

La stratégie de centralisation ESA, le virus, et la quarantaine d'épidémie (PVO) ne peuvent pas être activés

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Informations générales](#)

[Problème](#)

[Solution](#)

[Scénario 1](#)

[Scénario 2](#)

[Scénario 3](#)

[Scénario 4](#)

[Scénario 5](#)

[Scénario 6](#)

[Informations connexes](#)

Introduction

Ce document décrit un problème rencontré où la stratégie, le virus, et la quarantaine de centralisation d'épidémie (PVO) ne peuvent pas être activés sur l'apppliance de sécurité du courrier électronique de Cisco (ESA) parce que le bouton d'enable est grisé et offre une solution au problème.

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Comment activer PVO sur l'apppliance de Gestion de la sécurité (SMA).
- Comment ajouter le service PVO à chaque ESA géré.
- Comment configurer le transfert de PVO.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version 8.1 et ultérieures SMA
- Version 8.0 et ultérieures ESA

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

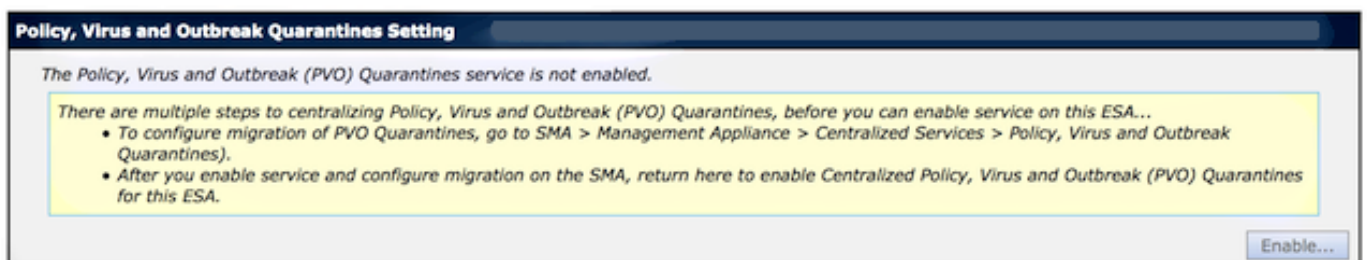
Informations générales

Des messages traités par certains filtres, stratégies, et opérations de balayage sur un ESA peuvent être placés dans des quarantaines pour les tenir temporairement pour davantage d'action. Dans certains cas, il s'avère que le PVO ne peut pas être activé sur l'ESA bien qu'il ait été correctement configuré sur le SMA et l'assistant de transfert a été utilisé. Le bouton pour activer cette caractéristique sur l'ESA habituellement est encore grisé parce que l'ESA ne peut pas se connecter au SMA sur le port 7025.



Problème

Sur l'ESA, le bouton d'enable est grisé.

Policy, Virus and Outbreak Quarantines



Les expositions SMA entretiennent non actif et l'action exigés

Migration		
Multiple steps are required to completely configure the Centralized Quarantine service and to migrate existing quarantines messages from the Email appliances.		
Service Migration Steps and Status		
Migration Steps	Status	
Step 1.	On this SMA, select ESA appliances to use the centralized Policy, Virus, and Outbreak Quarantines	1 Email Appliances (ESAs) have the Centralized Quarantines service selected on the SMA. <i>To select additional ESA appliances, go to Management Appliance > Centralized Services > Security Appliances.</i>
Step 2.	Configure migration of any messages currently quarantined on the ESAs	Migration is configured for all appliances. <i>Use the Migration Wizard to configure how quarantined messages will be migrated.</i> Launch Migration Wizard...
Step 3.	Log into each ESA to start migration and begin using centralized quarantines.	 Service is not active on 1 out of 1 selected ESAs. <i>Log into each ESA as required to enable the service (see status below).</i>
Email Appliance Status		
Selected Email Appliances (ESAs)	Status	
Sobek	 Action Required: Log into ESA to enable Centralized Quarantine.	

Solution

Il y a plusieurs scénarios, qui sont décrits ici.

Scénario 1

Sur le SMA, exécutez la commande d'**état** sur le CLI afin de s'assurer que l'appliance est dans un état en ligne. Si le SMA est hors ligne, le PVO ne peut pas être activé sur l'ESA parce que la connexion échoue.

```
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
```

Si le SMA est hors ligne, exécutez la commande de **reprise** afin de la rapporter en ligne, qui commence le cpq_listener.

```
sma.example.com> resume
```

Receiving resumed for euq_listener, cpq_listener.

