

WAAS - Identificação e solução de problemas do MAPI AO

Capítulo: Troubleshooting de MAPI AO

Este artigo descreve como solucionar problemas do MAPI AO.

Contents

- [1 Acelerador de MAPI](#)
- [2 Aceleração de MAPI criptografada](#)
 - [2.1 Summary](#)
 - [2.2 Informações do recurso](#)
 - [2.3 Metodologia de solução de problemas](#)
 - [2.3.1 Etapa 1 - Verificar a configuração da Identidade do serviço de criptografia e o sucesso da recuperação da chave](#)
 - [2.3.2 Etapa 2 - No 5.0.3, um novo comando de diagnóstico foi introduzido para verificar algumas das configurações necessárias.](#)
 - [2.3.3 Etapa 3 - Verificar manualmente as configurações do WAE que não foram verificadas pelo comando de diagnóstico acima.](#)
 - [2.4 Análise de dados](#)
 - [2.5 Problemas comuns](#)
 - [2.5.1 Problema 1: A identidade do serviço de criptografia configurada no Core WAE não tem as permissões corretas no AD.](#)

Co

Art

En

trát

Sol

Oti

Trc

Trc

Trc

Trc

Trc

Trc

Trc

Sol

Trc

Trc

Trc

Sol

Sol

Sol

Sol

Sol

Trc

- [2.5.2 Resolução 1: Consulte o guia de configuração e verifique se o objeto no AD tem as permissões corretas. "Replicando alterações de diretório" e "Replicando alterações de diretório tudo" devem ser definidos para permitir.](#)
 - [2.5.3 Problema 2: Há um desvio de tempo entre o Core WAE e o KDC a partir do qual ele tenta obter a chave](#)
 - [2.5.4 Resolução 2: Use a atualização em todos os WAEs \(especialmente o Núcleo\) para sincronizar o relógio com o KDC. Em seguida, aponte para o servidor NTP empresarial \(preferencialmente o mesmo que o KDC\).](#)
 - [2.5.5 Problema 3: O domínio definido para o serviço de Criptografia não corresponde ao domínio em que o servidor Exchange está.](#)
 - [2.5.6 Resolução 3: Se o seu Core WAE atender a vários servidores Exchange em domínios diferentes, você deverá configurar uma Identidade de serviço de criptografia para cada domínio em que os servidores Exchange residem.](#)
 - [2.5.7 Problema 4: Se a WANSecure falhar, suas conexões podem cair para TG](#)
 - [2.5.8 Resolução 4: Remova a configuração do peer cert de ambos os WAEs e reinicie o serviço de criptografia no\(s\) Core WAE\(s\).](#)
 - [2.5.9 Problema 5: Se o NTLM for usado pelo cliente do Outlook, a conexão será enviada para o AO genérico.](#)
 - [2.5.10 Resolução 5: O cliente deve habilitar/exigir a autenticação Kerberos em seu ambiente Exchange. NTLM NÃO é suportado \(a partir de 5.1\)](#)
- [3 Registro MAPI AO](#)

Acelerador de MAPI

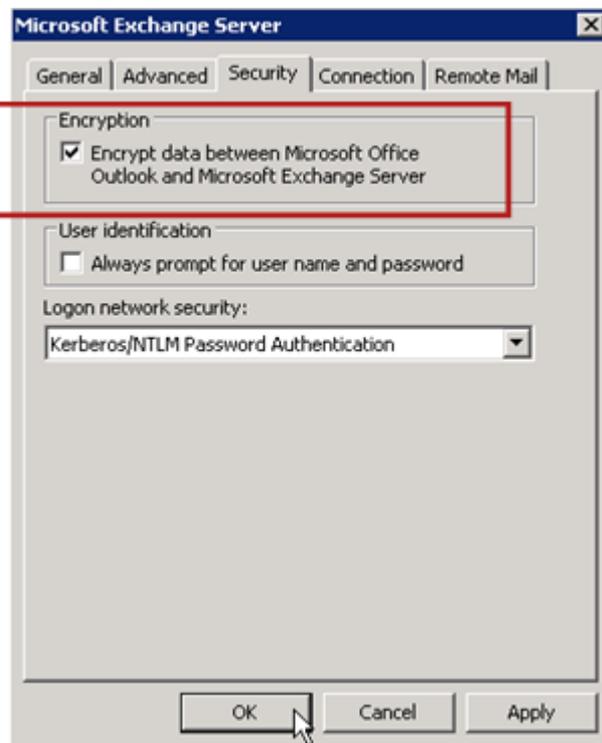
O acelerador MAPI otimiza o tráfego de e-mail do Microsoft Outlook Exchange. O Exchange usa o protocolo EMSMDB, que está em camadas no MS-RPC, que por sua vez usa TCP ou HTTP (não suportado) como transporte de baixo nível.

