A política de centralização ESA, o vírus, e a quarentena da manifestação (PVO) não podem ser permitidos

Índice

Introdução

Este documento descreve um problema encontrado onde a política, o vírus, e a quarentena de centralização da manifestação (PVO) não podem ser permitidos na ferramenta de segurança do email de Cisco (ESA) porque o botão Enable Button é esmaecida para fora e oferece uma solução ao problema.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Como permitir PVO no dispositivo do Gerenciamento de segurança (S A).
- Como adicionar o serviço PVO a cada ESA controlado.
- Como configurar a migração de PVO.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 8.1 e mais recente S A
- Versão 8.0 e mais recente ESA

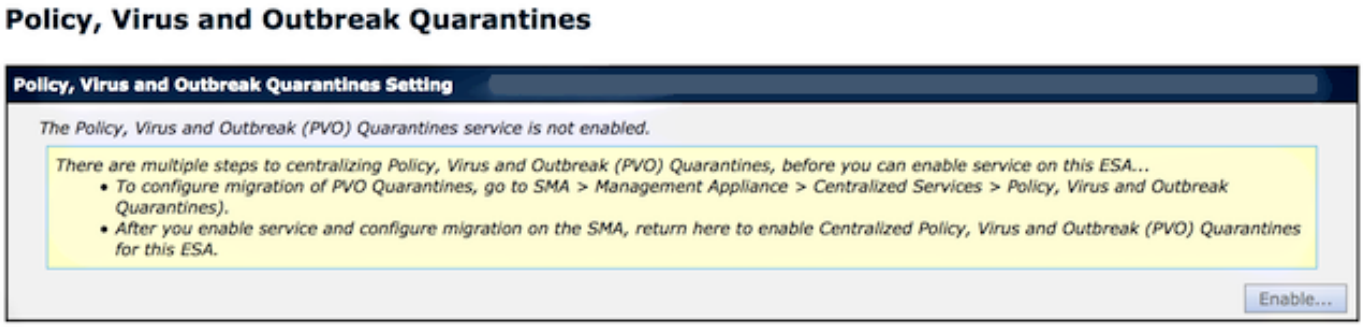
As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

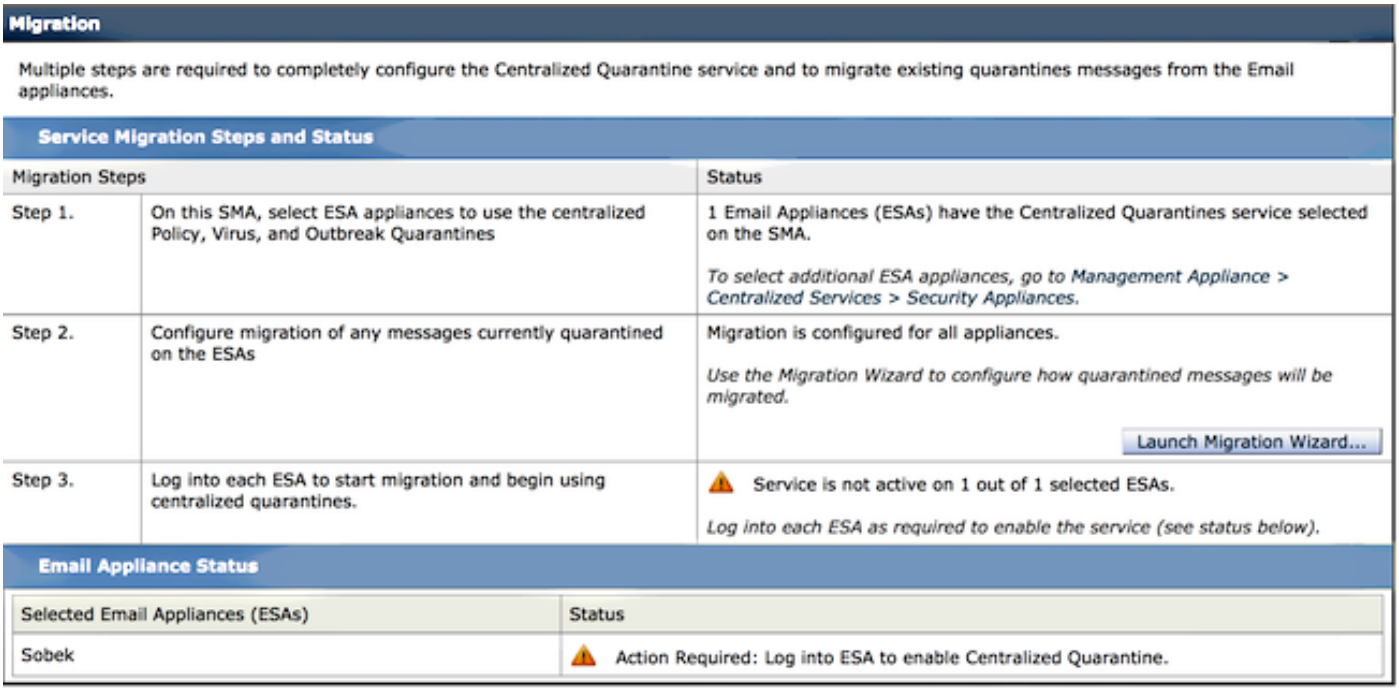
As mensagens processadas por determinados filtros, por políticas, e por operações de exploração em um ESA podem ser colocadas em quarentena para guardá-las temporariamente para uma ação mais adicional. Em alguns casos, parece que o PVO não pode ser permitido no ESA embora seja configurado corretamente no S A e o assistente da migração seja usado. O botão para permitir esta característica no ESA é geralmente ainda esmaecida para fora porque o ESA não pode conectar ao S A na porta 7025.

