

WAAS: resolución de problemas de MAPI AO

Capítulo: Resolución de problemas de MAPI AO

En este artículo se describe cómo resolver problemas de MAPI AO.

Co

[Art](#)
[Intr](#)
[trát](#)
[Re](#)
[Op](#)
[Re](#)
[apl](#)
[Re](#)
[Re](#)
[Re](#)
Re
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)
[Re](#)

Contenido

- [1 Acelerador MAPI](#)
- [2 Aceleración MAPI cifrada](#)
 - [2.1 Summary](#)
 - [2.2 Información sobre la Función](#)
 - [2.3 Metodología de solución de problemas](#)
 - [2.3.1 Paso 1 - Verificar la configuración de la identidad del servicio de cifrado y la recuperación de claves correcta](#)
 - [2.3.2 Paso 2 - En 5.0.3 se introdujo un nuevo comando de diagnóstico para verificar algunos de los ajustes requeridos.](#)
 - [2.3.3 Paso 3: verifique manualmente los parámetros de WAE que no están verificados por el comando de diagnóstico anterior.](#)
 - [2.4 Análisis de datos](#)
 - [2.5 Problemas Comunes](#)
 - [2.5.1 Problema 1: La identidad del servicio de cifrado configurada en el WAE de núcleo no tiene los permisos correctos en AD.](#)

- [2.5.2 Resolución 1: Consulte la guía de configuración y verifique que el objeto en AD tenga los permisos correctos. "Replicando cambios de directorio" y "Replicando cambios de directorio todo" deben configurarse para permitir.](#)
 - [2.5.3 Problema 2: Hay una desviación de tiempo entre el WAE de núcleo y el KDC del que intenta recuperar la clave](#)
 - [2.5.4 Resolución 2: Utilice la actualización en todos los dispositivos WAE \(especialmente en el núcleo\) para sincronizar el reloj con el KDC. A continuación, indique el servidor NTP de la empresa \(preferiblemente el mismo que el KDC\).](#)
 - [2.5.5 Problema 3: El dominio que definió para su servicio de cifrado no coincide con el dominio en el que se encuentra su servidor Exchange.](#)
 - [2.5.6 Resolución 3: Si su WAE central presta servicios a varios servidores Exchange en diferentes dominios, debe configurar una identidad de servicio de cifrado para cada dominio en el que residen los servidores Exchange.](#)
 - [2.5.7 Problema 4: Si WANSecure falla, las conexiones pueden caer a TG](#)
 - [2.5.8 Resolución 4: Elimine la configuración de verificación de certificado de peer de ambos WAE y reinicie el servicio de cifrado en los WAE de núcleo.](#)
 - [2.5.9 Problema 5: Si el cliente de Outlook utiliza NTLM, la conexión se enviará a Generic AO.](#)
 - [2.5.10 Resolución 5: El cliente debe habilitar/requerir la autenticación Kerberos en su entorno Exchange. NTLM NO es compatible \(a partir de 5.1\)](#)
- [3 Registro MAPI AO](#)

Acelerador MAPI

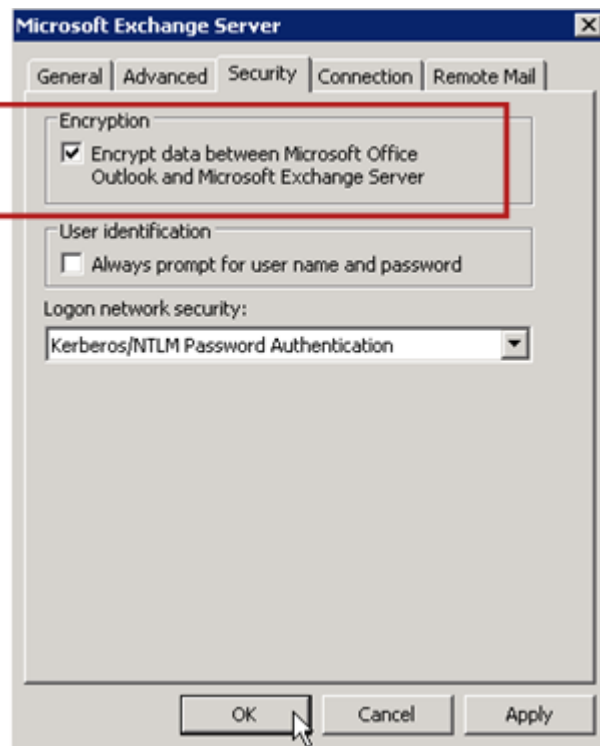
El acelerador MAPI optimiza el tráfico de correo electrónico de Microsoft Outlook Exchange. Exchange utiliza el protocolo EMSMDB, que está por capas en MS-RPC, que a su vez utiliza TCP o HTTP (no admitido) como transporte de bajo nivel.