Scénario 2

Après que vous utilisiez l'assistant de transfert sur le SMA, il est important de commettre les modifications. [Enable...] bouton sur les restes ESA grisés si vous ne commettez pas des modifications.

1. Le log dans le SMA et l'ESA avec le **compte administrateur**, pas l'**opérateur** (ou d'autres types de compte) ou l'installation peuvent être exécutés mais [l'enable...] le bouton sera grisé du côté ESA.
2. Sur le SMA, choisissez l'**appliance de Gestion > des services > stratégie, virus, et des quarantaines centralisés d'épidémie**.
3. Cliquez sur l'**assistant de transfert de lancement** et choisissez une méthode de transfert.
4. **Soumettez et commettez** vos modifications.

Scénario 3

Si l'ESA a été configuré avec une interface par défaut de la livraison par l'intermédiaire de la commande de **deliveryconfig** et si cette interface par défaut n'a aucune Connectivité vers le SMA parce qu'elle réside dans un différent sous-réseau ou là n'est aucune artère, le PVO ne peut pas être activé sur l'ESA.

Voici un ESA avec l'interface par défaut de la livraison configurée pour relier **dans** :

```
mx.example.com> deliveryconfig
```

```
Default interface to deliver mail: In
```

Voici un test de Connectivité ESA d'interface **dedans** au port 7025 SMA :

```
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
```

Afin de résoudre ce problème, configurez l'interface par défaut à l'**automatique** où l'ESA utilise l'interface appropriée automatiquement.

```
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**

## Scénario 4

Les connexions à la quarantaine centralisée sont Transport Layer Security (TLS) - chiffré par défaut. Si vous examinez le fichier journal de messagerie sur l'ESA et recherchez des id de connexion de la livraison (DCIDs) au port 7025 sur le SMA, vous pourriez voir que le TLS a manqué des erreurs de ce type :

```
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
```

Quand vous exécutez un `tlsverify` sur l'ESA CLI, vous voyez la même chose.

```
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.
```

Basé sur ceci, le chiffrement **ADH-CAMELLIA256-SHA** utilisé afin d'être en pourparlers avec le SMA fait le SMA pour présenter un certificat de pair. Les recherches plus approfondies indiquent que tous les chiffrements CAD utilisent l'authentification anonyme, qui ne fournit pas un certificat de pair. **La difficulté ici est d'éliminer des chiffrements anonymes.** Afin de faire ceci, changez la liste sortante de chiffrement à **HIGH:MEDIUM:ALL:-aNULL:-SSLv2.**

```
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
```

**Conseil :** Ajoutez également **-SSLv2** parce que ce sont des chiffrements non sécurisés aussi bien.

## Scénario 5

Le PVO ne peut pas être activé et affiche ce type de message d'erreur.

```
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**

Le message d'erreur peut indiquer qu'un des hôtes n'a pas une touche de fonction DLP appliquée et le DLP est désactivé. La solution est d'ajouter la clé de fonctionnalité manquante et d'appliquer des configurations DLP identiques comme sur l'hôte qui a la touche de fonction appliquée. Cette incohérence de touche de fonction pourrait avoir le même effet avec les filtres d'épidémie, l'antivirus de Sophos, et d'autres touches de fonction.

## Scénario 6

Le bouton d'enable pour le PVO sera grisé si, en configuration du cluster il y a configuration d'ordinateur ou de niveau du groupe pour le contenu, message filtre, configuration DLP, et DMARC. Afin de résoudre ce problème, tous les filtres de message et de contenu doivent être déplacés de la machine ou du niveau du groupe aux configurations batterie batterie aussi bien que DLP et DMARC. Alternativement, vous pouvez entièrement retirer l'ordinateur qui a la configuration de niveau d'ordinateur de la batterie. Entrez dans le **clusterconfig > le removemachine** de commande CLI et puis joignez-le de nouveau à la batterie afin d'hériter de la configuration du cluster.

## Informations connexes

- [Dépannez la livraison et derrière la quarantaine PVO sur SMA](#)
- [Conditions requises pour l'assistant de transfert PVO quand l'ESA est groupé](#)
- [Support et documentation techniques - Cisco Systems](#)