

Cisco WAAS-Fehlerbehebungsleitfaden für Version 4.1.3 und höher

Kapitel: Fehlerbehebung für HTTP AO

In diesem Artikel wird beschrieben, wie Sie eine Fehlerbehebung für HTTP AO durchführen.

Inh

Ha

An

Da

Vo

Op

Pro

Fel

Ha

Fel

vW

Fel

Fel

Inhalt

- [1 Fehlerbehebung für HTTP Accelerator](#)
 - [1,1 Anzeigen von HTTP-Statistiken](#)
 - [1,2 Anzeigen von HTTPS-Statistiken](#)
 - [1,3 Anzeigen des HTTP-Metadaten-Cache](#)
 - [1,4 Anzeigen des HTTPS-Metadaten-Cache](#)
 - [1,5 Cache-Steuerelement-Verhalten für Metadaten-Metadaten](#)
 - [1,6 Ausnahmen für das Zwischenspeichern von Metadaten](#)
- [2 HTTP AO-Protokollierung](#)

Fehlerbehebung für HTTP Accelerator

Der HTTP Accelerator optimiert HTTP- und HTTPS-Datenverkehr (ab Version 4.3.1) mithilfe der folgenden Techniken:

- **Wiederverwendung der TCP-Verbindung über das WAN.** Vermeidet einen Verbindungsaufbau für nachfolgende HTTP-Verbindungen, die vom gleichen Client angefordert werden. (Gilt nicht für HTTPS-Datenverkehr.)
- **Zwischenspeichern von HTTP-Metadaten.** Bestimmte HTTP-Antworten werden zusammen mit ihren URLs und Metadateninformationen zwischengespeichert, sodass die Edge-WAE lokal auf nachfolgende Anforderungen für dieselbe URL reagieren kann. (Nur in Version 4.2.1 und höher verfügbar.) Es gibt drei Arten von zwischengespeicherten Antworten:
 - 301 Dauerhaft umgeleitet
 - 304 Nicht geändert
 - 401 Autorisierung erforderlich
- **Zwischenspeichern von HTTPS-Metadaten** Bestimmte HTTPS-Antworten werden zusammen mit ihren URLs und Metadateninformationen zwischengespeichert, sodass die Edge-WAE auf nachfolgende Anforderungen für dieselbe URL lokal reagieren kann. (Nur in Version 4.3.1 und höher verfügbar.)
- **HTTP unterdrückt die Servercodierung.** Entfernt den Accept-Encoding-Header aus den HTTP- und HTTPS-Anforderungen, sodass der Server komprimierte Daten nicht an das WAN senden kann. Dadurch kann die WAE eine eigene Komprimierung anwenden, was in der Regel zu einem besseren Komprimierungsverhältnis führt. (Nur in Version 4.2.1 und höher verfügbar.)
- **DRE-Hinweise.** Stellt spezifische Hinweise für das DRE-Modul bereit, um den HTTP- und HTTPS-Datenverkehr basierend auf den zusätzlichen Informationen über das HTTP-Protokoll, das durch Analysieren der Layer-7-Payload bereitgestellt wird, besser zu komprimieren:
 - Header überspringen: Weist das DRE-Modul an, HTTP-/HTTPS-Header nicht zu komprimieren, was zu einer besseren Komprimierung des Objekts führt.
 - Flush: Weist das DRE-Modul an, mit der Komprimierung zu beginnen, sobald eine HTTP/HTTPS-Transaktion vollständig verarbeitet ist.
 - LZ überspringen: Weist das DRE-Modul an, keine LZ-Komprimierung auf alle Objekte anzuwenden, die bereits vom ursprünglichen Server komprimiert wurden, wodurch der CPU-Overhead verringert wird.

Die Features HTTP-Metadaten-Caching, Unterdrücken der Servercodierung und DRE-Hinweise können separat konfiguriert werden. Die Funktion zur Wiederverwendung von TCP-Verbindungen ist immer aktiv, wenn HTTP AO aktiviert ist, und gilt nur für HTTP-Datenverkehr.

Sie können die allgemeine AO-Konfiguration und den allgemeinen Status mit dem **Show Accelerator** überprüfen und **Lizenzbefehle anzeigen**, wie im Artikel [Problembehandlung bei Anwendungsbeschleunigung](#) beschrieben. Die Enterprise-Lizenz ist für den HTTP-Beschleunigungsvorgang erforderlich.

