WAAS - SSL AO故障排除

章节：SSL AO故障排除

本文介绍如何排除SSL AO故障。

目录

SSL加速器概述

SSL加速器（4.1.3及更高版本中提供）可优化加密安全套接字层(SSL)和传输层安全(TLS)流量。SSL加速器在WAAS内提供流量加密和解密，以实现端到端流量优化。SSL加速器还提供加密证书和密钥的安全管理。

在WAAS网络中，数据中心WAE充当客户端SSL请求的受信任中间节点。私钥和服务器证书存储在数据中心WAE上。数据中心WAE参与SSL握手，以生成会话密钥，该会话密钥在带内安全地分发到分支WAE，使分支WAE能够解密客户端流量、优化流量、重新加密流量，并通过广域网将其发送到数据中心WAE。数据中心WAE与源服务器维护单独的SSL会话。

以下服务与SSL/TLS优化相关：

- 加速服务 — 描述要应用于SSL服务器或服务器集的加速特性的配置实体。指定假定为受信任中间人时要使用的证书和私钥、要使用的密码、允许的SSL版本和证书验证设置。
- 对等服务 — 描述要应用于分支机构和数据中心WAE之间带内SSL连接的加速特性的配置实体。此服务用于将会话密钥信息从数据中心传输到分支WAE，以优化SSL连接。
- 中央管理器管理服务 — 不直接由SSL加速器使用，而是由管理员用于SSL加速服务的配置管理。也用于上传证书和私钥以用于SSL加速服务。
- 中央管理器管理服务 — 不直接由SSL加速器使用，而是用于应用程序加速器设备与中央管理器之间的通信。此服务用于配置管理、安全存储加密密钥检索和设备状态更新。

中央管理器安全存储对于SSL AO的运行至关重要，因为它存储所有WAE的安全加密密钥。每次重新加载中央管理器后，管理员需要通过使用cms secure-store open命令提供密码来重**新打开安全存储**区。每当WAE重新启动时，WAE都会从中央管理器自动检索其安全存储加密密钥，因此重新加载后，无需在WAE上执行任何操作。

如果客户端使用HTTP代理解决方案，则初始连接由HTTP AO处理，HTTP AO将其识别为端口443的SSL隧道请求。HTTP AO查找在数据中心WAE上定义的匹配SSL加速服务，当它找到匹配项时，请放弃与SSL AO的连接。但是，HTTP AO为HTTPS代理转移到SSL AO的流量将作为Web应用统计信息的一部分报告，而不是在SSL应用中报告。如果HTTP AO找不到匹配项，则根据静态HTTPS(SSL)策略配置优化连接。

SSL AO可以使用自签名证书而非CA签名证书，这有助于部署概念验证(POC)系统和排除SSL问题。通过使用自签名证书，您可以快速部署WAAS系统，而无需导入源服务器证书，并且您可以消除证书作为潜在问题源的可能。创建SSL加速服务时，可以在Central Manager中配置自签名证书。但是，当您使用自签名证书时，客户端浏览器将显示一个安全警报，表明证书不受信任（因为证书未由已知CA签名）。 要避免此安全警告，请在客户端浏览器的受信任根证书颁发机构存储中安装证书。(在Internet Explorer上，在安全警告中，单击**View Certificate**，然后在“Certificate”对话框中单击**Install Certificate**，并完成“Certificate Import Wizard”。)

