WAAS - Risoluzione dei problemi dell'oggetto attivazione MAPI

Capitolo: Risoluzione dei problemi di MAPI AO

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

Co

Art
Arc
Ris
Ott
Ris
app
Ris
Ris
Ris
Ris
Ris
Ris
Ris
ger
Ris
Ris
Ris
Ris
Ris
Inli
Ris
Ris
Ris

Sommario

Acceleratore MAPI

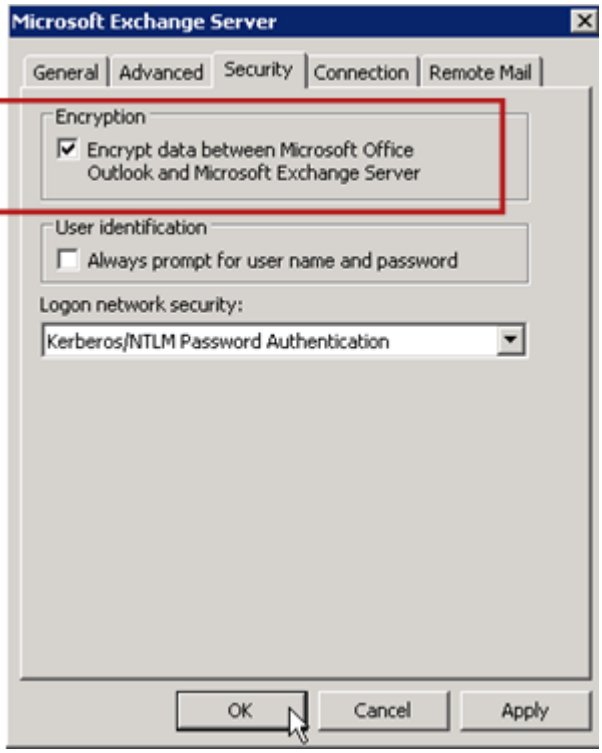
L'acceleratore MAPI ottimizza il traffico di posta elettronica di Microsoft Outlook Exchange. Exchange utilizza il protocollo EMSMDB, che è a livelli su MS-RPC, che a sua volta utilizza TCP o HTTP (non supportato) come trasporto di basso livello.

L'oggetto attivazione MAPI supporta i client Microsoft Outlook 2000-2007 sia per il traffico in modalità cache che per il traffico in modalità non cache. Le connessioni protette che utilizzano l'autenticazione (firma) o la crittografia dei messaggi non vengono accelerate dall'oggetto attivazione MAPI. Tali connessioni e connessioni dai client meno recenti vengono consegnate all'oggetto attivazione generico per le ottimizzazioni TFO. Inoltre, le connessioni OWA (Outlook Web Access) ed Exchange-Exchange non sono supportate.

Nota: In Microsoft Outlook 2007 la crittografia è attivata per impostazione predefinita. Per sfruttare i vantaggi dell'acceleratore applicazioni MAPI, è necessario disabilitare la crittografia. In Outlook scegliere **Strumenti > Account di posta elettronica**, **Visualizza o cambia gli account di posta elettronica esistenti** e quindi fare clic su **Avanti**. Scegliere l'account di Exchange e quindi fare clic su **Cambia**. Fare clic su **Altre impostazioni** e quindi sulla scheda **Protezione**. Deselezionare la casella di controllo **Crittografa dati tra Microsoft Office Outlook e Microsoft Exchange Server**, come mostrato nella Figura 1.

In alternativa, è possibile disattivare la crittografia per tutti gli utenti di un server di Exchange utilizzando Criteri di gruppo.

Figura 1. Disattivazione della crittografia in Outlook 2007



Nei casi seguenti, l'oggetto attivazione MAPI non gestisce una connessione:

- Connessione crittografata (consegnata all'oggetto attivazione generico)
- Client non supportato (consegnato all'oggetto attivazione generico)
- Errore di analisi irreversibile. Tutte le connessioni TCP tra il servizio client e il servizio server sono disconnesse. Quando il client si riconnette, tutte le connessioni vengono passate all'oggetto attivazione generico.
- Il client tenta di stabilire un nuovo gruppo di associazioni sulla connessione quando WAE è sovraccarico.
- Il client stabilisce una connessione quando WAE è sovraccarico e le risorse di connessione riservate MAPI non sono disponibili.

Il client e il server di Outlook interagiscono in una sessione tramite un gruppo di connessioni TCP denominato gruppo di associazione. All'interno di un gruppo di associazione, gli accessi agli oggetti possono estendersi su qualsiasi connessione e le connessioni vengono create e rilasciate in modo dinamico in base alle esigenze. Un client può avere più di un gruppo di associazione aperti contemporaneamente su server diversi o sullo stesso server. Le cartelle pubbliche vengono distribuite in server diversi dall'archivio della posta.

Èessenziale che tutte le connessioni MAPI all'interno di un gruppo di associazione passino attraverso la stessa coppia di WAE nella filiale e nel centro dati. Se alcune connessioni all'interno di un gruppo di associazione non passano attraverso l'oggetto attivazione MAPI in questi oggetti WAE, l'oggetto attivazione MAPI non vedrà le transazioni eseguite su tali connessioni e le connessioni verranno definite come "escape" per il gruppo di associazione. Per questo motivo, l'oggetto attivazione MAPI non deve essere distribuito in WAE in linea con cluster seriali che costituiscono un gruppo a disponibilità elevata.

I sintomi delle connessioni MAPI che sfuggono al gruppo di associazioni WAE sono sintomi di errore di Outlook, ad esempio messaggi duplicati o l'interruzione della risposta di Outlook.

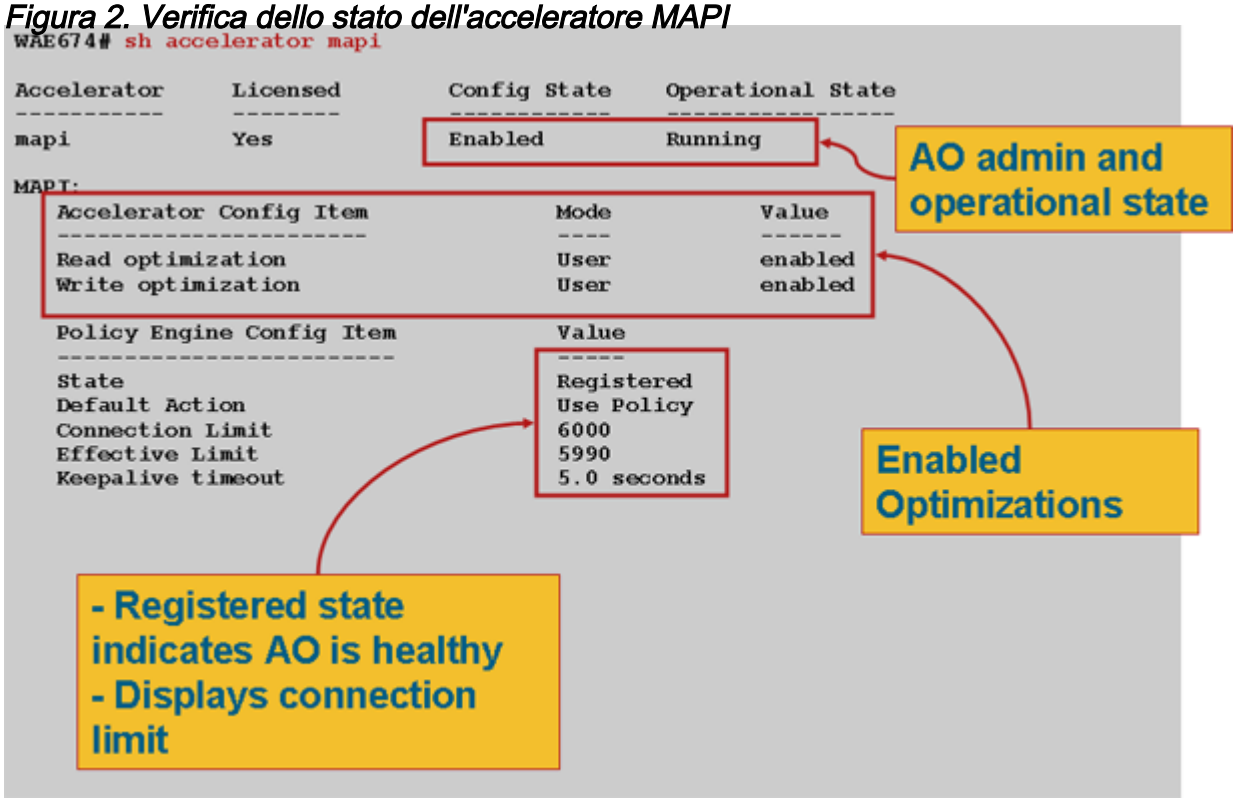
Durante una condizione di sovraccarico TFO, le nuove connessioni per un gruppo di associazioni esistente vengono passate attraverso l'oggetto attivazione (AO) MAPI e ne viene eseguita l'escape, pertanto l'oggetto attivazione MAPI riserva in anticipo una serie di risorse di connessione