MAPI AO soporta clientes de Microsoft Outlook 2000 a 2007 para el tráfico en modo en caché y no en caché. Las conexiones seguras que utilizan autenticación de mensajes (firma) o cifrado no se aceleran mediante MAPI AO. Estas conexiones y conexiones de clientes antiguos se transfieren al AO genérico para optimizaciones de TFO. Además, las conexiones de Outlook Web Access (OWA) y Exchange no son compatibles.

Nota: Microsoft Outlook 2007 tiene el cifrado habilitado de forma predeterminada. Debe desactivar el cifrado para beneficiarse del acelerador de aplicaciones MAPI. En Outlook, elija **Tools > E-mail Accounts**, elija **View or Change Existing E-mail Accounts** y luego haga clic en **Next**. Elija la cuenta Exchange y luego haga clic en **Cambiar**. Haga clic en **More Settings** y luego en la ficha **Security**. Desactive la casilla de verificación **Cifrar datos entre Microsoft Office Outlook y Microsoft Exchange Server**, como se muestra en la Figura 1.

Alternativamente, puede inhabilitar el cifrado para todos los usuarios de un servidor Exchange mediante una [directiva de grupo](#).

Figura 1. Inhabilitación del Cifrado en Outlook 2007



En los siguientes casos, MAPI AO no maneja una conexión:

- Conexión cifrada (transferida al AO genérico)
- Cliente no admitido (transferido al AO genérico)
- Error de análisis irreparable. Todas las conexiones TCP entre el cliente y el servicio de servidor se desconectan. Cuando el cliente se reconecta, todas las conexiones se transfieren al AO genérico.
- El cliente intenta establecer un nuevo grupo de asociación en la conexión cuando el WAE está sobrecargado.
- El cliente establece una conexión cuando el WAE está sobrecargado y los recursos de conexión reservados MAPI no están disponibles.

El cliente y el servidor de Outlook interactúan en una sesión sobre un grupo de conexiones TCP denominado grupo de asociaciones. Dentro de un grupo de asociación, los accesos a objetos pueden abarcar cualquier conexión y las conexiones se crean y liberan dinámicamente según sea necesario. Un cliente puede tener más de un grupo de asociación abierto al mismo tiempo a diferentes servidores o al mismo servidor. (Las carpetas públicas se implementan en distintos servidores del almacén de correo.)

Es esencial que todas las conexiones MAPI de un grupo de asociaciones pasen por el mismo par de WAE en la sucursal y en el Data Center. Si algunas conexiones dentro de un grupo de asociación no pasan por la AO MAPI en estos WAE, la AO MAPI no vería las transacciones realizadas en esas conexiones y se dice que las conexiones "escapan" del grupo de asociación. Por esta razón, la API MAPI no debe implementarse en WAEs en línea agrupados en serie que forman un grupo de alta disponibilidad.

Los síntomas de las conexiones MAPI que escapan a su grupo de asociación WAE son síntomas de error de Outlook, como mensajes duplicados o Outlook deja de responder.

