Cisco版本的4.1.3 WAAS故障排除指南及以后

章节：排除SSL AO故障

此条款描述如何排除SSL AO故障。

Contents

SSL加速器概述

SSL加速器(可用4.1.3及以后)优化被加密的安全套接字协议层(SSL)和传输层安全(TLS)数据流。SSL加速器提供数据流加密和解密在WAAS内给enable (event)端到端数据流最优化。SSL加速器也提供加密证明和键的安全管理。

在WAAS网络中，数据中心WAE作为SSL请求的一个委托的中介节点由客户端。专用密钥和服务器证明在数据中心WAE被存储。数据中心WAE参加SSL握手派生会议密钥，安全地分配在波段之内对分组WAE，允许分组WAE解码客户端的流量，优化它，再加密它和在广域网发送它到数据中心WAE。数据中心WAE维护一次分开的SSL会话用源服务器。

以下服务是与SSL/TLS最优化相关：

- 加速服务–描述将申请SSL服务器或套加速度特性服务器的配置实体。指定将使用的认证和专用密钥，当摆在，当一委托的中间，将使用的密码， SSL版本准许时和证书验证设置。
- 并列的服务–描述将申请分组和数据中心WAEs之间的在波段之内SSL连接加速度特性的配置实体。此服务使用调用会议密钥信息从数据中心分支最优化的SSL连接WAEs。
- 中央管理器Admin服务–没使用直接地由SSL加速器，但是使用将管理员SSL加速服务的配置管理。并且曾经加载用于SSL加速服务和专用密钥的证书。
- 中央管理器管理服务–没使用直接地由SSL加速器，而且使用应用程序加速器设备和中央管理器之间的通信。此服务使用配置管理，巩固存储加密密钥检索和设备状态更新。

因为存储所有WAEs的，安全的加密密钥中央管理器安全的存储是重要为了SSL AO能运行。在每中央管理器重新加载，管理员需要通过提供密码短语重新打开安全的存储后**cms安全存储打开命令**。WAE从中央管理器自动地检索其安全的存储加密密钥，每当WAE重新启动，因此动作在WAE没有需要在重新加载以后。

如果客户端使用一个HTTP代理解决方案，初始连接由HTTP AO处理，认可它作为SSL隧道请求对端口443。HTTP AO正在寻找在数据中心WAE和，当查找匹配时，手定义的一项配比的SSL加速服务与SSL AO的连接。然而， HTTP AO递交对HTTPS代理的SSL AO作为Web应用程序统计数据一部分的数据流得到报告，不在SSL应用程序。如果HTTP AO没找到匹配，连接根据静态HTTPS (SSL)策略配置被最优化。

SSL AO能使用自署名的认证而不是CA签发的证书，可以是有用的在配置概念证明(POC)系统和在排除SSL问题故障。通过使用自署名的认证，您能迅速配置WAAS系统，而不必导入源服务器证书，并且您能排除证书作为问题的潜在的来源。当创建SSL加速服务时，您能配置在中央管理器的一自签证书。然而，当您使用一自签证书，客户端浏览器将显示安全性预警认证不信任(因为没有由著名的CA签字)。要避免此安全警告，在可靠的根证书颁发机构存储上请安装认证在客户端浏览器上。(在Internet Explorer，安全警告的，请点击**查看证书**，然后在认证对话请点击**安装证书**并且完成认证导入向导。)

