WAAS - SSL AO故障排除

章節：排除SSL AO故障

本文描述如何對SSL AO進行故障排除。

目錄

SSL加速器概述

SSL加速器（在4.1.3及更高版本中提供）可最佳化加密的安全套接字層(SSL)和傳輸層安全(TLS)流量。SSL加速器在WAAS內提供流量加密和解密，以實現端到端流量最佳化。SSL加速器還提供對加密證書和金鑰的安全管理。

在WAAS網路中，資料中心WAE充當客戶端SSL請求的可信中間節點。私鑰和伺服器證書儲存在資料中心WAE上。資料中心WAE參與SSL握手來派生會話金鑰，該會話金鑰在帶內安全地分發到分支WAE，允許分支WAE解密客戶端流量、最佳化流量、重新加密流量並通過WAN將其傳送到資料中心WAE。資料中心WAE與源伺服器保持單獨的SSL會話。

以下服務與SSL/TLS最佳化相關：

- 加速服務 — 描述要應用於SSL伺服器或一組伺服器的加速特性的配置實體。指定要用作受信任中介軟體的證書和私鑰、要使用的密碼、允許的SSL版本以及證書驗證設定。
- 對等服務 — 描述分支機構與資料中心WAE之間的帶內SSL連線要應用的加速特性的配置實體。此服務用於將會話金鑰資訊從資料中心傳輸到分支WAE，以最佳化SSL連線。
- Central Manager Admin Service — 不直接由SSL加速器使用，但由管理員用於SSL加速服務的配置管理。還用於上傳將在SSL加速服務中使用的證書和私鑰。
- Central Manager Management Service — 不直接由SSL加速器使用，但用於應用程式加速器裝置與Central Manager之間的通訊。此服務用於配置管理、安全儲存加密金鑰檢索和裝置狀態更新。

Central Manager安全儲存對於SSL AO的運行至關重要，因為它儲存了所有WAE的安全加密金鑰。每次重新載入Central Manager後，管理員需要通過使用**cms secure-store open**命令提供密碼來重新開啟安全儲存。每當WAE重新啟動時，WAE都會自動從中央管理器檢索其安全儲存加密金鑰，因此重新載入後無需在WAE上執行任何操作。

如果客戶端使用HTTP代理解決方案，則初始連線由HTTP AO處理，HTTP AO將其識別為到埠443的SSL隧道請求。HTTP AO查詢在資料中心WAE上定義的匹配SSL加速服務，當找到匹配時，將斷開與SSL AO的連線。但是，HTTP AO傳遞給HTTPS代理的SSL AO的流量將報告為Web應用程式統計資訊的一部分，而不是SSL應用程式中。如果HTTP AO找不到相符專案，則系統會根據靜態HTTPS(SSL)策略配置對連線進行最佳化。

SSL AO可以使用自簽名證書而不是CA簽名證書，這有助於部署概念驗證(POC)系統並排除SSL問題。通過使用自簽名證書，您可以快速部署WAAS系統，而無需匯入源伺服器證書，並且您可以消除證書作為潛在的問題源。建立SSL加速服務時，可以在中央管理器中配置自簽名證書。但是，當您使用自簽名證書時，客戶端瀏覽器將顯示一個安全警報，指出該證書不可信（因為它不是由已知的CA簽名的）。 要避免此安全警告，請在客戶端瀏覽器上的受信任的根憑證授權機構儲存中安裝證書。(在Internet Explorer上的安全警告上，按一下**View Certificate**，然後在「Certificate」對話方塊上按一下**Install Certificate**，然後完成「Certificate Import Wizard」。)

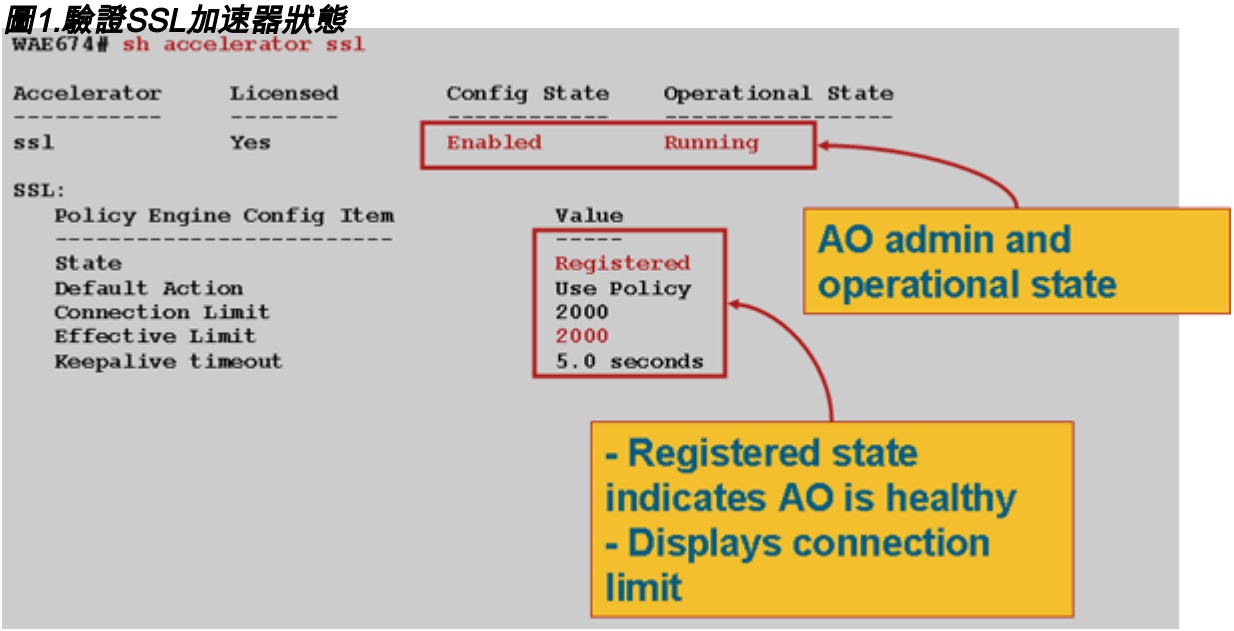
配置SSL管理服務是可選的，允許您將Central Manager通訊使用的SSL版本和密碼清單更改為WAE和瀏覽器（用於管理訪問）。 如果配置瀏覽器不支援的密碼，您將失去與中央管理器的連線。在這種情況下，請使用CLI中的**crypto ssl management-service**配置命令將SSL管理服務設定重新設定為預設值。

排除SSL AO故障

您可以使用**show accelerator**和**show license**命令驗證常規AO配置和狀態，如應用程式加速故障排除一文中所述。SSL加速器操作需要企業許可證。