O MAPI AO oferece suporte a clientes do Microsoft Outlook 2000 a 2007 para o tráfego em cache e no modo não em cache. As conexões seguras que usam autenticação de mensagens (assinatura) ou criptografia não são aceleradas pelo MAPI AO. Essas conexões e conexões de clientes mais antigos são transferidas ao AO genérico para otimização de TFO. Além disso, as conexões OWA (Outlook Web Access) e Exchange-Exchange não são suportadas.

Note: O Microsoft Outlook 2007 tem a criptografia habilitada por padrão. Você deve desativar a criptografia para se beneficiar do MAPI application accelerator. No Outlook, escolha **Ferramentas > Contas de E-mail**, escolha **Exibir ou Alterar Contas de E-mail Existentes** e clique em **Avançar**. Escolha a conta do Exchange e clique em **Alterar**. Clique em **Mais configurações** e, em seguida, clique na guia **Segurança**. Desmarque a caixa de seleção **Criptografar dados entre o Microsoft Office Outlook e o Microsoft Exchange Server**, como mostrado na Figura 1.

Como alternativa, você pode desativar a criptografia para todos os usuários de um Exchange Server usando uma [Política de Grupo](#).

Figura 1. Desativando a criptografia no Outlook 2007



Nos seguintes casos, o MAPI AO não lida com uma conexão:

- Conexão criptografada (entregue ao AO genérico)
- Cliente não suportado (entregue ao AO genérico)
- Erro de análise irrecuperável. Todas as conexões TCP entre o cliente e o serviço do servidor são desconectadas. Quando o cliente se reconecta, todas as conexões são transferidas para o AO genérico.
- O cliente tenta estabelecer um novo grupo de associação na conexão quando o WAE está sobrecarregado.
- O cliente estabelece uma conexão quando o WAE está sobrecarregado e os recursos de conexão reservados para MAPI não estão disponíveis.

O cliente e o servidor do Outlook interagem em uma sessão através de um grupo de conexões TCP chamado de grupo de associação. Em um grupo de associação, os acessos a objetos podem abranger qualquer conexão e as conexões são criadas e liberadas dinamicamente conforme necessário. Um cliente pode ter mais de um grupo de associação aberto ao mesmo tempo para servidores diferentes ou para o mesmo servidor. (As pastas públicas são implantadas em servidores diferentes do armazenamento de mensagens.)

É essencial que todas as conexões MAPI dentro de um grupo de associação passem pelo mesmo par de WAEs na filial e no data center. Se algumas conexões dentro de um grupo de associação não passarem pelo MAPI AO nesses WAEs, o MAPI AO não verá as transações executadas nessas conexões e as conexões serão consideradas para "escapar" do grupo de associação. Por esse motivo, o MAPI AO não deve ser implantado em WAEs em linha agrupadas em série que formam um grupo de alta disponibilidade.

Os sintomas das conexões MAPI que escapam de seu grupo de associação WAE são sintomas de erro do Outlook, como mensagens duplicadas ou o Outlook para de responder.

Durante uma condição de sobrecarga de TFO, novas conexões para um grupo de associação existente seriam passadas e escapariam do MAPI AO, de modo que o MAPI AO reserva uma série de recursos de conexão com antecedência para minimizar o impacto de uma condição de sobrecarga. Para obter mais detalhes sobre as conexões MAPI reservadas e seu impacto na

sobrecarga do dispositivo, consulte a seção ["MAPI Application Accelerator Reserved Connections Impact on Overload"](#) no artigo Troubleshooting de Condições de Sobrecarga.

Verifique a configuração e o status gerais do AO com os comandos **show accelerator** e **show license**, conforme descrito no artigo [Troubleshooting Application Acceleration](#). A licença Enterprise é necessária para a operação do MAPI accelerator e o EPM application accelerator deve ser ativado.

