolle

Durch Überprüfen von SHD_log können Sie einige Leistungskennzahlen analysieren, z. B. die Anzahl der Sitzungen von Benutzern für SWA (CliConn), die Anzahl der Sitzungen von SWA für das Internet (SrvConn), die durchschnittlichen Anforderungen pro Sekunde (Reqs) usw.

Weitere Informationen zum SHD-Protokoll finden Sie unter Troubleshoot Secure Web Appliance Performance with SHD Logs,

Einige wichtige Parameter, die in den SHD-Protokollen überprüft werden müssen, sind:

- Clientverbindungen: Anzahl der aktiven Client-Verbindungen

- ServerVerbindungen: Anzahl der aktiven Serververbindungen
- ProxLd: Durchschnittliche Proxy-Prozesslast
- CPULD: Durchschnittliche Gesamt-CPU-Last
- RAMUTIL: RAM-Nutzung
- Latenz: durchschnittliche Servicezeit in einer Minute
- DiskUtil: Festplattennutzung und E/A-Leistung

Wie in diesem Beispiel führt die Verarbeitung von ca. 1.600 Anfragen pro Sekunde zu einer hohen Proxy-Prozesslast.

```
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
```

Verwenden von Zugriffsprotokollen zur Behebung von Latenzproblemen

Bei Latenzproblemen im Zusammenhang mit dem Datenverkehr, der über ein SWA geleitet wird, können Zugriffsprotokolle als nützliches Tool zur Identifizierung der wahrscheinlichen Ursache dienen. Um die Fehlerbehebung zu verbessern, können Sie entweder die vorhandenen Zugriffsprotokolleinstellungen ändern oder ein neues Zugriffsprotokoll erstellen. Durch die Aufnahme von Leistungsparametern in das benutzerdefinierte Feld erhalten Sie tiefere Einblicke in Faktoren, die zu Latenz beitragen, und ermöglichen so eine effektivere Analyse und Auflösung.

Weitere Informationen zu den Leistungsparametern und den Konfigurationsschritten finden Sie unter: Configure Performance Parameter in Access Logs (Leistungsparameter konfigurieren in Zugriffsprotokollen).

Im Folgenden finden Sie eine detaillierte Anleitung zum Sammeln von Protokollen im SWA: Zugreifen auf Protokolle der sicheren Web-Appliance

Die Latenzquellen können analysiert werden, indem wichtige Parameter überprüft werden, mit denen bestimmt werden kann, ob es zu Verzögerungen zwischen dem Client und dem SWA, innerhalb der internen SWA-Prozesse oder zwischen dem SWA und dem Webserver kommt. Netzwerkbasierte Services wie DNS-Auflösung, Authentifizierungszeit und Reaktionszeiten von Servern oder Clients sind wichtige Indikatoren, die berücksichtigt werden sollten. Außerdem müssen die durch Scan-Engines wie AMP, Sophos und AVC verursachten Verzögerungen evaluiert werden, um die Auswirkungen auf die Latenz insgesamt zu ermitteln.