接下來，使用**show accelerator ssl**命令驗證資料中心和分支WAE上SSL AO的特定狀態，如圖1所示。您想看到SSL AO已啟用、正在運行且已註冊，並且顯示連線限制。如果Config State為Enabled，但Operational State為Shutdown，則表示存在許可問題。如果Operational State（操作狀態）為Disabled（禁用），可能是因為WAE無法從Central Manager安全儲存檢索SSL金鑰，原因可能是安全儲存未開啟或無法訪問Central Manager。使用**show cms info**和**ping**命令確認中心管理器可訪問。

圖1.驗證SSL加速器狀態



如果看到的是Gen Crypto Params的操作狀態，請等待狀態變為Running，這可能需要在重新啟動後幾分鐘時間。如果從CM中檢索金鑰的狀態超過幾分鐘，則可能表示中央Manager上的CMS服務沒有運行、沒有到中央Manager的網路連線、WAE和中央Manager上的WAAS版本不相容，或者中央Manager安全儲存沒有開啟。

您可以使用**show cms secure-store**命令驗證是否已初始化並開啟Central Manager安全儲存，如下所示：

```
cm# show cms secure-store
secure-store is initialized and open.
```

如果安全儲存未初始化或開啟，您將看到諸如mstore_key_failure和secure-store等嚴重警報。您可以使用**cms secure-store open**命令開啟安全儲存，或從中央管理器中選擇**Admin > Secure Store**。

提示：記錄安全儲存密碼，以避免如果您忘記密碼，則必須重置安全儲存。

如果WAE上的磁碟加密出現問題，也會阻止SSL AO運行。使用**show disk details**命令驗證是否已啟用磁碟加密，並檢查是否已裝入CONTENT和SPOOL分割槽。如果裝載了這些分割槽，則表示已成功從中央管理器中檢索磁碟加密金鑰，並且可以從磁碟中寫入和讀取加密資料。如果**show disk details**命令顯示「System is initializing」，表示尚未從Central Manager中檢索加密金鑰，並且尚未裝載磁碟。在此狀態下，WAE不會提供加速服務。如果WAE無法從Central Manager中檢索磁碟加密金鑰，將發出警報。

您可以驗證在資料中心WAE上是否配置了SSL加速服務且其狀態為「已啟用」(在中央管理器中，選擇裝置，然後選擇**Configure > Acceleration > SSL Accelerated Services**)。由於以下情況，配置和啟用的加速服務可能會被SSL加速器變為非活動狀態：

- 加速服務中配置的證書已從WAE中刪除。使用**show running-config**命令確定加速服務中使用的證書，然後使用**show crypto certificates**和**show crypto certificate-details**命令確認證書存在安全儲存。如果缺少證書，請重新匯入證書。
- 加速服務證書已過期。使用**show crypto certificates**和**show crypto certificate-details**命令檢查證書到期日期。
- 加速服務證書的有效日期從未來開始。使用**show crypto certificates**和**show crypto certificate-details**命令並檢查命令輸出的有效性部分。此外，請確保WAE時鐘和時區資訊準確。

您可以驗證SSL連線是否應用了正確的策略，即它們已使用SSL加速進行了完全最佳化，如圖2所示

。在中央管理器中，選擇WAE裝置，然後選擇**Monitor > Optimization > Connections Statistics**。

圖2.檢驗SSL連線上的正確策略

使用**show running-config**命令以驗證HTTPS流量策略是否配置正確。您想檢視**SSL應用程式操作的optimize DRE no compression none**，並且希望檢視HTTPS分類器列出的相應匹配條件，如下所示：

```
WAE674# sh run | include HTTPS
   classifier HTTPS
      name SSL classifier HTTPS action optimize DRE no compression none              <---------
----

WAE674# sh run | begin HTTPS

...skipping
   classifier HTTPS
      match dst port eq 443                                                          <---------
----
   exit
```

活動加速服務插入與加速服務中配置的伺服器IP:port、伺服器名稱：port或伺服器域：port對應的動態策略。可以使用**show policy-engine application dynamic**命令檢查這些策略。每個顯示的策略中的Dst欄位指示匹配加速服務的伺服器IP和埠。對於萬用字元域(例如，server-domain *.webex.com port 443),Dst欄位將為「Any:443」。 對於伺服器名稱配置，在啟用加速服務時執行轉發DNS查詢，DNS響應中返回的所有IP地址將插入策略引擎。此命令可用於捕獲加速服務標籤為「inservice」但因其他某個錯誤而使加速服務變為非活動狀態的情況。例如，所有加速服務都依賴於對等服務，如果對等服務因缺少/刪除證書而處於非活動狀態，則加速服務也將標籤為非活動狀態，儘管在show running-config輸出中該服務看起來是「inservice」。您可以使用**show policy-engine application dynamic**命令驗證資料中心WAE上的SSL動態策略是否處於活動狀態。您可以使用**show crypto ssl services host-service peering**命令驗證對等服務狀態。

SSL AO加速服務配置可以有四種型別的伺服器條目：

- 靜態IP（伺服器IP） — 4.1.3版及更高版本中提供
- 全部捕獲(server-ip any) — 在4.1.7及更高版本中提供
- 主機名(server-name) — 在4.2.1及更高版本中可用
- Wildcard domain(server-domain)- 4.2.1及更高版本中提供

SSL AO收到連線後，會決定應該使用哪個加速服務進行最佳化。靜態IP配置具有最高的優先順序

，其次是伺服器名稱、伺服器域，然後是伺服器ip any。如果所有已配置和啟用的加速服務均不與連線的伺服器IP匹配，則連線會被下推到通用AO。通過SSL AO插入到策略引擎中的cookie用於確定針對特定連線匹配的加速服務和伺服器條目的型別。此策略引擎cookie是一個32位數字，僅對SSL AO有意義。較高的位用於表示不同的伺服器條目型別，較低的位表示加速服務索引，如下所示：

SSL策略引擎Cookie值

Cookie值	伺服器條目型別	意見
0x8*xxxxxx* *x*	伺服器IP地址	靜態IP地址配置
0x4*xxxxxx* *x*	伺服器主機名	資料中心WAE對主機名執行轉發DNS查詢，並將返回的IP地址新增到動態策略
0x2FFFFF	伺服器域名	資料中心WAE對目標主機IP地址執行反向DNS查詢，以確定它是否與域匹配。
0x1*xxxxxx* *x*	任意伺服器	所有SSL連線都使用此加速服務配置進行加速