Em seguida, verifique o status específico do MAPI AO usando o comando **show accelerator mapi**, como mostrado na Figura 2. Você deseja ver que o MAPI AO está Habilitado, em Execução e Registrado e que o limite de conexão é exibido. Se o estado de configuração estiver ativado, mas o estado operacional estiver desativado, isso indica um problema de licenciamento.

Figura 2. Verificando o status do acelerador MAPI

```
WAE674# sh accelerator mapi
```

Accelerator	Licensed	Config State	Operational State
mapi	Yes	Enabled	Running

MAPI:

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

Policy Engine Config Item

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

AO admin and operational state

Enabled Optimizations

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

Use o comando **show statistics accelerator epm** para verificar se o EPM AO está funcional. Verifique se o Total de conexões tratadas, Total de solicitações analisadas com êxito e Total de respostas analisadas com êxito aumentam quando um cliente é iniciado.

Use o comando **show running-config** para verificar se as políticas de tráfego MAPI e EPM estão configuradas corretamente. Você deseja ver o **mapa acelerado** para a ação do aplicativo Email e Mensagens e deseja ver o classificador MS-EndPointMapper e a política de tráfego definidos da seguinte forma:

```
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
```

Use o comando **show policy-engine application dynamic** para verificar se as regras de correspondência dinâmica existem, como a seguir:

- Procure uma regra com ID de usuário: EPM e Nome do Mapa: uuida4f1db00-ca47-1067-b31f-00dd010662da.
- O campo Fluxos indica o número total de conexões ativas com o serviço do Exchange.
- Para cada cliente MAPI, você deve ver uma entrada separada com a ID de usuário: MAPI.

Use o comando **show statistics connection optimized mapi** para verificar se o dispositivo WAAS está estabelecendo conexões MAPI otimizadas. Verifique se "M" aparece na coluna Accel para conexões MAPI, o que indica que o MAPI AO foi usado, da seguinte forma:

```
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: Na versão 4.1.5, o contador Fluxos Reservados Atuais foi adicionado na saída. Este contador refere-se ao número de recursos de conexão MAPI reservados no WAE que estão atualmente não utilizados, mas reservados para futuras conexões MAPI. Para obter mais detalhes sobre as conexões MAPI reservadas e seu impacto na sobrecarga do dispositivo, consulte a seção ["MAPI Application Accelerator Reserved Connections Impact on Overload"](#) no artigo Troubleshooting de Condições de Sobrecarga.

Se você observar conexões com "TGDL" na coluna Accel, essas conexões foram enviadas ao AO genérico e otimizadas somente com otimizações de transporte. Se essas são conexões que você esperava que fossem tratadas pelo MAPI AO, pode ser porque são conexões MAPI criptografadas. Para verificar o número de conexões MAPI criptografadas que foram solicitadas, use o comando **show statistics accelerator mapi** da seguinte maneira:

```
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

```

Você pode encontrar os endereços IP dos clientes que solicitam conexões MAPI criptografadas no syslog, procurando mensagens como:

```

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

```

Você pode exibir as estatísticas da conexão MAPI usando o comando **show statistics connection optimized mapi detail** da seguinte forma:

```

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:               uuida4f1ldb00-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
. . .

```

As contagens de resposta local e remota e os tempos de resposta médios são mostrados nesta saída:

```

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

```

Aceleração de MAPI criptografada

Summary

A partir do WAAS 5.0.1, o acelerador MAPI pode acelerar o tráfego MAPI criptografado. Esse recurso será ativado por padrão na versão 5.0.3. No entanto, para acelerar com êxito o tráfego MAPI criptografado, há vários requisitos no ambiente WAAS e Microsoft AD. Este guia o ajudará a verificar e solucionar problemas da funcionalidade eMAPI.

Informações do recurso

O eMAPI será ativado por padrão no 5.0.3 e exigirá que os itens a seguir acelerem com êxito o tráfego criptografado.

- 1) O armazenamento seguro do CMS deve ser inicializado e aberto em todos os Núcleos WAEs
- 2) Os WAEs devem ser capazes de resolver o FQDN do(s) servidor(es) Exchange e o Kerberos KDC (Active Directory Controller)
- 3) Os relógios do WAE devem estar em sincronia com o KDC
- 4) O acelerador SSL, a WAN segura e o eMAPI devem ser ativados em todos os WAEs no caminho do Outlook para o Exchange
- 5) Os WAEs no caminho devem ter a configuração correta do mapa de políticas
- 6) O(s) WAE(s) principal(is) deve(m) ter(m) uma ou mais identidades de domínio de serviços criptografados configuradas (conta do usuário ou da máquina)
- 7) Se uma conta de máquina for usada, esse WAE deverá ser associado ao domínio do AD.
- 8) Em seguida, com o caso de uso da conta da máquina ou do usuário, esses objetos no Active Directory precisam receber permissões específicas. "Replicando alterações de diretório" e "Replicando alterações de diretório tudo" devem ser definidos para permitir.

A maneira recomendada de fazer isso é por meio de um grupo de Segurança Universal (por exemplo, atribuir as permissões ao grupo e, em seguida, adicionar os dispositivos WAAS e/ou nomes de usuário especificados no serviço de Criptografia a esse grupo). Consulte o guia anexado para obter capturas de tela da configuração do AD e da GUI do WAAS CM.

Metodologia de solução de problemas

Etapa 1 - Verificar a configuração da identidade do serviço de criptografia e o sucesso da recuperação da chave

Embora o comando de diagnóstico (etapa 2 abaixo) verifique a existência de um serviço de criptografia, ele não verifica se a recuperação da chave será bem-sucedida. Portanto, não sabemos apenas executando esse comando de diagnóstico se as permissões apropriadas foram dadas ao objeto no Active Directory (conta de máquina ou usuário).

Resumo do que precisa ser feito para configurar e verificar se o serviço de criptografia obterá êxito na recuperação de chave

Conta de usuário:

1. criar usuário do AD
2. criar grupo AD e definir "Replicando alterações de diretório" e "Replicando alterações de diretório tudo" como PERMITIR
3. adicionar o usuário ao grupo criado
4. definir identidade de domínio de conta de usuário em serviços de criptografia

5. run get key diagnostic cli

windows-domain diagnostics encryption-service get-key <exchange server FQDN> <domain name>

Observe que você deve usar o nome do servidor real/real do exchange configurado no servidor e não um FQDN do tipo NLB/VIP que possa ser resolvido para vários servidores Exchange.

6. se a recuperação da chave funcionou - concluído

Exemplo de sucesso:

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

SPN pdidc-exchange1.pdidc.cisco.com, Nome do domínio: pdidc.cisco.com

A recuperação da chave está em curso.

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

SPN pdidc-exchange1.pdidc.cisco.com, Nome do domínio: pdidc.cisco.com

**A chave para pdidc-exchange1.pdidc.cisco.com reside no cache de chave de memória
conta da máquina**

1. juntar dispositivos WAE principais ao domínio do AD

2. criar grupo do AD e definir "Replicando alterações de diretório" e "Replicando alterações de diretório tudo" como PERMITIR

3. adicionar conta(s) de máquina ao grupo criado

4. configurar serviços de criptografia para usar a conta da máquina

5. Dê algum tempo para que a Política de Grupo seja aplicada à máquina associada ou force a aplicação da política de grupo do AD. gpupdate /force.

6. run get key diagnostic cli

windows-domain diagnostics encryption-service get-key <exchange server FQDN> <domain name>

Observe que você deve usar o nome do servidor real/real do exchange configurado no servidor e não um FQDN do tipo NLB/VIP que possa ser resolvido para vários servidores Exchange.

7. se a recuperação da chave funcionou - concluído

Para obter mais detalhes e capturas de tela no serviço de criptografia e na configuração do AD, consulte o guia anexado.

Etapa 2 - No 5.0.3, um novo comando de diagnóstico foi introduzido para verificar algumas das

configurações necessárias.

– accelerator mapi verificar configurações de criptografia

1. A CLI faz várias verificações de validade. A saída é um resumo da capacidade de acelerar o tráfego MAPI criptografado como borda ou núcleo.
2. Verifica os atributos de status/configuração dos vários componentes para que o serviço de criptografia funcione corretamente.
3. Quando um problema de configuração é encontrado, ele mostra o que está faltando e a CLI ou ações para corrigi-lo.
4. Ele apresenta o resumo como dispositivo Edge e dispositivo Core. O dispositivo que pode ser tanto borda quanto núcleo deve ter a EMAPI operacional para borda e núcleo.

Abaixo está um exemplo de saída de um WAE configurado incorretamente:

```
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

```

Abaixo está a saída de um Core WAE configurado corretamente:

```

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

```

Etapa 3 - Verificar manualmente as configurações do WAE que não foram verificadas pelo comando de diagnóstico acima.

1) O comando acima, enquanto verifica a existência do NTP configurado, não verifica realmente se os horários estão em sincronia entre o WAE e o KDC. É muito importante que os tempos estejam em sincronia entre o Core e o KDC para que a recuperação de chaves seja bem-sucedida.

Se a verificação manual revelar que eles estão fora de sincronia, uma maneira simples de forçar o relógio do WAE a estar em sincronia seria o comando `ntpdate <KDC ip>`. Em seguida, aponte os WAEs para o servidor NTP da empresa.

2) Verifique se `dnslookup` foi bem-sucedido em todos os WAEs para o FQDN dos servidores Exchange e o FQDN dos KDCs

3) Verifique se o mapa de classe e o mapa de política estão configurados corretamente em todos os WAEs no caminho.

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

Class-map type waas match-any MAPI

Corresponder mapi de epm de destino tcp (0 correspondências de fluxo)

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

WAAS-GLOBAL (total de 6084690)

Classe MAPI (0 flow-match)

otimizar o aplicativo mapi completo de aceleração de e-mail e mensagens

4) Verifique se o armazenamento seguro do CMS está aberto e inicializado em todos os WAEs "show cms secure store"

Análise de dados

Além de analisar a saída do comando de diagnóstico e dos comandos show manuais, talvez você precise revisar o sysreport.

Especificamente, você vai querer rever os arquivos mapiao-errorlog, sr-errorlog (somente WAE central) e wsao-errorlog.

Haverá dicas em cada log, dependendo do cenário que o levará ao motivo das conexões caírem para o AO genérico.

Como referência, aqui está um exemplo de saída mostrando vários componentes em funcionamento

Esta saída é do sr-errorlog e mostra a validação da identidade do serviço de criptografia de conta da máquina

Note: Isso só confirma que o Core WAE ingressou no domínio e que a conta da máquina existe.