Überprüfen Sie anschließend den für HTTP AO spezifischen Status, indem Sie den Befehl **show accelerator http** verwenden, wie in Abbildung 1 gezeigt. Sie möchten sehen, dass HTTP AO aktiviert, ausgeführt und registriert ist und dass die Verbindungsbeschränkung angezeigt wird. Wenn der Config State (Konfigurationsstatus) aktiviert ist, der Operational State jedoch Shutdown lautet, weist dies auf ein Lizenzierungsproblem hin. Für jede der HTTP-Funktionen wird der aktuelle Modus (Benutzer/Standard) zusammen mit dem Wert (Aktiviert, Deaktiviert oder konfigurierter Wert) angezeigt. In Version 4.2.1 wurden die Elemente Suppress Server Encoding und MetadataCache hinzugefügt, und in Version 4.3.1 wurden die DRE-Hinweise und die HTTPS-Metadatenachelemente hinzugefügt.

Um HTTPS-Datenverkehr sowohl durch SSL- als auch durch HTTP-AOs zu optimieren, stellen Sie sicher, dass eine der folgenden optionalen Funktionen aktiviert ist: HTTPS-Metadatenzwischenspeicherung, Unterdrücken der Servercodierung oder DRE-Tipps.

Abbildung 1: Überprüfen des HTTP Accelerator-Status

Mit dem Befehl **show running-config** können Sie überprüfen, ob die HTTP-/HTTPS-Datenverkehrsrichtlinie ordnungsgemäß konfiguriert ist und welche der Funktionen aktiviert sind. Sie möchten **HTTP** für die Webanwendungsaktion **beschleunigen** und die entsprechenden Übereinstimmungsbedingungen für den HTTP-Klassifizierer wie folgt anzeigen:

```
WAE674# sh run | include HTTP

    accelerator http suppress-server-encoding enable          <----- in 4.2.1 and
later
    accelerator http metadataacache https enable            <----- in 4.3.1 and
later
    accelerator http dre-hints enable                       <----- in 4.3.1 and
later
                                                                at least one
of these must be enabled

    classifier HTTP
    classifier HTTPS
    name Web classifier HTTP action optimize full accelerate http <----- HTTP
acceleration
    name Web classifier HTTPS action optimize DRE no compression none <----- HTTPS static
policy applies to traffic not
                                                                matching any
SSL accelerated-services policy

WAE674# sh run | begin HTTP
...skipping
    classifier HTTP
```

```

match dst port eq 80
match dst port eq 8080
match dst port eq 8000
match dst port eq 8001
match dst port eq 3128

```

```
WAE674# sh run | begin HTTPS
```

```
...skipping
```

```
classifier HTTPS
```

```
match dst port eq 443
```

```
<----- add here any
```

```
nondefault HTTPS port
```

Anzeigen von HTTP-Statistiken

Verwenden Sie den Befehl **show statistics accelerator**, um die folgenden Statistiken anzuzeigen:

- Wie viel Zeit wird durch HTTP AO gespeichert? Sie können die Gesamtdauer der Zeitersparnis durch das gesamte HTTP-AO oder die von jedem der folgenden Features gesparte Zeit anzeigen:
 - Zeiteinsparung durch schnelle Wiederverwendung von Verbindungen
 - Durch die drei Metadaten-Caches gesparte Zeit
- Anzahl der Cache-Treffer/-Verluste für die Metadaten-Caches
- Anzahl der Fälle, in denen die Servercodierung auf HTTP-Anfragen angewendet wird
- Anzahl der Bereitstellungen von DRE-Hinweisen basierend auf dem Inhalt der HTTP-Header
- Anzahl der verarbeiteten HTTP-Transaktionen (Anfrage+Antwort)
- Anzahl der Fehler in der HTTP-Header-Verarbeitung
- Anzahl der Cache-erneuten Validierungen

```
WAE674# sh stat accel http
```

```
HTTP:
```

```
Global Statistics
```

```
-----
```

```

Time Accelerator was started: Tue Apr 6 06:04:06 2010
Time Statistics were Last Reset/Cleared: Tue Apr 6 06:04:06 2010
Total Handled Connections: 3743984
Total Optimized Connections: 3743984
Total Connections Handed-off with Compression Policies Unchanged: 0
Total Dropped Connections: 0
Current Active Connections: 48
Current Pending Connections: 0
Maximum Active Connections: 176
Total Time Saved (ms): 35584437 <-----Should be

```

```
incrementing
```

```

Current Active Connections Free For Fast Connection Use: 2
Total Connections Handed-off: 0
Total Connections Handed-off with Compression Policies Disabled: 0
Total Connections Handed-off to SSL: 0
Total Connection Hand-off Failures: 0
Total Fast Connection Successes: 3617244 <-----Should be

```

```
incrementing
```

```

Total Fast Connection Failures: 0
Maximum Fast Connections on a Single Connection: 100
Total CONNECT Requests with Incomplete Message: 0
Percentage of Connection Time Saved: 37
Total Round Trip Time For All Connections (ms): 4922767377
Total Fast Connections Initiated by Peer: 0

