Cisco WAAS-Fehlerbehebungsleitfaden für Version 4.1.3 und höher

Kapitel: Fehlerbehebung bei MAPI AO

In diesem Artikel wird beschrieben, wie eine Fehlerbehebung für MAPI AO durchgeführt wird.

Inh

Ha
An
Da
Vo
Op
Pro
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Fel
Ha
Fel
vW
Fel
Fel

Inhalt

MAPI Accelerator

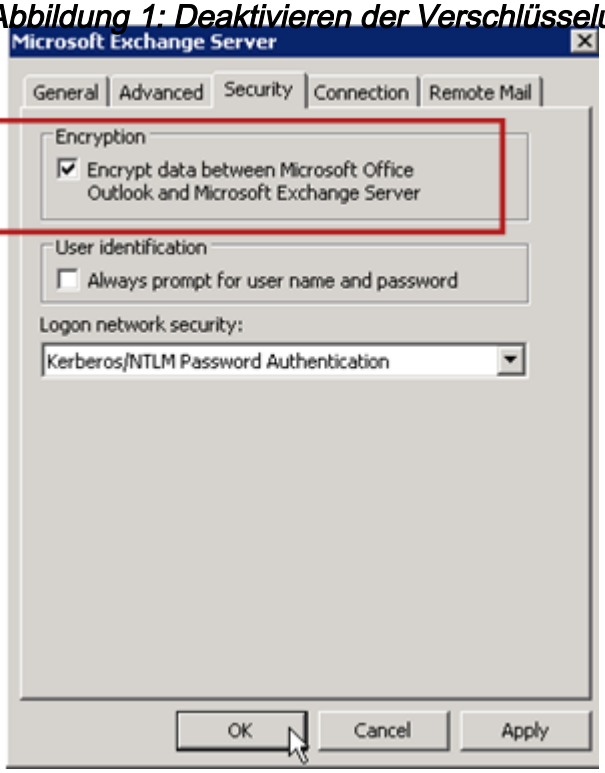
Der MAPI Accelerator optimiert den E-Mail-Verkehr in Microsoft Outlook Exchange. Exchange verwendet das EMSMDB-Protokoll, das auf MS-RPC Layer ist, das wiederum TCP oder HTTP (nicht unterstützt) als Transport auf niedriger Ebene verwendet.

Das MAPI AO unterstützt Microsoft Outlook 2000 bis 2007-Clients für Datenverkehr im Cache- und im Nicht-Cached-Modus. Sichere Verbindungen, die Nachrichtenauthentifizierung (Signierung) oder Verschlüsselung verwenden, werden durch die MAPI-AO nicht beschleunigt. Solche Verbindungen und Verbindungen älterer Clients werden zur TFO-Optimierung an das generische AO übergeben. Darüber hinaus werden Outlook Web Access (OWA)- und Exchange-Verbindungen nicht unterstützt.

Hinweis: In Microsoft Outlook 2007 ist die Verschlüsselung standardmäßig aktiviert. Sie müssen die Verschlüsselung deaktivieren, um vom MAPI-Anwendungsbeschleuniger profitieren zu können. Wählen Sie in Outlook **Extras > E-Mail-Konten**, wählen Sie **Vorhandene E-Mail-Konten anzeigen oder ändern aus**, und klicken Sie dann auf **Weiter**. Wählen Sie das Exchange-Konto aus, und klicken Sie dann auf **Ändern**. Klicken Sie auf **Weitere Einstellungen** und dann auf die Registerkarte **Sicherheit**. Deaktivieren Sie das Kontrollkästchen **Daten zwischen Microsoft Office Outlook und Microsoft Exchange Server verschlüsseln**, wie in Abbildung 1 gezeigt.

Alternativ können Sie die Verschlüsselung für alle Benutzer eines Exchange Servers deaktivieren, indem Sie eine Gruppenrichtlinie verwenden.