per ridurre al minimo l'impatto di una condizione di sovraccarico. Per ulteriori informazioni sulle connessioni MAPI riservate e sul relativo impatto sul sovraccarico del dispositivo, vedere la sezione "Impatto delle connessioni riservate di MAPI Application Accelerator sull'overload" nell'articolo Risoluzione dei problemi relativi alle condizioni di sovraccarico.

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. La licenza Enterprise è necessaria per il funzionamento dell'acceleratore MAPI e l'acceleratore applicazione EPM deve essere abilitato.

Verificare quindi lo stato specifico dell'oggetto attivazione MAPI utilizzando il comando **show accelerator mapi**, come mostrato nella Figura 2. Si desidera verificare che l'oggetto attivazione, esecuzione e registrazione dell'oggetto attivazione MAPI e che venga visualizzato il limite di connessioni. Se lo stato della configurazione è Abilitato ma lo stato operativo è Chiuso, è presente un problema di licenza.

Figura 2. Verifica dello stato dell'acceleratore MAPI



Utilizzare il comando **show statistics accelerator epm** per verificare che EPM AO funzioni. Verificare che i contatori Totale connessioni gestite, Totale richieste analizzate correttamente e Totale risposte analizzate correttamente aumentino all'avvio di un client.

Utilizzare il comando **show running-config** per verificare che i criteri di traffico MAPI e EPM siano configurati correttamente. Per visualizzare l'azione **accelera** l'**API** per l'applicazione di posta elettronica e messaggistica, visualizzare il classificatore MS-EndPortMapper e i criteri del traffico definiti, come indicato di seguito:

```
WAE674# sh run | include mapi
map adaptor EPM mapi
 name Email-and-Messaging All action optimize full accelerate mapi

WAE674# sh run | begin MS-EndPointMapper
...skipping
classifier MS-EndPointMapper
```

```
  match dst port eq 135
exit

WAE674# sh run | include MS-EndPointMapper
  classifier MS-EndPortMapper
    name Other classifier MS-EndPortMapper action optimize DRE no compression none accelerate
MS-port-mapper
```

Utilizzare il comando **show policy-engine application dynamic** per verificare l'esistenza di regole di corrispondenza dinamiche, come indicato di seguito:

- Cerca una regola con ID utente: Nome EPM e Map: uida4f1db00-ca47-1067-b31f-00dd010662da.
- Il campo Flussi indica il numero totale di connessioni attive al servizio di Exchange.
- Per ogni client MAPI dovrebbe essere visualizzata una voce separata con l'ID utente: MAPI

Utilizzare il comando **show statistics connection optimized mapi** per verificare che il dispositivo WAAS stabilisca connessioni MAPI ottimizzate. Verificare che nella colonna Accel per le connessioni MAPI sia visualizzato "M", a indicare che è stato utilizzato l'oggetto attivazione MAPI, come indicato di seguito:

```
WAE674# show stat conn opt mapi

Current Active Optimized Flows:                       2
 Current Active Optimized TCP Plus Flows:          1
 Current Active Optimized TCP Only Flows:          1
 Current Active Optimized TCP Preposition Flows:   0
Current Active Auto-Discovery Flows:                  0
Current Reserved Flows:                               12              <---------- Added in 4.1.5
Current Active Pass-Through Flows:                    0
Historical Flows:                                     161


D:DRE,L:LZ,T:TCP Optimization RR:Total Reduction Ratio
A:AOIM,C:CIFS,E:EPM,G:GENERIC,H:HTTP,M:MAPI,N:NFS,S:SSL,V:VIDEO

ConnID  Source IP:Port         Dest IP:Port        PeerID           Accel RR
342     10.56.94.101:4506    10.10.100.100:1456  0:1a:64:d3:2f:b8   TMDL  61.0%   <-----Look for
"M"
```

Nota: Nella versione 4.1.5 è stato aggiunto nell'output il contatore dei flussi riservati correnti. Questo contatore si riferisce al numero di risorse di connessione MAPI riservate su WAE che sono attualmente inutilizzate ma messe da parte per future connessioni MAPI. Per ulteriori informazioni sulle connessioni MAPI riservate e sul relativo impatto sul sovraccarico del dispositivo, vedere la sezione "Impatto delle connessioni riservate di MAPI Application Accelerator sull'overload" nell'articolo Risoluzione dei problemi relativi alle condizioni di sovraccarico.

Se nella colonna Accel vengono osservate connessioni con "TGDL", tali connessioni sono state spostate verso il basso nell'oggetto attivazione generico e ottimizzate solo con le ottimizzazioni di trasporto. Se si prevede che queste connessioni verranno gestite dall'oggetto attivazione MAPI, è possibile che si tratti di connessioni MAPI crittografate. Per controllare il numero di connessioni MAPI crittografate richieste, utilizzare il comando **show statistics accelerator mapi** come segue:

```
wae# sh stat accel mapi
```

```
MAPI:
Global Statistics
-----------------
Time Accelerator was started:                                    Thu Nov  5 19:45:19 2009
Time Statistics were Last Reset/Cleared:                         Thu Nov  5 19:45:19 2009
Total Handled Connections:                                       8615
Total Optimized Connections:                                     8614
Total Connections Handed-off with Compression Policies Unchanged:  0
Total Dropped Connections:                                       1
Current Active Connections:                                      20
Current Pending Connections:                                     0
Maximum Active Connections:                                      512
Number of Synch Get Buffer Requests:                             1052
Minimum Synch Get Buffer Size (bytes):                           31680
Maximum Synch Get Buffer Size (bytes):                           31680
Average Synch Get Buffer Size (bytes):                           31680
Number of Read Stream Requests:                                  3844
Minimum Read Stream Buffer Size (bytes):                         19
Maximum Read Stream Buffer Size (bytes):                         31744
Average Read Stream Buffer Size (bytes):                         14556
Minimum Accumulated Read Ahead Data Size (bytes):                0
Maximum Accumulated Read Ahead Data Size (bytes):                1172480
Average Accumulated Read Ahead Data Size (bytes):                594385
Local Response Count:                                            20827
Average Local Response Time (usec):                              250895
Remote Response Count:                                           70486
Average Remote Response Time (usec):                             277036
Current 2000 Accelerated Sessions:                               0
Current 2003 Accelerated Sessions:                               1
Current 2007 Accelerated Sessions:                               0
Secured Connections:                                             1               <-----
Encrypted connections
Lower than 2000 Sessions:                                        0
Higher than 2007 Sessions:                                       0
```

