WAAS - Risoluzione dei problemi relativi a SSL AO

Capitolo: Risoluzione dei problemi relativi a SSL AO

In questo articolo viene descritto come risolvere i problemi relativi all'oggetto attivazione SSL.

Sommario

Panoramica di SSL Accelerator

L'acceleratore SSL (disponibile nella versione 4.1.3 e successive) ottimizza il traffico SSL (Secure Sockets Layer) e TLS (Transport Layer Security) crittografato. L'acceleratore SSL fornisce la crittografia e la decrittografia del traffico all'interno di WAAS per consentire l'ottimizzazione del traffico end-to-end. L'acceleratore SSL garantisce inoltre la gestione sicura dei certificati e delle chiavi di crittografia.

In una rete WAAS, il WAE del centro dati funge da nodo intermedio attendibile per le richieste SSL da parte del client. La chiave privata e il certificato del server sono memorizzati nel WAE del centro dati. WAE del data center partecipa all'handshake SSL per derivare la chiave di sessione, che distribuisce in modo sicuro in banda alla filiale WAE, consentendo alla filiale WAE di decrittografare il traffico dei client, ottimizzarlo, crittografarlo di nuovo e inviarlo sulla WAN al data center WAE. WAE del data center mantiene una sessione SSL separata con il server di origine.

I seguenti servizi sono rilevanti per l'ottimizzazione SSL/TLS:

- Servizio accelerato: entità di configurazione che descrive le caratteristiche di accelerazione da applicare a un server SSL o a un insieme di server. Specifica il certificato e la chiave privata da utilizzare durante l'utilizzo come intermediario attendibile, le cifrature da utilizzare, la versione SSL consentita e le impostazioni di verifica del certificato.
- Peering Service - Entità di configurazione che descrive le caratteristiche di accelerazione da applicare per le connessioni SSL in banda tra WAE di filiali e centri dati. Questo servizio viene utilizzato per trasferire le informazioni sulle chiavi di sessione dal centro dati alle filiali WAE per ottimizzare le connessioni SSL.
- Servizio di amministrazione di Central Manager - Non utilizzato direttamente dall'acceleratore SSL, ma da un amministratore per la gestione della configurazione dei servizi accelerati SSL. Utilizzato anche per caricare certificati e chiavi private da utilizzare nei servizi accelerati SSL.
- Servizio di gestione di Central Manager - Non utilizzato direttamente dall'acceleratore SSL, ma per la comunicazione tra i dispositivi dell'acceleratore applicazioni e Central Manager. Questo servizio viene utilizzato per la gestione della configurazione, il recupero della chiave di crittografia dell'archivio sicuro e gli aggiornamenti dello stato del dispositivo.

L'archivio protetto di Central Manager è essenziale per il funzionamento dell'oggetto attivazione SSL perché archivia chiavi di crittografia sicure per tutti i WAE. Dopo ogni riavvio di Central Manager, l'amministratore deve riaprire l'archivio protetto fornendo la passphrase con il comando **cms secure-store open**. WAE recupera automaticamente la propria chiave di crittografia dell'archivio sicuro da Gestione centrale ogni volta che si riavvia WAE, quindi non è richiesta alcuna azione su WAE dopo un ricaricamento.

Se i client utilizzano una soluzione proxy HTTP, la connessione iniziale viene gestita dall'oggetto attivazione HTTP, che la riconosce come richiesta di tunnel SSL alla porta 443. L'oggetto attivazione HTTP cerca un servizio accelerato SSL corrispondente definito nel server WAE del data center e, quando trova una corrispondenza, interrompe la connessione all'oggetto attivazione SSL. Tuttavia, il traffico che l'oggetto attivazione HTTP consegna all'oggetto attivazione SSL per un proxy HTTPS viene segnalato come parte delle statistiche dell'applicazione Web e non nell'applicazione SSL. Se l'oggetto attivazione HTTP non trova una corrispondenza, la connessione viene ottimizzata in base alla configurazione statica dei criteri HTTPS (SSL).

L'oggetto attivazione SSL può utilizzare certificati autofirmati anziché certificati firmati dall'autorità di certificazione, il che può essere utile per la distribuzione di sistemi POC e per la risoluzione dei problemi relativi a SSL. Utilizzando i certificati autofirmati, è possibile distribuire rapidamente un

sistema WAAS senza dover importare i certificati del server di origine ed eliminare i certificati come potenziale fonte di problemi. È possibile configurare un certificato autofirmato in Gestione centrale durante la creazione di un servizio accelerato SSL. Quando si utilizza un certificato autofirmato, tuttavia, nel browser client verrà visualizzato un avviso di protezione per indicare che il certificato non è attendibile, in quanto non è firmato da una CA nota. Per evitare questo avviso di protezione, installare il certificato nell'archivio Autorità di certificazione radice attendibili nel browser client. In Internet Explorer, nell'avviso di protezione fare clic su **Visualizza certificato**, quindi nella finestra di dialogo Certificato fare clic su **Installa certificato** e completare l'Importazione guidata certificati.