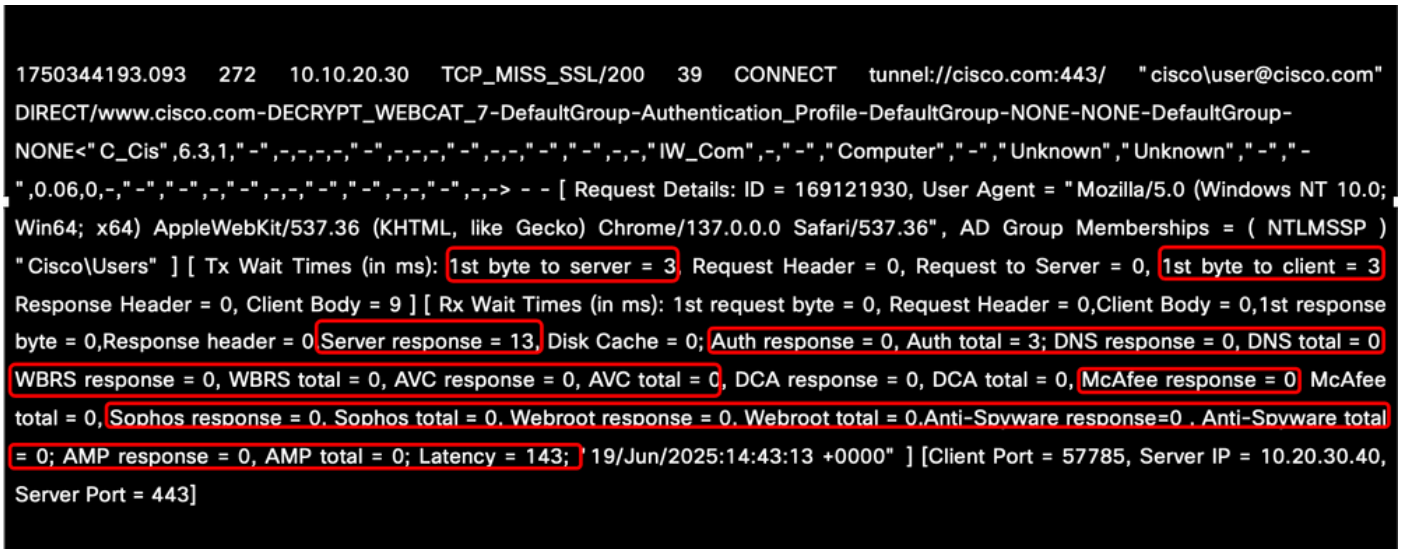


Image - Leistungsparameter im AccessLog

Hohe Authentifizierungszeit

Wenn die Antwortzeit für die Authentifizierung hoch ist, benötigt das TAC diese Informationen, um die Authentifizierungslatenz besser und schneller zu beheben:

- Aktuelle SWA-Konfiguration
- Authentifizierungsprotokolle im Debug- oder Ablaufverfolgungsmodus
- Paketerfassung von
    - Client-Computer.
    - SWA (Mit Filter zum Erfassen des Client-Datenverkehrs und des SWA-Datenverkehrs zu allen aktiven Verzeichnissen, die in den Bereichseinstellungen konfiguriert wurden.)
- Vergewissern Sie sich, dass AccessLogs über das benutzerdefinierte Feld %m und %g verfügt, um den Authentifizierungsmechanismus und die Gruppen zu identifizieren.
- HAR-Datei vom Client während der Wiedergabe des Problems
- Die Ausgabe des Befehls testauthconfig in der CLI

Dieses Beispiel zeigt die hohe Latenzzeit bei der Authentifizierung:

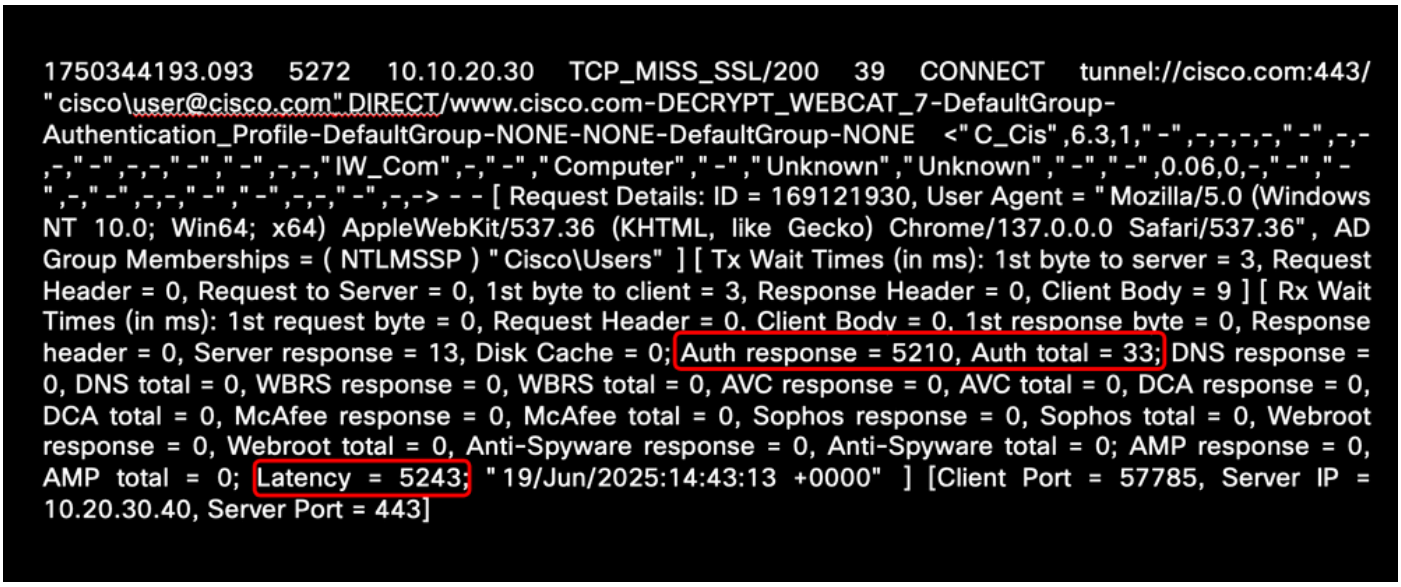


Image - Beispiel für hohe Authentifizierungslatenz

Hohe DNS-Zeit

Wenn die DNS-Reaktionszeit hoch ist, benötigt das TAC diese Informationen, um Probleme mit der DNS-Latenz zu beheben:

- Aktuelle SWA-Konfiguration
- System meldet sich im Ablaufverfolgungsmodus an
- IP-Adresse des DNS-Servers
- Paketerfassung von
    - Client-Computer
    - SWA (Filterung nach IP-Adresse des DNS-Servers)
- Vergewissern Sie sich, dass die Zugriffsprotokolle sowohl %:<d als auch %:>d im benutzerdefinierten Feld enthalten.
- HAR-Datei vom Client während der Wiedergabe des Problems

Weitere Informationen zur DNS-Konfiguration und Fehlerbehebung finden Sie unter dem Link [Fehlerbehebung bei sicherem Web-Appliance-DNS-Dienst]

Dieses Beispiel zeigt die hohe Latenzzeit bei der DNS-Namensauflösung:

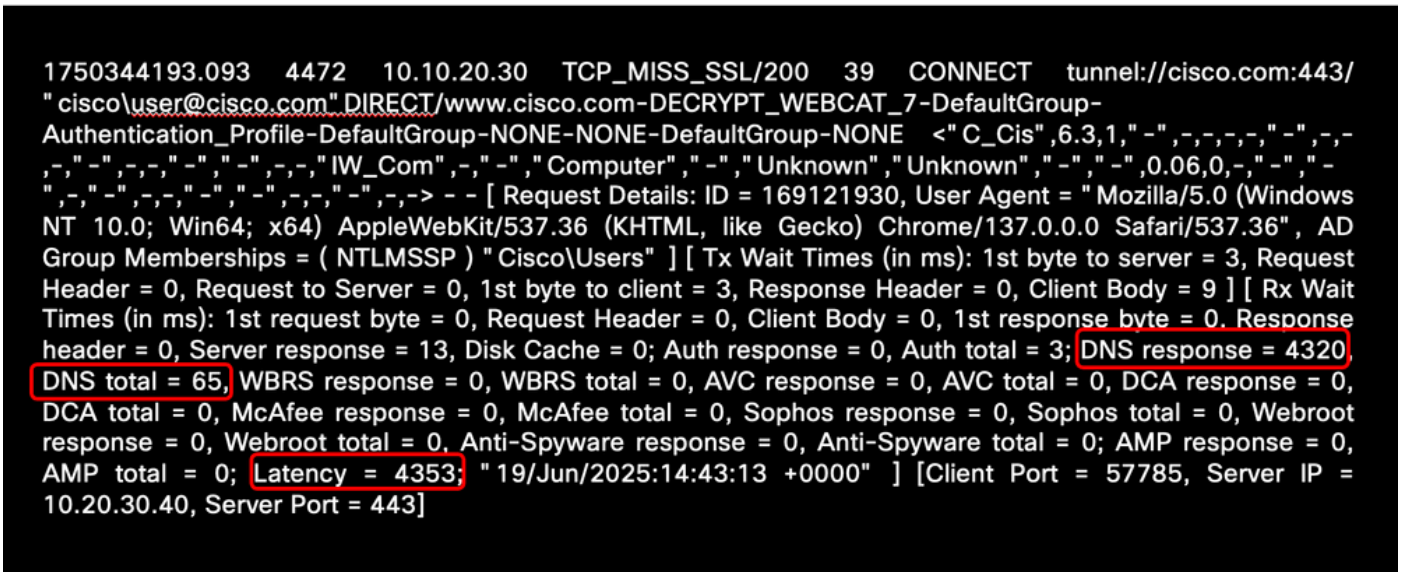


Bild - Beispiel für hohe DNS-Auflösungslatenz

Hohe Scanning-Engine-Zeit

Wenn die Reaktionszeit für die Module Web Reputation Score (WBRS), Application and Visibility Control (AVC) und Malware Scanning hoch ist, werden diese Informationen vom TAC benötigt, um die hohe Reaktionszeit der Scan Engine zu beheben:

- Aktuelle SWA-Konfiguration
- Abhängig von der Engine mit hoher Reaktionszeit, ändern Sie die Protokollierungsebene zu debug.

Dieses Beispiel zeigt die hohe Latenzzeit in Bezug auf die Sophos Engine:

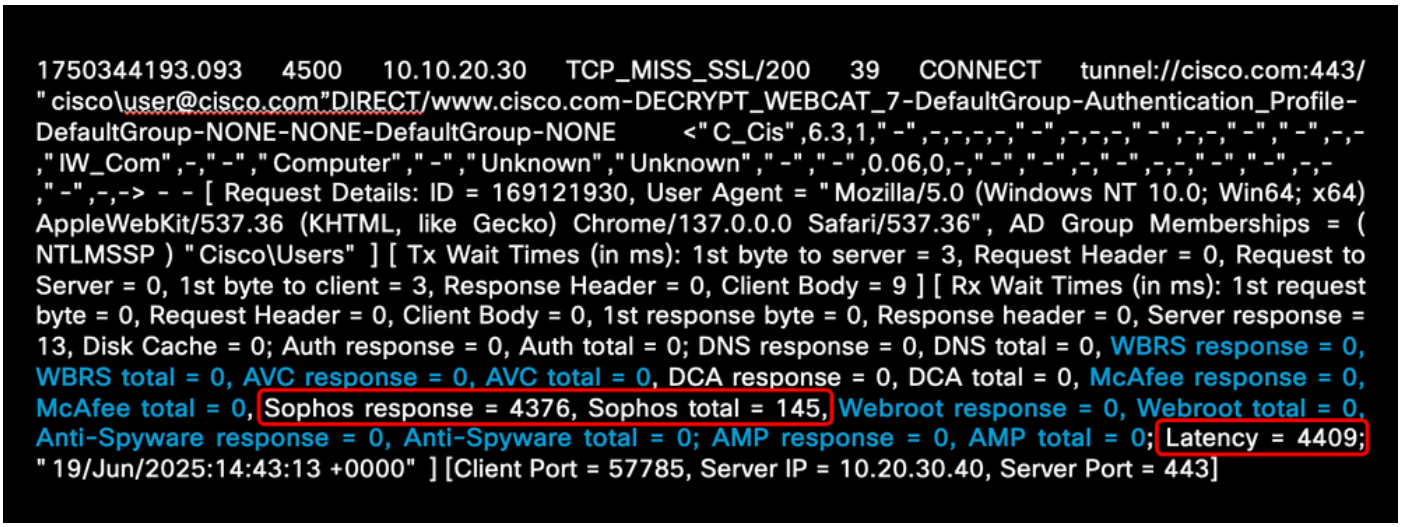


Image - Malware Scanning Engine - hohe Latenz

Wenn die Scan-Engines eine hohe Reaktion zeigen, können Sie zur sofortigen Wiederherstellung den Scan-Service von der CLI aus mit folgenden Schritten neu starten:

Schritt 1. Geben Sie diagnostic ein und drücken Sie die Eingabetaste (Dies ist ein ausgeblendeter Befehl, und Sie müssen den genauen Befehl eingeben.)

Schritt 2. Wählen Sie SERVICES.

Schritt 3: Um den WBRS-Dienst neu zu starten, wählen Sie WBRS aus, oder fahren Sie mit Schritt 6 fort.

Schritt 4: Wählen Sie RESTART.