Èpossibile trovare gli indirizzi IP dei client che richiedono connessioni MAPI crittografate nel syslog cercando messaggi come i seguenti:

```
2009 Jan 5 13:11:54 WAE512 mapi_ao: %WAAS-MAPIAO-3-132104: (929480) Encrypted connection. Client
ip: 10.36.14.82
```

Èpossibile visualizzare le statistiche della connessione MAPI utilizzando il comando **show statistics connection optimized mapi detail** nel modo seguente:

```
WAE674# show stat conn opt mapi detail
Connection Id:            1830
 Peer Id:                  00:14:5e:84:24:5f
 Connection Type:          EXTERNAL CLIENT
 Start Time:               Thu Jun 25 06:32:27 2009
 Source IP Address:        10.10.10.10
 Source Port Number:       3774
 Destination IP Address:   10.10.100.101
 Destination Port Number:  1146
 Application Name:         Email-and-Messaging                          <-----Should see
Email-and-Messaging
 Classifier Name:          **Map Default**
 Map Name:                 uuida4f1db00-ca47-1067-b31f-00dd010662da      <-----Should see this
UUID
```

```
 Directed Mode:            FALSE
 Preposition Flow:         FALSE
 Policy Details:
        Configured:        TCP_OPTIMIZE + DRE + LZ
           Derived:        TCP_OPTIMIZE + DRE + LZ
              Peer:        TCP_OPTIMIZE + DRE + LZ
        Negotiated:        TCP_OPTIMIZE + DRE + LZ
           Applied:        TCP_OPTIMIZE + DRE + LZ
 Accelerator Details:
             Configured:   MAPI                                    <-----Should see MAPI
configured
                Derived:   MAPI
                Applied:   MAPI                                    <-----Should see MAPI
applied
                   Hist:   None
                                        Original           Optimized
                                -------------------- --------------------
 Bytes Read:                                  4612                1973
 Bytes Written:                               4086                2096
. . .
```

Il conteggio delle risposte locali e remote e i tempi medi di risposta sono mostrati in questo output:

```
 . . .
MAPI : 1830

 Time Statistics were Last Reset/Cleared:                          Thu Jun 25
06:32:27 2009
 Total Bytes Read:                                               46123985
 Total Bytes Written:                                            40864046
Number of Synch Get Buffer Requests:                              0
Minimum Synch Get Buffer Size (bytes):                            0
Maximum Synch Get Buffer Size (bytes):                            0
Average Synch Get Buffer Size (bytes):                            0
Number of Read Stream Requests:                                   0
Minimum Read Stream Buffer Size (bytes):                          0
Maximum Read Stream Buffer Size (bytes):                          0
Average Read Stream Buffer Size (bytes):                          0
Minimum Accumulated Read Ahead Data Size (bytes):                 0
Maximum Accumulated Read Ahead Data Size (bytes):                 0
Average Accumulated Read Ahead Data Size (bytes):                 0
Local Response Count:                                             0                  <---------
-
Average Local Response Time (usec):                               0                  <---------
-
Remote Response Count:                                            19                 <---------
-
Average Remote Response Time (usec):                              89005              <---------
-
. . .
```

Accelerazione MAPI crittografata

Riepilogo

A partire dalla versione WAAS 5.0.1, l'acceleratore MAPI può accelerare il traffico MAPI crittografato. Questa funzione viene attivata per default nella release 5.0.3. Tuttavia, per accelerare correttamente il traffico MAPI crittografato, esistono diversi requisiti sia nell'ambiente WAAS che in quello Microsoft AD. Questa guida consente di verificare e risolvere i problemi relativi alle funzionalità eMAPI.

Informazioni sulle funzionalità

eMAPI verrà abilitato per impostazione predefinita nella versione 5.0.3 e richiederà quanto segue per accelerare correttamente il traffico crittografato.

1) L'archivio sicuro CMS deve essere inizializzato e aperto su tutti i componenti WAE di base

2) I WAE devono essere in grado di risolvere il nome di dominio completo dei server Exchange e del controller di dominio primario Kerberos (controller di Active Directory)

3) Gli orologi WAE devono essere sincronizzati con il KDC

4) SSL Accelerator, WAN Secure ed eMAPI devono essere abilitati su tutti i server WAE nel percorso da Outlook a Exchange

5) I WAE nel percorso devono avere la configurazione della mappa dei criteri corretta

6) I servizi WAE di base devono avere una o più identità di dominio di servizi crittografati configurate (account utente o computer)

7) Se viene utilizzato un account computer, questo WAE deve essere aggiunto al dominio AD.

8) Quindi, con lo use case dell'account computer o utente, è necessario assegnare autorizzazioni specifiche a tali oggetti in Active Directory. Le opzioni "Replica modifiche directory" e "Replica tutte le modifiche directory" devono essere entrambe impostate su Consenti.

Il modo consigliato per eseguire questa operazione è tramite un gruppo di protezione universale (ad esempio, assegnare le autorizzazioni al gruppo e quindi aggiungere al gruppo i dispositivi WAAS e/o i nomi utente specificati nel servizio di crittografia). Vedere la guida allegata per gli screenshot della configurazione di AD e dell'interfaccia grafica di WAAS CM.

Metodologia di risoluzione dei problemi

Passaggio 1 - Verificare la configurazione dell'identità del servizio di crittografia e il recupero della chiave

Mentre il comando di diagnostica (passaggio 2 riportato di seguito) verifica l'esistenza di un servizio di crittografia, non verifica se il recupero della chiave verrà eseguito correttamente. Non è pertanto possibile stabilire se, eseguendo semplicemente il comando di diagnostica, sono state concesse le autorizzazioni appropriate all'oggetto in Active Directory (account computer o utente).

Riepilogo delle operazioni da eseguire per configurare e verificare che il servizio di crittografia riesca a recuperare la chiave

Account utente:

1. creare un utente AD

2. creare un gruppo AD e impostare "Replica modifiche directory" e "Replica modifiche directory

tutte" su ALLOW

3. aggiungere l'utente al gruppo creato

4. definire l'identità del dominio dell'account utente nei servizi di crittografia

5. esegui get key diagnostic cli

windows-domain diagnostics encryption-service get-key <FQDN server Exchange> <nome dominio>

Si noti che è consigliabile utilizzare il nome effettivo/reale del server Exchange configurato nel server e non un nome di dominio completo (FQDN) di tipo Bilanciamento carico di rete/VIP che potrebbe essere risolto in più server Exchange.

6. recupero della chiave completato

Esempio di successo:

pdi-7541-dc#windows-domain diagnostics encryption-service get-key pdidc-exchange1.pdidc.cisco.com pdidc.cisco.com

SPN pdidc-exchange1.pdidc.cisco.com, Nome dominio: pdidc.cisco.com

Recupero della chiave in corso.

pdi-7541-dc#windows-domain diagnostics encryption-service get-key pdidc-exchange1.pdidc.cisco.com pdidc.cisco.com

SPN pdidc-exchange1.pdidc.cisco.com, Nome dominio: pdidc.cisco.com

La chiave per pdidc-exchange1.pdidc.cisco.com risiede nella cache delle chiavi di memoria

Account computer

1. aggiungere dispositivi WAE di base al dominio AD

2.Creare il gruppo AD e impostare "Replica modifiche directory" e "Replica modifiche directory tutto" su ALLOW

3. aggiunta account computer al gruppo creata

4. configura i servizi di crittografia per l'utilizzo dell'account computer

5. Concedere un certo tempo per ottenere l'applicazione dei Criteri di gruppo al computer collegato o forzare l'applicazione dei Criteri di gruppo da AD. gpupdate /force.