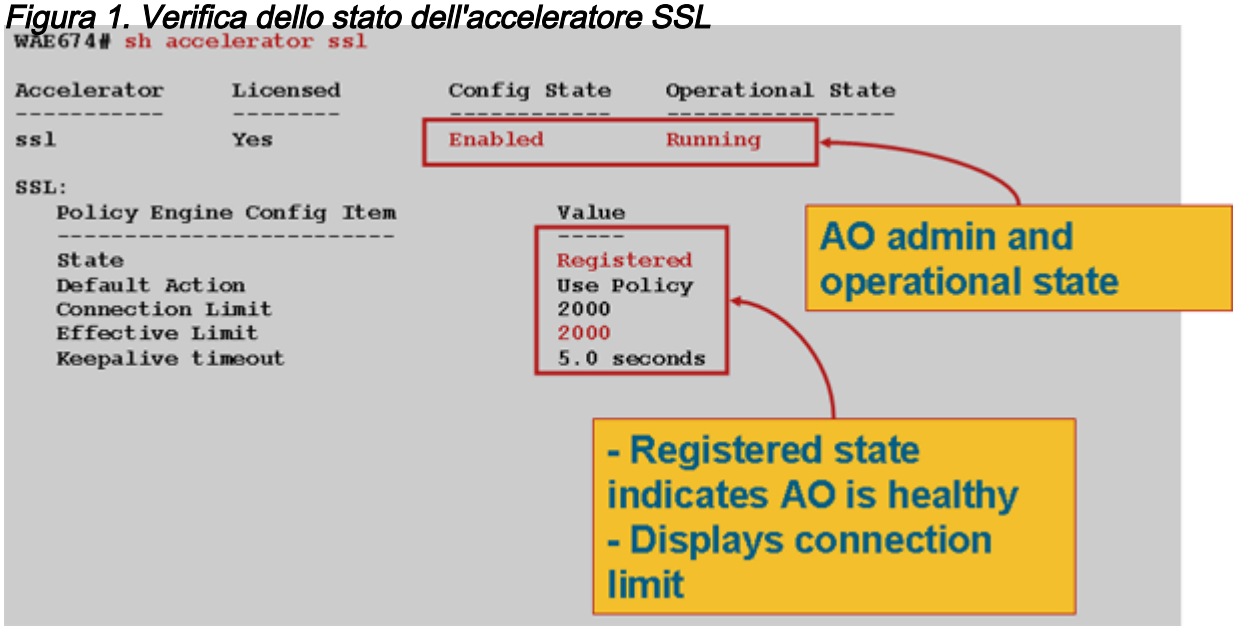
La configurazione dei servizi di gestione SSL è facoltativa e consente di modificare la versione SSL e l'elenco di cifratura utilizzati per le comunicazioni di Central Manager in WAE e nel browser (per l'accesso amministrativo). Se si configurano cifrari non supportati dal browser, la connessione a Gestione centrale verrà interrotta. In questo caso, usare il comando **crypto ssl management-service** configuration dalla CLI per ripristinare le impostazioni predefinite del servizio di gestione SSL.

Risoluzione dei problemi relativi a SSL AO

Èpossibile verificare la configurazione e lo stato generali dell'oggetto attivazione con i comandi **show accelerator** e **show license**, come descritto nell'articolo Risoluzione dei problemi di accelerazione delle applicazioni. Per il funzionamento dell'acceleratore SSL è necessaria la licenza Enterprise.

Verificare quindi lo stato specifico dell'oggetto attivazione SSL sia nel centro dati che nel ramo WAE utilizzando il comando **show accelerator ssl**, come mostrato nella Figura 1. Si desidera verificare che l'oggetto attivazione, esecuzione e registrazione dell'oggetto attivazione SSL e che il limite di connessione sia visualizzato. Se lo stato della configurazione è Abilitato ma lo stato operativo è Chiuso, è presente un problema di licenza. Se lo stato operativo è Disabilitato, è possibile che WAE non sia in grado di recuperare le chiavi SSL dall'archivio protetto di Gestione centrale, perché l'archivio protetto non è aperto o non è raggiungibile. Utilizzare i comandi **show cms info** e **ping** per verificare che Central Manager sia raggiungibile.

Figura 1. Verifica dello stato dell'acceleratore SSL



Se viene visualizzato lo stato operativo dei parametri di crittografia di generazione, attendere che lo stato diventi In esecuzione. L'operazione potrebbe richiedere alcuni minuti dopo il riavvio. Se lo stato di Recupero chiavi da Gestione configurazione è attivo per più di qualche minuto, è possibile

che il servizio CMS in Gestione centrale non sia in esecuzione, che non sia disponibile la connettività di rete a Gestione centrale, che le versioni WAAS in WAE e in Gestione centrale non siano compatibili o che l'archivio protetto di Gestione centrale non sia aperto.

Èpossibile verificare che l'archivio protetto di Central Manager sia inizializzato e aperto utilizzando il comando **show cms secure-store** come indicato di seguito:

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

Se l'archivio protetto non è inizializzato o aperto, verranno visualizzati allarmi critici quali mstore_key_failure e secure-store. È possibile aprire l'archivio protetto con il comando **cms secure-store open** oppure da Gestione centrale, scegliere **Amministrazione > Archivio protetto**.

Suggerimento: Documentare la password dell'archivio sicuro per evitare di doverla reimpostare se la si dimentica.

Se si verifica un problema con la crittografia del disco in un WAE, è possibile che anche l'oggetto attivazione SSL non funzioni. Utilizzare il comando **show disk details** per verificare che la crittografia del disco sia abilitata e controllare se le partizioni CONTENT e SPOOL sono attivate. Se queste partizioni sono montate, indica che le chiavi di crittografia del disco sono state recuperate correttamente da Gestione centrale e che i dati crittografati possono essere scritti e letti dai dischi. Se il comando **show disk details** restituisce "System is initializing", significa che le chiavi di crittografia non sono state ancora recuperate da Central Manager e che i dischi non sono stati ancora montati. WAE non fornirà servizi di accelerazione in questo stato. Se WAE non è in grado di recuperare le chiavi di crittografia del disco da Central Manager, viene generato un allarme.

Èpossibile verificare che il servizio con accelerazione SSL sia configurato e che il relativo stato sia "Abilitato" sul WAE del data center (in Central Manager, scegliere il dispositivo, quindi **Configura > Accelerazione > Servizi con accelerazione SSL**). Un servizio accelerato configurato e abilitato può essere reso inattivo dall'acceleratore SSL a causa delle seguenti condizioni:

- Il certificato configurato nel servizio accelerato è stato eliminato da WAE. Utilizzare il comando **show running-config** per determinare il certificato utilizzato nel servizio accelerato, quindi utilizzare i comandi **show crypto certificates** e **show crypto certificate-details** per confermare che il certificato sia presente in un archivio sicuro. Se il certificato è mancante, reimportarlo.
- Il certificato di servizio accelerato è scaduto. Utilizzare i comandi **show crypto certificates** e **show crypto certificate-details** per verificare la data di scadenza del certificato.
- La data del certificato di servizio accelerato è valida a partire da. Usare i comandi **show crypto certificates** e **show crypto certificate-details** e controllare la sezione sulla validità dell'output del comando. Verificare inoltre che le informazioni relative all'orologio WAE e al fuso orario siano accurate.

