WAAS - Dépannage de l'AO MAPI

Chapitre : Dépannage de l'AO MAPI

Cet article décrit comment dépanner l'AO MAPI.

Co

Art
Pré
WA
Dé
Op
Dé
Dé
Dé
Dé
Dé
Dé
Dé
Dé
Dé
Dé
Dé
Dé
Dé
Dé
Dé
Dé

Contenu

Accélérateur MAPI

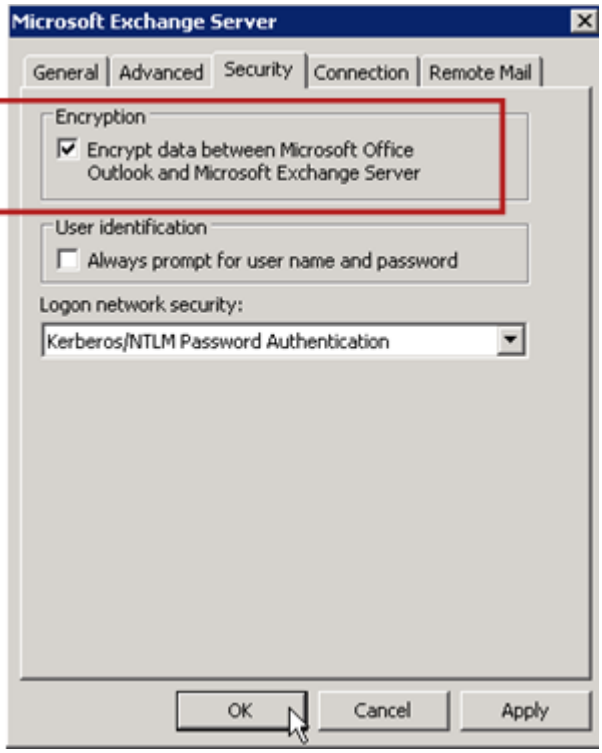
L'accélérateur MAPI optimise le trafic de messagerie Microsoft Outlook Exchange. Exchange utilise le protocole EMSMDB, qui est mis en couche sur MS-RPC, qui à son tour utilise TCP ou HTTP (non pris en charge) comme transport de bas niveau.

L'AO MAPI prend en charge les clients Microsoft Outlook 2000 à 2007 pour le trafic en mode cache et non mis en cache. Les connexions sécurisées qui utilisent l'authentification des messages (signature) ou le chiffrement ne sont pas accélérées par l'AO MAPI. Ces connexions et connexions des clients plus anciens sont transmises à l'AO générique pour les optimisations TFO. En outre, les connexions Outlook Web Access (OWA) et Exchange-Exchange ne sont pas prises en charge.

Note: Le chiffrement est activé par défaut dans Microsoft Outlook 2007. Vous devez désactiver le chiffrement pour bénéficier de l'accélérateur d'application MAPI. Dans Outlook, choisissez **Outils > Comptes de messagerie**, choisissez **Afficher ou modifier les comptes de messagerie existants**, puis cliquez sur **Suivant**. Choisissez le compte Exchange, puis cliquez sur **Modifier**. Cliquez sur **Autres paramètres**, puis sur l'onglet **Sécurité**. Décochez la case **Chiffrer les données entre Microsoft Office Outlook et Microsoft Exchange Server**, comme illustré à la Figure 1.

Vous pouvez également désactiver le chiffrement pour tous les utilisateurs d'un serveur Exchange à l'aide d'une stratégie de groupe.

Figure 1. Désactivation du chiffrement dans Outlook 2007



Dans les cas suivants, l'AO MAPI ne gère pas de connexion :

- Connexion chiffrée (transmise à l'AO générique)
- Client non pris en charge (remis à l'AO générique)
- Erreur d'analyse irrécupérable. Toutes les connexions TCP entre le service client et le service serveur sont déconnectées. Lorsque le client se reconnecte, toutes les connexions sont transmises à l'AO générique.
- Le client tente d'établir un nouveau groupe d'association sur la connexion lorsque le WAE est surchargé.
- Le client établit une connexion lorsque le WAE est surchargé et que les ressources de connexion MAPI réservées ne sont pas disponibles.

