無法啟用ESA集中策略、病毒和爆發隔離(PVO)

目錄

簡介

本文描述在思科郵件安全裝置(ESA)上無法啟用集中策略、病毒和病毒爆發隔離區(PVO)時遇到的問題，因為「啟用」按鈕呈灰色顯示，並且提供了問題的解決方案。

必要條件

需求

思科建議您瞭解以下主題：

- 如何在安全管理裝置(SMA)上啟用PVO。
- 如何將PVO服務新增到每個託管ESA。
- 如何配置PVO的遷移。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- SMA版本8.1及更高版本
- ESA 8.0版及更新版本

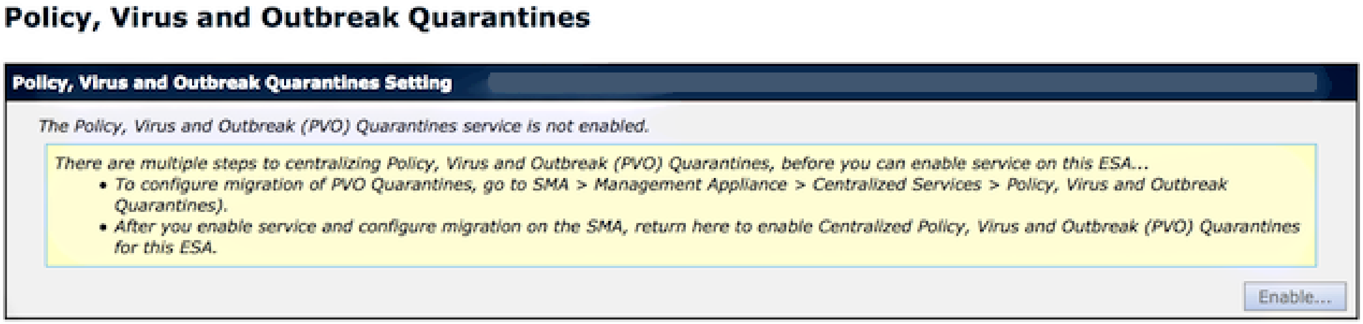
本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

背景資訊

ESA上某些過濾器、策略和掃描操作處理的郵件可以置於隔離區中，臨時保留這些郵件以採取進一步操作。在某些情況下，雖然已在SMA上正確配置了PVO並且使用了「遷移嚮導」，但似乎無法在ESA上啟用PVO。在ESA上啟用此功能的按鈕通常仍然呈灰色顯示，因為ESA無法連線到埠7025上的SMA。

問題

在ESA上，「啟用」按鈕呈灰色顯示。



Policy, Virus and Outbreak Quarantines

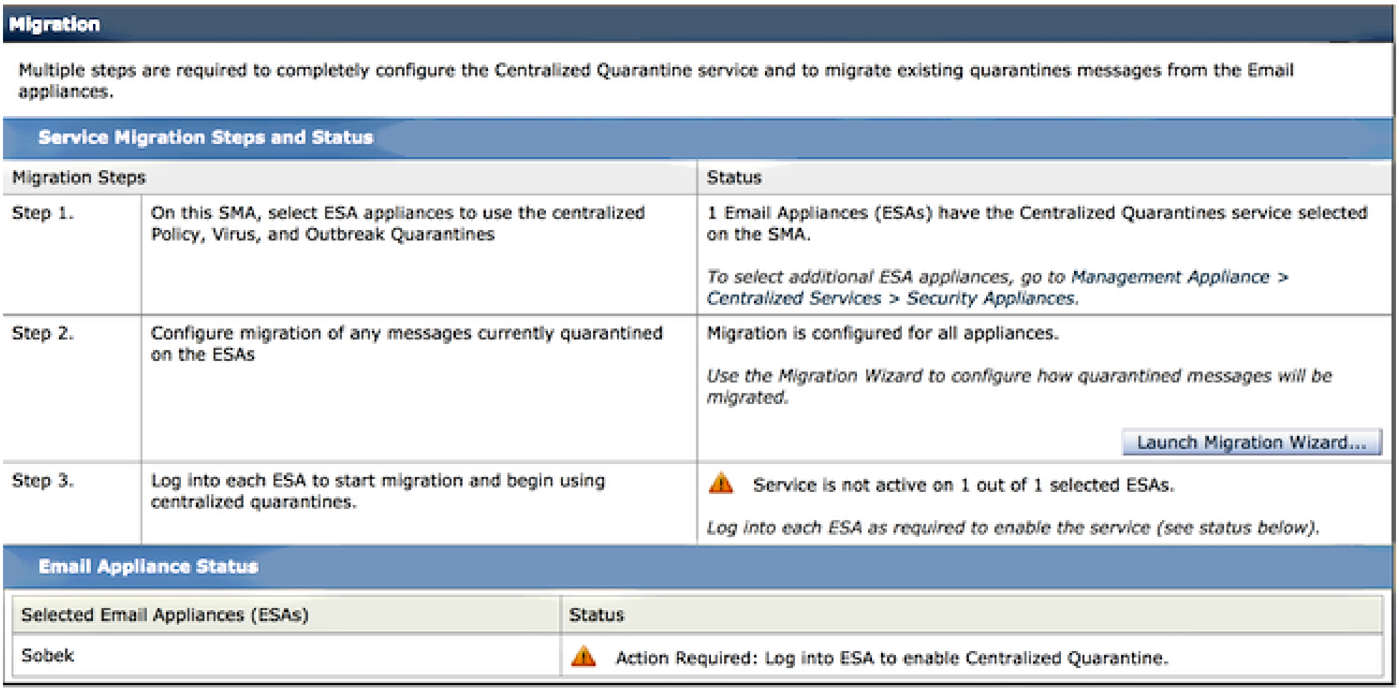
Policy, Virus and Outbreak Quarantines Setting

The Policy, Virus and Outbreak (PVO) Quarantines service is not enabled.