Èpossibile verificare che alle connessioni SSL sia applicato il criterio corretto, ovvero che abbiano l'ottimizzazione completa con l'accelerazione SSL, come mostrato nella Figura 2. In Central Manager, scegliere il dispositivo WAE, quindi **Monitor > Ottimizzazione > Statistiche connessioni**.

Figura 2. Verifica del criterio corretto per le connessioni SSL

Utilizzare il comando **show running-config** per verificare che i criteri del traffico HTTPS siano configurati correttamente. Si desidera visualizzare **ottimizza DRE nessuna compressione** per l'azione dell'applicazione SSL e le condizioni di corrispondenza appropriate elencate per il classificatore HTTPS, come indicato di seguito:

```
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
```

Un servizio accelerato attivo inserisce criteri dinamici corrispondenti all'indirizzo IP:porta del server, al nome del server:porta o al dominio del server:porta configurati all'interno del servizio accelerato. È possibile controllare questi criteri utilizzando il comando **show policy-engine application dynamic**. Il campo Dst in ciascun criterio visualizzato indica l'indirizzo IP e la porta del server corrispondenti al servizio accelerato. Per il dominio con caratteri jolly (ad esempio, dominio-server *.webex.com porta 443), il campo Dst sarà 'Any:443'. Per la configurazione del nome server, la ricerca DNS diretta viene eseguita quando viene attivato il servizio accelerato e tutti gli indirizzi IP restituiti nella risposta DNS verranno inseriti nel motore dei criteri. Questo comando è utile per rilevare le situazioni in cui un servizio accelerato è contrassegnato come "inservice" ma il servizio accelerato è reso inattivo a causa di altri errori. Ad esempio, tutti i servizi accelerati dipendono dal servizio di peering e, se il servizio di peering è inattivo a causa di un certificato mancante o eliminato, anche un servizio accelerato verrà contrassegnato come inattivo sebbene risulti "in servizio" nell'output show running-config. È possibile verificare che il criterio dinamico SSL sia attivo sul server WAE del data center utilizzando il comando **show policy-engine application dynamic**. È possibile verificare lo stato del servizio peer utilizzando il comando **show crypto ssl services host-service peering**.

Una configurazione del servizio accelerato SSL AO può includere quattro tipi di voci server:

- IP statico (server-ip): disponibile nella versione 4.1.3 e successive
- Catch All (server-ip any), disponibile a partire dalla versione 4.1.7

- Hostname (nome-server): disponibile nella versione 4.2.1 e successive
- Dominio jolly (dominio-server): disponibile nella versione 4.2.1 e successive

Una volta ricevuta la connessione dall'oggetto attivazione SSL, decide quale servizio accelerato utilizzare per l'ottimizzazione. Alla configurazione IP statica viene assegnata la preferenza più alta, seguita dal nome del server, dal dominio del server e quindi dall'indirizzo IP del server. Se nessuno dei servizi accelerati configurati e attivati corrisponde all'indirizzo IP del server per la connessione, la connessione viene indirizzata verso il basso all'oggetto attivazione generico. Il cookie inserito nel motore dei criteri dall'oggetto attivazione del servizio SSL viene utilizzato per determinare il servizio accelerato e il tipo di voce server corrispondente per una determinata connessione. Questo cookie del motore dei criteri è un numero a 32 bit ed è significativo solo per l'oggetto attivazione del servizio SSL. I bit più alti vengono utilizzati per indicare diversi tipi di voci server, mentre i bit più bassi indicano l'indice del servizio accelerato, come indicato di seguito:

Valori cookie motore criteri SSL

Valore cookie	Tipo voce server	Commenti
0x8*xxxxxxx*	Indirizzo IP server	Configurazione indirizzo IP statico
0x4*xxxxxxx*	Nome host server	WAE del data center esegue una ricerca DNS diretta per il nome host e aggiunge gli indirizzi IP restituiti nella configurazione dei criteri dinamici. Aggiornato ogni 10 minuti per impostazione predefinita.
0x2FFFFFFF	Nome dominio server	WAE del data center esegue una ricerca DNS inversa sull'indirizzo IP dell'host di destinazione per determinare se corrisponde al dominio. Se corrisponde, il traffico SSL viene accelerato e, se non corrisponde, viene gestito in base al criterio HTTPS statico.
0x1*xxxxxxx*	Qualsiasi server	Tutte le connessioni SSL vengono accelerate utilizzando questa configurazione del servizio accelerata

Esempio 1: Servizio accelerato con configurazione IP server:

```
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
```

La voce corrispondente del motore dei criteri viene aggiunta come segue:

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

Esempio 2: Servizio accelerato con configurazione nome server:

Questa configurazione consente una facile distribuzione per l'ottimizzazione delle applicazioni SSL aziendali. È adattabile alle modifiche della configurazione DNS e riduce le attività amministrative IT.

```
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
```

La voce corrispondente del motore dei criteri viene aggiunta come segue:

```
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
```

Esempio 3: Servizio accelerato con configurazione server-dominio:

Questa configurazione consente ai dispositivi WAAS di configurare un singolo dominio con caratteri jolly che evita la necessità di conoscere gli indirizzi IP per tutti i server. WAE del data center utilizza il DNS inverso (rDNS) per far corrispondere il traffico appartenente al dominio configurato. La configurazione di un dominio con caratteri jolly evita la configurazione di più indirizzi IP, rendendo la soluzione scalabile e applicabile all'architettura SaaS.

```
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
```