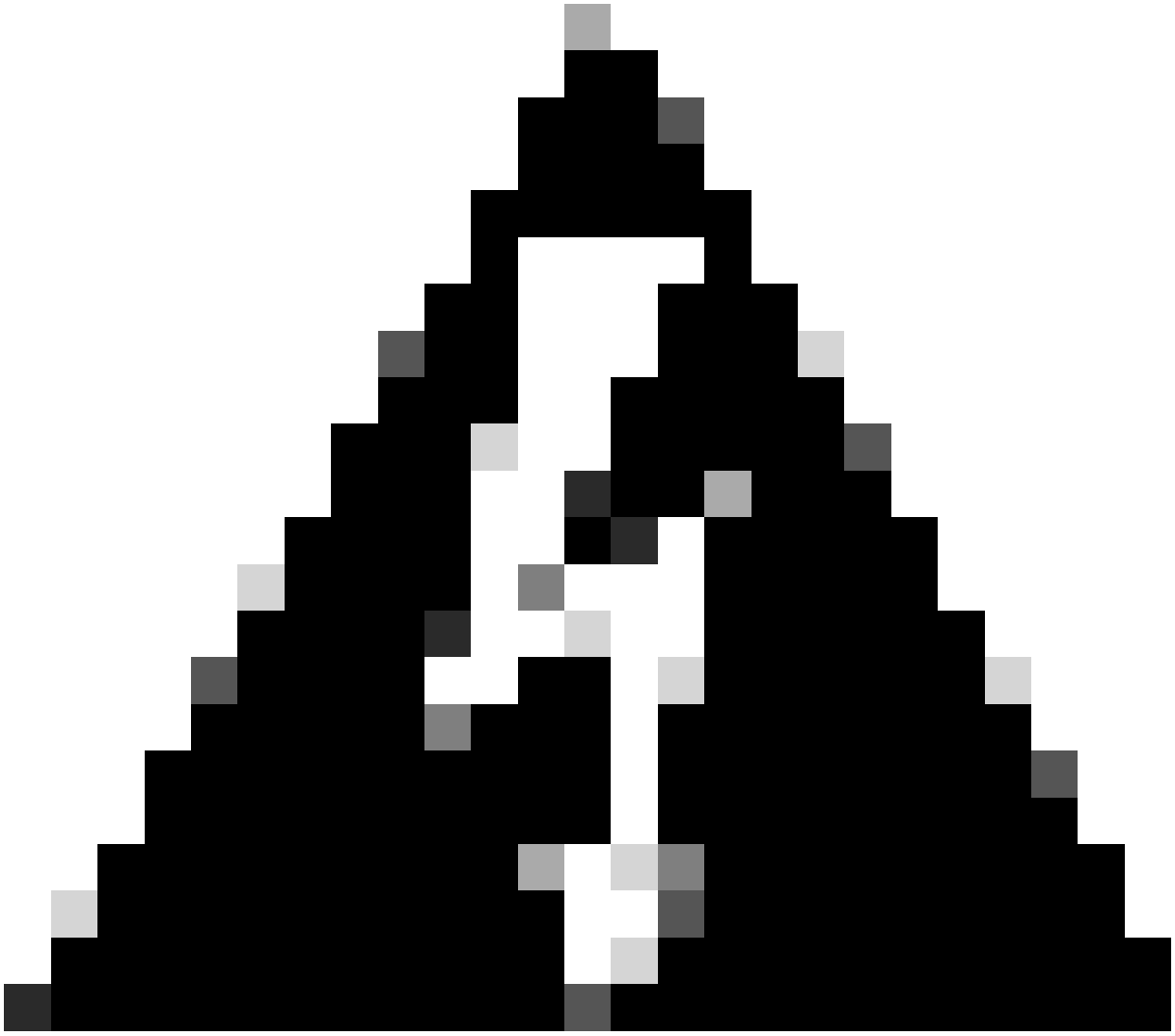
Schritt 5. Drücken Sie weiterhin die Eingabetaste, um den Assistenten zu beenden.

Schritt 6. Falls Sie einen Neustart einer Malware-Scan-Engine planen, wählen Sie ANTIVIRUS.

Schritt 7: Wählen Sie Ihre Scanner aus.