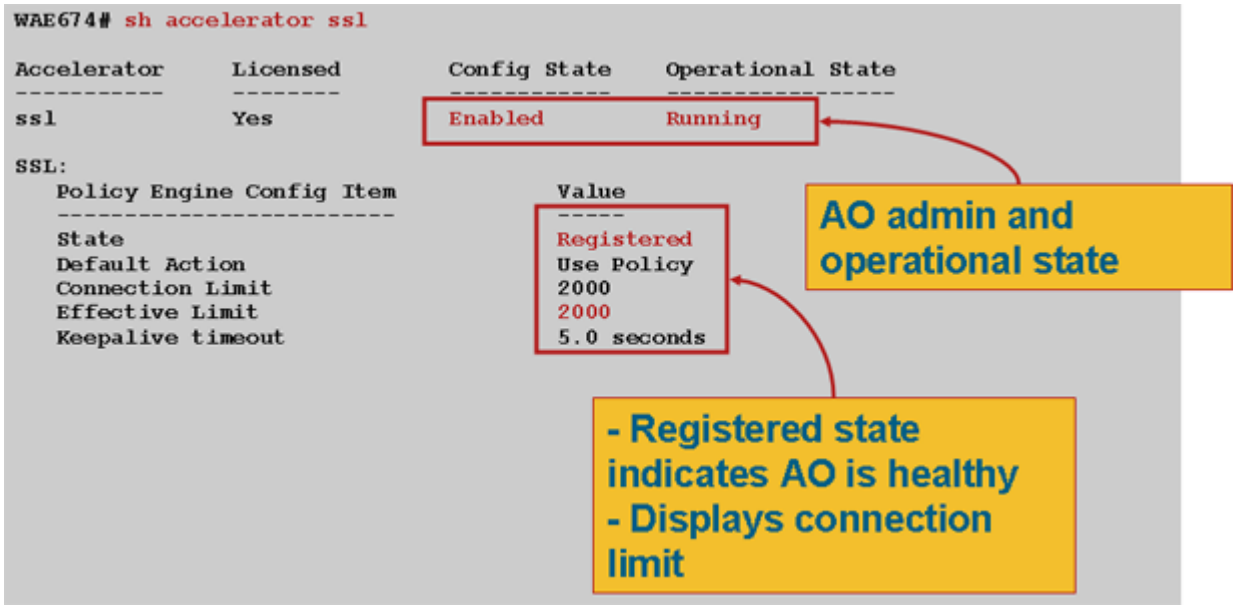
配置SSL管理服务是可选的，并且允许您更改用于中央管理器通信和密码列表的SSL版本到WAEs和到浏览器(管理访问)。如果配置您的浏览器不支持的密码，您将丢失与中央管理器的连接。在这种情况下，请使用从CLI的**crypto ssl管理服务**配置命令设SSL管理服务设置回到默认值。

排除SSL AO故障

您能验证一般AO配置和状态用**显示加速器**和**显示许可证**命令，正如排除应用程序加速度条款故障所描述。企业许可证对于SSL加速器操作是必需的。

其次，如图1所显示，请验证是特定的对在数据中心和分组WAEs的SSL AO通过使用**显示加速器ssl**命令的状态。您要发现SSL AO是启用的，运行和注册，并且连接限制显示。如果设置状态是启用的，但是操作状态被关闭，指示一个许可证问题。如果操作状态是失效的，可能这是因为WAE不能从中央管理器安全的存储检索SSL键，二者之一，因为安全的存储不开门或中央管理器是不可得到的。请使用**显示cms信息**和查验命令确认中央管理器可及的。

验证SSL加速器状态的图1.



如果看到Gen crypto氰胍一个操作状态，请等待，直到状态变运行，可能花费跟随重新启动的几分钟。如果为以上几分钟看到检索键状态从CM，可能表明在中央管理器的CMS服务不运行，没有网络连通性给中央管理器，在WAE和中央管理器的WAAS版本是不兼容的，或者中央管理器安全的存储不开门。

您能验证中央管理器安全的存储初始化和开门通过使用**显示cms安全存储**命令如下：

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

如果安全的存储没有初始化也不开门，您将看到严重告警例如mstore_key_failure和安全存储。您能开设安全的商店用**cms安全存储打开命令**或从中央管理器，选择**Admin >巩固存储**。

提示：如果忘记密码，请描述安全的存储密码避免必须重置安全的存储。

如果有磁盘加密的一个问题在WAE，那可以也防止SSL AO运行。请使用**show disk details命令**验证磁盘加密是启用的并且检查内容和SPOOL分区是否安放。如果这些分区安放，它表明磁盘加密密钥从中央管理器顺利地被检索了，并且加密的数据能被写和从磁盘读。如果**show disk details命令**显示“系统初始化”，指示加密密钥从中央管理器未被检索，并且磁盘未安放。WAE不会提供在此状态的加速度服务。如果WAE无法从中央管理器检索磁盘加密密钥，将发出警报。

您能验证配置SSL加速服务，并且其状态是“启用的”在数据中心WAE (在中央管理器，请选择设备，然后选择**配置>加速度> SSL加速服务**)。一项被配置的和被启用的加速服务可能由SSL加速器使非激活由于以下条件：