Durante una condición de sobrecarga de TFO, las nuevas conexiones para un grupo de asociación existente pasarían y escaparían de la AO MAPI, por lo que la AO MAPI reserva una serie de recursos de conexión con anticipación para minimizar el impacto de una condición de sobrecarga. Para obtener más detalles sobre las conexiones MAPI reservadas y su impacto en la

sobrecarga del dispositivo, vea la sección "[Impacto en la sobrecarga del acelerador de aplicaciones MAPI](#)" en el artículo Solución de problemas de condiciones de sobrecarga.

Verifique la configuración general de AO y el estado con los comandos **show Accelerator** y **show license**, como se describe en el artículo [Troubleshooting Application Acceleration](#). Se necesita la licencia Enterprise para el funcionamiento del acelerador MAPI y se debe habilitar el acelerador de aplicaciones EPM.

A continuación, verifique el estado específico de MAPI AO mediante el comando **show Accelerator mapi**, como se muestra en la figura 2. Desea ver que MAPI AO está habilitado, en ejecución y registrado y que se muestra el límite de conexión. Si el estado de configuración está habilitado pero el estado operativo es apagado, indica un problema de licencia.

Figura 2 Verificación del Estado del Acelerador MAPI

```
WAE674# sh accelerator mapi
```

Accelerator	Licensed	Config State	Operational State
mapi	Yes	Enabled	Running

MAPI:

Accelerator Config Item	Mode	Value
Read optimization	User	enabled
Write optimization	User	enabled

Policy Engine Config Item

	Value
State	Registered
Default Action	Use Policy
Connection Limit	6000
Effective Limit	5990
Keepalive timeout	5.0 seconds

AO admin and operational state

Enabled Optimizations

**- Registered state indicates AO is healthy
- Displays connection limit**

Utilice el comando **show statistics Accelerator epm** para verificar que EPM AO funciona. Compruebe que el total de conexiones manejadas, el total de solicitudes analizadas correctamente y el total de respuestas analizadas correctamente aumentan cuando se inicia un cliente.

Utilice el comando **show running-config** para verificar que las políticas de tráfico MAPI y EPM están configuradas correctamente. Desea ver **acelerar la asignación** para la acción de la aplicación Correo electrónico y mensajería y desea ver el clasificador MS-EndPointMapper y la política de tráfico definidos, de la siguiente manera:

```
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
```

Utilice el comando **show policy-engine application dynamic** para verificar que existan reglas de coincidencia dinámica, como se indica a continuación:

- Busque una regla con ID de usuario: EPM y nombre de mapa: uida4f1db00-ca47-1067-b31f-00dd010662da.
- El campo Flujos indica el número total de conexiones activas al servicio Exchange.
- Para cada cliente MAPI debe ver una entrada independiente con la ID de usuario: MAPI.

Utilice el comando **show statistics connection optimizada mapi** para verificar que el dispositivo WAAS está estableciendo conexiones MAPI optimizadas. Verifique que "M" aparezca en la columna Accel para las conexiones MAPI, lo que indica que se utilizó MAPI AO, como se indica a continuación:

```
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: En la versión 4.1.5, se agregó el contador Corrientes reservadas actuales en la salida. Este contador hace referencia al número de recursos de conexión MAPI reservados en el dispositivo WAE que actualmente no se utilizan pero que se reservan para futuras conexiones MAPI. Para obtener más detalles sobre las conexiones MAPI reservadas y su impacto en la sobrecarga del dispositivo, vea la sección ["Impacto en la sobrecarga del acelerador de aplicaciones MAPI"](#) en el artículo Solución de problemas de condiciones de sobrecarga.

Si observa conexiones con "TGDL" en la columna Accel, estas conexiones se redujeron al AO genérico y se optimizaron sólo con optimizaciones de transporte. Si se trata de conexiones que esperaba que fueran manejadas por MAPI AO, puede ser porque son conexiones MAPI cifradas. Para verificar el número de conexiones MAPI cifradas que se han solicitado, utilice el comando **show statistics Accelerator mapi** de la siguiente manera:

```
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

```

Puede encontrar las direcciones IP de los clientes que solicitan conexiones MAPI cifradas en syslog buscando mensajes como los siguientes:

```

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

```

Puede ver las estadísticas de conexión MAPI mediante el comando **show statistics connection optimizada mapi detail** de la siguiente manera:

```

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

...