```
07/03/2012 19:12:07.278(Local)(6249 1.5) NTCE (278902) Adding Identity MacchineAcctWAAS to map
active list in SRMain [SRMain.cpp:215]
07/03/2012 19:12:07.279(Local)(6249 1.5) NTCE (279018) Adding identity(MacchineAcctWAAS) to Map
[SRDiIdMgr.cpp:562]
07/03/2012 19:12:07.279(Local)(6249 1.5) NTCE (279282) Activate Id: MacchineAcctWAAS
[SRMain.cpp:260]
07/03/2012 19:12:07.279(Local)(6249 1.5) NTCE (279306) Identity MacchineAcctWAAS found in the
Map [SRDiIdMgr.cpp:702]
07/03/2012 19:12:07.279(Local)(6249 1.5) NTCE (279321) Authentication for ID: MacchineAcctWAAS
[SRDiIdMgr.cpp:398]
07/03/2012 19:12:07.330(Local)(6249 1.5) NTCE (330581) Authentication success, tkt validity
starttime 1341342727 endtime 1341378727 [SRDiIdMgr.cpp:456]
07/03/2012 19:12:07.330(Local)(6249 1.5) NTCE (330599)
ID_TAG :MacchineAcctWAAS
Name : pdi-7541-dc
Domain : PDIDC.CISCO.COM
Realm : PDIDC.CISCO.COM
CLI_GUID :
SITE_GUID :
CONF_GUID :
Status:ENABLED
Black_Listed:NO
AUTH_STATUS: SUCCESS
ACCT_TYPE:Machine [SRIdentityObject.cpp:85]
```

07/03/2012 19:12:07.331(Local)(6249 1.5) NTCE (331685) DN Info found for domain PDIDC.CISCO.COM [SRIdentityObject.cpp:168]
07/03/2012 19:12:07.347(Local)(6249 1.5) NTCE (347680) Import cred successfull for pn: pdi-7541-dc@PDIDC.CISCO.COM [AdsGssCli.cpp:111]

Esta saída é do Core sr-errorlog novamente e mostra a recuperação de chave bem-sucedida do KDC.

10/23/2012 15:46:55.673(Local)(3780 1.2) NTCE (673766) Key Not Found in cache, initiating retrieval for spn:exchangeMDB/pdidc-exchange1.pdidc.cisco.com [SRServer.cpp:297]
10/23/2012 15:46:55.673(Local)(3780 1.2) NTCE (673811) Queued InitiateKeyRetrieval task [SRServer.cpp:264]10/23/2012 15:46:55.673(Local)(3780 1.2) NTCE (673819)
Key retrieval is in Progress [SRServer.cpp:322]
10/23/2012 15:46:55.673(Local)(3780 0.0) NTCE (673818) Initiating key retrieval [SRServer.cpp:271]
10/23/2012 15:46:55.673(Local)(3780 1.2) NTCE (673827) initiating key retrieval in progress [SRDataServer.cpp:441]
10/23/2012 15:46:55.673(Local)(3780 1.2) NTCE (673834) Sending ack for result 2, item name /cfg/gl/sr/sr_get_key/pdidc-exchange1.pdidc.cisco.com@pdidc.cisco.com [SRDataServer.cpp:444]
10/23/2012 15:46:55.673(Local)(3780 0.0) NTCE (673922) Match found for DN: pdidc.cisco.com is ID:MacchineAcctWAAS [SRDiIdMgr.cpp:163]
10/23/2012 15:46:55.673(Local)(3780 0.0) NTCE (673937) Identity MacchineAcctWAAS found in the Map [SRDiIdMgr.cpp:702]
10/23/2012 15:46:55.673(Local)(3780 0.0) NTCE (673950) DN Info found for domain pdidc.cisco.com [SRIdentityObject.cpp:168]
10/23/2012 15:46:55.674(Local)(3780 0.0) NTCE (674011) DRS_SPN: E3514235-4B06-11D1-AB04-00C04FC2DCD2/e4c83c51-0b59-4647-b45d-780dd2dc3344/PDIDC.CISCO.COM for PDI-7541-DC@PDIDC.CISCO.COM [GssCli.cpp:51]
10/23/2012 15:46:55.674(Local)(3780 0.0) NTCE (674020) CREATED srkr obj(0x50aa00) for spn (exchangeMDB/pdidc-exchange1.pdidc.cisco.com) [SRKeyMgr.cpp:134]
10/23/2012 15:46:55.674(Local)(3780 1.3) NTCE (674421) Import cred successfull for pn: PDI-7541-DC@PDIDC.CISCO.COM [GssCli.cpp:135]
10/23/2012 15:46:55.676(Local)(3780 1.3) NTCE (676280) session(0x50aa00) Complete TGT stage of GSS Successful, Initiating AppApi [SRKeyRetriever.cpp:408]
10/23/2012 15:46:55.676(Local)(3780 0.1) NTCE (676415) SRKR: Success in posting connect to service <ip:0e:6e:03:a3><port:135> [IoOperation.cpp:222]
10/23/2012 15:46:55.676(Local)(3780 0.0) NTCE (676607) Connected to server. [IoOperation.cpp:389]
10/23/2012 15:46:55.677(Local)(3780 0.0) NTCE (677736) SRKR: Success in posting connect to service <ip:0e:6e:03:a3><port:1025> [IoOperation.cpp:222]
10/23/2012 15:46:55.678(Local)(3780 0.1) NTCE (678001) Connected to server. [IoOperation.cpp:389]
10/23/2012 15:46:55.679(Local)(3780 0.1) NTCE (679500) Cleaning up credential cache for PDI-7541-DC@PDIDC.CISCO.COM [GssCli.cpp:212]
10/23/2012 15:46:55.680(Local)(3780 0.1) NTCE (680011) Parsing DRSEBIND Response [AppApiDrsBind.cpp:222]
10/23/2012 15:46:55.680(Local)(3780 0.1) NTCE (680030) DRSEBind 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]
```

Esta saída é do arquivo mapiao-errorlog no Edge WAE para uma conexão eMAPI bem-sucedida

```
'''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]
```