```

Total SYN Timeouts:	0	
Total Time for Metadata Cache Miss (ms):	2	<-----Output
from here is in 4.2.1 and later only		
RTT saved by Redirect Metadata Cache (ms):	5988	<-----Should be
incrementing		
RTT saved by Authorization Redirect Metadata Cache (ms):	345	<-----Should be
incrementing		
RTT saved by Content Refresh Check Metadata Cache (ms):	44987	<-----Should be
incrementing		
Total Time Saved by Fast Connection Use (ms):	456	
Total Locally Served Redirect Responses:	453	<-----Should be
incrementing		
Total Locally Served Unauthorized Responses:	56	<-----Should be
incrementing		
Total Locally Served Conditional Responses:	4932	<-----Should be
incrementing		
Total Remotely Served Redirect Responses:	0	
Total Remotely Served Unauthorized Responses:	0	
Total Remotely Served Conditional Responses:	1	
Total Requests with URL Longer than 255 Characters:	0	
Total Requests with HTTP Pipelining:	0	
Total Transactions Handled:	2	<-----Total
number of HTTP transactions processed		
Total Server Compression Suppression:	1	<-----Total
number of Accept-Encoding removed		
Total Requests Requiring Server Content-Revalidation:	0	
Total Responses not to be Cached:	0	
Total Connections Expecting Authentication:	0	
Total Connections with Unsupported HTTP Requests:	0	
Total Connections with Unsupported HTTP Responses:	0	
Total Hints Sent to DRE Layer to Flush Data:	2	
Total Hints Sent to DRE Layer to Skip LZ:	0	
Total Hints Sent to DRE Layer to Skip Header Information:	1	

Wenn der Zähler "Total Time Saved" (Gespeicherte Gesamtzeit) in der Ausgabe oben nicht inkrementiert oder relativ klein ist, weist er darauf hin, dass der HTTP-AO nicht viel Nutzen bietet. Wenn die von einem der drei Metadaten-Caches gesparte Gesamtzeit nicht inkrementiert oder relativ klein ist, weist dies darauf hin, dass der entsprechende Metadaten-cache keinen großen Vorteil bietet.

Der Zähler für die Unterdrückung von Gesamtserverkomprimierung gibt an, wie oft der Accept-Encoding-Header entfernt wurde, um eine bessere Komprimierung durch das WAE-Gerät zu ermöglichen. Die an die Zähler der DRE-Schichten gesendeten Total Hints geben an, wie oft die DRE-Tipps (Flush Data, Skip LZ, Skip Header) jeweils an das DRE-Modul ausgegeben wurden, um die Daten besser zu komprimieren.

Um ähnliche Informationen von der zentralen Verwaltungsschnittstelle in Version 4.2.1 und höher anzuzeigen, wählen Sie das WAE-Gerät aus, wählen Sie dann **Monitor > Acceleration > HTTP Acceleration Report** und wählen die Registerkarte Details, um die folgenden Diagramme anzuzeigen:

- Eingesparte HTTP-Reaktionszeit (schnelle Wiederverwendung, Umleitung, bedingte und nicht autorisierte Zwischenspeicherung von Verbindungen)
- HTTP-Optimierungsanzahl (Anzahl der angewendeten Optimierungen)
- HTTP-Optimierungstechniken (für alle HTTP-Optimierungen, einschließlich Metadaten-Caches, Wiederverwendung von Verbindungen, DRE-Hinweise und Unterdrückung der Servercodierung)

Wenn Sie Debuginformationen über die HTTP-Header-Analyse und Fehlerbedingungen anzeigen

möchten, verwenden Sie den Befehl **show statistics accelerator** (in 4.3.1 und höher), um Folgendes zu bestimmen:

- Anzahl der zwischengespeicherten 301, 304 und 401 Antworten
- Anzahl der HTTP-Header, Versionen und Methoden
- Gründe für das Nichtzwischen speichern von HTTP-Antworten
- Gesamtzahl der zwischengespeicherten HTTP-Antworten
- Gründe, warum HTTP-Anforderungen nicht aus dem lokalen Cache bereitgestellt werden

Verwenden Sie den Befehl **show statistics connection optimierte http**, um zu überprüfen, ob das WAAS-Gerät optimierte HTTP-Verbindungen herstellt. Stellen Sie sicher, dass in der Spalte Accel (Aktiv) ein "H" für HTTP-Verbindungen angezeigt wird. Dies bedeutet, dass HTTP AO wie folgt verwendet wurde:

```
WAE674# sh stat conn opt http
Current Active Optimized Flows:                2
  Current Active Optimized TCP Plus Flows:      2
  Current Active Optimized TCP Only Flows:      0
  Current Active Optimized TCP Preposition Flows: 0
Current Active Auto-Discovery Flows:           0
Current Active Pass-Through Flows:             0
Historical Flows:                             100
D:DRE,L:LZ,T:TCP Optimization,
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO
ConnID  Source IP:Port      Dest IP:Port      PeerID              Accel
5929    10.10.10.10:3446     10.10.100.100:80  00:14:5e:84:24:5f  THDL      <-----Look
for "H"
```

Sie können Verbindungsstatistiken für geschlossene Verbindungen überprüfen, indem Sie den Befehl **show statistics connection closed http** verwenden.