Abbildung 1: Deaktivieren der Verschlüsselung in Outlook 2007



In den folgenden Fällen behandelt der MAPI AO keine Verbindung:

- Verschlüsselte Verbindung (wird an die generische AO übergeben)
- Nicht unterstützter Client (wird an generische AO übergeben)
- Unbehebbarer Analysefehler. Alle TCP-Verbindungen zwischen Client und Server-Dienst werden getrennt. Wenn der Client erneut eine Verbindung herstellt, werden alle Verbindungen an die generische AO übergeben.
- Der Client versucht, eine neue Zuordnungsgruppe für die Verbindung einzurichten, wenn die WAE überlastet ist.
- Der Client stellt eine Verbindung her, wenn die WAE überlastet ist und MAPI-reservierte Verbindungsressourcen nicht verfügbar sind.

Der Outlook-Client und -Server interagieren in einer Sitzung über eine Gruppe von TCP-Verbindungen, die als Zuordnungsgruppe bezeichnet werden. Innerhalb einer Zuordnungsgruppe können sich Objektzugriffe über alle Verbindungen erstrecken, und Verbindungen werden dynamisch erstellt und nach Bedarf freigegeben. Auf einem Client können mehrere Zuordnungsgruppen gleichzeitig für verschiedene Server oder denselben Server geöffnet sein. (Öffentliche Ordner werden auf verschiedenen Servern bereitgestellt, die sich vom E-Mail-Store unterscheiden.)

Alle MAPI-Verbindungen innerhalb einer Zuordnungsgruppe müssen über dieselben WAE-Paare in der Zweigstelle und im Rechenzentrum laufen. Wenn einige Verbindungen innerhalb einer Zuordnungsgruppe die MAPI-AO auf diesen WAEs nicht durchlaufen, würde der MAPI-AO die für diese Verbindungen ausgeführten Transaktionen nicht sehen, und die Verbindungen sollen der Zuordnungsgruppe "entweichen". Aus diesem Grund sollte die MAPI AO nicht auf seriell geclusterten Inline-WAEs bereitgestellt werden, die eine Hochverfügbarkeitsgruppe bilden.

Die Symptome von MAPI-Verbindungen, die ihrer WAE-Zuordnungsgruppe entgehen, sind Outlook-Fehlersymptome wie doppelte Nachrichten oder Outlook, das nicht mehr reagiert.

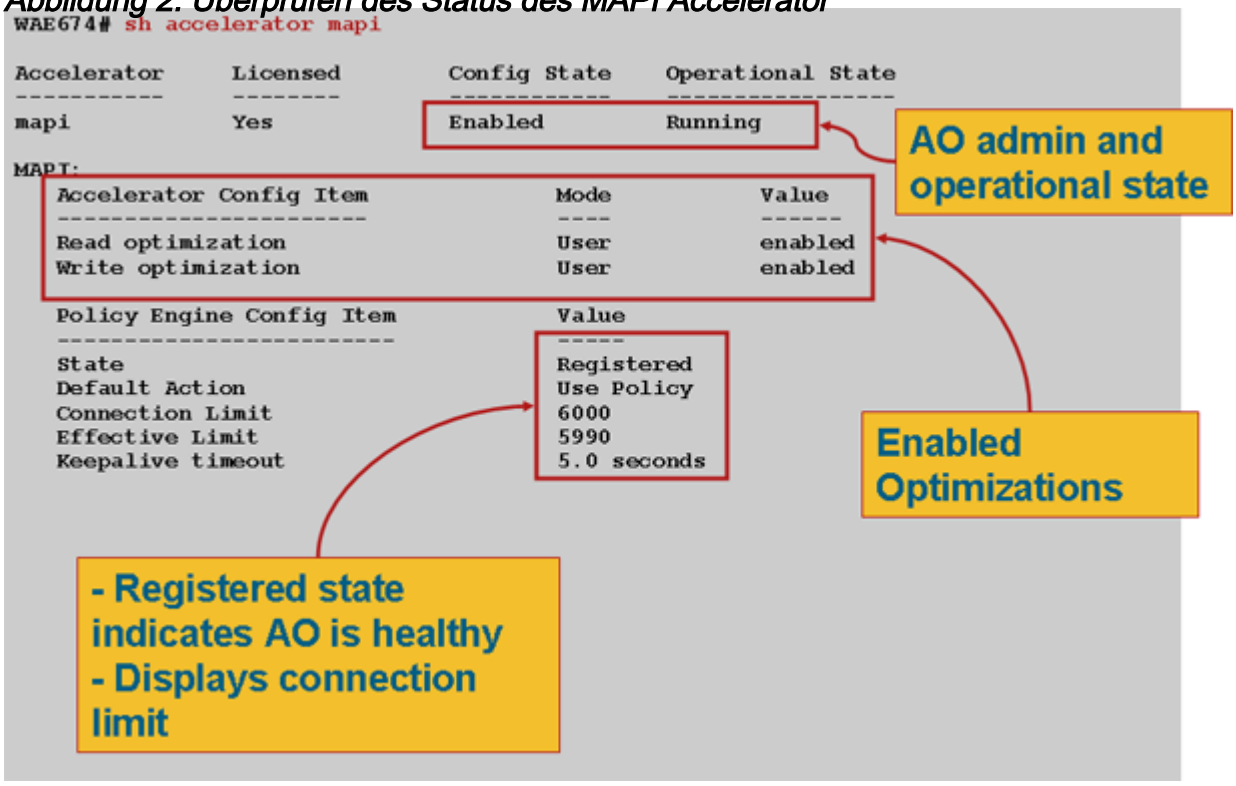
Bei einer TFO-Überlastung werden neue Verbindungen für eine bestehende Assoziationsgruppe durchlaufen und dem MAPI AO entweichen, sodass der MAPI AO eine Reihe von

