لا يمكن تمكين عزل السياسة والفيروسات والفاشيات (PVO) مركزيا ل ESA

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
معلومات أساسية
المشكلة
الحل
السيناريو 1
السيناريو 2
السيناريو 3
السيناريو 4
السيناريو 5
السيناريو 6
معلومات ذات صلة

المقدمة

يصف هذا المستند مشكلة تمت مواجهتها عند تعذر تمكين الحجر الصحي للسياسة المركزية والفيروسات والفاشية (PVO) على جهاز أمان البريد الإلكتروني من Cisco (ESA) نظرا لأنه يتم مسح زر التمكين ويقدم حلا للمشكلة.

المتطلبات الأساسية

المتطلبات

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- كيفية تمكين PVO على جهاز إدارة الأمان (SMA).
- كيفية إضافة خدمة PVO إلى كل ESA مدار.
- كيفية تكوين ترحيل PVO.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- SMA الإصدار 8.1 والإصدارات الأحدث
- ESA، الإصدار 8.0 والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

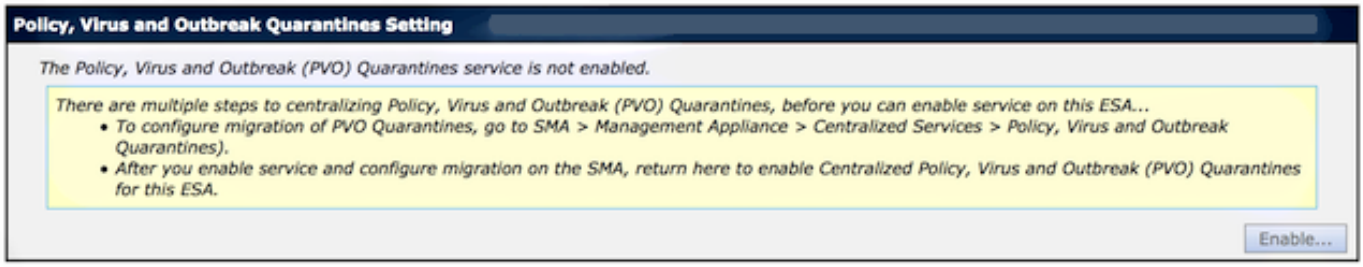
معلومات أساسية

يمكن وضع الرسائل التي تمت معالجتها بواسطة عوامل تصفية وسياسات وعمليات مسح ضوئي معينة على ESA في الحجر الصحي للاحتجاز المؤقت لها لمزيد من الإجراءات. في بعض الحالات، يبدو أنه لا يمكن تمكين PVO على ESA على الرغم من أنه تم تكوينه بشكل صحيح على SMA وتم إستخدام "معالج الترحيل". لا يزال الزر لتمكين هذه الميزة على ESA مبهما عادة لأن ESA غير قادر على الاتصال ب SMA على المنفذ 7025.