- 在加速服务中配置的认证从WAE被删除。请使用**show running-config命令**确定用于加速服务的认证，然后请使用**显示crypto证书**并且**显示crypto证书详细信息**命令确认认证存在请巩固存储。如果认证失踪，请再进口认证。
- 加速服务认证到期了。请使用**显示crypto证书**并且**显示crypto证书详细信息**命令检查认证到期日。
- 加速服务认证有在将来开始一个有效的日期。请使用**显示crypto证书**并且**显示crypto证书详细信息**命令并且检查命令输出的正确性部分。并且，请保证WAE时钟和时区信息是准确的。

您能验证SSL连接有被运用的正确的策略，如图2.所显示，即，他们有与SSL加速度的充分的最优化。在中央管理器，请选择WAE设备，然后选择**监控程序>最优化>连接统计**。

在SSL连接的验证正确的策略的图2.

请使用**show running-config命令**验证适当配置HTTPS流量策略。您要发现**优化DRE无压缩什么都**SSL应用程序动作和您的不要为HTTPS分类符发现列出的适当的匹配情况，如下：

```
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
```

一项活动加速服务插入动态策略与服务器IP相应：端口，服务器名：端口或者服务器域：在加速服务内被配置的端口。这些策略可以检查使用**dynamic命令显示策略引擎的应用程序**。在每个显示的策略的Dst字段指示匹配加速服务的服务器IP和端口。对于通配符域(例如，服务器域*.webex.com端口443)， Dst字段将是'Any:443。对于服务器名称配置，向前DNS查找执行，当启动时加速服务，并且在DNS回应返回的所有IP地址在策略引擎将插入。此命令是有用捉住加速服务被标记的“在职”的情况，但是加速服务使非激活由于某个其他错误。例如，所有加速服务依靠同位体服务和，如果同位体服务是非激活的由于一个缺少/被删除的认证，然后加速服务也将被标记作为非激活，虽然看起来是“在职”在show running-config输出中。您能验证SSL动态策略是活跃的在数据中心WAE通过使用**dynamic命令showpolicy引擎的应用程序**。通过使用showcrypto **ssl服务主机服务同位体命令，**您能验证同位体服务状态。

SSL AO加速服务配置能有服务器项的四种类型：

- 静态IP (服务器IP)--可用在版本4.1.3和以上
- 捉住所有(服务器IP其中任一)--可用4.1.7及以后
- 主机名(服务器名称)--可用4.2.1及以后
- 通配符域(服务器域)--可用4.2.1及以后

一旦连接由SSL AO接受，决定应该用于哪项加速服务最优化。提供静态IP配置最高的首选，跟随由服务器名、服务器域然后服务器IP其中任一。如果被配置的和被启动的加速服务都与连接的服务器IP不配比，连接增加与通用的AO。Cookie插入到策略引擎被SSL AO用确定哪项加速服务，并且什么类型的服务器项为特定的连接被匹配。此策略引擎Cookie是32位数字并且是仅有意义的对SSL AO。更高的位用于指示不同的服务器项类型和更低的位指示加速服务索引，如下：

SSL策略引擎Cookie值

Cookie值	服务器项类型	备注
0x8xxxxxxx	服务器IP地址	静态IP地址配置
0x4xxxxxxx	服务器主机名-	数据中心WAE执行主机名的向前DNS查找-，并且添加返回到动态策略配置
0x2FFFFFFF	服务器域名	数据中心WAE执行在目的地主机IP地址的逆向DNS查找确定是否与域配比。
0x1xxxxxxx	其中任一服务器	使用此加速服务配置，所有SSL连接加速

示例 1：与服务器IP配置的加速服务：

```
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
```

对应的策略引擎条目补充说如下：

```
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：与服务器名称配置的加速服务：

此配置允许企业SSL应用程序的最优化的容易的配置。它是能适应的对DNS配置更改并且减少IT管理任务。

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

对应的策略引擎条目补充说如下：

```
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：与服务器域配置的加速服务：

此配置允许WAAS设备配置避免需要认识所有服务器的IP地址的单个通配符域。匹配数据流的数据中心WAE用途反向DNS (rDNS)属于被配置的域。配置通配符域避免配置多个IP地址，使解决方案可升级和可适用为SaaS体系结构。

```
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
```