6. esegui get key diagnostic cli

windows-domain diagnostics encryption-service get-key <FQDN server Exchange> <nome dominio>

Si noti che è consigliabile utilizzare il nome effettivo/reale del server Exchange configurato nel server e non un nome di dominio completo (FQDN) di tipo Bilanciamento carico di rete/VIP che potrebbe essere risolto in più server Exchange.

7. recupero della chiave completato

Per ulteriori dettagli e schermate sul servizio di crittografia e sulla configurazione di AD, vedere la guida allegata.

2 - Nella versione 5.0.3 è stato introdotto un nuovo comando di diagnostica per controllare alcune delle impostazioni richieste.

–impostazioni di crittografia per la verifica delle API accelerator

1.CLI esegue diversi controlli di validità. L'output è un riepilogo della capacità di accelerare il traffico MAPI crittografato come edge o core.

2.Controlla lo stato e gli attributi di configurazione dei vari componenti per verificare che il servizio di crittografia funzioni correttamente.

3. Quando viene rilevato un problema di configurazione, viene generato l'output di ciò che manca e la CLI o le azioni per risolverlo.

4.It fornisce il riepilogo come dispositivo Edge e dispositivo Core. I dispositivi che possono essere sia edge che core devono avere EMAPI operativo sia per edge che core.

Di seguito viene riportato un esempio di output di un WAE configurato in modo errato:

```
Core#accelerator mapi verify encryption-settings
[EDGE:]
 Verifying Mapi Accelerator State
 --------------------------------
        Status: FAILED
        Accelerator     Config State    Operational State
        -----------     ------------    -----------------
        mapi            Disabled        Shutdown
        >>Mapi Accelerator should be Enabled
        >>Mapi Accelerator should be in Running state

 Verifying SSL Accelerator State
 -------------------------------
        Status: FAILED
        >>Accelerator   Config State    Operational State
        -----------     ------------    -----------------
        ssl             Disabled        Shutdown
        >>SSL Accelerator should be Enabled
        >>SSL Accelerator should be in Running state

 Verifying Wan-secure State
 --------------------------
        Status: FAILED
        >>Accelerator   Config State    Operational State
        -----------     ------------    -----------------
        wan-secure      Disabled        Shutdown
        >>Wan-secure should be Enabled
        >>Wan-secure should be in Running state
```

```
Verifying Mapi Wan-secure mode Setting
 --------------------------------
        Status: FAILED
        Accelerator Config Item                 Mode            Value
        -----------------------                 ----            ------
        WanSecure Mode                          User            Not Applicable
        >>Mapi wan-secure setting should be auto/always
 Verifying NTP State
 --------------------
       Status: FAILED
       >>NTP status should be enabled and configured

Summary [EDGE]:
 ===============
      Device has to be properly configured for one or more components

[CORE:]
Verifying encryption-service State
 ---------------------------------
        Status: FAILED
        Service                 Config State    Operational State
        -----------             ------------    -----------------
        Encryption-service      Disabled        Shutdown
        >>Encryption Service should be Enabled
       >>Encryption Service status should be in 'Running' state

Verifying Encryption-service Identity Settings
 -----------------------------------------------
        Status: FAILED
        >>No active Encryption-service Identity is configured.
        >>Please configure an active Windows Domain Encryption Service Identity.

 Summary [CORE]: Applicable only on CORE WAEs
 ============================================
        Device has to be properly configured for one or more components
```

Di seguito viene riportato l'output di un WAE Core configurato correttamente:

```
Core#acc mapi verify encryption-settings [EDGE:]

Verifying Mapi Accelerator State
--------------------------------
       Status: OK
Verifying SSL Accelerator State
--------------------------------
       Status: OK
Verifying Wan-secure State
```

```
-------------------------
       Status: OK
Verifying Mapi encryption Settings
----------------------------------
       Status: OK
Verifying Mapi Wan-secure mode Setting
----------------------------------
       Status: OK
Verifying NTP State
--------------------
       Status: OK
Summary [EDGE]:
===============
       Device has proper configuration to accelerate encrypted traffic

[CORE:]

Verifying encryption-service State
----------------------------------
       Status: OK
Verifying Encryption-service Identity Settings
-------------------------------------------
       Status: OK
Summary [CORE]: Applicable only on CORE WAEs
============================================
       Device has proper configuration to accelerate encrypted traffic
```

Passaggio 3 - Verificare manualmente le impostazioni WAE che non sono controllate dal comando di diagnostica precedente.

1) Il comando precedente, durante la verifica dell'esistenza di NTP configurato, non verifica effettivamente che i tempi siano sincronizzati tra WAE e KDC. È molto importante che i tempi siano sincronizzati tra Core e KDC per il corretto recupero della chiave.

Se il controllo manuale rivela che non sono sincronizzati, un modo semplice per forzare la sincronizzazione dell'orologio del WAE è tramite il comando ntpdate (**ntpdate <KDC ip>**). Quindi puntare il WAE al server NTP aziendale.

2) Verificare che **dnslookup** riesca su tutti i server WAE per il nome di dominio completo (FQDN) dei server Exchange e il nome di dominio completo (FQDN) dei KDC

3) Verificare che la mappa delle classi e la mappa dei criteri siano configurate correttamente su tutti i WAE nel percorso.

pdi-7541-dc#sh class-map type wa MAPI

Il tipo di mappa delle classi è match-any MAPI

Corrispondenza con epm mapi di destinazione tcp (0 corrispondenze di flusso)

pdi-7541-dc#show policy-map type waas Tipo di mappa criteri

WAAS-GLOBAL (6084690 in totale)

MAPI di classe (0 corrispondenze di flusso)
ottimizzazione dell'applicazione mapi accelerazione completa della posta elettronica e della messaggistica

4) Verificare che l'archivio protetto CMS sia aperto e inizializzato su tutti i WAE "show cms secure store"

Analisi dei dati

Oltre ad analizzare l'output del comando di diagnostica e i comandi show manuali, potrebbe essere necessario rivedere il sysreport.

In particolare, si desidera esaminare i file mapiao-errorlog, sr-errorlog (solo WAE core) e wsao-errorlog.

Ogni registro conterrà alcuni suggerimenti a seconda dello scenario che determinerà il motivo per cui le connessioni passano a un oggetto attivazione generico.

Di seguito è riportato un esempio di output con vari componenti di lavoro

Questo output proviene da sr-errorlog e mostra la convalida dell'identità del servizio di crittografia dell'account computer

Nota: Ciò conferma solo che il componente WAE principale è stato aggiunto al dominio e che l'account computer esiste.

```
07/03/2012 19:12:07.278(Local)(6249 1.5) NTCE (278902) Adding Identity MacchineAcctWAAS to map
active list in SRMain [SRMain.cpp:215]
07/03/2012 19:12:07.279(Local)(6249 1.5) NTCE (279018) Adding identity(MacchineAcctWAAS) to Map
[SRDiIdMgr.cpp:562]
07/03/2012 19:12:07.279(Local)(6249 1.5) NTCE (279282) Activate Id: MacchineAcctWAAS
[SRMain.cpp:260]
07/03/2012 19:12:07.279(Local)(6249 1.5) NTCE (279306) Identity MacchineAcctWAAS found in the
Map [SRDiIdMgr.cpp:702]
07/03/2012 19:12:07.279(Local)(6249 1.5) NTCE (279321) Authentication for ID: MacchineAcctWAAS
[SRDiIdMgr.cpp:398]
07/03/2012 19:12:07.330(Local)(6249 1.5) NTCE (330581) Authentication success, tkt validity
starttime 1341342727 endtime 1341378727 [SRDiIdMgr.cpp:456]
07/03/2012 19:12:07.330(Local)(6249 1.5) NTCE (330599)
ID_TAG :MacchineAcctWAAS
Name : pdi-7541-dc
Domain : PDIDC.CISCO.COM
Realm : PDIDC.CISCO.COM
CLI_GUID :
```

```
SITE_GUID :
CONF_GUID :
Status:ENABLED
Black_Listed:NO
AUTH_STATUS: SUCCESS
ACCT_TYPE:Machine [SRIdentityObject.cpp:85]
07/03/2012 19:12:07.331(Local)(6249 1.5) NTCE (331685) DN Info found for domain PDIDC.CISCO.COM
[SRIdentityObject.cpp:168]
07/03/2012 19:12:07.347(Local)(6249 1.5) NTCE (347680) Import cred successfull for pn: pdi-7541-
dc@PDIDC.CISCO.COM [AdsGssCli.cpp:111]
```