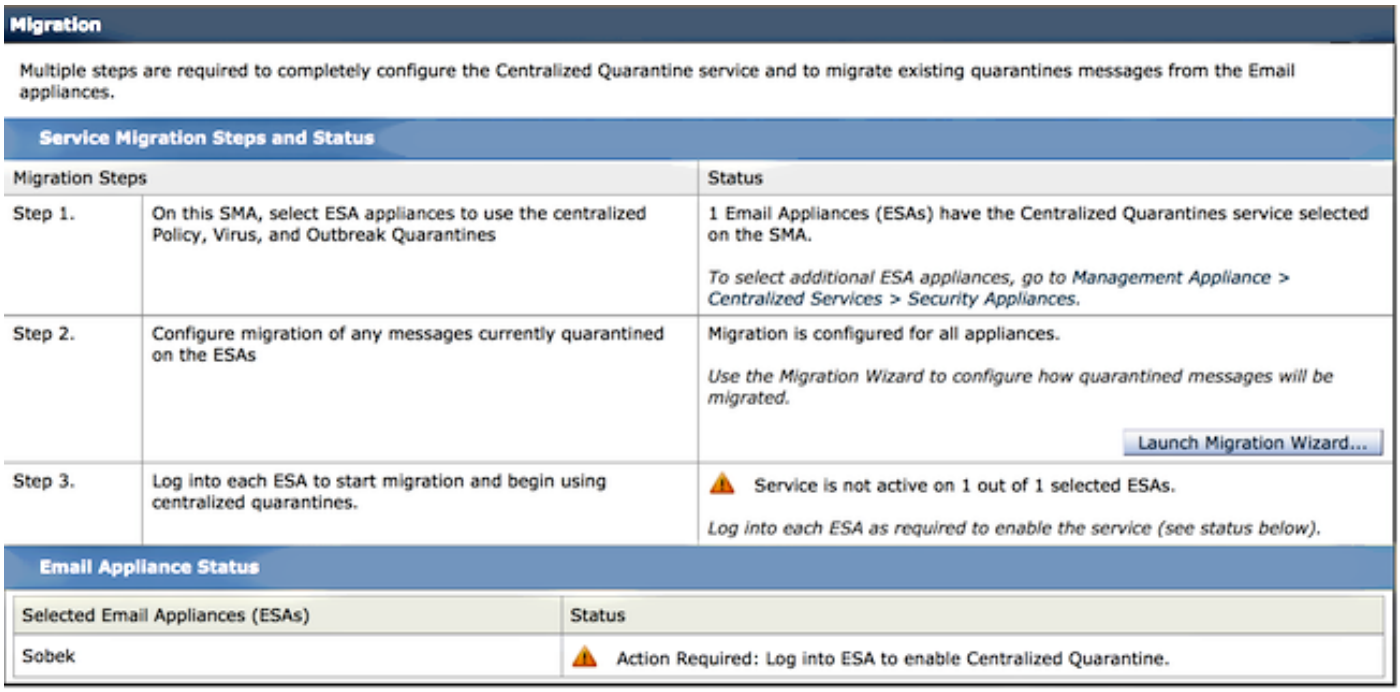
المشكلة

على ESA، يتم مسح زر التمكين.

Policy, Virus and Outbreak Quarantines



تظهر SMA الخدمة غير نشطة والإجراء المطلوب



الحل

وهناك عدة سيناريوهات يرد وصفها هنا.

السيناريو 1

على SMA، قم بتشغيل الأمر **status** على واجهة سطر الأوامر لضمان أن الجهاز في حالة اتصال. إذا كانت SMA غير متصلة، لا يمكن تمكين PVO على ESA بسبب فشل الاتصال.

```
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
```

إذا كانت SMA غير متصلة، فقم بتشغيل الأمر **إستئناف** من أجل إعادته إلى الإنترنت، والذي يقوم بتشغيل cpq_listener.

```
sma.example.com> resume

.Receiving resumed for euq_listener, cpq_listener
```

السيناريو 2

بعد إستخدام "معالج الترحيل" في SMA، من المهم إجراء التغييرات. يبقى الزر [enable...] الموجود في ESA متدرج إذا لم تقم بإجراء تغييرات.

1. قم بتسجيل الدخول إلى SMA و ESA باستخدام حساب **المسؤول**، وليس **عامل التشغيل** (أو أنواع الحسابات الأخرى) أو يمكن إجراء الإعداد ولكن سيتم تصنيف الزر [enable..] إلى الجانب الخاص ب ESA.

2. في SMA ، أختر **جهاز الإدارة > الخدمات المركزية > السياسة والفيروسات والحجر الصحي لتفشي الأمراض**.

3. انقر فوق **تشغيل معالج الترحيل** واختر طريقة ترحيل.

4. **إرسال** التغييرات **وتنفيذها**.

السيناريو 3

إذا تم تكوين ESA بواجهة تسليم افتراضية عبر الأمر **deliveryconfig** وإذا لم تكن تلك الواجهة الافتراضية تحتوي على اتصال ب SMA لأنها موجودة في شبكة فرعية مختلفة أو لا يوجد مسار، فلا يمكن تمكين PVO على ESA.