对应的策略引擎条目补充说如下：

```
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：与服务器IP的加速服务任何配置：

此配置提供一个全捕捉机制。当与**服务器IP的**一项加速服务**所有端口443**做激活时，允许在端口443的所有连接由SSL AO最优化。此配置可以用于在POCs期间优化在一个特定端口的所有数据流。

```
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
```

对应的策略引擎条目补充说如下：

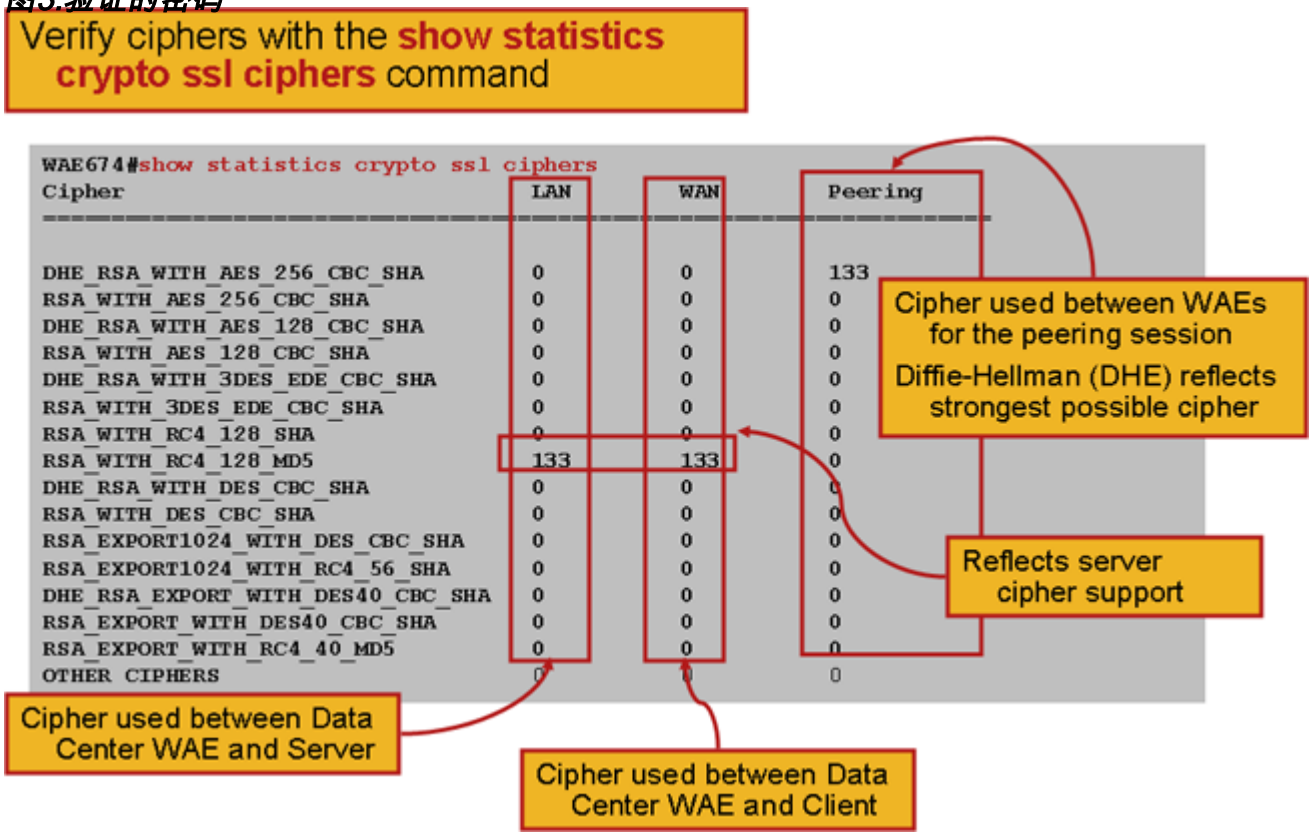
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< 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
```

您能验证密码与**show statistics crypto ssl密码**命令一起使用，如图3.所显示。

图3.验证的密码



您能验证这些密码匹配在源服务器配置的那些。**Note**:包括DHE Microsoft IIS服务器不支持的密码。

在阿帕契服务器上，您能验证在httpd.conf文件的SSL版本和密码详细资料。这些字段可能也在从httpd.conf (sslmod.conf)参考的一个独立的文件。寻找SSLProtocol和SSLCipherSuite字段如下：

```
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
```