Verbindungsressourcen vorab reserviert, um die Auswirkungen einer Überlastungsbedingung zu minimieren. Weitere Informationen zu reservierten MAPI-Verbindungen und deren Auswirkungen auf die Geräteüberlastung finden Sie im Abschnitt "MAPI Application Accelerator Reserved Connections Impact on Overload" im Artikel "Troubleshooting Overload Conditions".

Überprüfen Sie die allgemeine AO-Konfiguration und den allgemeinen Status mit dem **Show Accelerator** und **Anzeigen von Lizenzbefehlen**, wie im Artikel Problembehandlung bei Anwendungsbeschleunigung beschrieben. Die Enterprise-Lizenz ist für den MAPI Accelerator-Betrieb erforderlich, und der EPM Application Accelerator muss aktiviert sein.

Überprüfen Sie anschließend den für MAPI AO spezifischen Status, indem Sie den Befehl **show accelerator mapi** verwenden, wie in Abbildung 2 dargestellt. Sie möchten sehen, dass MAPI AO aktiviert, ausgeführt und registriert ist und dass die Verbindungsbeschränkung angezeigt wird. Wenn der Config State (Konfigurationsstatus) aktiviert ist, der Operational State jedoch Shutdown lautet, weist dies auf ein Lizenzierungsproblem hin.

Abbildung 2: Überprüfen des Status des MAPI Accelerator



Verwenden Sie den Befehl **show statistics accelerator epm**, um zu überprüfen, ob der EPM AO funktioniert. Stellen Sie sicher, dass die Zähler Gesamtzahl der verarbeiteten Verbindungen, Gesamtzahl der erfolgreich geparsten Anforderungen und Gesamtzahl der erfolgreich geparsten Antworten beim Starten eines Clients erhöht werden.

Mit dem Befehl **show running-config** können Sie überprüfen, ob die Datenverkehrsrichtlinien MAPI und EPM ordnungsgemäß konfiguriert sind. Sie möchten die **Mapi** für die Anwendungsaktion "E-Mail und Messaging" beschleunigen und möchten die MS-EndPortMapper-Klassifizierung und die Datenverkehrsrichtlinie wie folgt definieren:

```
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
```

Verwenden Sie den Befehl **show policy-engine application dynamic**, um zu überprüfen, ob dynamische Übereinstimmungsregeln vorhanden sind, wie folgt:

- Suchen Sie nach einer Regel mit Benutzer-ID: EPM und Map Name: uida4f1db00-ca47-1067-b31f-00dd010662da.
- Das Feld "Flows" gibt die Gesamtzahl der aktiven Verbindungen zum Exchange-Dienst an.
- Für jeden MAPI-Client sollte ein separater Eintrag mit der Benutzer-ID angezeigt werden: MAPI.

