集中策略、病毒和爆发检疫(PVO)的ESA不可能启用

目录

简介

本文描述遇到的问题集中的策略、病毒和爆发检疫(PVO)的地方在Cisco电子邮件安全工具(ESA)不可能启用，因为启用按钮变灰并且提供解决方案对问题。

先决条件

要求

Cisco 建议您了解以下主题：

- 如何启用在安全管理设备(SMA)的PVO。
- 如何添加对每个管理的ESA的PVO服务。
- 如何配置PVO的迁移。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- SMA版本8.1和以上
- ESA版本8.0和以上

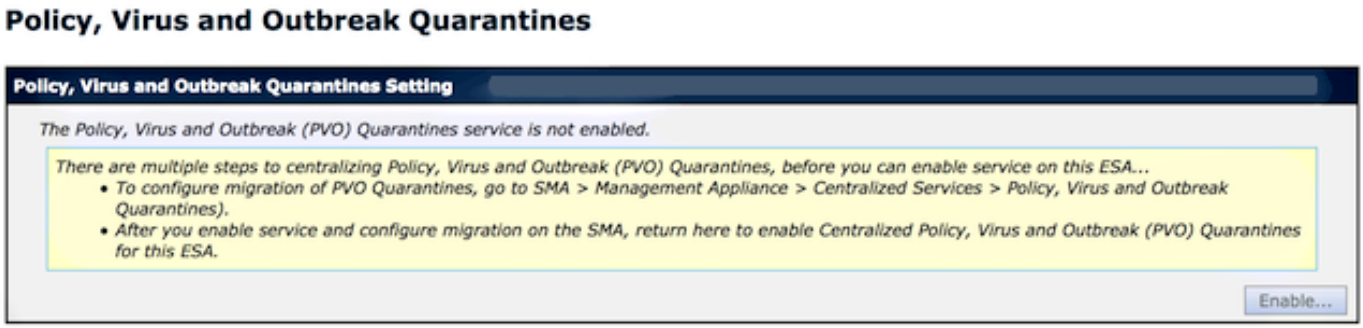
本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

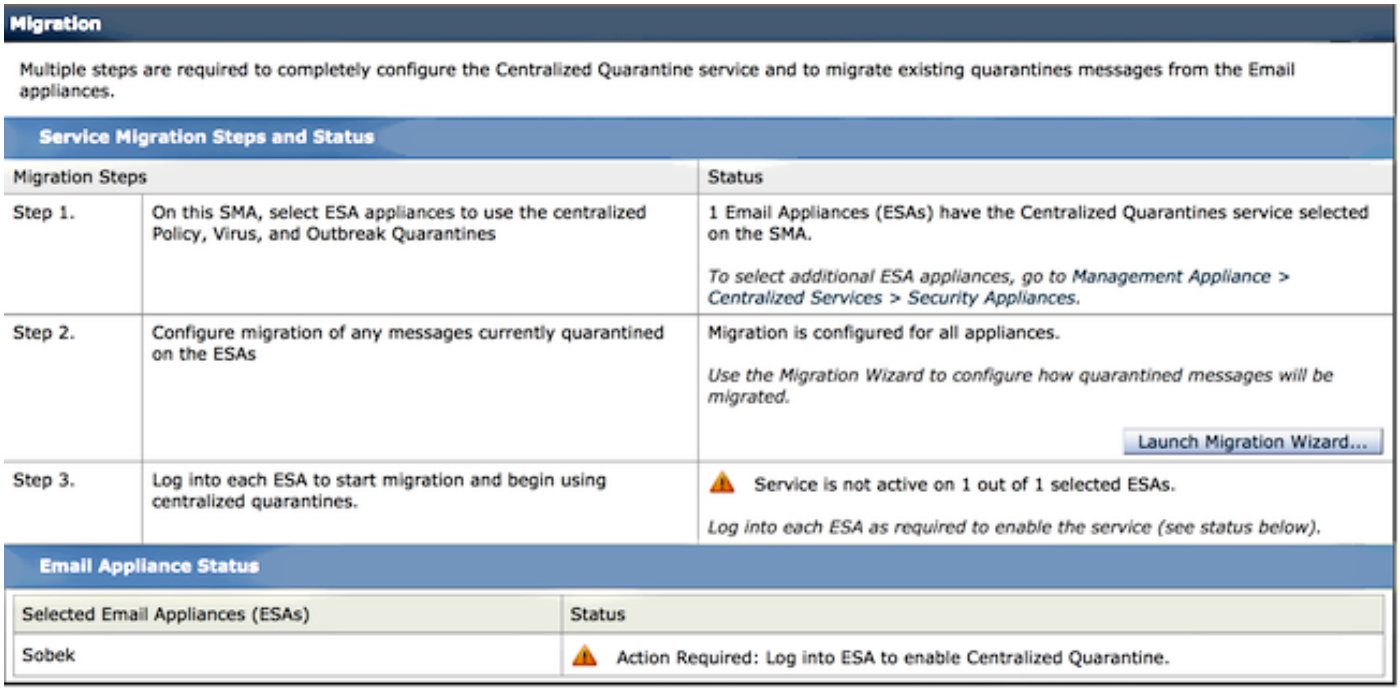
由某些过滤器、策略和扫描操作的已处理在ESA可以被放置到检疫临时地保持他们对于更加进一步的行动。有时，看来PVO在ESA不可能启用，虽然在SMA适当地配置，并且使用了迁移向导。因为ESA不能连接到在波尔特7025的SMA启用在ESA的此功能的按钮通常仍然变灰。