Questo output viene nuovamente generato dal registro errori di Core sr e indica che il recupero della chiave da KDC è riuscito.

```
10/23/2012 15:46:55.673(Local)(3780 1.2) NTCE (673766) Key Not Found in cache, initiating
retrieval for spn:exchangeMDB/pdidc-exchange1.pdidc.cisco.com [SRServer.cpp:297]
10/23/2012 15:46:55.673(Local)(3780 1.2) NTCE (673811) Queued InitiateKeyRetrieval task
[SRServer.cpp:264]10/23/2012 15:46:55.673(Local)(3780 1.2) NTCE (673819)
Key retrieval is in Progress [SRServer.cpp:322]
10/23/2012 15:46:55.673(Local)(3780 0.0) NTCE (673818) Initiating key retrieval
[SRServer.cpp:271]
10/23/2012 15:46:55.673(Local)(3780 1.2) NTCE (673827) initiating key retrieval in progress
[SRDataServer.cpp:441]
10/23/2012 15:46:55.673(Local)(3780 1.2) NTCE (673834) Sending ack for result 2, item name
/cfg/gl/sr/sr_get_key/pdidc-exchange1.pdidc.cisco.com@pdidc.cisco.com
[SRDataServer.cpp:444]
10/23/2012 15:46:55.673(Local)(3780 0.0) NTCE (673922) Match found for DN: pdidc.cisco.com is
ID:MacchineAcctWAAS [SRDiIdMgr.cpp:163]
10/23/2012 15:46:55.673(Local)(3780 0.0) NTCE (673937) Identity MacchineAcctWAAS found in the
Map [SRDiIdMgr.cpp:702]
10/23/2012 15:46:55.673(Local)(3780 0.0) NTCE (673950) DN Info found for domain pdidc.cisco.com
[SRIdentityObject.cpp:168]
10/23/2012 15:46:55.674(Local)(3780 0.0) NTCE (674011) DRS_SPN: E3514235-4B06-11D1-AB04-
00C04FC2DCD2/e4c83c51-0b59-4647-b45d-780dd2dc3344/PDIDC.CISCO.COM for
PDI-7541-DC@PDIDC.CISCO.COM [GssCli.cpp:51]
10/23/2012 15:46:55.674(Local)(3780 0.0) NTCE (674020) CREATED srkr obj(0x50aa00) for spn
(exchangeMDB/pdidc-exchange1.pdidc.cisco.com) [SRKeyMgr.cpp:134]
10/23/2012 15:46:55.674(Local)(3780 1.3) NTCE (674421) Import cred successfull for pn: PDI-7541-
DC@PDIDC.CISCO.COM [GssCli.cpp:135]
10/23/2012 15:46:55.676(Local)(3780 1.3) NTCE (676280) session(0x50aa00) Complete TGT stage of
GSS Successful, Initiating AppApi [SRKeyRetriever.cpp:408]
10/23/2012 15:46:55.676(Local)(3780 0.1) NTCE (676415) SRKR: Success in posting connect to
service <ip:0e:6e:03:a3><port:135> [IoOperation.cpp:222]
10/23/2012 15:46:55.676(Local)(3780 0.0) NTCE (676607) Connected to server.
[IoOperation.cpp:389]
10/23/2012 15:46:55.677(Local)(3780 0.0) NTCE (677736) SRKR: Success in posting connect to
service <ip:0e:6e:03:a3><port:1025> [IoOperation.cpp:222]
10/23/2012 15:46:55.678(Local)(3780 0.1) NTCE (678001) Connected to server.
[IoOperation.cpp:389]
10/23/2012 15:46:55.679(Local)(3780 0.1) NTCE (679500) Cleaning up credential cache for PDI-
```

```
7541-DC@PDIDC.CISCO.COM [GssCli.cpp:212]
10/23/2012 15:46:55.680(Local)(3780 0.1) NTCE (680011) Parsing DRSBIND Response
[AppApiDrsBind.cpp:222]
10/23/2012 15:46:55.680(Local)(3780 0.1) NTCE (680030) DRSBind Success, Status:00000000
[AppApiDrsBind.cpp:359]
10/23/2012 15:46:55.685(Local)(3780 0.1) NTCE (685502) session(0x50aa00) Successful in Key
Retrieval from AD for SPN:exchangeMDB/pdidc-exchange1.pdidc.cisco.com
[SRKeyRetriever.cpp:269]
10/23/2012 15:46:55.685(Local)(3780 0.1) NTCE (685583) Send Key response to the Client for spn:
exchangeMDB/pdidc-exchange1.pdidc.cisco.com, # of req's : 1
[SRKeyMgr.cpp:296]
10/23/2012 15:46:55.685(Local)(3780 0.1) NTCE (685594) Deleting spn: exchangeMDB/pdidc-
exchange1.pdidc.cisco.com entry from Pending key request map [SRKeyMgr.cpp:303]
```