Le client et le serveur Outlook interagissent dans une session sur un groupe de connexions TCP appelé groupe d'association. Au sein d'un groupe d'association, les accès aux objets peuvent s'étendre sur n'importe quelle connexion et les connexions sont créées et libérées de manière dynamique selon les besoins. Un client peut avoir plusieurs groupes d'association ouverts simultanément à différents serveurs ou au même serveur. (Les dossiers publics sont déployés sur différents serveurs du magasin de messagerie.)

Il est essentiel que toutes les connexions MAPI au sein d'un groupe d'association passent par la même paire de WAE dans la filiale et le centre de données. Si certaines connexions au sein d'un groupe d'association ne passent pas par l'AO MAPI sur ces WAE, l'AO MAPI ne verrait pas les transactions effectuées sur ces connexions et les connexions sont dites « échapper » au groupe d'association. Pour cette raison, l'AO MAPI ne doit pas être déployé sur des WAE en ligne en cluster en série qui forment un groupe de haute disponibilité.

Les symptômes des connexions MAPI qui échappent à leur groupe d'association WAE sont les symptômes d'erreur Outlook tels que les messages dupliqués ou l'arrêt de réponse d'Outlook.

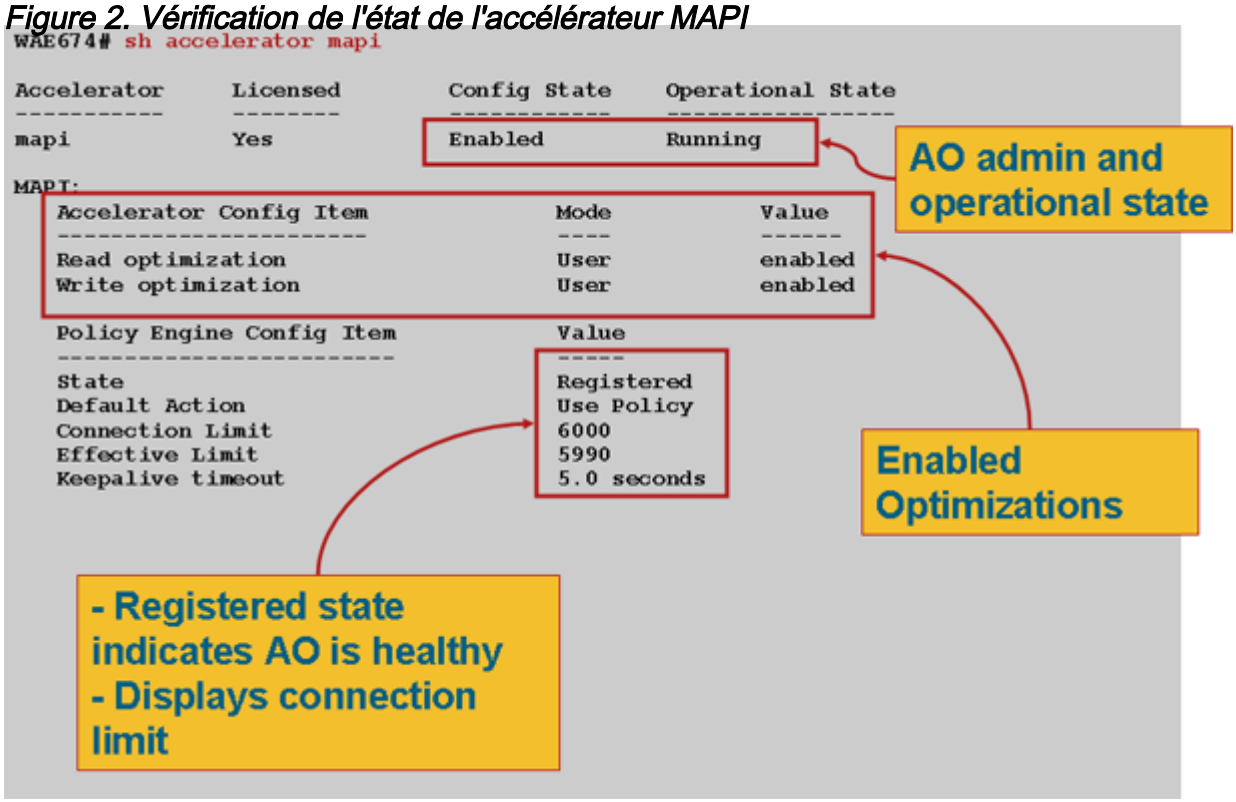
Lors d'une surcharge TFO, de nouvelles connexions pour un groupe d'association existant passeraient par et échapperaient à l'AO MAPI, de sorte que l'AO MAPI réserve un certain nombre de ressources de connexion à l'avance pour minimiser l'impact d'une condition de surcharge. Pour plus d'informations sur les connexions MAPI réservées et leur impact sur la surcharge de