範例 1：通過伺服器 — ip配置加速服務：

```
WAE(config)#crypto ssl services accelerated-service asvc-ip
WAE(config-ssl-accelerated)#description "Server IP acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-ip 171.70.150.5 port 443
WAE(config-ssl-accelerated)#inservice
```

新增相應的策略引擎條目如下：

```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
  Number:     1   Type: Any->Host (6)  User Id: SSL (4)           <----------------
    Src: ANY:ANY  Dst: 171.70.150.5:443                          <----------------
    Map Name: basic
    Flags: SSL
    Seconds: 0  Remaining: - NA -  DM Index: 32764
    Hits: 25  Flows: - NA -  Cookie: 0x80000001                  <----------------
```

範例 2：使用server-name配置的加速服務：

通過此配置，可以輕鬆部署最佳化企業SSL應用。它可以適應DNS配置更改並減少IT管理任務。

```
WAE(config)#crypto ssl services accelerated-service asvc-name
WAE(config-ssl-accelerated)#description "Server name acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-name www.google.com port 443
```

```
WAE(config-ssl-accelerated)#inservice
```

新增相應的策略引擎條目如下：

```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
 Number:     1   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: 74.125.19.104:443                           <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32762
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
 Number:     2   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: 74.125.19.147:443                           <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32763
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
 Number:     3   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: 74.125.19.103:443                           <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32764
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
 Number:     4   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: 74.125.19.99:443                            <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32765
   Hits: 0  Flows: - NA -  Cookie: 0x40000002                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
```

範例 3:通過伺服器域配置加速服務：

此配置允許WAAS裝置配置單個萬用字元域，從而無需瞭解所有伺服器的IP地址。資料中心WAE使用反向DNS(rDNS)來匹配屬於已配置域的流量。配置萬用字元域可避免配置多個IP地址，使解決方案可擴展並適用於SaaS架構。

```
WAE(config)#crypto ssl services accelerated-service asvc-domain
WAE(config-ssl-accelerated)#description "Server domain acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-name *.webex.com port 443
WAE(config-ssl-accelerated)#inservice
```

新增相應的策略引擎條目如下：

```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
 Number:     1   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: ANY:443                                     <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32762
   Hits: 0  Flows: - NA -  Cookie: 0x2FFFFFFF                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
```

範例 4:使用server-ip任意配置的加速服務：

此組態提供全面擷取機制。server-ip any port 443的加速服務處於活動狀態時，它允許埠443上的所有連線都通過SSL AO進行最佳化。此配置可在POC期間用於最佳化特定埠上的所有流量。

```
WAE(config)#crypto ssl services accelerated-service asvc-ipany
WAE(config-ssl-accelerated)#description "Server ipany acceleration"
WAE(config-ssl-accelerated)#server-cert-key server.p12
WAE(config-ssl-accelerated)#server-ip any port 443
WAE(config-ssl-accelerated)#inservice
```

新增相應的策略引擎條目如下：

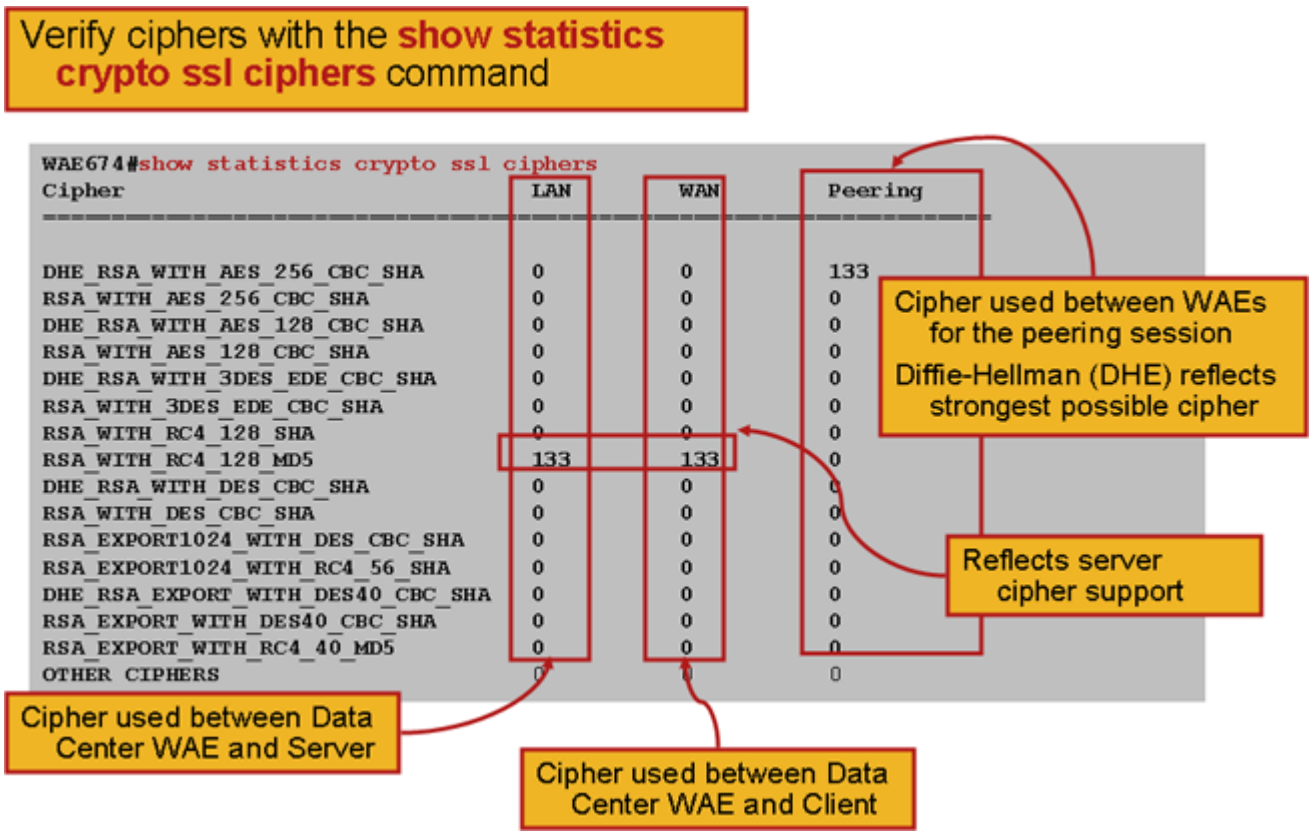
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< snip >