Schritt 8: Wählen Sie RESTART.

Schritt 9. Drücken Sie weiterhin die Eingabetaste, um den Assistenten zu beenden.



Warnung: Das Neustarten der internen Services führt zu einer Unterbrechung des Service. Empfehlen Sie, dies außerhalb der Produktionszeiten oder mit Vorsicht durchzuführen.

Best Practice beim Verbinden der Paketerfassung

Sammeln Sie diese Informationen bei der Paketerfassung, und geben Sie sie an das Cisco TAC weiter.

- Client-IP-Adresse
- Die URL, auf die Sie zugreifen wollten.
- Die IP-Adresse wurde für diese URL vom Client-PC und vom SWA aufgelöst.
- Benutzererfahrung (z. B. Seite wurde nicht oder nur teilweise geladen, und wenn Fehlermeldungen vorliegen, erstellen Sie einen Screenshot).
- Zeitstempel des Tests.
- Schließen Sie alle anderen Browser und Apps auf dem Client-Computer. Greifen Sie auf die

Website zu, erfassen Sie Protokolle im Editor für einen Erfolgs-/Fehlerversuch, und senden Sie diese an den Cisco Support.

Ausführliche Informationen zum Durchführen der Paketerfassung in SWA finden Sie unter Configure Packet Capture on Content Security Appliance.

Komplexität der Konfiguration

Eine weitere häufige Ursache für hohe Latenz und schlechte Leistung ist die Komplexität der Konfiguration. Dies tritt auf, wenn die SWA mit einer zu großen Anzahl an Bedingungen, Profilen und Richtlinien konfiguriert ist. Diese Komplexität kann die Reaktionszeiten deutlich erhöhen und den Proxy-Prozess stark belasten. In Spitzenzeiten, wenn der Verkehr am höchsten ist, tritt dieses Problem tendenziell häufiger auf.

Hier einige Tipps zur Optimierung der Konfiguration:

1. HTTPS-Entschlüsselung einschränken: Entschlüsseln Sie nur den Datenverkehr, der für Ihre Sicherheitsrichtlinien erforderlich ist. Reduzieren Sie, wann immer möglich, den Verarbeitungsaufwand, und wahren Sie die Sicherheit.
2. Mehr Effizienz durch die Priorisierung von Richtlinien: Ordnen Sie die am häufigsten verwendeten Richtlinien ganz oben in der Liste an. Dadurch wird eine schnellere Verarbeitung sichergestellt, da der anspruchsvollste Datenverkehr zuerst adressiert wird.
3. Optimiertes Richtliniendesign: Vereinfachen Sie Richtlinien, indem Sie deren Anzahl so weit wie möglich minimieren. Dies reduziert unnötige Verarbeitungsvorgänge und verbessert die Gesamtleistung des Systems.
4. Optimierung der Anti-Malware- und Anti-Virus-Suche: Überprüfen Sie die Scankonfigurationen für Anti-Malware- und Anti-Virus-Prozesse. Diese können CPU-intensiv sein, sodass eine Feinabstimmung den Ressourcenverbrauch erheblich reduzieren kann, ohne die Sicherheit zu beeinträchtigen.
5. Leichte reguläre Ausdrücke verwenden: Vermeiden Sie komplexe oder ressourcenintensive reguläre Ausdrücke. Stellen Sie sicher, dass Zeichen wie Punkte (.) und Sterne (*) ordnungsgemäß als Escapezeichen erkannt werden, um die Verarbeitungsleistung zu reduzieren und Ineffizienzen zu vermeiden.

Detaillierte Informationen zu den Best Practices für SWA finden Sie unter Best Practices für die Verwendung sicherer Web-Appliances.

CLI-Befehle

Version

Verwenden Sie den Befehl version, um die Hardwarezuweisung (für virtuelles SWA) und den RAID-Status (für physisches SWA) zu überprüfen. Überprüfen Sie die Hardwarekonfiguration: Stellen Sie sicher, dass die Anzahl der CPU-Kerne, Arbeitsspeicher und Festplatten wie erwartet zugewiesen sind. Bei virtuellen Modellen wird der RAID-Status als "Unbekannt" angezeigt. Wenn der RAID-Status in der physischen Appliance "Heruntergestuft" oder "Fehlgeschlagen" lautet,

wenden Sie sich an das Cisco TAC, um den Festplattenstatus vom Back-End aus zu überprüfen.