要验证在阿帕契服务器的认证发布者，请使用openssl命令读认证如下：

```
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
```

在浏览器中，您能查看认证和其详细资料确定证书链、版本、加密密钥类型、发布者共同名称(CN)和主题/站点CN。在Internet Explorer，请点击挂锁图标，点击**查看证书**，然后注视着详细资料和证书路径选项对于此信息。

多数浏览器需要客户端证书以PKCS12格式而不是X509 PEM格式。对PKCS12格式要导出X509 PEM格式，请使用openssl命令如下在阿帕契服务器：

```
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
```

如果专用密钥被加密，密码短语对于导出是必需的。导出密码再使用导入证件WAAS设备。

请使用**show statistics加速器ssl**命令发现SSL AO统计数据。

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

通过使用在**show statistics加速器ssl**命令的以下过滤器失败的会话和证书验证统计数据可以是有用的为排除故障和更加容易地被检索：

```
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涉及的统计数据可以是有用的为排除服务器名和通配符域配置故障。要检索这些统计数据请使用**show statistics加速器ssl**命令，如下：

```
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
 . . .
```

使用在**show statistics加速器ssl**命令的以下过滤器SSL rehandshake涉及的统计数据是有用的为排除故障并且可以被检索：

```
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
```

请使用**show statistics连接优化的ssl**命令检查WAAS设备建立被最优化的SSL连接。验证“TDLS”出现于连接的Accel列。“S”表明使用了SSL AO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"
```

通过使用**show statistics连接结束的ssl**命令，您能检查连接统计密切关系。

如果连接没获得优化，请检查WCCP/PBR是否是适当配置和工作，并且检查不对称路由。

您能查看SSL连接统计通过使用**detail命令show statistics连接优化的ssl**，其中您将看到该动态的策略从被配置的SSL加速服务的结果。**Note**:被配置的策略是仅TFO最优化，但是充分的最优化由于被配置的SSL服务适用。

```
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
. . .
```

以后在此输出中，延长的SSL会话级别详细资料显示如下：

```
. . .
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
```

排除对SSL AO移交连接的HTTP AO故障

如果客户端必须通过代理到达HTTPS服务器，客户端请求首先去作为HTTP CONNECT信息对代理(当实际HTTPS服务器IP地址被嵌入在CONNECT信息)。这时， HTTP AO处理在对等体WAEs的此连接。代理创建在客户端和服务器端口之间的一条隧道并且传递随后数据在客户端和那之间服务器IP地址和端口。因为客户端打算与在SSL的服务器谈代理回应回到有“200的好的”消息和手客户端与SSL AO的连接。客户端然后起动SSL握手用在代理设置的TCP连接(隧道)的SSL服务器。

请检查以下事，当排除问题故障用被递交的连接时：

- 检查**show statistics加速器http**命令的输出确认连接由HTTP AO处理然后被递交了与SSL AO。查看被递交的总被处理的连接和总连接与SSL计数器。如果有任何问题，请验证以下：
  - HTTP AO是启用和在对等体的WAEs运行状态。
  - SSL加速服务配置有客户端使用的端口在连接URL (或暗示的端口443，如果使用HTTPS)。通常代理端口是与连接URL端口不同，并且在SSL加速服务中不应该配置此代理端口。然而，在被映射对HTTP AO的数据流分类符应该包括代理端口。
- 检查**show statistics加速器http**命令的输出确认此连接由SSL AO处理并且最优化。查看总被处理的连接并且共计优化的连接计数器。如果统计数据计数器不是正确的，请执行排除故障如前面的部分所述的基本的SSL。
- 在数据中心WAE，请验证**show statistics连接优化的detail命令**输出显示实际SSL服务器的主机名-， IP地址和TCP端口。如果没有正确地设置这些字段，请检查以下：
  - 验证客户端浏览器代理设置是正确的。
  - 验证DNS服务器在数据中心WAE被配置并且可及的。您能用***a.b.c.d命令的ip name-server***配置在WAE的一个DNS服务器。