La voce corrispondente del motore dei criteri viene aggiunta come segue:

```
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
```

Esempio 4: Servizio accelerato con configurazione server-ip any:

Questa configurazione fornisce un meccanismo di attivazione totale. Quando un servizio accelerato con **server-ip qualsiasi porta 443** viene reso attivo, consente all'oggetto attivazione di ottimizzare tutte le connessioni sulla porta 443 da parte dell'oggetto attivazione (AO) SSL. Questa configurazione può essere utilizzata durante i POC per ottimizzare tutto il traffico su una determinata porta.

```
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
```

La voce corrispondente del motore dei criteri viene aggiunta come segue:

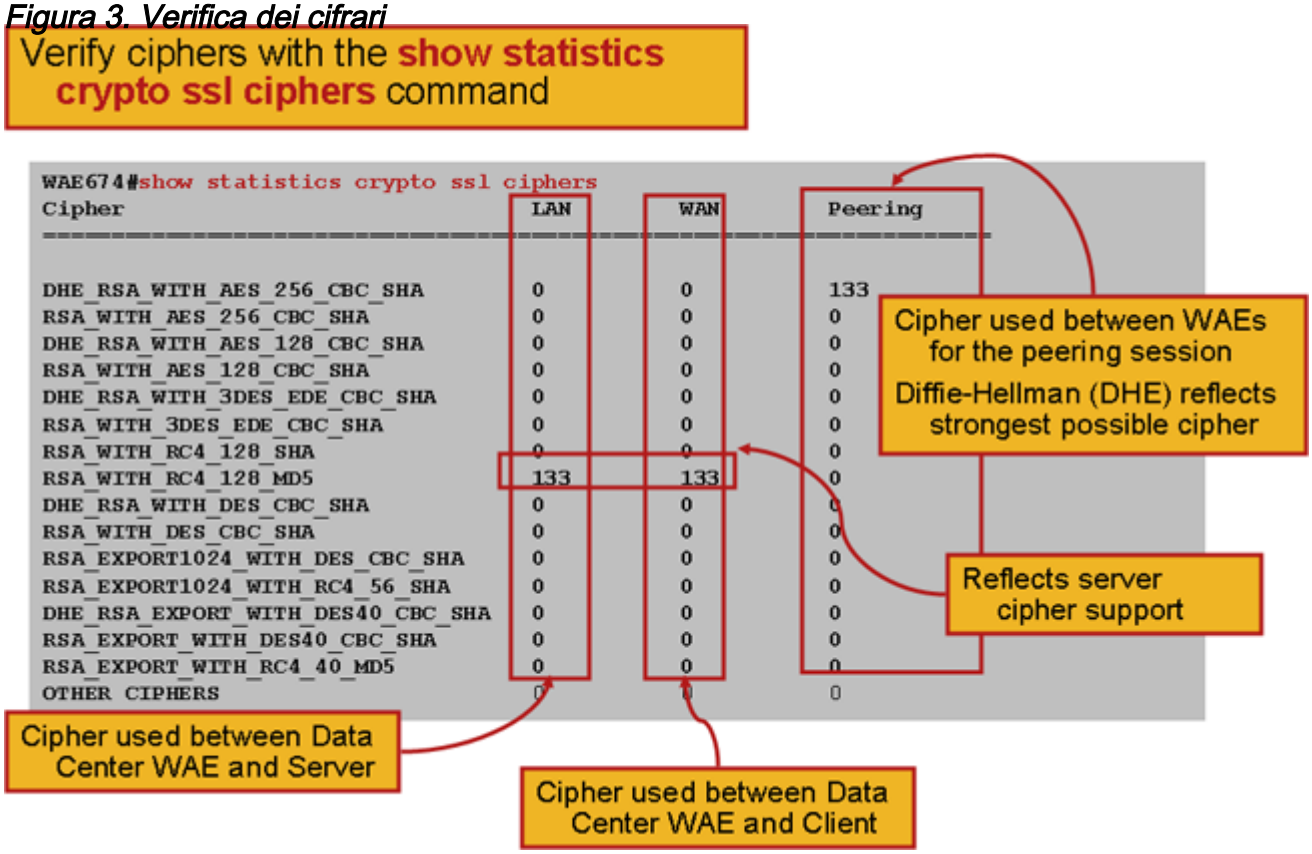
```
WAE# sh policy-engine application dynamic
Dynamic Match Freelist Information:
  Allocated: 32768  In Use: 3  Max In Use: 5  Allocations: 1751

< 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
```

Èpossibile verificare i cifrari utilizzati con i comandi **show statistics crypto ssl ciphers**, come mostrato nella Figura 3.

Figura 3. Verifica dei cifrari



Èpossibile verificare che queste cifrature corrispondano a quelle configurate nel server di origine.
Nota: Le cifrature che includono DHE non sono supportate dai server Microsoft IIS.

Su un server Apache, è possibile verificare la versione SSL e i dettagli della cifratura nel file httpd.conf. Questi campi possono trovarsi anche in un file separato (sslmod.conf) a cui si fa riferimento da httpd.conf. Cercare i campi SSLProtocol e SSLCipherSuite come indicato di seguito:

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

Per verificare l'autorità di certificazione su un server Apache, utilizzare il comando openssl per leggere il certificato come segue:

```
> 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
```

Nel browser è possibile visualizzare un certificato e i relativi dettagli per determinare la catena di certificati, la versione, il tipo di chiave di crittografia, il nome comune dell'emittente e il nome comune dell'oggetto/sito. In Internet Explorer fare clic sull'icona a forma di lucchetto, scegliere **Visualizza certificato** e quindi controllare le schede Dettagli e Percorso certificazione per ottenere queste informazioni.

La maggior parte dei browser richiede che i certificati client siano nel formato PKCS12 anziché nel formato PEM X509. Per esportare il formato PEM X509 nel formato PKCS12, utilizzare il comando openssl come segue su un server Apache:

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

Se le chiavi private sono crittografate, la passphrase è necessaria per l'esportazione. La password di esportazione viene utilizzata nuovamente per importare le credenziali sul dispositivo WAAS.