Aqui está a saída correspondente do Core WAE de mapiao-errorlog para a mesma conexão TCP

```
'''10/23/2012 17:56:54.092(Local)(6408 0.0) NTCE (92814) (fl=21) Core TCP connection initiated  
(11892640), Conn: [14.110.3.117:58352 <=> 14.110.3.99:27744], F  
lavor: 0 [CoreTcpConnectionDceRpcLayer.cpp:99]  
10/23/2012 17:56:54.092(Local)(6408 0.0) NTCE (92832) Core TCP connection initiated (11892640),  
Conn: [14.110.3.117:58352 <=> 14.110.3.99:27744], Flavor: 0  
[CoreTcpConnectionDceRpcLayer.cpp:104]'''  
10/23/2012 17:56:54.175(Local)(6408 0.0) NTCE (175035) SrplibCache Cache eviction starting:  
static void srplib::CSrplibCache:: OnAoShellDispatchCacheCleanup(vo  
id*, aosh_work*) [SrplibCache.cpp:453]  
10/23/2012 17:56:54.175(Local)(6408 0.0) NTCE (175068) last_cleanup_time (1344411860),  
evict_in_progress(1) handled_req_cnt (1) cache_size (0) [SrplibCache.  
cpp:464]  
10/23/2012 17:56:54.175(Local)(6408 0.0) NTCE (175121) SendNextCmd isDuringSend 0, WriteQueue sz  
1, isDuringclose 0 [SrplibClientTransport.cpp:163]  
10/23/2012 17:56:54.175(Local)(6408 0.0) NTCE (175132) SendNextCmd: Sending request:  
exchangeMDB/PDIDC-EXCHANGE1.pdidc.cisco.com:23[v:=11], WriteQueue sz 0  
[bClose 0] [SrplibClientTransport.cpp:168]  
10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185576) OnReadComplete len 4 status 0  
isDuringRead 1, isDuringHeaderRead 1, isDuringclose 0 [SrplibTransport.  
cpp:127]  
10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185587) Parse header, msg body len 152  
[SrplibTransport.cpp:111]  
10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185592) ReadNextMsg isDuringRead 0,  
isDuringHeaderRead 1, isDuringclose 0 [SrplibTransport.cpp:88]  
10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185623) OnReadComplete len 148 status 0  
isDuringRead 1, isDuringHeaderRead 0, isDuringclose 0 [SrplibTranspor  
t.cpp:127]  
'''10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185688) Insert new KrbKey: exchangeMDB/PDIDC-  
EXCHANGE1.pdidc.cisco.com::23[v:=11]:[{e,f,l}:= {0, 0x1, 16}] [S  
rplibCache.cpp:735]  
'''10/23/2012 17:56:54.185(Local)(6408 0.1) NTCE (185747) ReadNextMsg isDuringRead 0,  
isDuringHeaderRead 0, isDuringclose 0 [SrplibTransport.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  
.comOnxrpblND [GssServer.cpp:468]
```

```
10/23/2012 17:56:54.261(Local)(6408 0.1) NTCE (261613) (fl=21) Successfully added entry in
memory keytab. [GssServer.cpp:92]
10/23/2012 17:56:54.261(Local)(6408 0.1) NTCE (261858) (fl=21) Successfully acquired
credentials. [GssServer.cpp:135]'''
```

Problemas comuns

Abaixo estão alguns motivos comuns que resultam em transferência da conexão eMAPI para o AO genérico (TG).

Problema 1: A identidade do serviço de criptografia configurada no Core WAE não tem as permissões corretas no AD.

Saída do sr-errolog no 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
```

Resolução 1: Consulte o guia de configuração e verifique se o objeto no AD tem as permissões corretas. "Replicando alterações de diretório" e "Replicando alterações de diretório tudo" devem ser definidos para permitir.

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

Problema 2: Há um desvio de tempo entre o Core WAE e o KDC a partir do qual ele tenta obter a chave

Saída do sr-erolog no 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-exchangel.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-exchangel.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]
```

Resolução 2: Use a atualização em todos os WAEs (especialmente o Núcleo) para sincronizar o relógio com o KDC. Em seguida, aponte para o servidor NTP empresarial (preferencialmente o mesmo que o KDC).

Problema 3: O domínio definido para o serviço de Criptografia não corresponde ao domínio em que o servidor Exchange está.