Um ähnliche Informationen über den Central Manager anzuzeigen, wählen Sie das WAE-Gerät aus, und wählen Sie dann **Monitor > Optimization > Connections Statistics** aus.

Abbildung 2: Verbindungsstatistikbericht mit HTTP

Im Verbindungsstatistiken-Bericht zeigt das Globalsymbol in der Spalte Angewandte Richtlinie, dass HTTP AO für eine Verbindung verwendet wurde. (Platzieren Sie den Cursor über einem Symbol, um dessen Bedeutung anzuzeigen.)

Sie können die HTTP-Verbindungsstatistiken anzeigen, indem Sie den Befehl **show statistics connection optimized http detail** verwenden. Suchen Sie in der Ausgabe nach dem Zähler "Fast Connections" (Schnelle Verbindungen). Ein positiver Wert für diesen Zähler bedeutet, dass die HTTP-AO Clients durch die Wiederverwendung persistenter Verbindungen Vorteile bringt, wodurch die Latenz verringert wird.

```
WAE674# show stat conn opt http detail
```

```
Connection Id:          1496
Peer Id:                00:14:5e:84:24:5f
Connection Type:       EXTERNAL CLIENT
Start Time:            Wed Jul 15 05:09:52 2009
Source IP Address:     10.10.10.10
Source Port Number:    1760
Destination IP Address: 10.10.100.100
Destination Port Number: 80
Application Name:      Web                <-----Should see Web
Classifier Name:       HTTP               <-----Should see HTTP
Map Name:              basic
Directed Mode:        FALSE
Preposition Flow:     FALSE
Policy Details:
  Configured:         TCP_OPTIMIZE + DRE + LZ
  Derived:            TCP_OPTIMIZE + DRE + LZ
  Peer:               TCP_OPTIMIZE + DRE + LZ
  Negotiated:         TCP_OPTIMIZE + DRE + LZ
  Applied:            TCP_OPTIMIZE + DRE + LZ
Accelerator Details:
  Configured:         HTTP                <-----Should see HTTP configured
  Derived:            HTTP
```

Applied: HTTP
Hist: None

<-----Should see HTTP applied

	Original	Optimized
Bytes Read:	266	139160
Bytes Written:	82686	128

. . .
HTTP : 1496

Time Statistics were Last Reset/Cleared: Wed Jul 15
05:09:52 2009

Total Bytes Read:	56367	3269
Total Bytes Written:	56367	3269
Total Bytes Buffered:	0	0
Total Internal Bytes Read:		92
Total Internal Bytes Written:		92
Bit Flags for I/O state:		1040
Internal object pointer:		2046823200

Fast connections: 11 <-----Reused
connections

. . .

Anzeigen von HTTPS-Statistiken

(Dieser Abschnitt gilt nur für Version 4.3.1 und höher.)

Verwenden Sie den Befehl **show statistics accelerator http https**, um die folgenden Statistiken anzuzeigen:

- Wie viel Zeit wird vom HTTP-Betriebssystem für HTTPS-Datenverkehr gespeichert? Sie können die Gesamtdauer der Zeitersparnis im gesamten HTTPS-Metadaten-Cache oder die von jedem der drei Metadaten-Caches gesparte Zeit sehen.
- Anzahl der Cache-Treffer/-Verluste für die Metadaten-Caches
- Anzahl der Fälle, in denen die Servercodierung auf HTTPS-Anforderungen angewendet wird
- Anzahl der Bereitstellungen von DRE-Hinweisen basierend auf dem Inhalt der HTTPS-Header
- Anzahl verarbeiteter HTTPS-Transaktionen (Anfrage+Antwort)
- Anzahl der Fehler in der HTTPS-Headerverarbeitung
- Anzahl der Cache-erneuten Validierungen

```
WAE674# sh stat accel http https
```

```
HTTPS Statistics
-----
Total Optimized HTTPS Connections: 10 <-----Should be
incrementing
Total Handled HTTPS Connections: 10 <-----Should be
incrementing
Total Active HTTPS Connections: 2
Total Proxy-Connect HTTPS Connections: 0
Total Proxy-Connect HTTPS Insert Failures: 0
RTT saved by HTTPS Content Refresh Check Metadata Cache - (ms): 44 <-----Should be
```

```

incrementing
RTT saved by HTTPS Redirect Metadata Cache - (ms):          10    <-----Should be
incrementing
RTT saved by HTTPS Authorization Required Metadata Cache - (ms):  5    <-----Should be
incrementing
Total Locally Served HTTPS Conditional Responses:          44    <-----Should be
incrementing
Total Locally Served HTTPS Redirect Responses:              10    <-----Should be
incrementing
Total Locally Served HTTPS Unauthorized Responses:          5    <-----Should be
incrementing
Total Remotely Served HTTPS Conditional Responses:          32
Total Remotely Served HTTPS Redirect Responses:             2
Total Remotely Served HTTPS Unauthorized Responses:         1
Total Hints Sent to DRE Layer to Skip Header Information - HTTPS: 121
Total Hints Sent to DRE Layer to Flush Data - HTTPS:        121
Total Hints Sent to DRE Layer to Skip LZ - HTTPS:           0
Total Server Compression Suppression - HTTPS:               110
Total Time Saved from all HTTPS metadata cache hits:         59    <-----Should be
incrementing
Total Time HTTPS Cache Miss:                                4
Total HTTPS Requests Requiring Server Content-Revalidation: 32
Total HTTPS Responses not to be Cached:                     0
Total HTTPS Connections Bypassed due to URL Based Bypass List: 0
Total HTTPS Connections Bypassed due to IP Based Bypass List: 0