问题

在ESA，启用按钮变灰。



SMA显示不活动的服务和所需操作



解决方案

有几个方案，描述此处。

场景 1

在SMA，请运行**status命令**在CLI为了保证设备在线状态。如果SMA脱机， PVO在ESA不可能启用，因为连接发生故障。

```
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脱机，请运行**恢复**命令为了联机它回到，开始cpq_listener。

```
sma.example.com> resume

Receiving resumed for euq_listener, cpq_listener.
```

场景 2

在您使用SMA的后迁移向导，确认更改是重要的。[Enable…]如果不确认更改，在ESA的按钮保持变灰。

1. 登录SMA，并且与**管理员帐户**，**操作员**(或其他帐户类型)或不是设置的ESA可以执行，但是[Enable…]按钮在ESA侧变灰。
2. 在SMA，请选择**管理设备>集中式服务>Policy、病毒和爆发检疫**。
3. 点击**启动迁移向导**并且选择迁移方法。
4. **提交并且确认**您的更改。

场景 3

如果ESA配置与默认交付接口通过deliveryconfig命令，并且，如果该默认接口没有往SMA的连接，因为位于一不同的子网或那里是没有路由， PVO在ESA不可能启用。

这是与默认配置的交付接口的ESA建立接口**在**：

```
mx.example.com> deliveryconfig

Default interface to deliver mail: In
```

这是从接口的一ESA连通性测试对SMA波尔特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
```

为了解决此问题，请配置默认interace到ESA自动地使用正确接口的**自动**。

```
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
```

场景 4

对集中化检疫的连接是传输层安全(TLS)默认情况下-加密。如果查看在ESA的邮件日志文件并且搜索交付连接ID (DCIDs)给SMA的波尔特7025，您也许发现TLS失败的错误例如此：

```
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
```

当您运行在ESA CLI时的一**tlsverify**，您看到同样。

```
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.
```

基于此， ADH-CAMELLIA256-SHA密码器使用为了协商与SMA造成SMA不能提交对等项证书。进一步调查表示所有ADH密码器使用匿名验证，不提供一对等项证书。**此处修正是排除匿名密码器。**为了执行此，请更改流出的密码器列表对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：并且，因为这些是不安全密码器，请添加-SSLv2。

方案 5

PVO不可能启用并且表示此种错误消息。

```
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
```

错误消息能表明一个主机没有应用的一个DLP功能键，并且DLP禁用。解决方案是添加缺少功能键并且应用DLP设置相同和在有应用的功能键的主机。此功能键不一致也许有与爆发过滤器、Sophos防病毒和其它特性密钥的同样效果。

方案 6

PVO的启用按钮变灰，如果，在集群配置里有计算机或组级配置内容的，消息过滤， DLP和DMARC设置。为了解决此问题，必须从机器或组级团星级别以及DLP和DMARC设置移动所有消息

和内容过滤器。或者，有计算机成水平从集群的配置的您能完全地删除计算机。输入CLI命令clusterconfig > removemachine然后加入它回到集群为了继承集群配置。

相关信息

- 排除故障交付从和对在SMA的PVO检疫
- PVO迁移向导的需求，当ESA是集群
- 技术支持和文档 - Cisco Systems