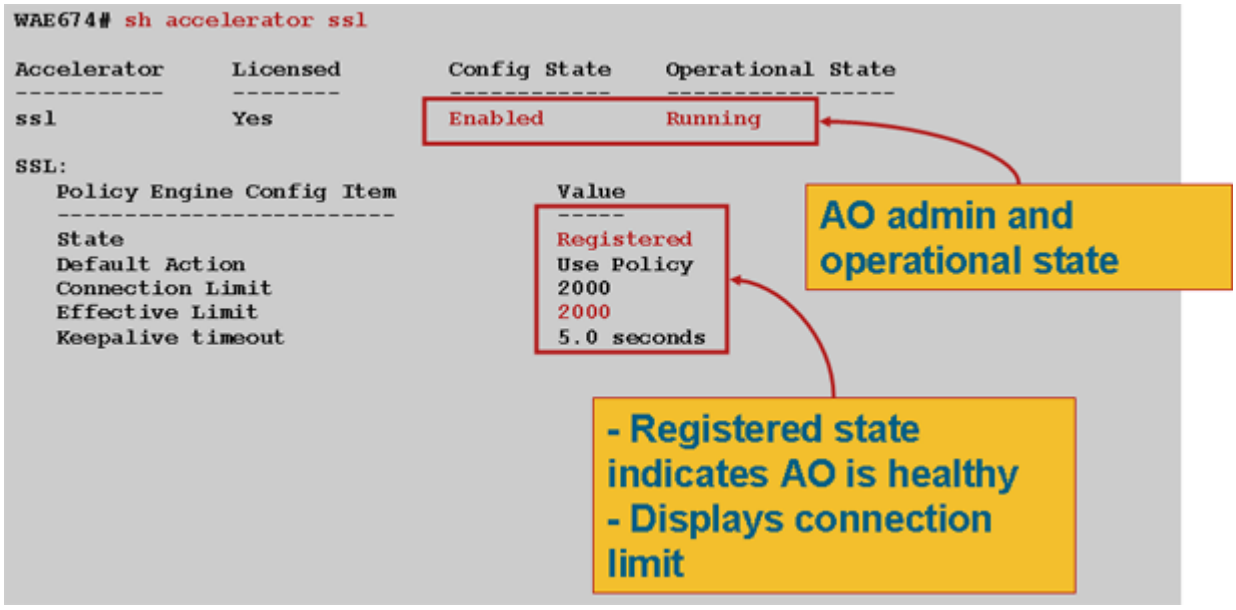
配置SSL管理服务是可选的，允许您将用于Central Manager通信到WAE和浏览器（用于管理访问）的SSL版本和密码列表更改为WAE。 如果配置浏览器不支持的密码，则与中央管理器的连接将断开。在这种情况下，请从CLI使用**crypto ssl management-service** 配置命令，将SSL管理服务设置设置恢复为默认值。

SSL AO故障排除

您可以使用**show accelerator**和**show license**命令验证常规AO配置和状态，如排除应用加速故障文章中所述。SSL加速器操作需要企业许可证。

接下来，使用**show accelerator ssl**命令（如图1所示）验证数据中心和分支WAE上特定于SSL AO的状态。您希望看到SSL AO已启用、运行和注册，并且显示连接限制。如果配置状态为启用，但操作状态为关闭，则表示许可问题。如果“运行状态”为“禁用”，则可能是因为WAE无法从中央管理器安全存储中检索SSL密钥，原因可能是安全存储未打开或中央管理器无法访问。使用**show cms info**和**ping**命令确认中央管理器可访问。

图1.检验SSL加速器状态



如果看到Gen Crypto Params的运行状态，请等待状态变为Running（运行），重新启动后可能需要几分钟时间。如果您看到从CM检索密钥的状态超过几分钟，则可能表示中央管理器上的CMS服务未运行，与中央管理器没有网络连接，WAE和中央管理器上的WAAS版本不兼容，或者中央管理器安全存储未打开。

您可以使用show cms secure-store命令来验证Central Manager安全存储是否已初**始化并打开，**如下所示：

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

如果安全存储未初始化或未打开，您将看到重要警报，如mstorekeyfailure和secure-store。您可以使用cms secure-store open命令打**开安全存储**，或从Central Manager中选择Admin > **Secure Store**。

提示：记录安全存储密码，以避免在忘记密码时必须重置安全存储。

如果WAE上的磁盘加密存在问题，也会阻止SSL AO运行。使用**show disk details**命令验证是否已启用磁盘加密，并检查是否已装载CONTENT和SPOOL分区。如果这些分区已装载，则表明磁盘加密密钥已从中央管理器成功检索，且加密数据可以从磁盘写入和读取。如果**show disk details**命令显示“System is initializing”，表示尚未从中央管理器检索加密密钥，且磁盘尚未装载。WAE在此状态下不提供加速服务。如果WAE无法从中央管理器检索磁盘加密密钥，将发出警报。

您可以验证SSL加速服务是否已配置，且其状态在数据中心WAE上为“已启用”(在中央管理器中，选择设备，然后选择**Configure > Acceleration > SSL Accelerated Services**)。由于以下条件，SSL加速器可能会使已配置和启用的加速服务变为非活动状态：