There are multiple steps to centralizing Policy, Virus and Outbreak (PVO) Quarantines, before you can enable service on this ESA...

- *To configure migration of PVO Quarantines, go to SMA > Management Appliance > Centralized Services > Policy, Virus and Outbreak Quarantines).*
- *After you enable service and configure migration on the SMA, return here to enable Centralized Policy, Virus and Outbreak (PVO) Quarantines for this ESA.*

SMA顯示服務非活動且需要操作



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. *To select additional ESA appliances, go to Management Appliance > Centralized Services > Security Appliances.*
Step 2.	Configure migration of any messages currently quarantined on the ESAs	Migration is configured for all appliances. *Use the Migration Wizard to configure how quarantined messages will be migrated.* 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. *Log into each ESA as required to enable the service (see status below).*

Email Appliance Status

Selected Email Appliances (ESAs)	Status
Sobek	⚠ Action Required: Log into ESA to enable Centralized Quarantine.

解決方案

有幾種方案，如下所述。

案例 1

在SMA上，在CLI上運行**status**命令以確保裝置處於聯機狀態。如果SMA處於離線狀態，則無法在ESA上啟用PVO，因為連線失敗。

```
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
```

如果SMA處於離線狀態，請運行**resume**命令使其重新聯機，這將啟動cpq_listener。

```
sma.example.com> resume

Receiving resumed for euq_listener, cpq_listener.
```

案例 2

在SMA上使用遷移嚮導後，必須提交更改。如果不提交更改，ESA上的[Enable...]按鈕將保持灰色。

1. 使用**Administrator**帳戶登入SMA和ESA，不能使用**Operator**（或其他帳戶型別）或可以執行設定，但ESA端的[Enable..]按鈕將呈灰色顯示。

2. 在SMA上，選擇**Management Appliance > Centralized Services > Policy， Virus， and Outbreak Quarantines**。

3. 按一下**啟動遷移嚮導**，然後選擇遷移方法。

4. **提交並提交**更改。

案例 3

如果已經通過**deliveryconfig**命令為ESA配置了預設傳送介面，並且如果該預設介面由於駐留在不同的子網或無路由而與SMA沒有連線，則無法在ESA上啟用PVO。

以下是已配置預設傳送介面以介面**In**的ESA:

```
mx.example.com> deliveryconfig

Default interface to deliver mail: In
```

以下是介面**In**到SMA連線埠7025的ESA連線測試：

```
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
```

為了解決此問題，請將預設介面配置為**自動**，其中ESA會自動使用正確的介面。

```
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
```

案例 4

預設情況下，與集中隔離區的連線是傳輸層安全(TLS)加密的。如果您檢視ESA上的郵件日誌檔案並搜尋SMA上到埠7025的傳送連線ID(DCID)，您可能會看到TLS失敗錯誤，如下所示：

```
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
```

在ESA CLI上運行**tlsverify**時，您會看到相同的結果。

```
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.
```

基於此，用於與SMA協商的**ADH-CAMELLIA256-SHA**密碼會導致SMA無法提供對等證書。進一步調查發現，所有ADH密碼均使用匿名身份驗證，而匿名身份驗證不提供對等證書。**解決方法是消除匿名密碼**。為此，請將傳出密碼清單更改為**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
```

提示：此外，還新增**-SSLv2**，因為這些密碼也是不安全的。

案例 5

無法啟用PVO並顯示這種型別的錯誤消息。

```
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.
```

該錯誤消息可能表示其中一個主機未應用DLP功能金鑰，並且DLP已禁用。解決方式是新增缺失的功能金鑰，並應用與應用了功能金鑰的主機相同的DLP設定。此功能金鑰不一致可能對爆發過濾器、Sophos防病毒和其他功能金鑰產生相同影響。

案例 6

如果在集群配置中存在針對內容、郵件過濾器、DLP和DMARC設定的電腦或組級配置，則PVO的啟用按鈕將呈灰色顯示。為了解決此問題，所有郵件和內容過濾器必須從電腦或組級別移動到群集級別，以及DLP和DMARC設定。或者，也可以從群集中完全刪除具有電腦級別配置的電腦。輸入CLI命令**clusterconfig > removemachine**，然後將其重新加入群集以繼承群集配置。

相關資訊

- 排除SMA上從PVO隔離區到送貨的故障
- ESA群集時PVO遷移嚮導的要求
- 技術支援與文件 - Cisco Systems