Im Folgenden finden Sie ein Beispiel dafür, wie der SWA mehr CPU zugewiesen wird, was zu Fehlverhalten führen kann:

```
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
```

Anzeigen von Warnmeldungen

Verwenden Sie den Befehl displayAlerts, um die netzwerkbezogenen Warnmeldungen von SWA zu überprüfen, die auf die Ursache hinweisen können.

In diesem Beispiel hat der DNS-Server mit der IP-Adresse 10.10.10.10 nicht geantwortet, und die Meldung "Der Dateireputations-Dienst ist nicht erreichbar" kann auf ein Problem mit der Netzwerkverbindung hinweisen.

```
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
```

Status des Prozesses

Verwenden Sie den Befehl process_status, um die Prozess- und Speichernutzung der internen SWA-Dienste anzuzeigen.

Wenn der Prox-Prozess, der als Hauptprozess für das Datenverkehr-Proxying fungiert, die Auslastung von 100 % für mehrere Minuten konstant überschreitet, weist dies auf eine anhaltend hohe Auslastung des Prozesses hin. Gelegentliche kurze Spitzen bei der CPU-Auslastung auf dem Proxy oder anderen Prozessen sind jedoch normal und werden erwartet.

<#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
```

Statusdetail

Der Befehl status detail bietet eine Echtzeitübersicht über die Nutzung der Systemressourcen, die Netzwerkverkehrsmetriken und die Verbindungsstatistiken, die den allgemeinen Status und die Leistung des SWA widerspiegeln. Er spiegelt die Systemstatusansicht in der GUI für eine schnelle Überwachung und Fehlerbehebung.

<#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

Der Befehl ipcheck zeigt detaillierte Systeminformationen für die sichere Web-Appliance an, einschließlich Hardware-Spezifikationen, Festplattennutzung, Netzwerkschnittstellen, installierte Softwareschlüssel und Versionsdetails, um einen umfassenden Überblick über den aktuellen Zustand der Appliance zu erhalten.

<#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
```

rate

Der Befehl rate gibt die Verbindungsraten und die Anzahl der Anfragen pro Sekunde für jeweils 10 Sekunden aus.