فيما يلي ESA مع واجهة تسليم افتراضية تم تكوينها لواجهة **في**:

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

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

فيما يلي إختبار اتصال ESA من الواجهة **in** إلى منفذ SMA 7025:

```
mx.example.com> telnet

.Please select which interface you want to telnet from
                                                    Auto .1
                                  (In (192.168.1.1/24: mx.example.com .2
                          (Management (10.172.12.18/24: mgmt.example.com .3
                                                    2 <[1]

                                .Enter the remote hostname or IP address
                                                10.172.12.17 <[]

                                                .Enter the remote port
                                                    7025 <[25]

                                                ...Trying 10.172.12.17
                    telnet: connect to address 10.172.12.17: Operation timed out
                                                telnet: Unable to connect to remote host
```

in order to حللت هذا مشكلة، شكلت التقصير قارن إلى **تلقائي** حيث ال ESA يستعمل القارن صحيح تلقائيا.

```
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
                                                Auto .1
                                  (In (192.168.1.1/24: mx.example.com .2
                          (Management (10.172.12.18/24: mgmt.example.com .3
                                                1 <[1]
```

السيناريو 4

يتم تشفير الاتصالات بالعزل المركزي بواسطة أمان طبقة النقل (TLS) بشكل افتراضي. إذا قمت بمراجعة ملف سجل البريد على ESA والبحث عن معرفات اتصال التسليم (DCIDs) لمنفذ 7025 على SMA، فقد ترى أخطاء فشل TLS مثل:

```
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
```

عندما تقوم بتشغيل **TLSVERIFY** على واجهة سطر الأوامر (CLI) ل ESA، سترى الأمر نفسه.

```
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
```

استنادا إلى هذا، يتسبب تشفير ADH-Camellia256-SHA المستخدم من أجل التفاوض مع SMA في فشل SMA في تقديم شهادة نظير. يكشف المزيد من التحقيق أن كل شفرات ADH تستخدم مصادقة مجهولة، والتي لا توفر شهادة نظير. **النقطة الثابتة هنا هي إزالة الشفرات المجهولة**. للقيام بذلك، قم بتغيير قائمة التشفير الصادرة إلى 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
                                                                                       .SSL v2 .1
                                                                                        SSL v3 .2
                                                                                        TLS v1 .3
                                                                                   SSL v2 and v3 .4
                                                                                SSL v3 and TLS v1 .5
                                                                             SSL v2, v3 and TLS v1 .6
                                                                                               <[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
```

تلميح: أيضا **add-SSLv2** لأنها شفرة غير آمنة أيضا.

السيناريو 5

لا يمكن تمكين PVO ويعرض هذا النوع من رسائل الخطأ.

```
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
```

يمكن أن تشير رسالة الخطأ إلى أن أحد المضيفين لا يحتوي على مفتاح ميزة DLP مطبق و DLP معطل. يكمن الحل في إضافة مفتاح الميزة المفقود وتطبيق إعدادات DLP متطابقة كما هو الحال على المضيف الذي تم تطبيق مفتاح الميزة عليه. قد يكون لعدم اتساق مفتاح الميزة هذا نفس التأثير مع عوامل تصفية التفشي، SOPHOS AntiVirus، ومفاتيح الميزات الأخرى.

السيناريو 6

سيتم حذف زر التمكين الخاص ب PVO إذا كان هناك، في تكوين نظام مجموعة، تكوين على مستوى الجهاز أو المجموعة للمحتوى وعوامل تصفية الرسائل و DLP وإعدادات DMARK. لحل هذه المشكلة، يجب نقل كافة عوامل تصفية الرسائل والمحتوى من مستوى الجهاز أو المجموعة إلى مستوى المجموعة بالإضافة إلى إعدادات DLP و DMARK. بدلا من ذلك، يمكنك إزالة الجهاز الذي يحتوي على تكوين على مستوى الجهاز بالكامل من نظام المجموعة. أدخل أمر واجهة سطر الأوامر (CLI) **clusterconfig > removeAmachine** ثم انضم إليه مرة أخرى إلى نظام المجموعة لترث تكوين نظام المجموعة.

معلومات ذات صلة

- أستكشاف أخطاء التسليم وإصلاحها من عزل PVO وإليه على SMA
- متطلبات معالج ترحيل PVO عندما تكون ESA مجمعة
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).