```

Wenn der Zähler "Total Time Saved" (Gespeicherte Gesamtzeit) in der oben angegebenen Ausgabe nicht inkrementiert oder recht klein ist, weist er darauf hin, dass der HTTP-AO für den HTTPS-Datenverkehr nicht viel Vorteile bietet. Wenn die von einem der drei Metadaten-Caches gesparte Gesamtzeit nicht inkrementiert oder relativ klein ist, weist dies darauf hin, dass der entsprechende Metadaten-cache keinen großen Vorteil bietet.

Der Zähler für die vollständige Serverkomprimierung gibt an, wie oft der Accept-Encoding-Header von HTTPS-Anforderungen entfernt wurde, um eine bessere Komprimierung durch das WAE-Gerät zu ermöglichen. Die an die Zähler der DRE-Schichten gesendeten Total Hints geben an, wie oft die DRE-Tipps (Flush Data, Skip LZ, Skip Header) jeweils an das DRE-Modul ausgegeben wurden, um die Daten besser zu komprimieren.

Um ähnliche Informationen von der zentralen Verwaltungsschnittstelle in Version 4.3.1 und höher anzuzeigen, wählen Sie das WAE-Gerät aus, wählen Sie dann **Monitor > Acceleration > HTTPS Acceleration Report** und wählen die Registerkarte Details, um die folgenden Diagramme anzuzeigen:

- Eingesparte HTTPS-Reaktionszeit (Umleitung, bedingte und nicht autorisierte Zwischenspeicherung)
- HTTPS-Optimierungsanzahl (Anzahl der angewendeten Optimierungen)
- HTTPS-Optimierungstechniken (für alle HTTPS-Optimierungen, einschließlich Metadaten-Caches, DRE-Tipps und Unterdrückung der Servercodierung)

Um Debuginformationen über die HTTPS-Header-Analyse und Fehlerbedingungen anzuzeigen, verwenden Sie den Befehl **show statistics accelerator (http debug)**, um Folgendes zu bestimmen:

- Anzahl der zwischengespeicherten 301, 304 und 401 Antworten
- Anzahl der HTTP-Header, Versionen und Methoden
- Gründe für das Nichtzwischenspeichern von HTTP-Antworten
- Gesamtzahl der zwischengespeicherten HTTP-Antworten

- Gründe, warum HTTP-Anforderungen nicht aus dem lokalen Cache bereitgestellt werden

Verwenden Sie den Befehl **show statistics connection optimierte http**, um zu überprüfen, ob das WAAS-Gerät optimierte HTTPS-Verbindungen herstellt. Stellen Sie sicher, dass sowohl "H" als auch "S" in der Spalte "Accel" (Aktiv) für HTTPS-Verbindungen angezeigt werden. Dies bedeutet, dass sowohl die HTTP- als auch die SSL-AOs wie folgt verwendet wurden:

```
WAE674# sh stat conn opt http
Current Active Optimized Flows:                2
  Current Active Optimized TCP Plus Flows:      2
  Current Active Optimized TCP Only Flows:      0
  Current Active Optimized TCP Preposition Flows: 0
Current Active Auto-Discovery Flows:            0
Current Active Pass-Through Flows:              0
Historical Flows:                              100
D:DRE,L:LZ,T:TCP Optimization,
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO
ConnID   Source IP:Port      Dest IP:Port      PeerID              Accel
5929     10.10.10.10:3446      10.10.100.100:80  00:14:5e:84:24:5f  THSDL              <-----Lock
for "H" and "S"
```

Sie können Verbindungsstatistiken für geschlossene Verbindungen überprüfen, indem Sie die Befehle **show statistics connection closed** oder **show statistics connection closed ssl** verwenden.

Um ähnliche Informationen über den Central Manager anzuzeigen, wählen Sie das WAE-Gerät aus, und wählen Sie dann **Monitor > Optimization > Connections Statistics** aus.

