

Non è possibile abilitare la policy di centralizzazione ESA, la quarantena per virus ed epidemie (PVO)

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Premesse](#)

[Problema](#)

[Soluzione](#)

[Scenario 1](#)

[Scenario 2](#)

[Scenario 3](#)

[Scenario 4](#)

[Scenario 5](#)

[Scenario 6](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive un problema riscontrato dove non è possibile abilitare la quarantena della centralizzazione di policy, virus ed epidemie (PVO) su Cisco Email Security Appliance (ESA) perché il pulsante Enable è disattivato e offre una soluzione al problema.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Come abilitare PVO su Security Management Appliance (SMA).
- Come aggiungere il servizio PVO a ciascuna ESA gestita.
- Come configurare la migrazione di PVO.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- SMA versione 8.1 e successive
- ESA versione 8.0 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

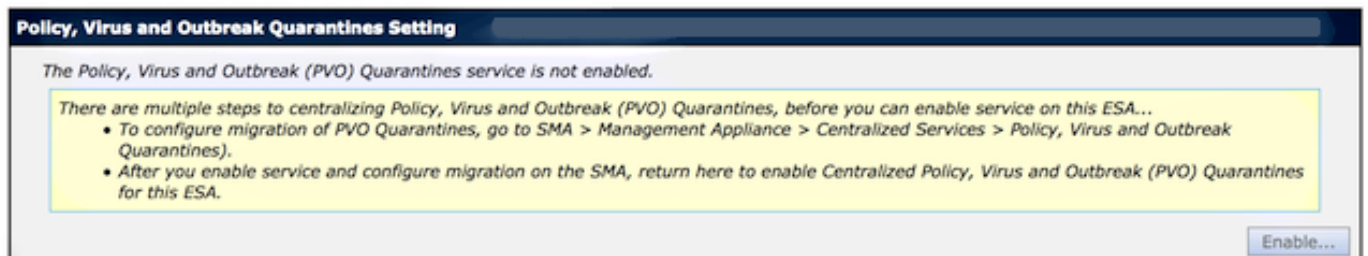
Premesse

I messaggi elaborati da determinati filtri, policy e operazioni di scansione su un ESA possono essere messi in quarantena per conservarli temporaneamente per ulteriori azioni. In alcuni casi, risulta che il PVO non può essere abilitato sull'ESA anche se è stato configurato correttamente sull'SMA ed è stata utilizzata la Migrazione guidata. Il pulsante che abilita questa funzione sull'ESA è in genere ancora disattivato perché l'ESA non è in grado di connettersi all'SMA sulla porta 7025.



Problema

Sull'ESA, il pulsante Enable è disattivato.

Policy, Virus and Outbreak Quarantines



L'SMA mostra il servizio non attivo e l'azione richiesta

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.	

Soluzione

Ci sono diversi scenari, che sono descritti qui.

Scenario 1

SMA, eseguire il comando **status** sulla CLI per verificare che l'accessorio sia in stato online. Se l'SMA non è in linea, non è possibile abilitare il PVO sull'ESA perché la connessione non riesce.

```
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
```

Se l'SMA è offline, eseguire il comando **resume** per riportarlo online, avviando così cpq_listener.

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

Receiving resumed for euq_listener, cpq_listener.

Scenario 2

Dopo aver utilizzato la Migrazione guidata nell'SMA, è importante eseguire il commit delle modifiche. Il pulsante [Enable...] sull'ESA rimane disattivato se non si esegue il commit delle modifiche.

1. Accedere a SMA e ESA con il conto **Amministratore**, non **Operatore** (o altri tipi di conto) o è possibile eseguire la configurazione, ma il pulsante [Abilita...] è disattivato sul lato ESA.
2. Nell'SMA, scegliere **Management Appliance > Centralized Services > Policy, Virus, and Outbreak Quarantines**.
3. Fare clic su **Avvia Migrazione guidata** e scegliere un metodo di migrazione.
4. **Inviare e confermare** le modifiche.

Scenario 3

Se l'ESA è stata configurata con un'interfaccia di consegna predefinita con il comando **deliveryconfig** e l'interfaccia predefinita non ha connettività con l'SMA perché risiede in una subnet diversa o non esiste alcuna route, non sarà possibile abilitare l'ESA.

Ecco un ESA con interfaccia di consegna predefinita configurata per l'interfaccia **In**:

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

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

Ecco un test di connettività ESA dall'interfaccia **In** alla porta SMA 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
```

Per risolvere questo problema, configurare l'interfaccia predefinita su **Auto** quando l'ESA usa automaticamente l'interfaccia corretta.

```
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

Per impostazione predefinita, le connessioni alla quarantena centralizzata sono crittografate tramite TLS (Transport Layer Security). Se si controlla il file di log di posta sull'ESA e si cercano gli ID delle connessioni di recapito (DCID) alla porta 7025 sullo SMA, potrebbero essere visualizzati errori TLS non riusciti, come i seguenti:

```
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
```

Quando si esegue un comando `tlsverify` sulla CLI dell'ESA, viene visualizzato lo stesso.

```
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.
```

Su questa base, la cifratura **ADH-CAMELLIA256-SHA** utilizzata per negoziare con l'SMA impedisce alla SMA di presentare un certificato peer. Ulteriori indagini rivelano che tutte le cifrature ADH utilizzano l'autenticazione anonima, che non fornisce un certificato peer. **Il rimedio è eliminare le cifrature anonime.** A tale scopo, modificare l'elenco di cifratura in uscita in **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
```

Suggerimento: Inoltre, add **-SSLv2** è dovuto al fatto che si tratta di cifrature non sicure.

Scenario 5

Impossibile abilitare l'UCP. Tipo di messaggio di errore visualizzato.

```
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.
```

Il messaggio di errore può indicare che a uno degli host non è stata applicata una chiave di funzione DLP e che questa è stata disabilitata. La soluzione è aggiungere la chiave di funzionalità mancante e applicare le impostazioni DLP nello stesso modo in cui si trovano sull'host a cui è applicata la chiave di funzionalità. Questa incoerenza tra le chiavi potrebbe avere lo stesso effetto con i filtri epidemie, l'antivirus Sophos e altri tasti funzione.

Scenario 6

Il pulsante di abilitazione per il POV è disattivato se in una configurazione cluster è presente una configurazione a livello di computer o di gruppo per il contenuto, i filtri messaggi, le impostazioni

DLP e DMARC. Per risolvere questo problema, tutti i filtri messaggi e contenuti devono essere spostati da livello di computer o di gruppo a livello di cluster, nonché dalle impostazioni DLP e DMARC. In alternativa, è possibile rimuovere completamente dal cluster il computer con configurazione a livello di computer. Immettere il comando CLI **clusterconfig > removemachine** e quindi unirlo nuovamente al cluster per ereditare la configurazione del cluster.

Informazioni correlate

- [Risoluzione dei problemi relativi alla consegna da e verso la quarantena PVO in SMA](#)
- [Requisiti per la Migrazione guidata di UCS quando l'ESA è raggruppata](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)