- 已从WAE中删除加速服务中配置的证书。使用**show running-config**命令确定加速服务中使用的证书，然后使用**show crypto certificates**和**show crypto certificate-details**命令确认证书是否存在安全存储。如果证书丢失，请重新导入证书。
- 加速服务证书已过期。使用**show crypto certificates**和**show crypto certificate-details**命令检查证书到期日期。
- 加速服务证书的有效日期从将来开始。使用**show crypto certificates**和**show crypto certificate-details**命令，并检查命令输出的有效性部分。此外，确保WAE时钟和时区信息准确。

您可以验证SSL连接是否应用了正确的策略，即，它们已通过SSL加速进行完全优化，如图2所示。在Central Manager中，选择WAE设备，然后选择**Monitor > Optimization > Connections Statistics**

。

图2.验证SSL连接上的正确策略

使用**show running-config**命令验证HTTPS流量策略是否已正确配置。您希望看到SSL应**用程序操作的**优化DRE no compression none，并且希望看到为HTTPS分类器列出的适当匹配条件，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
```

主动加速服务插入与加速服务中配置的服务器IP:port、服务器名称：port或服务器域：port对应的动态策略。可使用show policy-engine application dynamic命**令检查这些策**略。每个显示的策略中的Dst字段指示与加速服务匹配的服务器IP和端口。对于通配符域（例如，server-domain *.webex.com端口443），Dst字段将为“Any:443”。 对于服务器名称配置，当激活加速服务并将DNS响应中返回的所有IP地址插入策略引擎时，将执行正向DNS查找。此命令可用于捕获加速服务被标记为“服务中”但加速服务由于某些其他错误而变为非活动状态的情况。例如，所有加速服务都依赖于对等服务，如果对等服务因缺少/删除的证书而处于非活动状态，则加速服务也将标记为非活动状态，尽管在show running-config输出中该服务似乎为“inservice”。您可以使用show policy-engine application dynamic命令验证SSL动态策略在数据中心WAE**上是否处于活动状态**。可以使用show crypto ssl services host-service peering命**令验证对等服务状**态。

SSL AO加速服务配置可以有四种类型的服务器条目：

- 静态IP(server-ip) — 在4.1.3版及更高版本中提供
- 全部捕获(server-ip any)- 4.1.7及更高版本中提供
- 主机名（服务器名） — 在4.2.1及更高版本中可用
- 通配符域（服务器域） — 在4.2.1及更高版本中可用

一旦SSL AO收到连接，它将决定应使用哪种加速服务进行优化。静态IP配置的优先级最高，依次是

服务器名称、服务器域和服务器ip any。如果所有已配置和激活的加速服务均与连接的服务器IP不匹配，则连接会向下推送到通用AO。SSL AO插入到策略引擎中的Cookie用于确定特定连接匹配的加速服务和服务器条目的类型。此策略引擎Cookie是32位数，仅对SSL AO有意义。较高的位用于表示不同的服务器条目类型，较低的位用于表示加速的服务索引，如下所示：

SSL策略引擎Cookie值

Cookie值	服务器条目类型	备注
0x8 *xxxxxx*	服务器 IP 地址	静态IP地址配置
0x4 *xxxxxx*	服务器主机名	数据中心WAE对主机名执行正向DNS查找，并将返回的IP地址添加到动态策
0x2FFFFFFF	服务器域名	数据中心WAE对目的主机IP地址执行反向DNS查找，以确定其是否与域匹配
0x1 *xxxxxx*	服务器任意	使用此加速服务配置可加速所有SSL连接

示例 1：使用server-ip配置的加速服务：

```
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
```

相应的策略引擎条目添加如下：

```
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                  <----------------
```

示例 2：使用服务器名称配置的加速服务：

此配置可轻松部署，以优化企业SSL应用。它可适应DNS配置更改并减少IT管理任务。

```
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
```

相应的策略引擎条目添加如下：

```
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
```

示例 3：通过服务器域配置加速服务：

此配置允许WAAS设备配置单个通配符域，从而无需知道所有服务器的IP地址。数据中心WAE使用反向DNS(rDNS)来匹配属于已配置域的流量。配置通配符域可避免配置多个IP地址，使解决方案可扩展并适用于SaaS架构。