Individual Dynamic Match Information:
 Number:     1   Type: Any->Host (6)  User Id: SSL (4)            <----------------
   Src: ANY:ANY  Dst: ANY:443                                     <----------------
   Map Name: basic
   Flags: SSL
   Seconds: 0  Remaining: - NA -  DM Index: 32762
   Hits: 0  Flows: - NA -  Cookie: 0x10000004                     <----------------
   DM Ref Index: - NA -  DM Ref Cnt: 0
```

您可以驗證正在與show statistics crypto ssl ciphers命令一起使用的密碼，如圖3所示。

圖3.驗證密碼



您可以驗證這些密碼是否與源伺服器上配置的密碼匹配。**附註**：Microsoft IIS伺服器不支援包含DHE的密碼。

在Apache伺服器上，您可以在httpd.conf檔案中驗證SSL版本和密碼詳細資訊。這些欄位也可能位於從httpd.conf引用的單獨檔案(sslmod.conf)中。按如下方式查詢SSLProtocol和SSLCipherSuite欄位：

```
SSLProtocol -all +TLSv1 +SSLv3
SSLCipherSuite HIGH:MEDIUM:!aNULL:+SHA1:+MD5:+HIGH:+MEDIUM
. . .
SSLCertificateFile /etc/httpd/ssl/server.crt
SSLCertificateKeyFile /etc/httpd/ssl/server.key
```

要驗證Apache伺服器上的證書頒發者，請使用openssl命令按如下方式讀取證書：

```
> openssl x509 -in cert.pem -noout -issuer -issuer_hash
issuer= / C=US/ST=California/L=San
Jose/O=CISCO/CN=tools.cisco.com/emailAddress=webmaster@cisco.com be7cee67
```

在瀏覽器中，可以檢視證書及其詳細資訊以確定證書鏈、版本、加密金鑰型別、頒發者公用名(CN)以及主題/站點CN。在Internet Explorer中，按一下掛鎖圖示，按一下**檢視證書**，然後檢視詳細資訊和證書路徑頁籤以獲取此資訊。

大多數瀏覽器要求客戶端證書採用PKCS12格式，而不是X509 PEM格式。要將X509 PEM格式匯出為PKCS12格式，請在Apache伺服器上按如下所示使用openssl命令：

```
> openssl pkcs12 -export -in cert.pem -inkey key.pem -out cred.p12
Enter Export Password:
Verifying - Enter Export Password:
```

如果私鑰已加密，則需要使用密碼才能匯出。匯出密碼再次用於將憑證匯入到WAAS裝置。

使用**show statistics accelerator ssl**命令檢視SSL AO統計資訊。

```
WAE7326# show statistics accelerator ssl
SSL:

  Global Statistics
  -----------------
  Time Accelerator was started:                       Mon Nov 10     15:28:47 2008
  Time Statistics were Last Reset/Cleared:            Mon Nov 10    15:28:47 2008
  Total Handled Connections:                                          17                <-------
---------
  Total Optimized Connections:                                        17                <-------
---------
  Total Connections Handed-off with Compression Policies Unchanged:   0                 <-------
---------
  Total Dropped Connections:                                          0                 <-------
---------
  Current Active Connections:                                         0
  Current Pending Connections:                                        0
  Maximum Active Connections:                                         3
  Total LAN Bytes Read:                                               25277124          <-------
---------
  Total Reads on LAN:                                                 5798              <-------
---------
  Total LAN Bytes Written:                                            6398              <-------
---------
  Total Writes on LAN:                                                51                <-------
---------
  Total WAN Bytes Read:                                               43989             <-------
---------
  Total Reads on WAN:                                                 2533              <-------
---------
  Total WAN Bytes Written:                                            10829055          <-------
---------
  Total Writes on WAN:                                                3072              <-------
---------
. . .
```

失敗的會話和證書驗證統計資訊對於故障排除很有用，並且使用**show statistics accelerator ssl**命令上的以下過濾器可以更輕鬆地檢索這些統計資訊：

```
WAE# show statistics accelerator ssl | inc Failed
  Total Failed Handshakes:                                    47
  Total Failed Certificate Verifications:                     28
  Failed certificate verifications due to invalid certificates:      28
  Failed Certificate Verifications based on OCSP Check:       0
  Failed Certificate Verifications (non OCSP):                28
  Total Failed Certificate Verifications due to Other Errors:         0
  Total Failed OCSP Requests:                                 0
  Total Failed OCSP Requests due to Other Errors:             0
  Total Failed OCSP Requests due to Connection Errors:        0
  Total Failed OCSP Requests due to Connection Timeouts:      0
  Total Failed OCSP Requests due to Insufficient Resources:           0
```

與DNS相關的統計資訊可用於排除伺服器名稱和萬用字元域配置故障。要檢索這些統計資訊，請使用**show statistics accelerator ssl**命令，如下所示：

```
WAE# show statistics accelerator ssl
 . . .
 Number of forward DNS lookups issued:                          18
 Number of forward DNS lookups failed:                          0
 Number of flows with matching host names:                      8
 Number of reverse DNS lookups issued:                          46
 Number of reverse DNS lookups failed:                          4
 Number of reverse DNS lookups cancelled:                       0
 Number of flows with matching domain names:                    40
 Number of flows with matching any IP rule:                     6
 . . .
 Pipe-through due to domain name mismatch:                      6
 . . .
```

與SSL重新握手相關的統計資訊對於故障排除非常有用，可以使用**show statistics accelerator ssl**命令上的以下過濾器進行檢索：

```
WAE# show statistics accelerator ssl | inc renegotiation
  Total renegotiations requested by server:                      0
  Total SSL renegotiations attempted:                            0
  Total number of failed renegotiations:                         0
  Flows dropped due to renegotiation timeout:                    0
```

使用**show statistics connection optimized ssl**命令檢查WAAS裝置是否正在建立最佳化的SSL連線。驗證連線的Accel列中是否顯示「TDLS」。「S」表示按如下方式使用SSL AO:

```
WAE674# sh stat conn opt ssl
Current Active Optimized Flows:                    3
   Current Active Optimized TCP Plus Flows:        3
   Current Active Optimized TCP Only Flows:        0
   Current Active Optimized TCP Preposition Flows: 1
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  Local IP:Port         Remote IP:Port        PeerID             Accelerator
342     10.56.94.101:3406    10.10.100.100:443     0:1a:64:d3:2f:b8   TDLS                <---
--Look for "S"
```

可以使用**show statistics connection closed ssl**命令檢查已關閉連線的連線統計資訊。

如果連線未最佳化，請檢查WCCP/PBR是否正確配置且工作正常，並檢查非對稱路由。

您可以使用**show statistics connection optimized ssl detail**命令檢視SSL連線統計資訊，其中將看到來自已配置SSL加速服務的動態策略。**附註**：已配置的策略僅是TFO最佳化，但已配置的SSL服務將應用完全最佳化。

