ESA 一元化ポリシー、ウイルスおよびアウトブレイク隔離（PVO）を有効にできない

目次

概要

このドキュメントでは、Cisco E メール セキュリティ アプライアンス（ESA）で、[Enable] ボタンがグレー表示されるため、一元化されたポリシー、ウイルスおよびアウトブレイク隔離（PVO）が有効化できない問題について説明し、この問題の解決策を示します。

前提条件

要件

次の項目に関する知識が推奨されます。

- セキュリティ管理アプライアンス（SMA）で PVO を有効化する方法。
- 各管理型 ESA に PVO サービスを追加する方法。
- PVO の移行の設定方法。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- SMA バージョン 8.1 以降
- ESA バージョン 8.0 以降

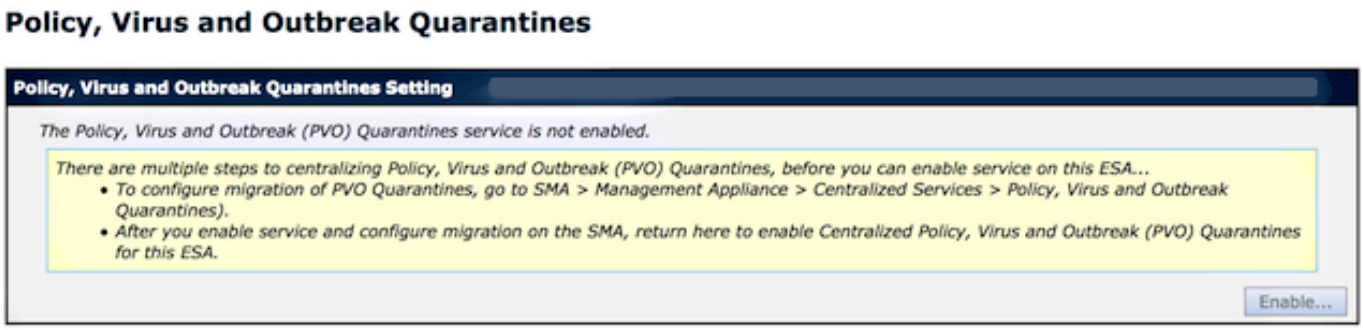
本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。 このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。 稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

背景説明

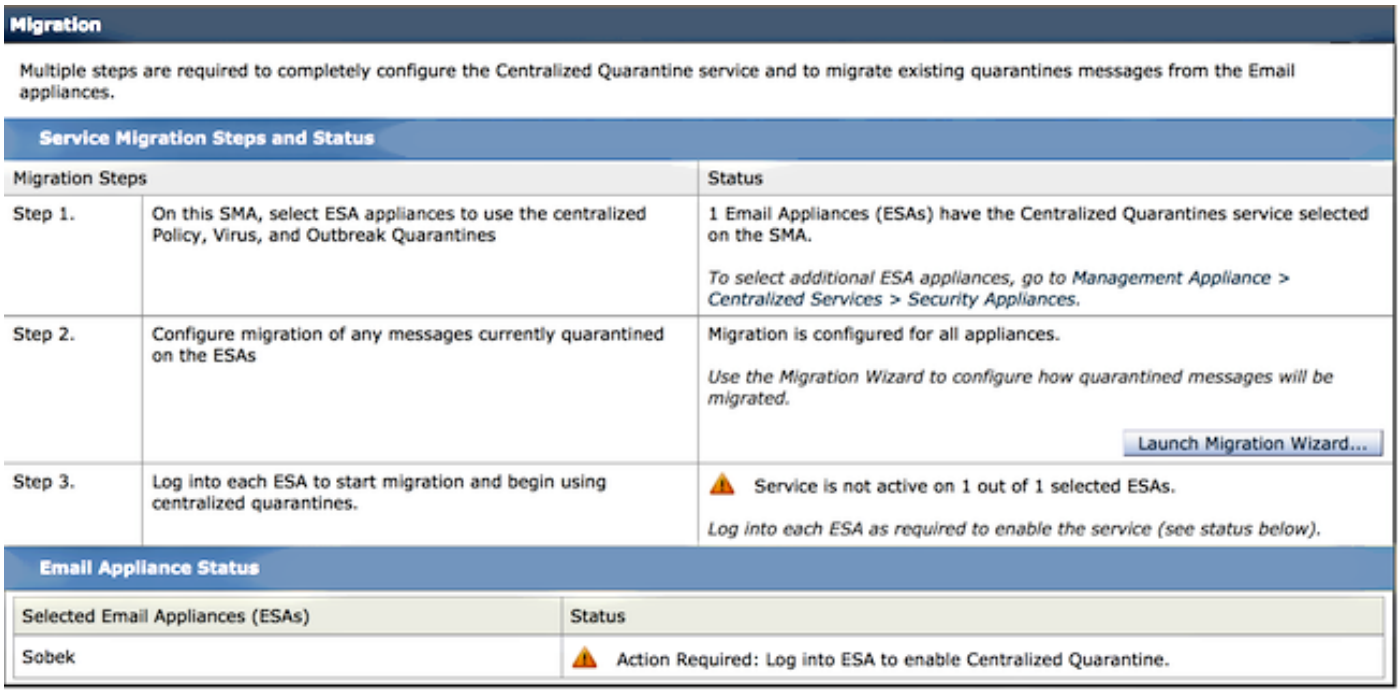
ESA で上の特定のフィルタ、ポリシー、およびスキャン操作により処理されたメッセージは、次の作業に備えて一時的に保管するために隔離内に置くことができます。 SMA で正しく設定し、移行ウィザードを使用したにもかかわらず、ESA で PVO を有効化できない場合があります。 ESA はポート 7025 の SMA に接続できないため、ESA のこの機能を有効にするボタンは、通常でもグレー表示されています。