```
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
```

相应的策略引擎条目添加如下：

```
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
```

示例 4：使用server-ip any配置的加速服务：

此配置提供了捕获全部机制。当使用server-ip **any端口443的加速服**务激活时，它允许端口443上的所有连接由SSL AO优化。此配置可在POC期间用于优化特定端口上的所有流量。

```
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
```

相应的策略引擎条目添加如下：

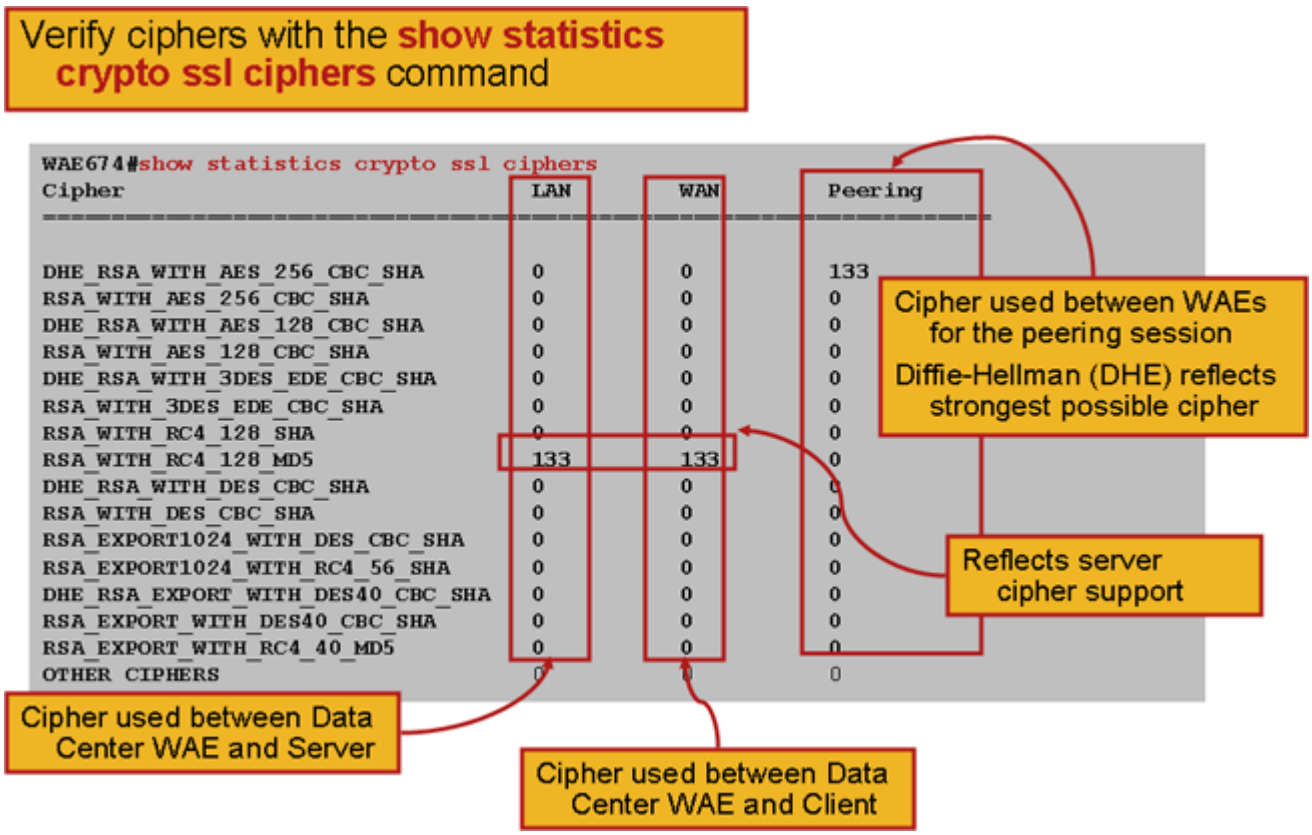
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< 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
```

如图3所示，您可以验证与**show statistics crypto ssl ciphers**命令一起使用的密码。

图3.检验密码



您可以验证这些密码是否与源服务器上配置的密码匹配。**注意**：Microsoft IIS服务器不支持包含DHE的密码。

在Apache服务器上，可以验证httpd.conf文件中的SSL版本和密码详细信息。这些字段也可能位于从httpd.conf引用的单独文件(sslmod.conf)中。按如下方式查找SSLProtocol和SSLCipherSuite字段：