```
WAE674# sh stat connection optimized ssl detail
Connection Id:            1633
   Peer Id:                  00:14:5e:84:24:5f
   Connection Type:          EXTERNAL CLIENT
   Start Time:               Wed Jul 15 06:35:48 2009
   Source IP Address:        10.10.10.10
```

```
   Source Port Number:       2199
   Destination IP Address:   10.10.100.100
   Destination Port Number:  443
   Application Name:         SSL
   Classifier Name:          HTTPS
   Map Name:                 basic
   Directed Mode:            FALSE
   Preposition Flow:         FALSE
   Policy Details:
          Configured:        TCP_OPTIMIZE                                    <------TFO only
is configured
             Derived:        TCP_OPTIMIZE + DRE + LZ
                Peer:        TCP_OPTIMIZE
           Negotiated:       TCP_OPTIMIZE + DRE + LZ
              Applied:       TCP_OPTIMIZE + DRE + LZ                         <------Full
optimization applied
   Accelerator Details:
               Configured:   None
                  Derived:   None
                  Applied:   SSL                                            <------SSL
acceleration applied
                     Hist:   None

                                        Original            Optimized
                                   -------------------- --------------------
   Bytes Read:                                   1318                  584
   Bytes Written:                                 208                 1950
. . .
```

稍後的輸出中，延伸型SSL作業階段層級詳細資訊顯示如下：

```
. . .
SSL : 1633

  Time Statistics were Last Reset/Cleared:                    Tue Jul 10 18:23:20 2009
  Total Bytes Read:                                           0          0
  Total Bytes Written:                                        0          0
  Memory address:                                             0x8117738
  LAN bytes read:                                             1318
  Number of reads on LAN fd:                                  4
  LAN bytes written out:                                      208
  Number of writes on LAN fd:                                 2
  WAN bytes read:                                             584
  Number of reads on WAN fd:                                  23
  WAN bytes written out:                                      1950
  Number of writes on WAN fd:                                 7
  LAN handshake bytes read:                                   1318
  LAN handshake bytes written out:                            208
  WAN handshake bytes read:                                   542
  WAN handshake bytes written out:                            1424
  AO bytes read:                                              0
  Number of reads on AO fd:                                   0
  AO bytes written out:                                       0
  Number of writes on AO fd:                                  0
  DRE bytes read:                                             10
  Number of reads on DRE fd:                                  1
  DRE bytes written out:                                      10
```

```
  Number of writes on DRE fd:                                    1
  Number of renegotiations requested by server:                  0
  Number of SSL renegotiations performed:                        0
  Flow state:                                                    0x00080000
  LAN work items:                                                1
  LAN conn state:                                                READ
  LAN SSL state:                                                 SSLOK (0x3)
  WAN work items:                                                0
  WAN conn state:                                                READ
  WAN SSL state:                                                 SSLOK (0x3)
  W2W work items:                                                1
  W2W conn state:                                                READ
  W2W SSL state:                                                 SSLOK (0x3)
  AO  work items:                                                1
  AO  conn state:                                                READ
  DRE work items:                                                1
  DRE conn state:                                                READ
  Hostname in HTTP CONNECT:                                                  <-----
Added in 4.1.5
  IP Address in HTTP CONNECT:                                                <-----
Added in 4.1.5
  TCP Port in HTTP CONNECT:                                                  <-----
Added in 4.1.5
```

排除HTTP AO到SSL AO切換連線故障

如果使用者端必須通過Proxy才能到達HTTPS伺服器，則使用者端的要求首先會作為HTTP CONNECT訊息傳送到Proxy（在CONNECT訊息中嵌有實際的HTTPS伺服器IP位址）。 此時，HTTP AO在對等WAE上處理此連線。代理在客戶端和伺服器埠之間建立隧道，並在客戶端和伺服器IP地址及埠之間中繼後續資料。Proxy使用「200 OK」訊息回應使用者端，並解除與SSL AO的連線，因為使用者端擬透過SSL與伺服器通話。然後，使用者端會透過代理設定的TCP連線（通道）與SSL伺服器發起SSL交握。

排除轉接連線故障時，請檢查以下事項：

- 檢查**show statistics accelerator http**命令的輸出，以確認連線已由HTTP AO處理，然後傳遞到SSL AO。檢視Total Handled Connections和Total Connections Handled-off to SSL計數器。如果存在任何問題，請驗證以下內容：
  - 在對等WAE上，HTTP AO已啟用且處於運行狀態。
  - SSL加速服務使用客戶端在連線URL中使用的埠進行配置（如果使用HTTPS，則為隱含埠443）。 通常，代理埠不同於連線URL埠，不應在SSL加速服務中配置此代理埠。但是，代理埠應包含在對映到HTTP AO的流量分類器中。
- 檢查**show statistics accelerator http**命令的輸出，以確認此連線已由SSL AO處理和最佳化。檢視Total Handled Connections和Total Optimized Connections計數器。如果統計計數器不正確，請按照上一節所述執行基本SSL故障排除。
- 在資料中心WAE上，驗證**show statistics connection optimized detail**命令輸出是否顯示了實際SSL伺服器的主機名、IP地址和TCP埠。如果未正確設定這些欄位，請檢查以下內容：
  - 驗證客戶端瀏覽器代理設定是否正確。
  - 驗證在資料中心WAE上配置了DNS伺服器並且可訪問。您可以使用**ip name-server *A.B.C.D***命令在WAE上配置DNS伺服器。

伺服器證書驗證故障排除

伺服器證書驗證要求您將正確的CA證書匯入到資料中心WAE。

要排除伺服器證書驗證故障，請執行以下步驟：

1.檢查伺服器證書並檢索頒發者名稱。伺服器證書中的此頒發者名稱必須與匹配的CA證書中的使用者名稱匹配。如果具有PEM編碼的證書，則可以在安裝了openssl的伺服器上使用以下**openssl** 命令：

```
> openssl x509 -in cert-file-name -noout -text
```

2.使用**show running-config**命令確保資料中心WAE上存在匹配的加密pki ca配置。對於WAE在驗證過程中使用的CA證書，匯入的每個CA證書都需要一個加密pki ca配置項。例如，如果匯入了CA證書company1.ca，則必須在資料中心WAE上進行以下配置：

```
crypto pki ca company1
   ca-certificate company1.ca
   exit
```

附註：如果使用Central Manager GUI匯入CA證書，則Central Manager會自動新增上述加密pki ca配置以包括匯入的CA證書。但是，如果通過CLI匯入CA證書，則需要手動新增上述配置。

3.如果正在驗證的證書包含證書鏈，則確保證書鏈一致，並且最頂端頒發者的CA證書在WAE上匯入。請先使用**openssl verify**命令單獨驗證證書。

4.如果驗證仍失敗，則檢查SSL加速器調試日誌。使用以下命令啟用調試日誌記錄：