En este resultado se muestran los recuentos de respuestas locales y remotas y los tiempos de respuesta promedio:

```

. . .
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        <-----
. . .

```

Aceleración MAPI cifrada

Summary

Desde WAAS 5.0.1, el acelerador MAPI puede acelerar el tráfico MAPI cifrado. Esta función se activará de forma predeterminada en la versión 5.0.3. Sin embargo, para acelerar correctamente

el tráfico MAPI cifrado, hay una serie de requisitos tanto en el entorno WAAS como en el entorno AD de Microsoft. Esta guía le ayudará a verificar y resolver problemas de la funcionalidad eMAPI.

Información sobre la Función

eMAPI se activará de forma predeterminada en 5.0.3 y necesitará lo siguiente para acelerar correctamente el tráfico cifrado.

- 1) El almacén seguro de CMS debe inicializarse y abrirse en todos los WAE de núcleo
- 2) Los WAE deben poder resolver el FQDN de los servidores Exchange y Kerberos KDC (controlador de Active Directory)
- 3) Los relojes WAE deben estar sincronizados con el KDC
- 4) El acelerador SSL, WAN Secure y eMAPI deben estar habilitados en todos los dispositivos WAE en la ruta de Outlook a Exchange
- 5) Los WAE en la trayectoria deben tener la configuración de mapa de políticas correcta
- 6) Los dispositivos WAE de núcleo deben tener uno o más identificadores de dominio de servicios cifrados configurados (cuenta de usuario o de equipo)
- 7) Si se utiliza una cuenta de máquina, este WAE se debe unir al dominio AD.
- 8) A continuación, con el caso de uso de la cuenta de usuario o del equipo, se deben conceder permisos específicos a los objetos de Active Directory. "Replicando cambios de directorio" y "Replicando cambios de directorio todo" deben configurarse para permitir.

La forma recomendada de hacerlo es a través de un grupo de seguridad universal (por ejemplo, asignar los permisos al grupo y, a continuación, agregar los dispositivos WAAS o los nombres de usuario especificados en el servicio de cifrado a este grupo). Consulte la guía adjunta para ver capturas de pantalla de la configuración de AD y la GUI de WAAS CM.

Metodología de solución de problemas

Paso 1 - Verificar la configuración de la identidad del servicio de cifrado y la recuperación de claves correcta

Si bien el comando `diagnostics` (paso 2 a continuación) verifica la existencia de un servicio de cifrado, no verifica si la recuperación de claves será exitosa. Por lo tanto, no sabemos simplemente ejecutar ese comando de diagnóstico si se han concedido los permisos adecuados al objeto en Active Directory (ya sea Machine o User account).

El resumen de lo que se debe hacer para configurar y verificar el servicio de cifrado se realizará correctamente al recuperar la clave

Cuenta de usuario:

1. crear usuario AD
2. cree un grupo AD y establezca "Replicando cambios de directorio" y "Replicando cambios de directorio todos" para PERMITIR
3. agregar el usuario al grupo creado

4. definir la identidad de dominio de cuenta de usuario en servicios de cifrado

5. comando de diagnóstico get key

windows-domain diagnostics encryption-service get-key <exchange server FQDN> <nombre de dominio>

Tenga en cuenta que debe utilizar el nombre de servidor de intercambio real/real configurado en el servidor y no un FQDN de tipo NLB/VIP que pueda resolverse en varios servidores de intercambio.

6. si la recuperación de claves funcionó - hecho

Ejemplo de éxito:

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

SPN pdidc-exchange1.pdidc.cisco.com, Nombre de dominio: pdidc.cisco.com

La recuperación de claves está en curso.