Utilizzare il comando **show statistics accelerator ssl** per visualizzare le statistiche degli oggetti ADO SSL.

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

Le statistiche relative alle sessioni non riuscite e alle verifiche dei certificati possono essere utili per la risoluzione dei problemi e possono essere recuperate più facilmente utilizzando il seguente filtro del comando **show statistics accelerator ssl**:

```
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
```

Le statistiche relative al DNS possono essere utili per la risoluzione dei problemi relativi alla configurazione del nome del server e del dominio con caratteri jolly. Per recuperare queste statistiche, utilizzare il comando **show statistics accelerator ssl**, come indicato di seguito:

```
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
 . . .
```

Le statistiche relative al rehandshake SSL possono essere utili per la risoluzione dei problemi e possono essere recuperate utilizzando il seguente filtro del comando **show statistics accelerator ssl**:

```
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
```

Utilizzare il comando **show statistics connection optimized ssl** per verificare che il dispositivo WAAS stabilisca connessioni SSL ottimizzate. Verificare che nella colonna Accel sia visualizzato

"TDLS" per una connessione. "S" indica che l'oggetto attivazione SSL è stato utilizzato nel modo seguente:

```
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"
```

Èpossibile controllare le statistiche di connessione per le connessioni chiuse utilizzando il comando **show statistics connection closed ssl**.

Se le connessioni non vengono ottimizzate, verificare che WCCP/PBR sia configurato e funzioni correttamente e verificare la presenza di un routing asimmetrico.

Èpossibile visualizzare le statistiche di connessione SSL utilizzando il comando **show statistics connection optimized ssl detail**, in cui viene visualizzato il criterio dinamico risultante dal servizio accelerato SSL configurato. **Nota:** Il criterio configurato è solo l'ottimizzazione TFO, ma l'ottimizzazione completa viene applicata come risultato del servizio SSL configurato.

```
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
. . .
```

Più avanti in questo output, i dettagli estesi a livello di sessione SSL vengono mostrati come segue:

```
. . .
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
```

Risoluzione dei problemi relativi alle connessioni da HTTP AO a SSL AO Handoff

Se un client deve passare attraverso un proxy per raggiungere un server HTTPS, la richiesta del client va prima come messaggio HTTP CONNECT al proxy (con l'indirizzo IP effettivo del server HTTPS incorporato nel messaggio CONNECT). A questo punto, l'oggetto attivazione HTTP gestisce la connessione nei server WAE peer. Il proxy crea un tunnel tra la porta del client e quella del server e inoltra i dati successivi tra il client e la porta e l'indirizzo IP del server. Il proxy risponde al client con un messaggio "200 OK" e consegna la connessione all'oggetto attivazione SSL perché il client intende comunicare con il server tramite SSL. Il client avvia quindi un handshake SSL con il server SSL sulla connessione TCP (tunnel) impostata dal proxy.

Per la risoluzione dei problemi relativi alle connessioni non gestite, verificare quanto segue:

- Controllare l'output del comando **show statistics accelerator http** per verificare che una connessione sia stata gestita dall'oggetto attivazione HTTP e quindi consegnata all'oggetto attivazione SSL. Esaminare il totale delle connessioni gestite e il totale delle connessioni passate ai contatori SSL. In caso di problemi, verificare quanto segue:
  - L'oggetto attivazione HTTP è abilitato e in stato di esecuzione nei server WAE peer.
  - Il servizio accelerato SSL è configurato con la porta utilizzata dal client nell'URL CONNECT (o nella porta implicita 443 se HTTPS è in uso). Spesso la porta proxy è diversa dalla porta CONNECT URL e non deve essere configurata nel servizio con accelerazione SSL. Tuttavia, la porta proxy deve essere inclusa nel classificatore del traffico mappato all'oggetto attivazione HTTP.
- Controllare l'output del comando **show statistics accelerator http** per verificare che la connessione sia stata gestita e ottimizzata dall'oggetto attivazione SSL. Esaminare i contatori Totale connessioni gestite e Totale connessioni ottimizzate. Se i contatori delle statistiche non sono corretti, eseguire la risoluzione dei problemi SSL di base, come descritto nella sezione precedente.
- Sul server WAE del data center, verificare che l'output del comando **show statistics connection optimized detail** visualizzi il nome host, l'indirizzo IP e la porta TCP effettivi del server SSL. Se questi campi non sono impostati correttamente, verificare quanto segue:
  - Verificare che le impostazioni proxy del browser client siano corrette.
  - Verificare che il server DNS sia configurato nel server WAE del centro dati e sia raggiungibile. È possibile configurare un server DNS sul server WAE con il comando **ip name-server** *A.B.C.D*.

Risoluzione dei problemi di verifica dei certificati server

Per la verifica del certificato del server è necessario importare il certificato CA corretto nel server WAE del centro dati.

Per risolvere i problemi relativi alla verifica dei certificati server, eseguire la procedura seguente:

1. Esaminare il certificato del server e recuperare il nome dell'autorità emittente. Il nome dell'autorità emittente nel certificato del server deve corrispondere al nome del soggetto nel

certificato CA corrispondente. Se si dispone di certificati codificati PEM, è possibile utilizzare il seguente comando **openssl** in un server in cui è installato openssl:

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

2. Verificare che la configurazione della chiave PAK crittografica corrispondente esista nel server WAE del data center utilizzando il comando **show running-config**. Affinché un certificato CA venga utilizzato da WAE nel processo di verifica, è necessario un elemento di configurazione della CA della chiave pubblica crittografica per ogni certificato CA importato. Ad esempio, se si importa il file company1.ca di un certificato CA, è necessario eseguire la configurazione seguente nel file WAE del centro dati:

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

Nota: Se un certificato CA viene importato utilizzando l'interfaccia utente grafica di Central Manager, quest'ultimo aggiunge automaticamente la configurazione dell'autorità di certificazione crittografica indicata in precedenza per includere il certificato CA importato. Tuttavia, se il certificato CA viene importato tramite la CLI, sarà necessario aggiungere manualmente la configurazione precedente.