périphériques, reportez-vous à la section « Impact sur la surcharge des connexions réservées à l'accélérateur d'applications MAPI » dans l'article Troubleshooting Overload Conditions.

Vérifiez la configuration et l'état généraux de l'AO à l'aide des commandes **show accélérator** et **show license**, comme décrit dans l'article Dépannage de l'accélération des applications. La licence Enterprise est requise pour le fonctionnement de l'accélérateur MAPI et l'accélérateur d'application EPM doit être activé.

Ensuite, vérifiez l'état spécifique à l'AO MAPI à l'aide de la commande **show accélérator mapi**, comme illustré à la Figure 2. Vous voulez voir que l'AO MAPI est activée, en cours d'exécution et inscrite et que la limite de connexion est affichée. Si l'état de configuration est Activé mais que l'état opérationnel est Arrêté, cela indique un problème de licence.

Figure 2. Vérification de l'état de l'accélérateur MAPI



Utilisez la commande **show statistics Accelerator epm** pour vérifier que l'AO EPM est fonctionnel. Vérifiez que les compteurs Nombre total de connexions traitées, Nombre total de demandes analysées avec succès et Nombre total de réponses analysées avec succès augmentent au démarrage d'un client.

Utilisez la commande **show running-config** pour vérifier que les politiques de trafic MAPI et EPM sont correctement configurées. Vous voulez voir **accélérer le mappage** pour l'action de l'application E-mail et messagerie et vous voulez voir le classifieur MS-EndPortMapper et la politique de trafic définis, comme suit :

```
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
```

Utilisez la commande **show policy-engine application dynamic** pour vérifier que des règles de correspondance dynamique existent, comme suit :

- Recherchez une règle avec l'ID utilisateur : Nom du MPI et du Mappage : uuida4f1db00-ca47-1067-b31f-00dd010662da.
- Le champ Flux indique le nombre total de connexions actives au service Exchange.
- Pour chaque client MAPI, une entrée distincte doit s'afficher avec l'ID utilisateur : MAPI.

Utilisez la commande **show statistics connection optized mapi** pour vérifier que le périphérique WAAS établit des connexions MAPI optimisées. Vérifiez que « M » apparaît dans la colonne Accel pour les connexions MAPI, ce qui indique que l'AO MAPI a été utilisé, comme suit :

```
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"
```

Note: Dans la version 4.1.5, le compteur Flux actuellement réservés a été ajouté dans la sortie. Ce compteur fait référence au nombre de ressources de connexion MAPI réservées sur le WAE qui sont actuellement inutilisées mais réservées pour les connexions MAPI futures. Pour plus d'informations sur les connexions MAPI réservées et leur impact sur la surcharge de périphériques, reportez-vous à la section « Impact sur la surcharge des connexions réservées à l'accélérateur d'applications MAPI » dans l'article Troubleshooting Overload Conditions.