Verwenden Sie den Befehl **show statistics connection optimied mapi**, um zu überprüfen, ob das WAAS-Gerät optimierte MAPI-Verbindungen herstellt. Stellen Sie sicher, dass in der Spalte "Accel" (Aktiv) für MAPI-Verbindungen "M" angezeigt wird. Dies bedeutet, dass die MAPI-AO wie folgt verwendet wurde:

```
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"
```

Hinweis: In Version 4.1.5 wurde der Zähler Aktuelle reservierte Datenflüsse in die Ausgabe aufgenommen. Dieser Zähler bezieht sich auf die Anzahl der reservierten MAPI-Verbindungsressourcen auf der WAE, die derzeit nicht verwendet werden, aber für zukünftige MAPI-Verbindungen reserviert sind. Weitere Informationen zu reservierten MAPI-Verbindungen und deren Auswirkungen auf die Geräteüberlastung finden Sie im Abschnitt "MAPI Application Accelerator Reserved Connections Impact on Overload" im Artikel "Troubleshooting Overload Conditions".

Wenn Sie Verbindungen mit "TGDL" in der Spalte "Accel" beobachten, wurden diese Verbindungen auf die generische AO gedrückt und nur mit Transportoptimierungen optimiert. Wenn es sich um Verbindungen handelt, von denen erwartet wird, dass sie vom MAPI AO verarbeitet werden, kann dies daran liegen, dass es sich um verschlüsselte MAPI-Verbindungen handelt. Um die Anzahl der angeforderten verschlüsselten MAPI-Verbindungen zu überprüfen, verwenden Sie den Befehl **show statistics accelerator mapi**:

```
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
```

Die IP-Adressen von Clients, die verschlüsselte MAPI-Verbindungen anfordern, finden Sie im Syslog, indem Sie nach folgenden Nachrichten suchen:

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

Sie können die MAPI-Verbindungsstatistiken anzeigen, indem Sie den folgenden Befehl **show statistics connection optimied mapi detail** verwenden:

```
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
. . .
```

In dieser Ausgabe werden die Anzahl der lokalen und Remote-Antworten und die durchschnittlichen Antwortzeiten angezeigt:

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

Verschlüsselte MAPI-Beschleunigung

Zusammenfassung

Ab WAAS 5.0.1 kann der MAPI Accelerator den verschlüsselten MAPI-Datenverkehr beschleunigen. Diese Funktion wird in Version 5.0.3 standardmäßig aktiviert. Um jedoch den verschlüsselten MAPI-Datenverkehr erfolgreich zu beschleunigen, gibt es sowohl in der WAAS- als auch in der Microsoft AD-Umgebung eine Reihe von Anforderungen. Diese Anleitung hilft Ihnen, die eMAPI-Funktion zu überprüfen und Fehler zu beheben.

Informationen zu Funktionen

eMAPI wird standardmäßig in Version 5.0.3 aktiviert und erfordert Folgendes, um den verschlüsselten Datenverkehr erfolgreich zu beschleunigen.

1) Der sichere CMS-Speicher muss initialisiert und auf allen Core-WAEs geöffnet werden.

2) Die WAEs müssen in der Lage sein, den FQDN der Exchange-Server(s) und Kerberos KDC (Active Directory Controller) aufzulösen.

3) Die WAE-Uhren müssen mit dem KDC synchronisiert sein.

4) SSL ACCelerator, WAN Secure und eMAPI müssen auf allen WAEs im Pfad von Outlook zu Exchange aktiviert sein.

5) Die WAEs im Pfad müssen über die richtige Richtlinienzuordnungskonfiguration verfügen.

6) Für die Core-WAE(s) müssen eine oder mehrere konfigurierte Domänen-IDs für verschlüsselte Dienste konfiguriert sein (Benutzer- oder Systemkonto)

7) Wenn ein Computerkonto verwendet wird, muss diese WAE der AD-Domäne hinzugefügt werden.

8) Anschließend müssen die Objekte im Active Directory im Anwendungsfall für das System- oder Benutzerkonto spezifische Berechtigungen erhalten. "Verzeichnisänderungen replizieren" und "Alle Verzeichnisänderungen replizieren" müssen jeweils auf Zulassen eingestellt werden.