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

要验证Apache服务器上的证书颁发者，请使用openssl命令读取证书，如下所示：

```
> 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
```

在浏览器中，您可以查看证书及其详细信息以确定证书链、版本、加密密钥类型、颁发者公用名(CN)和使用者/站点CN。在Internet Explorer中，单击挂锁图标，单击**查看证书**，然后查看详细信息和证书路径选项卡以了解此信息。

大多数浏览器要求客户端证书采用PKCS12格式，而不是X509 PEM格式。要将X509 PEM格式导出为PKCS12格式，请在Apache服务器上使用如下openssl命令：

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

如果私钥已加密，则导出时需要密码短语。导出密码再次用于将凭证导入WAAS设备。

使用**show statistics accelerator ssl**命令查看SSL AO统计信息。

```
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              <-------
---------
. . .
```

失败的会话和证书验证统计信息对于故障排除非常有用，在show statistics accelerator ssl命令上使用以下过滤器可更**轻松地检索这些**统计信息：

```
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
```

DNS相关统计信息对于排除服务器名称和通配符域配置故障非常有用。要检索这些统计信息，请使**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
 . . .
```

SSL重握手相关统计信息对于故障排除非常有用，可使用show statistics accelerator ssl命令上的以**下过滤器进行**检索：

```
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命令检查WAAS设备是否正在建立优化的SSL连接。**验证连接的Accel列中是否显示“TDLS”。“S”表示SSL AO的使用如下：

```
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"
```

您可以使用show statistics connection closed ssl命令检查已关闭连接**的连接统计信息。**

如果连接未得到优化，请检查WCCP/PBR是否配置正确且工作正常，并检查非对称路由。

您可以使用**show statistics connection optimized ssl detail**命令查看SSL连接统计信息，在该命令中，您将看到配置的SSL加速服务所产生的动态策略。**注意：**配置的策略仅是TFO优化，但是，配置的SSL服务会应用完全优化。

```
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
. . .
```

在此输出的后面部分，扩展SSL会话级别详细信息如下所示：

```
. . .
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切换连接故障

如果客户端必须通过代理才能访问HTTPS服务器，则客户端的请求首先作为HTTP CONNECT消息发送到代理（实际HTTPS服务器IP地址嵌入在CONNECT消息中）。 此时，HTTP AO在对等WAE上处理此连接。代理在客户端和服务器端口之间创建隧道，并在客户端和该服务器IP地址和端口之间中继后续数据。代理以“200 OK”消息响应客户端，并取消与SSL AO的连接，因为客户端打算通过SSL与服务器通信。然后，客户端通过代理设置的TCP连接（隧道）发起与SSL服务器的SSL握手。

排除切换连接故障时，请检查以下事项：

- 检查show statistics accelerator http命**令的输出**，以确认HTTP AO已处理连接，然后将其移交给SSL AO。查看Total Handled Connections和Total Connections Havded-off to SSL计数器。如果存在任何问题，请验证以下内容：
  - HTTP AO已启用，并且处于对等WAE的运行状态。
  - SSL加速服务配置有客户端在CONNECT URL中使用的端口（如果使用HTTPS，则为隐含端口443）。 代理端口通常与CONNECT URL端口不同，此代理端口不应在SSL加速服务中配置。但是，代理端口应包含在映射到HTTP AO的流量分类器中。
- 检查show statistics accelerator http命**令的输出**，以确认此连接已由SSL AO处理和优化。查看“已处理连接总数”和“已优化连接总数”计数器。如果统计计数器不正确，请按照上一节所述执行基本SSL故障排除。
- 在数据中心WAE上，验证**show statistics connection optimized detail命令输**出是否显示实际SSL服务器的主机名、IP地址和TCP端口。如果这些字段设置不正确，请检查以下项：
  - 验证客户端浏览器代理设置是否正确。
  - 验证DNS服务器是否在数据中心WAE上配置且可访问。可以使用ip name-server A.B.C.D命令**在WAE上配*置DNS服务器***。

服务器证书验证故障排除

服务器证书验证要求您将正确的CA证书导入数据中心WAE。

要排除服务器证书验证故障，请执行以下步骤：

1.检查服务器证书并检索颁发者名称。服务器证书中的此颁发者名称必须与匹配CA证书中的使用者名称匹配。如果您有PEM编码的证书，则可以在安装了openssl的服务器上使用以下**openssl**命令：

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

2.使用show running-config命令确保数据中心WAE上存在匹配的crypto pki ca**配置。**对于WAE在验证过程中要使用的CA证书，每个导入的CA证书都需要加密pki ca配置项。例如，如果导入CA证书company1.ca，则必须在数据中心WAE上进行以下配置：

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

注意：如果使用中央管理器GUI导入CA证书，中央管理器会自动添加上述加密pki ca配置以包括导入的CA证书。但是，如果CA证书是通过CLI导入的，则需要手动添加上述配置。

3.如果要验证的证书包括证书链，则确保证书链一致，并且最顶层颁发者的CA证书在WAE上导入。首先使用**openssl verify**命令单独验证证书。

4.如果验证仍然失败，则检查SSL加速器调试日志。使用以下命令启用调试日志记录：