Questo output viene generato dal file mapiao-errorlog su Edge WAE per una connessione eMAPI riuscita

```
'''10/23/2012 17:56:23.080(Local)(8311 0.1) NTCE (80175) (fl=2433) Edge TCP connection initiated
(-1409268656), Conn: [14.110.3.117:58352 <=> 14.110.3.99:27744],
Flavor: 0 [EdgeTcpConnectionDceRpcLayer.cpp:43]
10/23/2012 17:56:23.080(Local)(8311 0.1) NTCE (80199) Edge TCP connection initiated (-
1409268656), Conn: [14.110.3.117:58352 <=> 14.110.3.99:27744], Flavor: 0
[EdgeTcpConnectionDceRpcLayer.cpp:48]
10/23/2012 17:56:23.108(Local)(8311 0.0) NTCE (108825) (fl=2433) Bind Request from client with
AGID 0x0, callId 2, to dest-ip 14.110.3.99, AuthLevel: PRIVACY
AuthType: SPNEGO AuthCtxId: 0 WsPlumb:1
[EdgeTcpConnectionDceRpcLayer.cpp:1277]'''
10/23/2012 17:56:23.109(Local)(8311 0.0) NTCE (109935) CheckAndDoAoshReplumbing perform
replumbing wsPlumbState 1 [Session.cpp:315]
10/23/2012 17:56:23.109(Local)(8311 0.0) NTCE (109949) (fl=2433) AOSH Replumbing was performed
returned Status 0 [Session.cpp:337]
10/23/2012 17:56:23.109(Local)(8311 0.0) NTCE (109956) CheckAndPlumb WanSecure(14) ret:= [1,0]
WsPlumb:4 fd[client,server]:=[25,26] [AsyncOperationsQueue.cpp:180]
10/23/2012 17:56:23.312(Local)(8311 0.1) NTCE (312687) (fl=2433) Connection multiplexing enabled
by server on the connection. [EdgeTcpConnectionDceRpcLayer.cpp:499]
10/23/2012 17:56:23.312(Local)(8311 0.1) NTCE (312700) (fl=2433) Header signing enabled by
server on the connection. [EdgeTcpConnectionDceRpcLayer.cpp:510]
10/23/2012 17:56:23.312(Local)(8311 0.1) NTCE (312719) (fl=2433) OnNewConnection - Client IP
14.110.3.117 (0xe6e0375), Serv IP 14.110.3.99 (0xe6e0363), nDstPort=27744,
nAssociationGroup=0x11de4,conn_fd=26,
bWasConnectionFromReservedPool=0, bIsNewMapiSession=1 [ConnectionReservationManager.cpp:255]
'''10/23/2012 17:56:23.366(Local)(8311 0.1) NTCE (366789) (fl=2433) Received security context
from core with auth context id: 0 [EdgeTcpConnectionDceRpcLayer.cpp:2912]
10/23/2012 17:56:23.367(Local)(8311 0.1) NTCE (367157) (fl=2433) Security Layer moved to ESTB
state [FlowSecurityLayer.cpp:311]'''
10/23/2012 17:56:23.368(Local)(8311 0.1) NTCE (368029) (fl=2433) Informational:: Send APC set to
WS: asking for Cipher 2 [EdgeTcpConnectionDceRpcLayer.cpp:809]
10/23/2012 17:56:23.368(Local)(8311 0.1) NTCE (368041) (fl=2433) Sec-Params [CtxId, AL, AT, ACT,
DCT, [Hs, ConnMplx, SecMplx]]:=[0, 6, 9, 18, 18 [1,1,0]]
```

```
[FlowIOBuffers.cpp:477]
10/23/2012 17:56:23.369(Local)(8311 0.0) NTCE (369128) (fl=2433)
CEdgeTcpConnectionEmsMdbLayer::ConnectRequestCommon (CallId 2): client version is
ProductMajor:14,
Product Minor:0, Build Major:6117,
Build Minor:5001 Client ip 14.110.3.117 Client port 58352 Dest ip 14.110.3.99 Dest port 27744
[EdgeTcpConnectionEmsMdbLayer.cpp:1522]
10/23/2012 17:56:23.868(Local)(8311 0.1) ERRO (868390) (fl=2433) ContextHandle.IsNull()
[EdgeTcpConnectionEmsMdbLayer.cpp:1612]
10/23/2012 17:56:23.890(Local)(8311 0.0) NTCE (890891) (fl=2433)
CEdgeTcpConnectionEmsMdbLayer::ConnectRequestCommon (CallId 3): client version is
ProductMajor:14,
Product Minor:0, Build Major:6117,
Build Minor:5001 Client ip 14.110.3.117 Client port 58352 Dest ip 14.110.3.99 Dest port 27744
[EdgeTcpConnectionEmsMdbLayer.cpp:1522]
```

Di seguito è riportato l'output WAE dei core corrispondente da mapiao-errorlog per la stessa connessione TCP

```
'''10/23/2012 17:56:54.092(Local)(6408 0.0) NTCE (92814) (fl=21) Core TCP connection initiated
(11892640), Conn: [14.110.3.117:58352 <=> 14.110.3.99:27744], F
lavor: 0 [CoreTcpConnectionDceRpcLayer.cpp:99]
10/23/2012 17:56:54.092(Local)(6408 0.0) NTCE (92832) Core TCP connection initiated (11892640),
Conn: [14.110.3.117:58352 <=> 14.110.3.99:27744], Flavor: 0
[CoreTcpConnectionDceRpcLayer.cpp:104]'''
10/23/2012 17:56:54.175(Local)(6408 0.0) NTCE (175035) SrlibCache Cache eviction starting:
static void srlib::CSrlibCache:: OnAoShellDispatchCacheCleanup(vo
id*, aosh_work*) [SrlibCache.cpp:453]
10/23/2012 17:56:54.175(Local)(6408 0.0) NTCE (175068) last_cleanup_time (1344411860),
evict_in_progress(1) handled_req_cnt (1) cache_size (0) [SrlibCache.
cpp:464]
10/23/2012 17:56:54.175(Local)(6408 0.0) NTCE (175121) SendNextCmd isDuringSend 0, WriteQueue sz
1, isDuringclose 0 [SrlibClientTransport.cpp:163]
10/23/2012 17:56:54.175(Local)(6408 0.0) NTCE (175132) SendNextCmd: Sending request:
exchangeMDB/PDIDC-EXCHANGE1.pdidc.cisco.com:23[v:=11], WriteQueue sz 0
[bClose 0] [SrlibClientTransport.cpp:168]
10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185576) OnReadComplete len 4 status 0
isDuringRead 1, isDuringHeaderRead 1, isDuringclose 0 [SrlibTransport.
cpp:127]
10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185587) Parse header, msg body len 152
[SrlibTransport.cpp:111]
10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185592) ReadNextMsg isDuringRead 0,
isDuringHeaderRead 1, isDuringclose 0 [SrlibTransport.cpp:88]
10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185623) OnReadComplete len 148 status 0
isDuringRead 1, isDuringHeaderRead 0, isDuringclose 0 [SrlibTranspor
t.cpp:127]
```

```
'''10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185688) Insert new KrbKey: exchangeMDB/PDIDC-
EXCHANGE1.pdidc.cisco.com::23[v:=11]:[{e,f,l}:={0, 0x1, 16} [S
rlibCache.cpp:735]
'''10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185747) ReadNextMsg isDuringRead 0,
isDuringHeaderRead 0, isDuringclose 0 [SrlibTransport.cpp:88]
'''10/23/2012 17:56:54.261(Local)(6408 0.1) NTCE (261575) (fl=21) Successfully created memory
keytab with name: MEMORY:exchangeMDB@PDIDC-EXCHANGE1.pdidc.cisco
.com0nxrPblND [GssServer.cpp:468]
10/23/2012 17:56:54.261(Local)(6408 0.1) NTCE (261613) (fl=21) Successfully added entry in
memory keytab. [GssServer.cpp:92]
10/23/2012 17:56:54.261(Local)(6408 0.1) NTCE (261858) (fl=21) Successfully acquired
credentials. [GssServer.cpp:135]'''
```

Problemi comuni

Di seguito sono riportati alcuni motivi comuni che determinano la connessione eMAPI Consegna a Generic AO (TG).

Problema 1: L'identità del servizio di crittografia configurata in WAE di base non dispone delle autorizzazioni corrette in AD.

Output di sr-errolog su Core WAE

```
09/25/2012 18:47:54.147(Local)(9063 0.1) ERRO (147570) session(0x517fa0) Failed to Retrieve Key
from AD for SPN:exchangeMDB/outlook.sicredi.net.br error:16 [SRKeyRetriever.cpp:267]
'''09/25/2012 18:47:54.147(Local)(9063 0.1) ERRO (147592) Key retrieval failed with Status 16
[SRKeyMgr.cpp:157]
''''''09/25/2012 18:47:54.147(Local)(9063 0.1) ERRO (147623) Identity "WAASMacAct" has been
blacklisted [SRDiIdMgr.cpp:258]
''''''09/25/2012 18:47:54.147(Local)(9063 0.1) ERRO (147631) Key retrieval failed due to
permission issue [SRKeyMgr.cpp:167]
'''09/25/2012 18:47:54.147(Local)(9063 0.1) ERRO (147636) Identity: WAASMacAct will be black
listed. [SRKeyMgr.cpp:168]
09/25/2012 18:47:54.147(Local)(9063 0.1) NTCE (147657) Calling KrbKeyResponse  key handler in
srlib [SRServer.cpp:189]
09/25/2012 18:47:54.147(Local)(9063 0.1) NTCE (147722) Queued send reponse buffer to client task
[SrlibServerTransport.cpp:136]
09/25/2012 18:47:54.147(Local)(9063 0.1) NTCE (147730) KrbKeyResponse, sent to client session
object [SrlibServer.cpp:203]
09/25/2012 18:47:54.147(Local)(9063 0.0) NTCE (147733) SendNextCmd isDuringSend 0, WriteQueue
size 1 isDuringClose 0 [SrlibServerTransport.cpp:308]
09/25/2012 18:47:54.147(Local)(9063 0.1) NTCE (147740) Send Key response to the Client
```