Die empfohlene Vorgehensweise hierfür ist die Verwendung einer Universal Security-Gruppe (z. B. die Berechtigungen der Gruppe zuweisen und dann die im Verschlüsselungsdienst angegebenen WAAS-Geräte und/oder Benutzernamen dieser Gruppe hinzufügen). Screenshots der AD-Konfiguration und der grafischen Benutzeroberfläche von WAAS CM finden Sie in der beigefügten Anleitung.

Fehlerbehebungsmethode

Schritt 1: Überprüfen der Konfiguration der Identität des Verschlüsselungsdienstes und des erfolgreichen Abrufs von Schlüsseln

Während der Diagnosebefehl (Schritt 2 unten) das Vorhandensein eines Verschlüsselungsdienstes überprüft, überprüft er nicht, ob der Schlüsselabruf erfolgreich ist. Daher wissen wir nicht, wenn wir nur diesen Diagnosebefehl ausführen, wenn dem Objekt in Active Directory (entweder System- oder Benutzerkonto) die entsprechenden Berechtigungen erteilt wurden.

Zusammenfassung der erforderlichen Schritte zur Konfiguration und Verifizierung des Verschlüsselungsdienstes für den erfolgreichen Abruf von Schlüsseln

Benutzerkonto:

1. AD-Benutzer erstellen

2. AD-Gruppe erstellen und "Verzeichnisänderungen replizieren" und "Alle Verzeichnisänderungen replizieren" auf ZULÄSSIG einstellen

3. Fügen Sie den Benutzer der erstellten Gruppe hinzu

4. Definition der Domänenidentität von Benutzerkonten in Verschlüsselungsdiensten

5. get-Schlüsseldiagnose-CLI ausführen

windows-domain diagnostics encryption-service get-key <Exchange-Server-FQDN> <Domänenname>

Beachten Sie, dass Sie den auf dem Server konfigurierten tatsächlichen/echten Exchange-Servernamen und nicht einen NLB/VIP-Typ FQDN verwenden sollten, der in mehrere Exchange-Server aufgelöst werden kann.

6. ob Schlüsselabruf funktioniert hat - fertig

Erfolgsbeispiel:

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

SPN pdidc-exchange1.pdidc.cisco.com, Domänenname: pdidc.cisco.com

Schlüsselabruf wird durchgeführt.

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

SPN pdidc-exchange1.pdidc.cisco.com, Domänenname: pdidc.cisco.com

Der Schlüssel für pdidc-exchange1.pdidc.cisco.com befindet sich im Speicherschlüssel-Cache.

Systemkonto

1. Verbinden von Core-WAE-Geräten mit AD-Domäne

2. erstellen Sie die AD-Gruppe, und legen Sie "Verzeichnisänderungen replizieren" und "Alle Verzeichnisänderungen replizieren" auf ZULASSEN fest.

3. Hinzufügen von Maschinenkonten zur erstellten Gruppe

4. Konfiguration von Verschlüsselungsdiensten zur Verwendung des Computerkontos

5. Geben Sie einige Zeit, um die Gruppenrichtlinie auf den verbundenen Computer anzuwenden, oder erzwingen Sie die Anwendung der Gruppenrichtlinie vom AD. gpupdate /force.

6. get-Schlüsseldiagnose-CLI ausführen

windows-domain diagnostics encryption-service get-key <Exchange-Server-FQDN> <Domänenname>

Beachten Sie, dass Sie den auf dem Server konfigurierten tatsächlichen/echten Exchange-Servernamen und nicht einen NLB/VIP-Typ FQDN verwenden sollten, der in mehrere Exchange-Server aufgelöst werden kann.

7. ob Schlüsselabruf funktioniert hat - fertig

Weitere Informationen und Screenshots zum Verschlüsselungsdienst und zur AD-Konfiguration finden Sie in der angehängten Anleitung.

Schritt 2 - In 5.0.3 wurde ein neuer Diagnosebefehl eingeführt, um einige der erforderlichen Einstellungen zu überprüfen.

Beschleunigungszuordnung

1.CLI führt verschiedene Validierungsprüfungen durch. Die Ausgabe ist eine Zusammenfassung der Fähigkeit, den verschlüsselten MAPI-Datenverkehr als Edge oder Core zu beschleunigen.