```
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.启动测试连接，然后检查/local/local1/errorlog/sslao-errorlog.current日志文件。此文件应指示包含在服务器证书中的颁发者名称。确保此颁发者名称与CA证书的使用者名称完全匹配。

如果日志中有任何其他内部错误，则启用其他调试选项可能会很有帮助。

6.即使颁发者名称和使用者名称匹配，CA证书也可能不正确。在这种情况下，如果服务器证书由已知CA颁发，则可使用浏览器直接（不带WAAS）访问服务器。当浏览器设置连接时，可以通过单击浏览器窗口右下角或浏览器地址栏中显示的锁定图标来检查证书。证书详细信息可能指示与此服务器证书匹配的适当CA证书。检查CA证书中的序列号字段。此序列号应与在数据中心WAE上导入的证书的序列号匹配。

7.如果启用了OCSP撤销检查，请禁用它并检查证书验证本身是否有效。有关OCSP设置故障排除的帮助，请参阅“OCSP撤销检查故障排除”部分。

客户端证书验证故障排除

可在源服务器和/或数据中心WAE上启用客户端证书的验证。当WAAS用于加速SSL流量时，如果未配置machine-cert-key，则源服务器接收的客户端证书是在数据中心WAE的**crypto ssl services global-settings**命令中指定的machine-cert-key中指示的证书。因此，如果源服务器上的客户端证书验证失败，则可能是因为数据中心WAE机器证书在源服务器上不可验证。

如果数据中心WAE上的客户端证书验证不工作，可能是因为与客户端证书匹配的CA证书未在数据中心WAE上导入。有关如何检查WAE上是否导入了正确的CA证书的说明，请参阅“服务器证书验证故障排除”部分。

对等WAE证书验证故障排除

要排除对等证书验证问题，请执行以下步骤：

1.验证所验证的证书是CA签名的证书。一个WAE的自签名证书不能由另一个WAE验证。默认情况下，WAE加载自签名证书。必须使用crypto ssl services global-settings machine-cert-key**命令配置自签名证**书。

2.验证在验证证书的设备上加载了正确的CA证书。例如，如果在数据中心WAE上配置了peer-cert-verify，则分支WAE证书必须由CA签名，并且应在数据中心WAE上导入相同的签名CA证书。如果要通过CLI手动导入证书，请不要忘记使用**crypto pki ca**命令创建CA以使用导入的证书。当由中央管理器GUI导入时，中央管理器会自动创建匹配的加密pki ca配置。