```
wae# config
wae(config)# logging disk priority debug
wae(config)# logging disk enable
wae(config)# exit
wae# undebug all
wae# debug accelerator ssl verify
wae# debug tfo connection all
```

5.啟動測試連線，然後檢查/local/local1/errorlog/sslao-errorlog.current日誌檔案。此檔案應指明伺服器證書中包含的頒發者名稱。確保此頒發者名稱與CA證書的使用者名稱完全匹配。

如果日誌中有任何其他內部錯誤，啟用其他調試選項可能會有所幫助。

6.即使頒發者名稱和使用者名稱匹配，CA證書也可能不正確。在這種情況下，如果伺服器憑證是由已知的CA核發，則可以使用瀏覽器直接（不帶WAAS）到達伺服器。當瀏覽器建立連線時，可通過按一下瀏覽器視窗右下角或瀏覽器位址列中顯示的鎖定圖示來檢查證書。證書詳細資訊可能指示與此伺服器證書匹配的適當CA證書。檢查CA證書中的Serial Number欄位。此序列號應與資料中心WAE上匯入的證書的序列號匹配。

7.如果已啟用OCSP撤銷檢查，請禁用該檢查並檢查證書驗證本身是否有效。有關OCSP設定疑難解答的幫助，請參閱「疑難解答OCSP吊銷檢查」部分。

客戶端證書驗證故障排除

可以在源伺服器和/或資料中心WAE上啟用客戶端證書驗證。當使用WAAS加速SSL流量時，源伺服器接收的客戶端證書是資料中心WAE上**crypto ssl services global-settings**命令中指定的電腦證書金鑰中指示的證書，如果未配置電腦證書金鑰，則為資料中心WAE電腦自簽名證書。因此，如果源伺

服器上的客戶端證書驗證失敗，則可能是由於源伺服器上無法驗證資料中心WAE電腦證書。

如果資料中心WAE上的客戶端證書驗證無法正常工作，則很可能是因為未在資料中心WAE上匯入與客戶端證書匹配的CA證書。請參閱「伺服器證書驗證故障排除」部分，瞭解有關如何檢查是否在WAE上匯入了正確的CA證書的說明。

對等WAE憑證驗證疑難排解

要解決對等證書驗證問題，請執行以下步驟：

1.驗證正在驗證的證書是CA簽名的證書。一個WAE的自簽名證書不能由另一個WAE驗證。預設情況下，WAE載入自簽名證書。必須使用**crypto ssl services global-settings machine-cert-key**命令配置自簽名證書。

2.檢驗在驗證證書的裝置上載入了正確的CA證書。例如，如果在資料中心WAE上配置了對等證書驗證，則分支WAE證書必須採用CA簽名，並且應在資料中心WAE上匯入相同的簽名CA證書。如果您要通過CLI手動匯入證書，請不要忘記使用**crypto pki ca**命令建立一個CA來使用匯入的證書。通過中央管理器GUI匯入時，中央管理器將自動建立匹配的加密pki ca配置。

3.如果對等WAE的驗證仍失敗，請按照「SSL AO記錄」一節所述檢查調試日誌。

排除OCSP吊銷檢查故障

如果系統在啟用線上證書狀態協定(OCSP)撤銷檢查的情況下成功建立SSL連線時遇到問題，請執行以下故障排除步驟：

1. 確保OCSP響應程式服務正在響應程式伺服器上運行。
2. 確保WAE和響應方之間的連線良好。從WAE使用**ping**和**telnet**命令（指向相應的埠）進行檢查。
3. 確認正在驗證的證書確實有效。到期日期和正確的響應方URL通常是存在問題的區域。
4. 驗證是否已在WAE上匯入OCSP響應的證書。來自OCSP響應方的響應也經過簽名，與OCSP響應匹配的CA證書必須位於WAE上。
5. 檢查**show statistics accelerator ssl**命令輸出以檢查OCSP統計資訊並檢查與OCSP故障對應的計數器。
6. 如果OCSP HTTP連線正在通過HTTP代理，請嘗試禁用代理以檢視它是否有幫助。如果確實有用，請檢查代理配置是否未導致連線故障。如果Proxy組態正常，則可能會有某些HTTP標頭的特性，從而造成與Proxy的某種不相容性。擷取封包追蹤軌跡以進行進一步調查。
7. 如果所有其他操作均失敗，您可能必須捕獲傳出OCSP請求的資料包跟蹤以進行進一步調試。您可以使用**tcpdump**或**tethereal**命令，如初步WAAS故障排除文章中的捕獲和分析資料包部分所述。

資料中心WAE用於連線OCSP響應方的URL通過兩種方式之一匯出：

- **crypto pki global-settings**配置命令配置的靜態OCSP URL
- 在被檢查的證書中指定的OCSP URL

如果該URL源自正在檢查的證書，則必須確保該URL可訪問。啟用SSL加速器OCSP調試日誌以確定URL，然後檢查與響應方的連線。請參見下一節瞭解有關使用調試日誌的詳細資訊。

排除DNS配置故障

如果系統在使用伺服器名稱和伺服器域配置最佳化SSL連線時遇到問題，請執行以下故障排除步驟

：

1.確保WAE上配置的DNS伺服器可訪問並且可以解析名稱。使用以下命令檢查配置的DNS伺服器：

```
WAE# sh running-config | include name-server
ip name-server 2.53.4.3

Try to perform DNS or reverse DNS lookup on the WAE using the following commands:

WAE# dnslookup www.cisco.com
The specified host/domain name is unknown !
```

此響應表示所配置的名稱伺服器無法解析該名稱。

嘗試對已配置的名稱伺服器執行ping/traceoute以檢查其連通性和往返時間。

```
WAE# ping 2.53.4.3
PING 2.53.4.3 (2.53.4.3) 56(84) bytes of data.
--- 2.53.4.3 ping statistics ---
5 packets transmitted, 0 received, 100% packet loss, time 4008ms


WAE# traceroute 2.53.4.3
traceroute to 2.53.4.3 (2.53.4.3), 30 hops max, 38 byte packets
1  2.53.4.33 (2.53.4.33)  0.604 ms  0.288 ms  0.405 ms
2  * * *
3  * * *
4  * * *
5  * * *
```

2.如果DNS伺服器可訪問，且可以解析名稱，但仍未最佳化SSL連線，請確保配置指定域或主機名的加速服務處於活動狀態，並且SSL AO沒有警報。使用以下命令：