Si vous observez des connexions avec « TGDL » dans la colonne Accel, ces connexions ont été repoussées vers l'AO générique et optimisées uniquement avec des optimisations de transport. S'il s'agit de connexions que vous attendiez à être gérées par l'AO MAPI, c'est peut-être parce qu'elles sont des connexions MAPI chiffrées. Pour vérifier le nombre de connexions MAPI cryptées qui ont été demandées, utilisez la commande **show statistics Accelator mapi** comme suit :

```
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
```

Vous pouvez trouver les adresses IP des clients qui demandent des connexions MAPI chiffrées dans le syslog en recherchant des messages tels que :

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

Vous pouvez afficher les statistiques de connexion MAPI à l'aide de la commande **show statistics connection optized mapi detail** comme suit :

```
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
. . .
```

Le nombre de réponses locales et distantes et les temps de réponse moyens sont indiqués dans ce résultat :

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

Accélération MAPI chiffrée

Résumé

Depuis WAAS 5.0.1, l'accélérateur MAPI peut désormais accélérer le trafic MAPI chiffré. Cette fonctionnalité sera activée par défaut dans la version 5.0.3. Cependant, afin d'accélérer le trafic

MAPI chiffré, il existe un certain nombre de besoins dans l'environnement WAAS et Microsoft AD. Ce guide vous aidera à vérifier et à dépanner la fonctionnalité eMAPI.

Informations sur les fonctionnalités

eMAPI sera activé par défaut dans la version 5.0.3 et nécessitera les éléments suivants pour accélérer avec succès le trafic chiffré.

1) Le magasin sécurisé CMS doit être initialisé et ouvert sur tous les périphériques WAE principaux

2) Les WAE doivent pouvoir résoudre le nom de domaine complet du ou des serveurs Exchange et le contrôleur de domaine Kerberos (contrôleur Active Directory)

3) Les horloges du WAE doivent être synchronisées avec le KDC

4) L'acclérateur SSL, WAN Secure et eMAPI doivent être activés sur tous les WAE du chemin d'Outlook à Exchange

5) Les WAE du chemin doivent avoir la configuration de la carte de stratégie correcte

6) Les WAE principaux doivent avoir une ou plusieurs identités de domaine de services cryptés configurées (compte d'utilisateur ou d'ordinateur)

7) Si un compte machine est utilisé, ce WAE doit être joint au domaine AD.

8) Ensuite, avec le cas d'utilisation du compte Ordinateur ou Utilisateur, ces objets dans Active Directory doivent recevoir des autorisations spécifiques. « Réplication des modifications de répertoire » et « Réplication de tous les changements de répertoire » doivent tous deux être définis pour autoriser.

Pour ce faire, il est recommandé d'utiliser un groupe de sécurité universelle (par exemple, attribuer les autorisations au groupe, puis ajouter les périphériques WAAS et/ou les noms d'utilisateur spécifiés dans le service de chiffrement à ce groupe). Reportez-vous au guide ci-joint pour obtenir des captures d'écran de la configuration AD et de l'interface graphique utilisateur de WAAS CM.

Méthodologie de dépannage

Étape 1 : vérification de la configuration de l'identité du service de chiffrement et du succès de la récupération des clés

Bien que la commande diagnostics (étape 2 ci-dessous) vérifie l'existence d'un service de chiffrement, elle ne vérifie pas si la récupération de clé réussit. Par conséquent, nous ne savons pas simplement en exécutant cette commande de diagnostic si les autorisations appropriées ont été accordées à l'objet dans Active Directory (compte d'ordinateur ou d'utilisateur).