Risoluzione 1: Consultare la guida alla configurazione e verificare che l'oggetto in Active Directory disponga delle autorizzazioni corrette. Le opzioni "Replica modifiche directory" e "Replica tutte le modifiche directory" devono essere entrambe impostate su Consenti.

http://www.cisco.com/en/US/docs/app_ntwk_services/waas/waas/v511/configuration/guide/policy.html#wp1256547

Problema 2: Si è verificato uno sfasamento temporale tra il Core WAE e il KDC dal quale viene eseguito il tentativo di recuperare la chiave

Output di sr-errolog su Core WAE

```
10/23/2012 01:31:33.507(Local)(1832 0.1) NTCE (507836) Initiating key retrieval
[SRServer.cpp:271]
10/23/2012 01:31:33.507(Local)(1832 0.1) NTCE (507878) Match found for DN: pdidc.cisco.com is
ID:MacchineAcctWAAS [SRDiIdMgr.cpp:163]
10/23/2012 01:31:33.507(Local)(1832 0.1) NTCE (507888) Identity MacchineAcctWAAS found in the
Map [SRDiIdMgr.cpp:702]
10/23/2012 01:31:33.507(Local)(1832 0.1) NTCE (507901) DN Info found for domain pdidc.cisco.com
[SRIdentityObject.cpp:168]
10/23/2012 01:31:33.507(Local)(1832 0.1) NTCE (507923) DRS_SPN: E3514235-4B06-11D1-AB04-
00C04FC2DCD2/e4c83c51-0b59-4647-b45d-780dd2dc3344/PDIDC.CISCO.COM for
PDI-7541-DC@PDIDC.CISCO.COM [GssCli.cpp:51]
10/23/2012 01:31:33.507(Local)(1832 0.1) NTCE (507933) CREATED srkr obj(0x2aaaac0008c0) for spn
(exchangeMDB/pdidc-exchange1.pdidc.cisco.com) [SRKeyMgr.cpp:134]
10/23/2012 01:31:33.508(Local)(1832 1.6) NTCE (508252) Import cred successfull for pn: PDI-7541-
DC@PDIDC.CISCO.COM [GssCli.cpp:135]
10/23/2012 01:31:33.511(Local)(1832 1.6) ERRO (511151) CreateSecurityContext:
gss_init_sec_context failed [majorStatus = 851968 (0xd0000)] [GssCli.cpp:176]
'''10/23/2012 01:31:33.511(Local)(1832 1.6) ERRO (511170) GSS_MAJOR ERROR:851968 msg_cnt:0,
Miscellaneous failure (see text)CD2 [GssCli.cpp:25]
10/23/2012 01:31:33.511(Local)(1832 1.6) ERRO (511177) GSS_MINOR ERROR:2529624064 msg_cnt:0,
Clock skew too great [GssCli.cpp:29]
10/23/2012 01:31:33.511(Local)(1832 1.6) ERRO (511182) gsskrb5_get_subkey failed: 851968,22,
[GssCli.cpp:198]
10/23/2012 01:31:33.511(Local)(1832 1.6) ERRO (511188) session(0x2aaaac0008c0) Error: Invalid
security ctx state, IsContinue is false with out token exchange
[SRKeyRetriever.cpp:386]
10/23/2012 01:31:33.511(Local)(1832 1.6) ERRO (511193) session(0x2aaaac0008c0) Failed to
Retrieve Key from AD for SPN:exchangeMDB/pdidc-exchange1.pdidc.cisco.com error:1
[SRKeyRetriever.cpp:267]'''
10/23/2012 01:31:33.511(Local)(1832 0.0) ERRO (511213) Key retrieval failed with Status 1
[SRKeyMgr.cpp:157]
```

Risoluzione 2: Utilizzare ntpdate su tutti i WAE (in particolare i Core) per sincronizzare l'orologio con il KDC. Quindi puntare al server NTP aziendale (preferibilmente lo stesso di KDC).

Problema 3: Il dominio definito per il servizio di crittografia non corrisponde al dominio in cui si trova il server Exchange.

Output di sr-errolog su Core WAE

```
10/23/2012 18:41:21.918(Local)(3780 1.5) NTCE (918788) Key retrieval is in Progress
[SRServer.cpp:322]
10/23/2012 18:41:21.918(Local)(3780 1.5) NTCE (918793) initiating key retrieval in progress
[SRDataServer.cpp:441]
10/23/2012 18:41:21.918(Local)(3780 0.0) NTCE (918790) Initiating key retrieval
[SRServer.cpp:271]
10/23/2012 18:41:21.918(Local)(3780 1.5) NTCE (918798) Sending ack for result 2, item name
/cfg/gl/sr/sr_get_key/pdidc-exchange.cisco.com@cisco.com [SRDataServer.cpp:444]
10/23/2012 18:41:21.918(Local)(3780 0.0) ERRO (918813) Failed to find Identity match for domain
cisco.com [SRDiIdMgr.cpp:157]
10/23/2012 18:41:21.918(Local)(3780 0.0) NTCE (918821) Failed to find identity match for domain
[SRKeyMgr.cpp:120]
10/23/2012 18:41:21.918(Local)(3780 0.0) NTCE (918832) Send Key response to the Client for spn:
exchangeMDB/pdidc-exchange.cisco.com, # of req's: 1 [SRKeyMgr.cpp:296]
```

Risoluzione 3: Se il server WAE di base supporta più server Exchange in domini diversi, è necessario configurare un'identità del servizio di crittografia per ogni dominio in cui risiedono i server Exchange.

Nota, al momento NON è disponibile il supporto per l'inclusione di sottodomini. Se si dispone di myexchange.sub-domain.domain.com, l'identità del servizio di crittografia deve trovarsi in sub-domain.domain.com; NON PUÒ trovarsi nel dominio padre.

Problema 4: Se WANSecure non riesce, le connessioni possono passare al TG

Le connessioni eMAPI possono essere trasferite a un oggetto attivazione generico a causa di un errore di PLUMB sicuro WAN. PLUMB di sicurezza WAN non riuscito. Verifica del certificato non riuscita. La verifica del certificato peer non riuscirà perché è in uso il certificato peer predefinito autofirmato o perché il controllo OCSP del certificato non è riuscito correttamente.