問題

ESAで [Enable] ボタンがグレー表示されます。



SMA には、サービスがアクティブでなく、アクションが必要だと表示されます



解決策

ここではいくつかのシナリオについて説明します。

シナリオ 1

SMAで、アプライアンスがオンライン状態であることを確認するため、CLI の **status** コマンドを実行します。 SMA がオフラインの場合、接続が失敗するため、ESA で PVO を有効にすることはできません。

```
sma.example.com> status

Enter "status detail" for more information.

Status as of:                  Mon Jul 21 11:57:38 2014 GMT
Up since:                      Mon Jul 21 11:07:04 2014 GMT (50m 34s)
Last counter reset:            Never
System status:                 Offline
Oldest Message:                No Messages
```

SMA がオフラインの場合、これをオンラインに戻し、cpq_listener を起動するため、**resume** コマンドを実行します。

```
sma.example.com> resume

Receiving resumed for euq_listener, cpq_listener.
```

シナリオ2

SMA の移行ウィザードを使用した後、変更を確定することが重要です。 変更を確定しない場合、[Enable...] ボタンはグレー表示のままです。

1. SMA および ESA に **Operator**（またはその他のアカウント タイプ）ではなく、**管理者アカウント**でログインします。そうでない場合、セットアップは実行できますが、ESA 側の [Enable...] ボタンはグレー表示されます。

2. SMA で、[Management Appliance] > [Centralized Services] > [Policy, Virus, and Outbreak Quarantines] を選択します。

3. [Launch Migration Wizard] をクリックし、移行方法を選択します。

4. 変更を送信し、確定します。

シナリオ 3

ESA に **deliveryconfig** コマンドを通じてデフォルトの配信インターフェイスを設定し、それが別のサブネットにあるか、ルートがないため、そのデフォルトのインターフェイスに SMA への接続がない場合、PVO は ESA で有効化できません。

インターフェイス In に設定されているデフォルトの配信インターフェイスがある ESA を次に示します。

```
mx.example.com> deliveryconfig

Default interface to deliver mail: In
```

インターフェイス In から SMA ポート 7025 への ESA の接続テストを次に示します。

```
mx.example.com> telnet

Please select which interface you want to telnet from.
1. Auto
2. In (192.168.1.1/24: mx.example.com)
3. Management (10.172.12.18/24: mgmt.example.com)
[1]> 2

Enter the remote hostname or IP address.
[]> 10.172.12.17

Enter the remote port.
[25]> 7025

Trying 10.172.12.17...
telnet: connect to address 10.172.12.17: Operation timed out
telnet: Unable to connect to remote host
```

この問題を解決するには、デフォルトのインターフェイスに Auto を設定します。これにより、ESA は適切なインターフェイスを自動的に使用します。

```
mx.example.com> deliveryconfig

Default interface to deliver mail: In

Choose the operation you want to perform:
- SETUP - Configure mail delivery.
[]> setup

Choose the default interface to deliver mail.
1. Auto
2. In (192.168.1.1/24: mx.example.com)
3. Management (10.172.12.18/24: mgmt.example.com)
[1]> 1
```

シナリオ 4

一元化された隔離への接続は、デフォルトでは Transport Layer Security（TLS）暗号化されています。 ESA のメール ログ ファイルを確認し、SMA の ポート 7025 への送信接続 ID（DCID）を検索すると、次のような TLS 失敗エラーが表示されることがあります。

```
Mon Apr 7 15:48:42 2014 Info: New SMTP DCID 3385734 interface 172.16.0.179
address 172.16.0.94 port 7025
Mon Apr 7 15:48:42 2014 Info: DCID 3385734 TLS failed: verify error: no certificate
from server
Mon Apr 7 15:48:42 2014 Info: DCID 3385734 TLS was required but could not be
successfully negotiated
```