Abbildung 3: Verbindungsstatistik-Bericht mit HTTP und SSL

Im Connection Statistics-Bericht zeigt das Globussymbol in der Spalte Applied Policy (Angewandte Richtlinie), dass HTTP AO für eine Verbindung verwendet wurde, und das Lock-Symbol zeigt an, dass SSL AO angewendet wurde. (Platzieren Sie den Cursor über einem Symbol, um dessen Bedeutung anzuzeigen.)

Sie können die HTTPS-Verbindungsstatistiken anzeigen, indem Sie die **für HTTP-Detailangaben optimierte Verbindung anzeigen** und **für die statistische Verbindung optimierte SSL Detail-Befehle anzeigen**.

```
WAE674# show stat conn opt http detail
```

```

Connection Id:          34
Peer Id:                00:14:5e:cd:9c:c9
Connection Type:       EXTERNAL CLIENT
Start Time:            Thu Oct 28 14:47:56 2010
Source IP Address:     10.3.2.1
Source Port Number:    40829
Destination IP Address: 110.1.1.100
Destination Port Number: 443
Application Name:      SSL <-----Should see SSL
Classifier Name:       HTTPS <-----Should see HTTPS
Map Name:              basic
Directed Mode:         FALSE
Preposition Flow:      FALSE
Policy Details:
    Configured:         TCP_OPTIMIZE
    Derived:           TCP_OPTIMIZE
    Peer:              TCP_OPTIMIZE
    Negotiated:        TCP_OPTIMIZE + DRE + LZ
    Applied:           TCP_OPTIMIZE + DRE + LZ
Accelerator Details:
    Configured:        None
    Derived:          None
    Applied:          HTTP,SSL <-----Should see HTTP and SSL applied
    Hist:             None

```

	Original	Optimized
Bytes Read:	5162	21874
Bytes Written:	1977819	5108

Total Reduction Ratio: 98.639%

HTTP : 34

```

Time Statistics were Last Reset/Cleared: Thu Oct 28
14:47:56 2010
Total Bytes Read: 4620
1972570
Total Bytes Written: 4620
1972570
. . .

```

SSL : 34

```

Time Statistics were Last Reset/Cleared: Thu Oct 28
14:47:56 2010
Total Bytes Read: 0
0
Total Bytes Written: 0
0
. . .

```

```

Hostname in HTTP CONNECT: <----- the last three counters
apply only to
IP Address in HTTP CONNECT: Proxy Connect type of
HTTPS connections
TCP Port in HTTP CONNECT:

```

Anzeigen des HTTP-Metadaten-Cache

Um den Inhalt der drei HTTP-Metadaten-Caches anzuzeigen (umleiten, bedingt und nicht autorisiert), verwenden Sie den Befehl **show cache http-Metadaten**. Nur der vollständige URL und der Ablauf (in Sekunden) werden angezeigt. Sie können den Inhalt jedes der drei Caches auch separat anzeigen, indem Sie die folgenden Befehle verwenden:

- **show cache HTTP-Metadacache Redirect-Response**
- **show cache http-Metadacache bedingt-response**
- **show cache http-Metadacache unauthorized-response**

Die typische Ausgabe der obigen Befehle lautet wie folgt:

Redirect Cache

Active entries: 1, Max Entries: 1500

URL: www.abcnews.com/, Expiration (sec): 3206

Conditional Cache

Active entries: 6, Max Entries: 10500

URL: www.cisco.com/web/fw/i/quicklinks-rnd-corners.gif, Expiration (sec): 3594

URL: www.cisco.com/web/fw/i/hp-sprites.gif, Expiration (sec): 3594

URL: www.cisco.com/en/US/home/images/ba-actsGreen-logo.jpg, Expiration (sec): 3594

URL: www.cisco.com/en/US/home/images/fp-eos3.jpg, Expiration (sec): 3594

URL: www.cisco.com/en/US/home/images/fp-AP541n.jpg, Expiration (sec): 3594

URL: www.cisco.com/web/fw/c/home.min.css, Expiration (sec): 3592

Unauthorized Cache

Active entries: 1, Max Entries: 3000

URL: l.yimg.com/index.html, Expiration (sec): 86393

Sie können den Inhalt der drei Caches mit dem Befehl **clear cache http-Metadacache löschen**.