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

SPN pdidc-exchange1.pdidc.cisco.com, Nombre de dominio: pdidc.cisco.com

La clave para pdidc-exchange1.pdidc.cisco.com reside en la memoria caché de claves

Cuenta de máquina

1. unir dispositivos WAE centrales al dominio AD

2.cree un grupo AD y establezca "Replicando cambios de directorio" y "Replicando cambios de directorio todos" para PERMITIR

3. agregar cuentas de máquina al grupo creado

4. configurar servicios de cifrado para utilizar la cuenta de máquina

5. Consiga que la política de grupo se aplique a la máquina unida o fuerce la aplicación de la política de grupo desde el AD. gpupdate /force.

6. comando de diagnóstico get key

windows-domain diagnostics encryption-service get-key <exchange server FQDN> <nombre de dominio>

Tenga en cuenta que debe utilizar el nombre de servidor de intercambio real/real configurado en el servidor y no un FQDN de tipo NLB/VIP que pueda resolverse en varios servidores de intercambio.

7. si la recuperación de claves funcionó - hecho

Para obtener más detalles y capturas de pantalla del servicio de cifrado y de la configuración de AD, consulte la guía adjunta.

Paso 2 - En 5.0.3 se introdujo un nuevo comando de diagnóstico para verificar algunos de los ajustes requeridos.

– Accelerator mapi verify encryption settings

1. CLI realiza varias comprobaciones de validez. El resultado es un resumen de la capacidad de acelerar el tráfico MAPI cifrado como perímetro o núcleo.
2. Comprueba los atributos de estado/configuración de los distintos componentes para que el servicio de cifrado funcione correctamente.
3. Cuando se detecta un problema de configuración, se produce lo que falta y la CLI o acciones para corregirlo.
4. Proporciona el resumen como dispositivo Edge y dispositivo Core. El dispositivo que puede ser tanto de borde como de núcleo debe tener EMAPI operativa tanto para el perímetro como para el núcleo.

A continuación se muestra un ejemplo de salida de un WAE configurado incorrectamente:

```
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

```

A continuación se muestra el resultado de un WAE de núcleo configurado correctamente:

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

```

Paso 3 - Verifique manualmente la configuración de WAE que no está marcada por el comando de diagnóstico anterior.

1) El comando anterior mientras verifica la existencia de NTP configurado, no verifica realmente los tiempos están sincronizados entre WAE y KDC. Es muy importante que los tiempos estén sincronizados entre el núcleo y la KDC para que la recuperación de claves tenga éxito.

Si la comprobación manual revela que no están sincronizados, una forma sencilla de forzar el reloj del WAE a estar sincronizado sería el comando `ntpdate (ntpdate <KDC ip>)`. A continuación, señale los WAE al servidor NTP empresarial.

2) Verifique que `dnslookup` se realice correctamente en todos los WAE para el FQDN de los servidores Exchange y el FQDN de los KDC

3) Verifique que el mapa de clase y el mapa de política estén configurados correctamente en todos los WAE en la trayectoria.

```
pdi-7541-dc#sh class-map type waas MAPI
```

El tipo de mapa de clase era match-any MAPI

Match tcp destination epm mapi (0 flow-match)

```
pdi-7541-dc#show policy-map type waas Policy-map type waas
```

WAAS-GLOBAL (6084690 en total)

Clase MAPI (0 coincidencias de flujo)

optimizar la aplicación mapi completa Correo electrónico y mensajería

4) Verifique que el almacén seguro de CMS esté abierto e inicializado en todos los WAE "show cms secure store"

Análisis de datos

Además de analizar el resultado del comando diagnostic y los comandos show manuales, puede que necesite revisar el sysreport.

Específicamente, querrá revisar los archivos mapiao-errorlog, sr-errorlog (sólo WAE de núcleo) y wsao-errorlog.

Habrá pistas en cada registro dependiendo del escenario que le llevará a la caída de conexiones de motivo a la AO genérica.

A modo de referencia, se muestra un ejemplo de resultado que muestra varios componentes en funcionamiento

Este resultado es de sr-errorlog y muestra la validación de la identidad del servicio de cifrado de cuenta de máquina

Nota: Esto solo confirma que el WAE principal se unió al dominio y que la cuenta de máquina existe.