2. Überprüft die Status-/Konfigurationsattribute der verschiedenen Komponenten, damit der Verschlüsselungsdienst ordnungsgemäß funktioniert.

3. Wenn ein Konfigurationsproblem gefunden wird, werden fehlende Elemente sowie die CLI oder die zu seiner Behebung erforderlichen Aktionen ausgegeben.

4. Die Zusammenfassung wird als Edge-Gerät und Core-Gerät angezeigt. Geräte, die sowohl Edge- als auch Core-Geräte sein können, sollten über EMAPI verfügen, die sowohl für Edge- als auch Core-Geräte verwendet werden kann.

Im Folgenden finden Sie eine Beispielausgabe einer falsch konfigurierten WAE:

```
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
```

Die folgende Ausgabe stammt von einer Core-WAE, die richtig konfiguriert wurde:

```
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
```

Schritt 3 - Überprüfen Sie manuell die WAE-Einstellungen, die nicht mit dem Diagnosehandbuch oben überprüft werden.

1) Der obige Befehl überprüft zwar, ob NTP konfiguriert ist, überprüft jedoch nicht, ob die Zeiten zwischen der WAE und dem KDC synchronisiert sind. Es ist sehr wichtig, dass die Zeiten zwischen Core und KDC synchronisiert sind, damit der Schlüsselabruf erfolgreich ist.

Wenn bei der manuellen Prüfung festgestellt wird, dass die Synchronisierung der WAE nicht durchgeführt werden kann, ist der Befehl ntpdate (**ntpdate <KDC ip>**) ein einfaches Verfahren, um die Synchronisierung der WAE zu erzwingen. Zeigen Sie dann die WAEs auf den NTP-Server des Unternehmens.

2) Überprüfen Sie, ob **dnslookup** auf allen WAEs für den FQDN der Exchange-Server und den FQDN der KDCs erfolgreich ist.

3) Überprüfen Sie, ob die Klassenzuordnung und die Richtlinienzuordnung auf allen WAEs im Pfad korrekt konfiguriert sind.

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

Class-Map-Typ waas match-any MAPI

Zuordnen von TCP-Ziel-epm-Mapi (0 Flow-Matches)

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

WAAS-GLOBAL (insgesamt 6084690)

Class MAPI (0 Flow-Matches)
Optimierung der vollständigen Beschleunigung von Mapi-Anwendungen E-Mail und Messaging

4) Überprüfen Sie, ob der sichere CMS-Speicher geöffnet und auf allen WAEs "show cms secure store" initialisiert ist.

Datenanalyse

Neben der Analyse der Ausgabe des Diagnosebefehls und der manuellen Anzeigebefehle müssen Sie möglicherweise auch den Sysreport überprüfen.

Insbesondere sollten Sie die mapiao-errorlog, sr-errorlog (nur Core WAE) und wsao-errorlog Dateien überprüfen.

Je nach Szenario gibt es Hinweise in jedem Protokoll, die dazu führen, dass Verbindungen zu Generic AO (Generische AO) abgelegt werden.

Als Referenz dient hier eine Beispielausgabe mit verschiedenen Arbeitskomponenten.

Diese Ausgabe stammt von sr-errorlog und zeigt die Validierung der Identität des Maschinenkontenverschlüsselungsdienstes an.

Hinweis: Dies bestätigt nur, dass die Core-WAE der Domäne beigetreten ist und das Computerkonto vorhanden ist.

```
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]
```

Diese Ausgabe stammt wieder aus dem Core sr-errorlog und zeigt einen erfolgreichen Schlüsselabruf von 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]
```

Diese Ausgabe stammt aus der mapiao-errorlog-Datei auf der Edge WAE für eine erfolgreiche eMAPI-Verbindung.

```
'''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]
```

Hier ist die entsprechende Core-WAE-Ausgabe von mapiao-errorlog für die gleiche TCP-Verbindung.