<#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
```

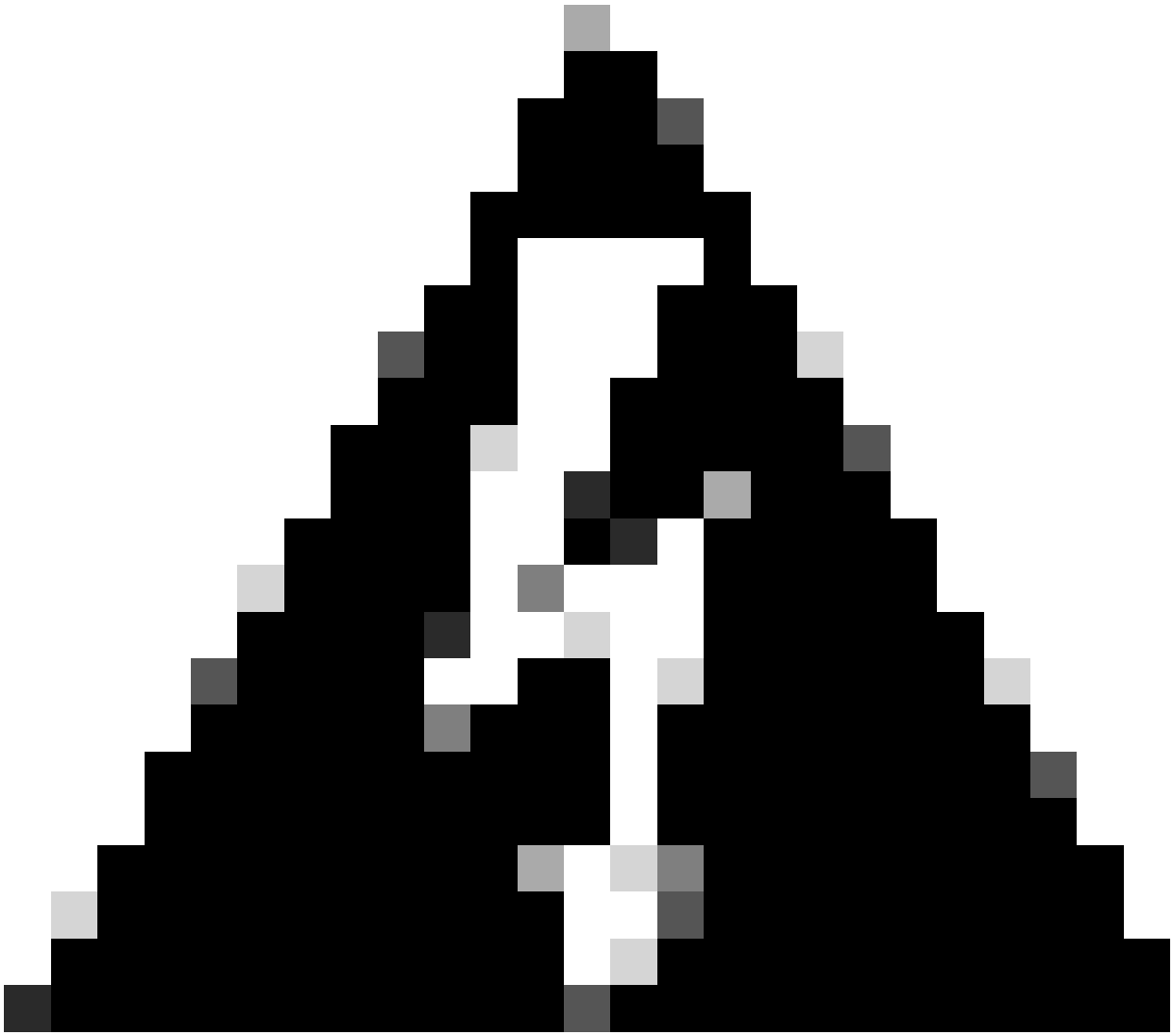
100.00 1800 17 16352 1626 178551 178551 0.0 2366 0

100.00 1813 18 16453 1659 226301 224952 0.6 3008 0

99.00 1799 10 16338 1645 206234 206234 0.0 3430 1

Sammeln von Protokollen für hohe Latenz

Es hängt von dem Abschnitt ab, dass Sie eine hohe Reaktionszeit von den Zugriffsprotokollen oder eine hohe Prozesslast von den SHD-Protokollen sehen. Für weitere Fehlerbehebungen ist es am besten, das entsprechende Protokoll-Abonnement in Debug zu ändern.



Warnung: Das Festlegen der Protokollebene auf debug oder trace kann zu einer erhöhten Ressourcenauslastung führen und dazu, dass Protokolldateien schnell gedreht oder überschrieben werden.

Zugriffsprotokollfeld	SHD-Protokollfeld	Entsprechendes Protokoll-Abonnement
Auth-Antwort, Auth gesamt	—	Authentilog
DNS-Antwort, DNS gesamt	—	Systemprotokolle
WBRS-Antwort, WBRS gesamt	WBRS_WUCId	Cisco TAC kontaktieren
AVC-Antwort, AVC gesamt	—	AVC-Protokolle
McAfee-Antwort, McAfee gesamt	McafeeLd	mcafee_logs
Sophos-Antwort, Sophos gesamt	SophosLd	sophos_logs
Webroot-Antwort, Webroot gesamt	WebrootLd	Webrootlogs
AMP-Antwort, AMP gesamt	AMPLd	AMP-Protokolle

Zugehörige Informationen

Fehlerbehebung bei der Leistung sicherer Web-Appliances mit SHD-Protokollen

Zugreifen auf Protokolle der sicheren Web-Appliance

Konfigurieren der Paketerfassung auf der Content Security Appliance

Best Practices für sichere Web-Appliances

Konfigurieren von Leistungsparametern in Zugriffsprotokollen

Fehlerbehebung bei ungewöhnlichen Prozesszuständen in SWA

Ermitteln der Entschlüsselungsrate in SWA

Fehlerbehebung beim DNS-Dienst der sicheren Webappliance

Zugreifen auf Protokolle der sicheren Web-Appliance

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.