ESA CLI で tlsverify を実行すると、同じ結果になります。

```
mx.example.com> tlsverify

Enter the TLS domain to verify against:
[]> the.cpq.host

Enter the destination host to connect to.  Append the port (example.com:26) if you are not
connecting on port 25:
[the.cpq.host]> 10.172.12.18:7025

Connecting to 10.172.12.18 on port 7025.
Connected to 10.172.12.18 from interface 10.172.12.17.
Checking TLS connection.
TLS connection established: protocol TLSv1, cipher ADH-CAMELLIA256-SHA.
Verifying peer certificate.
Certificate verification failed: no certificate from server.
TLS connection to 10.172.12.18 failed: verify error.
TLS was required but could not be successfully negotiated.

Failed to connect to [10.172.12.18].
TLS verification completed.
```

これに基づき、SMA とネゴシエートするために使用する ADH-CAMELLIA256-SHA 暗号により、SMA はピア証明書の表示に失敗します。 さらに調査すると、すべての ADH 暗号は匿名認証を使用し、ピア証明書を提供しないことがわかります。 **ここで行う修正は、匿名の暗号を削除することです。** これを行うため、出力暗号リストを HIGH:MEDIUM:ALL:-aNULL:-SSLv2 に変更します。

```
mx.example.com> sslconfig

sslconfig settings:
 GUI HTTPS method:  sslv3tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> OUTBOUND

Enter the outbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]>

Enter the outbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> HIGH:MEDIUM:ALL:-aNULL:-SSLv2

sslconfig settings:
 GUI HTTPS method:  sslv3tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
```

```
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: HIGH:MEDIUM:ALL:-aNULL:-SSLv2

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]>

mx.example.com> commit
```

ヒント：また、**-SSLv2** も追加します。理由はこれらも安全でない暗号であるためです。

シナリオ 5

PVO は有効化できず、次ののような**エラー メッセージが表示されます。**

```
mx.example.com> sslconfig

sslconfig settings:
 GUI HTTPS method:  sslv3tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
- VERIFY - Verify and show ssl cipher list.
[]> OUTBOUND

Enter the outbound SMTP ssl method you want to use.
1. SSL v2.
2. SSL v3
3. TLS v1
4. SSL v2 and v3
5. SSL v3 and TLS v1
6. SSL v2, v3 and TLS v1
[5]>

Enter the outbound SMTP ssl cipher you want to use.
[RC4-SHA:RC4-MD5:ALL]> HIGH:MEDIUM:ALL:-aNULL:-SSLv2

sslconfig settings:
 GUI HTTPS method:  sslv3tlsv1
 GUI HTTPS ciphers: RC4-SHA:RC4-MD5:ALL
 Inbound SMTP method:  sslv3tlsv1
 Inbound SMTP ciphers: RC4-SHA:RC4-MD5:ALL
 Outbound SMTP method:  sslv3tlsv1
 Outbound SMTP ciphers: HIGH:MEDIUM:ALL:-aNULL:-SSLv2

Choose the operation you want to perform:
- GUI - Edit GUI HTTPS ssl settings.
- INBOUND - Edit Inbound SMTP ssl settings.
- OUTBOUND - Edit Outbound SMTP ssl settings.
```

```
- VERIFY - Verify and show ssl cipher list.
[]>

mx.example.com> commit
```

このエラー メッセージは、いずれかのホストに、適用される DLP 機能キーがなく、DLP が無効になったことを示します。 ソリューションは、不足している機能キーを追加し、機能キーが適用されたホストと同じ DLP 設定を適用することです。 この機能キーの不一致が、アウトブレイク フィルタや Sophos ウイルス対策、および他の機能キーと同じ影響を与える可能性があります。

シナリオ 6

クラスタ設定に、コンテンツ、メッセージ フィルタ、DLP、DMARC 設定用のマシンまたはグループ レベルの設定がある場合、PVO の [Enable] ボタンは、グレー表示されます。 この問題を解決するには、すべてのメッセージおよびコンテンツフィルタをマシンレベルまたはグループ レベルからクラスタ レベルに移動し、DLP と DMARC 設定も同様にします。 または、マシン レベルの設定があるマシンをクラスタから完全に削除します。 CLIコマンド **[clusterconfig] > [removemachine]** を入力し、クラスタ設定を継承するため、クラスタに戻します。

関連情報

- SMA における PVO 隔離との配信に関するトラブルシューティング
- ESA がクラスタリングされている場合の PVO 移行ウィザードの要件
- テクニカル サポートとドキュメント – Cisco Systems