```
'''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]'''
```

Häufige Probleme

Nachstehend finden Sie einige häufige Gründe, die zu einer eMAPI-Verbindung führen Übergabe an Generic AO (TG).

Problem 1: Die auf der Core-WAE konfigurierte Identität des Verschlüsselungsdiensts verfügt nicht über die richtigen Berechtigungen in AD.

Ausgabe von SRE-Fehlerprotokollen auf Core WAE

```
09/25/2012 18:47:54.147(Local)(9063 0.1) ERRO (147570) session(0x517fa0) Failed to Retrieve Key
from AD for SPN:exchangeMDB/outlook.sicredi.net.br error:16 [SRKeyRetriever.cpp:267]
'''09/25/2012 18:47:54.147(Local)(9063 0.1) ERRO (147592) Key retrieval failed with Status 16
[SRKeyMgr.cpp:157]
''''''09/25/2012 18:47:54.147(Local)(9063 0.1) ERRO (147623) Identity "WAASMacAct" has been
blacklisted [SRDiIdMgr.cpp:258]
''''''09/25/2012 18:47:54.147(Local)(9063 0.1) ERRO (147631) Key retrieval failed due to
permission issue [SRKeyMgr.cpp:167]
'''09/25/2012 18:47:54.147(Local)(9063 0.1) ERRO (147636) Identity: WAASMacAct will be black
listed. [SRKeyMgr.cpp:168]
```

```
09/25/2012 18:47:54.147(Local)(9063 0.1) NTCE (147657) Calling KrbKeyResponse  key handler in
srlib [SRServer.cpp:189]
09/25/2012 18:47:54.147(Local)(9063 0.1) NTCE (147722) Queued send reponse buffer to client task
[SrlibServerTransport.cpp:136]
09/25/2012 18:47:54.147(Local)(9063 0.1) NTCE (147730) KrbKeyResponse, sent to client session
object [SrlibServer.cpp:203]
09/25/2012 18:47:54.147(Local)(9063 0.0) NTCE (147733) SendNextCmd isDuringSend 0, WriteQueue
size 1 isDuringClose 0 [SrlibServerTransport.cpp:308]
09/25/2012 18:47:54.147(Local)(9063 0.1) NTCE (147740) Send Key response to the Client
```

Auflösung 1: Lesen Sie den Konfigurationsleitfaden, und überprüfen Sie, ob das Objekt in AD über die richtigen Berechtigungen verfügt. "Verzeichnisänderungen replizieren" und "Alle Verzeichnisänderungen replizieren" müssen jeweils auf Zulassen eingestellt werden.

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

Problem 2: Zwischen der Core-WAE und dem KDC, von dem der Schlüssel abgerufen werden soll, besteht ein Zeitverzug.

Ausgabe von SRE-Fehlerprotokollen auf 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]
```

Auflösung 2: Verwenden Sie ntpdate auf allen WAEs (insbesondere dem Core), um die Uhr mit dem KDC zu synchronisieren. Zeigen Sie dann auf den NTP-Server des Unternehmens (vorzugsweise identisch mit dem KDC).

Problem 3: Die Domäne, die Sie für den Verschlüsselungsdienst definiert haben, stimmt nicht mit der Domäne überein, in der sich Ihr Exchange-Server befindet.

Ausgabe von SRE-Fehlerprotokollen auf 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]
```

Auflösung 3: Wenn Ihre Core-WAE-Services mehrere Exchange-Server in verschiedenen Domänen umfassen, müssen Sie eine Verschlüsselungs-Service-Identität für jede Domäne konfigurieren, in der sich die Exchange-Server befinden.

Beachten Sie, dass es derzeit KEINE Unterstützung für Subdomain include gibt. Wenn Sie also myexchange.sub-domain.com haben, muss sich die Identität des Verschlüsselungsdiensts unter domain.domain.com befinden. KANN NICHT in der übergeordneten Domäne sein.

Problem 4: Wenn WANSecure ausfällt, können Ihre Verbindungen auf TG

eMAPI-Verbindungen können an generische AO übergeben werden, da die sichere WAN-Einrichtung fehlschlägt. WAN Secure Plumb ist fehlgeschlagen, weil die Zertifikatsüberprüfung fehlgeschlagen ist. Die Peer-Zertifizierungsprüfung schlägt fehl, da das selbstsignierte Peer-Standardzertifikat verwendet wird oder die Zertifizierung die OCSP-Prüfung rechtmäßig nicht bestanden hat.

Core-WAE-Einstellungen