```
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]

Este resultado proviene del registro de errores de vcprd principal de nuevo y muestra una recuperación de claves exitosa de KDC.

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 DRSEBIND Response

```
[AppApiDrvsBind.cpp:222]
10/23/2012 15:46:55.680(Local) (3780 0.1) NTCE (680030) DRSSBind Success, Status:00000000
[AppApiDrvsBind.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]
```

Esta salida proviene del archivo mapiao-errorlog en el WAE perimetral para una conexión eMAPI correcta

```
'''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]
```

Esta es la salida de núcleo WAE correspondiente del mapiao-errorlog para la misma conexión 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) SrplibCache Cache eviction starting:
static void srplib::CSrplibCache:: OnAoShellDispatchCacheCleanup(vo
id*, aosh_work*) [SrplibCache.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) [SrplibCache.
cpp:464]
10/23/2012 17:56:54.175(Local) (6408 0.0) NTCE (175121) SendNextCmd isDuringSend 0, WriteQueue sz
1, isDuringclose 0 [SrplibClientTransport.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] [SrplibClientTransport.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 [SrplibTransport.
cpp:127]
10/23/2012 17:56:54.185(Local) (6408 0.1) NTCE (185587) Parse header, msg body len 152
[SrplibTransport.cpp:111]
10/23/2012 17:56:54.185(Local) (6408 0.1) NTCE (185592) ReadNextMsg isDuringRead 0,
isDuringHeaderRead 1, isDuringclose 0 [SrplibTransport.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 [SrplibTranspor
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
```



```
rllibCache.cpp:735]
'''10/23/2012 17:56:54.185(Local) (6408 0.1) NTCE (185747) ReadNextMsg isDuringRead 0,
isDuringHeaderRead 0, isDuringClose 0 [SrllibTransport.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]'''
```

Problemas Comunes

A continuación se exponen algunas razones comunes que dan lugar a la conexión eMAPI de mano a la AO genérica (TG).

Problema 1: La identidad del servicio de cifrado configurada en el WAE de núcleo no tiene los permisos correctos en AD.

Salida de sr-errolog en 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
srllib [SRServer.cpp:189]
09/25/2012 18:47:54.147(Local) (9063 0.1) NTCE (147722) Queued send reponse buffer to client task
[SrllibServerTransport.cpp:136]
09/25/2012 18:47:54.147(Local) (9063 0.1) NTCE (147730) KrbKeyResponse, sent to client session
object [SrllibServer.cpp:203]
09/25/2012 18:47:54.147(Local) (9063 0.0) NTCE (147733) SendNextCmd isDuringSend 0, WriteQueue
size 1 isDuringClose 0 [SrllibServerTransport.cpp:308]
09/25/2012 18:47:54.147(Local) (9063 0.1) NTCE (147740) Send Key response to the Client
```

Resolución 1: Consulte la guía de configuración y verifique que el objeto en AD tenga los permisos correctos. "Replicando cambios de directorio" y "Replicando cambios de directorio todo"

deben configurarse para permitir.

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

Problema 2: Hay una desviación de tiempo entre el WAE de núcleo y el KDC del que intenta recuperar la clave

Salida de sr-errolog en 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]
```

Resolución 2: Utilice la actualización en todos los dispositivos WAE (especialmente en el núcleo) para sincronizar el reloj con el KDC. A continuación, indique el servidor NTP de la empresa (preferiblemente el mismo que el KDC).

Problema 3: El dominio que definió para su servicio de cifrado no coincide con el dominio en el que se encuentra su servidor Exchange.

Salida de sr-errolog en 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]
```

Resolución 3: Si su WAE central presta servicios a varios servidores Exchange en diferentes dominios, debe configurar una identidad de servicio de cifrado para cada dominio en el que residen los servidores Exchange.