3. Se il certificato da verificare include una catena di certificati, verificare che tale catena sia coerente e che il certificato CA dell'emittente di livello superiore venga importato nel WAE. Utilizzare il comando **openssl verify** per verificare prima il certificato separatamente.

4. Se il problema persiste, esaminare il log di debug dell'acceleratore SSL. Utilizzare i comandi seguenti per abilitare la registrazione del debug:

```
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. Avviare una connessione di prova, quindi esaminare il file di registro /local/local1/errorlog/sslao-errorlog.current. Questo file deve indicare il nome dell'autorità emittente incluso nel certificato del server. Verificare che il nome dell'autorità di certificazione corrisponda esattamente al nome soggetto del certificato CA.

Se nei log sono presenti altri errori interni, potrebbe essere utile abilitare opzioni di debug aggiuntive.

6. Anche se il nome dell'autorità emittente e il nome del soggetto corrispondono, il certificato CA potrebbe non essere quello corretto. In questi casi, se il certificato del server è rilasciato da una CA nota, è possibile utilizzare un browser per raggiungere direttamente il server (senza WAAS). Quando il browser imposta la connessione, il certificato può essere esaminato facendo clic sull'icona a forma di lucchetto che appare in basso a destra nella finestra del browser o all'interno della barra degli indirizzi del browser. I dettagli del certificato possono indicare il certificato CA appropriato corrispondente al certificato del server. Controllare il campo Numero di serie all'interno del certificato CA. Questo numero di serie deve corrispondere al numero di serie del certificato

importato sul WAE del data center.

7. Se il controllo delle revoche OCSP è abilitato, disabilitarlo e verificare che la verifica del certificato funzioni da sola. Per informazioni sulla risoluzione dei problemi relativi alle impostazioni OCSP, vedere la sezione "Risoluzione dei problemi relativi al controllo delle revoche OCSP".

Risoluzione dei problemi di verifica dei certificati client

La verifica del certificato client può essere abilitata sul server di origine e/o sul WAE del centro dati. Quando WAAS viene utilizzato per accelerare il traffico SSL, il certificato client ricevuto dal server di origine corrisponde al certificato indicato nella chiave machine-cert specificata nel comando **crypto ssl services global-settings** sul WAE del data center o nel certificato autofirmato del computer WAE del data center, se la chiave machine-cert non è configurata. Di conseguenza, se la verifica del certificato client non riesce sul server di origine, è possibile che il certificato del computer WAE del centro dati non sia verificabile sul server di origine.

Se la verifica del certificato client sul WAE del centro dati non funziona, è probabile che il certificato CA corrispondente al certificato client non venga importato sul WAE del centro dati. Per istruzioni su come controllare se il certificato CA corretto è stato importato in WAE, vedere la sezione "Risoluzione dei problemi di verifica del certificato server".

Risoluzione dei problemi di verifica dei certificati WAE peer

Per risolvere i problemi relativi alla verifica dei certificati peer, eseguire la procedura seguente:

1. Verificare che il certificato da verificare sia un certificato firmato dalla CA. Un certificato autofirmato da un WAE non può essere verificato da un altro WAE. Per impostazione predefinita, i WAE vengono caricati con certificati autofirmati. È necessario configurare un certificato autofirmato utilizzando il comando **crypto ssl services global-settings machine-cert-key**.

2. Verificare che il certificato CA corretto sia caricato nel dispositivo di verifica del certificato. Ad esempio, se la verifica del certificato peer è configurata sul WAE del centro dati, è essenziale che il certificato WAE della filiale sia firmato dall'autorità di certificazione e che lo stesso certificato dell'autorità di certificazione della firma sia importato sul WAE del centro dati. Non dimenticare di creare una CA utilizzando il comando **crypto pki ca** per utilizzare il certificato importato, se il certificato viene importato manualmente dalla CLI. Quando viene importata dall'interfaccia utente di Central Manager, quest'ultimo crea automaticamente una configurazione della chiave crittografica corrispondente.

3. Se la verifica di WAE peer non riesce, controllare i log di debug come descritto nella sezione "SSL AO Logging".

Risoluzione dei problemi relativi al controllo delle revoche OCSP

Se il sistema non riesce a stabilire connessioni SSL riuscite con il controllo delle revoche OCSP (Online Certificate Status Protocol) abilitato, eseguire la procedura per la risoluzione dei problemi seguente:

1. Verificare che il servizio risponditore OCSP sia in esecuzione nel server risponditore.
2. Garantire una buona connettività tra WAE e il risponditore. Usare i comandi **ping** e **telnet** (sulla porta appropriata) dal server WAE per controllare.
3. Confermare che il certificato da convalidare sia effettivamente valido. La data di scadenza e l'URL del responder corretto sono in genere aree in cui si verificano problemi.

4. Verificare che il certificato per le risposte OCSP sia importato in WAE. Anche le risposte di un risponditore OCSP sono firmate e il certificato CA corrispondente alle risposte OCSP deve risiedere nel WAE.
5. Controllare l'output del comando **show statistics accelerator ssl** per verificare le statistiche OCSP e controllare i contatori corrispondenti agli errori OCSP.
6. Se la connessione HTTP OCSP utilizza un proxy HTTP, provare a disabilitarlo per verificare se è utile. Se il problema persiste, verificare che la configurazione del proxy non causi l'errore di connessione. Se la configurazione del proxy è corretta, è possibile che l'intestazione HTTP presenti alcune peculiarità che potrebbero causare incompatibilità con il proxy. Acquisire una traccia del pacchetto per ulteriori indagini.
7. Se il problema persiste, potrebbe essere necessario acquisire una traccia dei pacchetti della richiesta OCSP in uscita per eseguire ulteriori operazioni di debug. È possibile utilizzare i comandi **tcpdump** o **tetheral** come descritto nella sezione "Cattura e analisi dei pacchetti" dell'articolo preliminare sulla risoluzione dei problemi WAAS.

L'URL utilizzato da WAE del data center per raggiungere un risponditore OCSP viene derivato in uno dei due modi seguenti:

- URL OCSP statico configurato dal comando **crypto pki global-settings** configuration
- URL OCSP specificato nel certificato da controllare

Se l'URL deriva dal certificato controllato, è essenziale verificare che sia raggiungibile. Abilitare i registri di debug OCSP dell'acceleratore SSL per determinare l'URL e quindi verificare la connettività al risponditore. Per i dettagli sull'utilizzo dei log di debug, vedere la sezione successiva.

Risoluzione dei problemi di configurazione DNS

Se si verificano problemi durante l'ottimizzazione delle connessioni SSL con le configurazioni del nome del server e del dominio del server, eseguire la procedura seguente per la risoluzione dei problemi:

1. Verificare che il server DNS configurato nel server WAE sia raggiungibile e in grado di risolvere i nomi. Utilizzare il comando seguente per controllare il server DNS configurato:

```
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 !
```

Questa risposta indica che il nome non può essere risolto dai server dei nomi configurati.

Provare a eseguire il ping/traceroute per i server dei nomi configurati per verificare la loro raggiungibilità e il tempo di andata e ritorno.

```
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. Se il server DNS è raggiungibile e è in grado di risolvere i nomi ma le connessioni SSL non vengono comunque ottimizzate, verificare che il servizio accelerato che configura il dominio o il nome host specificato sia attivo e che non siano presenti avvisi per l'oggetto attivazione (AO) SSL. Utilizzare i seguenti comandi:

```
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
```

La presenza dell'allarme "accl_svc_inactive" indica una discrepanza nella configurazione del servizio accelerato e uno o più servizi accelerati potrebbero avere configurazioni sovrapposte per le voci server. Controllare la configurazione del servizio accelerato e verificare che sia corretta. Utilizzare il comando seguente per verificare la configurazione:

```
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
```

Per verificare i dettagli relativi a un particolare servizio accelerato, utilizzare il comando seguente:

```
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
```

Uno dei motivi per cui lo stato operativo del servizio accelerato potrebbe essere INACTIVE è un errore DNS. Ad esempio, se nella configurazione del servizio accelerato è presente un nome host

del server e WAE non è in grado di risolvere l'indirizzo IP del server, non è in grado di configurare il criterio dinamico appropriato.

3. Se il contatore delle statistiche per "Pipe-through a causa di un nome di dominio non corrispondente" è in aumento, indica che la connessione SSL è per un server configurato per l'ottimizzazione. Controllare le voci del modulo criteri utilizzando il comando seguente:

```
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
```

Verificare lo stato della connessione utilizzando il comando **show statistics connection**. La prima connessione deve mostrare un acceleratore di TSGDL e le connessioni successive, fino alla durata della voce del criterio TIME_DENY, devono essere TDL.

4. Se il server DNS si trova sulla WAN rispetto al WAE del centro dati o se il tempo di risposta DNS inverso è troppo lungo, alcune connessioni potrebbero essere interrotte. Dipende dal timeout del client e dal tempo di risposta rDNS. In questo caso, il contatore per "Numero di ricerche DNS inverse annullate" aumenta e la connessione viene interrotta. Questa situazione indica che il server DNS non risponde o è molto lento e/o NSCD su WAAS non funziona. Lo stato NSCD può essere controllato con il comando **show alarms**. La probabilità che ciò avvenga è molto bassa in quanto nella maggior parte delle distribuzioni il server DNS dovrebbe trovarsi sulla stessa LAN del server WAE del centro dati.

Risoluzione dei problemi di concatenamento da HTTP a ADO SSL

NOTA: Il concatenamento da HTTP a ADO SSL è stato introdotto in WAAS versione 4.3.1. Questa sezione non è applicabile alle versioni WAAS precedenti.

Il concatenamento consente a un oggetto attivazione di inserire un altro oggetto attivazione in qualsiasi momento durante la durata di un flusso ed entrambi gli oggetti attivazione possono applicare la propria ottimizzazione specifica dell'oggetto attivazione in modo indipendente nel flusso. Il concatenamento degli oggetti AO è diverso dalla funzione di handoff degli oggetti AO fornita da WAAS nelle versioni precedenti alla 4.3.1 perché con il concatenamento degli oggetti AO il primo oggetto AO continua a ottimizzare il flusso.

L'oggetto attivazione SSL gestisce due tipi di connessioni:

- SSL byte-0: L'oggetto attivazione SSL riceve prima la connessione e completa l'handshake SSL. Analizza la parte iniziale del payload per verificare la presenza di un metodo HTTP. Se il payload indica HTTP, inserisce l'oggetto ADO HTTP; in caso contrario, applica l'ottimizzazione TSDL standard.
- Connessione proxy: L'oggetto attivazione HTTP riceve prima la connessione. Identifica il metodo dell'intestazione CONNECT nella richiesta del client e inserisce l'oggetto attivazione del protocollo SSL dopo che il proxy ha confermato con un messaggio OK 200.

L'oggetto attivazione SSL utilizza un parser HTTP lightweight che rileva i metodi HTTP seguenti: GET, HEAD, POST, PUT, OPTIONS, TRACE, COPY, LOCK, POLL, BCOPY, BMOVE, MKCOL, DELETE, SEARCH, UNLOCK, BDELETE, PROPFIND, BPROPFIND, PROPPATCH, SUBSCRIBE, BPROPPATCH, UNSUBSCRIBE E X_MS_ENUMATTS. È possibile utilizzare il comando **debug accelerator ssl parser** per eseguire il debug dei problemi correlati al parser. È possibile utilizzare il comando **show stat accel ssl payload http/other** per visualizzare le statistiche del traffico classificate in base al tipo di payload.