```
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
```

Dies führt zu folgenden mapiao-errorlog- und wsao-errorlog-Einträgen:

Der Hinweis hier ist die erste hervorgehobene Zeile "Mehr als vier Mal in Folge getrennt".

Mapiao-errorlog auf clientseitiger 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]
```

WAE-Fehlerprotokoll auf clientseitiger 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]
```

Auflösung 4: Entfernen Sie Peer-Zertifikate, und überprüfen Sie die Konfiguration von beiden WAEs, und starten Sie den Verschlüsselungsdienst auf den Core-WAEs neu.

```
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
```

Problem 5: Wenn NTLM vom Outlook-Client verwendet wird, wird die Verbindung auf Generic AO (Generisches AO) gekürzt.

Im mapiao-errorlog auf der Client-Seite wird Folgendes angezeigt:

```
'''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]
```

Auflösung 5: Der Kunde muss die Kerberos-Authentifizierung in seiner Exchange-Umgebung aktivieren/erfordern. NTLM wird NICHT unterstützt (ab 5.1)

Beachten Sie, dass es eine Microsoft-Technikbeschreibung gibt, in der ein Fall auf NTLM zurückgerufen wird, wenn ein CAS verwendet wird.

Das Szenario, in dem Kerberos nicht funktioniert, ist spezifisch für Exchange 2010 und im folgenden Szenario beschrieben:

Mehrere Exchange Client Access Server (CAS) in einer Organisation/Domäne.
Diese CAS-Server werden mithilfe beliebiger Methoden geclustert, entweder mithilfe der integrierten Client-Array-Funktion von Microsoft oder eines Load Balancers eines Drittanbieters.

Im obigen Szenario funktioniert Kerberos nicht - und die Clients werden standardmäßig auf NTLM zurückgreifen. Ich glaube, dies ist darauf zurückzuführen, dass die Clients zum CAS-Server AUTH haben gegenüber dem Mailbox-Server, wie sie es in früheren Exchange-Veröffentlichungen getan haben.

In Exchange 2010 RTM gibt es dafür keine Lösung! Kerberos in dem obigen Szenario funktioniert nie vor Exchange 2010-SP1.

In SP1 kann Kerberos in diesen Umgebungen aktiviert werden, aber es ist ein manueller Prozess. Lesen Sie den Artikel hier: http://technet.microsoft.com/en-us/library/ff808313.aspx

MAPI AO-Protokollierung

- Die folgenden Protokolldateien sind zur Behebung von MAPI AO-Problemen verfügbar:
- Transaktionsprotokolldateien: /local1/logs/tfo/working.log (und /local1/logs/tfo/tfo_log_*.txt)

Debugging-Protokolldateien: /local1/errorlog/mapiao-errorlog.current (und mapiao-errorlog.*)

Um das Debuggen zu vereinfachen, sollten Sie zunächst eine ACL einrichten, um Pakete auf einen Host zu beschränken.

```
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
```

Um die Transaktionsprotokollierung zu aktivieren, verwenden Sie den folgenden Konfigurationsbefehl für Transaktionsprotokolle:

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

Sie können das Ende einer Transaktionsprotokolldatei mithilfe des Befehls type-tail wie folgt anzeigen:

```
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
```

Verwenden Sie die folgenden Befehle, um die Debug-Protokollierung des MAPI AO einzurichten

und zu aktivieren.
HINWEIS: Die Debug-Protokollierung ist CPU-intensiv und kann eine große Menge an Ausgabe generieren. Verwenden Sie sie sorgfältig und sparsam in einer Produktionsumgebung.
Sie können die detaillierte Protokollierung auf dem Datenträger wie folgt aktivieren:

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

Sie können die Debug-Protokollierung für Verbindungen in der ACL wie folgt aktivieren:

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

Die Optionen für das MAPI-AO-Debuggen sind wie folgt:

```
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
```

Sie können die Debug-Protokollierung für MAPI-Verbindungen aktivieren und dann das Ende des Debug-Fehlerprotokolls wie folgt anzeigen:

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