

ESA Zentralisierung von Policy, Virus und Outbreak Quarantine (PVO) kann nicht aktiviert werden

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Problem](#)

[Lösung](#)

[Szenario 1](#)

[Szenario 2](#)

[Szenario 3](#)

[Szenario 4](#)

[Szenario 5](#)

[Szenario 6](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird ein Problem beschrieben, bei dem die Zentralisierung von Richtlinien, Viren und Outbreak Quarantine (PVO) auf der Cisco E-Mail Security Appliance (ESA) nicht aktiviert werden kann, da die Schaltfläche Aktivieren ausgegraut ist und eine Lösung für das Problem bietet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- So aktivieren Sie PVO auf der Security Management Appliance (SMA).
- Hinzufügen des PVO-Service zu jeder verwalteten ESA.
- Konfiguration der PVO-Migration

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- SMA Version 8.1 und höher
- ESA Version 8.0 oder höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

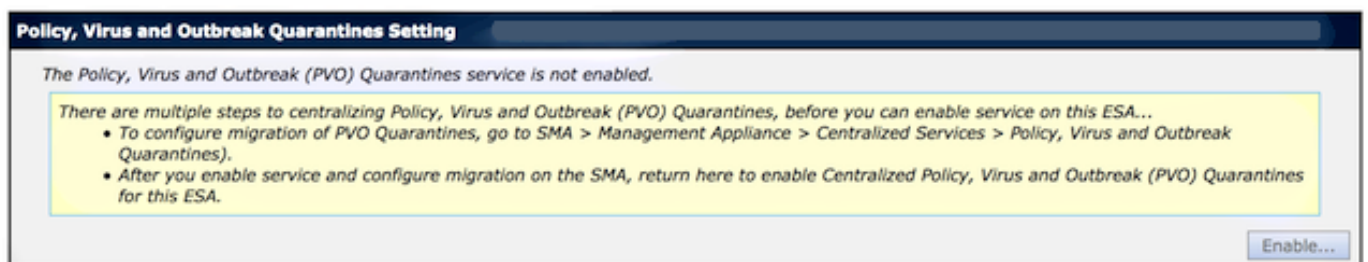
Hintergrundinformationen

Nachrichten, die von bestimmten Filtern, Richtlinien und Scanvorgängen auf einer ESA verarbeitet werden, können unter Quarantäne gestellt werden, um sie vorübergehend für weitere Aktionen aufzubewahren. In einigen Fällen scheint das PVO auf der ESA nicht aktiviert zu sein, obwohl es auf der SMA richtig konfiguriert wurde und der Migrations-Assistent verwendet wurde. Die Taste zum Aktivieren dieser Funktion auf der ESA ist in der Regel noch grau ausgegraut, da die ESA keine Verbindung mit der SMA auf Port 7025 herstellen kann.

Problem

Auf der ESA ist die Schaltfläche "Aktivieren" abgeblendet.

Policy, Virus and Outbreak Quarantines




SMA zeigt an, dass der Service nicht aktiv ist und dass eine Aktion erforderlich ist


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.

Lösung

Es gibt mehrere Szenarien, die hier beschrieben werden.

Szenario 1

Führen Sie auf der SMA den **Status**-Befehl in der CLI aus, um sicherzustellen, dass die Appliance online ist. Wenn das SMA offline ist, kann das PVO auf der ESA nicht aktiviert werden, da die Verbindung fehlschlägt.

```
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
```

Wenn die SMA offline ist, führen Sie den Befehl **Resume (Fortsetzen)** aus, um sie wieder online zu stellen, wodurch der cpq_listener gestartet wird.

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

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

Szenario 2

Nachdem Sie den Migrationsassistenten für SMA verwendet haben, ist es wichtig, die Änderungen zu bestätigen. Die Schaltfläche [Aktivieren..] auf der ESA bleibt grau, wenn Sie keine Änderungen bestätigen.