Problema

No ESA, o botão Enable Button é esmaecida para fora.



As mostras S A prestam serviços de manutenção a não ativo e à ação exigidos



Solução

Há diversas encenações, que são descritas aqui.

Cenário 1

No S A, execute o **comando status no** CLI a fim assegurar-se de que o dispositivo esteja em um estado on-line. Se o S A é autônomo, o PVO não pode ser permitido no ESA porque a conexão falha.

```
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 o S A é autônomo, execute o comando do **resumo** a fim trazê-lo para trás em linha, que começa o cpq_listener.

```
sma.example.com> resume

Receiving resumed for euq_listener, cpq_listener.
```

Cenário 2

Depois que você usa o assistente da migração no S A, é importante comprometer as mudanças. O [Enable…] o botão no ESA permanece esmaecida para fora se você não compromete mudanças.

1. O log no S A e no ESA com a **conta de administrador**, não o **operador** (ou outro tipos da conta) ou a instalação podem ser executados mas o [Enable…] o botão será esmaecida para fora no lado ESA.

2. No S A, escolha o **dispositivo do Gerenciamento > serviços > política, vírus, e quarentena centralizados da manifestação**.

3. Clique o **assistente da migração do lançamento** e escolha um método da migração.

4. **Submeta e comprometa** suas mudanças.

Cenário 3

Se o ESA esteve configurado com uma relação da entrega do padrão através do comando do **deliveryconfig** e se essa interface padrão não tem nenhuma Conectividade para o S A porque reside em uma sub-rede diferente ou lá não é nenhuma rota, o PVO não pode ser permitido no ESA.

Está aqui um ESA com a relação da entrega do padrão configurada para conectar **em**:

```
mx.example.com> deliveryconfig

Default interface to deliver mail: In
```

Está aqui um teste de conectividade ESA da relação **dentro à** porta 7025 S A:

```
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
```

A fim resolver este problema, configurar o interace do padrão ao **automóvel** onde o ESA usa a relação correta automaticamente.

```
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
```

Encenação 4

As conexões à quarentena centralizada são o Transport Layer Security (TLS) - cifrado à revelia. Se você revê o arquivo de registro do correio no ESA e o procura por identificadores de conexão da entrega (DCIDs) à porta 7025 no S A, você pôde ver erros falhados TLS tais como este:

```
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 você executa um **tlsverify no** ESA CLI, você vê o mesmos.

```
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.
```

Baseado nisto, a cifra **ADH-CAMELLIA256-SHA** usada a fim negociar com o S A faz com que o S A não apresenta um certificado de peer. As investigações adicionais revelam que todas as cifras alimentador automático do papel usam a autenticação anônima, que não fornece um certificado de peer. **O reparo aqui é eliminar cifras anônimas**. A fim fazer isto, mude a lista que parte da cifra a **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
```

Tip: Igualmente adicionar **-SSLv2** porque estas são cifras incertas também.

Encenação 5

O PVO não pode ser permitido e mostra este tipo de mensagem de erro.

```
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
```

O Mensagem de Erro pode indicar que um dos anfitriões não tem uma chave de recurso DLP aplicada e o DLP está desabilitado. A solução é adicionar a chave de recurso faltante e aplicar os ajustes DLP idênticos como no host que tem a chave de recurso aplicada. Esta inconsistência da chave de recurso pôde ter o mesmo efeito com filtros da manifestação, Antivirus de Sophos, e chaves dos outros recursos.

Encenação 6

O botão Enable Button para o PVO será esmaecida para fora se, em uma configuração de grânulos há uma configuração da máquina ou do grupo-nível para o índice, mensagem filtra, ajuste DLP, e DMARC. A fim resolver este problema, todos os filtros da mensagem e do índice devem ser movidos do conjunto-nível da máquina ou do grupo-nível assim como dos ajustes DLP e DMARC. Alternativamente, você pode inteiramente remover a máquina que tem a configuração nivelada da máquina do conjunto. Entre no **clusterconfig > no removemachine do** comando CLI e junte-se então lhe de volta ao conjunto a fim herdar a configuração de grânulos.

Informações Relacionadas

- Pesquise defeitos a entrega e à quarentena PVO no S A
- Exigências para o assistente da migração PVO quando o ESA for aglomerado
- Suporte Técnico e Documentação - Cisco Systems