3.如果对等WAE的验证仍然失败，请按照“SSL AO日志记录”部分所述检查调试日志。

排除OCSP撤销检查故障

如果系统在启用在线证书状态协议(OCSP)撤销检查的情况下无法成功建立SSL连接，请执行以下故障排除步骤：

1. 确保OCSP响应器服务在响应器服务器上运行。
2. 确保WAE和响应器之间连接良好。从WAE使用**ping**和**telnet**命令（到适当的端口）进行检查。
3. 确认正在验证的证书确实有效。到期日期和正确的响应方URL通常是出现问题的区域。
4. 验证OCSP响应的证书是否已导入WAE。来自OCSP响应方的响应也会签名，且与OCSP响应匹配的CA证书必须驻留在WAE上。
5. 检查**show statistics accelerator ssl**命令输出以检查OCSP统计信息，并检查与OCSP故障对应的计数器。
6. 如果OCSP HTTP连接正在通过HTTP代理，请尝试禁用该代理以查看其是否有用。如果它确实有帮助，则检查代理配置是否未导致连接故障。如果代理配置正常，则可能存在某些HTTP报头特性，这可能导致与代理不兼容。捕获数据包跟踪以进一步调查。
7. 如果所有其他操作都失败，则可能必须捕获传出OCSP请求的数据包跟踪，以便进一步调试。您可以使用WAAS故障排除初步文章**“捕获和分析数据包”一**节中所述的tcpdump或tethereal命令。

数据中心WAE用于到达OCSP响应器的URL通过以下两种方式之一派生：

- 由crypto pki global-settings配置命令配**置的静态OCSP** URL
- 在要检查的证书中指定的OCSP URL

如果URL是从要检查的证书派生的，则确保URL可访问至关重要。启用SSL加速器OCSP调试日志以确定URL，然后检查与响应方的连接。有关使用调试日志的详细信息，请参阅下一节。

排除DNS配置故障

如果系统无法使用服务器名称和服务器域配置优化SSL连接，请执行以下故障排除步骤：

1.确保在WAE上配置的DNS服务器可访问并可解析名称。使用以下命令检查已配置的DNS服务器：

```
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 !
```

此响应表示配置的名称服务器无法解析该名称。

尝试对已配置的名称服务器执行ping/traceoute命令，检查其可达性和往返时间。

```
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服务器可访问，并且它可以解析名称，但SSL连接仍未优化，请确保配置指定域或主机名的加速服务处于活动状态，并且没有SSL AO的警报。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
```

出现“accl_svc_inactive”警报表示加速服务配置中存在一些差异，并且可能存在一个或多个加速服务具有服务器条目的重叠配置。检查加速服务配置并确保配置正确。使用以下命令检验配置：

```
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
```

要检查有关特定加速服务的详细信息，请使用以下命令：

```
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
```