Récapitulatif de ce qui doit être fait pour configurer et vérifier le service de chiffrement réussira la récupération de clé

Compte utilisateur :

1. créer un utilisateur AD

2. créer un groupe AD et définir « Réplication des modifications de répertoire » et « Réplication de

tous les changements de répertoire » pour AUTORISER

3. ajouter l'utilisateur au groupe créé

4. définir l'identité du domaine du compte d'utilisateur dans les services de chiffrement

5. run get key diagnostic cli

windows-domain diagnostics encryption-service get-key <nom de domaine complet du serveur d'échange> <nom de domaine>

Notez que vous devez utiliser le nom de serveur d'échange réel/réel configuré sur le serveur et non un nom de domaine complet de type NLB/VIP qui peut être converti en plusieurs serveurs d'échange.

6. si la récupération de clé a fonctionné - effectué

Exemple de réussite :

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

SPN pdidc-exchange1.pdidc.cisco.com, nom de domaine : pdidc.cisco.com

La récupération de clé est en cours.

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

SPN pdidc-exchange1.pdidc.cisco.com, nom de domaine : pdidc.cisco.com

La clé de pdidc-exchange1.pdidc.cisco.com réside dans le cache de clé de mémoire

Compte machine

1. Joindre les périphériques WAE principaux au domaine AD

2.créer un groupe AD et définir « Réplication des modifications de répertoire » et « Réplication des modifications de répertoire toutes » pour AUTORISER

3. ajouter des comptes d'ordinateur au groupe créé

4. configurer les services de chiffrement pour utiliser le compte d'ordinateur

5. Donnez un certain temps pour que la stratégie de groupe soit appliquée à la machine jointe ou forcez l'application de la stratégie de groupe à partir de l'AD. gpupdate /force.

6. run get key diagnostic cli

windows-domain diagnostics encryption-service get-key <nom de domaine complet du serveur d'échange> <nom de domaine>

Notez que vous devez utiliser le nom de serveur d'échange réel/réel configuré sur le serveur et non un nom de domaine complet de type NLB/VIP qui peut être converti en plusieurs serveurs d'échange.

7. si la récupération de clé a fonctionné - effectué

Pour plus d'informations et de captures d'écran sur le service de chiffrement et la configuration AD, reportez-vous au guide ci-joint.

Étape 2 - Dans la version 5.0.3, une nouvelle commande de diagnostic a été introduite pour vérifier certains des paramètres requis.

Carte accélérateur de vérification des paramètres de chiffrement

1.L'interface de ligne de commande effectue diverses vérifications de validité. Le résultat est un résumé de la capacité à accélérer le trafic MAPI chiffré en tant que périphérie ou coeur.

2.Vérifie que les attributs d'état/de configuration des différents composants du service de chiffrement fonctionnent correctement.

3.Lorsqu'un problème de configuration est détecté, il affiche ce qui manque et l'interface de ligne de commande (CLI) ou les actions pour le résoudre.

4.Il fournit le résumé en tant que périphérique Edge et périphérique principal. Le périphérique qui peut être à la fois de périphérie et de coeur de réseau doit être opérationnel EMAPI pour la périphérie et le coeur de réseau.

Voici un exemple de sortie d'un périphérique WAE mal configuré :

```
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
```

Voici le résultat d'un périphérique WAE principal configuré correctement :

```
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
```

Étape 3 - Vérifiez manuellement les paramètres WAE qui ne sont pas vérifiés par la commande de diagnostic ci-dessus.

1) La commande ci-dessus, bien qu'elle vérifie l'existence de NTP configuré, ne vérifie pas réellement que les heures sont synchronisées entre le WAE et le KDC. Il est très important que les temps soient synchronisés entre le coeur et le KDC pour que la récupération des clés soit réussie.