Suggerimenti per la risoluzione dei problemi:

1. Verificare che la funzionalità HTTPS sia abilitata nella configurazione HTTP AO, in quanto di proprietà dell'oggetto HTTP AO. Per ulteriori informazioni, vedere l'articolo Risoluzione dei problemi relativi agli oggetti attivazione HTTP.
2. Controllare lo stato della connessione utilizzando il comando **show stat connection**. Se ottimizzato correttamente, dovrebbe visualizzare il file THSDL che indica l'ottimizzazione di TCP, HTTP, SSL e DRE-LZ. Se una di queste ottimizzazioni risulta mancante, eseguire il debug ulteriormente su tale ottimizzatore (SSL, HTTP e così via). Ad esempio, se lo stato della connessione visualizza THDL, significa che l'ottimizzazione SSL non è stata applicata alla connessione. Di seguito sono riportati i dettagli sui problemi di debug relativi all'oggetto attivazione SSL.
3. Verificare che l'oggetto attivazione (AO) SSL sia abilitato e in esecuzione (vedere la sezione "Risoluzione dei problemi relativi all'oggetto attivazione (AO) SSL").
4. Verificare che non vi siano allarmi utilizzando il comando **show alarms**.
5. Se il traffico SSL non viene ottimizzato, verificare che l'indirizzo IP, il nome host o il nome di dominio e il numero di porta del server siano stati aggiunti come parte del servizio accelerato.
6. Verificare che il servizio accelerato sia in stato ACTIVE utilizzando il comando **show crypto ssl services accelerated-service** ***ASVC-name*** (vedere la sezione "Risoluzione dei problemi di configurazione DNS").
7. Verificare che il motore dei criteri disponga di una voce per il server e la porta utilizzando il comando **show policy-engine application dynamic**.
8. Se il server di destinazione utilizza SSL su una porta non predefinita (il valore predefinito è 443), verificare che ciò sia riflesso nella configurazione del motore delle policy. Central Manager si basa su queste informazioni per la segnalazione dei dati del traffico SSL.
9. Verificare che il nome host configurato venga risolto in un indirizzo IP valido utilizzando il comando **show crypto ssl services accelerated-service** ***ASVC-name***. Se non viene trovato alcun indirizzo IP, verificare che il server dei nomi sia configurato correttamente. Verificare inoltre l'output del comando **dnslookup** ***IP-address***.

```
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
```

Registrazione oggetti ADO SSL

Per la risoluzione dei problemi relativi agli oggetti attivazione SSL sono disponibili i seguenti file di registro:

- File di log delle transazioni: /local1/logs/tfo/working.log (e /local1/logs/tfo/tfo_log_*.txt)
- File registro di debug: /local1/errorlog/sslao-errorlog.current (e sslao-errorlog.*)

Per semplificare il debug, è necessario innanzitutto configurare un ACL in modo da limitare i pacchetti a un solo host.

```
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
```

Per abilitare la registrazione delle transazioni, utilizzare il comando di configurazione **transaction-logs** come segue:

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

Per visualizzare la fine di un file di log delle transazioni, utilizzare il comando **type-tail** nel modo seguente:

```
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
```

Per impostare e abilitare la registrazione di debug dell'oggetto attivazione SSL, utilizzare i comandi seguenti.

NOTA: La registrazione del debug richiede un utilizzo intensivo della CPU e può generare un'elevata quantità di output. Utilizzarlo con cautela e moderazione in un ambiente di produzione.

Èpossibile abilitare la registrazione dettagliata sul disco come indicato di seguito:

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

Èpossibile abilitare la registrazione del debug per le connessioni nell'ACL nel modo seguente:

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

Di seguito sono riportate le opzioni per il debug degli oggetti ADO SSL.

```
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
```

Èpossibile abilitare la registrazione debug per le connessioni SSL e quindi visualizzare la fine del registro errori di debug come indicato di seguito:

```
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
```

Risoluzione dei problemi relativi agli avvisi di scadenza dei certificati sui moduli NME e SRE

L'oggetto attivazione SSL genera avvisi quando il certificato del computer autofirmato è scaduto (o è scaduto entro 30 giorni dalla scadenza) e un certificato del computer globale personalizzato non è configurato nel dispositivo WAAS. Il software WAAS genera certificati autofirmati in fabbrica con una data di scadenza di 5 anni dal primo avvio del dispositivo WAAS.

L'orologio in tutti i moduli WAAS NME e SRE è impostato sul 1° gennaio 2006 al primo avvio, anche se il modulo NME o SRE è più recente. In questo modo il certificato autofirmato scadrà il 1 gennaio 2011 e il dispositivo genererà avvisi di scadenza del certificato.

Se non si utilizza il certificato predefinito di fabbrica come certificato globale e si utilizza invece un certificato personalizzato per l'oggetto attivazione (AO) SSL, non si verificherà questa scadenza imprevista ed è possibile aggiornare il certificato personalizzato ogni volta che scade. Inoltre, se il modulo NME o SME è stato aggiornato con una nuova immagine software e l'orologio è stato sincronizzato a una data più recente, questo problema potrebbe non verificarsi.

Il sintomo della scadenza del certificato è uno dei seguenti allarmi (mostrati qui nell'output del comando **show alarms**):

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

o

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

La GUI di Central Manager riporta il seguente allarme: "Certificato__waas-self__.p12 prossimo alla scadenza è configurato come certificato computer nelle impostazioni globali"

Per risolvere il problema, è possibile utilizzare una delle soluzioni seguenti:

- Configurare un certificato diverso per le impostazioni globali:

```
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
```

- Aggiornare il certificato del produttore autofirmato con una data di scadenza successiva. Questa soluzione richiede uno script che è possibile ottenere contattando Cisco TAC.

NOTA: Questo problema è risolto dalla risoluzione dell'avviso CSCte05426, rilasciato nelle versioni software WAAS 4.1.7b, 4.2.3c e 4.3.3. La data di scadenza della certificazione viene modificata in 2037.