加速服务的运行状态可能为非活动状态的一个原因是DNS故障。例如，如果加速服务配置中有服务器主机名，而WAE无法解析服务器IP地址，则无法配置适当的动态策略。

3.如果“由于域名不匹配而导通”的统计计数器增加，则表明SSL连接用于已配置进行优化的服务器。使用以下命令检查策略引擎条目：

```
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命令检查连接状态。第一个连接应显示TSGDL的加速器和后续连接，直到TIME_DENY策略条目的生存期为TDL。

4.如果DNS服务器与数据中心WAE相关地位于WAN上，或者反向DNS响应时间过长，则某些连接可能会断开。这取决于客户端超时和rDNS响应时间。在这种情况下，“已取消反向DNS查找的数量”的计数器会增加，并且连接会被丢弃。此情况表明DNS服务器响应不迅速或速度很慢，和/或WAAS上的NSCD不工作。可以使用show alarms命令检查NSCD状态。发生这种情况的可能性非常低，因为在大多数部署中，DNS服务器预计与数据中心WAE位于同一个LAN中。

排除HTTP到SSL AO链路故障

NOTE:WAAS版本4.3.1中引入了HTTP到SSL AO链。本节不适用于早期的WAAS版本。

链允许AO在流的生命周期内随时插入另一个AO，并且两个AO可以独立地在流上应用其AO特定优化。AO链与WAAS在4.3.1之前版本中提供的AO切换功能不同，因为通过AO链，第一AO继续优化流。

SSL AO处理两种类型的连接：

- 字节0 SSL:SSL AO首先接收连接并完成SSL握手。它解析负载的初始部分以检查HTTP方法。如果负载指示HTTP，则会插入HTTP AO;否则，将应用常规TSDL优化。
- 代理连接：HTTP AO首先接收连接。它在客户端请求中标识CONNECT报头方法，并在代理使用200 OK消息确认后插入SSL AO。

SSL AO使用轻量HTTP解析器来检测以下HTTP方法：GET、HEAD、POST、PUT、OPTIONS、TRACE、COPY、LOCK、POLL、BCOPY、BMOVE、MKCOL、DELETE、SEARCH、UNLOCK、BDELETE、PROPFIND、PROPPATCH、SUBSCRIBE、PROPATCH、

UNSUBSCRIBE和X__MS_ENUMATTS。可以使用debug accelerator **ssl parser命令**调试与解析器相关的问题。可以使用show stat accel ssl **payload http/other命令查**看基于负载类型分类的流量的统计信息。

故障排除提示:

1. 确保在HTTP AO配置中启用HTTPS功能，因为HTTP AO拥有此功能。有关详细信息，请参阅HTTP AO故障排除文章。
2. 使用show stat connection命令检**查连接**状态。如果优化正确，应显示THSDL，指示TCP、HTTP、SSL和DRE-LZ优化。如果缺少任何这些优化，请对该优化程序（SSL、HTTP等）进一步调试。 例如，如果连接状态显示THDL，则意味着未对连接应用SSL优化。有关与SSL AO相关的调试问题的详细信息如下。
3. 确保SSL AO已启用且处于运行状态(请参阅“排除SSL AO故障”一节)。
4. 使用show alarms命令确保没有**警报**。
5. 如果SSL流量未优化，请确保服务器IP地址、主机名或域名和端口号已作为加速服务的一部分添加。
6. 使用**show crypto ssl services accelerated-service ASVC-name命令**(请参阅“DNS配置故障排除”部分)。
7. 使用show policy-engine application dynamic命令，确保策略引擎具有此服务器和**端口的一个**条目。
8. 如果目标服务器在非默认端口上使用SSL（默认值为443），请确保这反映在策略引擎配置中。中央管理器依靠此信息来报告SSL流量数据。
9. 使用show crypto ssl services accelerated-service ASVC-name命令，确保配置的主机名解析为**有效的IP地址。**如果未找到IP地址，请检查名称服务器是否配置正确。另请检查dnslookup IP-**address*命令的输***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日志记录

以下日志文件可用于排除SSL AO问题：

- 事务日志文件：/local1/logs/tfo/working.log（和/local1/logs/tfo/tfo_log_*.txt）
- 调试日志文件：/local1/errorlog/sslao-errorlog.current（和sslao-errorlog.*）

为便于调试，您应首先设置ACL，将数据包限制到一台主机。

```
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
```

要启用事务记录，请按如下方式使用transaction-logs配置命令：

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

您可以使用type-tail命令查看事务日志文件的结尾，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
```

要设置和启用SSL AO的调试日志记录，请使用以下命令。

NOTE:调试日志记录占用大量CPU资源，并且可以生成大量输出。在生产环境中谨慎、谨慎地使用它。

您可以按如下方式启用详细的日志记录到磁盘：

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

您可以为ACL中的连接启用调试日志记录，如下所示：

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

SSL AO调试的选项如下：

```
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
```

您可以为SSL连接启用调试日志记录，然后显示调试错误日志的结尾，如下所示：

```
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模块上的证书过期警报故障排除

当自签名计算机证书已过期（或在过期后30天内）且未在WAAS设备上配置自定义全局计算机证书时，SSL AO会生成警报。WAAS软件会生成出厂自签证书，从WAAS设备的首次启动开始到期日期为5年。

所有WAAS NME和SRE模块的时钟在首次启动时设置为2006年1月1日，即使NME或SRE模块更新。这会导致自签名证书在2011年1月1日到期，设备生成证书过期警报。

如果不使用默认出厂证书作为全局证书，而是使用SSL AO的自定义证书，您将不会遇到此意外过期，并且您可以在自定义证书过期时更新该证书。此外，如果您已使用新软件映像更新了NME或SME模块，并且已将时钟同步到更新的日期，则可能不会遇到此问题。

证书过期的症状是以下警报之一(显示在show alarms命令的输出中):

```
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
```

中央管理器GUI报告以下警报："Certificate__waas-self_.p12即将过期，它在全局设置中配置为计算机证书"

您可以使用以下解决方案之一解决此问题：

- 为全局设置配置其他证书：

```
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
```

- 更新自签工厂证书，并在以后过期。此解决方案需要您通过联系思科TAC获得的脚本。

NOTE:此问题通过WAAS软件版本4.1.7b、4.2.3c和4.3.3中发布的警告CSCte05426的解决方案解决。认证过期日期更改为2037。