Политика Централизации ESA, Вирус и Карантин Вспышки (PVO) не Могут быть Включены

Содержание

Введение

Этот документ описывает проблему, с которой встречаются, где Политика Централизации, Вирус и Карантин Вспышки (PVO) не могут быть включены на Cisco Email Security Appliance (ESA), потому что кнопка Enable отображается серым и предлагает решение проблемы.

Предварительные условия

Требования

Компания Cisco рекомендует предварительно ознакомиться со следующими предметами:

- Как включить PVO на устройстве управления безопасностью (SMA).
- Как добавить Сервис PVO к каждому управляемому ESA.
- Как настроить миграцию PVO.

Используемые компоненты

Сведения, содержащиеся в данном документе, касаются следующих версий программного обеспечения и оборудования:

- Версия 8.1 SMA и позже
- Версия 8.0 ESA и позже

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Общие сведения

Сообщения, обработанные определенными фильтрами, политикой и операциями сканирования на ESA, могут быть размещены в карантин для временного удержания их для дальнейших действий. В некоторых случаях кажется, что PVO не может быть включен на ESA невзирая на то, что это было должным образом настроено на SMA, и Мастер Миграции использовался. Кнопка для активации этой опции на ESA обычно все еще затенена, потому что ESA не в состоянии соединиться с SMA на порте 7025.

Проблема

На ESA отображается серым кнопка Enable.

SMA показывает сервис, не активный и требуемое действие

Решение

Существует несколько сценариев, которые описаны здесь.

Сценарий 1

На SMA выполненном, команда **статуса** на CLI для обеспечения устройства находится в онлайновом состоянии. Если SMA является офлайновым, PVO не может быть включен на ESA, потому что прерывается связь.

```
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
```

Если SMA является офлайновым, выполните команду **резюме** для возвращения его онлайн, который запускает cpq_listener.

```
sma.example.com> resume

Receiving resumed for euq_listener, cpq_listener.
```

Сценарий 2

После использования Мастера Миграции на SMA важно передать изменения. [Включают...], кнопка на ESA остается затененной, если вы не передаете изменения.

1. Войдите в SMA и ESA с **Учетной записью администратора**, не **, Оператор** (или другие типы учетных записей) или настройка может быть выполнен , но [Включают...], кнопка отобразится серым на стороне ESA.

2. На SMA выберите **Management Appliance> Centralized Services> Policy, Virus и Outbreak Quarantines**.

3. Нажмите **Launch Migration Wizard** и выберите метод миграции.

4. **Отправьте и передайте** свои изменения.

Ситуация 3

Если ESA был настроен с интерфейсом доставки по умолчанию через **deliveryconfig** команду и если тот интерфейс по умолчанию не имеет никакого подключения к SMA, потому что это находится в другой подсети или существует никакой маршрут, PVO не может быть включен на ESA.

Вот ESA с интерфейсом доставки по умолчанию, настроенным для взаимодействия через интерфейс **B**:

```
mx.example.com> deliveryconfig

Default interface to deliver mail: In
```

Вот тест подключения ESA от интерфейса **B** к порту 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
```

Для решения этой проблемы настройте межасе по умолчанию к **Автоматическому**, где ESA

использует корректный интерфейс автоматически.

```
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
```

Сценарий 4

Соединениями с централизованным карантином является Transport Layer Security (TLS) - зашифрованный по умолчанию. Если вы рассматриваете почтовый файл журнала на ESA и ищете Идентификаторы соединения Доставки (DCIDs) к порту 7025 на SMA, вы могли бы видеть, что TLS отказал ошибки, такие как это:

```
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
```

При выполнении tlsverify на CLI ESA вы видите то же.

```
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.
```

На основе этого ADH-CAMELLIA256-SHA шифр, используемый для согласования с SMA, заставляет SMA быть не в состоянии представлять сертификат однорангового узла. Дополнительное исследование показывает, что все шифры ADH используют анонимную аутентификацию, которая не предоставляет сертификат однорангового узла. Исправление здесь должно устранить анонимные шифры. Чтобы сделать это, измените исходящий список шифра на 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
```

Совет: Также добавьте **-SSLv2**, потому что это опасные шифры также.

Сценарий 5

PVO не может быть включен и показывает этот тип сообщения об ошибках.

```
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
```

Сообщение об ошибках может указать, что одному из хостов не применили характерную черту DLP, и DLP отключен. Решение состоит в том, чтобы добавить ключ недостающей возможности и применить параметры настройки DLP, идентичные как на хосте, которому применили характерную черту. Это несоответствие характерной черты могло бы иметь тот же эффект с Фильтрами Вспышки, Антивирусом Sophos и другими характерными чертами.

Сценарий 6

Если, в конфигурации кластера будет конфигурация машины или уровня группы для содержания, фильтров сообщения, DLP и параметров настройки DMARC, кнопка enable для PVO отобразится серым. Для решения этой проблемы все сообщение и фильтры контента должны быть перемещены от машины - или уровень группы к кластерному уровню, а также DLP и параметрам настройки DMARC. Также можно полностью демонтировать машину, которая имеет конфигурацию уровня машины от кластера. Введите команду CLI **clusterconfig> removemachine** и затем присоединитесь к ней назад к кластеру для наследования конфигурации кластера.

Дополнительные сведения

- Доставка устранения неполадок от и до PVO изолирует на SMA

- Требования для Мастера Миграции PVO, когда кластеризован ESA
- Cisco Systems – техническая поддержка и документация