Si la vérification manuelle révèle qu'ils ne sont pas synchronisés, une façon simple de forcer l'horloge du WAE à être synchronisée serait la commande ntpdate (**ntpdate <KDC ip>**). Pointez ensuite les WAE vers le serveur NTP d'entreprise.

2) Vérifiez que **dnslookup** réussit sur tous les WAE pour le FQDN des serveurs Exchange et le FQDN des KDC

3) Vérifiez que la carte-classe et la carte-politique sont configurées correctement sur tous les WAE du chemin.

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

Type de mappage de classe waas match-any MAPI

Correspondance tcp destination epm mapi (0 correspondance de flux)

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

WAAS-GLOBAL (6084690 au total)

Classe MAPI (0 correspondance de flux)
optimiser l'accélération complète de l'application mapi E-mail-and-Messaging

4) Vérifiez que le magasin sécurisé CMS est ouvert et initialisé sur tous les WAE « show cms secure store »

Analyse des données

Outre l'analyse des résultats de la commande de diagnostic et des commandes show manuelles, vous devrez peut-être examiner le rapport sysreport.

Plus précisément, vous voudrez revoir les fichiers mapiao-errorlog, sr-errorlog (noyau WAE uniquement) et wsao-errorlog.

Il y aura des indications dans chaque journal en fonction du scénario qui vous mènera à la raison pour laquelle les connexions tombent sur l'AO générique.

Àtitre de référence, voici un exemple de sortie montrant différents composants de travail

Ce résultat provient de sr-errorlog et montre la validation de l'identité du service de chiffrement de compte d'ordinateur

Note: Cela confirme uniquement que le périphérique WAE principal a rejoint le domaine et que le compte d'ordinateur 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]
```

Ce résultat provient à nouveau du journal principal sr-errorlog et montre la récupération de clé réussie à partir 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 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]
```

Cette sortie provient du fichier mapiao-errorlog sur le périphérique WAE pour une connexion eMAPI réussie

```
'''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]
```

Voici la sortie principale WAE de mapiao-errorlog correspondante pour la même connexion 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]'''
```

Problèmes courants

Voici quelques raisons courantes qui donnent lieu à une connexion eMAPI manuelle à l'AO générique (TG).

Problème 1 : L'identité du service de chiffrement configurée sur le périphérique WAE principal ne dispose pas des autorisations correctes dans AD.

Sortie de sr-errlogg sur le périphérique WAE principal

```
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
```

Résolution 1 : Consultez le guide de configuration et vérifiez que l'objet dans AD dispose des autorisations appropriées. « Réplication des modifications de répertoire » et « Réplication de tous les changements de répertoire » doivent tous deux être définis pour autoriser.

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

Problème 2 : Il y a un décalage temporel entre le périphérique WAE principal et le contrôleur de domaine KDC à partir duquel il tente de récupérer la clé

Sortie de sr-errlogg sur le périphérique WAE principal

```
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]
```

Résolution 2 : Utilisez ntpdate sur tous les WAE (en particulier le coeur) pour synchroniser l'horloge avec le KDC. Pointez ensuite vers le serveur NTP d'entreprise (de préférence le même que le KDC).

Problème 3 : Le domaine que vous avez défini pour votre service de chiffrement ne correspond pas au domaine dans lequel se trouve votre serveur Exchange.

Sortie de sr-errlogg sur le périphérique WAE principal

```
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]
```

Résolution 3 : Si votre périphérique WAE principal dessert plusieurs serveurs Exchange dans différents domaines, vous devez configurer une identité de service de chiffrement pour chaque domaine dans lequel résident les serveurs Exchange.

Remarque : AUCUNE prise en charge de l'inclusion de sous-domaine n'est disponible pour le moment. Si vous avez myexchange.sub-domain.domain.com, l'identité du service de chiffrement doit se trouver dans sub-domain.domain.com ; il NE PEUT PAS se trouver dans le domaine parent.

Problème 4 : Si WANecure échoue, vos connexions peuvent passer à TG

Les connexions eMAPI peuvent être transmises à l'AO générique en raison d'une défaillance de la plomberie sécurisée WAN. Échec de la plomberie WAN Secure, car échec de la vérification du certificat. La vérification du certificat homologue échouera car le certificat homologue auto-signé par défaut est utilisé ou le certificat a légitimement échoué la vérification OCSP.

Paramètres WAE principaux