```
WAE#  show alarms
Critical Alarms:
----------------
      Alarm ID                Module/Submodule              Instance
  ---------------            --------------------          ---------------
  1 accl_svc_inactive         sslao/ASVC/asvc-host         accl_svc_inactive
  2 accl_svc_inactive         sslao/ASVC/asvc-domain       accl_svc_inactive

Major Alarms:
-------------
None

Minor Alarms:
-------------
None
```

出現「accl_svc_inactive」警報表示加速服務配置中存在一些差異，並且可能有一個或多個加速服務具有重疊的伺服器條目配置。檢查加速服務配置並確保配置正確。使用以下命令驗證設定：

```
WAE# show crypto ssl accelerated service
Accelerated Service     Config State    Oper State      Cookie
-------------------     ------------    -----------     ------
asvc-ip                  ACTIVE          ACTIVE          0
```

```
 asvc-host                ACTIVE          INACTIVE        1
 asvc-domain              ACTIVE          INACTIVE        2
```

要檢查有關特定加速服務的詳細資訊，請使用以下命令：

```
WAE# show crypto ssl accelerated service asvc-host
 Name: asvc-host
   Config state: ACTIVE, Oper state: INACTIVE, Cookie: 0x3, Error vector: 0x0
   No server IP addresses are configured
   The following server host names are configured:
     lnxserv.shilpa.com port 443
         Host 'lnxserv.shilpa.com' resolves to following IPs:
         --none--
   No server domain names are configured
```

加速服務的運行狀態可能為INACTIVE的一個原因是DNS故障。例如，如果在加速服務配置中存在伺服器主機名，而WAE無法解析伺服器IP地址，則它無法配置相應的動態策略。

3.如果「由於不匹配域名而導致的直通管道」的統計計數器增加，則表示SSL連線針對的是已配置為最佳化的伺服器。使用以下命令檢查策略引擎條目：

```
WAE#sh policy-engine application dynamic
       Number:     1   Type: Any->Host (6)  User Id: SSL (4)
       Src: ANY:ANY  Dst: 2.53.4.2:443
       Map Name: basic
       Flags: TIME_LMT DENY
       Seconds: 10  Remaining: 5  DM Index: 32767
       Hits: 1  Flows: - NA -  Cookie: 0x2EEEEEEE
       DM Ref Index: - NA -  DM Ref Cnt: 0
```

使用**show statistics connection**命令檢查連線狀態。第一個連線應顯示TSGDL的加速器，並且在TIME_DENY策略項的生存期之前，後續連線應是TDL。

4.如果DNS伺服器通過廣域網與資料中心WAE連線，或者反向DNS響應時間過長，則可能會丟棄某些連線。這取決於客戶端超時和rDNS響應時間。在這種情況下，「取消的反向DNS查詢數」的計數器將增加，連線將被丟棄。這種情況表明DNS伺服器沒有響應或速度非常慢和/或WAAS上的NSCD無法正常工作。可以使用**show alarms**命令檢查NSCD狀態。發生這種情況的概率非常低，因為在大多數部署中，DNS伺服器預計與資料中心WAE位於同一個LAN中。

HTTP到SSL AO鏈故障排除

附註：HTTP到SSL AO連結是在WAAS版本4.3.1中引入的。本節不適用於較早的WAAS版本。

連結允許AO在流的生存期內隨時插入另一個AO，並且兩個AO都可以獨立地將其特定於AO的最佳化應用於流。AO連結與4.3.1之前版本中由WAAS提供的AO切換功能不同，因為使用AO連結，第一個AO將繼續最佳化流量。

SSL AO處理兩種型別的連線：

- 位元組0的SSL:SSL AO首先收到連線並完成SSL握手。它會分析負載的初始部分以檢查HTTP方法。如果負載表示HTTP，則會插入HTTP AO;如果沒有，則應用常規TSDL最佳化。
- 代理連線：HTTP AO首先接收連線。它識別客戶端請求中的CONNECT報頭方法，並在代理使

用200 OK消息確認後插入SSL AO。

SSL AO使用檢測以下HTTP方法的輕量HTTP解析器：GET、HEAD、POST、PUT、選項、跟蹤、複製、鎖定、輪詢、BCOPY、BMOVE、MKCOL、刪除、搜尋、解鎖、BDELETE、PROPFIND、BPROPFIND、PROPPATCH、訂閱、BPROPPATCH、取消訂閱和X__MS_ENUMATTS。您可以使用**debug accelerator ssl parser**命令調試與解析器相關的問題。您可以使用**show stat accel ssl payload http/other**命令檢視根據負載型別分類的流量的統計資訊。

故障排除提示：

1. 請確保HTTP AO配置中啟用了HTTPS功能，因為該功能屬於HTTP AO。有關詳細資訊，請參閱HTTP AO故障排除文章。
2. 使用**show stat connection**命令檢查連線狀態。如果最佳化正確，應顯示THSDL，指示TCP、HTTP、SSL和DRE-LZ最佳化。如果缺少這些最佳化中的任何一個，請在該最佳化程式（SSL、HTTP等）上進一步調試。 例如，如果連線狀態顯示THDL，則表示未對連線應用SSL最佳化。有關SSL AO的調試問題的詳細資訊如下。
3. 確保SSL AO已啟用且處於運行狀態(請參閱「SSL AO故障排除」一節)。
4. 使用**show alarms**命令確保沒有警報。
5. 如果未最佳化SSL流量，請確保將伺服器IP地址、主機名或域名和埠號作為加速服務的一部分新增。
6. 使用**show crypto ssl services accelerated-service *ASVC-name***命令確保加速服務處於ACTIVE狀態(請參閱「排除DNS配置故障」部分)。
7. 使用**show policy-engine application dynamic**命令，確保策略引擎具有此伺服器和埠的條目。
8. 如果目標伺服器在非預設埠上使用SSL（預設埠為443），請確保這在策略引擎配置中反映出來。中央管理器依靠此資訊來報告SSL流量資料。
9. 使用**show crypto ssl services accelerated-service *ASVC-name***命令，確保配置的主機名解析為有效IP地址。如果未找到IP地址，請檢查名稱伺服器是否配置正確。另請檢查**dnslookup** IP-address命令的輸出。

```
wae# sh run no-policy
. . .
crypto ssl services accelerated-service sslc
  version all
  server-cert-key test.p12
  server-ip 2.75.167.2 port 4433
  server-ip any port 443
  server-name mail.yahoo.com port 443
  server-name mail.google.com port 443
  inservice


wae# sh crypto ssl services accelerated-service sslc
Name: sslc
Config state: ACTIVE, Oper state: ACTIVE, Cookie: 0x0, Error vector: 0x0

