

ESA Centralizing Policy, Virus en Outbreak Quarantine (PVO) kunnen niet worden ingeschakeld

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Achtergrondinformatie](#)

[Probleem](#)

[Oplossing](#)

[Scenario 1](#)

[Scenario 2](#)

[Scenario 3](#)

[Scenario 4](#)

[Scenario 5](#)

[Scenario 6](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft een probleem dat is ondervonden wanneer PVO (Centralizing Policy, Virus en Outbreak Quarantine) niet in staat zijn op Cisco Email Security Appliance (ESA) omdat de knop Enable er uit is gezet en een oplossing voor het probleem biedt.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Hoe kan PVO op de Security Management-applicatie (SMA) worden ingeschakeld.
- Hoe kan de PVO-dienst aan elk beheerd ESA worden toegevoegd?
- Hoe moet u de migratie van PVO configureren.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- SMA versie 8.1 en hoger
- ESR versie 8.0 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

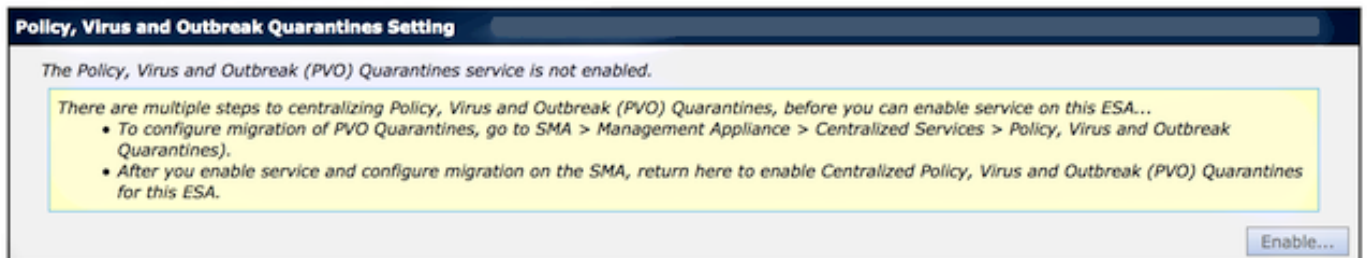
Achtergrondinformatie

Berichten die zijn verwerkt door bepaalde filters, beleid en scanbewerkingen op een ESA kunnen in quarantaine worden geplaatst om ze tijdelijk vast te houden voor verdere actie. In sommige gevallen blijkt dat het VVB niet kan worden ingeschakeld op het ESR, hoewel het op de juiste wijze is ingesteld op het SMA en de migratiewizard is gebruikt. De knop om deze functie in te schakelen op de ESA wordt gewoonlijk nog grijs weergegeven omdat de ESA geen verbinding kan maken met de SMA in Port 7025.



Probleem

In het ESR wordt de knop Inschakelen ingedrukt.

Policy, Virus and Outbreak Quarantines



SMA toont service niet actief en vereist actie

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.	

Oplossing

Er zijn verschillende scenario's, die hier worden beschreven.

Scenario 1

Start in het SMA de **status**-opdracht van de CLI om er zeker van te zijn dat het apparaat in een online toestand verkeert. Indien de SMA offline is, kan het VVB niet op de ESA worden ingeschakeld omdat de verbinding mislukt.

```
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
```

Als de SMA offline is, voer de **hervatte** opdracht uit om het online terug te brengen, wat de cpq_lister start.

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

```
Receiving resumed for euq_listener, cpq_listener.
```

Scenario 2

Nadat u de Migratiewizard op de SMA hebt gebruikt, is het belangrijk om de wijzigingen door te voeren. De knop [Inschakelen...] op het ESA blijft grijs als u geen wijzigingen doorvoert.

1. Meld u aan bij het SMA en het ESA met de **Administrator**-account, niet bij de **operator** (of andere rekeningtypen) of de instelling, maar de knop [Enable..] wordt aan de ESR-kant gegraveerd.
2. Kies in het SMA Management-applicatie > **Gecentraliseerde services > Policy, Virus en Outbreak Quarantines**.
3. Klik op **Start Migration Wizard** en kies een migratiemethode.
4. **Indienen en je wijzigingen engageren**.

Scenario 3

Indien het ESA is ingesteld met een standaardovermakingsinterface via het commando "**Deliyfig**" en indien die standaardinstelling geen verbinding heeft met het SMA omdat het zich in een ander net bevindt of er geen route is, kan het PVO niet worden ingeschakeld op het ESA.

Hier is een ESA met een standaardoverloopinterface geconfigureerd voor interface **In**:

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

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

Hier is een ESA connectiviteitstest van interface **In** tot SMA Port 7025:

```
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
```

Om dit probleem op te lossen, moet u de standaardinstelling op **Auto** configureren waar de ESA automatisch de juiste interface gebruikt.

```
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
```

Scenario 4

De verbindingen met de gecentraliseerde quarantaine zijn Transport Layer Security (TLS)-versleuteld standaard. Als u het postlogbestand op het ESA bekijkt en op zoek bent naar Delivery Connection-id's (DCID's) naar Port 7025 op het SMA, dan ziet u mogelijk TLS-fouten zoals deze:

```
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
```

Wanneer u een **verificatie** uitvoert op de ESA CLI, ziet u hetzelfde.

```
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.
```

Op basis hiervan zorgt het **ADH-CAMELLIA256-SHA**-algoritme dat wordt gebruikt om met de SMA te onderhandelen ervoor dat de SMA geen peer-certificaat overlegt. Uit verder onderzoek blijkt dat alle ADH-ciphers anonieme authenticatie gebruiken, hetgeen geen peer certificate oplevert. **De oplossing is om anonieme ciphers te elimineren.** Om dit te doen, verander de vertrekkende algoritme lijst in **HOOG: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
```

Tip: Voeg ook **SSLv2** toe omdat dit ook onveilige ciphers zijn.

Scenario 5

Het PVO kan niet worden ingeschakeld en laat dit soort foutmelding zien.

```
Unable to proceed with Centralized Policy, Virus and Outbreak Quarantines
configuration as host1 and host2 in Cluster have content filters / DLP actions
available at a level different from the cluster Level.
```

De foutmelding kan aangeven dat een van de hosts geen DLP-functiesleutel heeft toegepast en DLP is uitgeschakeld. De oplossing is om de ontbrekende functiesleutel toe te voegen en DLP-instellingen identiek toe te passen zoals op de host waarop de functiesleutel van toepassing is. Deze optie-key inconsistenties kunnen hetzelfde effect hebben als bij Outbreak Filters, Sofos Antivirus en andere functietoetsen.

Scenario 6

De selectieknop voor het PVO wordt weergegeven als er in een clusterconfiguratie sprake is van een machine- of groepsconfiguratie voor inhoud, berichtfilters, DLP- en DMARC-instellingen. Om

dit probleem op te lossen, moeten alle bericht- en contentfilters van machine- of groepsniveau naar clusterniveau worden verplaatst, evenals DLP- en DMARC-instellingen. U kunt ook de machine met de configuratie van het machineniveau volledig uit het cluster verwijderen. Voer de CLI opdracht **clusterconfiguratie > removemachine in** en sluit zich vervolgens aan bij het cluster om de clusterconfiguratie te erven.

Gerelateerde informatie

- [Probleemoplossing bij levering vanaf en naar PVO quarantaine op SMA](#)
- [Vereisten voor de PVO-migratiewizard wanneer ESA zich heeft gevestigd](#)
- [Technische ondersteuning en documentatie – Cisco Systems](#)