```
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
```

Ceci entraînera les entrées mapiao-errorlog et wsao-errorlog suivantes :

L'indice ici est la première ligne mise en surbrillance « déconnectée plus de quatre fois de suite »

Mapiao-errorlog côté client 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 côté client 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]
```

Résolution 4 : Supprimez le certificat homologue pour vérifier la configuration des deux WAE et redémarrez le service de chiffrement sur les WAE principaux.

```
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
```

Problème 5 : Si NTLM est utilisé par le client Outlook, la connexion sera repoussée vers l'AO générique.

Vous verrez ce qui suit dans le mapiao-errorlog côté client 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]
```

Résolution 5 : Le client doit activer/exiger l'authentification Kerberos dans son environnement Exchange. NTLM n'est PAS pris en charge (à partir de la version 5.1)

Sachez qu'il existe un dossier technique Microsoft qui signale un retour vers NTLM lorsqu'un CAS est utilisé.

Le scénario dans lequel Kerberos ne fonctionne pas est spécifique à Exchange 2010 et se présente dans le scénario suivant :

Plusieurs serveurs d'accès client Exchange (CAS) dans une organisation/un domaine.
Ces serveurs CAS sont mis en grappe en utilisant n'importe quelle méthode, à l'aide de la fonction Client-Array intégrée de Microsoft ou d'un équilibreur de charge tiers.

Dans le scénario ci-dessus, Kerberos ne fonctionne pas - et les clients retomberont par défaut sur NTLM. Je crois que cela est dû au fait que les clients doivent AUTH au serveur CAS par rapport au serveur de boîtes aux lettres, comme ils l'ont fait dans les versions précédentes d'Exchange.

Dans Exchange 2010 RTM, il n'y a pas de solution ! Kerberos dans le scénario ci-dessus ne fonctionnera jamais avant Exchange 2010-SP1.

Dans SP1, Kerberos peut être activé dans ces environnements, mais c'est un processus manuel. Voir l'article ici : http://technet.microsoft.com/en-us/library/ff808313.aspx

Journalisation AO MAPI

- Les fichiers journaux suivants sont disponibles pour le dépannage des problèmes d'AO MAPI :
- Fichiers journaux des transactions : /local1/logs/tfo/working.log (et /local1/logs/tfo/tfo_log_*.txt)

Fichiers journaux de débogage : /local1/errorlog/mapiao-errorlog.current (et mapiao-errorlog.*)

Pour faciliter le débogage, vous devez d'abord configurer une liste de contrôle d'accès pour limiter les paquets à un hôte.

```
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
```

Pour activer la journalisation des transactions, utilisez la commande de configuration transaction-logs comme suit :

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

Vous pouvez afficher la fin d'un fichier journal de transactions à l'aide de la commande type-tail comme suit :

```
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
```

Pour configurer et activer la journalisation de débogage de l'AO MAPI, utilisez les commandes suivantes.
NOTE: La journalisation de débogage est gourmande en CPU et peut générer une grande quantité de sortie. Utilisez-le judicieusement et avec parcimonie dans un environnement de production.
Vous pouvez activer la journalisation détaillée sur le disque comme suit :

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

Vous pouvez activer la journalisation de débogage pour les connexions dans la liste de contrôle

d'accès comme suit :

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

Les options de débogage AO MAPI sont les suivantes :

```
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
```

Vous pouvez activer la journalisation de débogage pour les connexions MAPI, puis afficher la fin du journal des erreurs de débogage comme suit :

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