Wenn Sie den Inhalt jedes Cache separat löschen möchten, können Sie die folgenden Befehle verwenden:

- **Clear Cache HTTP-Metadacache Redirect-Response**
- **Clear Cache http-Metadacache bedingte Reaktion**
- **Löschen des Cache HTTP-MetadatenUnauthorized-response**

Wenn Sie eine URL angeben möchten, die gelöscht werden soll, können Sie den folgenden Befehl verwenden:

HTTP-Metadaten-Cache löschen {all|redirect|Conditional|unauthorized}-URL

Anzeigen des HTTPS-Metadaten-Cache

Um die Anzahl der Einträge in den drei HTTPS-Metadaten-Caches (Umleitung, bedingt und nicht autorisiert) anzuzeigen, verwenden Sie den Befehl **show cache http-metadacache https**. Im Gegensatz zum entsprechenden Befehl für den HTTP-Metadaten-Cache werden der URL und die Ablaufzeit nicht angezeigt. Mithilfe der folgenden Befehle können Sie auch die Anzahl der Einträge für jeden der drei Caches einzeln anzeigen:

- **show cache HTTP-Metadacache HTTPS Redirect-Response**
- **show cache http-Metadacache https bedingt-response**
- **show cache http-Metadacache https unauthorized-response**

Die typische Ausgabe der obigen Befehle lautet wie folgt:

```
HTTPS Redirect Cache
Active HTTP entries: 0, Active HTTPS entries: 0 Max Entries: 3250
HTTPS Conditional Cache
Active HTTP entries: 0, Active HTTPS entries: 11 Max Entries: 22750
HTTPS Unauthorized Cache
Active HTTP entries: 0, Active HTTPS entries: 0 Max Entries: 6500
```

Sie können den Inhalt der drei Caches mit dem Befehl **clear cache http-metadacache https** löschen.

Wenn Sie den Inhalt jedes Cache separat löschen möchten, können Sie die folgenden Befehle verwenden:

- **Clear Cache HTTP-Metadacache HTTPS Redirect-Response**
- **Clear Cache HTTP-Metadacache HTTPS Conditional-Response**
- **Löschen des Cache HTTP-MetadatenCache HTTPS Unauthorized-response**

Cache-Steuererelement-Verhalten für Metadaten-Metadaten

Bei HTTP- und HTTPS-Antworten (in Version 4.3.1) werden alle Cache-Control-Direktiven (Cache-Control: no-cache, no-store, private, must-revalidate, proxy-revalidate, max-age=0, Pragma: no-cache). Es gibt eine Option, solche Cache-Control-Prüfungen zu deaktivieren. Dies bedeutet, dass alle 304 Antworten mit Cache-Control-Headern, die keine Zwischenspeicherung angeben, zwischengespeichert werden und alle Anforderungen mit Cache-Control-Headern, die die Nicht-Zwischenspeicherung angeben, aus dem lokalen Cache bereitgestellt werden können.

Wenn Sie sich darüber im Klaren sind, dass die Deaktivierung der Cache-Steuerungsprüfungen die Vorteile des Metadaten-Cache erhöhen kann, da einige Browser oder Webserver möglicherweise über eine Standardoption verfügen, in allen Antworten einen Cache-Steuererelementheader aufzunehmen, um die erneute Validierung des Objekts über den ursprünglichen Server zu erzwingen. Dies würde den Metadaten-Cache für 304 Antworten ineffektiv machen.

Die Option kann unabhängig für HTTP/S-Anforderungen (Cache-Lookups) und -Antworten (Cache-Einfügungen) gesteuert werden.

Verwenden Sie den folgenden Befehl, um die Cache-Kontrollprüfungen für HTTP/S 304-Anforderungen zu deaktivieren:

```
WAE#accelerator http metadacache request-ignore-no-cache enable
```

Dieser Befehl erzwingt, dass die Metadaten alle Cache-Control-Direktiven in HTTP/S 304-Anforderungen ignorieren. (Die Standardform [no] dieses Befehls zwingt die Metadaten, alle Cache-Control-Direktiven in HTTP/S 304-Anforderungen zu berücksichtigen.)

Um die Cache-Steuerungsprüfungen für HTTP/S 304-Antworten zu deaktivieren, verwenden Sie den folgenden Befehl:

```
WAE#accelerator http metadacache response-ignore-no-cache enable
```

Dieser Befehl zwingt die Metadaten, alle Cache-Control-Direktiven in HTTP/S 304-Antworten zu ignorieren. (Die Standardform [no] dieses Befehls zwingt die Metadaten, alle Cache-Control-Direktiven in HTTP/S 304-Antworten zu berücksichtigen.)

Der Metadaten-Cache berücksichtigt Cache-Control-Header für 301- und 401-Antworten. Wenn die Antwort einen der Cache-Control-Header (no-cache, no-store, private, must-revalidate, proxy-revalidate, max-age=0, Pragma: no-cache), wird er nicht zwischengespeichert.