Nota, no hay soporte para la inclusión de subdominios en este momento. Por lo tanto, si tiene myexchange.sub-domain.domain.com , la identidad del servicio de cifrado debe estar en sub-domain.domain.com; NO PUEDE estar en el dominio primario.

Problema 4: Si WANSecure falla, las conexiones pueden caer a TG

Las conexiones eMAPI se pueden entregar a Generic AO porque falló la conexión segura WAN. Error en la conexión segura de WAN porque falló la verificación de certificado. La verificación de certificado de par fallará porque se está utilizando el certificado de par autofirmado predeterminado o el certificado ha fallado legítimamente la comprobación de OCSP.

Configuración de WAE de núcleo

```
crypto pki global-settings

    oosp url http://pdidc.cisco.com/oosp
    revocation-check oosp-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

Esto resultará en las siguientes entradas mapiao-errorlog y wsao-errorlog:

La pista aquí es la primera línea resaltada "desconectada más de cuatro veces consecutivas"

Mapiao-errorlog en el lado del cliente WAE:

```
'''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 en el lado del cliente WAE:

```
'''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]
```

Resolución 4: Elimine la configuración de verificación de certificado de peer de ambos WAE y reinicie el servicio de cifrado en los WAE de núcleo.

```
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: Si el cliente de Outlook utiliza NTLM, la conexión se enviará a Generic AO.

Verá lo siguiente en el mapiao-errorlog del lado del cliente WAE:

```
'''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]
```

Resolución 5: El cliente debe habilitar/requerir la autenticación Kerberos en su entorno Exchange. NTLM NO es compatible (a partir de 5.1)

Tenga en cuenta que hay un resumen técnico de Microsoft que indica un retorno a NTLM cuando se utiliza un CAS.

El escenario en el que Kerberos no funciona es específico de Exchange 2010 y se encuentra en el siguiente escenario:

Varios servidores de acceso de cliente Exchange (CAS) en una organización/dominio. Estos servidores CAS se agrupan mediante cualquier método, mediante la función integrada de matriz cliente de Microsoft o un equilibrador de carga de terceros.

En el escenario anterior, Kerberos no funciona y los clientes volverán a NTLM de forma predeterminada. Creo que esto se debe al hecho de que los clientes tienen que AUTH al servidor CAS frente al servidor de buzón, como lo hicieron en las versiones anteriores de Exchange.

En Exchange 2010 RTM, ¡no hay solución para esto! Kerberos en el escenario anterior nunca funcionará antes de Exchange 2010-SP1.

En SP1, Kerberos se puede habilitar en estos entornos, pero es un proceso manual. Vea el artículo aquí: <http://technet.microsoft.com/en-us/library/ff808313.aspx>

Registro MAPI AO

- Los siguientes archivos de registro están disponibles para resolver problemas de MAPI AO:
- Archivos de registro de transacciones: /local1/logs/tfo/working.log (y /local1/logs/tfo/tfo_log_*.txt)

Archivos de registro de depuración: /local1/errorlog/mapiao-errorlog.current (y mapiao-errorlog.*)

Para una depuración más sencilla, primero debe configurar una ACL para restringir los paquetes a un 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
```

Para habilitar el registro de transacciones, utilice el comando de configuración Transaction-logs de la siguiente manera:

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

Puede ver el final de un archivo de registro de transacciones utilizando el comando type-tail de la siguiente manera:

```
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
```

Para configurar y habilitar el registro de depuración de MAPI AO, utilice los siguientes comandos. **NOTE:** El registro de depuración hace un uso intensivo de la CPU y puede generar una gran cantidad de resultados. Utilícelo de manera sensata y moderada en un entorno de producción. Puede habilitar el registro detallado en el disco de la siguiente manera:

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

Puede habilitar el registro de depuración para las conexiones en la ACL de la siguiente manera:

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

Las opciones para la depuración MAPI AO son las siguientes:

```
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
```

Puede habilitar el registro de depuración para las conexiones MAPI y, a continuación, mostrar el final del registro de errores de depuración de la siguiente manera:

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