排除服务器证书验证故障

服务器证书验证要求您导入正确的CA证书数据中心WAE。

要排除服务器证书验证故障请遵从这些步骤：

1. 检查服务器证明并且检索发证者名字。在服务器证明内的此发证者名字必须匹配在配比的CA证书内的主题名称。如果有PEM编码的证书，您能以openssl使用以下**openssl** on命令服务器安装的：

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

2. 保证通过使用**show running-config命令，**配比的crypto pki加州配置在数据中心WAE存在。对于WAE将使用的CA证书在验证进程，对于每个CA证书是必需的被导入的crypto pki加州配置条目。例如，如果导入CA证书company1.ca，然后在数据中心WAE必须做以下配置：

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

Note:使用中央管理器GUI，如果CA证书被导入，中央管理器自动地添加上述crypto pki加州配置包括被导入的CA证书。然而，如果CA证书通过CLI被导入，然后您将需要手工添加上述配置。

3. 如果被验证的认证包括一条证书链，则请保证证书链是连贯的，并且最上面的签发人的CA证书在WAE被导入。请使用**verify命令的openssl**分开验证认证首先。

4. 如果验证仍然发生故障，则请检查SSL加速器调试日志。请使用以下命令对enable (event)调试记录：

```
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. 首次测试连接然后检查/local/local1/errorlog/sslao-errorlog.current日志文件。此文件应该指示在服务器证明包括的发证者名字。保证此发证者名字完全地匹配CA证书的主题名称。

如果有在日志的任何其他内部错误，可能是有用的对enable (event)另外的调试选项。

6. 即使发证者名字和主题名称配比， CA证书可能不是正确一个。在这类情况下，如果著名的CA发行服务器证明，然后浏览器可以使用到直接地(没有WAAS)到达服务器。当浏览器设置连接，认证可以通过出现在浏览器窗口右下或在浏览器的地址栏内的点击锁图标检查。证书详细信息可能指示匹配此服务器证明的适当的CA证书。检查在CA证书内的Serial Number字段。此序列号应该匹配在数据中心WAE被导入认证的序列号。

7. 如果安排OCSP撤销检查被启用，请禁用它并且检查证书验证单独运作。关于排除OCSP设置故障的帮助请参阅"故障排除检查"部分的OCSP撤销。

排除客户端证书验证故障

客户端证书的验证可能被启用在源服务器并且/或者在数据中心WAE。当WAAS用于加速SSL流量时，源服务器接收的客户端证书是在机器CERT KEY指示的认证指定在**crypto ssl服务全局设置**on命令数据中心WAE或数据中心WAE机器自签证书，如果没有配置机器CERT KEY。结果，如果客户端证书验证是失败在源服务器，可能这是因为数据中心WAE机器认证不是可核实的在源服务器。

如果在数据中心WAE的客户端证书验证不工作，是可能的，因为匹配客户端证书的CA证书在数据中心WAE没有被导入。请参阅"排除服务器证书验证故障"部分关于指令如何检查在WAE有正确的CA证书导入是否。

排除对等体WAE证书验证故障

要排除对等体证书验证问题故障请遵从这些步骤：

1. 验证被验证的认证是CA签名的证书。由一个WAE的一自签证书由另一个WAE不是可核实的。默认情况下WAEs装载有自已签名的证书。必须配置使用**crypto ssl服务全局设置机器CERT KEY**命令，自签证书。

2. 验证正确的CA证书在验证认证的设备被装载。例如，如果请对等体CERT验证被配置对数据中心WAE，然后此是重要为了分组WAE认证能CA签名的，并且在数据中心WAE应该导入同一个签署的CA证书。如果通过CLI，手工导入认证使用**crypto pki加州**命令使用进口证明书，请勿忘记创建CA。当导入由中央管理器GUI，中央管理器自动地创建配比的crypto pki加州配置。

3. 如果对等体WAE的验证仍然发生故障，请检查调试日志正如记录”部分的“SSL AO所描述。

排除OCSP撤销检查故障

如果系统有建立与联机证书状态协议(OCSP)撤销检查的麻烦成功的SSL联系被启用，请遵从这些故障排除步骤：

1. 保证OCSP回应者服务在回应者服务器运行。
2. 保证WAE和回应者之间的好连接。请使用**ping**和**Telnet命令**(对适当的端口)从WAE检查。
3. 确认被验证的认证的确是有效的。到期日和正确的回应者URL典型地是有问题的区域。
4. 验证OCSP回应的认证在WAE被导入。自OCSP回应者的回应也签字，并且匹配OCSP回应的CA证书在WAE必须驻留。
5. 检查**show statistics加速器ssl**命令输出检查OCSP统计数据和检查计数器与OCSP故障相应。
6. 如果OCSP HTTP连接通过HTTP代理，请设法禁用代理发现是否帮助。如果它帮助，则请检查代理配置不导致连接失败。如果代理配置优良是，则可能有可能导致与代理的某不兼容的某HTTP包头特异。捕获进一步调查的一个信息包踪影。
7. 如果所有发生故障，您可以必须捕获流出的OCSP要求的信息包踪影进一步调试。您能使用**tcpdump**或**tethereal**命令正如“获取和分析信息包的”部分所描述在排除条款故障的初步的WAAS。

数据中心用于的URL WAE到达OCSP回应者在两种方式之一中派生：

- **crypto pki全局设置**配置命令配置的静态OCSP URL
- 在认证指定的OCSP URL被检查

如果URL从被检查的认证派生，则保证是重要的URL可及的。Enable (event)确定URL然后检查的SSL加速器OCSP调试日志连接对回应者。请参阅下个部分关于在使用调试日志的详细资料。

排除DNS配置故障

如果系统有最优化与服务器名和服务器域配置的麻烦SSL连接，请遵从这些故障排除步骤：

1. 保证在WAE配置的DNS服务器可及的，并且能解析名字。请使用以下命令检查被配置的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 !
```