Impostazioni WAE core

```
crypto pki global-settings

  ocsp url http://pdidc.cisco.com/ocsp
revocation-check ocsp-cert-url
exit

!

crypto ssl services host-service peering
```

```
  peer-cert-verify
exit

!

WAN Secure:

  Accelerator Config Item              Mode           Value
-----------------------              ----           ------
SSL AO                               User           enabled
Secure store                         User           enabled
Peer SSL version                     User           default
Peer cipher list                     User           default
Peer cert                            User           default
Peer cert verify                     User           enabled
```

Di conseguenza, verranno restituite le seguenti voci mapiao-errorlog e wsao-errorlog:

Il suggerimento qui è la prima riga evidenziata "disconnessa più di quattro volte consecutive"

Mapiao-errorlog su WAE lato client:

```
'''10/08/2012 20:02:15.025(Local)(24333 0.0) NTCE (25621) (fl=267542) Client 10.16.1.201
disconnected more than four consecutive times - push down to generic ao.
[EdgeTcpConnectionDceRpcLayer.cpp:1443]
'''10/08/2012 20:02:15.025(Local)(24333 0.0) NTCE (25634) (fl=267542) CEdgeIOBuffers::
StartHandOverProcessSingleConnection: SECURED_STATE_NOT_ESTABLISHED
[EdgeIOBuffers.cpp:826]
10/08/2012 20:02:15.025(Local)(24333 0.0) NTCE (25644) (fl=267542)
CEdgeIOBuffers::CheckSendHandOverRequestToCoreAndBlockLan - Blocking LAN for read operations
after last
fragment of call id 0, current call id is 2 [EdgeIOBuffers.cpp:324]
10/08/2012 20:02:15.048(Local)(24333 0.1) NTCE (48753) (fl=267542) Connection multiplexing
enabled by server on the connection. [EdgeTcpConnectionDceRpcLayer.cpp:499]
10/08/2012 20:02:15.048(Local)(24333 0.1) NTCE (48771) (fl=267542) Header signing enabled by
server on the connection. [EdgeTcpConnectionDceRpcLayer.cpp:510]
10/08/2012 20:02:15.048(Local)(24333 0.1) NTCE (48779) (fl=267542) CEdgeIOBuffers::
StartHandOverProcessSingleConnection: GENERAL_UNCLASSIFIED [EdgeIOBuffers.cpp:826]
```

Wsao-errorlog su WAE lato client:

```
'''10/08/2012 20:04:34.430(Local)(5939 4.0) ERRO (430001) certificate verification failed 'self
signed certificate' [open_ssl.cpp:1213]
'''10/08/2012 20:04:34.430(Local)(5939 4.0) ERRO (430047) ssl_read failed: 'SSL_ERROR_SSL'
[open_ssl.cpp:1217]
10/08/2012 20:04:34.430(Local)(5939 4.0) ERRO (430055) openssl errors: error:14090086: SSL
routines: SSL3_GET_SERVER_CERTIFICATE:certificate verify failed:s3_clnt.c:1244:
[open_ssl.cpp:1220]
```

Risoluzione 4: Rimuovere la configurazione di verifica del certificato peer da entrambi i server WAE e riavviare il servizio di crittografia sui server WAE di base.

```
pdi-7541-dc(config)#crypto ssl services host-service peering

pdi-7541-dc(config-ssl-peering)#no peer-cert-verify

pdi-7541-dc(config)#no windows-domain encryption-service enable

pdi-7541-dc(config)#windows-domain encryption-service enable
```

Problema 5: Se NTLM viene utilizzato dal client Outlook, la connessione verrà spostata verso il basso a un oggetto attivazione generico.

Nel log degli errori di mapiao sul lato client WAE viene visualizzato quanto segue:

```
'''waas-edge#find-patter match ntlm mapiao-errorlog.current
'''
09/21/2012 20:30:32.154(Local)(8930 0.1) NTCE (154827) (fl=83271) Bind Request from client with
AGID 0x0, callId 1, to dest-ip 172.21. 12.96, AuthLevel:
PRIVACY '''AuthType:NTLM '''AuthCtxId: 153817840 WsPlumb: 2
[EdgeTcpConnectionDceRpcLayer.cpp:1277]
09/21/2012 20:30:32.154(Local)(8930 0.1) NTCE (154861) (fl=83271) '''Unsupported''' '''Auth
Type :NTLM''' [EdgeTcpConnectionDceRpcLayer.cpp:1401] 09/21/2012 20:30:40.157(Local)
(8930 0.0) NTCE (157628) (fl=83283) Bind Request from client with AGID 0x0, callId 2, to dest-ip
172.21. 12.96, AuthLevel: PRIVACY AuthType:NTLM AuthCtxId: 153817840
WsPlumb: 2 [EdgeTcpConnectionDceRpcLayer.cpp:1277]
```

Risoluzione 5: Il cliente deve abilitare o richiedere l'autenticazione Kerberos nel proprio ambiente Exchange. NTLM NON supportato (versione 5.1)

Tenere presente che è disponibile una descrizione tecnica di Microsoft che indica un fallback a NTLM quando si utilizza un server CAS.

Lo scenario in cui Kerberos non funziona è specifico di Exchange 2010 ed è il seguente:

Più server Accesso client (CAS) di Exchange in un'organizzazione/dominio.
Questi server CAS vengono raggruppati in cluster utilizzando qualsiasi metodo, utilizzando la funzione di array client integrata di Microsoft o un servizio di bilanciamento del carico di terze parti.

Nello scenario precedente, Kerberos non funziona e per impostazione predefinita i client eseguiranno il fallback a NTLM. Credo che ciò sia dovuto al fatto che i client devono eseguire l'autenticazione al server CAS rispetto al server Cassette postali, come nelle precedenti versioni di Exchange.

In Exchange 2010 RTM non è disponibile alcuna correzione. Nello scenario precedente, Kerberos non funzionerà mai prima di Exchange 2010-SP1.

In SP1 è possibile attivare Kerberos in questi ambienti, ma si tratta di un processo manuale. Vedere l'articolo qui: http://technet.microsoft.com/en-us/library/ff808313.aspx

Registrazione oggetti MAPI

- Per la risoluzione dei problemi relativi agli oggetti attivazione MAPI sono disponibili i file di registro seguenti:
- File di log delle transazioni: /local1/logs/tfo/working.log (e /local1/logs/tfo/tfo_log_*.txt)

File registro di debug: /local1/errorlog/mapiao-errorlog.current (e mapiao-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 indicato di seguito:

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

Èpossibile visualizzare la fine di un file di log delle transazioni utilizzando il comando type-tail nel modo seguente:

```
wae# type-tail tfo_log_10.10.11.230_20090715_130000.txt
Wed Jul 15 19:12:35 2009 :2289 :10.10.10.10 :3740 :10.10.100.101 :1146 :OT :END :EXTERNAL
CLIENT :(MAPI) :822 :634 :556 :706
Wed Jul 15 19:12:35
2009 :2289 :10.10.10.10 :3740 :10.10.100.101 :1146 :SODRE :END :730 :605 :556 :706 :0
Wed Jul 15 19:12:35 2009 :2290 :10.10.10.10 :3738 :10.10.100.101 :1146 :OT :END :EXTERNAL
CLIENT :(MAPI) :4758 :15914 :6436 :2006
Wed Jul 15 19:12:35
2009 :2290 :10.10.10.10 :3738 :10.10.100.101 :1146 :SODRE :END :4550 :15854 :6436 :2006 :0
Wed Jul 15 19:12:35 2009 :2284 :10.10.10.10 :3739 :10.10.100.101 :1146 :OT :END :EXTERNAL
CLIENT :(MAPI) :1334 :12826 :8981 :1031
```

Per impostare e abilitare la registrazione di debug dell'oggetto attivazione MAPI, 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 MAPI AO:

```
WAE674# debug accelerator mapi ?
all enable all MAPI accelerator debugs
Common-flow enable MAPI Common flow debugs
DCERPC-layer enable MAPI DCERPC-layer flow debugs
EMSMDB-layer enable MAPI EMSMDB-layer flow debugs
IO enable MAPI IO debugs
ROP-layer enable MAPI ROP-layer debugs
ROP-parser enable MAPI ROP-parser debugs
RPC-parser enable MAPI RPC-parser debugs
shell enable MAPI shell debugs
Transport enable MAPI transport debugs
Utilities enable MAPI utilities debugs
```

Èpossibile abilitare la registrazione di debug per le connessioni MAPI e quindi visualizzare la fine del log degli errori di debug come indicato di seguito:

```
WAE674# debug accelerator mapi Common-flow
WAE674# type-tail errorlog/mapiao-errorlog.current follow
```