1. Melden Sie sich beim SMA und der ESA mit dem **Administrator**-Konto an, nicht mit dem **Operator** (oder anderen Kontotypen) oder der Einrichtung, aber die Schaltfläche [Aktivieren..] wird auf der ESA-Seite abgeblendet.
2. Wählen Sie im SMA **Management Appliance > Centralized Services > Policy, Virus, and Outbreak Quarantines (Verwaltungs-Appliance > Zentrale Dienste > Richtlinien, Virus und Outbreak-Quarantäne)**.
3. Klicken Sie auf **Migrationsassistent starten** und wählen Sie eine Migrationsmethode aus.
4. **Senden und bestätigen Sie Ihre Änderungen.**

Szenario 3

Wenn die ESA mit dem Befehl **Delivery** mit einer Standardzustellungsschnittstelle konfiguriert wurde und diese Standardschnittstelle keine Verbindung zur SMA hat, weil sie sich in einem anderen Subnetz befindet oder keine Route existiert, kann das PVO auf der ESA nicht aktiviert werden.

Es folgt eine ESA mit einer Standardzustellungsschnittstelle, die für die Schnittstelle **In** konfiguriert ist:

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

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

Es folgt ein ESA-Verbindungstest von Interface **In** zum 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
```

Um dieses Problem zu beheben, konfigurieren Sie die Standardschnittstelle auf **Auto (Automatisch)**, wobei die ESA die richtige Schnittstelle automatisch verwendet.

```
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**

Szenario 4

Verbindungen zur zentralen Quarantäne sind standardmäßig TLS-verschlüsselt. Wenn Sie die E-Mail-Protokolldatei auf der ESA überprüfen und nach Delivery Connection IDs (DCIDs) für Port 7025 auf der SMA suchen, können folgende Fehler auftreten:

```
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
```

Wenn Sie eine **tlsverify** auf der ESA-CLI ausführen, sehen Sie das Gleiche.

```
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.

Auf dieser Grundlage veranlasst die **ADH-CAMELLIA256-SHA**-Verschlüsselung, die zur Aushandlung mit der SMA verwendet wird, die SMA dazu, kein Peer-Zertifikat vorzulegen. Weitere Untersuchungen zeigen, dass alle ADH-Verschlüsselungen anonyme Authentifizierung verwenden, die kein Peer-Zertifikat bereitstellt. **Das Problem besteht hier darin, anonyme Chiffren zu beseitigen.** Dazu ändern Sie die Liste der ausgehenden Verschlüsselungen 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**

Tipp: Add-SSLv2, da es sich ebenfalls um unsichere Verschlüsselungen handelt.

Szenario 5

Das PVO kann nicht aktiviert werden, und es wird eine solche Fehlermeldung angezeigt.

```
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.
```

Die Fehlermeldung kann angeben, dass auf einem der Hosts kein SvD-Feature-Schlüssel angewendet wurde und SvD deaktiviert ist. Die Lösung besteht darin, den fehlenden Feature-Schlüssel hinzuzufügen und SvD-Einstellungen anzuwenden, die identisch sind mit den Einstellungen auf dem Host, auf dem der Feature-Schlüssel angewendet wurde. Diese Feature-Schlüsselinkonsistenz kann bei Outbreak-Filtern, Sophos Antivirus und anderen Feature-Schlüsseln die gleiche Wirkung haben.

Szenario 6

Die Aktivierungstaste für das PVO wird deaktiviert, wenn in einer Clusterkonfiguration eine Konfiguration auf Computer- oder Gruppenebene für Inhalte, Nachrichtenfilter, DLP- und DMARC-Einstellungen vorhanden ist. Um dieses Problem zu beheben, müssen alle Filter für Nachrichten und Inhalte von der Computer- oder Gruppenebene auf die Cluster-Ebene sowie SvD- und DMARC-Einstellungen verschoben werden. Alternativ können Sie den Computer mit Konfiguration auf Computerebene vollständig aus dem Cluster entfernen. Geben Sie den CLI-Befehl `clusterconfig > removemachine ein`, und schließen Sie ihn dann wieder an den Cluster an, um die Clusterkonfiguration zu übernehmen.

Zugehörige Informationen

- [Fehlerbehebung bei der Bereitstellung von und zu PVO-Quarantäne auf SMA](#)
- [Anforderungen für den PVO Migration Wizard \(PVO-Migrationsassistent\) bei Clustering der ESA](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)