此回应指示名字不可能由被配置的名称服务器解析。

设法ping/traceoute被配置的名称服务器的检查他们的可到达性和往返时间。

```
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服务器可及的，并且能解析名字，并且SSL连接仍然没获得优化，请确定配置指定的域或主机名的加速服务-是活跃的，并且没有SSL AO的警报。根据命令，请使用：

```
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
```

“accl_svc_inactive”警报的出现是征兆有在加速服务配置的若干差误，并且也许有有一个或更多的加速服务服务器项的重叠配置。检查加速服务配置并且确定配置是正确的。请使用以下命令验证配置：

```
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
```

要检查关于一项特定的加速服务的详细资料使用以下命令：

```
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
```

一个原因加速服务的操作状态也许是非激活的是DNS故障。例如，如果有服务器主机名-在加速服务配置和WAE不能解决服务器IP地址，然后不能配置适当的动态策略。

3. 如果统计计数器为“管道通过由于不匹配的域名”增加，它是暗示SSL连接是为为最优化被配置的服务器。使用以下命令，检查策略引擎条目：

```
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
```

检查连接状态使用**connection命令的show statistics**。第一个连接应该显示TSGDL加速器，并且随后的连接，直到TIME_DENY策略项的寿命，应该是TDL。

4. 如果DNS服务器是在广域网间关于数据中心WAE，或者，如果反向DNS响应时间是太长的，然后一些连接可能切。这取决于客户端超时和rDNS响应时间。在这种情况下，“被取消的逆向DNS查找的编号的计数器”增加，并且连接切。此情况是征兆DNS服务器不是响应能力或慢的并且/或者在WAAS的NSCD不工作。使用**show alarms命令，** NSCD状态可以被检查。发生的此的可能性是非常低的，因为在多数配置， DNS服务器预计在和一样数据中心WAE的LAN。

排除对SSL AO串连的HTTP故障

NOTE:对SSL AO串连的HTTP在WAAS版本4.3.1介绍。此部分不是可适用的对初期的WAAS版本。

连锁允许AO在任何时间插入另一个AO在流的一生期间，并且两AOs在流能独立地适用他们的AO特定最优化。因为与AO串连第一个AO继续优化流， AO串连是与在pre-4.3.1版本的WAAS提供的AO移交功能不同。

SSL AO处理两种连接类型：

- Byte-0 SSL ：SSL AO首先接受连接并且完成SSL握手。它解析有效载荷的最初的部分检查HTTP方法。如果有效载荷指示HTTP，插入HTTP AO;否则，它适用正常TSDL最优化。
- 代理连接：HTTP AO首先接受连接。在代理确认与一个200 OK消息后，它识别在客户端请求的连接报头方法并且插入SSL AO。

SSL AO使用发现以下HTTP方法的一个轻量HTTP分析程序：GET， HEAD， POST， PUT，选项，跟踪，复制， LOCK， POLL， BCOPY， BMOVE， MKCOL，删除，搜索，开锁， BDELETE， PROPFIND， BPROPFIND， PROPPATCH，预订， BPROPPATCH，取消预订和X__MS_ENUMATTS。您能使用**调试加速器ssl分析程序**命令调试问题与分析程序有关。您能使用**显示stat accel ssl有效载荷http/其他**命令查看根据有效载荷类型被分类的数据流统计数据。

故障检修提示：

1. 确定HTTPS功能在HTTP AO配置被启用，当这由HTTP AO拥有。关于详细资料，请参阅故障排除HTTP AO条款。
2. 检查连接状态使用**connection命令显示的stat**。如果正确地优化，它应该显示指示TCP、HTTP、SSL和DRE-LZ最优化的THSDL。如果这些最优化中的任一失踪，请调试进一步在该优化程序(SSL， HTTP，等等)。例如，如果连接状态显示THDL，意味着SSL最优化在连接未适用。关于调试问题的详细资料与SSL AO有关跟随。
3. 确定SSL AO是启用的并且在运行状态(请参阅部分"排除SSL AO故障")。