Ausnahmen für das Zwischenspeichern von Metadaten

Es gibt einige Ausnahmen für das, was zwischengespeichert wird. Die Cacheeinfügung oder -suche tritt nicht auf, wenn die HTTP-AO eine der folgenden Bedingungen auf der verarbeiteten HTTP/S-Anforderung/Antwort erkennt:

- RFC-Beschwerde-Anfragen und -Antworten: Fehlgeformte/ungültige Header, wiederholte Header, fehlende Header, unerwarteter Text, unerwartete Chunkodierung
- Die URL-Größe beträgt mehr als 255 Zeichen.
- HTTP-Pipeline-Transaktionen
- WebDav-Methoden
- HEAD-Methode
- 301/401-Antworten mit Cookie-Headern
- 301 Antworten mit einer Gesamtlänge des Headers von mehr als 768 Byte
- 401 Antworten mit einer Headerlänge von mehr als 384 Byte
- 401 Antworten mit geteiltem Körper
- 401 Antworten mit nicht unterstützter Authentifizierungsmethode (unterstützte Methoden sind: Basic, NTLM, Negotiate, Kerberos, Digest, Oauth)
- Partieller HTTP-Header (Header Split) zur Verarbeitung verfügbar

HTTP AO-Protokollierung

Die folgenden Protokolldateien sind zur Behebung von HTTP-AO-Problemen verfügbar:

- Transaktionsprotokolldateien: /local1/logs/tfo/working.log (und /local1/logs/tfo/tfo_log_*.txt)
- Debugging-Protokolldateien: /local1/errorlog/httpao-errorlog.current (und httpao-errorlog.*)

Um das Debuggen zu vereinfachen, sollten Sie zunächst eine ACL einrichten, um Pakete auf einen Host zu beschränken.

```
WAE674(config)# ip access-list extended 150 permit tcp host 10.10.10.10 any
WAE674(config)# ip access-list extended 150 permit tcp any host 10.10.10.10
```

Um die Transaktionsprotokollierung zu aktivieren, verwenden Sie den Konfigurationsbefehl **transaction-logs** wie folgt:

```
wae(config)# transaction-logs flow enable
wae(config)# transaction-logs flow access-list 150
```

Sie können das Ende einer Transaktionsprotokolldatei anzeigen, indem Sie den Befehl **type-tail** wie folgt verwenden:

```

wae# type-tail tfo_log_10.10.11.230_20090715_130000.txt
Wed Jul 15 13:37:00 2009 :1529 :10.10.10.10 :2004 :10.10.100.100 :80 :OT :END :EXTERNAL
CLIENT :(HTTP) :0 :0 :107 :117
Wed Jul 15 13:37:00 2009 :1529 :10.10.10.10 :1880 :10.10.100.100 :80 :SODRE :END
:14357 :8406 :2181 :2761 :0
Wed Jul 15 13:38:19 2009 :1533 :10.10.10.10 :2008 :10.10.100.101 :135 :OT :START :EXTERNAL
CLIENT :00.14.5e.84.24.5f :basic
:Other :MS-EndPointMapper :F :(TFO) (TFO) (TFO) (TFO) (TFO) :<None> :(EPM) (EPM)
(EPM) :<None> :<None> :0 :120
Wed Jul 15 13:38:19 2009 :1534 :10.10.10.10 :2009 :10.10.100.101 :1025 :OT :START :EXTERNAL
CLIENT :00.14.5e.84.24.5f
:uuide3514235-4b06-11d1-ab04-00c04fc2dcd2

```

Verwenden Sie die folgenden Befehle, um die Debug-Protokollierung des HTTP-AO einzurichten und zu aktivieren.

HINWEIS: Die Debug-Protokollierung ist CPU-intensiv und kann eine große Menge an Ausgabe generieren. Verwenden Sie sie sorgfältig und sparsam in einer Produktionsumgebung.

Sie können die detaillierte Protokollierung auf dem Datenträger aktivieren:

```

WAE674(config)# logging disk enable
WAE674(config)# logging disk priority detail

```

Sie können die Debug-Protokollierung für Verbindungen in der ACL aktivieren:

```

WAE674# debug connection access-list 150

```

Die Optionen für HTTP-AO-Debugging (ab 4.2.1) sind wie folgt:

```

WAE674# debug accelerator http ?
all                enable all HTTP accelerator debugs
bypass-list        enable HTTP bypass-list debugs
cli                enable HTTP CLI debugs
conditional-response enable HTTP metadatatocache conditional (304) response
                   debugs
connection         enable HTTP connection debugs
dre-hints          enable HTTP dre-hints debugs
metadatatocache   enable HTTP metadatatocache debugs
prefetch          enable HTTP prefetch debugs
redirect-response  enable HTTP metadatatocache redirect (301) response
                   debugs
shell              enable HTTP shell debugs
suppress-server-encoding enable HTTP suppress-server-encoding debugs
transaction        enable HTTP transaction debugs
unauthorized-response enable HTTP auth-optimization debugs bugs

```

Sie können die Debug-Protokollierung für HTTP-Verbindungen aktivieren und dann das Ende des Debug-Fehlerprotokolls wie folgt anzeigen:

```

WAE674# debug accelerator http connection
WAE674# type-tail errorlog/httpao-errorlog.current follow

```