Saída do sr-erolog no 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]
```

Resolução 3: Se o seu Core WAE atender a vários servidores Exchange em domínios diferentes, você deverá configurar uma Identidade de serviço de criptografia para cada domínio em que os servidores Exchange residem.

Observação: NÃO há suporte para o subdomínio incluir no momento. Se você tiver myexchange.subdomain.domain.com , a Identidade do serviço de criptografia deve estar em subdomain.domain.com; ELE NÃO PODE estar no domínio pai.

Problema 4: Se a WANSecure falhar, suas conexões podem cair para TG

As conexões eMAPI podem ser transferidas para o AO genérico porque o plumb seguro da WAN falhou. Falha no plumb seguro da WAN porque a verificação do certificado falhou. A verificação de certificado de peer falhará porque o certificado de peer autoassinado padrão está sendo usado ou o certificado falhou legitimamente na verificação de OCSP.

Configurações principais do WAE

```
crypto pki global-settings

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

!

crypto ssl services host-service peering

    peer-cert-verify
    exit

!
```

WAN Secure:

Accelerator Config Item	Mode	Value
-------------------------	------	-------

-----	----	-----
SSL AO	User	enabled
Secure store	User	enabled
Peer SSL version	User	default
Peer cipher list	User	default
Peer cert	User	default
Peer cert verify	User	enabled

Isso resultará nas seguintes entradas mapiao-errorlog e wsao-errorlog:

A dica aqui é a primeira linha realçada "desconectado mais de quatro vezes consecutivas"

Mapiao-errorlog no WAE do lado do cliente:

```

'''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 no WAE do lado do cliente:

```

'''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]

```

Resolução 4: Remova a configuração do peer cert de ambos os WAEs e reinicie o serviço de criptografia no(s) Core WAE(s).

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

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

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

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

Problema 5: Se o NTLM for usado pelo cliente do Outlook, a conexão será enviada para o AO genérico.

Você verá o seguinte no mapiao-errorlog no WAE do lado do cliente:

```
'''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]
```

Resolução 5: O cliente deve habilitar/exigir a autenticação Kerberos em seu ambiente Exchange. NTLM NÃO é suportado (a partir de 5.1)

Esteja ciente de que há um resumo técnico da Microsoft que chama a atenção para uma queda de NTLM quando um CAS é usado.

O cenário em que Kerberos não funciona é específico para o Exchange 2010 e está no seguinte cenário:

Vários Servidores de Acesso de Cliente Exchange (CAS) em uma organização/domínio. Esses servidores CAS são agrupados usando qualquer método - usando a função de matriz de cliente incorporada da Microsoft ou um balanceador de carga de terceiros.

No cenário acima, o Kerberos não funciona - e os clientes voltarão ao NTLM por padrão. Acredito que isso se deve ao fato de que os clientes devem AUTH para o servidor CAS versus o servidor Mailbox, como fizeram em versões anteriores do Exchange.

No Exchange 2010 RTM, não há solução para isso! O Kerberos no cenário acima nunca funcionará antes do Exchange 2010-SP1.

No SP1, o Kerberos pode ser ativado nesses ambientes, mas é um processo manual. Veja o artigo aqui: <http://technet.microsoft.com/en-us/library/ff808313.aspx>

Registro MAPI AO

- Os seguintes arquivos de log estão disponíveis para solução de problemas de MAPI AO:
- Arquivos de log de transação: /local1/logs/tfo/working.log (e /local1/logs/tfo/tfo_log_*.txt)

Depurar arquivos de log: /local1/errorlog/mapiao-errorlog.current (e mapiao-errorlog.*)

Para facilitar a depuração, você deve primeiro configurar uma ACL para restringir pacotes a um host.

```
WAE674(config)# ip access-list extended 150 permit tcp host 10.10.10.10 any
WAE674(config)# ip access-list extended 150 permit tcp any host 10.10.10.10
```

Para ativar o registro de transações, use o comando de configuração transaction-logs da seguinte maneira:

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

Você pode exibir o final de um arquivo de log de transações usando o comando type-tail da seguinte maneira:

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

Para configurar e ativar o registro de depuração do MAPI AO, use os seguintes comandos.

NOTE: O registro de depuração exige muito da CPU e pode gerar uma grande quantidade de saída. Use-o de forma inteligente e moderna em um ambiente de produção.

Você pode ativar o registro detalhado no disco da seguinte maneira:

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

Você pode ativar o registro de depuração para conexões na ACL da seguinte maneira:

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

As opções para depuração MAPI AO são as seguintes:

```
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
```

Você pode ativar o registro de depuração para conexões MAPI e, em seguida, exibir o final do registro de erros de depuração da seguinte maneira:

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