4. 确定通过使用**show alarms命令，**没有警报。
5. 如果SSL流量没有优化，请确定作为加速服务一部分，服务器IP地址、主机名或者domain-name和端口号被添加。
6. 确定加速服务是在激活状态通过使用**显示crypto ssl服务加速服务**ASVC ***NAME***命令(请参阅"排除DNS配置故障"部分)。
7. 确定策略引擎有此服务器的一个条目和端口通过使用**dynamic命令显示策略引擎的应用程序**。
8. 如果目的地服务器使用在一个非默认端口的SSL (默认值是443)，请确定这在策略引擎配置被反射。中央管理器取决于报告SSL流量数据此信息。
9. 确定配置的主机名解决对有效IP地址通过使用**显示crypto ssl服务加速服务**ASVC ***NAME***命令。如果没有找到IP地址，请检查是否正确地配置名称服务器。并且请检查***ip-address命令的dnslookup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记录

以下日志文件为排除SSL AO问题故障是可用的：

- 事务处理日志文件：/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.*)

对于更加容易的调试，您应该首先设置ACL对一台主机限制信息包。

```
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
```

对enable (event)处理日志，请使用**处理日志**配置命令如下：

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

您能查看事务处理日志文件的末端通过使用类型**尾标**命令如下：

```
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enable (event) SSL AO的调试记录，使用以下命令。

NOTE:调试记录强化中央处理，并且能生成很多输出。明智地和稀少请使用它在生产环境。

您能enable (event)详细日志到磁盘如下：

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

您能enable (event)连接的调试记录在ACL如下：

```
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
```

您能enable (event) SSL连接的调试记录然后显示调试错误日志的末端如下：

```
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
```

排除认证在NME和SRE模块的终止警报故障

SSL AO生成警报，当自已签署的机器认证到期了时(或是在30个期满日内)，并且自定义全局机器认证在WAAS设备没有被配置。WAAS软件生成与5年有效期的出厂自署名的认证从WAAS设备的第一启动的。

在所有WAAS NME和SRE模块的时钟设置为2006年1月1日在第一启动期间，即使NME或SRE模块是最近的。这造成自签证书到期2011年1月1日，并且设备生成证书到期警报。

如果不使用默认厂家认证作为全局认证和使用一个自定义认证SSL AO，您不会体验此意外的到期，并且您能更新自定义认证，每当到期。并且，如果更新有一个新的软件镜像的NME或SME模块和同步时钟对一个最近日期，您不可以遇到此问题。

证书到期的症状是以下警报之一(显示这里在输出的**show alarms命令中**)：

```
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
```

或

```
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
```

中央管理器GUI报告以下警报：被配置作为在整体设置的机器cert”的"Certificate__waas-self__.p12是最近的到期

您能使用以下解决方案之一解决此问题：

- 配置整体设置的一不同的身份验证：

```
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
```

- 更新与最新有效期的自已签署的出厂认证。此解决方案要求您能由接触的Cisco TAC得到的一个脚本。

NOTE:此问题由警告调整CSCte05426的解决方法，发布在WAAS软件版本4.1.7b， 4.2.3c和4.3.3。证明有效期更改到2037。