   The following server IP addresses are configured:
     2.75.167.2 port 4433
     any port 443

   The following server host names are configured:
     mail.yahoo.com port 443
         Host 'mail.yahoo.com' resolves to following IPs:
         66.163.169.186
```

```
    mail.google.com port 443
        Host 'mail.google.com' resolves to following IPs:
        74.125.19.17
        74.125.19.18
        74.125.19.19
        74.125.19.83


wae# dnslookup mail.yahoo.com
Official hostname: login.lga1.b.yahoo.com
         address: 66.163.169.186
Aliases: mail.yahoo.com
Aliases: login.yahoo.com
Aliases: login-global.lgg1.b.yahoo.com

wae# dnslookup mail.google.com
Official hostname: googlemail.l.google.com
         address: 74.125.19.83
         address: 74.125.19.17
         address: 74.125.19.19
         address: 74.125.19.18
Aliases: mail.google.com
```

SSL AO記錄

以下日誌檔案可用於排除SSL AO問題：

- 事務日誌檔案：/local1/logs/tfo/working.log(和/local1/logs/tfo/tfo_log_*.txt)
- 調試日誌檔案：/local1/errorlog/sslao-errorlog.current（和sslao-errorlog。*）

為了更輕鬆地進行調試，您應該首先設定ACL以限制資料包只訪問一台主機。

```
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
```

要啟用事務日誌記錄，請使用**transaction-logs** configuration命令，如下所示：

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

可以使用**type-tail**命令檢視事務日誌檔案的結尾，如下所示：

```
wae# type-tail tfo_log_10.10.11.230_20090715_130000.txt
Wed Jul 15 14:35:48 2009 :1633 :10.10.10.10 :2199 :10.10.100.100 :443 :OT :START  :EXTERNAL
CLIENT :00.14.5e.84.24.5f :basic
 :SSL :HTTPS :F :(TFO) (DRE,LZ,TFO) (TFO) (DRE,LZ,TFO) (DRE,LZ,TFO) :<None> :(None) (None)
(SSL) :<None> :<None>  :0 :332
Wed Jul 15 14:36:06
2009 :1633 :10.10.10.10 :2199 :10.10.100.100 :443 :SODRE :END :165 :15978764 :63429 :10339 :0
Wed Jul 15 14:36:06 2009 :1633 :10.10.10.10 :2199 :10.10.100.100 :443 :OT :END :EXTERNAL
CLIENT :(SSL) :468 :16001952 :80805 :27824
```

要設定並啟用SSL AO的調試日誌記錄，請使用以下命令。

附註：調試日誌記錄是CPU密集型，可以生成大量輸出。在生產環境中慎重而謹慎地使用它。

您可以按如下方式啟用磁碟的詳細日誌記錄：

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

您可以在ACL中啟用連線的調試日誌記錄，如下所示：

```
WAE674# debug connection access-list 150
```

SSL AO調試選項如下：

```
WAE674# debug accelerator ssl ?
 accelerated-svc   enable accelerated service debugs
 alarm             enable SSL AO alarm debugs
 all               enable all SSL accelerator debugs
 am                enable auth manager debugs
 am-generic-svc    enable am generic service debugs
 bio               enable bio layer debugs
 ca                enable cert auth module debugs
 ca-pool           enable cert auth pool debugs
 cipherlist        enable cipherlist debugs
 client-to-server  enable client-to-server datapath debugs
 dataserver        enable dataserver debugs
 flow-shutdown     enable flow shutdown debugs
 generic           enable generic debugs
 ocsp              enable ocsp debugs
 oom-manager       enable oom-manager debugs
 openssl-internal  enable opnessl internal debugs
 peering-svc       enable peering service debugs
 session-cache     enable session cache debugs
 shell             enable SSL shell debugs
 sm-alert          enable session manager alert debugs
 sm-generic        enable session manager generic debugs
 sm-io             enable session manager i/o debugs
 sm-pipethrough    enable sm pipethrough debugs
 synchronization   enable synchronization debugs
 verify            enable certificate verification debugs
 waas-to-waas      enable waas-to-waas datapath debugs
```

您可以為SSL連線啟用調試日誌記錄，然後按如下方式顯示調試錯誤日誌的結束：

```
WAE674# debug accelerator ssl all
WAE674# debug connection all
Enabling debug messages for all connections.
Are you sure you want to do this? (y/n) [n]y
WAE674# type-tail errorlog/sslao-errorlog.current follow
```

NME和SRE模組上的證書過期警報故障排除

當自簽名的電腦證書已過期（或在過期後的30天內）並且未在WAAS裝置上配置自定義全域性電腦證書時，SSL AO將生成警報。WAAS軟體會生成工廠自簽名證書，該證書的到期日期為自WAAS裝置首次啟動起的5年。

在首次啟動期間，所有WAAS NME和SRE模組中的時鐘都設定為2006年1月1日，即使NME或SRE模組是較新的模組也是如此。這會導致自簽名證書在2011年1月1日過期，並且裝置會生成證書過期警報。

如果不使用預設工廠證書作為全域性證書，而是使用用於SSL AO的自定義證書，則不會遇到此意

外過期，並且可以在該證書過期時更新該自定義證書。此外，如果您已使用新的軟體映像更新NME或SME模組並將時鐘同步到較新的日期，則您可能不會遇到此問題。

證書到期的症狀是下列警報之一(此處顯示在**show alarms**命令的輸出中):

```
Major Alarms:
-------------
       Alarm ID                 Module/Submodule               Instance
  ---------------             --------------------          ---------------
  1 cert_near_expiration      sslao/SGS/gsetting           cert_near_expiration
```

或

```
       Alarm ID                 Module/Submodule               Instance
  ---------------             --------------------          ---------------
  1 cert_expired              sslao/SGS/gsetting           cert_expired
```

Central Manager GUI報告以下警報："Certificate__waas-self__.p12即將過期，它已在全域性設定中配置為電腦證書"

您可以使用下列解決方案之一來解決此問題：

- 為全域性設定配置其他證書：

```
SRE# crypto generate self-signed-cert waas-self.p12 rsa modulus 1024
SRE# config
SRE(config)# crypto ssl services global-settings machine-cert-key waas-self.p12
```

- 更新自簽名工廠證書，使其到期日更晚。此解決方案需要您聯絡Cisco TAC獲得的指令碼。

附註：此問題已通過解決方法解決，即WAAS軟體版本4.1.7b、4.2.3c和4.3.3發佈的CSCte05426。認證過期日期更改為2037。